aws

Guida per l'utente

AWS Site-to-Site VPN

AWS Site-to-Site VPN: Guida per l'utente

Table of Contents

Cos'è AWS Site-to-Site VPN?

Per impostazione predefinita, le istanze avviate in un Amazon VPC non possono comunicare con la propria rete (remota). Puoi abilitare l'accesso alla rete remota dal VPC creando una connessione AWS Site-to-Site VPN (Site-to-Site VPN) e configurando il routing per passare il traffico attraverso la connessione.

Sebbene il termine connessione VPN sia generale, in questa documentazione una connessione VPN si riferisce alla connessione tra il VPC e la propria rete locale. Il VPN da sito a sito supporta le connessioni VPN di sicurezza del protocollo Internet (IPsec).

Indice

Concetti

Di seguito sono riportati i concetti chiave per la Site-to-Site VPN:

- Connessione VPN: una connessione sicura tra le apparecchiature locali e i VPC.
- Tunnel VPN: un collegamento crittografato in cui i dati possono passare dalla rete del cliente da o verso AWS.

  Ogni connessione VPN include due tunnel VPN che è possibile utilizzare contemporaneamente per una disponibilità elevata.
- Gateway del cliente: una risorsa AWS che fornisce informazioni a AWS sul dispositivo gateway del cliente.
- Dispositivo gateway del cliente: un dispositivo fisico o un'applicazione software sul lato della connessione Site-to-Site VPN.
- Gateway di destinazione: un termine generico per l'endpoint VPN sul lato Amazon della connessione VPN Site-to-Site.

- Gateway privato virtuale: un gateway virtuale privato è l'endpoint VPN sul lato Amazon della connessione VPN Site-to-Site che può essere collegato a un singolo VPC.
- Gateway di transito: un hub di transito che può essere utilizzato per interconnettere più VPC e reti On-Premise e come un endpoint VPN per il lato Amazon della connessione VPN Site-to-Site.

Funzioni di Site-to-Site VPN

Le seguenti funzioni sono supportate solo su connessioni AWS Site-to-Site VPN:

- Internet Key Exchange versione 2 (IKEv2)
- NAT Traversal
- ASN a 4 byte nell'intervallo 1-2147483647 per la configurazione VGW (Virtual Private Gateway). Per ulteriori informazioni, consulta Opzioni di gateway del cliente per la connessione Site-to-Site VPN.
- ASN a 2 byte per Customer Gateway (CGW) nell'intervallo 1-65535. Per ulteriori informazioni, consulta Opzioni di gateway del cliente per la connessione Site-to-Site VPN.
- Parametri di CloudWatch
- Indirizzi IP riutilizzabili per gateway del cliente
- Opzioni di crittografia aggiuntive, inclusa la crittografia a 256 bit AES, l'hashing SHA-2 e i gruppi Diffie-Hellman aggiuntivi
- Opzioni tunnel configurabili
- ASN privato personalizzato per il lato Amazon di una sessione BGP
- Certificato privato da una CA subordinata di AWS Private Certificate Authority
- Il traffico IPv6 è supportato solo per le connessioni VPN su un gateway di transito.

Limitazioni di Site-to-Site VPN

Una connessione Site-to-Site VPN presenta le seguenti limitazioni.

- Il traffico IPv6 non è supportato per le connessioni VPN su un gateway virtuale privato.
- Una connessione AWS VPN non supporta il rilevamento della MTU del percorso.

Inoltre, quando utilizzi Site-to-Site VPN prendi in considerazione quanto segue:

- Quando si connettono i VPC a una rete locale comune, si consiglia di utilizzare blocchi CIDR non sovrapposti per le reti.

Utilizzo di Site-to-Site VPN

Puoi creare, accedere e gestire le risorse Site-to-Site VPN utilizzando una qualsiasi delle seguenti interfacce:

- AWS Management Console: fornisce un'interfaccia Web che puoi utilizzare per accedere alle risorse Site-to-Site VPN.
- AWS Command Line Interface (AWS CLI): fornisce comandi per un ampio set di servizi AWS, incluso Amazon VPC, e offre il supporto per Windows, macOS e Linux. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS SDK: forniscono interfacce API specifiche per ogni linguaggio e si prendono carico di molti dettagli della connessione, ad esempio il calcolo delle firme e la gestione dei tentativi di richiesta e degli errori. Per ulteriori informazioni, consulta SDK di AWS.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'API di query è il modo più diretto per accedere ad Amazon VPC, ma richiede che la propria applicazione gestisca dettagli di basso livello, come la generazione di un hash per la firma della richiesta e la gestione degli errori. Per ulteriori informazioni, consulta il documento Riferimento alle API di Amazon EC2.

Prezzi

Ti viene addebitato il costo per ogni ora di connessione VPN in cui la tua connessione VPN è fornita e disponibile. Per ulteriori informazioni, consulta Prezzi di AWS Site-to-Site VPN e della connessione VPN Site-to-Site accelerata.

Ti viene addebitato un costo per il trasferimento dei dati da Amazon EC2 a Internet. Per ulteriori informazioni, consulta Trasferimento dati sulla pagina dei prezzi on demand di Amazon EC2.

Quando crei una connessione VPN accelerata, vengono automaticamente creati e gestiti due acceleratori. Per ogni acceleratore verrà addebitata una tariffa oraria e i costi di trasferimento dati. Per ulteriori informazioni, consulta Prezzi di AWS Global Accelerator.

Funzionamento di AWS Site-to-Site VPN

Una connessione VPN sito-sito è composta dai componenti seguenti:

- Un gateway privato virtuale esistente o un gateway di transito
- Un dispositivo gateway del cliente
- Un gateway del cliente

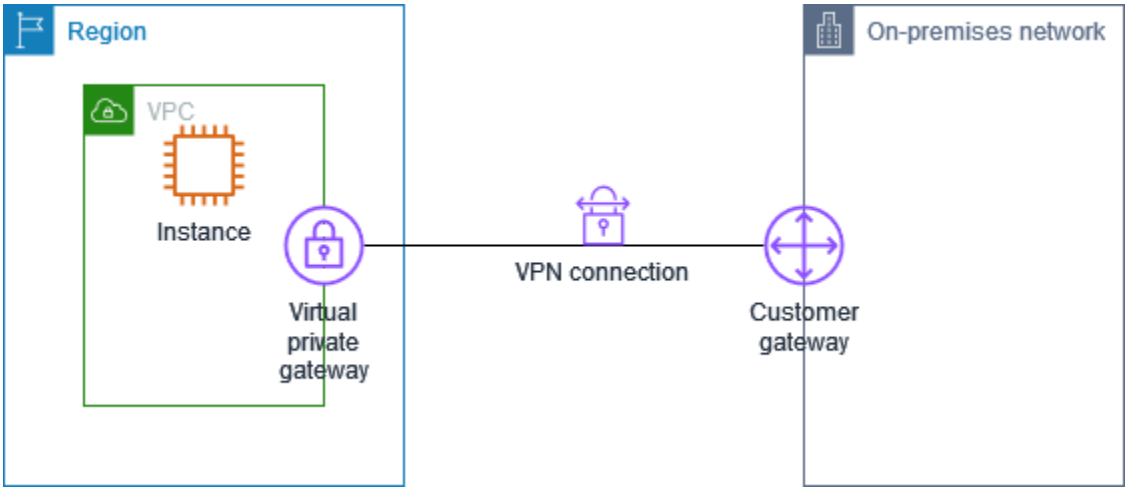
La connessione VPN offre due tunnel VPN tra un gateway privato virtuale o un gateway di transito sul lato AWS e un gateway del cliente sul lato on-premise.

Per ulteriori informazioni sulle quote di Site-to-Site VPN, consulta Quote di VPN sito-sito.

Gateway privato virtuale

Un gateway virtuale privato è il concentratore VPN sul lato Amazon della connessione Site-to-Site VPN. Si crea un gateway privato virtuale e lo si collega a un cloud privato virtuale (VPC) con risorse che devono accedere alla connessione VPN sito-sito.

Il diagramma seguente mostra una connessione VPN tra un VPC e la rete on-premise utilizzando un gateway privato virtuale.



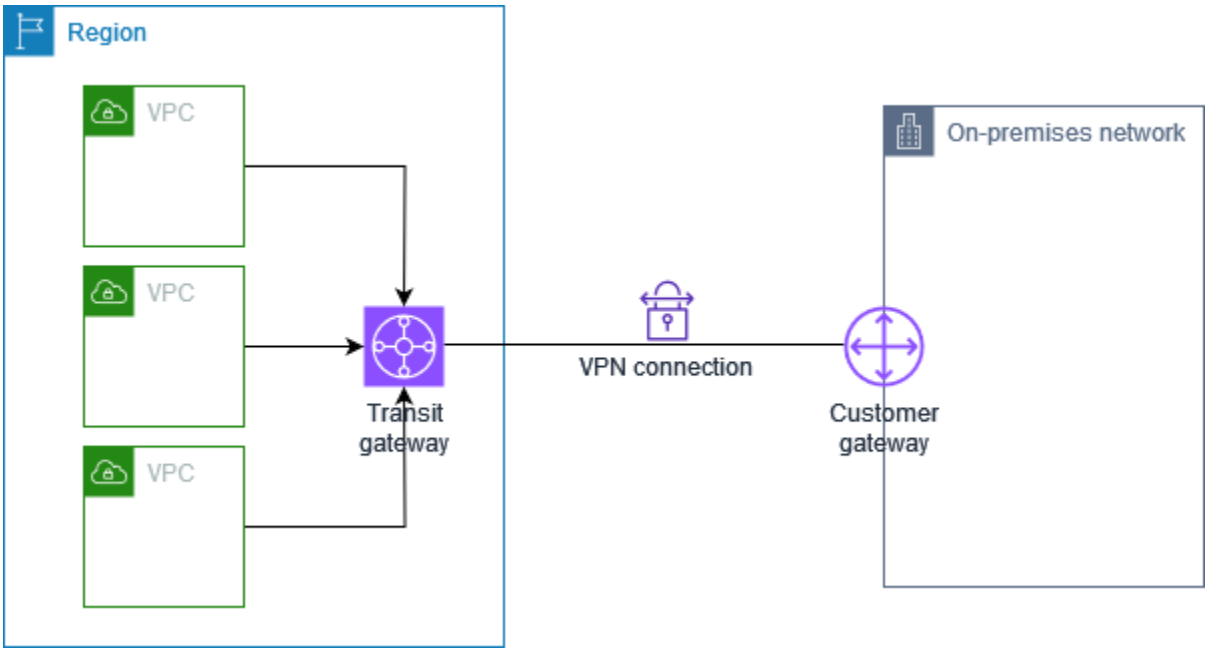
Quando crei un gateway virtuale privato, puoi specificare un Autonomous System Number (ASN) privato per il lato Amazon del gateway. Se non specifichi un ASN, il gateway virtuale privato viene creato con l'ASN predefinito (64512). Dopo aver creato il gateway virtuale privato, non puoi modificare l'ASN. Per controllare l'ASN per il gateway privato virtuale, visualizza i relativi dettagli nella

schermata Gateway privati virtuali nella console Amazon VPC o utilizza il comando describe-vpn-gateways dell'AWS CLI.

Transit Gateway

Un gateway di transito è un hub di transito che è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta Gateway di transito di Amazon VPC. Puoi creare una connessione Site-to-Site VPN come collegamento in un gateway di transito.

Il diagramma seguente mostra una connessione VPN tra più VPC e la rete on-premise utilizzando un gateway di transito. Il gateway di transito dispone di tre collegamenti VPC e un collegamento VPN.



La connessione Site-to-Site VPN su un gateway di transito può supportare il traffico IPv4 o il traffico IPv6 all'interno dei tunnel VPN. Per ulteriori informazioni, consulta Traffico IPv4 e IPv6.

Puoi modificare il gateway target di una connessione Site-to-Site VPN da un gateway virtuale privato in un gateway di transito. Per ulteriori informazioni, consulta the section called “Modifica del gateway di destinazione di una connessione VPN”.

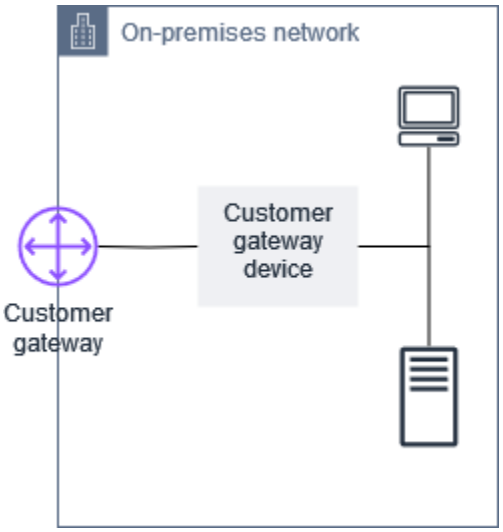
Dispositivo gateway del cliente

Un dispositivo gateway del cliente è un dispositivo fisico o un'applicazione software sul tuo lato della connessione Site-to-Site VPN. Configura il dispositivo in modo per utilizzare la connessione Site-to-Site VPN. Per ulteriori informazioni, consulta Il dispositivo gateway del cliente.

Per impostazione predefinita, il dispositivo gateway del cliente deve richiamare i tunnel per la connessione Site-to-Site VPN generando il traffico e avviando il processo di negoziazione IKE (Internet Key Exchange). Puoi configurare la connessione Site-to-Site VPN per specificare che AWS deve avviare il processo di negoziazione IKE. Per ulteriori informazioni, consulta Opzioni di avvio del tunnel Site-to-Site VPN.

Gateway del cliente

Un gateway del cliente è una risorsa creata in AWS che rappresenta il dispositivo gateway del cliente nella rete locale. Quando crei un gateway del cliente, fornisci ad le informazioni sul dispositiv AWS. Per ulteriori informazioni, consulta the section called “Opzioni gateway del cliente”.

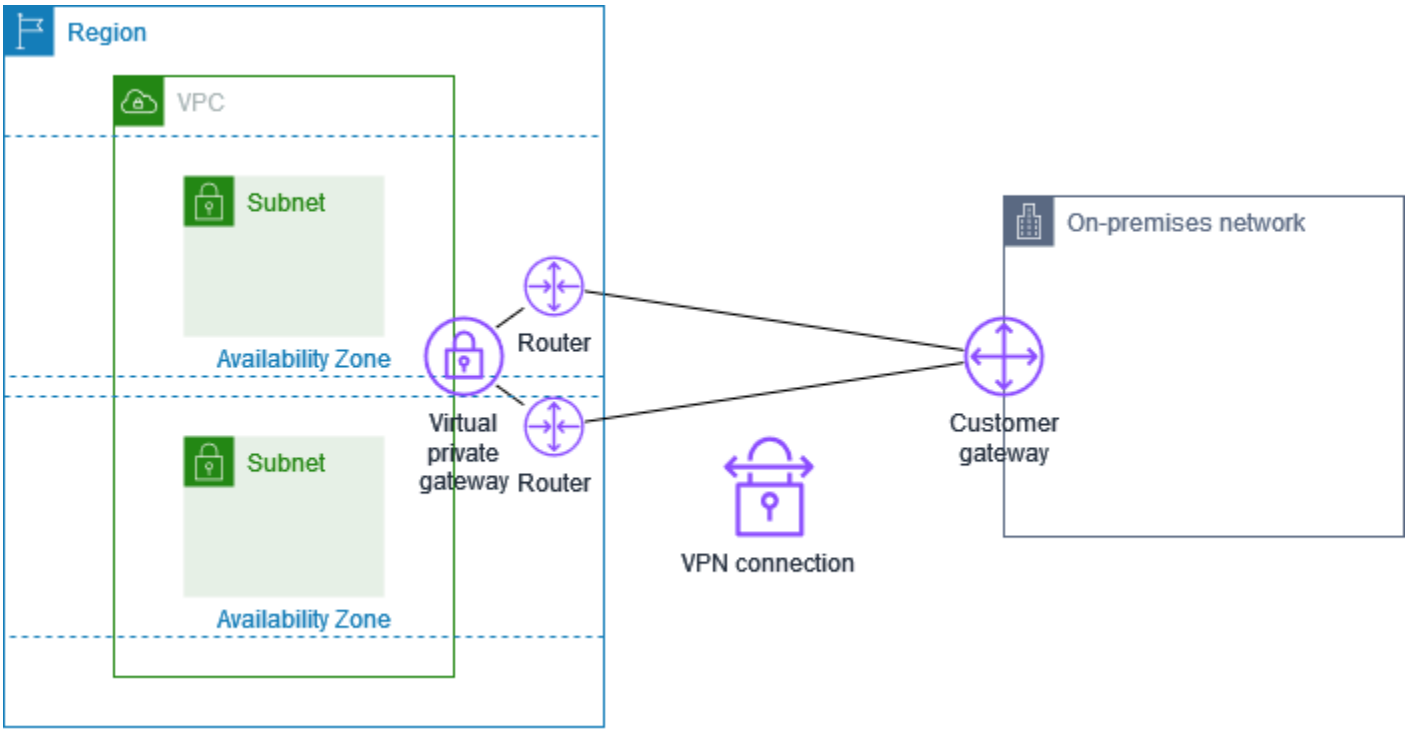


Per utilizzare Amazon VPC come connessione Site-to-Site VPN, l'utente o l'amministratore di rete deve anche configurare il dispositivo o l'applicazione gateway del cliente nella rete remota. Quando crei la connessione Site-to-Site VPN, riceverai le informazioni di configurazione richieste e l'amministratore di rete esegue in genere questa configurazione. Per informazioni sui requisiti e sulla configurazione del gateway del cliente, consulta Il dispositivo gateway del cliente.

Opzioni di tunnel per la connessione Site-to-Site VPN

Utilizza una connessione Site-to-Site VPN per connettere la rete remota a un VPC. Ogni connessione VPN Site-to-Site dispone di due tunnel, in cui ogni tunnel utilizza un indirizzo IP pubblico. È importante configurare Entrambi i tunnel per la ridondanza. Quando un tunnel diventa non disponibile (ad esempio, inattivo per manutenzione), il traffico di rete viene instradato automaticamente al tunnel disponibile per tale connessione Site-to-Site VPN specifica.

Nel seguente diagramma vengono mostrati i due tunnel di una connessione VPN. Ogni tunnel termina in una zona di disponibilità diversa per fornire una maggiore disponibilità. Il traffico proveniente dalla rete on-premise ad AWS utilizza entrambi i tunnel. Il traffico da AWS verso la rete on-premise preferisce uno dei tunnel, ma può eseguire automaticamente il failover sull'altro tunnel in caso di guasto sul lato AWS.



Quando crei una connessione Site-to-Site VPN, scarica una file di configurazione specifico per il dispositivo gateway del cliente contenente informazioni per configurare il dispositivo, incluse informazioni per configurare ogni tunnel. Facoltativamente puoi specificare alcune delle opzioni tunnel quando crei la connessione Site-to-Site VPN. In caso contrario, AWS fornisce valori predefiniti.

> **Note**
>
> Gli endpoint del tunnel Site-to-Site VPN valutano le proposte del gateway del cliente a partire dal valore configurato più basso dall'elenco riportato di seguito, indipendentemente dall'ordine della proposta del gateway del cliente. È possibile utilizzare il commando `modify-vpn-connection-options` per limitare l'elenco delle opzioni che gli endpoint AWS accetteranno. Per ulteriori informazioni, consulta modify-vpn-connection-options nella Guida di riferimento alla riga di comando di Amazon EC2.

Di seguito sono riportate le opzioni tunnel che è possibile configurare.

Timeout Dead Peer Detection (DPD)

La durata in secondi dopo la quale si verifica il timeout DPD. Un timeout DPD di 40 secondi significa che l'endpoint VPN considererà il peer morto 30 secondi dopo il primo keep-alive fallito. Puoi specificare una valore maggiore o uguale a 30.

Impostazione predefinita: 40

Operazione di timeout DPD

L'azione da eseguire dopo il timeout di rilevamento del peer morto (DPD). È possibile specificare le forme seguenti:

- `Clear`: terminare la sessione IKE quando si verifica il timeout DPD (arrestare il tunnel e cancellare i percorsi)
- `None`: non eseguire alcuna azione quando si verifica un timeout DPD
- `Restart`: riavviare la sessione IKE quando si verifica il timeout DPD

Per ulteriori informazioni, consulta Opzioni di avvio del tunnel Site-to-Site VPN.

Default: `Clear`

Opzioni di registrazione VPN

Con i registri VPN sito-sito, è possibile accedere ai dettagli sulla creazione del tunnel IP Security (IPSec), le negoziazioni Internet Key Exchange (IKE) e i messaggi di protocollo Dead Peer Detection (DPD).

Per ulteriori informazioni, consulta AWS Site-to-Site VPN registri.

Formati di registro disponibili: `json`, `text`

Versioni IKE

Le versioni IKE consentite per il tunnel VPN. Puoi specificare uno o più dei valori predefiniti.

`ikev1`, `ikev2` (impostazione predefinita)

CIDR IPv4 tunnel interno

L'intervallo di indirizzi IPv4 interni del tunnel VPN. Puoi specificare un blocco CIDR di dimensione /30 dall'intervallo `169.254.0.0/16`. Il blocco CIDR devono essere univoco per tutte le connessioni Site-to-Site VPN che utilizzano lo stesso gateway virtuale privato.

> **Note**
>
> Il blocco CIDR non deve essere univoco per tutte le connessioni su un gateway di transito. Tuttavia, se non sono univoci, può verificarsi un conflitto sul gateway del cliente. Procedi con attenzione quando riutilizzi lo stesso blocco CIDR su più connessioni Site-to-Site VPN su un gateway di transito.

I seguenti blocchi CIDR sono riservati e non possono essere utilizzati:

- `169.254.0.0/30`
- `169.254.1.0/30`
- `169.254.2.0/30`
- `169.254.3.0/30`
- `169.254.4.0/30`
- `169.254.5.0/30`
- `169.254.169.252/30`

Impostazione predefinita: un blocco CIDR IPv4 di dimensione /30 dall'intervallo `169.254.0.0/16`.

CIDR IPv6 tunnel interno

(Solo connessioni VPN IPv6) Intervallo di indirizzi IPv6 interni per il tunnel VPN. Puoi specificare un blocco CIDR di dimensione /126 dall'intervallo `fd00::/8` locale. Il blocco CIDR deve essere univoco per tutte le connessioni Site-to-Site VPN che utilizzano lo stesso gateway di transito.

Impostazione predefinita: un blocco CIDR IPv6 di dimensione /126 dall'intervallo `fd00::/8` locale.

CIDR rete IPv4 locale

(Facoltativo) Per CIDR di rete IPv4 locale, specificare l'intervallo CIDR IPv4 sul lato customer gateway (on-premises) a cui è consentito comunicare attraverso i tunnel VPN.

Impostazione predefinita: 0.0.0.0/0

CIDR rete IPv4 remota

(Solo connessione VPN IPv4) L'intervallo CIDR IPv4 sul lato AWS a cui è consentito comunicare attraverso i tunnel VPN.

Impostazione predefinita: 0.0.0.0/0

CIDR rete IPv6 locale

(Solo connessione VPN IPv6) Intervallo CIDR IPv6 sul lato customer gateway (on-premises) a cui è consentito comunicare tramite i tunnel VPN.

Impostazione predefinita: 0

CIDR rete IPv6 remota

(Solo connessione VPN IPv6) L'intervallo CIDR IPv6 sul lato AWS a cui è consentito comunicare attraverso i tunnel VPN.

Impostazione predefinita: 0

Numeri di gruppo fase 1 Diffie-Hellman (DH)

I numeri di gruppo DH consentiti per il tunnel VPN per la fase 1 delle negoziazioni IKE. Puoi specificare uno o più dei valori predefiniti.

Impostazione predefinita: 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Numeri di gruppo fase 2 Diffie-Hellman (DH)

I numeri di gruppo DH consentiti per il tunnel VPN per la fase 2 delle negoziazioni IKE. Puoi specificare uno o più dei valori predefiniti.

Impostazione predefinita: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Algoritmi di crittografia fase 1

Gli algoritmi di crittografia consentiti per il tunnel VPN per la fase 1 delle negoziazioni IKE. Puoi specificare uno o più dei valori predefiniti.

Impostazione predefinita: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Algoritmi di crittografia fase 2

Gli algoritmi di crittografia consentiti per il tunnel VPN per la fase 2 delle negoziazioni IKE. Puoi specificare uno o più dei valori predefiniti.

Impostazione predefinita: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Algoritmi di integrità fase 1

Gli algoritmi di integrità consentiti per il tunnel VPN per la fase 1 delle negoziazioni IKE. Puoi specificare uno o più dei valori predefiniti.

Di Default: SHA1, SHA2-256, SHA2-384, SHA2-512

Algoritmi di integrità fase 2

Gli algoritmi di integrità consentiti per il tunnel VPN per la fase 2 delle negoziazioni IKE. Puoi specificare uno o più dei valori predefiniti.

Di Default: SHA1, SHA2-256, SHA2-384, SHA2-512

Durata della fase 1

> **Note**
>
> AWS avvia la reimpostazione delle chiavi con i valori di temporizzazione impostati nei campi Durata della fase 1 e Durata della fase 2. Se tali durate sono diverse dai valori di handshake negoziati, ciò potrebbe interrompere la connettività del tunnel.

La durata in secondi per la fase 1 delle negoziazioni IKE. Puoi specificare un numero compreso tra 900 e 28.800.

Impostazione predefinita: 28.800 (8 ore)

Durata della fase 2

> **Note**
>
> AWS avvia la reimpostazione delle chiavi con i valori di temporizzazione impostati nei campi Durata della fase 1 e Durata della fase 2. Se tali durate sono diverse dai valori di handshake negoziati, ciò potrebbe interrompere la connettività del tunnel.

La durata in secondi per la fase 2 delle negoziazioni IKE. Puoi specificare un numero compreso tra 900 e 3.600. Il numero specificato deve essere inferiore al numero di secondi di durata della fase 1.

Impostazione predefinita: 3.600 (1 ora)

Chiave precondivisa (PSK)

La chiave precondivisa (PSK) per stabilire l'associazione di sicurezza Internet Key Exchange (IKE) tra il gateway di destinazione e il gateway del cliente.

La PSK deve Essere compresa tra 8 e 64 caratteri di lunghezza e non può iniziare con zero (0). Sono consentiti caratteri alfanumerici, spazi, trattini, punti (.) e trattini bassi (_).

Impostazione predefinita: una stringa alfanumerica di 32 caratteri.

Fuzz di emissione nuova chiave

La percentuale della finestra di rekey (determinata dal tempo di margine di rekey) entro la quale il tempo di rekey viene selezionato in modo casuale.

È possibile specificare un valore percentuale compreso tra 0 e 100.

Impostazione predefinita: 100

Tempo di margine di emissione nuova chiave

Il tempo di margine in secondi prima che scadano la fase 1 e la fase 2, durante le quali il lato AWS della connessione VPN esegue una emissione nuova chiave IKE.

Puoi specificare un numero compreso tra 60 e metà del valore di durata della fase 2.

L'ora esatta di emissione nuova chiave viene selezionata in modo casuale in base al valore di fuzz di emissione nuova chiave.

Impostazione predefinita: 270 (4,5 minuti)

Pacchetti dimensioni finestra di riproduzione

Il numero di pacchetti in una finestra di riproduzione IKE.

Puoi specificare un valore compreso tra 64 e 2048.

Impostazione predefinita: 1024

Azione di avvio

L'azione da intraprendere quando si stabilisce il tunnel per una connessione VPN. È possibile specificare le forme seguenti:

- `Start`: AWS avvia la negoziazione IKE per aprire il tunnel. Supportato solo se il gateway del cliente è configurato con un indirizzo IP.
- `Add`: il dispositivo gateway del cliente deve avviare la negoziazione IKE per attivare il tunnel.

Per ulteriori informazioni, consulta Opzioni di avvio del tunnel Site-to-Site VPN.

Default: `Add`

Controllo del tunnel

Il controllo del ciclo di vita degli endpoit del tunnel consente di controllare la pianificazione delle sostituzioni degli endpoint.

Per ulteriori informazioni, consulta Controllo del ciclo di vita dell'endpoint del tunnel.

Default: `Off`

Puoi specificare le opzioni di tunnel quando crei una connessione Site-to-Site VPN oppure modifichi le opzioni di tunnel per una connessione VPN esistente. Per ulteriori informazioni, consulta i seguenti argomenti:

- Fase 5: creazione di una connessione VPN
- Modifica delle opzioni del tunnel per Site-to-Site VPN

Opzioni di autenticazione del tunnel Site-to-Site VPN

Puoi utilizzare chiavi precondivise o certificati per autenticare gli endpoint del tunnel Site-to-Site VPN.

Chiavi precondivise

Una chiave precondivisa è l'opzione di autenticazione predefinita.

Una chiave precondivisa è un'opzione del tunnel Site-to-Site VPN che puoi specificare quando crei un tunnel Site-to-Site VPN.

Una chiave precondivisa è una stringa che immetti quando configuri il dispositivo gateway del cliente. Se non specifichi una stringa, ne viene generata automaticamente una. Per ulteriori informazioni, consulta Il dispositivo gateway del cliente.

Certificato privato di AWS Private Certificate Authority

Se non desideri utilizzare chiavi precondivise, puoi utilizzare un certificato privato da AWS Private Certificate Authority per autenticare la VPN.

Il certificato privato deve essere creato da una CA subordinata utilizzando AWS Private Certificate Authority (CA privata AWS). Per firmare la CA subordinata ACM, puoi utilizzare una CA root ACM o

una CA esterna. Per informazioni sulla creazione di un certificato privato, consulta la sezione relativa alla Creazione e gestione di una CA privata nella Guida per l'utente di AWS Private Certificate Authority .

Per generare e utilizzare il certificato per il lato AWS dell'endpoint del tunnel VPN site-to-site è necessario creare un ruolo collegato ai servizi. Per ulteriori informazioni, consulta the section called "Ruoli collegati ai servizi".

Dopo aver generato il certificato privato, specifica il certificato quando crei il gateway del cliente e quindi applicalo al dispositivo gateway del cliente.

Se non specifichi l'indirizzo IP del dispositivo gateway del cliente, l'indirizzo IP non viene controllato. Questa operazione consente di spostare il dispositivo gateway del cliente in un indirizzo IP diverso senza dover riconfigurare la connessione VPN.

Opzioni di avvio del tunnel Site-to-Site VPN

Per impostazione predefinita, il dispositivo gateway del cliente deve richiamare i tunnel per la connessione Site-to-Site VPN generando il traffico e avviando il processo di negoziazione IKE (Internet Key Exchange). Puoi configurare i tunnel VPN per specificare che AWS deve invece avviare o riavviare il processo di negoziazione IKE.

Opzioni di avvio IKE del tunnel VPN

Sono disponibili le seguenti opzioni di avvio IKE. Puoi implementare una o entrambe le opzioni per uno o entrambi i tunnel nella connessione Site-to-Site VPN. Vedi Opzioni per tunnel VPN per maggiori dettagli su queste e altre impostazioni delle opzioni di tunnel.

- Azione di avvio: l'azione da intraprendere quando si stabilisce il tunnel VPN per una connessione VPN nuova o modificata. Per impostazione predefinita, il dispositivo gateway cliente avvia il processo di negoziazione IKE per attivare il tunnel. È possibile specificare che AWS deve invece avviare il processo di negoziazione IKE.
- Azione di timeout DPD: l'azione da eseguire dopo il timeout del rilevamento peer morto (DPD). Per impostazione predefinita, la sessione IKE viene interrotta, il tunnel si abbassa e i route vengono rimossi. È possibile specificare che AWS deve riavviare la sessione IKE quando si verifica il timeout DPD oppure specificare che non AWS deve eseguire alcuna azione quando si verifica il timeout DPD.

Regole e limitazioni

Si applicano le le seguenti regole e limitazioni:

- Per avviare la negoziazione IKE, è AWS necessario l'indirizzo IP pubblico del dispositivo gateway del cliente. Se hai configurato l'autenticazione basata su certificati per la tua connessione VPN e non hai specificato un indirizzo IP quando hai creato la risorsa Customer Gateway in AWS, devi creare un nuovo gateway cliente e specificare l'indirizzo IP. Quindi, modificare la connessione VPN e specificare il nuovo gateway cliente. Per ulteriori informazioni, consulta Modifica del gateway del cliente per una connessione VPN site-to-site.
- L'avvio IKE (azione di avvio) dal AWS lato della connessione VPN è supportato solo per IKEv2.
- Se si utilizza l'iniziazione IKE dal AWS lato della connessione VPN, non include un'impostazione di timeout. Cercherà continuamente di stabilire una connessione finché non ne verrà stabilita una. Inoltre, il AWS lato della connessione VPN riavvierà la negoziazione IKE quando riceverà un messaggio SA di eliminazione dal gateway del cliente.
- Se il dispositivo gateway del cliente è protetto da un firewall o da un altro dispositivo che utilizza NAT (Network Address Translation), deve essere configurata un'identità (IDr). Per ulteriori informazioni su IDr, vedere RFC 7296.

Se non configuri l'avvio IKE AWS lateralmente per il tunnel VPN e la connessione VPN subisce un periodo di inattività (in genere 10 secondi, a seconda della configurazione), il tunnel potrebbe interrompersi. Per evitare ciò, è possibile utilizzare uno strumento di monitoraggio della rete per generare ping keepalive.

Utilizzo delle opzioni di avvio del tunnel VPN

Per ulteriori informazioni sull'utilizzo delle opzioni di avvio del tunnel VPN, vedere i seguenti argomenti:

- Per creare una nuova connessione VPN e specificare le opzioni di avvio del tunnel VPN: Fase 5: creazione di una connessione VPN
- Per modificare le opzioni di avvio del tunnel VPN per una connessione VPN esistente: Modifica delle opzioni del tunnel per Site-to-Site VPN

Sostituzioni degli endpoint del tunnel Site-to-Site VPN

La connessione Site-to-Site VPN è costituita da due tunnel VPN per la ridondanza. A volte uno o entrambi gli endpoint del tunnel VPN vengono sostituiti quando AWS esegue aggiornamenti del tunnel o quando modifichi la connessione VPN. Durante la sostituzione di un endpoint del tunnel, la connettività attraverso il tunnel potrebbe interrompersi durante il provisioning del nuovo endpoint del tunnel.

Argomenti

Sostituzioni degli endpoint avviati dal cliente

Quando modifichi i seguenti componenti della connessione VPN, uno o entrambi gli endpoint del tunnel vengono sostituiti.

Modifica	Azione API	Impatto del tunnel
Modifica il gateway di destinazione per la connessione VPN	ModifyVpnConnection	Entrambi i tunnel non sono disponibili mentre viene eseguito il provisioning di nuovi endpoint del tunnel.
Modifica il gateway del cliente per la connessione VPN	ModifyVpnConnection	Entrambi i tunnel non sono disponibili mentre viene eseguito il provisioning di nuovi endpoint del tunnel.
Modifica le opzioni di connessione VPN	ModifyVpnConnectionOptions	Entrambi i tunnel non sono disponibili mentre viene eseguito il provisioning di nuovi endpoint del tunnel.

Modifica	Azione API	Impatto del tunnel
Modifica le opzioni del tunnel VPN	ModifyVpnTunnelOptions	Il tunnel modificato non è disponibile durante l'aggiorn amento.

Sostituzioni degli endpoint gestiti da AWS

AWS Site-to-Site VPN è un servizio gestito e applica periodicamente gli aggiornamenti agli endpoint del tunnel VPN. Questi aggiornamenti si verificano per una serie di motivi, tra cui i seguenti:

- Per applicare gli aggiornamenti generali, ad esempio patch, miglioramenti alla resilienza e altri miglioramenti
- Per ritirare l'hardware sottostante
- Quando il monitoraggio automatico determina che un endpoint del tunnel VPN non è integro

AWS applica gli aggiornamenti degli endpoint a un tunnel della connessione VPN alla volta. Durante l'aggiornamento dell'endpoint del tunnel, la connessione VPN potrebbe determinare una breve perdita di ridondanza. È quindi importante configurare entrambi i tunnel nella connessione VPN per un'elevata disponibilità.

Controllo del ciclo di vita dell’endpoint del tunnel

Il controllo del ciclo di vita degli endpoint del tunnel fornisce il controllo sulla pianificazione delle sostituzioni degli endpoint e può aiutare a ridurre al minimo le interruzioni della connettività durante le sostituzioni degli endpoint dei tunnel AWS gestiti. Con questa funzionalità, puoi scegliere di accettare gli aggiornamenti AWS gestiti degli endpoint del tunnel nel momento migliore per la tua azienda. Utilizza questa funzione se hai esigenze aziendali a breve termine o puoi supportare un solo tunnel per connessione VPN.

> **Note**
>
> In rare circostanze, AWS potrebbe applicare immediatamente gli aggiornamenti critici agli endpoint del tunnel, anche se la funzionalità di controllo del ciclo di vita degli endpoint del tunnel è abilitata.

Argomenti

Come funziona il controllo del ciclo di vita degli endpoint del tunnel

Attiva la funzionalità di controllo del ciclo di vita degli endpoint del tunnel per i singoli tunnel all'interno di una connessione VPN. Può essere abilitato al momento della creazione della VPN o modificando le opzioni del tunnel per una connessione VPN esistente.

Dopo aver abilitato il controllo del ciclo di vita degli endpoint del tunnel, otterrai ulteriore visibilità sui prossimi eventi di manutenzione del tunnel in due modi:

- Riceverai notifiche AWS Health per le prossime sostituzioni degli endpoint del tunnel.
- Lo stato della manutenzione in sospeso, insieme ai timestamp della manutenzione auto-applicata dopo e dell'ultima manutenzione applicata, può essere visualizzato in AWS Management Console o utilizzando il comando AWS CLI get-vpn-tunnel-replacement-status.

Quando è disponibile la manutenzione dell'endpoint del tunnel, avrai la possibilità di accettare l'aggiornamento nel momento che ritieni opportuno, prima che la manutenzione specificata venga auto-applicata dopo il timestamp.

Se non applichi gli aggiornamenti prima della Manutenzione auto-applicata dopo la data, AWS eseguirà automaticamente la sostituzione dell'endpoint del tunnel subito dopo, come parte del normale ciclo di aggiornamento di manutenzione.

Abilita il controllo del ciclo di vita degli endpoint del tunnel

È possibile abilitare questa funzionalità utilizzando AWS Management Console o AWS CLI.

> **Note**
>
> Per impostazione predefinita, quando si attiva la funzionalità per una connessione VPN esistente, verrà avviata contemporaneamente la sostituzione dell'endpoint del tunnel. Se si desidera attivare la funzionalità, ma non avviare immediatamente la sostituzione dell'endpoint del tunnel, è possibile utilizzare l'opzione di sostituzione del tunnel con esclusione del tunnel.

Existing VPN connection

I passaggi seguenti mostrano come abilitare il controllo del ciclo di vita degli endpoint del tunnel su una connessione VPN esistente.

Per abilitare il controllo del ciclo di vita degli endpoint del tunnel utilizzando AWS Management Console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione appropriata in Connessioni VPN.
4. Selezionare Operazioni, Modifica opzioni tunnel VPN.
5. Selezionare il tunnel che si desidera modificare scegliendo il Tunnel VPN esterno all'indirizzo IP.
6. In Controllo del ciclo di vita dell’endpoint del tunnel, seleziona la casella di controllo Abilita.
7. (Facoltativo) Seleziona Salta la sostituzione del tunnel.
8. Seleziona Salva modifiche.

Per abilitare il controllo del ciclo di vita degli endpoint del tunnel utilizzando AWS CLI

Usa il comando modify-vpn-tunnel-options per attivare il controllo del ciclo di vita degli endpoint del tunnel.

New VPN connection

I passaggi seguenti mostrano come abilitare il controllo del ciclo di vita degli endpoint del tunnel durante la creazione di una nuova connessione VPN.

Per abilitare il controllo del ciclo di vita degli endpoint del tunnel durante la creazione di una nuova connessione VPN utilizzando AWS Management Console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Site-to-Site VPN Connections (Connessioni VPN site-to-site).
3. Scegliere Create VPN Connection (Crea connessione VPN).
4. Nelle sezioni relative alle opzioni Tunnel 1 e opzioni Tunnel 2, in Controllo del ciclo di vita dell'endpoint del tunnel, seleziona Abilita.
5. Scegliere Create VPN Connection (Crea connessione VPN).

Per abilitare il controllo del ciclo di vita degli endpoint del tunnel durante la creazione di una nuova connessione VPN utilizzando AWS CLI

Usa il comando create-vpn-connection per attivare il controllo del ciclo di vita degli endpoint del tunnel.

Verifica se il controllo del ciclo di vita degli endpoint del tunnel è abilitato

È possibile verificare se il controllo del ciclo di vita degli endpoint del tunnel è abilitato su un tunnel VPN esistente utilizzando AWS Management Console o l'interfaccia a riga di comando.

Per verificare se il controllo del ciclo di vita degli endpoint del tunnel è abilitato utilizzando AWS Management Console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione appropriata in Connessioni VPN.
4. Seleziona la scheda Dettagli del tunnel.
5. Nei dettagli del tunnel, cerca Controllo del ciclo di vita dell'endpoint del tunnel, che segnalerà se la funzionalità è abilitata o disattivata.

Per verificare se il controllo del ciclo di vita degli endpoint del tunnel è abilitato utilizzando AWS CLI

Usa il comando describe-vpn-connections per verificare se il controllo del ciclo di vita degli endpoint del tunnel è abilitato.

Verifica gli aggiornamenti disponibili

Dopo aver abilitato la funzionalità di controllo del ciclo di vita, puoi determinare se è disponibile un aggiornamento di manutenzione per la connessione VPN tramite AWS Management Console o la CLI.

Per verificare la presenza di aggiornamenti disponibili, utilizzare AWS Management Console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione appropriata in Connessioni VPN.
4. Seleziona la scheda Dettagli del tunnel.
5. Controlla la colonna Manutenzione in sospeso. Lo stato sarà Disponibile o Nessuno.

Per verificare la presenza di aggiornamenti disponibili, utilizzare AWS CLI

Usa il comando get-vpn-tunnel-replacement-status per verificare gli aggiornamenti disponibili.

Accettato un aggiornamento di manutenzione

Quando è disponibile un aggiornamento di manutenzione, puoi accettarlo utilizzando l'interfaccia a riga di comando AWS Management Console o la CLI.

Per accettare un aggiornamento di manutenzione disponibile utilizzando AWS Management Console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione appropriata in Connessioni VPN.
4. Scegli Azioni, quindi Sostituisci tunnel VPN.
5. Selezionare il tunnel che si desidera modificare scegliendo il Tunnel VPN esterno all'indirizzo IP.
6. Scegliere Replace (Sostituisci).

Per accettare un aggiornamento di manutenzione disponibile utilizzando AWS CLI

Usa il comando replace-vpn-tunnel per accettare un aggiornamento di manutenzione disponibile.

Disattiva il controllo del ciclo di vita degli endpoint del tunnel

Se non desideri più utilizzare la funzione di controllo del ciclo di vita degli endpoint del tunnel, puoi disattivarla utilizzando AWS Management Console o AWS CLI. Quando disattivi questa funzionalità, AWS distribuirà automaticamente aggiornamenti di manutenzione periodicamente e questi aggiornamenti potrebbero avvenire durante l'orario lavorativo. Per evitare qualsiasi impatto sull'azienda, ti consigliamo vivamente di configurare entrambi i tunnel nella connessione VPN per un'elevata disponibilità.

> **Note**
>
> Sebbene sia disponibile una manutenzione in sospeso, non è possibile specificare l'opzione salta sostituzione del tunnel mentre si disattiva la funzione. Puoi sempre disattivare la funzionalità senza utilizzare l'opzione salta sostituzione del tunnel, maAWS distribuirà automaticamente gli aggiornamenti di manutenzione disponibili in sospeso avviando immediatamente la sostituzione dell'endpoint del tunnel.

Per disattivare il controllo del ciclo di vita degli endpoint del tunnel utilizzando AWS Management Console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione appropriata in Connessioni VPN.
4. Selezionare Operazioni, Modifica opzioni tunnel VPN.
5. Selezionare il tunnel che si desidera modificare scegliendo l'indirizzo IP appropriato dall'elenco Tunnel VPN esterno all'indirizzo IP.
6. Per disattivare il controllo del ciclo di vita degli endpoint del tunnel in controllo del ciclo di vita degli endpoint del tunnel, deseleziona la casella di controllo Abilita.
7. (Facoltativo) Seleziona Salta la sostituzione del tunnel.
8. Seleziona Salva modifiche.

Per disattivare il controllo del ciclo di vita degli endpoint del tunnel utilizzando AWS CLI

Usa il comando modify-vpn-tunnel-options per disattivare il controllo del ciclo di vita degli endpoint del tunnel.

Opzioni di gateway del cliente per la connessione Site-to-Site VPN

Nella tabella seguente vengono descritte le informazioni necessarie per creare una risorsa gateway del cliente in AWS.

Elemento	Descrizione
(Facoltativo) Tag del nome.	Crea un tag con una chiave "Name" e un valore specificato dall'utente.
(Solo routing dinamico) Il Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway del cliente.	È supportato un numero ASN compreso tra 1 e 4.294.967.295. Puoi utilizzare un ASN pubblico esistente assegnato alla tua rete, ad eccezione dei seguenti: • 7224 - Riservato in tutte le regioni • 9059 - riservato nella regione `eu-west-1` • 10124 - riservato nella regione `ap-northeast-1` • 17943 - riservato nella regione `ap-southeast-1` Se non disponi di un ASN pubblico, puoi utilizzare un ASN privato compreso tra 64.512 e 65.534 o 4.200.000.000 - 4.294.967.294. L'ASN predefinito è 65000. Per ulteriori dettagli sull'instradamento, consulta Opzioni di routing per Site-to-Site VPN.
(Facoltativo) L'indirizzo IP dell'interfaccia esterna del dispositivo gateway del cliente.	L'indirizzo IP deve essere statico. Se il dispositivo gateway del cliente risiede dietro a un dispositivo Network Address Translation (NAT), utilizza l'indirizzo IP del dispositivo NAT. Inoltre, assicurati che i pacchetti UDP sulla porta 500 (e sulla porta 4500, se si utilizza NAT-Traversal) possano

Elemento	Descrizione
	passare tra la rete e gli endpoint. AWS Site-to-Site VPN Per ulteriori informazioni, consulta Regole firewall. Non è necessario un indirizzo IP quando si utilizza un certificato privato e una VPN pubblica. AWS Private Certificate Authority
(Facoltativo) Certificato privato rilasciato da una CA subordinata che utilizza AWS Certificate Manager (ACM).	Se si desidera utilizzare l'autenticazione basata su certificati, fornire l'ARN di un certificato privato ACM che verrà utilizzato sul dispositivo gateway del cliente. Quando si crea un gateway del cliente, è possibile configurarlo per utilizzare certificati privati AWS Private Certificate Authority per autenticare Site-to-Site VPN. Quando si sceglie di utilizzare questa opzione, si crea un'autorità di certificazione (CA) privata interamente AWS ospitata per uso interno dell'organizzazione. Sia il certificato CA principale che i certificati CA subordinati vengono archiviati e gestiti da. CA privata AWS Prima di creare il customer gateway, si crea un certificato privato da una CA subordinata utilizzando AWS Private Certificate Authority e quindi si specifica il certificato quando si configura il gateway del cliente. Per informazioni sulla creazione di un certificato privato, consulta la sezione relativa alla creazione e gestione di una CA privata nella Guida per l'utente di AWS Private Certificate Authority .

Elemento	Descrizione
(Facoltativo) Dispositivo.	Un nome per il dispositivo gateway del cliente associato a tale gateway del cliente.

Connessioni Site-to-Site VPN accelerate

Facoltativamente puoi abilitare l'accelerazione per la connessione Site-to-Site VPN. Una connessione VPN accelerata da sito a sito (connessione VPN accelerata AWS Global Accelerator) viene utilizzata per instradare il traffico dalla rete locale a una posizione periferica più vicina AWS al dispositivo gateway del cliente. AWS Global Accelerator ottimizza il percorso di rete, utilizzando la rete AWS globale priva di congestione per indirizzare il traffico verso l'endpoint che offre le migliori prestazioni applicative (per ulteriori informazioni, consulta). AWS Global Accelerator Puoi utilizzare una connessione VPN accelerata per evitare interruzioni di rete che si possono verificare quando il traffico viene instradato sulla rete Internet pubblica.

Quando crei una connessione VPN accelerata, vengono automaticamente creati e gestiti due acceleratori, uno per ogni tunnel VPN. Non è possibile visualizzare o gestire autonomamente questi acceleratori utilizzando la console o le API. AWS Global Accelerator

Per informazioni sulle AWS regioni che supportano le connessioni VPN accelerate, consulta le Domande frequenti sulla VPN AWS accelerata da sito a sito.

Abilitazione dell'accelerazione

Per impostazione predefinita, quando crei una connessione Site-to-Site VPN, l'accelerazione è disabilitata. Facoltativamente puoi abilitare l'accelerazione quando crei un nuovo collegamento Site-to-Site VPN in un gateway di transito. Per ulteriori informazioni e fasi, consulta Creazione di un collegamento VPN al gateway di transito.

Le connessioni VPN accelerate utilizzano un pool separato di indirizzi IP per gli indirizzi IP dell'endpoint del tunnel. Gli indirizzi IP per i due tunnel VPN sono selezionati da due zone di reteseparate.

Regole e restrizioni

Per utilizzare una connessione VPN accelerata, si applicano le seguenti regole:

- L'accelerazione è supportata solo per connessioni Site-to-Site VPN collegate a un gateway di transito. I gateway virtuali privati non supportano le connessioni VPN accelerate.
- Una connessione VPN accelerata da sito a sito non può essere utilizzata con un'interfaccia virtuale pubblica. AWS Direct Connect
- Non puoi abilitare o disabilitare l'accelerazione per una connessione Site-to-Site VPN esistente. Puoi invece creare una nuova connessione Site-to-Site VPN con accelerazione abilitata o disabilitata in base alle esigenze. Quindi, configura il dispositivo gateway del cliente per utilizzare la nuova connessione Site-to-Site VPN ed elimina la vecchia connessione Site-to-Site VPN.
- NAT-traversal (NAT-T) è obbligatorio per una connessione VPN accelerata ed è abilitato per impostazione predefinita. Se è stato scaricato un file di configurazione dalla console Amazon VPC, controlla l'impostazione NAT-T e modificala se necessario.
- La negoziazione IKE per i tunnel VPN accelerati deve essere avviata dal dispositivo gateway del cliente. Le due opzioni di tunnel che influiscono su questo comportamento sono e. `Startup Action` `DPD Timeout Action` Per ulteriori informazioni, consulta Opzioni per tunnel VPN e Opzioni di avvio del tunnel VPN.
- Le connessioni VPN da sito a sito che utilizzano l'autenticazione basata su certificati potrebbero non essere compatibili AWS Global Accelerator con, a causa del supporto limitato per la frammentazione dei pacchetti in Global Accelerator. Per ulteriori informazioni, consulta Funzionamento di AWS Global Accelerator. Se è necessaria una connessione VPN accelerata che utilizza l'autenticazione basata su certificato, il dispositivo gateway cliente deve supportare la frammentazione IKE. In caso contrario, non abilitare la VPN per l'accelerazione.

Opzioni di routing per Site-to-Site VPN

Quando crei una connessione Site-to-Site VPN devi eseguire le seguenti operazioni:

- Specificare il tipo di routing che prevedi di utilizzare (statico o dinamico)
- Aggiorna la tabella di routing per la sottorete

Esistono quote al numero di route che puoi aggiungere a una tabella di routing. Per ulteriori informazioni, consulta la sezione Tabelle di routing in Quote di Amazon VPC nella Guida per l'utente di Amazon VPC.

Argomenti

- Routing statico e dinamico

- Tabelle di routing e priorità della route VPN
- Routing durante gli aggiornamenti degli endpoint del tunnel VPN
- Traffico IPv4 e IPv6

Routing statico e dinamico

Il tipo di routing selezionato può dipendere dalla marca e dal modello del dispositivo gateway del cliente. Se il dispositivo gateway del cliente supporta Border Gateway Protocol (BGP), specifica il routing dinamico quando configuri la connessione VPN sito-sito. Se il dispositivo gateway del cliente non supporta BGP, specifica il routing statico.

Se utilizzi un dispositivo che supporta la pubblicità BGP, non puoi specificare le route statiche alla connessione Site-to-Site VPN perché il dispositivo utilizza BGP per pubblicizzare le sue route al gateway virtuale privato. Se utilizzi un dispositivo che non supporta la pubblicità BGP, devi selezionare il routing statico e immettere le route (prefissi IP) per la rete che devono essere comunicate al gateway virtuale privato.

Ti consigliamo di utilizzare dispositivi dotati della funzionalità BGP, quando disponibili, perché il protocollo BGP offre controlli di rilevamento liveness affidabili che possono rispondere alle Esigenze di failover al secondo tunnel VPN se il primo tunnel non è disponibile. I dispositivi che non supportano BGP possono anche Eseguire controlli dello stato per rispondere alle Esigenze di failover al secondo tunnel quando necessario.

È necessario configurare il dispositivo gateway del cliente per instradare il traffico dalla rete locale alla connessione Site-to-Site VPN. La configurazione dipende dalla marca e dal modello del dispositivo. Per ulteriori informazioni, consulta Il dispositivo gateway del cliente.

Tabelle di routing e priorità della route VPN

Le tabelle di routing determinano la destinazione del traffico di rete proveniente dal VPC. Nella tabella di routing VPC devi aggiungere una route per la rete remota e specificare il gateway virtuale privato come target. Questo consente di instradare il traffico dal VPC che è destinato alla rete remota al gateway virtuale privato e su uno dei tunnel VPN. Puoi abilitare la propagazione della route per la tabella di routing per propagare automaticamente le route di rete alla tabella.

Utilizziamo la route più specifica della tua tabella di routing che corrisponde al traffico per determinare il modo in cui instradare il traffico (corrispondenza di prefisso più lunga). Se la tabella di routing presenta percorsi sovrapposti o corrispondenti, si applicano le seguenti regole:

- Se le route propagate da una connessione Site-to-Site VPN o da una connessione AWS Direct Connect si sovrappongono alla route locale per il VPC, la route locale è la preferita anche se le route propagate sono più specifiche.
- Se le route propagate da una connessione Site-to-Site VPN o da una connessione AWS Direct Connect hanno lo stesso blocco CIDR di destinazione delle altre route statiche esistenti (la corrispondenza prefisso più lungo non può essere applicata), diamo la priorità alle route statiche i cui target sono un gateway Internet, un gateway virtuale privato, un'interfaccia di rete, un ID istanza, una connessione peering VPC, un gateway NAT, un gateway di transito o un endpoint VPC del gateway.

Ad esempio, la seguente tabella di routing dispone di una route statica a un Internet Gateway e una route propagata a una gateway virtuale privato. La destinazione di entrambe le regole è `172.31.0.0/24`. In questo caso, tutto il traffico destinato a `172.31.0.0/24` viene instradato all'Internet gateway, perché si tratta di una route statica che ha priorità sulla route propagata.

Destinazione	Target
10.0.0.0/16	Locale
172.31.0.0/24	vgw-11223344556677889 (propagato)
172.31.0.0/24	igw-12345678901234567 (statico)

Solo i prefissi IP noti al gateway virtuale privato, tramite annunci pubblicitari BGP o una voce route statica, possono ricevere traffico dal VPC. Il gateway virtuale privato non instradata eventuale altro traffico destinato all'esterno di promozioni BGP ricevute, alle voci della route statica o al relativo CIDR VPC collegato. I gateway virtuali privati non supportano il traffico IPv6.

Quando un gateway virtuale privato riceve informazioni di routing, utilizza la selezione percorso per determinare in che modo instradare il traffico. Si applica la corrispondenza di prefisso più lunga, se tutti gli endpoint sono integri. L'integrità di un endpoint del tunnel ha la precedenza sugli altri attributi di routing. Questa precedenza si applica alle VPN su gateway privati virtuali e gateway di transito. Se i prefissi sono identici, il gateway virtuale privato assegna la priorità alle route come segue, dalla più preferita alla meno preferita:

- Route propagate BGP da una connessione AWS Direct Connect
- Route statiche aggiunte manualmente per una connessione Site-to-Site VPN

- Route propagate BGP da una connessione Site-to-Site VPN
- Per prefissi corrispondenti in cui ciascuna connessione Site-to-Site VPN utilizza BGP, AS PATH viene confrontato e il prefisso con AS PATH più breve viene preferito.

> **Note**
>
> AWS consiglia vivamente di utilizzare dispositivi gateway del cliente che supportano il routing asimmetrico.
> Per i dispositivi gateway del cliente che supportano il routing asimmetrico, non consigliamo di utilizzare AS PATH anteposto, per garantire che i tunnel abbiano AS PATH uguale. Ciò consente di garantire che il valore multi-exit discriminator (MED) impostato su un tunnel durante gli aggiornamenti degli endpoint del tunnel VPN venga utilizzato per determinare la priorità del tunnel.
> Per i dispositivi gateway del cliente che non supportano il routing asimmetrico, è possibile utilizzare AS-Path anteposto e Local-Preference per preferire un tunnel rispetto all'altro. Tuttavia, quando il percorso di uscita cambia, ciò può causare una riduzione del traffico.

- Quando i percorsi AS hanno la stessa lunghezza e se il primo AS in AS_SEQUENCE è lo stesso su più percorsi, vengono confrontati i multi-exit discriminators (MED). Il percorso preferito è quello con il valore MED più basso.

La priorità della route è influenzata durante gli aggiornamenti degli endpoint del tunnel VPN.

In una connessione Site-to-Site VPN, AWS seleziona uno dei due tunnel ridondanti come percorso di uscita primario. Questa selezione a volte può cambiare e si consiglia di configurare entrambi i tunnel per la disponibilità elevata e per consentire un routing asimmetrico. L'integrità di un endpoint del tunnel ha la precedenza sugli altri attributi di routing. Questa precedenza si applica alle VPN su gateway privati virtuali e gateway di transito.

Per un gateway virtuale privato, verrà selezionato un tunnel per tutte le connessioni Site-to-Site VPN sul gateway. Per utilizzare entrambi i tunnel, è consigliabile esplorare Equal Cost Multipath (ECMP), supportato per le connessioni Site-to-Site VPN su un gateway di transito. Per ulteriori informazioni, consulta Gateway di transito in Gateway di transito di Amazon VPC. ECMP non è supportato per le connessioni Site-to-Site VPN in un gateway virtuale privato.

Per le connessioni Site-to-Site VPN che utilizzano BGP, il tunnel primario può essere identificato dal valore multi-exit discriminator (MED). Consigliamo di pubblicizzare percorsi BGP più specifici per influenzare le decisioni di routing.

Per le connessioni Site-to-Site VPN che utilizzano il routing statico, il tunnel principale può essere identificato dalle statistiche o dai parametri del traffico.

Routing durante gli aggiornamenti degli endpoint del tunnel VPN

Una connessione Site-to-Site VPN è costituita da due tunnel VPN tra un dispositivo gateway del cliente e un gateway virtuale privato o un gateway di transito. Si consiglia di configurare entrambi i tunnel per la ridondanza. Occasionalmente, AWS esegue anche manutenzione di routine sulla connessione VPN, che potrebbe brevemente disabilitare uno dei due tunnel della connessione VPN. Per ulteriori informazioni, consulta Notifiche di sostituzione degli endpoint del tunnel.

Quando eseguiamo aggiornamenti su un tunnel VPN, viene impostato un valore multi-exit discriminator (MED) in uscita inferiore sull'altro tunnel. Se il dispositivo gateway del cliente è stato configurato per utilizzare entrambi i tunnel, la connessione VPN utilizza l'altro tunnel durante il processo di aggiornamento dell'endpoint del tunnel.

> **Note**
>
> Per assicurarsi che il tunnel up con il MED inferiore sia quello preferito, assicurarsi che il dispositivo gateway cliente utilizzi gli stessi valori Peso e Preferenza locale per entrambi i tunnel (Peso e Preferenza locale hanno priorità più alta rispetto a MED).

Traffico IPv4 e IPv6

La connessione Site-to-Site VPN su un gateway di transito può supportare il traffico IPv4 o il traffico IPv6 all'interno dei tunnel VPN. Per impostazione predefinita, una connessione Site-to-Site VPN supporta il traffico IPv4 all'interno dei tunnel VPN. Puoi configurare una nuova connessione Site-to-Site VPN per supportare il traffico IPv6 all'interno dei tunnel VPN. Quindi, se il VPC e la rete locale sono configurati per l'indirizzamento IPv6, è possibile inviare traffico IPv6 tramite la connessione VPN.

Se attivi IPv6 per i tunnel VPN per la connessione Site-to-Site VPN, ogni tunnel ha due blocchi CIDR. Uno è un blocco CIDR di dimensione /30 IPv4 e l'altro è un blocco CIDR di dimensione /126 IPv6.

Si applicano le regole seguenti:

- Gli indirizzi IPv6 sono supportati solo per gli indirizzi IP interni dei tunnel VPN. Gli indirizzi IP del tunnel esterno per gli endpoint AWS sono indirizzi IPv4 e l'indirizzo IP pubblico del gateway del cliente deve essere un indirizzo IPv4.

- Le connessioni Site-to-Site VPN su un gateway virtuale privato non supportano IPv6.
- Non è possibile abilitare il supporto IPv6 per una connessione Site-to-Site VPN esistente.
- Una connessione Site-to-Site VPN non può supportare sia il traffico IPv4 che IPv6.

Per ulteriori informazioni sulla creazione di una connessione VPN, consulta Fase 5: creazione di una connessione VPN.

Guida introduttiva con AWS Site-to-Site VPN

Per configurare una AWS Site-to-Site VPN connessione, utilizzare la procedura seguente. Durante la creazione dovrai specificare un gateway privato virtuale, un gateway di transito oppure "Non associato" come tipo di gateway di destinazione. Se specifichi «Non associato», puoi scegliere il tipo di gateway di destinazione in un secondo momento oppure puoi utilizzarlo come allegato VPN per AWS Cloud WAN. Questo tutorial ti aiuta a creare una connessione VPN mediante un gateway privato virtuale. Si basa sul presupposto che disponi di un VPC esistente con una o più sottoreti.

Per configurare una connessione VPN tramite un gateway privato virtuale, completa le seguenti fasi:

Attività

- Prerequisiti
- Fase 1: creazione di un gateway del cliente
- Fase 2: creazione di un gateway di destinazione
- Fase 3: configurazione dell'instradamento
- Fase 4: aggiornamento del gruppo di sicurezza
- Fase 5: creazione di una connessione VPN
- Fase 6: download del file di configurazione
- Fase 7: configurazione del dispositivo gateway del cliente

Attività correlate

- Per creare una connessione VPN per AWS Cloud WAN, consultaCrea un allegato VPN per Cloud WAN AWS .
- Per creare una connessione VPN su un gateway di transito, consulta Creazione di un collegamento VPN al gateway di transito.

Prerequisiti

Per impostare e configurare i componenti di una connessione VPN, sono necessarie le seguenti informazioni.

Elemento	Informazioni
Dispositivo gateway del cliente	Il dispositivo fisico o software dal lato utente della connessione VPN. Sono richiesti il fornitore (ad esempio, Cisco), la piattaforma (ad esempio, router della serie ISR) e la versione software (ad esempio, IOS 12.4)
Gateway del cliente	Per creare la risorsa Customer Gateway in AWS, sono necessarie le seguenti informazioni: • L'indirizzo IP Internet instradabile per l'interfaccia esterna del dispositivo. • Il tipo di routing: statico o dinamico. • Per routing dinamico, il Border Gateway Protocol (BGP) Autonomous System Number (ASN) • (Facoltativo) Certificato privato da AWS Private Certificate Authority cui autenticare la tua VPN Per ulteriori informazioni, consulta Opzioni gateway del cliente.
(Facoltativo) L'ASN per la AWS sessione BGP	Specificare quando si crea un gateway virtuale privato o un gateway di transito. Se non specifichi un valore, si applica l'ASN predefinito. Per ulteriori informazioni, consulta Gateway privato virtuale.
Connessione VPN	Per creare una connessione VPN, sono necessarie le seguenti informazioni: • Per il routing statico, i prefissi IP per la rete privata. • (Facoltativo) Opzioni tunnel per ogni tunnel VPN. Per ulteriori informazioni, consulta

Elemento	Informazioni
	Opzioni di tunnel per la connessione Site-to-Site VPN.

Fase 1: creazione di un gateway del cliente

Un customer gateway fornisce informazioni sul dispositivo o AWS sull'applicazione software Customer Gateway. Per ulteriori informazioni, consulta Gateway del cliente.

Se prevedi di utilizzare un certificato privato per autenticare la tua VPN, crea un certificato privato da una CA subordinata utilizzando. AWS Private Certificate Authority Per informazioni sulla creazione di un certificato privato, consulta la sezione relativa alla creazione e gestione di una CA privata nella Guida per l'utente di AWS Private Certificate Authority .

> **Note**
>
> È necessario specificare un indirizzo IP o l'Amazon Resource Name del certificato privato.

Per creare un gateway del cliente utilizzando la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gateway del cliente.
3. Scegli Crea gateway del cliente.
4. (Facoltativo) In Name (Nome), inserire un nome per il gateway del cliente. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
5. In BGP ASN, inserire un Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway del cliente.
6. (Facoltativo) In IP Address (Indirizzo IP), inserire l'indirizzo IP Internet instradabile statico per il dispositivo gateway del cliente. Se il dispositivo gateway del cliente si trova dietro un dispositivo NAT abilitato per NAT-T, utilizzare l'indirizzo IP pubblico del dispositivo NAT.
7. (Facoltativo) Se si desidera utilizzare un certificato privato, in Certificate ARN (ARN certificato), scegliere l'Amazon Resource Name del certificato privato.
8. (Opzionale) Per Dispositivo inserisci un nome per il dispositivo gateway del cliente associato a tale gateway del cliente.

9. Scegli Crea gateway del cliente.

Per creare un gateway del cliente utilizzando l'API o la riga di comando

- CreateCustomerGateway (API di interrogazione Amazon EC2)
- create-customer-gateway (AWS CLI)
- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Fase 2: creazione di un gateway di destinazione

Per stabilire una connessione VPN tra il tuo VPC e la tua rete locale, devi creare un gateway di destinazione sul AWS lato della connessione. Il gateway target può essere un gateway virtuale privato o un gateway di transito.

Creazione di gateway virtuale privato

Quando crei un gateway virtuale privato, puoi specificare un Autonomous System Number (ASN) personalizzato privato per il lato Amazon del gateway o utilizzare un ASN di default di Amazon. L'ASN deve essere diverso dall'ASN specificato per il gateway del cliente.

Dopo aver creato un gateway virtuale privato, devi collegarlo al VPC.

Per creare un gateway virtuale privato e collegarlo al VPC

1. Nel riquadro di navigazione, scegli Gateway privati virtuali.
2. Selezionare Create Virtual Private Gateway (Crea gateway virtuale privato).
3. (Facoltativo) Inserisci un nome per il gateway privato virtuale per Tag del nome. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
4. In Numero di sistema autonomo (ASN), mantieni la selezione predefinita, Numero ASN di Amazon predefinito, per utilizzare l'ASN Amazon predefinito. In caso contrario, scegliere Custom ASN (ASN personalizzato) e immettere un valore. Per un ASN a 16 bit, il valore deve Esser compreso nell'intervallo da 64512 a 65534. Per un ASN a 32 bit, il valore deve Essere compreso nell'intervallo da 4200000000 a 4294967294.
5. Selezionare Create Virtual Private Gateway (Crea gateway virtuale privato).
6. Selezionare il gateway virtuale privato creato, quindi scegliere Actions (Operazioni), Attach to VPC (Collega a VPC).

7. Per VPC disponibili, scegli il VPC, quindi scegli Collega al VPC.

Per creare un gateway virtuale privato utilizzando l'API o la riga di comando

- CreateVpnGateway (API di interrogazione Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Per collegare un gateway virtuale privato a un VPC utilizzando la riga di comando o l'API

- AttachVpnGateway (API di interrogazione Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Creazione di un gateway di transito

Per ulteriori informazioni sulla creazione di un gateway di transito, consulta Gateway di transito in Gateway di transito Amazon VPC.

Fase 3: configurazione dell'instradamento

Per consentire alle istanze nel VPC di raggiungere il gateway del cliente, occorre configurare la tabella di routing per includere gli instradamenti utilizzati dalla connessione VPN e indirizzarli al gateway privato virtuale o al gateway di transito.

(Gateway virtuale privato) Abilitazione della propagazione della route nella tabella di routing

Puoi abilitare la propagazione della route per la tabella di routing per propagare automaticamente le route Site-to-Site VPN.

Per il routing statico, i prefissi IP statici specificati per la configurazione VPN vengono propagati alla tabella di routing quando lo stato della connessione VPN è UP. Analogamente, per il routing dinamico, le route pubblicizzate BGP dal gateway del cliente vengono propagate alla tabella di routing quando lo stato della connessione VPN è UP.

> **Note**
>
> Se la connessione viene interrotta ma la connessione VPN rimane UP, le eventuali route propagate presenti nella tabella di routing non vengono rimosse automaticamente. Ricordarlo se, ad esempio, si desidera che il traffico non vada a buon fine su una route statica. In tal caso, potrebbe essere necessario disabilitare la propagazione della route per rimuovere le route propagate.

Per abilitare la propagazione della route tramite la console

1. Nel riquadro di navigazione, seleziona Tabelle di routing.
2. Seleziona la tabella di routing associata alla sottorete.
3. Nella scheda Propagazione dell'instradamento, scegli Modifica propagazione dell'instradamento. Seleziona il gateway privato virtuale creato nella procedura precedente e scegli Salva.

> **Note**
>
> Se non abiliti la propagazione dell'instradamento, devi inserire manualmente gli instradamenti statici utilizzati dalla connessione VPN. A questo scopo, selezionare la tabella di routing, scegliere Routes (Route), Edit (Modifica). In Destination (Destinazione) aggiungi la route statica utilizzata dalla connessione Site-to-Site VPN. In Target, selezionare l'ID gateway virtuale privato e scegliere Save (Salva).

Per disabilitare la propagazione delle route utilizzando la console

1. Nel riquadro di navigazione, seleziona Tabelle di routing.
2. Seleziona la tabella di routing associata alla sottorete.
3. Nella scheda Propagazione dell'instradamento, scegli Modifica propagazione dell'instradamento. Deseleziona la casella di controllo Propaga relativa al gateway privato virtuale.
4. Selezionare Salva.

Per abilitare la propagazione della route tramite la riga di comando o l'API

- EnableVgwRoutePropagation(API di interrogazione Amazon EC2)

- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Per disabilitare la propagazione della route tramite la riga di comando o l'API

- DisableVgwRoutePropagation(API di interrogazione Amazon EC2)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

(Gateway di transito) Aggiunta di una route alla tabella di routing

Se hai abilitato la propagazione della tabella di routing per il gateway di transito, le route per il collegamento VPN vengono propagate alla tabella di routing del gateway di transito. Per ulteriori informazioni, consulta Routing in Gateway di transito di Amazon VPC.

Se colleghi un VPC al gateway di transito e desideri consentire alle risorse nel VPC di raggiungere il gateway del cliente, devi aggiungere una route alla tabella di routing della sottorete affinché faccia riferimento al gateway di transito.

Per aggiungere una nuova route a una tabella di routing di un VPC

1. Nel riquadro di navigazione, seleziona Tabelle di routing.
2. Scegliere la tabella di routing associata al VPC.
3. Nella scheda Route, scegli Modifica route.
4. Scegli Aggiungi route.
5. Nella colonna Destinazione, immetti l'intervallo di indirizzi IP di destinazione. Per Target (Destinazione) scegli il gateway di transito.
6. Seleziona Salvataggio delle modifiche.

Fase 4: aggiornamento del gruppo di sicurezza

Per consentire l'accesso a istanze nel VPC dalla rete, occorre aggiornare le regole del gruppo di sicurezza per abilitare l'accesso SSH, RDP e ICMP in entrata.

Aggiunta di regole al gruppo di sicurezza per abilitare l'accesso

1. Nel riquadro di navigazione, fai clic su Gruppi di sicurezza.
2. Seleziona il gruppo di sicurezza per le istanze del tuo VPC a cui desideri consentire l'accesso.
3. Nella scheda Inbound rules (Regole in entrata), seleziona Edit inbound rules (Modifica regole in entrata).
4. Aggiungi le regole che consentono l'accesso SSH, RDP e ICMP in entrata dalla rete, quindi seleziona Salva regole. Per ulteriori informazioni, consulta Utilizzo delle regole dei gruppi di sicurezza nella Guida per l'utente di Amazon VPC.

Fase 5: creazione di una connessione VPN

Crea la connessione VPN utilizzando il gateway del cliente in combinazione con il gateway privato virtuale o il gateway di transito creato in precedenza.

Per creare una connessione VPN

1. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
2. Scegliere Create VPN Connection (Crea connessione VPN).
3. (Facoltativo) In Tag del nome, immettere un nome per la connessione VPN. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
4. Per Target gateway type (Tipo di gateway di destinazione), scegliere Virtual private gateway (Gateway virtuale privato) o Transit gateway (Gateway di transito). Quindi, scegliere il gateway virtuale privato o il gateway di transito creato in precedenza.
5. Per Gateway del cliente, seleziona Esistente, quindi scegli il gateway del cliente creato in precedenza da ID gateway del cliente.
6. Selezionare una delle opzioni di routing a seconda che il dispositivo gateway del cliente supporti Border Gateway Protocol (BGP):

   - Se il dispositivo gateway del cliente supporta BGP, scegliere Dynamic (requires BGP) (Dinamico (richiede BGP)).
   - Se il dispositivo gateway del cliente non supporta BGP, scegliere Static (Statico). In Static IP Prefixes (Prefissi IP statici), specificare ogni prefisso IP per la rete privata della connessione VPN.

7. Se il tipo di gateway di destinazione è un gateway di transito, per Tunnel interno alla versione IP, specifica se i tunnel VPN supportano il traffico IPv4 o IPv6. Il traffico IPv6 è supportato solo per le connessioni VPN su un gateway di transito.
8. Se hai specificato IPv4 per la versione IP di Tunnel inside, puoi facoltativamente specificare gli intervalli CIDR IPv4 per il gateway e AWS i lati del cliente autorizzati a comunicare tramite i tunnel VPN. Il valore predefinito è `0.0.0.0/0`.

   Se hai specificato IPv6 per la versione IP di Tunnel Inside, puoi facoltativamente specificare gli intervalli CIDR IPv6 per il gateway e i lati del cliente che sono autorizzati a comunicare tramite i tunnel VPN. AWS Il valore predefinito per entrambi gli intervalli è `::/0`.
9. Per il tipo di indirizzo IP esterno, mantieni l'opzione predefinita, 4. PublicIpv
10. (Facoltativo) per Opzioni tunnel, è possibile specificare le seguenti informazioni per ciascun tunnel:

    - Un blocco CIDR IPv4 di dimensione /30 dall'intervallo `169.254.0.0/16` per gli indirizzi IPv4 del tunnel interno.
    - Se hai specificato IPv6 per Tunnel interno alla versione IP, un blocco CIDR IPv6 /126 dall'intervallo `fd00::/8` per gli indirizzi IPv6 del tunnel interno.
    - La chiave precondivisa IKE (PSK). Sono supportate le seguenti versioni: IKEv1 o IKEv2.
    - Per modificare le opzioni avanzate del tunnel, scegli Modifica le opzioni tunnel. Per ulteriori informazioni, consulta Opzioni per tunnel VPN.
11. Scegliere Create VPN Connection (Crea connessione VPN). Per creare la connessione VPN potrebbero essere necessari alcuni minuti.

Per creare una connessione VPN utilizzando la riga di comando o l'API

- CreateVpnConnessione (API di interrogazione Amazon EC2)
- create-vpn-connection (AWS CLI)
- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

Fase 6: download del file di configurazione

Dopo aver creato la connessione VPN, puoi scaricare un file di configurazione di esempio da utilizzare per configurare il dispositivo gateway del cliente.

> **Important**
>
> Il file di configurazione è solo un esempio e potrebbe non corrispondere completamente alle impostazioni di connessione VPN previste. Specifica i requisiti minimi per una connessione VPN del gruppo AES128, SHA1 e Diffie-Hellman 2 nella maggior parte delle regioni e del gruppo AES128, SHA2 e Diffie-Hellman 14 AWS nelle regioni. AWS GovCloud Specifica anche le chiavi precondivise per autenticazione. È necessario modificare il file di configurazione di esempio per sfruttare i vantaggi di algoritmi di sicurezza aggiuntivi, gruppi Diffie-Hellman, certificati privati e traffico IPv6.
> Abbiamo introdotto il supporto IKEv2 nei file di configurazione per molti dispositivi gateway del cliente e continueremo ad aggiungere file aggiuntivi nel tempo. Consulta Il dispositivo gateway del cliente per un elenco completo dei file di configurazione con supporto IKEv2.

Autorizzazioni

Per caricare correttamente la schermata di configurazione del download da AWS Management Console, devi assicurarti che il tuo ruolo o utente IAM disponga dell'autorizzazione per le seguenti API Amazon EC2: e. `GetVpnConnectionDeviceTypes` `GetVpnConnectionDeviceSampleConfiguration`

Download del file di configurazione mediante la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione VPN e scegli Scarica configurazione.
4. Seleziona Fornitore, Piattaforma, Software e Versione IKE che corrisponde al dispositivo gateway del cliente. Se il dispositivo non è presente nell'elenco, scegliere Generic (Generico).
5. Scegli Download (Scarica).

Per eseguire il download di un file di configurazione di esempio utilizzando la riga di comando o API

- GetVpnConnectionDeviceTipi (API Amazon EC2)
- GetVpnConnectionDeviceSampleConfiguration(API di interrogazione Amazon EC2)
- get-vpn-connection-device-types (AWS CLI)
- get-vpn-connection-device-sample-configuration (AWS CLI)

Fase 7: configurazione del dispositivo gateway del cliente

Utilizza il file di configurazione di esempio per configurare il dispositivo gateway del cliente. Il dispositivo gateway del cliente è un'appliance fisica o software sul tuo lato della connessione VPN. Per ulteriori informazioni, consulta Il dispositivo gateway del cliente.

Architetture Site-to-Site VPN

Di seguito sono riportate le architetture Site-to-Site VPN comuni:

- the section called “Connessioni VPN singole e multiple”
- the section called “Connessioni VPN ridondanti”
- the section called “AWS VPN CloudHub”

Esempi di connessione VPN site-to-site singola e multipla

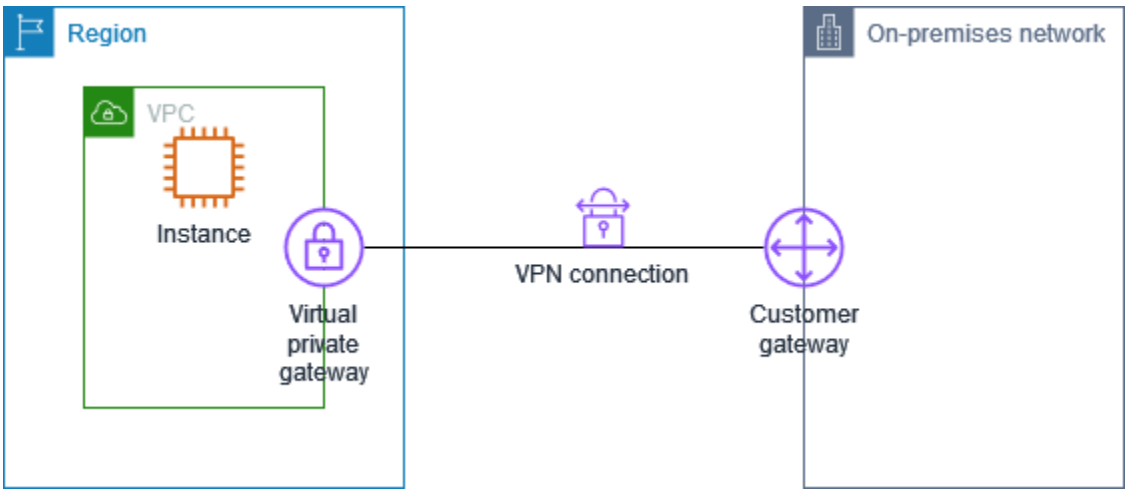
Nei seguenti diagrammi vengono mostrate le connessioni Site-to-Site VPN singole e multiple.

Esempi

- Connessione Site-to-Site VPN singola
- Connessione Site-to-Site VPN singola con gateway di transito
- Connessioni Site-to-Site VPN multiple
- Connessioni Site-to-Site VPN multiple con un gateway di transito
- Connessione Site-to-Site VPN con AWS Direct Connect
- Connessione Site-to-Site VPN IP privata con AWS Direct Connect

Connessione Site-to-Site VPN singola

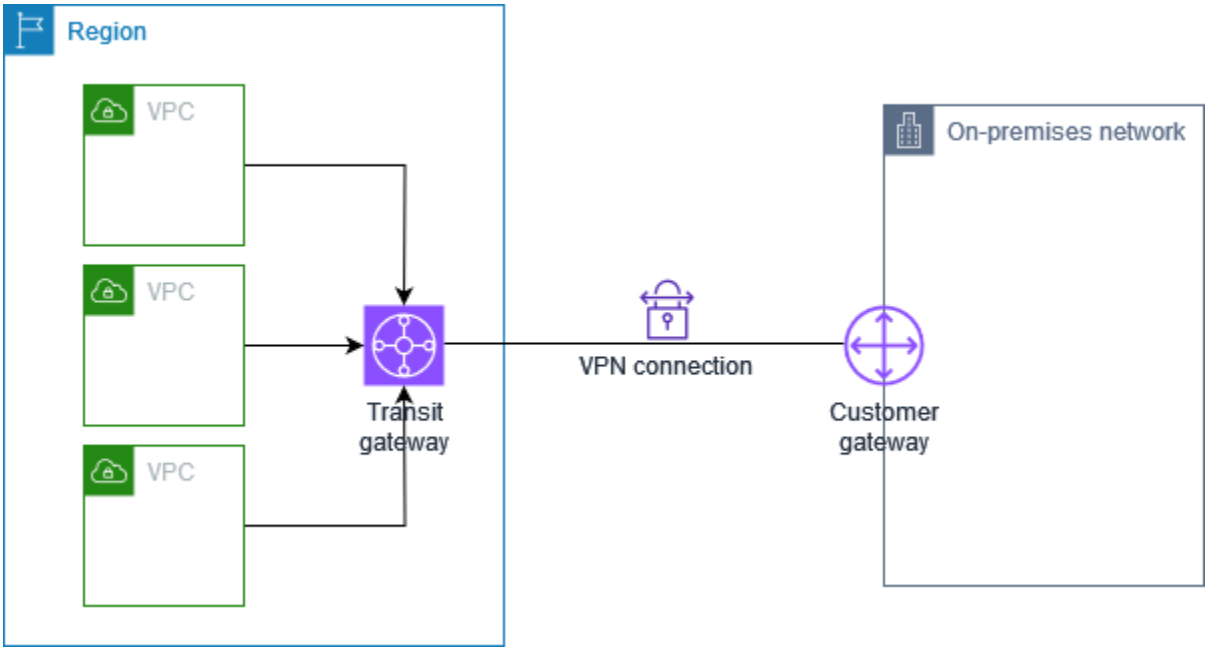
Il VPC dispone di un gateway privato virtuale e la rete remota on-premise include un dispositivo gateway del cliente che devi configurare per abilitare la connessione VPN. È necessario configurare le tabelle di routing per instradare l'eventuale traffico dal VPC destinato alla rete al gateway privato virtuale.



Per le fasi di impostazione di questo scenario, consulta Guida introduttiva con AWS Site-to-Site VPN.

Connessione Site-to-Site VPN singola con gateway di transito

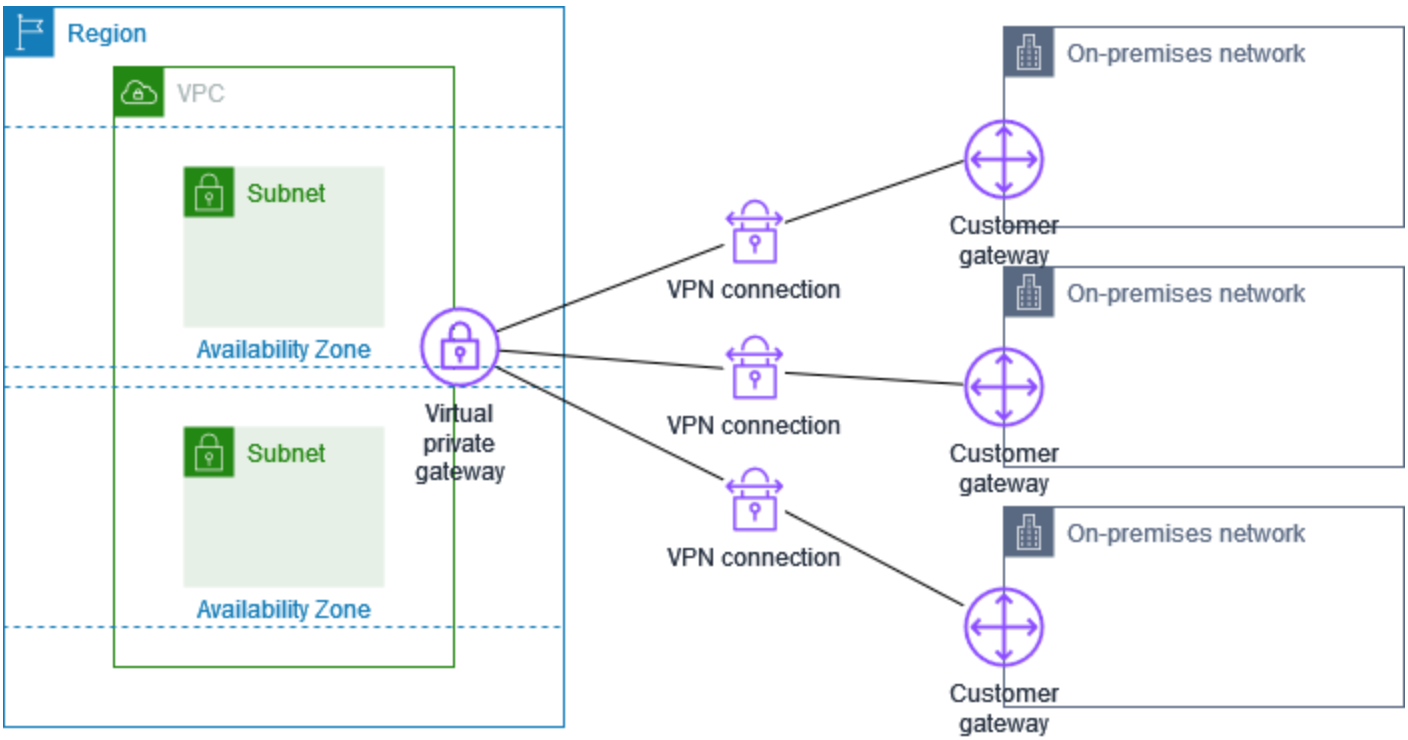
Il VPC dispone di un gateway di transito collegato e la rete remota on-premise include un dispositivo gateway del cliente che devi configurare per abilitare la connessione VPN sito-sito. È necessario configurare le tabelle di routing per instradare l'eventuale traffico dal VPC destinato alla rete al gateway di transito.



Per le fasi di impostazione di questo scenario, consulta Guida introduttiva con AWS Site-to-Site VPN.

Connessioni Site-to-Site VPN multiple

Il VPC dispone di un gateway virtuale privato collegato e hai più connessioni Site-to-Site VPN a più posizioni locali. Configura il routing per instradare l'eventuale traffico dal VPC destinato alle reti al gateway virtuale privato.

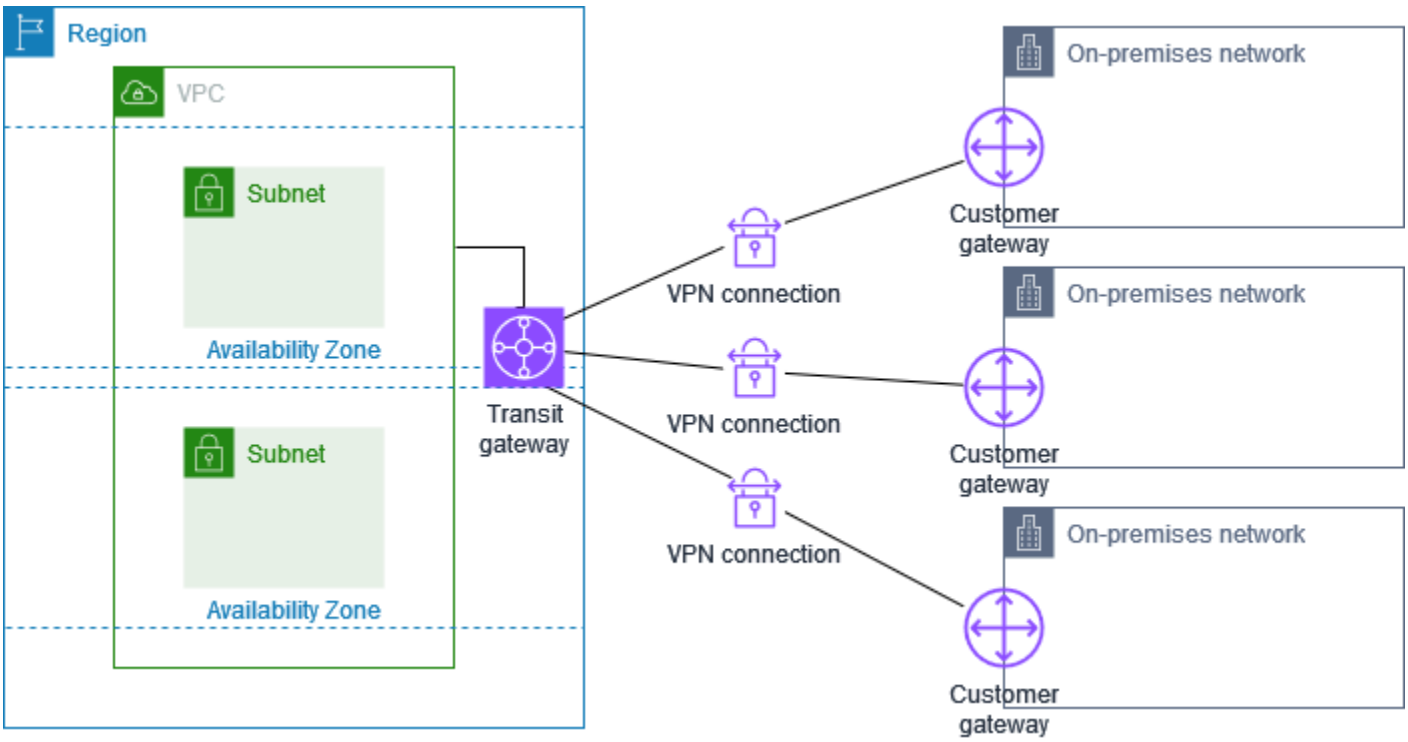


Quando crei più connessioni Site-to-Site VPN a un VPC singolo, puoi configurare un secondo gateway del cliente per creare una connessione ridondante alla stessa ubicazione esterna. Per ulteriori informazioni, consulta Utilizzo di connessioni Site-to-Site VPN ridondanti per fornire il failover.

Puoi inoltre utilizzare questo scenario per creare connessioni Site-to-Site VPN a più località geografiche e fornire comunicazioni sicure tra i siti. Per ulteriori informazioni, consulta Fornire una comunicazione sicura tra siti utilizzando VPN CloudHub.

Connessioni Site-to-Site VPN multiple con un gateway di transito

Il VPC dispone di un gateway di transito collegato e hai più connessioni Site-to-Site VPN a più posizioni locali. Configura il routing per instradare l'eventuale traffico dal VPC destinato alle reti al gateway di transito.

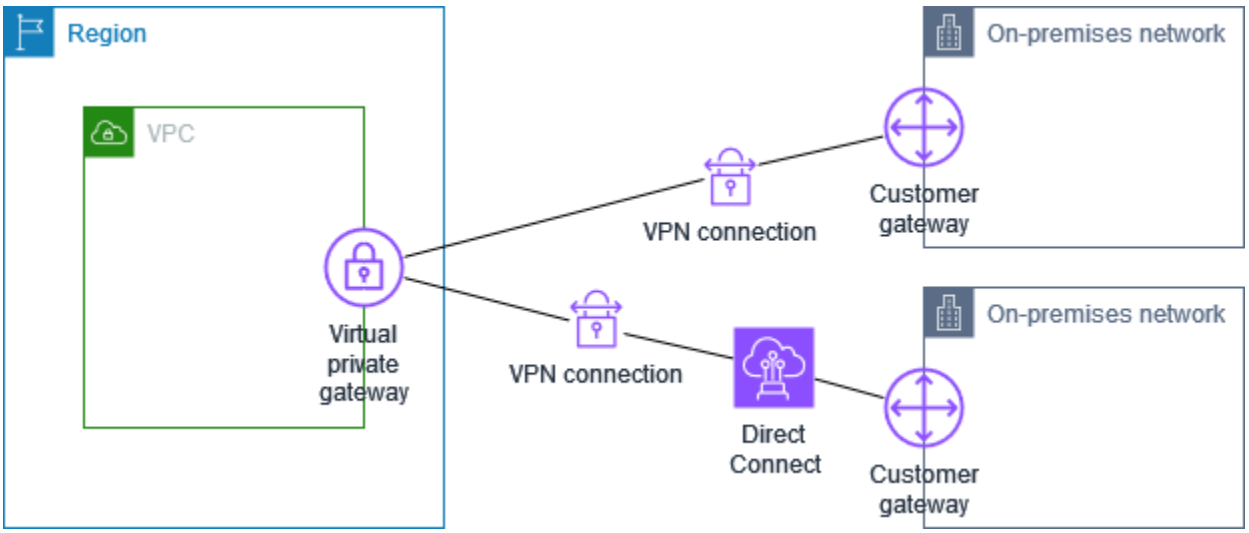


Quando crei più connessioni Site-to-Site VPN a un gateway di transito singolo, puoi configurare un secondo gateway del cliente per creare una connessione ridondante alla stessa ubicazione esterna.

Puoi inoltre utilizzare questo scenario per creare connessioni Site-to-Site VPN a più località geografiche e fornire comunicazioni sicure tra i siti.

Connessione Site-to-Site VPN con AWS Direct Connect

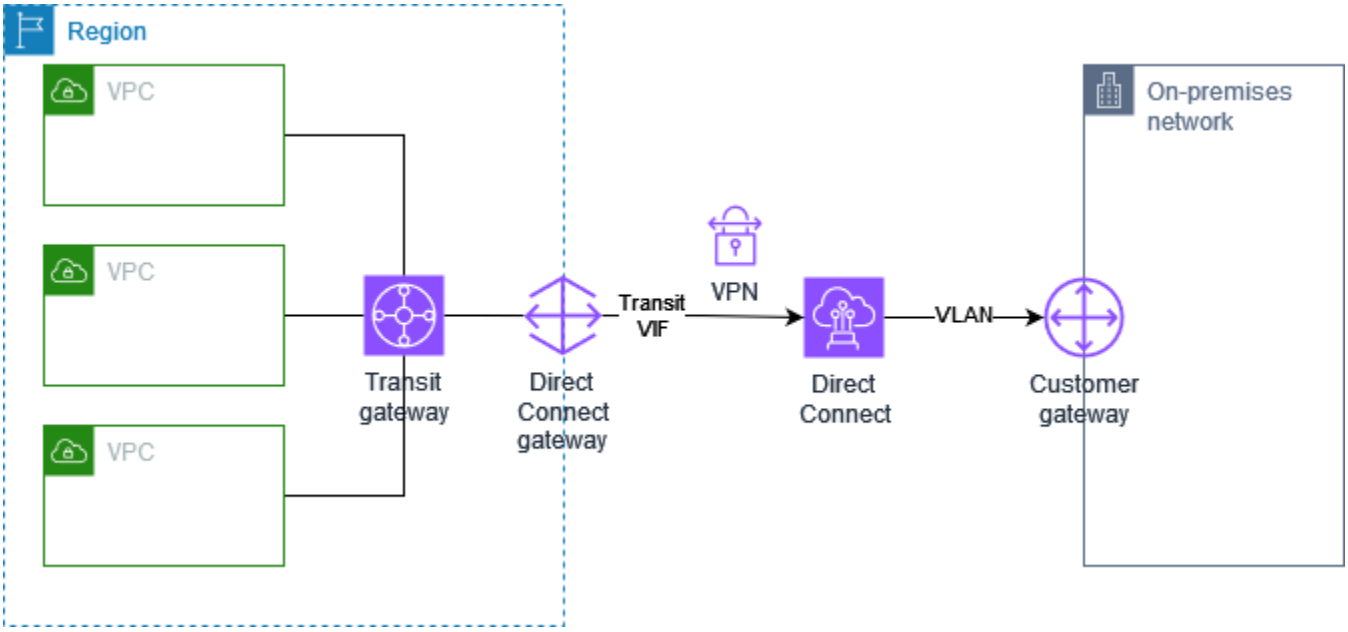
Il VPC dispone di un gateway virtuale privato collegato e si connette alla rete locale (remota) tramite AWS Direct Connect. È possibile configurare un'interfaccia virtuale pubblica AWS Direct Connect per stabilire una connessione di rete dedicata tra la rete alle risorse AWS pubbliche tramite un gateway virtuale privato. Configura il routing per instradare l'eventuale traffico dal VPC destinato agli instradamenti della rete al gateway virtuale privato e alla connessione AWS Direct Connect.



Quando sia AWS Direct Connect che la connessione VPN sono impostati sullo stesso gateway virtuale privato, l'aggiunta o la rimozione di oggetti potrebbe indurre il gateway virtuale privato a entrare nello stato 'collegamento in corso'. Questo indica che viene apportata una modifica al routing interno che passerà da AWS Direct Connect alla connessione VPN per ridurre al minimo le interruzioni e la perdita di pacchetti. Al termine, il gateway virtuale privato torna allo stato 'collegato'.

Connessione Site-to-Site VPN IP privata con AWS Direct Connect

Con una VPN Site-to-Site IP privata è possibile crittografare il traffico di AWS Direct Connect tra rete on-premise e AWS senza l'uso di indirizzi IP pubblici. La VPN IP privata su AWS Direct Connect assicura che il traffico tra AWS e le reti on-premise sia sicuro e privato, consentendo ai clienti di rispettare i mandati normativi e di sicurezza.



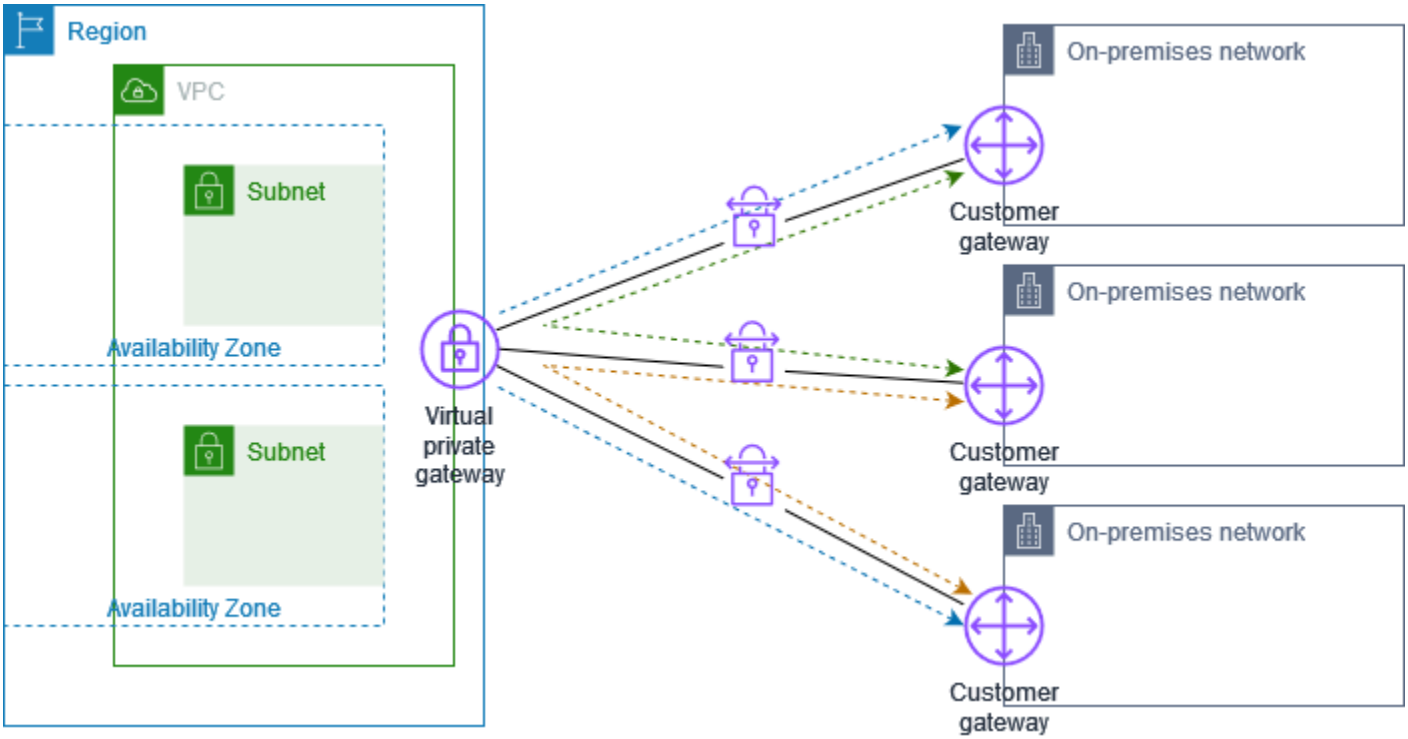
Per ulteriori informazioni, consulta il seguente post sul blog: Introducing AWS Site-to-Site VPN Private IP VPN.

Fornire una comunicazione sicura tra siti utilizzando VPN CloudHub

Se disponi di più connessioni AWS Site-to-Site VPN, puoi fornire una comunicazione sicura tra siti utilizzando AWS VPN CloudHub. Ciò consente ai siti remoti di comunicare tra loro e non solo con le risorse nel VPC. VPN CloudHub funziona su un semplice modello hub-and-spoke che puoi utilizzare con o senza un VPC. Questa progettazione è idonea se si dispone di più filiali e connessioni Internet esistenti e si desidera implementare un modello hub-and-spoke potenzialmente economico per la connettività principale o di backup tra questi siti.

Panoramica

Il diagramma seguente illustra l'architettura VPN CloudHub. Le linee tratteggiate mostrano il traffico di rete tra siti remoti che viene instradato tramite le connessioni VPN. I siti non devono disporre di intervalli IP che si sovrappongono.



Per questo scenario, effettuare le operazioni seguenti:

1. Creare un singolo gateway virtuale privato.

2. Creare più gateway del cliente, ciascuno con l'indirizzo IP pubblico del gateway. Utilizza un Border Gateway Protocol (BGP) Autonomous System Number (ASN) univoco per ogni gateway del cliente.
3. Crea una connessione Site-to-Site VPN instradata dinamicamente da ogni gateway del cliente al gateway virtuale privato comune.
4. Configurare i dispositivi gateway del cliente per pubblicizzare un prefisso specifico del sito (ad esempio 10.0.0.0/24, 10.0.1.0/24) al gateway virtuale privato. Queste pubblicità di routing vengono ricevute E pubblicizzate nuovamente in ciascun peer BGP, abilitando ciascun sito per inviare E ricevere dati da altri siti. Ciò viene fatto utilizzando le istruzioni di rete dei file di configurazione VPN per la connessione Site-to-Site VPN. Le istruzioni di rete differiscono leggermente in base al tipo di router utilizzato.
5. Configurare le route nelle tabelle di routing della sottorete per consentire alle istanze del VPC di comunicare con i siti. Per ulteriori informazioni, consulta (Gateway virtuale privato) Abilitazione della propagazione della route nella tabella di routing. Puoi configurare una route aggregata nella tabella di routing (ad esempio, 10.0.0.0/16). Utilizza prefissi più specifici tra i dispositivi gateway del cliente e il gateway virtuale privato.

I siti che utilizzano connessioni AWS Direct Connect al gateway virtuale privato possono anche fare parte di AWS VPN CloudHub. Ad esempio, le sedi principali in New York possono disporre di una connessione AWS Direct Connect al VPC e le filiali possono utilizzare connessioni Site-to-Site VPN al VPC. Le filiali a Los Angeles e Miami possono inviare E ricevere dati tra di loro e con le sedi centrali, tutte utilizzando AWS VPN CloudHub.

Prezzi

Per utilizzare AWS VPN CloudHub vengono addebitate le tipiche tariffe di connessione Site-to-Site VPN di Amazon VPC. Ti viene addebitata la tariffa di connessione per ogni ora di connessione di ciascuna VPN al gateway virtuale privato. Quando invii dati da un sito a un altro utilizzando AWS VPN CloudHub, non esistono costi di invio dei dati dal sito al gateway virtuale privato. To vengono addebitati solo i costi di trasferimento dei dati AWS standard per i dati che vengono inoltrati dal gateway virtuale privato all'endpoint.

Ad esempio, se hai un sito a Los Angeles e un secondo sito a New York ed entrambi dispongono di una connessione Site-to-Site VPN al gateway virtuale privato, ti viene addebitata una tariffa oraria per ogni connessione Site-to-Site VPN (pertanto, se la tariffa fosse 0,05 USD, si avrebbe un totale di 0,10 USD l'ora). Ti vengono anche addebiti i costi di trasferimento dei dati AWS standard per tutti i dati

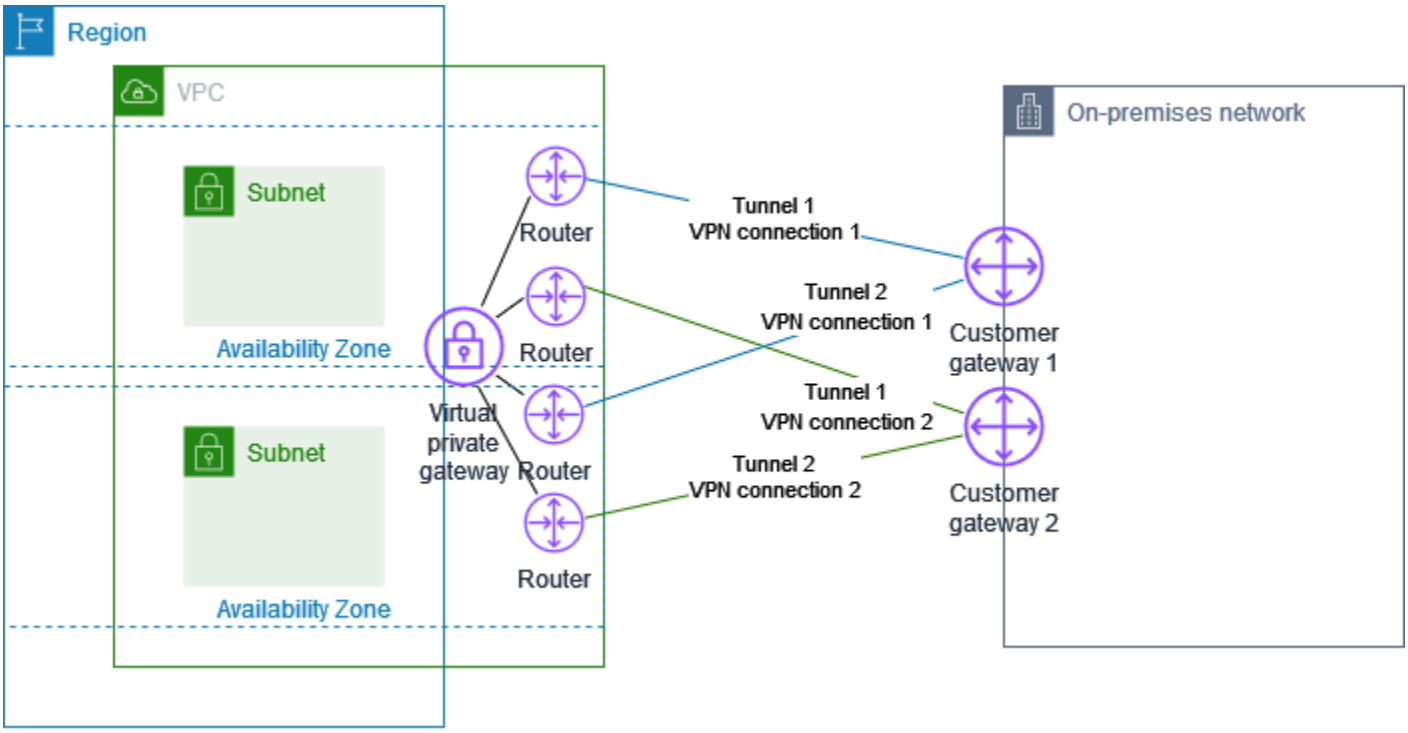
inviati da Los Angeles a New York (e viceversa) che attraversano ogni connessione Site-to-Site VPN. Il traffico di rete inviato sulla connessione Site-to-Site VPN al gateway virtuale privato è gratuito, ma il traffico di rete inviato sulla connessione Site-to-Site VPN dal gateway virtuale privato all'endpoint viene fatturato alla tariffa di trasferimento dei dati AWS standard.

Per ulteriori informazioni, consulta Prezzi della connessione Site-to-Site VPN.

Utilizzo di connessioni Site-to-Site VPN ridondanti per fornire il failover

Per evitare la perdita di connettività nel caso in cui il dispositivo gateway del cliente non sia disponibile, è possibile configurare una seconda connessione VPN sito-sito al VPC e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente. Utilizzando le connessioni VPN ridondanti e i dispositivi gateway del cliente, è possibile eseguire la manutenzione di uno o più dispositivi mentre il traffico continua a scorrere sulla connessione del secondo gateway del cliente.

Il seguente diagramma mostra due connessioni VPN. Ogni connessione VPN ha i propri tunnel e il proprio gateway del cliente.



Per questo scenario, effettuare le operazioni seguenti:

- Impostare una seconda connessione Site-to-Site VPN utilizzando lo stesso gateway virtuale privato e creando un nuovo gateway del cliente. L'indirizzo IP del gateway del cliente per la seconda connessione Site-to-Site VPN deve essere accessibile pubblicamente.
- Configurare un secondo dispositivo gateway del cliente. Entrambi i dispositivi devono pubblicizzare gli stessi intervalli IP al gateway virtuale privato. Il routing BGP serve a determinare il percorso per il traffico. Se si verifica un errore in un dispositivo gateway del cliente, il gateway virtuale privato indirizza tutto il traffico al dispositivo gateway del cliente in funzione.

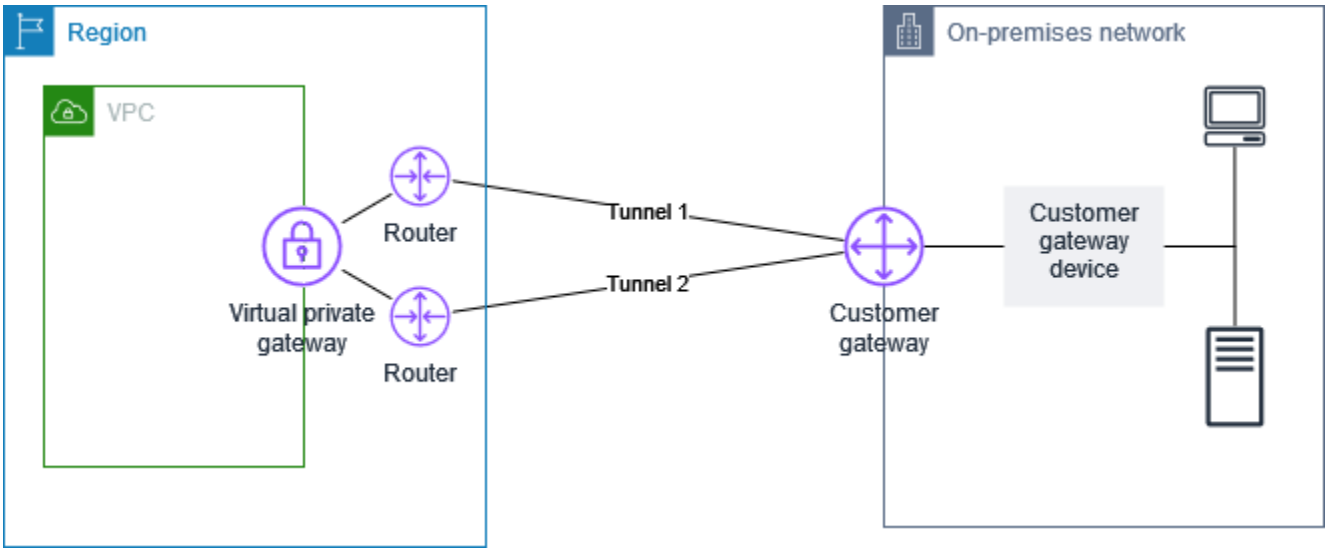
Le connessioni Site-to-Site VPN instradate dinamicamente utilizzano Border Gateway Protocol (BGP) per scambiare informazioni di routing tra i gateway del cliente e i gateway virtuali privati. Le connessioni Site-to-Site VPN instradate staticamente richiedono di immettere route statiche per la rete remota sul lato del gateway del cliente. Le informazioni sulla route pubblicizzate BGP e immesse staticamente consentono ai gateway su entrambi i lati di determinare quali tunnel sono disponibili e reinstradare il traffico se si verifica un errore. Ti consigliamo di configurare la rete per utilizzare le informazioni di routing fornite da BGP (se disponibile) per selezionare un percorso disponibile. La configurazione Esatta dipende dall'architettura della rete.

Per ulteriori informazioni sulla creazione e la configurazione di un gateway del cliente e di una connessione Site-to-Site VPN, consulta Guida introduttiva con AWS Site-to-Site VPN.

Il dispositivo gateway del cliente

Un dispositivo gateway del cliente è un'appliance fisica o software che possiedi o gestisci nella rete on-premise (sul lato di una connessione Site-to-Site VPN). Tu o l'amministratore di rete dovete configurare il dispositivo in modo che funzioni con la connessione Site-to-Site VPN.

Il diagramma sottostante mostra la rete, il dispositivo gateway del cliente e la connessione VPN che va al gateway privato virtuale che è collegato al VPC. Le due linee tra il dispositivo gateway del cliente e il gateway privato virtuale rappresentano i tunnel per la connessione VPN. Se si verifica un guasto del dispositivo all'interno AWS, la connessione VPN passa automaticamente al secondo tunnel in modo che l'accesso non venga interrotto. Di tanto in tanto, esegue AWS anche la manutenzione ordinaria della connessione VPN, il che potrebbe disabilitare brevemente uno dei due tunnel della connessione VPN. Per ulteriori informazioni, consulta Sostituzioni degli endpoint del tunnel Site-to-Site VPN. Durante la configurazione del dispositivo gateway del cliente, è pertanto importante configurare entrambi i tunnel.



Per le fasi di configurazione di una connessione VPN, consulta Guida introduttiva con AWS Site-to-Site VPN. Durante questo processo, crei una risorsa Customer Gateway in AWS, che fornisce informazioni AWS sul dispositivo, ad esempio l'indirizzo IP rivolto al pubblico. Per ulteriori informazioni, consulta Opzioni di gateway del cliente per la connessione Site-to-Site VPN. La risorsa Customer Gateway in AWS non configura o crea il dispositivo Customer Gateway. È necessario configurare autonomamente il dispositivo.

È inoltre possibile trovare le appliance software VPN in AWS Marketplace.

Argomenti

File di configurazione di esempio

Dopo aver creato la connessione VPN, è inoltre possibile eseguire il download di un file di configurazione di esempio fornito da AWS dalla console Amazon VPC o utilizzando l'API EC2. Per ulteriori informazioni, consulta Fase 6: download del file di configurazione. È inoltre possibile eseguire il download di file .zip di configurazioni di esempio specificamente per il routing statico e dinamico:

Eseguire il download di file .zip

- Dati di configurazione statici: the section called “File di configurazione di esempio”
- Configurazione dinamica: the section called “File di configurazione di esempio”

Il file AWS di configurazione di esempio fornito contiene informazioni specifiche sulla connessione VPN che puoi utilizzare per configurare il dispositivo gateway del cliente. Questi file di configurazione specifici del dispositivo sono disponibili solo per i dispositivi che sono stati sottoposti a test da AWS. Se il dispositivo gateway del cliente specifico non è elencato, è possibile eseguire il download di file di configurazione generico per cominciare.

> **Important**
>
> Il file di configurazione è solo un esempio e potrebbe non corrispondere interamente alle impostazioni di connessione Site-to-Site VPN previste. Specifica i requisiti minimi per una connessione VPN da sito a sito di AES128, SHA1 e Diffie-Hellman gruppo 2 AWS nella

maggior parte delle regioni e AES128, SHA2 e Diffie-Hellman gruppo 14 nelle regioni. AWS GovCloud Specifica anche le chiavi precondivise per autenticazione. È necessario modificare il file di configurazione di esempio per sfruttare i vantaggi di algoritmi di sicurezza aggiuntivi, gruppi Diffie-Hellman, certificati privati e traffico IPv6.

Note

Questi file AWS di configurazione specifici del dispositivo vengono forniti da con la massima diligenza possibile. Sebbene siano stati testati da AWS, questi test sono limitati. Se si verifica un problema con i file di configurazione, potrebbe essere necessario contattare il fornitore specifico per ottenere ulteriore supporto.

La tabella seguente contiene un elenco di dispositivi che dispongono di un file di configurazione di esempio disponibile per il download che è stato aggiornato per supportare IKEv2. Abbiamo introdotto il supporto IKEv2 nei file di configurazione per molti dispositivi gateway del cliente e continueremo ad aggiungere file aggiuntivi nel tempo. Questo elenco verrà aggiornato man mano che vengono aggiunti altri file di configurazione di esempio.

Vendor	Piattaforma	Software
Checkpoint	Gaia	R80.10+
Cisco Meraki	Serie MX	15.12+ (WebUI)
Cisco Systems, Inc.	Serie ASA 5500	ASA 9.7+ VTI
Cisco Systems, Inc.	CSRv AMI	IOS 12.4+
Fortinet	Serie Fortigate 40+	FortiOS 6.4.4+ (GUI)
Juniper Networks, Inc.	Router Serie J	JunOS 9.5+
Juniper Networks, Inc.	Router SRX	JunOS 11.0+
Mikrotik	RouterOS	6.4.3
Palo Alto Networks	Serie PA	PANOS 7.0+

Vendor	Piattaforma	Software
SonicWall	NSA, TZ	OS 6.5
Sophos	Firewall Sophos	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	Router RTX	Rev.10.01.16+

Requisiti per il dispositivo gateway del cliente

Se è disponibile un dispositivo non incluso nell'elenco precedente di esempi, in questa sezione vengono descritti i requisiti che il dispositivo deve soddisfare affinché possa essere utilizzato per stabilire una connessione Site-to-Site VPN.

La configurazione del dispositivo gateway del cliente comprende quattro parti principali. I seguenti simboli rappresentano ciascuna parte della configurazione.

	Associazione di sicurezza Internet key exchange (IKE). Richiesta per scambiare chiavi utilizzate per stabilire l'associazione di sicurezza IPsec.
	Associazione di sicurezza IPsec. Consente di gestire la crittografia, l'autenticazione e così via del tunnel.
	Interfaccia tunnel. Riceve il traffico in uscita e in entrata dal tunnel.
	(Facoltativo) Peer secondo il protocollo BGP (Border Gateway Protocol). Per dispositivi che utilizzano BGP, consente di scambiare route tra il dispositivo gateway del cliente e il gateway virtuale privato.

Nella tabella seguente vengono elencate i requisiti del dispositivo gateway del cliente, l'RFC (per riferimento) correlato e i commenti sui requisiti.

Ogni connessione VPN è composta da due tunnel distinti. Ogni tunnel contiene un'associazione di sicurezza IKE, un'associazione di sicurezza IPsec e un peering BGP. Esiste un vincolo di una 1 coppia di associazione di sicurezza univoca (SA) per tunnel (1 in entrata e 1 in uscita), ovvero 2

coppie SA univoche in totale per 2 tunnel (4 SA). Alcuni dispositivi utilizzano una VPN basata su policy e creano il numero massimo consentito di SA come voci ACL. Pertanto, potrebbe essere necessario consolidare le regole e filtrare in modo da non consentire traffico non desiderato.

Per impostazione predefinita, il tunnel VPN si verifica quando viene generato il traffico e la negoziazione IKE viene avviata dal lato della connessione VPN. Puoi invece configurare la connessione VPN per avviare la negoziazione IKE dal AWS lato della connessione. Per ulteriori informazioni, consulta Opzioni di avvio del tunnel Site-to-Site VPN.

Gli endpoint VPN supportano l'emissione nuova chiave e possono avviare rinegoziazioni quando la fase 1 sta per scadere se il dispositivo gateway del cliente non ha inviato alcun traffico di rinegoziazione.

Requisito	RFC	Commenti
Stabilire l'associazione di sicurezza IKE IKE	RFC 2409 RFC 7296	L'associazione di sicurezza IKE viene stabilita innanzitutto tra il gateway privato virtuale e il dispositivo gateway del cliente utilizzando una chiave precondivisa o un certificato privato che utilizza come autenticatore. AWS Private Certificate Authority Al termine, IKE negozia una chiave effimera per rendere sicuri i messaggi IKE futuri. Ci deve essere un accordo completo tra i parametri, inclusi i parametri di crittografia e autenticazione. Quando crei una connessione VPN in AWS, puoi specificare la tua chiave già condivisa per ogni tunnel, oppure puoi lasciare AWS che ne generi una per te. In alternativa, puoi specificare il certificato privato AWS Private Certificate Authority da utilizzare per il dispositivo gateway del cliente. Per ulteriori informazioni sulla configurazione dei tunnel VPN, consulta Opzioni di tunnel per la connessione Site-to-Site VPN. Sono supportate le seguenti versioni: IKEv1 e IKEv2. Con IKEv1 supportiamo solamente la modalità Main.

Requisito	RFC	Commenti
		Il servizio Site-to-Site VPN è una soluzione basata su route. Se usi una configurazione basata su policy, devi limitare la configurazione a un'unica associazione di sicurezza (SA).
Stabilire associazioni di sicurezza IPsec in modalità Tunnel IPsec	RFC 4301	Utilizzando la chiave effimera IKE, le chiavi vengono stabilite tra il gateway virtuale privato e il dispositivo gateway del cliente per formare un'associazione di sicurezza IPsec (SA). Il traffico tra i gateway è crittografato e decrittografato utilizzando questa SA. Le chiavi effimere utilizzate per crittografare il traffico all'interno della SA IPsec vengono automaticamente ruotate da IKE periodicamente per garantire la riservatezza delle comunicazioni.
Utilizzare la funzione di crittografia a 128 bit o 256 bit AES	RFC 3602	La funzione di crittografia viene utilizzata per garantire la privacy per le associazioni di sicurezza IKE e IPsec.
Utilizzare la funzione di hashing SHA-1 o SHA-2 (256)	RFC 2404	Questa funzione di hashing viene utilizzata per autenticare le associazioni di sicurezza IKE è IPsec.
Utilizzare Diffie-Hellman Perfect Forward Secrecy.	RFC 2409	IKE utilizza Diffie-Hellman per stabilire chiavi effimere per rendere sicura tutta la comunicazione tra i dispositivi gateway del cliente e i gateway virtuali privati. Sono supportati i seguenti gruppi: • Gruppi fase 1: 2, 14-24 • Gruppi fase 2: 2, 5, 14-24

Requisito	RFC	Commenti
(Connessioni VPN instradate dinamicamente) Utilizzare IPSec Dead Peer Detection	RFC 3706	Dead Peer Detection consente ai dispositivi VPN di identificare rapidamente quando una condizione di rete impedisce la consegna di pacchetti su Internet. Quando ciò si verifica, i gateway eliminano le associazioni di sicurezza e tentano di creare nuove associazioni. Durante questo processo, viene utilizzato il tunnel IPsec alternativo, se possibile.
(Connessioni VPN instradate dinamicamente) Vincolare tunnel a interfaccia logica (VPN basata su route) 	Nessuno	Il dispositivo deve essere in grado di associare il tunnel IPSec a un'interfaccia logica. L'interfaccia logica contiene un indirizzo IP utilizzato per stabilire il peering BGP al gateway virtuale privato. Questa interfaccia logica non deve eseguire ulteriore incapsulamento (ad esempio, GRE o IP in IP). L'interfaccia deve Essere impostata su un'unità massima di trasmissione (MTU) di 1399 byte.
(Connessioni VPN instradate dinamicamente) Stabilire peering BGP 	RFC 4271	BGP viene utilizzato per scambiare route tra i dispositivi gateway del cliente e il gateway virtuale privato per dispositivi che utilizzano BGP. Tutto il traffico BGP è crittografato e trasmesso tramite l'associazione di sicurezza IPsec. BGP è obbligatorio per entrambi i gateway per scambiare i prefissi IP raggiungibili tramite l'SA IPsec.

Una connessione AWS VPN non supporta Path MTU Discovery (RFC 1191).

Se tra il dispositivo gateway del cliente e Internet è presente un firewall, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente.

Best practice per il dispositivo gateway del cliente

Usa IKEv2

Consigliamo vivamente di utilizzare IKEv2 per la connessione VPN da sito a sito. IKEv2 è un protocollo più semplice, robusto e sicuro di IKEv1. È necessario utilizzare IKEv1 solo se il dispositivo gateway del cliente non supporta IKEv2. Per ulteriori dettagli sulle differenze tra IKEv1 e IKEv2, vedere l'Appendice A della RFC7296.

Ripristina il flag "Don't Fragment" (Non frammentare) sui pacchetti

Alcuni pacchetti trasportano un flag, noto come il flag Don't Fragment (DF), che indica che il pacchetto non deve Essere frammentato. Se i pacchetti trasportano il flag, i gateway generano un messaggio ICMP Path MTU Exceeded (MTU percorso ICMP superato). In alcuni casi, le applicazioni non contengono meccanismi adeguati per elaborare questi messaggi ICMP e per ridurre la quantità di dati trasmessa in ogni pacchetto. Alcuni dispositivi VPN possono ignorare il flag DF e frammentare i pacchetti incondizionatamente come richiesto. Se il dispositivo gateway del cliente dispone di questa capacità, ti consigliamo di utilizzarla in maniera adeguata. Consulta .RFC 791per ulteriori dettagli.

Frammentare pacchetti IP prima della crittografia

Se i pacchetti inviati tramite la connessione VPN da sito a sito superano la dimensione MTU, devono essere frammentati. Per evitare una riduzione delle prestazioni, consigliamo di configurare il dispositivo gateway del cliente in modo da frammentare i pacchetti prima che vengano crittografati. La VPN da sito a sito riassemblerà quindi tutti i pacchetti frammentati prima di inoltrarli alla destinazione successiva, al fine di ottenere flussi più elevati attraverso la rete. packet-per-second AWS Consulta RFC 4459 per ulteriori dettagli.

Assicurati che la dimensione dei pacchetti non superi l'MTU per le reti di destinazione

Poiché la VPN da Site-to-Site riassembla tutti i pacchetti frammentati ricevuti dal dispositivo gateway del cliente prima di inoltrarli alla destinazione successiva, tieni presente che potrebbero esserci considerazioni sulla dimensione dei pacchetti/MTU per le reti di destinazione in cui questi pacchetti verranno successivamente inoltrati, ad esempio. AWS Direct Connect

Regolare le dimensioni MTU e MSS in base agli algoritmi in uso

I pacchetti TCP sono spesso il tipo più comune di pacchetti su tunnel IPsec. La VPN Site-to-Site supporta un'unità di trasmissione massima (MTU) di 1446 byte e una corrispondente dimensione massima del segmento (MSS) di 1406 byte. Tuttavia, gli algoritmi di crittografia hanno dimensioni di intestazione diverse e possono impedire la possibilità di raggiungere questi valori massimi. Per ottenere prestazioni ottimali evitando la frammentazione, si consiglia di impostare MTU e MSS in base agli algoritmi utilizzati.

Utilizza la seguente tabella per impostare MTU/MSS per evitare la frammentazione e ottenere prestazioni ottimali:

Algoritmo di crittografia	Algoritmo hash	NAT-Traversal	MTU	MSS (IPv4)	MSS (IPv6-in-IPv4)
AES-GCM-16	N/D	disabled	1446	1406	1386
AES-GCM-16	N/D	abilitato	1438	1398	1378
AES-CBC	SHA1/SHA2-256	disabled	1438	1398	1378
AES-CBC	SHA1/SHA2-256	abilitato	1422	1382	1362
AES-CBC	SHA2-384	disabled	1422	1382	1362
AES-CBC	SHA2-384	abilitato	1422	1382	1362
AES-CBC	SHA2-512	disabled	1422	1382	1362
AES-CBC	SHA2-512	abilitato	1406	1366	1346

> **Note**
>
> Gli algoritmi AES-GCM includono sia la crittografia che l'autenticazione, quindi non esiste una scelta distinta di algoritmo di autenticazione che influenzi MTU.

Disattiva gli ID univoci IKE

Alcuni dispositivi gateway del cliente supportano un'impostazione che garantisce l'esistenza al massimo di un'associazione di sicurezza di Fase 1 per configurazione del tunnel. Questa impostazione può causare stati di Fase 2 non coerenti tra i peer VPN. Se il dispositivo gateway del cliente supporta questa impostazione, consigliamo di disabilitarla.

Configurazione di un firewall tra Internet e il dispositivo gateway del cliente

È necessario disporre di un indirizzo IP statico da utilizzare come endpoint per i tunnel IPSec che collegano il dispositivo gateway del cliente agli endpoint. AWS Site-to-Site VPN Se è installato un firewall tra il dispositivo gateway del cliente AWS e il dispositivo gateway del cliente, è necessario applicare le regole riportate nelle tabelle seguenti per stabilire i tunnel IPSec. Gli indirizzi IP per il AWS lato -side si troveranno nel file di configurazione.

In entrata (da Internet)

Regola in entrata I1	
IP di origine	IP esterno Tunnel1
IP dest	Gateway del cliente
Protocollo	UDP
Porta sorgente	500
Destinazione	500
Regola in entrata I2	
IP di origine	IP esterno Tunnel2
IP dest	Gateway del cliente
Protocollo	UDP
Porta sorgente	500
Porta di destinazione	500
Regola in entrata I3	
IP di origine	IP esterno Tunnel1
IP dest	Gateway del cliente

Protocollo	IP 50 (ESP)
Regola in entrata I4	
IP di origine	IP esterno Tunnel2
IP dest	Gateway del cliente
Protocollo	IP 50 (ESP)

In uscita (a Internet)

Regola in uscita O1	
IP di origine	Gateway del cliente
IP dest	IP esterno Tunnel1
Protocollo	UDP
Porta sorgente	500
Porta di destinazione	500
Regola in uscita O2	
IP di origine	Gateway del cliente
IP dest	IP esterno Tunnel2
Protocollo	UDP
Porta sorgente	500
Porta di destinazione	500
Regola in uscita O3	
IP di origine	Gateway del cliente
IP dest	IP esterno Tunnel1

Protocollo	IP 50 (ESP)
Regola in uscita O4	
IP di origine	Gateway del cliente
IP dest	IP esterno Tunnel2
Protocollo	IP 50 (ESP)

Le regole I1, I2, O1 e O2 abilitano la trasmissione di pacchetti IKE. Le regole I3, I4, O3 e O4 abilitano la trasmissione di pacchetti IPsec contenenti il traffico di rete crittografato.

> **Note**
>
> Se utilizzi NAT traversal (NAT-T) sul tuo dispositivo, assicurati che anche il traffico UDP sulla porta 4500 possa passare tra la tua rete e gli endpoint. AWS Site-to-Site VPN Verifica se il dispositivo pubblicizza NAT-T.

Più scenari di connessione VPN

Di seguito sono riportati gli scenari in cui è possibile creare più connessioni VPN con uno o più dispositivi gateway del cliente.

Più connessioni VPN che utilizzano lo stesso dispositivo gateway del cliente

È possibile creare connessioni VPN aggiuntive dalla posizione in locale ad altri VPC utilizzando lo stesso dispositivo gateway del cliente. Puoi riutilizzare lo stesso indirizzo IP del gateway del cliente per ciascuna di tali connessioni VPN.

Connessione VPN ridondante utilizzando un secondo dispositivo gateway del cliente

Per garantire la protezione da una perdita di connettività nel caso in cui il dispositivo gateway del cliente diventi non disponibile, puoi configurare una seconda connessione VPN mediante un secondo dispositivo gateway del cliente. Per ulteriori informazioni, consulta Utilizzo di connessioni Site-to-Site VPN ridondanti per fornire il failover. Quando stabilisci dispositivi gateway del cliente ridondanti in una singola posizione, entrambi i dispositivi devono promuovere gli stessi intervalli IP.

Più dispositivi gateway per i clienti verso un unico gateway privato virtuale ()AWS VPN CloudHub

Puoi stabilire più connessioni VPN a un singolo gateway virtuale privato da più dispositivi gateway del cliente. Ciò consente di avere più postazioni connesse alla AWS VPN CloudHub. Per ulteriori informazioni, consulta Fornire una comunicazione sicura tra siti utilizzando VPN CloudHub. Quando disponi di dispositivi gateway del cliente in corrispondenza di più posizioni geografiche, ogni dispositivo deve promuovere un set univoco di intervalli IP specifici per la posizione.

Routing per il dispositivo gateway del cliente

AWS consiglia di pubblicizzare percorsi BGP specifici per influenzare le decisioni di routing nel gateway privato virtuale. Controlla la documentazione del fornitore per i comandi specifici del dispositivo.

Quando crei più connessioni VPN, il gateway virtuale privato invia il traffico di rete alla connessione VPN appropriata utilizzando route assegnate staticamente o annunci di routing BGP, a seconda della configurazione della connessione VPN. Le route assegnate staticamente sono preferite rispetto alle route pubblicizzate BGP nei casi in cui sono presenti route identiche nel gateway virtuale privato. Se selezioni l'opzione per utilizzare l'annuncio BGP, non puoi specificare route statiche.

Per ulteriori informazioni sulla priorità delle route, consulta Tabelle di routing e priorità della route VPN.

Esempio di configurazioni del dispositivo gateway del cliente per il routing statico

Argomenti

File di configurazione di esempio

Per scaricare un file di configurazione di esempio con valori specifici per la configurazione della connessione VPN da sito a sito, usa la console Amazon VPC, la AWS riga di comando o l'API Amazon EC2. Per ulteriori informazioni, consulta Fase 6: download del file di configurazione.

È inoltre possibile il download di file di configurazione generici di esempio per il routing statico che non includono valori specifici per la configurazione della connessione Site-to-Site VPN: static-routing-examples.zip

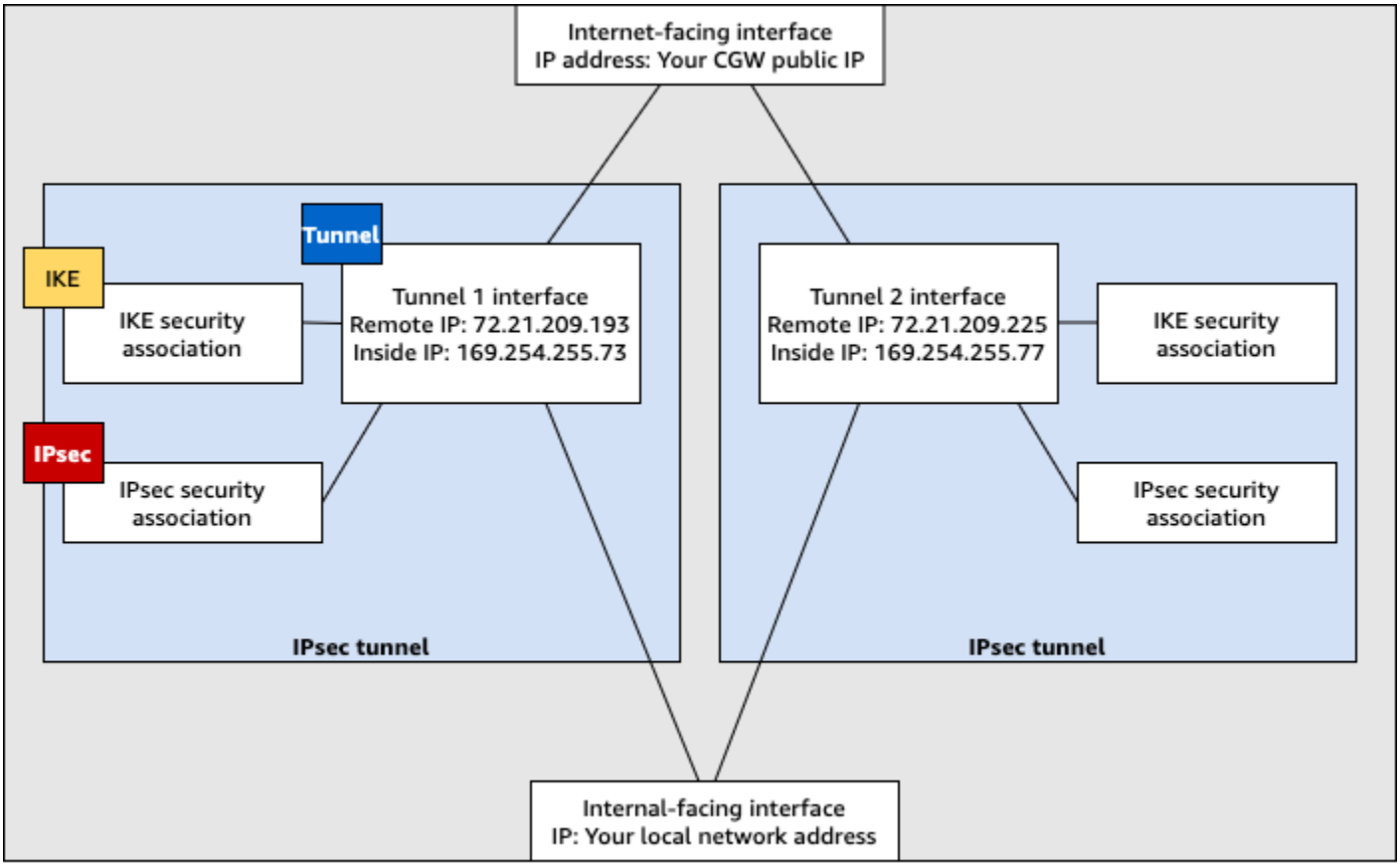
I file utilizzano valori segnaposto per alcuni componenti. Ad esempio, utilizzano:

- Valori di esempio per l'ID connessione VPN l'ID gateway del cliente e l'ID gateway virtuale privato
- *Segnaposto per gli endpoint degli indirizzi IP remoti (esterni) (AWS_ENDPOINT_1 e AWS_ENDPOINT_2) AWS*
- Un segnaposto per l'indirizzo IP per l'interfaccia esterna Internet instradabile sul dispositivo gateway del cliente (*your-cgw-ip-address*).
- Un segnaposto per la chiave-valore pre-condivisa (chiave pre-condivisa)
- Valori di esempio per indirizzi IP interni del tunnel.
- Valori di esempio per l'impostazione MTU.

> **Note**
>
> Le impostazioni MTU fornite nei file di configurazione di esempio sono solo esempi. Fai riferimento a Best practice per il dispositivo gateway del cliente per informazioni sull'impostazione del valore MTU ottimale per la tua situazione.

Oltre a fornire valori segnaposto, i file specificano i requisiti minimi per una connessione VPN da sito a sito di AES128, SHA1 e Diffie-Hellman gruppo 2 AWS nella maggior parte delle regioni e AES128, SHA2 e Diffie-Hellman gruppo 14 nelle regioni. AWS GovCloud Specificano inoltre le chiavi precondivise per l'autenticazione. È necessario modificare il file di configurazione di esempio per sfruttare i vantaggi di algoritmi di sicurezza aggiuntivi, gruppi Diffie-Hellman, certificati privati e traffico IPv6.

Nel diagramma seguente viene fornita una panoramica dei diversi componenti configurati nel dispositivo gateway del cliente. Questa include valori di esempio per gli indirizzi IP di interfaccia di tunnel.



Procedure dell'interfaccia utente per il routing statico

Di seguito sono riportate alcune procedure di esempio per configurare un dispositivo gateway del cliente utilizzando l'interfaccia utente (se disponibile).

Check Point

Di seguito sono riportati i passaggi per configurare il dispositivo gateway del cliente se il dispositivo è un dispositivo Check Point Security Gateway con R77.10 o versione successiva, utilizzando il sistema operativo Gaia e Check Point SmartDashboard. Puoi anche fare riferimento all'articolo Check Point Security Gateway IPsec VPN to Amazon Web Services VPC nel Check Point Support Center.

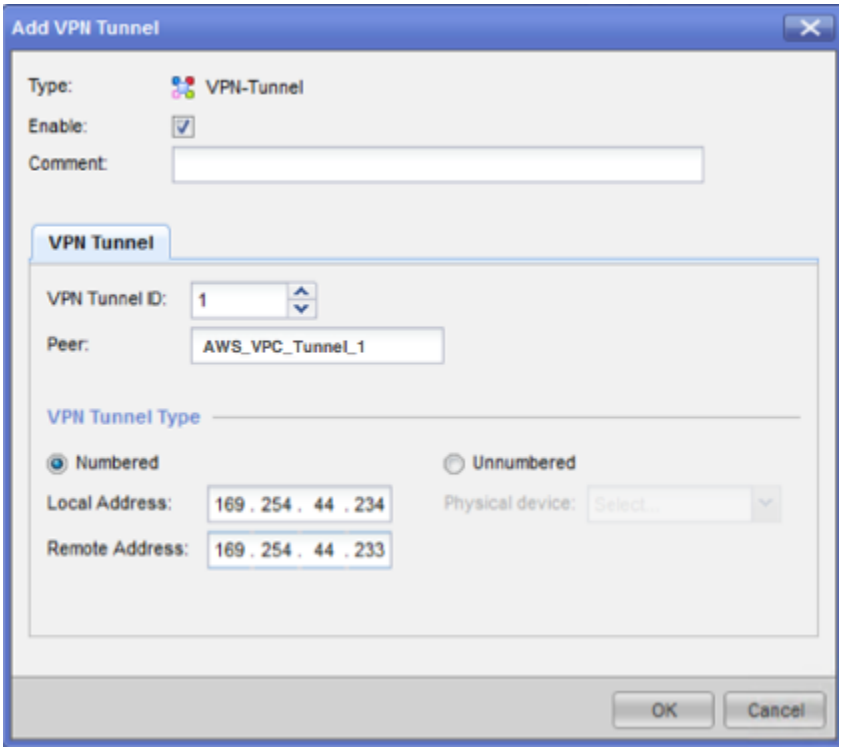
Per configurare l'interfaccia del tunnel

La prima fase consiste nel creare i tunnel VPN e fornire gli indirizzi IP (interni) privati del gateway del cliente E del gateway virtuale privato per ogni tunnel. Per creare il primo tunnel, utilizza le

informazioni fornite nella sezione `IPSec Tunnel #1` del file di configurazione. Per creare il secondo tunnel, utilizza i valori forniti nella sezione `IPSec Tunnel #2` del file di configurazione.

1. Aprire il portale Gaia del dispositivo Check Point Security Gateway.
2. Selezionare Network Interfaces (Interfacce di rete), Add (Aggiungi), VPN Tunnel (Tunnel VPN).
3. Nella finestra di dialogo, configurare le impostazioni come riportato di seguito e, al termine, scegliere OK:

   - In VPN Tunnel ID (ID tunnel VPN), immettere un valore univoco, ad esempio 1.
   - In Peer, immettere un nome univoco per il tunnel, ad esempio `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.
   - Assicurarsi che Numbered (Numerato) sia selezionato e in Local Address (Indirizzo locale) immettere l'indirizzo IP specificato per `CGW Tunnel IP` nel file di configurazione, ad esempio, `169.254.44.234`.
   - In Remote Address (Indirizzo remoto), immettere l'indirizzo IP specificato per `VGW Tunnel IP` nel file di configurazione, ad esempio, `169.254.44.233`.



4. Connettersi al gateway di sicurezza su SSH. Se si utilizza la shell non predefinita, modificare in clish eseguendo il seguente comando: `clish`

5. Per tunnel 1, eseguire il seguente comando.

   ```
   set interface vpnt1 mtu 1436
   ```

   Per tunnel 2, eseguire il seguente comando.

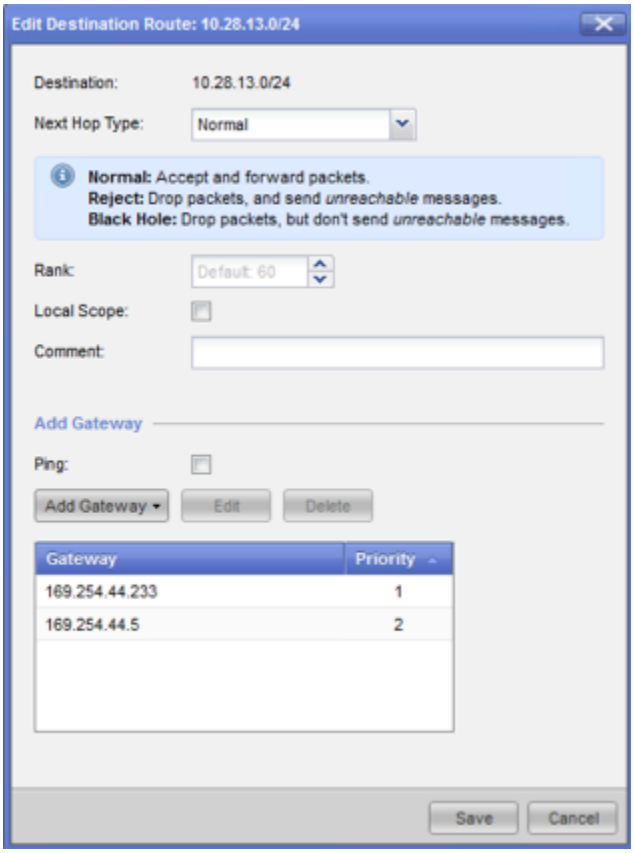
   ```
   set interface vpnt2 mtu 1436
   ```

6. Ripetere queste fasi per creare un secondo tunnel, utilizzando le informazioni nella sezione `IPSec Tunnel #2` del file di configurazione.

Per configurare le route statiche

In questa fase specifica la route statica alla sottorete nel VPC per ogni tunnel in modo da poter inviare traffico attraverso le interfacce di tunnel. Il secondo tunnel consente il failover nel caso si verifichi un problema con il primo tunnel. Se viene rilevato un problema, la route statica basata su policy viene rimossa dalla tabella di routing e viene attivato il secondo instradamento. Devi inoltre abilitare il gateway Check Point per eseguire il ping dell'altra estremità del tunnel per verificare se il tunnel è attivo.

1. Nel portale Gaia, scegliere IPv4 Static Routes (Route statiche IPv4), Add (Aggiungi).
2. Specificare il CIDR della sottorete, ad esempio, `10.28.13.0/24`.
3. Selezionare Add Gateway (Aggiungi gateway), IP Address (Indirizzo IP).
4. Immettere l'indirizzo IP specificato per `VGW Tunnel IP` nel file di configurazione (ad esempio `169.254.44.233`) e specificare la priorità 1.
5. Selezionare Ping.
6. Ripetere le fasi 3 e 4 per il secondo tunnel utilizzando il valore `VGW Tunnel IP` nella sezione `IPSec Tunnel #2` del file di configurazione. Specificare la priorità 2.



7. Selezionare Salva.

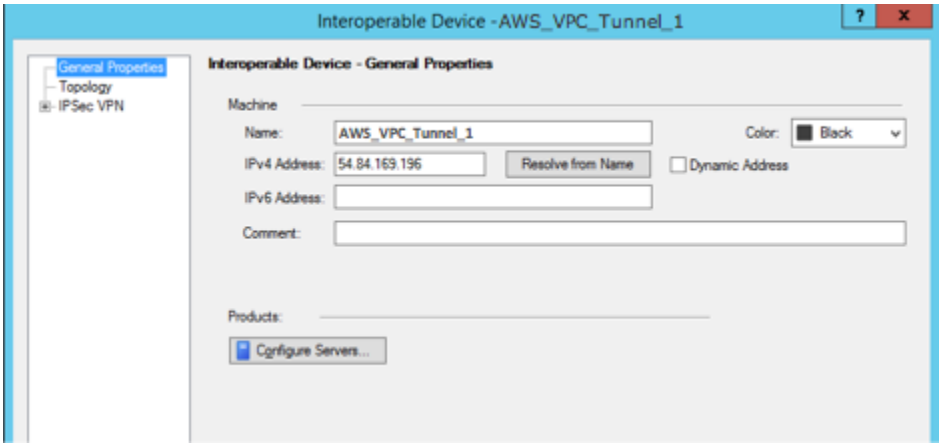
Se utilizzi un cluster, ripeti le fasi precedenti per gli altri membri del cluster.

Per definire un nuovo oggetto di rete

In questa fase, viene creato un oggetto di rete per ogni tunnel VPN, specificando gli indirizzi IP (esterni) pubblici per il gateway virtuale privato. In seguito questi oggetti vengono aggiunti come gateway satellite per la comunità VPN. Occorre anche creare un gruppo vuoto che agisce come segnaposto per il dominio VPN.

1. Apri il Check Point. SmartDashboard
2. In Groups (Gruppi), aprire il menu contestuale e scegliere Groups (Gruppi), Simple Group (Gruppo semplice). Lo stesso gruppo può essere utilizzato per ogni oggetto di rete.
3. In Network Objects (Oggetti di rete), aprire il menu contestuale (tasto destro del mouse) e scegliere New (Nuovo), Interoperable Device (Dispositivo interoperabile).
4. In Name (Nome), immettere il nome fornito per il tunnel, ad esempio `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.

5. In IPv4 Address (Indirizzo IPv4), immettere l'indirizzo IP esterno del gateway virtuale privato fornito nel file di configurazione, ad esempio `54.84.169.196`. Salvare le impostazioni e chiudere la finestra di dialogo.



6. In SmartDashboard, apri le proprietà del gateway e nel riquadro delle categorie, scegli Topologia.
7. Per recuperare la configurazione dell'interfaccia, scegliere Get Topology (Ottieni topologia).
8. Nella sezione VPN Domain (Dominio VPN), scegliere Manually defined (Definito manualmente), quindi individuare e selezionare il gruppo semplice vuoto creato nella fase 2. Scegli OK.

> **Note**
>
> È possibile mantenere qualsiasi dominio VPN esistente che è stato configurato. Tuttavia, assicurarsi che host e reti utilizzate o servite dalla nuova connessione VPN non siano dichiarate in tale dominio VPN, in particolare se il dominio VPN viene derivato automaticamente.

9. Ripetere queste fasi per creare un secondo oggetto di rete, utilizzando le informazioni fornite nella sezione `IPSec Tunnel #2` del file di configurazione.

> **Note**
>
> Se stai utilizzando cluster, modifica la topologia e definisci le interfacce come interfacce del cluster. Utilizza gli indirizzi IP specificati nel file di configurazione.

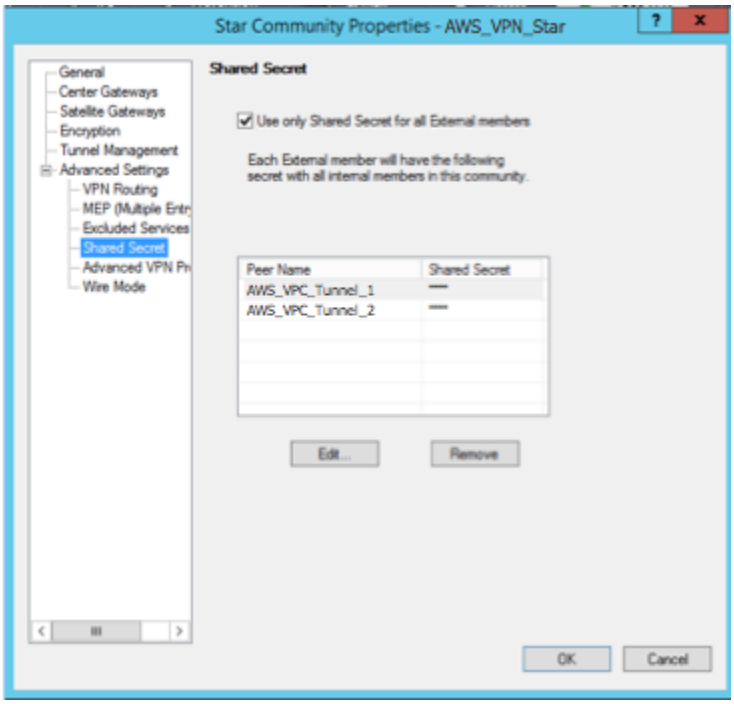
Per creare e configurare le impostazioni comunità VPN, IKE e IPsec

In questa fase, viene creata una comunità VPN nel gateway Check Point a cui aggiungere oggetti di rete (dispositivi interoperabili) per ogni tunnel. Vengono anche configurate le impostazioni Internet Key Exchange (IKE) e IPsec.

1. Dalle proprietà del gateway, scegliere IPSec VPN (VPN IPSec) nel riquadro delle categorie.
2. Selezionare Communities (Comunità), New (Nuova), Star Community (Comunità stella).
3. Fornire un nome per la comunità (ad esempio, `AWS_VPN_Star`), quindi selezionare Center Gateways (Gateway centrali) nel riquadro delle categorie.
4. Selezionare Add (Aggiungi) e aggiungere il gateway o il cluster all'elenco dei gateway partecipanti.
5. Nel riquadro delle categorie, selezionare Satellite Gateways (Gateway satellite), Add (Aggiungi), quindi aggiungere i dispositivi interoperabili creati in precedenza (`AWS_VPC_Tunnel_1` e `AWS_VPC_Tunnel_2`) all'elenco di gateway partecipanti.
6. Nel riquadro delle categorie, selezionare Encryption (Crittografia). Nella sezione Encryption Method (Metodo di crittografia), scegliere IKEv1 only (Solo IKEv1). Nella sezione Encryption Suite (Suite di crittografia), scegliere Custom (Personalizzato), Custom Encryption (Crittografia personalizzata).
7. Nella finestra di dialogo, configurare le proprietà di crittografia come riportato di seguito e, al termine, scegliere OK:

   - Proprietà IKE Security Association (fase 1):
     - Perform key exchange Encryption with (Esegui crittografia scambio delle chiavi con): AES-128
     - Perform data integrity with (Esegui integrità dei dati con): SHA-1
   - Proprietà IPSec Security Association (fase 2):
     - Perform IPsec data encryption with (Esegui crittografia dati IPsec con): AES-128
     - Perform data integrity with (Esegui integrità dei dati con): SHA-1
8. Nel riquadro delle categorie, selezionare Tunnel Management (Gestione tunnel). Selezionare Set Permanent Tunnels (Imposta tunnel permanenti), On all tunnels in the community (Su tutti i tunnel nelle comunità). Nella sezione VPN Tunnel Sharing (Condivisione tunnel VPN), scegliere One VPN tunnel per Gateway pair (Un tunnel VPN per coppia gateway).
9. Nel riquadro delle categorie, espandere Advanced Settings (Impostazioni avanzate) e scegliere Shared Secret (Segreto condiviso).

10. Selezionare il nome peer per il primo tunnel, scegliere Edit (Modifica) e immettere la chiave precondivisa come specificato nel file di configurazione nella sezione `IPSec Tunnel #1`.
11. Selezionare il nome peer per il secondo tunnel, scegliere Edit (Modifica) e immettere la chiave precondivisa come specificato nel file di configurazione nella sezione `IPSec Tunnel #2`.



12. Nella categoria Advanced Settings (Impostazioni avanzate), scegliere Advanced VPN Properties (Proprietà VPN avanzate), configurare le proprietà come segue e, al termine, scegliere OK:

    - IKE (fase 1):
        - Use Diffie-Hellman group (Utilizza gruppo Diffie-Hellman): `Group 2`
        - Renegotiate IKE security associations every (Rinegozia associazioni sicurezza IKE ogni) `480` minutes (minuti)
    - IPsec (fase 2):
        - Selezionare Use Perfect Forward Secrecy (Utilizza Perfect Forward Secrecy)
        - Use Diffie-Hellman group (Utilizza gruppo Diffie-Hellman): `Group 2`
        - Renegotiate IPsec security associations every (Rinegozia associazioni sicurezza IPsec ogni) `3600` seconds (secondi)

Per creare regole del firewall

In questa fase viene configurata una policy con regole del firewall e regole di corrispondenza direzionali che consentono la comunicazione tra il VPC e la rete locale. Viene quindi installata la policy nel gateway.

1. Nella finestra SmartDashboard, scegli Proprietà globali per il tuo gateway. Nel riquadro delle categorie, espandere VPN e scegliere Advanced (Avanzate).
2. Selezionare Enable VPN Directional Match in VPN Column (Abilita corrispondenza VPN direzionale nella colonna VPN) e salvare le modifiche.
3. Nella SmartDashboard, scegli Firewall e crea una politica con le seguenti regole:
   - Consente la comunicazione tra la sottorete VPC e la rete locale sui protocolli richiesti.
   - Consente la comunicazione tra la rete locale e la sottorete VPC sui protocolli richiesti.
4. Aprire il menu contestuale per la cella nella colonna VPN e scegliere Edit Cell (Modifica cella).
5. Nella finestra di dialogo VPN Match Conditions (Condizioni corrispondenza VPN), scegliere Match traffic in this direction only (Corrispondenza traffico solo in questa direzione). Creare le seguenti regole di corrispondenza direzionale scegliendo Add (Aggiungi) per ognuna e, al termine, selezionare OK:
   - `internal_clear` > comunità VPN (la comunità stella VPN creata in precedenza, ad esempio `AWS_VPN_Star`)
   - Comunità VPN > Comunità VPN
   - Community VPN > `internal_clear`
6. Nel SmartDashboard, scegli Policy, Installa.
7. Nella finestra di dialogo, scegliere il gateway e quindi OK per installare la policy.

Per modificare la proprietà tunnel_keepalive_method

Il gateway Check Point può utilizzare Dead Peer Detection (DPD) per identificare quando un'associazione IKE è inattiva. Per configurare DPD per un tunnel permanente, il tunnel permanente deve essere configurato nella community AWS VPN (fare riferimento al passaggio 8).

Per impostazione predefinita, la proprietà `tunnel_keepalive_method` per un gateway VPN è impostata su `tunnel_test`. Occorre modificare il valore in dpd. Ogni gateway VPN nella

community VPN che richiede il monitoraggio DPD deve essere configurato con la proprietà `tunnel_keepalive_method`, inclusi eventuali gateway VPN di terze parti. Non è possibile configurare meccanismi di monitoraggio diversi per lo stesso gateway.

Puoi aggiornare la proprietà `tunnel_keepalive_method` utilizzando lo strumento GuiDBedit.

1. Apri il Check Point SmartDashboard e scegli Security Management Server, Domain Management Server.
2. Selezionare File, Database Revision Control... (Controllo revisione database...) e creare una snapshot di revisione.
3. Chiudi tutte le SmartConsole finestre, come SmartView Tracker e SmartView Monitor. SmartDashboard
4. Avviare lo strumento GuiBDedit. Per ulteriori informazioni, consulta l'articolo Check Point Database Tool in Check Point Support Center.
5. Selezionare Security Management Server (Server di gestione della sicurezza), Domain Management Server (Server di gestione domini).
6. Nel riquadro in alto a sinistra, scegliere Table (Tabella), Network Objects (Oggetti di rete), network_objects.
7. Nel riquadro in alto a destra, selezionare l'oggetto Security Gateway (Gateway di sicurezza), Cluster pertinente.
8. Premere CTRL+F o utilizzare il menu Search (Cerca) per cercare quanto segue: `tunnel_keepalive_method`.
9. Nel riquadro inferiore aprire il menu contestuale per `tunnel_keepalive_method` e scegliere Edit... (Modifica...). Scegliere dpd, quindi selezionare OK.
10. Ripetere le fasi da 7 a 9 per ogni gateway che fa parte della community AWS VPN.
11. Selezionare File, Save All (Salva tutto).
12. Chiudere lo strumento GuiDBedit.
13. Apri il Check Point SmartDashboard e scegli Security Management Server, Domain Management Server.
14. Installare la policy nell'oggetto Security Gateway (Gateway di sicurezza), Cluster pertinente.

Per ulteriori informazioni, consulta l'articolo New VPN features in R77.10 in Check Point Support Center.

Per abilitare TCP MSS Clamping

TCP MSS Clamping riduce la dimensione segmento massima dei pacchetti TCP per impedire la frammentazione pacchetti.

1. Accedere alla seguente directory: `C:\Program Files (x86)\CheckPoint \SmartConsole\R77.10\PROGRAM\`.
2. AprireCheck Point Database Tool eseguendo il file `GuiDBEdit.exe`.
3. Selezionare Table (Tabella), Global Properties (Proprietà globali), properties (proprietà).
4. In `fw_clamp_tcp_mss`, scegliere Edit (Modifica). Modificare il valore in `true` e scegliere OK.

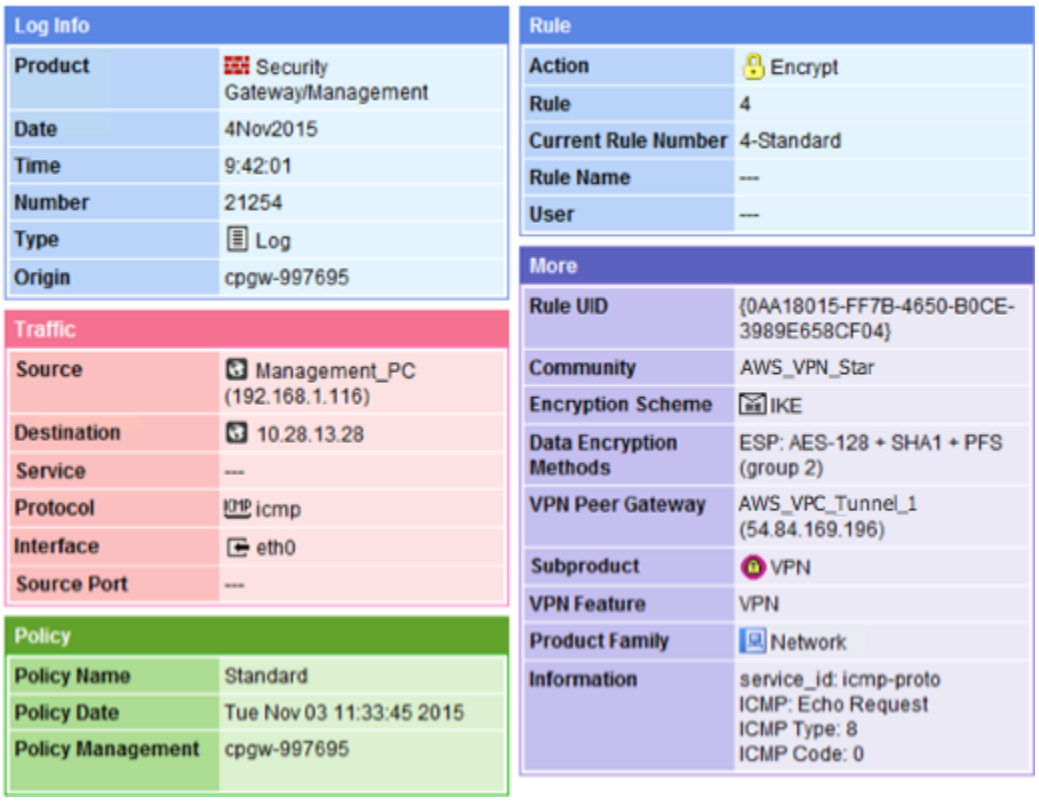
Per verificare lo stato del tunnel

Puoi verificare lo stato del tunnel eseguendo il seguente comando dallo strumento a riga di comando in modalità esperto.

```
vpn tunnelutil
```

Nelle opzioni visualizzate, scegli 1 per verificare le associazioni IKE e 2 per verificare le associazioni IPsec.

Puoi anche utilizzare Check Point Smart Tracker Log per verificare che i pacchetti sulla connessione siano crittografati. Ad esempio, il seguente log indica che un pacchetto al VPC è stato inviato su tunnel 1 ed è stato crittografato.



SonicWALL

La procedura seguente mostra come configurare i tunnel VPN nel dispositivo SonicWALL tramite l'interfaccia di gestione SonicOS.

Per configurare i tunnel

1. Aprire l'interfaccia di gestione SonicOS di SonicWALL
2. Nel riquadro a sinistra, scegliere VPN, Settings (Impostazioni). In VPN Policies (Policy VPN), scegliere Add... (Aggiungi...).
3. Nella finestra della policy VPN della scheda General (Generale) , completa le seguenti informazioni:

   - Policy Type (Tipo di policy): scegliere Tunnel Interface (Interfaccia tunnel).
   - Authentication Method (Metodo di autenticazione): selezionare IKE using Preshared Secret (IKE con segreto precondiviso).
   - Name (Nome): inserire un nome per la policy VPN. Ti consigliamo di utilizzare il nome dell'ID VPN fornito nel file di configurazione.
   - Nome o indirizzo del gateway primario IPsec: immetti l'indirizzo IP del gateway virtuale privato fornito nel file di configurazione, ad esempio `72.21.209.193`.

- IPsec Secondary Gateway Name or Address (Nome o indirizzo del gateway secondario IPsec): lasciare il valore predefinito.
- Shared Secret (Segreto condiviso): immettere la chiave già condivisa fornita nel file di configurazione e immetterla nuovamente in Confirm Shared Secret (Conferma segreto condiviso).
- Local IKE ID (ID IKE locale): immettere l'indirizzo IPv4 del gateway del cliente (il dispositivo SonicWALL).
- ID IKE in peering: immetti l'indirizzo IPv4 del gateway virtuale privato.

4. Nella scheda Network (Rete), completare le seguenti informazioni:

- In Local Networks (Reti locali), scegliere Any address (Qualsiasi indirizzo). Suggeriamo questa opzione per evitare problemi di connettività dalla rete locale.
- In Remote Networks (Reti locali), selezionare Choose a destination network from list (Scegli una rete di destinazione dall'elenco). Crea un oggetto dell'indirizzo con il blocco CIDR del VPC in AWS.

5. Nella scheda Proposals (Proposte), completare le seguenti informazioni.

- In IKE (Phase 1) Proposal (Proposta IKE fase 1), segui la procedura riportata di seguito:
  - Exchange (Scambio): scegliere Main Mode (Modalità principale).
  - DH Group (Gruppo DH): immettere un valore per il gruppo Diffie-Hellman; ad esempio 2.
  - Encryption (Crittografia): selezionare AES-128 o AES-256.
  - Authentication (Autenticazione): selezionare SHA1 o SHA256.
  - Life Time (Durata): immettere `28800`.
- In IKE (Phase 2) Proposal (Proposta IKE fase 2), segui la procedura riportata di seguito:
  - Protocol (Protocollo): selezionare ESP.
  - Encryption (Crittografia): selezionare AES-128 o AES-256.
  - Authentication (Autenticazione): selezionare SHA1 o SHA256.
  - Selezionare la casella di controllo Enable Perfect Forward Secrecy (Abilita Perfect Forward Secrecy) e scegliere il gruppo Diffie-Hellman.
  - Life Time (Durata): immettere `3600`.

> **Important**
>
> Se il gateway virtuale privato è stato creato prima dell'ottobre 2015, dovrai specificare gruppo Diffie-Hellman 2, AES-128 e SHA1 per entrambe le fasi.

6. Nella scheda Advanced (Avanzate), completare le seguenti informazioni:
   - Selezionare Enable Keep Alive (Abilita keep-alive).
   - Selezionare Enable Phase2 Dead Peer Detection (Abilita fase 2 della funzione Dead Peer Detection) e immettere quanto segue:
     - In Dead Peer Detection Interval (Intervallo Dead Peer Detection, immettere `60` (il minimo accettato dal dispositivo SonicWALL).
     - In Failure Trigger Level (Livello di attivazione dell'errore, immettere `3`.
   - In VPN Policy bound to (Policy VPN associata a), selezionare Interface X1 (Interfaccia X1). Questa interfaccia è generalmente progettata per gli indirizzi IP pubblici.
7. Scegli OK. Nella pagina Settings (Impostazioni), la casella di controllo Enable (Abilita) relativa al tunnel deve Essere selezionata per impostazione predefinita. Un punto verde indica che il tunnel è attivo.

Ulteriori informazioni per dispositivi Cisco

Alcuni dispositivi Cisco ASA supportano soltanto la modalità Active/Standby. Quando utilizzi questi Cisco ASA, puoi avere un solo tunnel attivo alla volta. Il tunnel in standby diventa attivo se il primo tunnel non è più disponibile. Con questa ridondanza, dovresti disporre sempre di una connessione al VPC via uno dei tunnel.

Cisco ASA versione 9.7.1 o versione successiva supporta la modalità attivo/attivo. Quando utilizzi i dispositivi Cisco ASA, entrambi i tunnel possono essere contemporaneamente attivi. Con questa ridondanza, dovresti disporre sempre di una connessione al VPC via uno dei tunnel.

Per dispositivi Cisco, è necessario effettuare le seguenti operazioni:

- Configurare l'interfaccia esterna.
- Verificare che il numero di sequenza della policy Crypto ISAKMP sia univoco.
- Assicurarti che il numero di sequenza della policy della lista Crypto sia univoco.

- Verificare che il set di trasformazione Crypto IPsec e la sequenza della policy Crypto ISAKMP siano compatibili con qualsiasi altro tunnel IPsec configurato sul dispositivo.
- Verificare che il numero di monitoraggio SLA sia univoco.
- Configurare l'intero routing interno che sposta il traffico tra il dispositivo gateway del cliente e la tua rete locale.

Test in corso

Per ulteriori informazioni sul test della connessione Site-to-Site VPN, consulta Test di una connessione VPN site-to-site.

Esempio di configurazioni del dispositivo gateway del cliente per il routing dinamico (BGP)

Argomenti

File di configurazione di esempio

Per scaricare un file di configurazione di esempio con valori specifici per la configurazione della connessione VPN da sito a sito, usa la console Amazon VPC, la AWS riga di comando o l'API Amazon EC2. Per ulteriori informazioni, consulta Fase 6: download del file di configurazione.

È inoltre possibile il download di file di configurazione generici di esempio per il routing dinamico che non includono valori specifici per la configurazione della connessione Site-to-Site VPN: dynamic-routing-examples.zip

I file utilizzano valori segnaposto per alcuni componenti. Ad esempio, utilizzano:

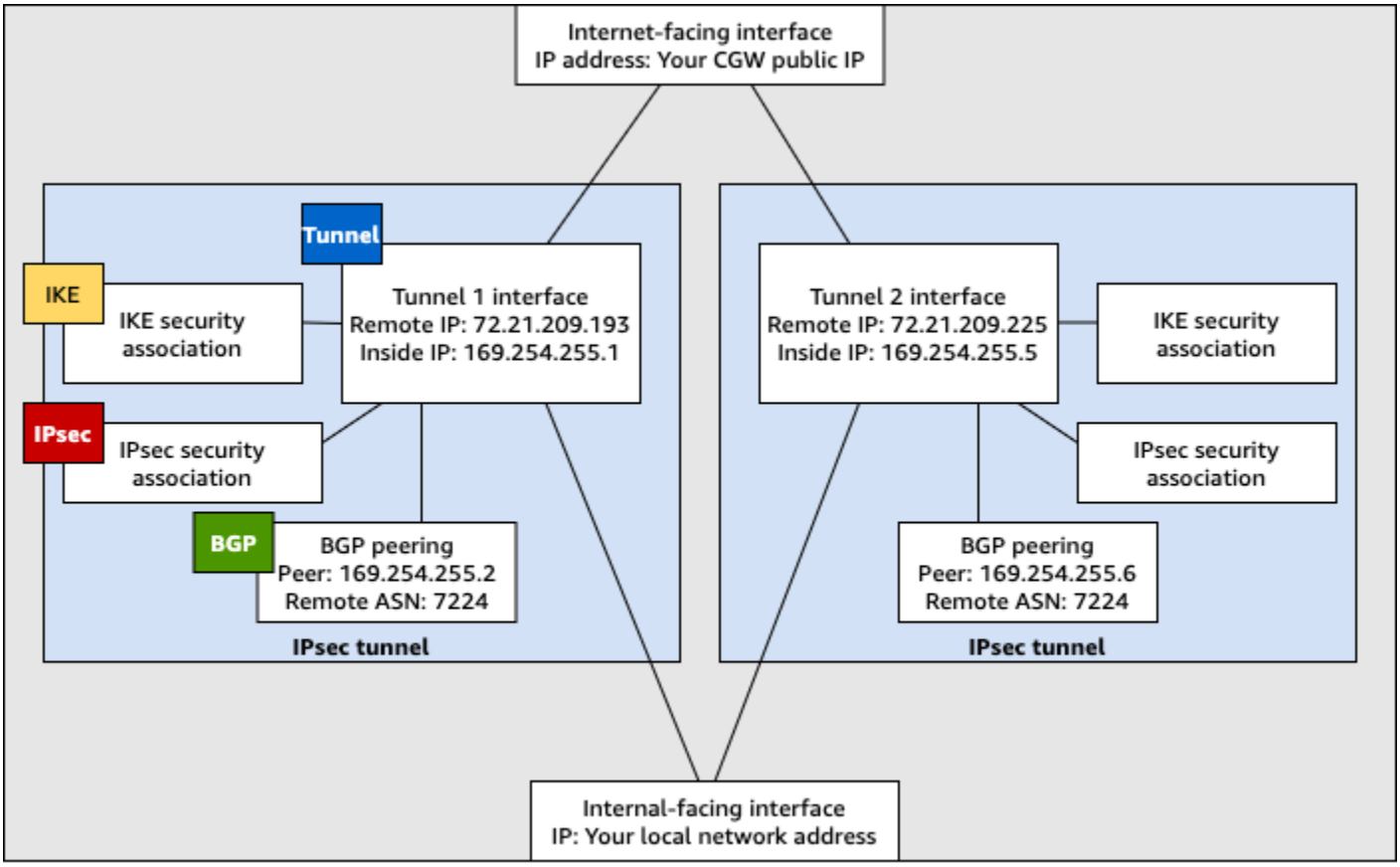
- Valori di esempio per l'ID connessione VPN l'ID gateway del cliente e l'ID gateway virtuale privato

- *Segnaposto per gli endpoint degli indirizzi IP remoti (esterni) (AWS_ENDPOINT_1 e AWS_ENDPOINT_2) AWS*
- Un segnaposto per l'indirizzo IP per l'interfaccia esterna Internet instradabile sul dispositivo gateway del cliente (*your-cgw-ip-address*).
- Un segnaposto per la chiave-valore pre-condivisa (chiave pre-condivisa)
- Valori di esempio per indirizzi IP interni del tunnel.
- Valori di esempio per l'impostazione MTU.

> **Note**
>
> Le impostazioni MTU fornite nei file di configurazione di esempio sono solo esempi. Fai riferimento a Best practice per il dispositivo gateway del cliente per informazioni sull'impostazione del valore MTU ottimale per la tua situazione.

Oltre a fornire valori segnaposto, i file specificano i requisiti minimi per una connessione VPN da sito a sito di AES128, SHA1 e Diffie-Hellman gruppo 2 AWS nella maggior parte delle regioni e AES128, SHA2 e Diffie-Hellman gruppo 14 nelle regioni. AWS GovCloud Specificano inoltre le chiavi precondivise per l'autenticazione. È necessario modificare il file di configurazione di esempio per sfruttare i vantaggi di algoritmi di sicurezza aggiuntivi, gruppi Diffie-Hellman, certificati privati e traffico IPv6.

Nel diagramma seguente viene fornita una panoramica dei diversi componenti configurati nel dispositivo gateway del cliente. Questa include valori di esempio per gli indirizzi IP di interfaccia di tunnel.



Customer gateway device

Procedure dell'interfaccia utente per il routing dinamico

Di seguito sono riportate alcune procedure di esempio per configurare un dispositivo gateway del cliente utilizzando l'interfaccia utente (se disponibile).

Check Point

Di seguito sono riportati i passaggi per configurare un dispositivo Check Point Security Gateway con R77.10 o versione successiva, utilizzando il portale web Gaia e Check Point. SmartDashboard È anche possibile fare riferimento all'articolo Amazon Web Services (AWS) VPN BGP in Check Point Support Center.

Per configurare l'interfaccia del tunnel

La prima fase consiste nel creare i tunnel VPN e fornire gli indirizzi IP (interni) privati del gateway del cliente E del gateway virtuale privato per ogni tunnel. Per creare il primo tunnel, utilizza le informazioni fornite nella sezione `IPSec Tunnel #1` del file di configurazione. Per creare il secondo tunnel, utilizza i valori forniti nella sezione `IPSec Tunnel #2` del file di configurazione.

1. Connettersi al gateway di sicurezza su SSH. Se si utilizza la shell non predefinita, modificare in clish eseguendo il seguente comando: `clish`
2. Imposta l'ASN del gateway del cliente (l'ASN fornito al momento della creazione del gateway del cliente AWS) eseguendo il comando seguente.

```
set as 65000
```

3. Creare l'interfaccia del tunnel per il primo tunnel utilizzando le informazioni fornite nella sezione `IPSec Tunnel #1` del file di configurazione. Fornire un nome univoco per il tunnel, ad esempio `AWS_VPC_Tunnel_1`.

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
 peer AWS_VPC_Tunnel_1
set interface vpnt1 state on
set interface vpnt1 mtu 1436
```

4. Ripetere questi comandi per creare il secondo tunnel utilizzando le informazioni fornite nella sezione `IPSec Tunnel #2` del file di configurazione. Fornire un nome univoco per il tunnel, ad esempio `AWS_VPC_Tunnel_2`.

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
 peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. Impostare l'ASN del gateway virtuale privato.

```
set bgp external remote-as 7224 on
```

6. Configurare il BGP per il primo tunnel, utilizzando le informazioni fornite nella sezione `IPSec Tunnel #1` del file di configurazione.

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. Configurare il BGP per il secondo tunnel, utilizzando le informazioni fornite nella sezione `IPSec Tunnel #2` del file di configurazione.

```
set bgp external remote-as 7224 peer 169.254.44.37 on
```

```
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. Salvare la configurazione.

```
save config
```

Per creare una policy BGP

Crea una policy BGP che consente di importare route pubblicizzate da AWS. Quindi, configureremo il gateway del cliente per pubblicizzare le route locali ad AWS.

1. Nella interfaccia utente Web Gaia, scegli Advanced Routing (Routing avanzato), Inbound Route Filters (Filtri route in entrata). Scegli Add (Aggiungi) e seleziona Add BGP Policy (Based on AS) (Aggiungi policy BGP (basata su AS)).
2. Per Add BGP Policy (Aggiungi policy BGP), seleziona un valore compreso tra 512 e 1024 nel primo campo e immetti l'ASN del gateway virtuale privato nel secondo campo, ad esempio 7224.
3. Selezionare Salva.

Per pubblicizzare route locali

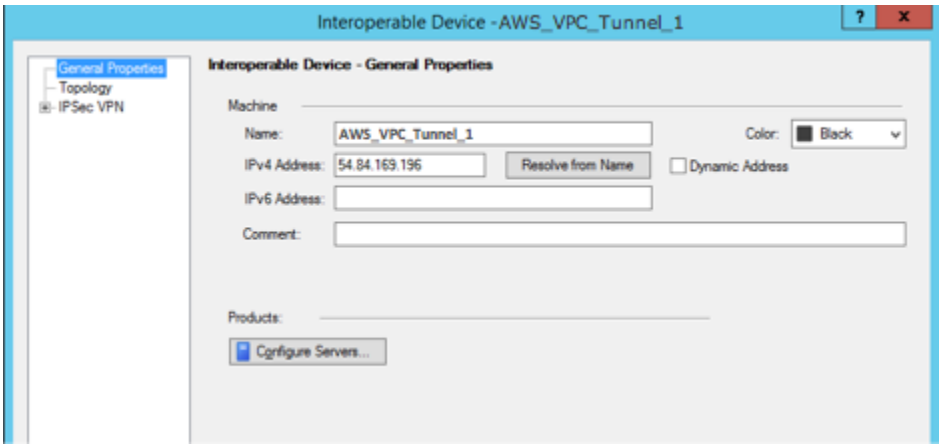
Le fasi seguenti sono relative alla distribuzione delle route dell'interfaccia locale. Puoi anche ridistribuire route da origini diverse; ad esempio, route statiche o route ottenute tramite protocolli di routing dinamici. Per ulteriori informazioni, consulta la Gaia Advanced Routing R77 Versions Administration Guide.

1. Nella interfaccia utente Web Gaia, scegliere Advanced Routing (Routing avanzato), Routing Redistribution (Ridistribuzione routing). Scegliere Add Redistribution From (Aggiungi ridistribuzione da) e selezionare Interface (Interfaccia).
2. In To Protocol (A protocollo), selezionare l'ASN del gateway virtuale privato, ad esempio 7224.
3. In Interface (Interfaccia), selezionare un'interfaccia interna. Selezionare Salva.

Per definire un nuovo oggetto di rete

Crea un oggetto di rete per ogni tunnel VPN, specificando gli indirizzi IP (esterni) pubblici per il gateway virtuale privato. In seguito questi oggetti vengono aggiunti come gateway satellite per la comunità VPN. Occorre anche creare un gruppo vuoto che agisce come segnaposto per il dominio VPN.

1. Apri il Check Point. SmartDashboard
2. In Groups (Gruppi), aprire il menu contestuale e scegliere Groups (Gruppi), Simple Group (Gruppo semplice). Lo stesso gruppo può essere utilizzato per ogni oggetto di rete.
3. In Network Objects (Oggetti di rete), aprire il menu contestuale (tasto destro del mouse) e scegliere New (Nuovo), Interoperable Device (Dispositivo interoperabile).
4. In Name (Nome), immettere il nome fornito per il tunnel nella fase 1, ad esempio `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.
5. In IPv4 Address (Indirizzo IPv4), immettere l'indirizzo IP esterno del gateway virtuale privato fornito nel file di configurazione, ad esempio `54.84.169.196`. Salvare le impostazioni e chiudere la finestra di dialogo.



6. Nel riquadro delle categorie a sinistra, scegliere Topology (Topologia).
7. Nella sezione VPN Domain (Dominio VPN), scegliere Manually defined (Definito manualmente), quindi individuare e selezionare il gruppo semplice vuoto creato nella fase 2. Scegli OK.
8. Ripetere queste fasi per creare un secondo oggetto di rete, utilizzando le informazioni fornite nella sezione `IPSec Tunnel #2` del file di configurazione.
9. Passare all'oggetto di rete gateway, aprire il gateway o l'oggetto cluster e scegliere Topology (Topologia).

10. Nella sezione VPN Domain (Dominio VPN), scegliere Manually defined (Definito manualmente), quindi individuare e selezionare il gruppo semplice vuoto creato nella fase 2. Scegli OK.

> **Note**
>
> È possibile mantenere qualsiasi dominio VPN esistente che è stato configurato. Tuttavia, assicurarsi che host e reti utilizzate o servite dalla nuova connessione VPN non siano dichiarate in tale dominio VPN, in particolare se il dominio VPN viene derivato automaticamente.

> **Note**
>
> Se stai utilizzando cluster, modifica la topologia e definisci le interfacce come interfacce del cluster. Utilizza gli indirizzi IP specificati nel file di configurazione.

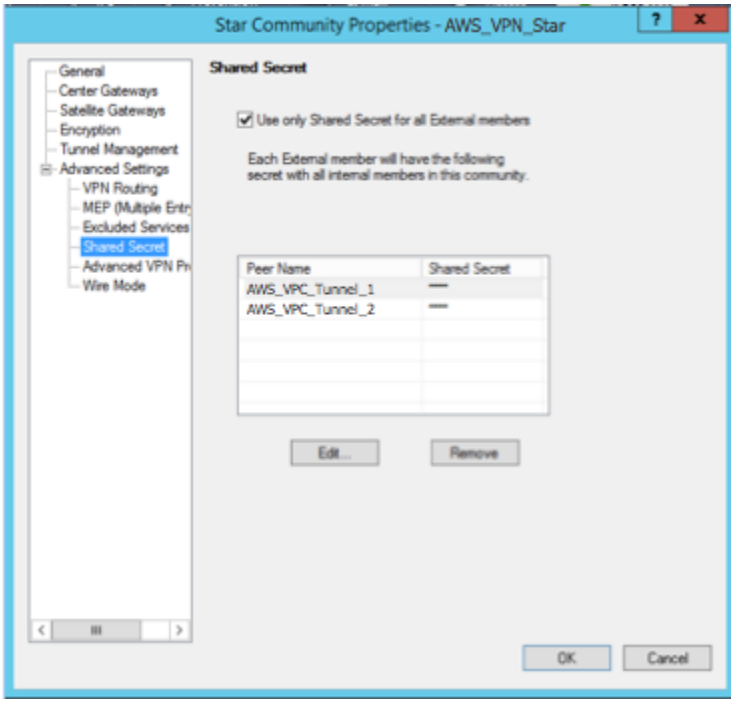
Per creare e configurare le impostazioni comunità VPN, IKE e IPsec

Crea quindi una comunità VPN nel gateway Check Point a cui aggiungere oggetti di rete (dispositivi interoperabili) per ogni tunnel. Vengono anche configurate le impostazioni Internet Key Exchange (IKE) e IPsec.

1. Dalle proprietà del gateway, scegliere IPSec VPN (VPN IPSec) nel riquadro delle categorie.
2. Selezionare Communities (Comunità), New (Nuova), Star Community (Comunità stella).
3. Fornire un nome per la comunità (ad esempio, `AWS_VPN_Star`), quindi selezionare Center Gateways (Gateway centrali) nel riquadro delle categorie.
4. Selezionare Add (Aggiungi) e aggiungere il gateway o il cluster all'elenco dei gateway partecipanti.
5. Nel riquadro delle categorie, selezionare Satellite Gateways (Gateway satellite), Add (Aggiungi) e aggiungere i dispositivi interoperabili creati in precedenza (`AWS_VPC_Tunnel_1` e `AWS_VPC_Tunnel_2`) all'elenco di gateway partecipanti.
6. Nel riquadro delle categorie, selezionare Encryption (Crittografia). Nella sezione Encryption Method (Metodo di crittografia), scegliere IKEv1 for IPv4 and IKEv2 for IPv6 (IKEv1 per IPv4 e IKEv2 per IPv6). Nella sezione Encryption Suite (Suite di crittografia), scegliere Custom (Personalizzato), Custom Encryption (Crittografia personalizzata).

> **Note**
>
> È necessario selezionare l'opzione IKEv1 for IPv4 and IKEv2 for IPv6 (IKEv1 per IPv4 e IKEv2 per IPv6) per la funzionalità IKEv1.

7. Nella finestra di dialogo, configurare le proprietà di crittografia come riportato di seguito e, al termine, scegliere OK:
   - Proprietà IKE Security Association (fase 1):
     - Perform key exchange Encryption with (Esegui crittografia scambio delle chiavi con): AES-128
     - Perform data integrity with (Esegui integrità dei dati con): SHA-1
   - Proprietà IPSec Security Association (fase 2):
     - Perform IPsec data encryption with (Esegui crittografia dati IPsec con): AES-128
     - Perform data integrity with (Esegui integrità dei dati con): SHA-1
8. Nel riquadro delle categorie, selezionare Tunnel Management (Gestione tunnel). Selezionare Set Permanent Tunnels (Imposta tunnel permanenti), On all tunnels in the community (Su tutti i tunnel nelle comunità). Nella sezione VPN Tunnel Sharing (Condivisione tunnel VPN), scegliere One VPN tunnel per Gateway pair (Un tunnel VPN per coppia gateway).
9. Nel riquadro delle categorie, espandere Advanced Settings (Impostazioni avanzate) e scegliere Shared Secret (Segreto condiviso).
10. Selezionare il nome peer per il primo tunnel, scegliere Edit (Modifica) e immettere la chiave precondivisa come specificato nel file di configurazione nella sezione `IPSec Tunnel #1`.
11. Selezionare il nome peer per il secondo tunnel, scegliere Edit (Modifica) e immettere la chiave precondivisa come specificato nel file di configurazione nella sezione `IPSec Tunnel #2`.



12. Nella categoria Advanced Settings (Impostazioni avanzate), scegliere Advanced VPN Properties (Proprietà VPN avanzate), configurare le proprietà come segue e, al termine, scegliere OK:

    - IKE (fase 1):
        - Use Diffie-Hellman group (Utilizza gruppo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegotiate IKE security associations every (Rinegozia associazioni sicurezza IKE ogni) `480` minutes (minuti)
    - IPsec (fase 2):
        - Selezionare Use Perfect Forward Secrecy (Utilizza Perfect Forward Secrecy)
        - Use Diffie-Hellman group (Utilizza gruppo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegotiate IPsec security associations every (Rinegozia associazioni sicurezza IPsec ogni) `3600` seconds (secondi)

Per creare regole del firewall

Viene quindi configurata una policy con regole del firewall e regole di corrispondenza direzionali che consentono la comunicazione tra il VPC e la rete locale. Viene quindi installata la policy nel gateway.

1. Nella SmartDashboard, scegli Proprietà globali per il tuo gateway. Nel riquadro delle categorie, espandere VPN e scegliere Advanced (Avanzate).
2. Selezionare Enable VPN Directional Match in VPN Column (Abilita corrispondenza VPN direzionale nella colonna VPN) e scegliere OK.
3. Nella SmartDashboard, scegli Firewall e crea una politica con le seguenti regole:
   - Consente la comunicazione tra la sottorete VPC e la rete locale sui protocolli richiesti.
   - Consente la comunicazione tra la rete locale e la sottorete VPC sui protocolli richiesti.
4. Aprire il menu contestuale per la cella nella colonna VPN e scegliere Edit Cell (Modifica cella).
5. Nella finestra di dialogo VPN Match Conditions (Condizioni corrispondenza VPN), scegliere Match traffic in this direction only (Corrispondenza traffico solo in questa direzione). Creare le seguenti regole di corrispondenza direzionale scegliendo Add (Aggiungi) per ognuna e, al termine, selezionare OK:
   - `internal_clear` > comunità VPN (la comunità stella VPN creata in precedenza, ad esempio `AWS_VPN_Star`)
   - Comunità VPN > Comunità VPN
   - Community VPN > `internal_clear`
6. Nel SmartDashboard, scegli Policy, Installa.
7. Nella finestra di dialogo, scegliere il gateway e quindi OK per installare la policy.

Per modificare la proprietà tunnel_keepalive_method

Il gateway Check Point può utilizzare Dead Peer Detection (DPD) per identificare quando un'associazione IKE è inattiva. Per configurare DPD per un tunnel permanente, il tunnel permanente deve essere configurato nella community AWS VPN.

Per impostazione predefinita, la proprietà `tunnel_keepalive_method` per un gateway VPN è impostata su `tunnel_test`. Occorre modificare il valore in dpd. Ogni gateway VPN nella community VPN che richiede il monitoraggio DPD deve essere configurato con la proprietà `tunnel_keepalive_method`, inclusi eventuali gateway VPN di terze parti. Non è possibile configurare meccanismi di monitoraggio diversi per lo stesso gateway.

Puoi aggiornare la proprietà `tunnel_keepalive_method` utilizzando lo strumento GuiDBedit.

1. Apri il Check Point SmartDashboard e scegli Security Management Server, Domain Management Server.
2. Selezionare File, Database Revision Control... (Controllo revisione database...) e creare una snapshot di revisione.
3. Chiudi tutte le SmartConsole finestre, come SmartView Tracker e SmartView Monitor. SmartDashboard
4. Avviare lo strumento GuiBDedit. Per ulteriori informazioni, consulta l'articolo Check Point Database Tool in Check Point Support Center.
5. Selezionare Security Management Server (Server di gestione della sicurezza), Domain Management Server (Server di gestione domini).
6. Nel riquadro in alto a sinistra, scegliere Table (Tabella), Network Objects (Oggetti di rete), network_objects.
7. Nel riquadro in alto a destra, selezionare l'oggetto Security Gateway (Gateway di sicurezza), Cluster pertinente.
8. Premere CTRL+F o utilizzare il menu Search (Cerca) per cercare quanto segue: `tunnel_keepalive_method`.
9. Nel riquadro inferiore, aprire il menu contestuale per `tunnel_keepalive_method` e selezionare Edit... (Modifica...). Scegliere dpd, OK.
10. Ripetere le fasi da 7 a 9 per ogni gateway che fa parte della community AWS VPN.
11. Selezionare File, Save All (Salva tutto).
12. Chiudere lo strumento GuiDBedit.
13. Apri il Check Point SmartDashboard e scegli Security Management Server, Domain Management Server.
14. Installare la policy nell'oggetto Security Gateway (Gateway di sicurezza), Cluster pertinente.

Per ulteriori informazioni, consulta l'articolo New VPN features in R77.10 in Check Point Support Center.

Per abilitare TCP MSS Clamping

TCP MSS Clamping riduce la dimensione segmento massima dei pacchetti TCP per impedire la frammentazione pacchetti.

1. Accedere alla seguente directory: `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.

2. AprireCheck Point Database Tool eseguendo il file `GuiDBEdit.exe`.
3. Selezionare Table (Tabella), Global Properties (Proprietà globali), properties (proprietà).
4. In `fw_clamp_tcp_mss`, scegliere Edit (Modifica). Modificare il valore in `true`, quindi scegliere OK.

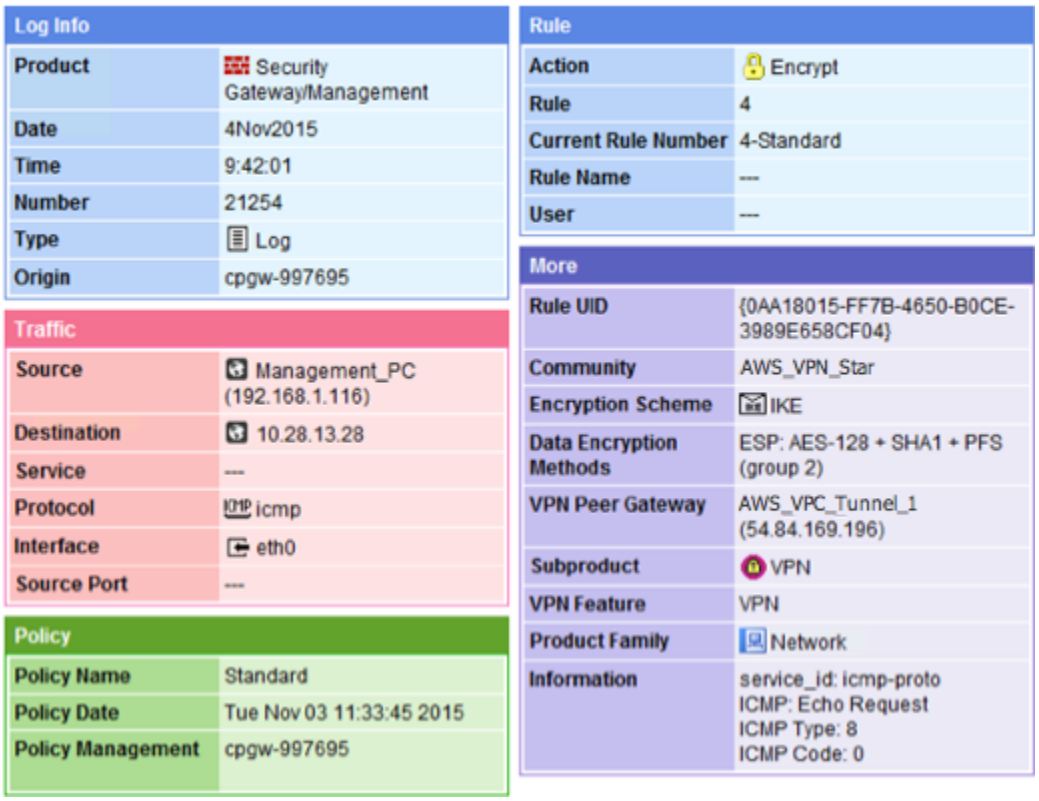
Per verificare lo stato del tunnel

Puoi verificare lo stato del tunnel eseguendo il seguente comando dallo strumento a riga di comando in modalità esperto.

```
vpn tunnelutil
```

Nelle opzioni visualizzate, scegli 1 per verificare le associazioni IKE e 2 per verificare le associazioni IPsec.

Puoi anche utilizzare Check Point Smart Tracker Log per verificare che i pacchetti sulla connessione siano crittografati. Ad esempio, il seguente log indica che un pacchetto al VPC è stato inviato su tunnel 1 ed è stato crittografato.



SonicWALL

Puoi configurare un dispositivo SonicWALL tramite l'interfaccia di gestione SonicOS. Per ulteriori informazioni sulla configurazione dei tunnel, consulta Procedure dell'interfaccia utente per il routing statico.

Non puoi configurare BGP per il dispositivo utilizzando l'interfaccia di gestione. Utilizza invece le istruzioni della riga di comando fornite nel file di configurazione di esempio precedente, nella sezione denominata BGP.

Ulteriori informazioni per dispositivi Cisco

Alcuni dispositivi Cisco ASA supportano soltanto la modalità Active/Standby. Quando utilizzi questi Cisco ASA, puoi avere un solo tunnel attivo alla volta. Il tunnel in standby diventa attivo se il primo tunnel non è più disponibile. Con questa ridondanza, dovresti disporre sempre di una connessione al VPC via uno dei tunnel.

Cisco ASA versione 9.7.1 o versione successiva supporta la modalità attivo/attivo. Quando utilizzi i dispositivi Cisco ASA, entrambi i tunnel possono essere contemporaneamente attivi. Con questa ridondanza, dovresti disporre sempre di una connessione al VPC via uno dei tunnel.

Per dispositivi Cisco, è necessario effettuare le seguenti operazioni:

- Configurare l'interfaccia esterna.
- Verificare che il numero di sequenza della policy Crypto ISAKMP sia univoco.
- Assicurarti che il numero di sequenza della policy della lista Crypto sia univoco.
- Verificare che il set di trasformazione Crypto IPsec e la sequenza della policy Crypto ISAKMP siano compatibili con qualsiasi altro tunnel IPsec configurato sul dispositivo.
- Verificare che il numero di monitoraggio SLA sia univoco.
- Configurare l'intero routing interno che sposta il traffico tra il dispositivo gateway del cliente e la tua rete locale.

Ulteriori informazioni per dispositivi Juniper

Le seguenti informazioni si applicano ai file di configurazione di esempio per i dispositivi gateway del cliente Juniper serie J e SRX.

- L'interfaccia esterna è indicata come *ge-0/0/0.0*.

- Gli ID dell'interfaccia di tunnel sono indicati come `st0.1` e `st0.2`.
- Assicurarsi di identificare la zona di sicurezza per l'interfaccia di collegamento (le informazioni di configurazione utilizzano la zona predefinita "untrust").
- Assicurarsi di identificare la zona di sicurezza per l'interfaccia interna (le informazioni di configurazione utilizzano la zona predefinita "trust").

Test in corso

Per ulteriori informazioni sul test della connessione Site-to-Site VPN, consulta Test di una connessione VPN site-to-site.

Configurazione di Windows Server come dispositivo customer gateway

È possibile configurare il tuo server che esegue Windows Server come dispositivo gateway del cliente per il VPC. Utilizza la procedura seguente se Esegui Windows Server su EC2instance in un VPC o sul tuo server. Le procedure seguenti si applicano a Windows Server 2012 R2 e versioni successive.

Indice

Configurazione dell'istanza Windows

Se si sta configurando Windows Server in EC2 instance avviata da un Windows AMI, eseguire le operazioni seguenti:

- Disabilitare il controllo dell'origine/della destinazione per l'istanza:
  1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Selezionare l'istanza di Windows Server, scegliere Operazioni, Reti, Modifica origine/destinazione di controllo. Seleziona Aggiungi,, quindi seleziona Salva.

- Aggiornare le impostazioni della scheda in modo da instradare il traffico da altre istanze:
  1. Connettersi all'istanza Windows. Per ulteriori informazioni, consulta Connessione all'istanza Windows.
  2. Aprire il pannello di controllo, quindi avviare Gestione dispositivi.
  3. Espandere il nodo Schede di rete.
  4. Select la scheda di rete (a seconda dell'instance type, potrebbe essere scheda di rete Elastic Amazon o Intel 82599 Virtual Function) e scegliere Azione, Proprietà.
  5. Nella scheda Avanzate, disabilitare le proprietà Offload di checksum IPv4, Offload di checksum TCP (IPv4) e Offload di checksum UDP (IPv4), quindi selezionare OK.
- Allocare un indirizzo IP elastico per l'account e associarlo all'istanza. Per ulteriori informazioni, consulta Utilizzo degli indirizzi IP elastici. Annota questo indirizzo, sarà necessario per creare il gateway del cliente nel VPC.
- Assicurarsi che le regole del gruppo di sicurezza dell'istanza consentano il traffico IPsec in uscita. Per impostazione predefinita, un gruppo di sicurezza abilita tutto il traffico in uscita. Tuttavia, se le regole in uscita del gruppo di sicurezza sono state modificate rispetto allo stato originale, è necessario creare le seguenti regole di protocollo personalizzate in uscita per il traffico IPsec: protocollo IP 50, protocollo IP 51 e UDP 500.

Prendere nota dell'intervallo CIDR della rete in cui si trova l'istanza di Windows, ad esempio, `172.31.0.0/16`.

Fase 1: creazione di una connessione VPN e configurazione del VPC

Per creare una connessione VPN dal VPC, effettuare le seguenti operazioni:

1. Per creare un virtual private gateway e collegarlo al VPC Per ulteriori informazioni, consulta Creazione di gateway virtuale privato.
2. Quindi, crea una connessione VPN e un nuovo customer gateway. Per il customer gateway, specificare l'indirizzo IP pubblico del server Windows. Per la connessione VPN, scegliere il routing statico e quindi inserire l'intervallo CIDR per la rete in cui si trova il server Windows, ad esempio `172.31.0.0/16`. Per ulteriori informazioni, consulta Fase 5: creazione di una connessione VPN.

Dopo aver creato la connessione VPN, configurare il VPC per abilitare la comunicazione tramite la connessione VPN.

Per configurare il VPC

- Creare una sottorete privata nel VPC (se ancora non esiste) per l'avvio delle istanze che comunicheranno con il server Windows. Per ulteriori informazioni, consultare Creazione di una sottorete nel VPC

  > **Note**
  >
  > Una sottorete privata è una sottorete che non dispone di una route a un Internet Gateway. Il routing per questa sottorete è descritto di seguito.

- Aggiornare le tabelle di routing per la connessione VPN:
  - Aggiungere una route alla tabella di routing della virtual private gateway come target e la rete del server Windows (intervallo CIDR) come destinazione. Per ulteriori informazioni, consultare la sezione relativa ad Aggiungere e rimuovere route da una tabella di routing nella Guida per l'utente di Amazon VPC.
  - Abilitare la propagazione della route per il gateway virtuale privato. Per ulteriori informazioni, consulta (Gateway virtuale privato) Abilitazione della propagazione della route nella tabella di routing.
- Creare una configurazione di gruppi di sicurezza per le istanze che consente la comunicazione tra il VPC e la rete:
  - Aggiungere regole che consentono l'accesso RDP o SSH in entrata dalla rete. In questo modo, è possibile connettersi alle istanze nel VPC dalla rete. Ad esempio, per consentire ai computer nella rete di accedere alle istanze Linux nel VPC, creare una regola in entrata con un tipo SSH e l'origine impostata sull'intervallo CIDR della rete (ad esempio `172.31.0.0/16`). Per ulteriori informazioni, consultare Gruppi di sicurezza per il VPC nella Guida per l'utente di Amazon VPC.
  - Aggiungere una regola che consente l'accesso ICMP in entrata dalla rete. Ciò consente di testare la connessione VPN tramite il ping di un'istanza nel VPC dal server Windows.

Fase 2: download del file di configurazione per la connessione VPN

Puoi utilizzare la console Amazon VPC per scaricare una file di configurazione Windows Server per la connessione VPN.

Per scaricare il file di configurazione

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Site-to-Site VPN Connections (Connessioni VPN site-to-site).
3. Selezionare la connessione VPN e scegliere Download Configuration (Scarica configurazione).
4. Selezionare Microsoft come fornitore, Windows Server come piattaforma e 2012 R2 come software. Scegli Download (Scarica). È possibile aprire il file o salvarlo.

Il file di configurazione contiene una sezione di informazioni simile all'esempio seguente. Queste informazioni vengono visualizzate due volte, una volta per ogni tunnel.

```
vgw-1a2b3c4d Tunnel1
-----------------------------------------------------------------
Local Tunnel Endpoint:       203.0.113.1
Remote Tunnel Endpoint:      203.83.222.237
Endpoint 1:                  [Your_Static_Route_IP_Prefix]
Endpoint 2:                  [Your_VPC_CIDR_Block]
Preshared key:               xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE
```

`Local Tunnel Endpoint`

L'indirizzo IP specificato per il gateway del cliente quando hai creato la connessione VPN.

`Remote Tunnel Endpoint`

Uno dei due indirizzi IP del gateway privato virtuale che interrompe la connessione VPN sul AWS lato della connessione.

`Endpoint 1`

Il prefisso IP specificato come route statica alla creazione della connessione VPN. Sono gli indirizzi IP nella rete a cui è consentito utilizzare la connessione VPN per accedere al VPC.

`Endpoint 2`

L'intervallo di indirizzi IP (blocco CIDR) del VPC collegato al gateway virtuale privato (ad esempio 10.0.0.0/16).

`Preshared key`

La chiave già condivisa utilizzata per stabilire la connessione VPN IPsec tra `Local Tunnel Endpoint` e `Remote Tunnel Endpoint`.

Ti suggeriamo di configurare entrambi i tunnel come parte della connessione VPN. Ogni tunnel si collega a un concentratore VPN separato sul lato Amazon della connessione VPN. Sebbene sia attivo solo un tunnel alla volta, il secondo tunnel si stabilisce automaticamente se il primo tunnel si interrompe. La presenza di tunnel ridondanti garantisce una disponibilità continua in caso di guasto del dispositivo. Poiché un solo tunnel è disponibile alla volta, la console Amazon VPC indica che un tunnel è inattivo. Questo è il comportamento previsto, di conseguenza non deve Eseguire alcuna operazione.

Con due tunnel configurati, se si verifica un guasto del dispositivo all'interno AWS, la connessione VPN passa automaticamente al secondo tunnel del gateway privato virtuale nel giro di pochi minuti. Durante la configurazione del dispositivo gateway del cliente, è importante configurare Entrambi i tunnel.

> **Note**
>
> Di tanto in tanto, AWS esegue la manutenzione ordinaria sul gateway privato virtuale. Questa manutenzione potrebbe disabilitare uno dei due tunnel della connessione VPN per un breve periodo di tempo. La connessione VPN esegue automaticamente il failover al secondo tunnel durante l'esecuzione di questa manutenzione.

Ulteriori informazioni relative alle associazioni di sicurezza (SA) IKe E IPsec sono contenute nel file di configurazione scaricato.

```
MainModeSecMethods:         DHGroup2-AES128-SHA1
MainModeKeyLifetime:        480min,0sess
QuickModeSecMethods:        ESP:SHA1-AES128+60min+100000kb
QuickModePFS:               DHGroup2
```

`MainModeSecMethods`

Gli algoritmi di crittografia e autenticazione per la SA IKE. Sono le impostazioni suggerite per la connessione VPN e le impostazioni predefinite per le connessioni VPN IPsec di Windows Server.

`MainModeKeyLifetime`

Il ciclo di vita della chiave SA IKE. È l'impostazione suggerita per la connessione VPN e l'impostazione predefinita per le connessioni VPN IPsec di Windows Server.

`QuickModeSecMethods`

Gli algoritmi di crittografia e autenticazione per la SA IPsec. Sono le impostazioni suggerite per la connessione VPN e le impostazioni predefinite per le connessioni VPN IPsec di Windows Server.

`QuickModePFS`

Per le sessioni IPsec ti consigliamo di utilizzare PFS (Perfect Forward Secrecy) chiave master.

Fase 3: configurazione di Window Server

Prima di configurare il tunnel VPN, devi installare e configurare i servizi di Routing e Accesso remoto nel server Windows per consentire agli utenti remoti di accedere alla risorse sulla rete.

Installare i Servizi di Routing e Accesso Remoto:

1. Accedere a Windows Server.
2. Andare al menu Start (Inizia) e scegliere Server Manager.
3. Installare i servizi di Routing e Accesso remoto:
    a. Dal menu Gestisci, scegliere Aggiunta guidata ruoli e funzionalità:
    b. Nella pagina Prima di iniziare, verificare che il server soddisfi i prerequisiti, quindi selezionare Avanti.
    c. Selezionare Installazione basata su ruoli o basata su funzionalità, quindi selezionare Avanti.
    d. Selezionare Select un server dal pool di server, select il server Windows, quindi selezionare Avanti.
    e. Selezionare Servizi di accesso e criteri di rete nell'elenco. Nella finestra di dialogo visualizzata, scegliere Aggiungi funzionalità per confermare le funzionalità necessarie per questo ruolo.
    f. Nello stesso elenco scegliere Accesso remoto, quindi Avanti.
    g. Nella pagina Select features (Seleziona funzionalità), scegli Next (Successivo).
    h. Nella pagina Servizi di accesso e criteri di rete, scegliere Avanti.
    i. Nella pagina Accesso remoto scegliere Avanti. Nella pagina successiva, seleziona DirectAccess and VPN (RAS). Nella finestra di dialogo visualizzata, scegliere Aggiungi funzionalità per confermare le funzionalità necessarie per questo servizio ruolo. Nello stesso elenco, selezionare Routing, quindi selezionare Avanti.

j. Nella pagina Ruolo Server Web (IIS), scegliere Avanti. Lasciare la selezione predefinita e scegliere Avanti.

k. Scegli Installa. Al termine dell'installazione, scegliere Chiudi.

Per configurare E abilitare il server di Routing e Accesso remoto

1. Nel dashboard, scegliere Notifiche (l'icona a bandiera). Un'operazione deve Essere Effettuata per completare la configurazione post-distribuzione. Selezionare il collegamento Apre Attività iniziali guidate.
2. Selezionare Distribuisci solo VPN.
3. Nella finestra di dialogo Routing and Remote Access (Routing e Accesso remoto), scegliere il nome di server, scegliere Action (Operazione), quindi selezionare Configure and Enable Routing and Remote Access (Configura e abilita routing e accesso remoto).
4. In Configurazione guidata server di Routing e Accesso remoto, nella prima pagina, scegliere Avanti.
5. Nella pagina Configurazione scegliere Configurazione personalizzata, quindi Avanti.
6. Scegliere Routing di rete locale (LAN), Avanti e Fine.
7. Quando richiesto dalla finestra di dialogo Routing e Accesso remoto, scegliere Avvia servizio

Fase 4: configurazione del tunnel VPN

Puoi configurare il tunnel VPN eseguendo gli script netsh inclusi nel file di configurazione scaricato o utilizzando l'interfaccia utente Windows Server.

> **Important**
>
> Ti consigliamo di utilizzare la chiave principale Perfect Forward Secrecy (PFS) per le tue sessioni IPSec. Se scegliete di eseguire lo script netsh, questo include un parametro per abilitare PFS (). `qmpfs=dhgroup2` Non è possibile abilitare PFS utilizzando l'interfaccia utente Windows Server, si deve abilitare utilizzando la riga di comando.

Opzioni

- Opzione 1: Eseguire lo script netsh

- Opzione 2: utilizzo dell'interfaccia utente di Windows Server

Opzione 1: Eseguire lo script netsh

Copia lo script netsh dal file di configurazione scaricato e sostituisci le variabili. Di seguito è riportato un esempio di script.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name: puoi sostituire il nome suggerito (`vgw-1a2b3c4d Tunnel 1`) con un nome di tua scelta.

LocalTunnelEndpoint: immettete l'indirizzo IP privato di Windows Server sulla rete.

Endpoint1: il block CIDR della rete in cui si trova il server Windows, ad esempio `172.31.0.0/16`. Circondare questo valore tra virgolette doppie («).

Endpoint2: il blocco CIDR del VPC o di una sottorete nel VPC, ad esempio `10.0.0.0/16`. Circondare questo valore tra virgolette doppie («).

Esegui lo script aggiornato in una finestra del prompt dei comandi sul server Windows. (il carattere ^ ti consente di tagliare E incollare testo con ritorno a capo nella riga di comando). Per configurare il secondo tunnel VPN per questa connessione VPN, ripeti la procedura utilizzando il secondo script netsh nel file di configurazione.

Al termine, vai a Configurare Windows Firewall.

Per ulteriori informazioni sui parametri netsh, vedere Comandi Netsh AdvFirewall Consec nella libreria Microsoft. TechNet

Opzione 2: utilizzo dell'interfaccia utente di Windows Server

Per configurare il tunnel VPN, puoi anche utilizzare l'interfaccia utente di Windows Server.

> **Important**
>
> Non puoi abilitare PFS (Perfect Forward Secrecy) chiave master utilizzando l'interfaccia utente di Windows Server. Devi abilitare PFS utilizzando la riga di comando, come descritto in Abilitazione di PFS (Perfect Forward Secrecy) chiave master.

Attività

- Configurare una regola di sicurezza per un tunnel VPN
- Confermare la configurazione dei tunnel
- Abilitazione di PFS (Perfect Forward Secrecy) chiave master
- Configurare Windows Firewall

Configurare una regola di sicurezza per un tunnel VPN

In questa sezione, configuri un ruolo di sicurezza sul server Windows per creare un tunnel VPN.

Per configurare una regola di sicurezza per un tunnel VPN

1. Aprire Server Manager, scegliere Tools (Strumenti), quindi select Windows Firewall with Advanced Security (Windows Firewall con sicurezza avanzata).
2. Selezionare Regole di sicurezza delle connessioni, scegliere Azione, quindi Nuova regola.
3. In Creazione guidata nuova regola di sicurezza della connessione, nella pagina Tipo di regola, scegliere Tunnel, quindi selezionare Avanti.
4. Nella pagina Tipo di tunnel, in Selezionare il tipo di tunnel che si desidera creare, scegliere Configurazione personalizzata. In Would you like to exempt IPsec-protected connections from this tunnel (Escludere dal tunnel le connessioni protette con IPsec?), lasciare selezionato il valore predefinito (No. Send all network traffic that matches this connection security rule through the tunnel (No. Invia tutto il traffico di rete che soddisfa questa regola di sicurezza della connessione tramite il tunnel)), quindi selezionare Next (Avanti).
5. Nella pagina Requisiti, scegli Richiedi l'autenticazione per le connessioni in entrata. Non stabilire tunnel per le connessioni in uscita, quindi scegli Avanti.
6. Nella pagina Tunnel Endpoints (Endpoint del tunnel), in Which computers are in Endpoint 1 (Selezionare i computer inclusi nell'endpoint 1), scegliere Add (Aggiungi). Immettere l'intervallo di CIDR della rete (dietro il dispositivo customer gateway del server Windows, ad esempio,

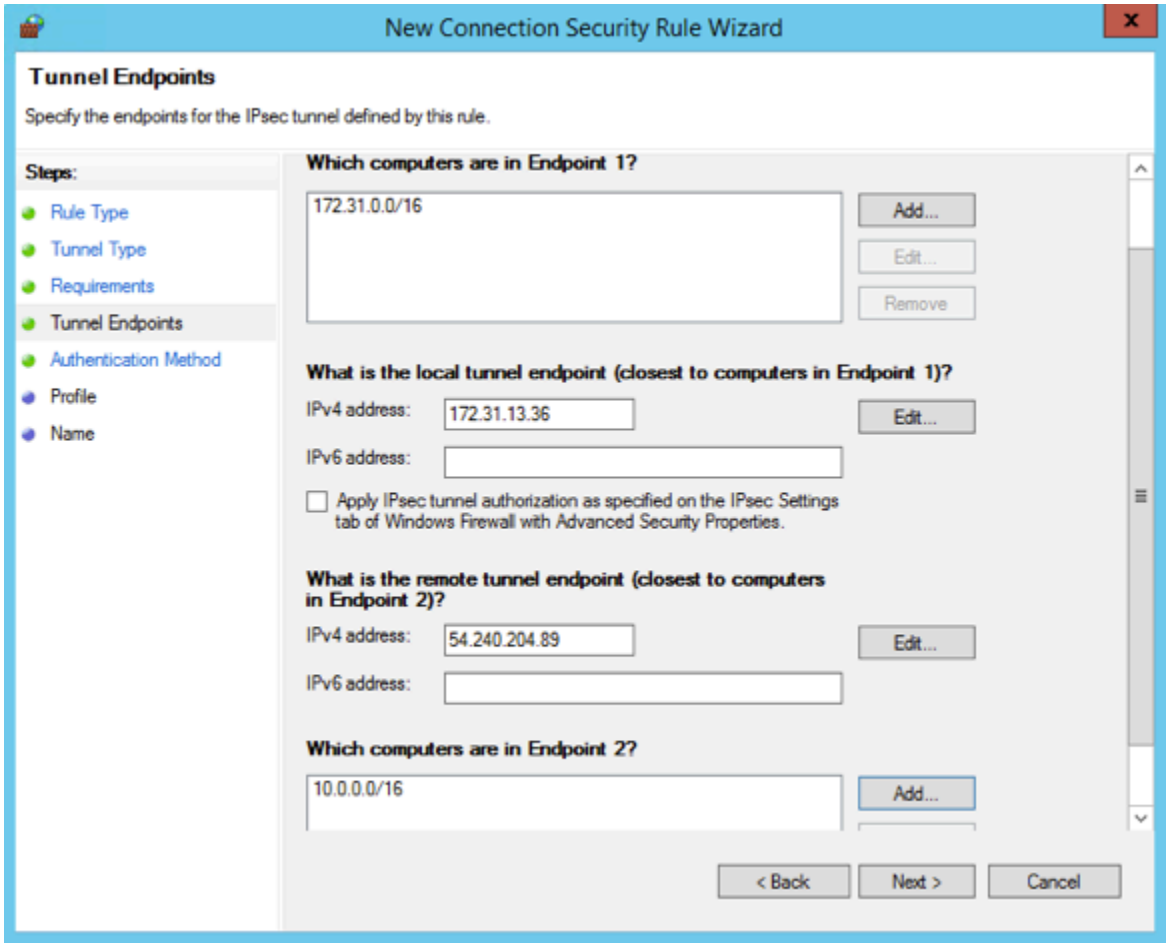
`172.31.0.0/16`), quindi selezionare OK. L'intervallo può includere l'indirizzo IP del dispositivo gateway del cliente.

7. In Endpoint del tunnel locale più vicino ai computer nell'endpoint 1, scegliere Modifica. Nel campo Indirizzo IPv4, inserire l'indirizzo IP privato del server Windows, quindi selezionare OK.
8. In Endpoint del tunnel remoto più vicino ai computer nell'endpoint 2, scegliere Modifica. Nel campo Indirizzo IPv4, immettere l'indirizzo IP del gateway virtuale privato per Tunnel 1 dal file di configurazione (consulta `Remote Tunnel Endpoint`), quindi selezionare OK.

> **Important**
>
> Se si ripete questa procedura per Tunnel 2, assicurarsi di selezionare l'endpoint per Tunnel 2.

9. In Selezionare i computer inclusi nell'endpoint 2, scegliere Aggiungi. Nel campo Subnet o indirizzo IP, immettere il blocco CIDR del VPC, quindi selezionare OK.

> **Important**
>
> Scorrere la finestra di dialogo fino a trovare Selezionare i computer inclusi nell'endpoint 2. Non scegliere Avanti fino al completamento di questa fase altrimenti non sarà possibile connettersi al server.



10. Confermare che tutte le impostazioni specificate siano corrette, quindi selezionare Next (Avanti).
11. Nella pagina Metodo di autenticazione selezionare Avanzate e scegliere Personalizza.
12. In Metodi per prima autenticazione, scegliere Aggiungi.
13. Selezionare Preshared key (Chiave precondivisa), immettere il valore della chiave precondivisa del file di configurazione e scegliere OK.

> **Important**
>
> Se si ripete questa procedura per Tunnel 2, assicurarsi di selezionare la chiave già condivisa per Tunnel 2.

14. Assicurarsi che l'opzione Prima autenticazione facoltativa non sia selezionata, quindi selezionare OK.
15. Seleziona Successivo.

16. Nella pagina Profilo selezionare tutte e tre le caselle di controllo: Dominio, Privato e Pubblico. Seleziona Successivo.
17. Nella pagina Name (Nome), immettere un nome per la regola di connessione, ad esempio `VPN to Tunnel 1`, quindi selezionare Finish (Fine).

Ripeti la procedura precedente, specificando i dati per Tunnel 2 dal file di configurazione.

Al termine, avrai due tunnel configurati per la connessione VPN.

Confermare la configurazione dei tunnel

Per confermare la configurazione dei tunnel

1. Aprire Server Manager, scegliere Strumenti, selezionare Windows Firewall con sicurezza avanzata, quindi selezionare Regole di sicurezza delle connessioni.
2. Verificare quanto segue per entrambi i tunnel:
   - Abilitato è `Yes`
   - Endpoint 1 è il blocco CIDR per la rete.
   - Endpoint 2 è il blocco CIDR del VPC.
   - Modalità di autenticazione è `Require inbound and clear outbound`
   - Metodo di autenticazione è `Custom`.
   - Porta endpoint 1 è `Any`.
   - Porta endpoint 2 è `Any`.
   - Protocollo è `Any`.
3. Selezionare la prima regola, quindi selezionare Proprietà.
4. Nella scheda Authentication (Autenticazione) in Method (Metodo), scegliere Customize (Personalizza). Verificare che First authentication methods (Metodi per prima autenticazione) contenga la chiave precondivisa corretta del file di configurazione per il tunnel, quindi scegliere OK.
5. Nella scheda Avanzate, verificare che le caselle di controllo Dominio, Privato e Pubblico siano tutte selezionate.
6. In Tunneling IPsec, scegliere Personalizza. Verificare le impostazioni di tunnelling IPsec seguenti, quindi selezionare OK e di nuovo OK per chiudere la finestra di dialogo.
   - Usa tunneling IPsec è selezionata.

- Endpoint del tunnel locale (il più vicino all'endpoint 1) contiene l'indirizzo IP del Server Windows. Se il dispositivo gateway del cliente è un'istanza EC2, questa è l'indirizzo IP privato dell'istanza.
- Endpoint del tunnel remoto più vicino all'endpoint 2 contiene l'indirizzo IP del gateway virtuale privato per questo tunnel.

7. Visualizzare le proprietà del secondo tunnel. Ripetere le fasi da 4 a 7 per questo tunnel.

Abilitazione di PFS (Perfect Forward Secrecy) chiave master

Puoi abilitare PFS (Perfect Forward Secrecy) chiave master utilizzando la riga di comando. Non puoi abilitare questa funzionalità tramite l'interfaccia utente.

Per abilitare PFS (Perfect Forward Secrecy) chiave master

1. Nel server Windows, aprire una finestra del prompt dei comandi.
2. Immettere il comando seguente sostituendo `rule_name` con il nome assegnato alla prima regola di connessione.

```
netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
 QMSecMethods=ESP:SHA1-AES128+60min+100000kb
```

3. Ripetere la fase 2 per il secondo tunnel, questa volta sostituendo `rule_name` con il nome assegnato alla seconda regola di connessione.

Configurare Windows Firewall

Dopo la configurazione delle regole di sicurezza sul tuo server, configura alcune impostazioni IPsec di base da utilizzare con il gateway virtuale privato.

Per configurare Windows Firewall

1. Aprire Server Manager, scegliere Strumenti, select Windows Firewall con Sicurezza Advanced, quindi selezionare Proprietà.
2. Nella scheda Impostazioni IPSec, in Esenzioni IPSec, verificare che Esenzione di ICMP da IPSec sia No (predefinito). Verificare che Autorizzazione tunnel IPsec sia Nessuna.
3. In Impostazioni predefinite IPSec, scegliere Personalizza.

4. In Scambio di chiavi (modalità principale), selezionare Avanzate, quindi selezionare Personalizza.
5. In Customize Advanced Key Exchange Settings (Personalizza impostazioni avanzate scambio chiavi), sotto Security methods (Metodi di sicurezza), verificare che i seguenti valori predefiniti siano utilizzati per la prima voce.

   - Integrità: SHA-1
   - Crittografia: AES-CBC 128
   - Algoritmo di scambio chiavi: Gruppo Diffie-Hellman 2
   - In Durata chiavi, verificare che Minuti sia `480` e Sessioni sia `0`.

   Queste impostazioni corrispondono a queste voci nel file di configurazione.

   ```
   MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
   MainModeKeyLifetime: 480min,0sec
   ```

6. In Opzioni di scambio chiavi, selezionare Utilizza Diffie-Hellman per una sicurezza avanzata, quindi selezionare OK.
7. In Protezione dati (modalità rapida), selezionare Avanzate, quindi selezionare Personalizza.
8. Selezionare Richiedi crittografia per le tutte le regole di sicurezza di connessione che utilizzano queste impostazioni.
9. In Integrità e crittografia dei dati, mantenere i valori predefiniti:

   - Protocollo: ESP
   - Integrità: SHA-1
   - Crittografia: AES-CBC 128
   - Durata: 60 minuti

   Questi valori corrispondono alla voce seguente del file di configurazione.

   ```
   QuickModeSecMethods:
   ESP:SHA1-AES128+60min+100000kb
   ```

10. Scegliere OK per tornare alla finestra di dialogo Personalizza impostazioni IPsec e scegliere di nuovo OK per salvare la configurazione.

Fase 5: abilitazione del rilevamento Dead Gateway

Ora devi configurare TCP per rilevare quando un gateway diventa indisponibile. A questo proposito, modifica questa chiave di registro: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. Non effettuare questa procedura se non hai completato le sezioni precedenti. Dopo la modifica della chiave di registro, devi riavviare il server.

Per abilitare il rilevamento Dead Gateway

1. Da Windows Server, avvia il prompt dei comandi o una PowerShell sessione e digita regedit per avviare l'editor del registro.
2. Espandi HKEY_LOCAL_MACHINE, espandi SYSTEM, espandi CurrentControlSet, espandi Services, espandi Tcpip e quindi espandi Parametri.
3. Dal menu Modifica, selezionare Nuovo, quindi selezionare Valore DWORD (32 bit).
4. Immettete EnableDeadil nome GWDetect.
5. Seleziona EnableDeadGWDetect e scegli Modifica, Modifica.
6. In Dati valore, immettere 1, quindi selezionare OK.
7. Chiudere l'editor del Registro di sistema e riavviare il server.

Per ulteriori informazioni, vedere EnableDeadGWDetect nella Microsoft TechNet Library.

Fase 6: test della connessione VPN

Per assicurare il corretto funzionamento della connessione VPN, avvia un'istanza nel VPC e accertati che non sia associata ad alcuna connessione Internet. Dopo l'avvio dell'istanza, esegui il ping del relativo indirizzo IP privato per il Server Windows. Il tunnel VPN viene visualizzato quando il traffico viene generato dal dispositivo gateway del cliente. Pertanto, il comando ping avvia anche la connessione VPN.

Per le fasi di test della connessione VPN, consulta Test di una connessione VPN site-to-site.

Se il comando `ping` non riesce, procedi come descritto di seguito:

- Assicurati di aver configurato le regole di gruppo di sicurezza per consentire il traffico ICMP all'istanza nel VPC. Se il Server Windows è una EC2 instance, assicurarsi che le regole in uscita del gruppo di sicurezza consentano il traffico IPsec. Per ulteriori informazioni, consulta Configurazione dell'istanza Windows.

- Assicurati che il sistema operativo sull'istanza di cui stai eseguendo il ping sia configurato per rispondere a ICMP. È consigliabile utilizzare una delle AMI Amazon Linux.
- Se l'istanza di cui stai eseguendo il ping è un'istanza Windows, connettiti all'istanza e abilita ICMPv4 in entrata sul firewall Windows.
- Assicurati di aver configurato correttamente le tabelle di routing per il VPC o la sottorete. Per ulteriori informazioni, consulta Fase 1: creazione di una connessione VPN e configurazione del VPC.
- Se il dispositivo customer gateway è una EC2 instance, assicurarsi di aver disabilitato il controllo dell'origine/della destinazione per l'istanza. Per ulteriori informazioni, consulta Configurazione dell'istanza Windows.

Nella console Amazon VPC, nella pagina VPN Connections (Connessioni VPN), seleziona la connessione VPN. Il primo tunnel è attivo (stato UP). Il secondo tunnel deve essere configurato, ma verrà utilizzato solo se il primo tunnel diventa inattivo. È possibile che siano necessari alcuni secondi per impostare i tunnel crittografati.

Risoluzione dei problemi relativi al dispositivo gateway del cliente

Negli argomenti seguenti viene descritto come risolvere i problemi di connettività sui dispositivi gateway del cliente.

Per le istruzioni generali di test, consulta Test di una connessione VPN site-to-site.

Oltre agli argomenti di questa sezione, puoi anche utilizzare AWS Site-to-Site VPN registri per individuare e risolvere i problemi di connettività VPN.

Argomenti

- Risoluzione dei problemi di connettività quando si utilizza Border Gateway Protocol
- Risoluzione dei problemi di connettività senza Border Gateway Protocol
- Risoluzione dei problemi di connettività del dispositivo gateway del cliente CISCO ASA
- Risoluzione dei problemi di connettività del gateway del cliente CISCO IOS
- Risoluzione dei problemi relativi alla connettività del dispositivo gateway del cliente CISCO IOS senza Border Gateway Protocol
- Risoluzione dei problemi di connettività del dispositivo gateway del cliente Juniper JunOS
- Risoluzione dei problemi di connettività del gateway del cliente Juniper ScreenOS

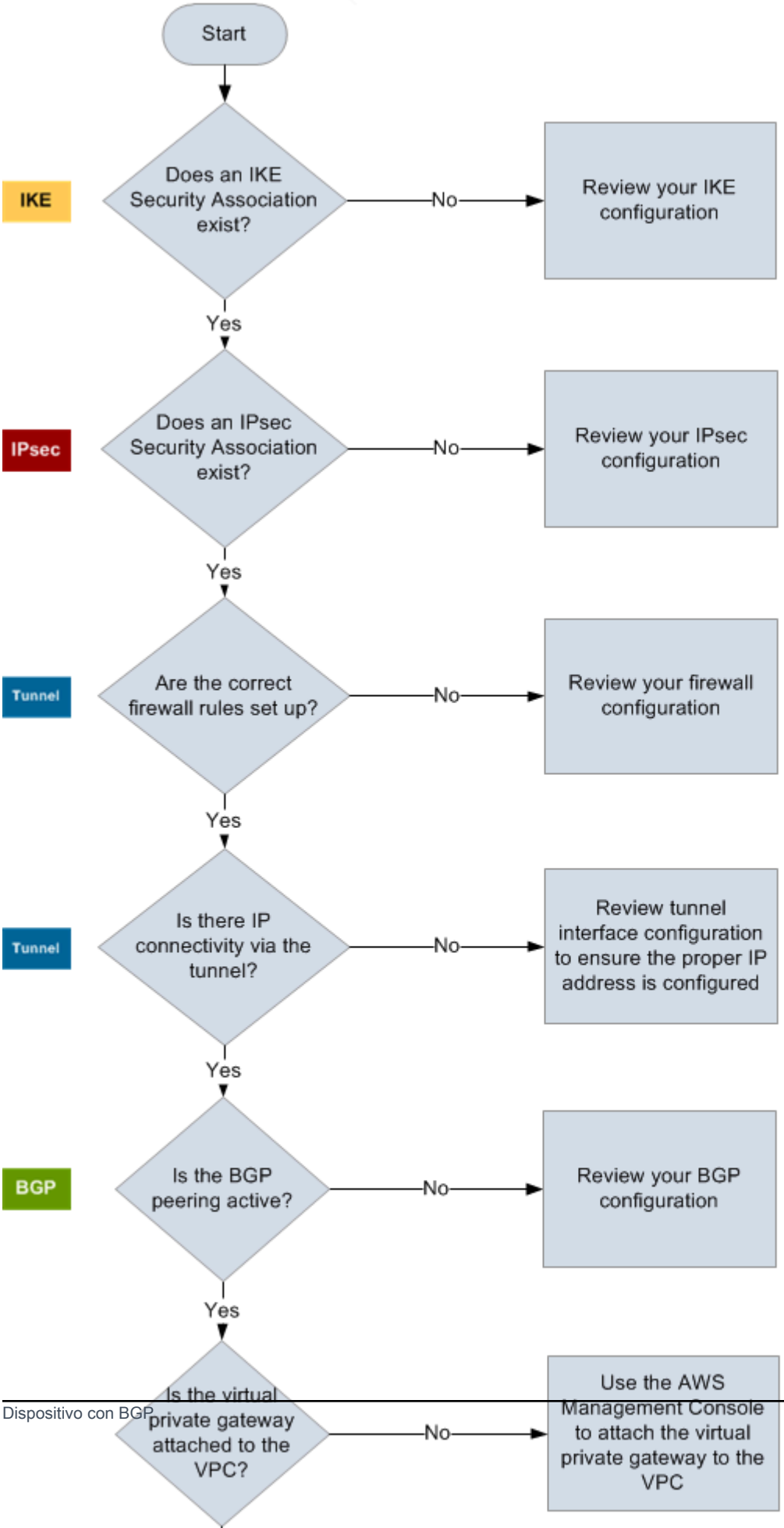
- Risoluzione dei problemi di connettività del dispositivo gateway del cliente Yamaha

Risorse aggiuntive

- Forum su Amazon VPC
- In che modo è possibile risolvere i problemi di connettività del tunnel VPN ad Amazon VPC?

Risoluzione dei problemi di connettività quando si utilizza Border Gateway Protocol

Il diagramma e la tabella seguenti forniscono istruzioni generali per la risoluzione dei problemi di un dispositivo gateway del cliente che utilizza Border Gateway Protocol (BGP). Ti consigliamo inoltre di abilitare le funzionalità di debug del dispositivo. Per informazioni dettagliate, consulta il fornitore del dispositivo gateway.

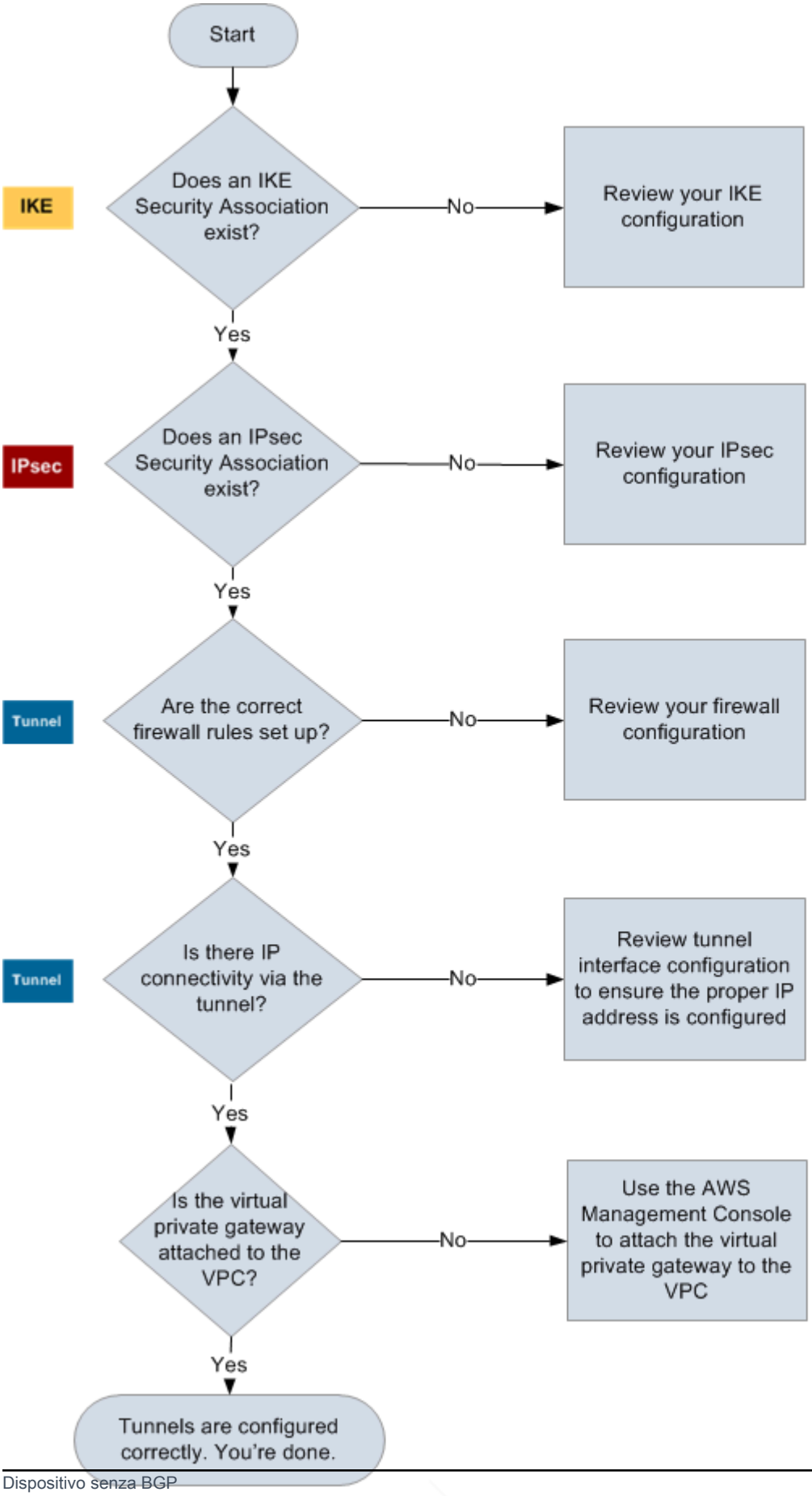

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
BGP
Is the BGP peering active?
No
Review your BGP configuration
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC

IKE	Determina se esiste un'associazione di sicurezza IKE. Un'associazione di sicurezza IKE è necessaria per scambiare chiavi utilizzate per stabilire l'associazione di sicurezza IPsec. Se non esiste un'associazione di questo tipo, esamina le impostazioni di configura zione IKE. Devi configurare i parametri di crittografia, autenticazione, perfect-forward-secrecy e di modalità come elencato nel file di configurazione. Se esiste un'associazione di sicurezza IKE, passa a 'IPsec'.
IPsec	Determina se esiste un'associazione di sicurezza (SA) IPsec. Una SA IPsec è il tunnel stesso. Esegui una query sul gateway del cliente per determinare se una SA IPsec è attiva. Assicurati di configurare i parametri di crittogra fia, autenticazione, perfect-forward-secrecy e di modalità come elencato nel file di configurazione. Se non esiste alcuna SA IPsec, esamina le impostazioni di configurazione IPsec. Se esiste una SA IPsec, passa a 'Tunnel'.
Tunnel	Verifica che le regole di firewall necessarie siano configurate (per un elenco delle regole, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente). Se lo sono, continua. Determina se esiste una connettività IP tramite il tunnel. Ogni lato del tunnel dispone di un indirizzo IP come specificato nel file di configura zione. L'indirizzo del gateway virtuale privato è quello utilizzato come indirizzo router BGP. Dal dispositivo gateway del cliente, esegui il ping di questo indirizzo per determinare se il traffico IP è stato crittografato e decrittografato correttamente. Se il ping non riesce, esamina la configurazione di interfaccia di tunnel per assicurarti che l'indirizzo IP sia configurato correttamente. Se il ping va a buon fine, passa a 'BGP'.
BGP	Determina se la sessione di peering BGP è attiva.

	Per ogni tunnel, procedi come segue: • Nel dispositivo gateway del cliente, determina se lo stato di BGP è `Active` o `Established` . È possibile che siano necessari circa 30 secondi perché un peering BGP diventi attivo. • Assicurati che il dispositivo gateway del cliente annunci la route predefinita (0.0.0.0/0) al gateway virtuale privato. Se i tunnel non sono in questo stato, esamina la configurazione BGP. Se il peering BGP viene stabilito, ricevi un prefisso e annunci un prefisso, il tunnel è configurato correttamente. Verifica che entrambi i tunnel siano in questo stato.

Risoluzione dei problemi di connettività senza Border Gateway Protocol

Il diagramma e la tabella seguenti forniscono istruzioni generali per la risoluzione dei problemi di un dispositivo gateway del cliente che non utilizza Border Gateway Protocol (BGP). Ti consigliamo inoltre di abilitare le funzionalità di debug del dispositivo. Per informazioni dettagliate, consulta il fornitore del dispositivo gateway.


Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC
Yes
Tunnels are configured correctly. You're done.

IKE	Determina se esiste un'associazione di sicurezza IKE. Un'associazione di sicurezza IKE è necessaria per scambiare chiavi utilizzate per stabilire l'associazione di sicurezza IPsec. Se non esiste un'associazione di questo tipo, esamina le impostazioni di configura zione IKE. Devi configurare i parametri di crittografia, autenticazione, perfect-forward-secrecy e di modalità come elencato nel file di configurazione. Se esiste un'associazione di sicurezza IKE, passa a 'IPsec'.
IPsec	Determina se esiste un'associazione di sicurezza (SA) IPsec. Una SA IPsec è il tunnel stesso. Esegui una query sul gateway del cliente per determinare se una SA IPsec è attiva. Assicurati di configurare i parametri di crittogra fia, autenticazione, perfect-forward-secrecy e di modalità come elencato nel file di configurazione. Se non esiste alcuna SA IPsec, esamina le impostazioni di configurazione IPsec. Se esiste una SA IPsec, passa a 'Tunnel'.
Tunnel	Verifica che le regole di firewall necessarie siano configurate (per un elenco delle regole, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente). Se lo sono, continua. Determina se esiste una connettività IP tramite il tunnel. Ogni lato del tunnel dispone di un indirizzo IP come specificato nel file di configura zione. L'indirizzo del gateway virtuale privato è quello utilizzato come indirizzo router BGP. Dal dispositivo gateway del cliente, esegui il ping di questo indirizzo per determinare se il traffico IP è stato crittografato e decrittografato correttamente. Se il ping non riesce, esamina la configurazione di interfaccia di tunnel per assicurarti che l'indirizzo IP sia configurato correttamente. Se il ping ha esito positivo, passa a 'Route statiche'.
Route statiche	Per ogni tunnel, procedi come segue:

	• Verifica di aver aggiunto una route statica al CIDR VPC con i tunnel come hop successivo. • Verifica di aver aggiunto una route statica sulla console Amazon VPC per indicare al gateway virtuale privato di reinstradare il traffico alle reti interne. Se i tunnel non sono in questo stato, esamina la configurazione del dispositivo. Assicurati infine che entrambi i tunnel siano in questo stato.

Risoluzione dei problemi di connettività del dispositivo gateway del cliente CISCO ASA

Per la risoluzione dei problemi di connettività di un dispositivo gateway del cliente Cisco, considera tre elementi: IKE, IPsec e routing. Puoi risolvere i problemi di queste aree in qualsiasi ordine, ma ti consigliamo di iniziare con IKE (nella parte inferiore dello stack di rete) e di risalire.

> **Important**
>
> Alcuni dispositivi Cisco ASA supportano soltanto la modalità Active/Standby. Quando utilizzi questi Cisco ASA, puoi avere un solo tunnel attivo alla volta. Il tunnel in standby diventa attivo solo se il primo tunnel non è più disponibile. Il tunnel in standby potrebbe generare l'errore seguente nei file di log, che può essere ignorato: `Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside`.

IKE

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IKE configurato correttamente.

```
ciscoasa# show crypto isakmp sa
```

```
   Active SA: 2
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2
```

```
1   IKE Peer: AWS_ENDPOINT_1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Devono essere visualizzate una o più linee contenenti un valore `src` del gateway remoto specificato nei tunnel. Il valore `state` deve essere `MM_ACTIVE` e `status` deve essere `ACTIVE`. L'assenza di una voce o qualsiasi voce in un altro stato indica che IKE non è configurato in modo appropriato.

Per un'ulteriore risoluzione dei problemi, esegui i comandi seguenti per abilitare i messaggi di log che forniscono informazioni di diagnostica.

```
router# term mon
router# debug crypto isakmp
```

Per disabilitare il debug, utilizza il comando seguente.

```
router# no debug crypto isakmp
```

IPsec

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IPsec configurato correttamente.

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
    Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

      access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
      current_peer: integ-ppe1

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 6D9F8D3B
      current inbound spi : 48B456A6

    inbound esp sas:
      spi: 0x48B456A6 (1219778214)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x6D9F8D3B (1839172923)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
         0x00000000 0x00000001
```

Per ogni interfaccia di tunnel, devono essere visualizzati `inbound esp sas` e `outbound esp sas`. Ciò presuppone che un'associazione di sicurezza (SA) è elencata (ad esempio, `spi: 0x48B456A6`) e che IPsec è configurato correttamente.

In Cisco ASA, l'IPsec si presenta solo dopo l'invio di traffico interessante (traffico che deve essere crittografato). Per mantenere l'IPsec sempre attivo, consigliamo di configurare un monitoraggio SLA. Il monitoraggio SPLA continua a inviare traffico interessante, mantenendo IPsec attivo.

Puoi anche utilizzare il comando ping seguente per forzare IPsec a iniziare la negoziazione E risalire.

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:
```

```
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Per un'ulteriore risoluzione dei problemi, utilizza il comando seguente per abilitare il debug.

```
router# debug crypto ipsec
```

Per disabilitare il debug, utilizza il comando seguente.

```
router# no debug crypto ipsec
```

Routing

Esegui il ping dell'altra estremità del tunnel. Se questo funziona, allora l'IPsec viene stabilito. In caso contrario, verifica gli elenchi di accesso e fai riferimento alla sezione IPsec precedente.

Se le istanze non sono accessibili, controlla le seguenti informazioni:

1. Verificare che l'elenco di accesso sia configurato per consentire il traffico associato alla mappa crypto.

   A questo proposito, utilizzare il seguente comando.

   ```
   ciscoasa# show run crypto
   ```

   ```
   crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
   crypto map VPN_crypto_map_name 1 match address access-list-name
   crypto map VPN_crypto_map_name 1 set pfs
   crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
   crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
   crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
   ```

2. Controllare l'elenco di accesso utilizzando il seguente comando.

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. Verificare che l'elenco di accesso sia corretto. L'elenco di accesso di esempio consente tutto il traffico interno alla sottorete VPC 10.0.0.0/16.

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Eseguire un traceroute dal dispositivo Cisco ASA per verificare se raggiunge i router Amazon (ad esempio *AWS_ENDPOINT_1*/*AWS_ENDPOINT_2*).

   Se li raggiunge, verifica le route statiche che sono state aggiunte nella console Amazon VPC, nonché i gruppi di sicurezza per le specifiche istanze.
5. Per un'ulteriore risoluzione dei problemi, esaminare la configurazione.

Risoluzione dei problemi di connettività del gateway del cliente CISCO IOS

Per la risoluzione dei problemi di connettività di un dispositivo gateway del cliente Cisco, considera quattro elementi: IKE, IPsec, il tunnel e BGP. Puoi risolvere i problemi di queste aree in qualsiasi ordine, ma ti consigliamo di iniziare con IKE (nella parte inferiore dello stack di rete) e di risalire.

IKE

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IKE configurato correttamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.37.160  72.21.209.193   QM_IDLE           2001    0 ACTIVE
192.168.37.160  72.21.209.225   QM_IDLE           2002    0 ACTIVE
```

Devono essere visualizzate una o più linee contenenti un valore `src` del gateway remoto specificato nei tunnel. `state` deve essere `QM_IDLE` e `status` deve essere `ACTIVE`. L'assenza di una voce o qualsiasi voce in un altro stato indica che IKE non è configurato in modo appropriato.

Per un'ulteriore risoluzione dei problemi, esegui i comandi seguenti per abilitare i messaggi di log che forniscono informazioni di diagnostica.

```
router# term mon
router# debug crypto isakmp
```

Per disabilitare il debug, utilizza il comando seguente.

```
router# no debug crypto isakmp
```

IPsec

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IPsec configurato correttamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
```

```
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xB8357C22(3090512930)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

interface: Tunnel2
      Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

      protected vrf: (none)
      local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer 72.21.209.193 port 500
       PERMIT, flags={origin_is_acl,}
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts compr. failed: 0
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
      current outbound spi: 0xF59A3FF6(4120526838)

      inbound esp sas:
       spi: 0xB6720137(3060924727)
        transform: esp-aes esp-sha-hmac ,
```

```
       in use settings ={Tunnel, }
       conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
       sa timing: remaining key lifetime (k/sec): (4387273/3492)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF59A3FF6(4120526838)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
       sa timing: remaining key lifetime (k/sec): (4387273/3492)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Per ogni interfaccia di tunnel, devono essere visualizzati `inbound esp sas` e `outbound esp sas`. Presupponendo che una SA è elencata (ad esempio, `spi: 0xF95D2F3C`) e che `Status` è `ACTIVE`, IPsec è configurato correttamente.

Per un'ulteriore risoluzione dei problemi, utilizza il comando seguente per abilitare il debug.

```
router# debug crypto ipsec
```

Per disabilitare il debug, utilizza il comando seguente.

```
router# no debug crypto ipsec
```

Tunnel

Innanzi tutto, accertati che le regole di firewall necessarie siano applicate. Per ulteriori informazioni, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente.

Se le regole di firewall sono configurate correttamente, continua con la risoluzione dei problemi utilizzando il comando seguente.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Assicurarsi che il file `line protocol` sia attivo. Verificare che l'indirizzo IP di origine del tunnel, l'interfaccia di origine e la destinazione corrispondano rispettivamente alla configurazione del tunnel per l'indirizzo IP esterno del dispositivo gateway del cliente, all'interfaccia e all'indirizzo IP esterno del gateway virtuale privato. Assicurarsi che il file `Tunnel protection via IPSec` sia presente. Eseguire il comando su entrambe le interfacce di tunnel. Per risolvere qualsiasi tipo di problema, rivedere la configurazione e controllare le connessioni fisiche al dispositivo gateway del cliente.

Utilizza inoltre il comando seguente, sostituendo `169.254.255.1` con l'indirizzo IP interno del gateway virtuale privato.

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Devono essere visualizzati 5 punti esclamativi.

Per un'ulteriore risoluzione dei problemi, esaminare la configurazione.

BGP

Utilizza il seguente comando.

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.255.1   4  7224     363     323        8    0    0 00:54:21        1
169.254.255.5   4  7224     364     323        8    0    0 00:00:24        1
```

Entrambi i router devono essere elencati. Per ciascuno, il valore di `State/PfxRcd` deve essere 1.

Se il peering BGP è attivo, verifica che il router del dispositivo gateway del cliente pubblicizzi la route predefinita (0.0.0.0/0) al VPC.

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network             Next Hop            Metric   LocPrf Weight Path
*> 10.120.0.0/16    169.254.255.1          100        0   7224    i

Total number of prefixes 1
```

Assicurati inoltre di ricevere il prefisso corrispondente al VPC dal gateway virtuale privato.

```
router# show ip route bgp
```

```
 10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

Per un'ulteriore risoluzione dei problemi, esaminare la configurazione.

Risoluzione dei problemi relativi alla connettività del dispositivo gateway del cliente CISCO IOS senza Border Gateway Protocol

Per la risoluzione dei problemi di connettività di un dispositivo gateway del cliente Cisco, considera tre elementi: IKE, IPsec e tunnel. Puoi risolvere i problemi di queste aree in qualsiasi ordine, ma ti consigliamo di iniziare con IKE (nella parte inferiore dello stack di rete) e di risalire.

IKE

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IKE configurato correttamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE           2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE           2002    0 ACTIVE
```

Devono essere visualizzate una o più linee contenenti un valore `src` del gateway remoto specificato nei tunnel. `state` deve essere `QM_IDLE` e `status` deve essere `ACTIVE`. L'assenza di una voce o qualsiasi voce in un altro stato indica che IKE non è configurato in modo appropriato.

Per un'ulteriore risoluzione dei problemi, esegui i comandi seguenti per abilitare i messaggi di log che forniscono informazioni di diagnostica.

```
router# term mon
router# debug crypto isakmp
```

Per disabilitare il debug, utilizza il comando seguente.

```
router# no debug crypto isakmp
```

IPsec

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IPsec configurato correttamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
```

```
       spi: 0x6ADB173(112046451)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
     Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 72.21.209.193 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
     #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
```

```
    current outbound spi: 0xF59A3FF6(4120526838)

    inbound esp sas:
     spi: 0xB6720137(3060924727)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xF59A3FF6(4120526838)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

Per ogni interfaccia di tunnel, deve essere visualizzato un `esp sas` in entrata e un `esp sas` in uscita. Ciò presuppone che una SA è elencata (ad esempio, `spi: 0x48B456A6`), che lo stato è `ACTIVE` e che IPsec è configurato correttamente.

Per un'ulteriore risoluzione dei problemi, utilizza il comando seguente per abilitare il debug.

```
router# debug crypto ipsec
```

Per disabilitare il debug, utilizza il comando seguente.

```
router# no debug crypto ipsec
```

Tunnel

Innanzi tutto, accertati che le regole di firewall necessarie siano applicate. Per ulteriori informazioni, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente.

Se le regole di firewall sono configurate correttamente, continua con la risoluzione dei problemi utilizzando il comando seguente.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Assicurati che il protocollo di linea sia attivo. Verificare che l'indirizzo IP di origine del tunnel, l'interfaccia di origine e la destinazione corrispondano rispettivamente alla configurazione del tunnel per l'indirizzo IP esterno del dispositivo gateway del cliente, all'interfaccia e all'indirizzo IP esterno del gateway virtuale privato. Assicurarsi che il file `Tunnel protection through IPSec` sia presente. Eseguire il comando su entrambe le interfacce di tunnel. Per risolvere qualsiasi tipo di problema, rivedere la configurazione e controllare le connessioni fisiche al dispositivo gateway del cliente.

Puoi anche utilizzare il comando seguente, sostituendo `169.254.249.18` con l'indirizzo IP interno del gateway virtuale privato.

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Devono essere visualizzati 5 punti esclamativi.

Routing

Per visualizzare la tabella di routing statica, utilizza il comando seguente.

```
router# sh ip route static
```

```
     1.0.0.0/8 is variably subnetted
S       10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

Verifica che la route statica esista per il CIDR VPC via i due tunnel. In caso contrario, aggiungi le route statiche come mostrato di seguito.

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Verifica del monitoraggio SLA

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
```

```
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

Il valore per `Number of successes` indica se il monitor SLA è stato configurato correttamente.

Per un'ulteriore risoluzione dei problemi, esaminare la configurazione.

Risoluzione dei problemi di connettività del dispositivo gateway del cliente Juniper JunOS

Per la risoluzione dei problemi di connettività di un dispositivo gateway del cliente Juniper, considera quattro elementi: IKE, IPsec, tunnel e BGP. Puoi risolvere i problemi di queste aree in qualsiasi ordine, ma ti consigliamo di iniziare con IKE (nella parte inferiore dello stack di rete) e di risalire.

IKE

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IKE configurato correttamente.

```
user@router> show security ike security-associations
```

```
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       72.21.209.225   UP     c4cd953602568b74  0d6d194993328b02  Main
3       72.21.209.193   UP     b8c8fb7dc68d9173  ca7cb0abaedeb4bb  Main
```

Devono essere visualizzate una o più linee contenenti un indirizzo remoto del gateway remoto specificato nei tunnel. `State` deve essere `UP`. L'assenza di una voce, o qualsiasi voce in un altro stato (come `DOWN`), indica che IKE non è configurato in modo appropriato.

Per un'ulteriore risoluzione dei problemi, abilita le opzioni di monitoraggio IKE come consigliato nel file di configurazione di esempio. Esegui quindi il comando seguente per stampare vari messaggi di debug sullo schermo.

```
user@router> monitor start kmd
```

Da un host esterno, puoi recuperare l'intero file di log con il comando seguente.

```
scp username@router.hostname:/var/log/kmd
```

IPsec

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IPsec configurato correttamente.

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway        Port  Algorithm        SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225  500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
>131073 72.21.209.225  500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193  500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193  500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

In particolare, devono essere visualizzate almeno due linee per indirizzo di gateway (corrispondente al gateway remoto). Le parentesi angolare all'inizio di ogni linea (**< >**) indica la direzione del traffico per la particolare voce. L'output ha linee distinte per il traffico in entrata ("**<**", traffico dal gateway virtuale privato a questo dispositivo gateway del cliente) e il traffico in uscita ("**>**").

Per un'ulteriore risoluzione dei problemi, abilita le opzioni di monitoraggio IKE (per ulteriori informazioni, consulta la sezione precedente su IKE).

Tunnel

Innanzi tutto, accertati che le regole di firewall necessarie siano applicate. Per un elenco di regole, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente.

Se le regole di firewall sono configurate correttamente, continua con la risoluzione dei problemi utilizzando il comando seguente.

```
user@router> show interfaces st0.1
```

```
 Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
    Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
    Input packets : 8719
    Output packets: 41841
    Security: Zone: Trust
    Allowed host-inbound traffic : bgp ping ssh traceroute
    Protocol inet, MTU: 9192
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
      Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Assicurati che il valore di `Security: Zone` sia corretto e che l'indirizzo `Local` corrisponda all'indirizzo interno del tunnel del dispositivo gateway del cliente.

Successivamente, utilizza il comando seguente, sostituendo `169.254.255.1` con l'indirizzo IP interno del gateway virtuale privato. I risultati devono essere simili alla risposta riportata di seguito.

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

Per un'ulteriore risoluzione dei problemi, esaminare la configurazione.

BGP

Esegui il comando seguente.

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 2          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1          7224          9         10       0       0        1:00 1/1/1/0
            0/0/0/0
```

```
169.254.255.5          7224          8          9       0       0          56 0/1/1/0
            0/0/0/0
```

Per un'ulteriore risoluzione dei problemi, puoi anche utilizzare il comando seguente, sostituendo `169.254.255.1` con l'indirizzo IP interno del gateway virtuale privato.

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ EXPORT-DEFAULT ]
  Options: <Preference HoldTime PeerAS LocalAS Refresh>
  Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
  Number of flaps: 0
  Peer ID: 169.254.255.1    Local ID: 10.50.0.10       Active Holdtime: 30
  Keepalive Interval: 10         Peer index: 0
  BFD: disabled, down
  Local Interface: st0.1
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 7224)
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:              1
    Received prefixes:            1
    Accepted prefixes:            1
    Suppressed due to damping:    0
    Advertised prefixes:          1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24     Updates 2       Refreshes 0     Octets 505
Output messages: Total 26     Updates 1       Refreshes 0     Octets 582
```

```
Output Queue[0]: 0
```

Il valore di `Received prefixes` e `Advertised prefixes` deve essere 1 nella sezione `Table inet.0`.

Se il valore di `State` non è `Established`, verifica il valore di `Last State` e `Last Error` per informazioni dettagliate su come procedere per risolvere il problema.

Se il peering BGP è attivo, verifica che il router del dispositivo gateway del cliente pubblicizzi la route predefinita (0.0.0.0/0) al VPC.

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               Self                                    I
```

Assicurati, inoltre, di ricevere il prefisso che corrisponde al VPC dal gateway virtuale privato.

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.110.0.0/16           169.254.255.1        100                7224 I
```

Risoluzione dei problemi di connettività del gateway del cliente Juniper ScreenOS

Per la risoluzione dei problemi di connettività di un dispositivo gateway del cliente basato su Juniper ScreenOS, considera quattro elementi: IKE, IPsec, tunnel e BGP. Puoi risolvere i problemi di queste aree in qualsiasi ordine, ma ti consigliamo di iniziare con IKE (nella parte inferiore dello stack di rete) e di risalire.

IKE e IPsec

Utilizza il seguente comando. La risposta mostra un dispositivo gateway del cliente con IKE configurato correttamente.

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000002<   72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-    -1 0
00000002>   72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-    -1 0
00000001<   72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-    -1 0
00000001>   72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-    -1 0
```

Devono essere visualizzate una o più linee contenenti un indirizzo remoto del gateway remoto specificato nei tunnel. Il valore di `Sta` deve essere `A/-` e quello di `SPI` deve essere un numero esadecimale diverso da `00000000`. Le voci in altri stati indicano che IKE non è configurato in modo appropriato.

Per un'ulteriore risoluzione dei problemi, abilita le opzioni di monitoraggio IKE come consigliato nel file di configurazione di esempio.

Tunnel

Innanzi tutto, accertati che le regole di firewall necessarie siano applicate. Per un elenco di regole, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente.

Se le regole di firewall sono configurate correttamente, continua con la risoluzione dei problemi utilizzando il comando seguente.

```
ssg5-serial-> get interface tunnel.1
```

```
  Interface tunnel.1:
  description tunnel.1
  number 20, if_info 1768, if_index 1, mode route
  link ready
  vsys Root, zone Trust, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
  *ip 169.254.255.2/30
  *manage ip 169.254.255.2
  route-deny disable
  bound vpn:
    IPSEC-1

  Next-Hop Tunnel Binding table
```

```
  Flag Status Next-Hop(IP)    tunnel-id  VPN

  pmtu-v4 disabled
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled

  OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  NHRP disabled
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

Assicurati che `link:ready` sia visualizzato e che l'indirizzo `IP` corrisponda all'indirizzo interno del tunnel del dispositivo gateway del cliente.

Successivamente, utilizza il comando seguente, sostituendo `169.254.255.1` con l'indirizzo IP interno del gateway virtuale privato. I risultati devono essere simili alla risposta riportata di seguito.

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

Per un'ulteriore risoluzione dei problemi, esaminare la configurazione.

BGP

Esegui il comando seguente.

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

```
Peer AS Remote IP       Local IP          Wt Status   State     ConnID Up/Down
------------------------------------------------------------------------------
   7224 169.254.255.1   169.254.255.2    100 Enabled  ESTABLISH     10 00:01:01
   7224 169.254.255.5   169.254.255.6    100 Enabled  ESTABLISH     11 00:00:59
```

Per entrambi i peer BGP lo stato deve essere `ESTABLISH`. Questo indica che la connessione BGP al gateway virtuale privato è attiva.

Per un'ulteriore risoluzione dei problemi, puoi anche utilizzare il comando seguente, sostituendo `169.254.255.1` con l'indirizzo IP interno del gateway virtuale privato.

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1,  remote AS: 7224, admin status: enable
type: EBGP, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
 retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:  advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
 subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

Se il peering BGP è attivo, verifica che il router del dispositivo gateway del cliente pubblicizzi la route predefinita (0.0.0.0/0) al VPC. Questo comando si applica a ScreenOS versione 6.2.0 e versione successiva.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
-------------------------------------------------------------------------------
>i          0.0.0.0/0         0.0.0.0 32768   100     0  IGP
Total IPv4 routes advertised: 1
```

Assicurati, inoltre, di ricevere il prefisso corrispondente al VPC dal gateway virtuale privato. Questo comando si applica a ScreenOS versione 6.2.0 e versione successiva.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
-------------------------------------------------------------------------------
>e*     10.0.0.0/16   169.254.255.1   100   100   100  IGP   7224
Total IPv4 routes received: 1
```

Risoluzione dei problemi di connettività del dispositivo gateway del cliente Yamaha

Per la risoluzione dei problemi di connettività di un dispositivo gateway del cliente Yamaha, considera quattro elementi: IKE, IPsec, tunnel e BGP. Puoi risolvere i problemi di queste aree in qualsiasi ordine, ma ti consigliamo di iniziare con IKE (nella parte inferiore dello stack di rete) e di risalire.

> **Note**
>
> Per impostazione predefinita, l'impostazione `proxy ID` utilizzata nella fase 2 di IKE è disabilitata sul router Yamaha. Ciò può causare problemi di connessione a Site-to-Site VPN. Se non `proxy ID` è configurato sul router, consulta il file di configurazione AWS di esempio fornito per Yamaha per impostarlo correttamente.

IKE

Esegui il comando seguente. La risposta mostra un dispositivo gateway del cliente con IKE configurato correttamente.

```
# show ipsec sa gateway 1
```

```
sgw  flags local-id                    remote-id        # of sa
-------------------------------------------------------------------------
1    U K   YOUR_LOCAL_NETWORK_ADDRESS     72.21.209.225    i:2 s:1 r:1
```

Deve essere visualizzata una linea con un valore `remote-id` del gateway remoto specificato nei tunnel. Puoi elencare tutte le associazioni di sicurezza (SA) omettendo il numero di tunnel.

Per un'ulteriore risoluzione dei problemi, esegui i comandi seguenti per abilitare i messaggi di log di livello DEBUG che forniscono informazioni di diagnostica.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Per annullare gli elementi registrati, esegui il comando seguente:

```
# no ipsec ike log
# no syslog debug on
```

IPsec

Esegui il comando seguente. La risposta mostra un dispositivo gateway del cliente con IPsec configurato correttamente.

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
```

```
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
```

Per ogni interfaccia di tunnel, devono essere visualizzati `receive sas` e `send sas`.

Per un'ulteriore risoluzione dei problemi, utilizza il comando seguente per abilitare il debug.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Per disabilitare il debug, esegui il comando seguente.

```
# no ipsec ike log
# no syslog debug on
```

Tunnel

Innanzi tutto, accertati che le regole di firewall necessarie siano applicate. Per un elenco di regole, consulta Configurazione di un firewall tra Internet e il dispositivo gateway del cliente.

Se le regole di firewall sono configurate correttamente, continua con la risoluzione dei problemi utilizzando il comando seguente.

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds  connection.
  Received:    (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
  Transmitted: (IPv4) 3933 packets [241407 octets]
               (IPv6) 0 packet [0 octet]
```

Assicurati che il valore `current status` sia online e che `Interface type` sia IPsec. e di eseguire il comando su entrambe le interfacce di tunnel. Per risolvere qualsiasi problema in questa fase, esamina la configurazione.

BGP

Esegui il comando seguente.

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
```

```
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:
```

Entrambi i router devono essere elencati. Per ciascuno, il valore di BGP `state` deve essere `Active`.

Se il peering BGP è attivo, verifica che il router del dispositivo gateway del cliente pubblicizzi la route predefinita (0.0.0.0/0) al VPC.

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```
Total routes: 1
*: valid route
  Network            Next Hop        Metric LocPrf Path
* default            0.0.0.0              0        IGP
```

Assicurati, inoltre, di ricevere il prefisso corrispondente al VPC dal gateway virtuale privato.

```
# show ip route
```

```
Destination         Gateway          Interface       Kind  Additional Info.
default             ***.***.***.***   LAN3(DHCP)    static
10.0.0.0/16         169.254.255.1    TUNNEL[1]       BGP  path=10124
```

Utilizzo della VPN site-to-site

Puoi utilizzare le risorse Site-to-Site VPN con la console Amazon VPC o la AWS CLI.

Indice

Crea un allegato VPN da sito a sito per Cloud WAN AWS

Segui la procedura seguente per creare un allegato VPN da sito a sito per Cloud WAN. AWS

Per creare un allegato VPN per AWS Cloud WAN utilizzando la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Scegliere Create VPN Connection (Crea connessione VPN).
4. (Facoltativo) In Tag nome, immetti un nome per la connessione. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
5. Per Target Gateway Type (Tipo di gateway di destinazione), scegli Not Associated (Non associato).

6. In Customer Gateway (Gateway del cliente), eseguire una delle seguenti operazioni:
   - Per utilizzare un gateway del cliente esistente, seleziona Esistente, quindi seleziona il gateway del cliente.
   - Per creare un gateway del cliente, scegliere New (Nuovo). In IP Address (Indirizzo IP), inserire un indirizzo IP pubblico statico. In Certificate ARN (ARN certificato), scegliere l'ARN del certificato privato (se si utilizza l'autenticazione basata su certificati). In BGP ASN, immettere il Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway del cliente. Per ulteriori informazioni, consulta Opzioni gateway del cliente.
7. In Opzioni di routing, seleziona se utilizzare la modalità Dinamica o Statica.
8. Per Tunnel all'interno della versione IP, scegli se utilizzare IPv4 o IPv6.
9. (Facoltativo) In Enable Acceleration (Abilita accelerazione), selezionare la casella di controllo per abilitare l'accelerazione. Per ulteriori informazioni, consulta Connessioni VPN accelerate.

   Se si abilita l'accelerazione, vengono creati due acceleratori utilizzati dalla connessione VPN. Vengono applicati costi aggiuntivi.
10. (Facoltativo) Per Local IPv4 network CIDR (CIDR di rete IPv4 locale), specificare l'intervallo CIDR IPv4 sul lato gateway del cliente (On-Premise) a cui è consentito comunicare attraverso i tunnel VPN. Il valore di default è `0.0.0.0/0`.

    Per il CIDR della rete IPv4 remota, specifica l'intervallo CIDR IPv4 sul AWS lato autorizzato a comunicare attraverso i tunnel VPN. Il valore predefinito è `0.0.0.0/0`.

    Se hai specificato IPv6 per la versione IP di Tunnel inside, specifica gli intervalli CIDR IPv6 sul lato gateway del cliente e sul lato a cui è consentito comunicare tramite i tunnel VPN. AWS Il valore predefinito per entrambi gli intervalli è `::/0`.
11. (Facoltativo) per Opzioni tunnel, è possibile specificare le seguenti informazioni per ciascun tunnel:

    - Un blocco CIDR IPv4 di dimensione /30 dall'intervallo `169.254.0.0/16` per gli indirizzi IPv4 del tunnel interno.
    - Se hai specificato IPv6 per Tunnel interno alla versione IP, un blocco CIDR IPv6 /126 dall'intervallo `fd00::/8` per gli indirizzi IPv6 del tunnel interno.
    - La chiave precondivisa IKE (PSK). Sono supportate le seguenti versioni: IKEv1 o IKEv2.
    - Per modificare le opzioni avanzate del tunnel, scegli Modifica le opzioni tunnel. Per ulteriori informazioni, consulta Opzioni per tunnel VPN.
12. Scegliere Create VPN Connection (Crea connessione VPN).

Per creare una connessione Site-to-Site VPN utilizzando la riga di comando o l'API

- CreateVpnConnessione (API di interrogazione Amazon EC2)
- create-vpn-connection (AWS CLI)

Creazione di un collegamento VPN al gateway di transito

Per creare un allegato VPN su un gateway di transito, è necessario specificare il gateway di transito e il gateway del cliente. Il gateway di transito dovrà essere creato prima di seguire questa procedura. Per ulteriori informazioni sulla creazione di un gateway di transito, consulta Gateway di transito in Gateway di transito Amazon VPC.

Per creare un allegato VPN su un gateway di transito mediante la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Scegliere Create VPN Connection (Crea connessione VPN).
4. (Facoltativo) In Tag nome, immetti un nome per la connessione. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
5. Per Tipo di gateway di destinazione, scegli Gateway di transito, quindi scegli il gateway di transito.
6. In Customer Gateway (Gateway del cliente), eseguire una delle seguenti operazioni:
   - Per utilizzare un gateway del cliente esistente, seleziona Esistente, quindi seleziona il gateway del cliente.

     Se il gateway del cliente si trova dietro un dispositivo NAT abilitato per NAT Traversal (NAT-T), utilizzare l'indirizzo IP pubblico del dispositivo NAT e modificare le regole del firewall per sbloccare la porta UDP 4500.
   - Per creare un gateway del cliente, scegliere New (Nuovo). In IP Address (Indirizzo IP), immettere un indirizzo IP pubblico statico. In Certificate ARN (ARN certificato), scegliere l'ARN del certificato privato (se si utilizza l'autenticazione basata su certificati). In BGP ASN, immettere il Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway del cliente. Per ulteriori informazioni, consulta Opzioni gateway del cliente.
7. In Opzioni di routing, seleziona se utilizzare la modalità Dinamica o Statica.

8. Per Tunnel all'interno della versione IP, specifica se i tunnel VPN supportano il traffico IPv4 o IPv6. Il traffico IPv6 è supportato solo per le connessioni VPN su un gateway di transito.
9. (Facoltativo) In Enable Acceleration (Abilita accelerazione), selezionare la casella di controllo per abilitare l'accelerazione. Per ulteriori informazioni, consulta Connessioni VPN accelerate.

   Se si abilita l'accelerazione, vengono creati due acceleratori utilizzati dalla connessione VPN. Vengono applicati costi aggiuntivi.
10. (Facoltativo) Per Local IPv4 network CIDR (CIDR di rete IPv4 locale), specificare l'intervallo CIDR IPv4 sul lato gateway del cliente (On-Premise) a cui è consentito comunicare attraverso i tunnel VPN. Il valore di default è `0.0.0.0/0`.

    Per Remote IPv4 network CIDR (CIDR di rete IPv4 remota), specificare l'intervallo CIDR IPv4 sul lato AWS a cui è consentito comunicare attraverso i tunnel VPN. Il valore di default è `0.0.0.0/0`.

    Se hai specificato IPv6 per Tunnel inside IP version (Versione IP tunnel interno), specifica gli intervalli CIDR IPv6 sul lato gateway del cliente e sul lato AWS che possono comunicare attraverso i tunnel VPN. Il valore predefinito per entrambi gli intervalli è `::/0`.
11. (Facoltativo) per Opzioni tunnel, è possibile specificare le seguenti informazioni per ciascun tunnel:

    - Un blocco CIDR IPv4 di dimensione /30 dall'intervallo `169.254.0.0/16` per gli indirizzi IPv4 del tunnel interno.
    - Se hai specificato IPv6 per Tunnel interno alla versione IP, un blocco CIDR IPv6 /126 dall'intervallo `fd00::/8` per gli indirizzi IPv6 del tunnel interno.
    - La chiave precondivisa IKE (PSK). Sono supportate le seguenti versioni: IKEv1 o IKEv2.
    - Per modificare le opzioni avanzate del tunnel, scegli Modifica le opzioni tunnel. Per ulteriori informazioni, consulta Opzioni per tunnel VPN.
12. Scegliere Create VPN Connection (Crea connessione VPN).

Per creare un collegamento a una VPN utilizzando la AWS CLI

Utilizza il comando create-vpn-connection e specifica l'ID del gateway di transito per l'opzione `--transit-gateway-id`.

Test di una connessione VPN site-to-site

Dopo aver creato la AWS Site-to-Site VPN connessione e configurato il gateway del cliente, puoi avviare un'istanza e testare la connessione eseguendo il ping dell'istanza.

Prima di iniziare, assicurati di:

- Utilizzare un'AMI che risponda alle richieste di ping. È consigliabile utilizzare una delle AMI Amazon Linux.
- Configurare qualsiasi gruppo di sicurezza o lista di controllo degli accessi di rete nel VPC che filtra il traffico all'istanza per consentire traffico ICMP in entrata e in uscita. Ciò consente all'istanza di ricevere richieste `ping`.
- Se si utilizzano istanze che eseguono Windows Server, connettersi all'istanza e abilitare ICMPv4 in entrata sul firewall Windows per eseguire il ping dell'istanza.
- (Routing statico) Assicurarsi che il dispositivo gateway del cliente disponga di un percorso statico al VPC e che la connessione VPN disponga di un percorso statico per consentire al traffico di tornare al dispositivo gateway del cliente.
- (Routing dinamico) Assicurarsi di aver stabilito lo stato BGP sul dispositivo gateway del cliente. Per stabilire una sessione peering BGP occorrono circa 30 secondi. Assicurarsi che le route siano pubblicizzate correttamente con BGP e visualizzate nella tabella di routing della sottorete, in modo che il traffico possa tornare al gateway del cliente. Assicurati che Entrambi i tunnel siano configurati con il routing BGP.
- Assicurarsi di aver configurato il routing nelle tabelle di routing della sottorete per la connessione VPN.

Per testare la connettività

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di controllo scegliere Avvia istanza.
3. (Facoltativo) Per Nome, inserisci un nome descrittivo per l'istanza.
4. In Immagini di applicazioni e sistema operativo (Amazon Machine Image), scegli Avvio rapido, quindi scegli il sistema operativo per l'istanza.
5. Per Nome della coppia di chiavi, scegli una coppia di chiavi esistente o creane una nuova.
6. Per Impostazioni di rete, scegli Seleziona gruppo di sicurezza esistente, quindi scegli il gruppo di sicurezza configurato.

7. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).
8. Quando l'istanza è in esecuzione, recuperarne l'indirizzo IP privato (ad esempio, 10.0.0.4). La console Amazon EC2 visualizza l'indirizzo come parte dei dettagli dell'istanza.
9. Da un computer nella rete che si trova dietro il gateway del cliente, utilizzare il comando ping con l'indirizzo IP privato dell'istanza.

   ```
   ping 10.0.0.4
   ```

   Una risposta con esito positivo è simile a quella riportata di seguito.

   ```
   Pinging 10.0.0.4 with 32 bytes of data:

   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

   Ping statistics for 10.0.0.4:
   Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

   Approximate round trip times in milliseconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
   ```

   Per verificare il failover del tunnel, puoi disabilitare temporaneamente uno dei tunnel sul dispositivo gateway del cliente e quindi ripetere questa fase. Non puoi disabilitare un tunnel sul lato AWS della connessione VPN.
10. Per testare la connessione dalla AWS rete locale, puoi utilizzare SSH o RDP per connetterti all'istanza dalla rete. È quindi possibile eseguire il comando `ping` con l'indirizzo IP privato di un altro computer della rete, per verificare che entrambi i lati della connessione possano avviare e ricevere richieste.

    Per ulteriori informazioni su come connettersi a un'istanza Linux, consulta Connect to your Linux istance nella Amazon EC2 User Guide. Per ulteriori informazioni su come connettersi a un'istanza Windows, consulta Connect to your Windows istance nella Amazon EC2 User Guide.

Eliminazione di una connessione VPN site-to-site

Se non hai più bisogno di una AWS Site-to-Site VPN connessione, puoi eliminarla. Quando si elimina una connessione Site-to-Site VPN, non viene eliminato il gateway del cliente o il gateway virtuale

privato associato alla connessione Site-to-Site VPN. Se non sono più necessari il gateway cliente e il gateway privato virtuale, è possibile eliminarli.

> **Warning**
>
> Se elimini la connessione VPN site-to-site e ne crei una nuova, è necessario scaricare un nuovo file di configurazione e riconfigurare il dispositivo gateway del cliente.

Attività

- Eliminazione di una connessione VPN
- Eliminazione di un gateway del cliente
- Scollegamento ed eliminazione di un gateway privato virtuale

Eliminazione di una connessione VPN

Dopo aver eliminato la connessione Site-to-Site VPN, quest'ultima rimane visibile per un breve periodo con uno stato di `deleted`, quindi la voce viene automaticamente rimossa.

Per eliminare una connessione VPN tramite la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione VPN, quindi scegli Operazioni, Elimina connessione VPN.
4. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare una connessione VPN utilizzando la riga di comando o l'API

- DeleteVpnConnessione (API di interrogazione Amazon EC2)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

Eliminazione di un gateway del cliente

Se un gateway cliente non è più necessario, puoi eliminarlo. Non puoi eliminare un gateway del cliente utilizzato in una connessione Site-to-Site VPN.

Per eliminare un gateway del cliente tramite la console

1. Nel riquadro di navigazione, scegli Gateway del cliente.
2. Seleziona il gateway del cliente e scegli Operazioni, Elimina gateway del cliente.
3. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare un gateway del cliente utilizzando la riga di comando o l'API

- DeleteCustomerGateway (API di interrogazione Amazon EC2)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Scollegamento ed eliminazione di un gateway privato virtuale

Se un gateway virtuale privato per il VPC non è più necessario, puoi scollegarlo.

Per scollegare un gateway virtuale privato tramite la console

1. Nel riquadro di navigazione, scegli Gateway privati virtuali.
2. Selezionare il gateway virtuale privato e scegliere Actions (Operazioni), Detach from VPC (Scollega da VPC).
3. Scegli Scollega gateway privato virtuale.

Se un gateway virtuale privato scollegato non è più necessario, puoi eliminarlo. Non puoi eliminare un gateway virtuale privato ancora collegato a un VPC. Dopo essere stato eliminato, il gateway virtuale privato rimane visibile per un breve periodo con uno stato di `deleted` e quindi la voce viene rimossa automaticamente.

Per eliminare un gateway virtuale privato tramite la console

1. Nel riquadro di navigazione, scegli Gateway privati virtuali.
2. Seleziona il gateway privato virtuale da eliminare e scegli Operazioni, Elimina gateway privato virtuale.
3. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per scollegare un gateway virtuale privato utilizzando la riga di comando o l'API

- DetachVpnGateway (API di interrogazione Amazon EC2)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

Per eliminare un gateway virtuale privato utilizzando la riga di comando o l'API

- DeleteVpnGateway (API di interrogazione Amazon EC2)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Modifica del gateway di destinazione della connessione VPN site-to-site

È possibile modificare il gateway di destinazione di una connessione AWS Site-to-Site VPN. Sono disponibili le seguenti opzioni di migrazione:

- Un gateway virtuale privato esistente a un gateway di transito
- Un gateway virtuale privato esistente a un altro gateway virtuale privato
- Un gateway di transito esistente a un altro gateway di transito
- Un gateway di transito esistente a un gateway virtuale privato

Dopo aver modificato il gateway di destinazione, la connessione Site-to-Site VPN sarà temporaneamente non disponibile per un breve periodo durante il provisioning dei nuovi endpoint.

Le seguenti attività ti consentono di completare la migrazione a un nuovo gateway.

Attività

- Fase 1: creazione del nuovo gateway di destinazione
- Fase 2: eliminazione degli instradamenti statici (condizionale)
- Fase 3: esecuzione della migrazione a un nuovo gateway
- Fase 4: aggiornamento delle tabelle di routing VPC
- Fase 5: aggiorna l'instradamento del gateway di destinazione (condizionale)

- Fase 6: aggiornamento dell'ASN del gateway del cliente (condizionale)

Fase 1: creazione del nuovo gateway di destinazione

Prima di eseguire la migrazione al nuovo gateway di destinazione, è necessario prima configurarlo. Per ulteriori informazioni sull'aggiunta di un gateway virtuale privato, consulta the section called "Creazione di gateway virtuale privato". Per ulteriori informazioni sull'aggiunta di un gateway di transito, consulta Creare un gateway di transito in Gateway di transito Amazon VPC.

Se il nuovo gateway di destinazione è un gateway di transito, collega i VPC al gateway di transito. Per informazioni sugli allegati VPC, consulta la sezione relativa ai collegamenti del gateway di transito a un VPC in Gateway di transito Amazon VPC.

Quando modifichi la destinazione da un gateway virtuale privato a un gateway di transito, puoi impostare facoltativamente l'ASN del gateway di transito sullo stesso valore dell'ASN del gateway virtuale privato. Se scegli di avere un ASN diverso, devi impostare l'ASN sul dispositivo gateway del cliente sull'ASN del gateway di transito. Per ulteriori informazioni, consulta the section called "Fase 6: aggiornamento dell'ASN del gateway del cliente (condizionale)".

Fase 2: eliminazione degli instradamenti statici (condizionale)

Questa fase è obbligatoria quando esegui la migrazione da un gateway virtuale privato con route statiche a un gateway di transito.

È necessario eliminare la route statiche prima di eseguire la migrazione al nuovo gateway.

> **Tip**
>
> Mantieni una copia delle route statiche prima di eliminarle. Dovrai aggiungere di nuovo queste route al gateway di transito al termine della migrazione della connessione VPN.

Per eliminare una route da una tabella di routing

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di instradamento e seleziona la tabella di instradamento.
3. Nella scheda Route, scegli Modifica route.

4. Scegli Rimuovi per l'instradamento statico al gateway privato virtuale.
5. Seleziona Salva modifiche.

Fase 3: esecuzione della migrazione a un nuovo gateway

Modifica del gateway di destinazione

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione VPN e scegli Operazioni, Modifica connessione VPN.
4. Per Tipo di destinazione, scegli il tipo di gateway.
    a. Se il nuovo gateway di destinazione è un gateway privato virtuale, scegli gateway VPN.
    b. Se il nuovo gateway di destinazione è un gateway di transito, scegli Gateway di transito.
5. Seleziona Salva modifiche.

Per modificare una connessione Site-to-Site VPN tramite la riga di comando o l'API

- ModifyVpnConnection (API della query Amazon EC2)
- modify-vpn-connection (AWS CLI)

Fase 4: aggiornamento delle tabelle di routing VPC

Dopo la migrazione al nuovo gateway, potrebbe essere necessario modificare la tabella di routing VPC. Per ulteriori informazioni, consulta le tabelle di routing nella Guida per l'utente di Amazon VPC.

La tabella seguente fornisce informazioni sugli aggiornamenti della tabella di routing VPC da apportare dopo aver modificato la destinazione del gateway VPN.

Gateway esistente	Nuovo gateway	Modifica della tabella di routing VPC
Gateway virtuale privato con route propagate	Transit Gateway	Aggiunta di un instradamento che contenga l'ID del gateway di transito.

Gateway esistente	Nuovo gateway	Modifica della tabella di routing VPC
Gateway virtuale privato con route propagate	Gateway virtuale privato con route propagate	Non è necessaria alcuna azione.
Gateway virtuale privato con route propagate	Gateway virtuale privato con route statica	Aggiunta di un instradamento che contenga l'ID del nuovo gateway privato virtuale.
Gateway virtuale privato con route statiche	Transit Gateway	Aggiornamento dell'inst radamento contenente l'ID del gateway privato virtuale con l'ID del gateway di transito.
Gateway virtuale privato con route statiche	Gateway virtuale privato con route statiche	Aggiornamento dell'inst radamento contenente l'ID del gateway privato virtuale con l'ID del nuovo gateway privato virtuale.
Gateway virtuale privato con route statiche	Gateway virtuale privato con route propagate	Eliminazione dell'inst radamento contenente l'ID del gateway privato virtuale.
Transit Gateway	Gateway virtuale privato con route statiche	Aggiornamento dell'inst radamento contenente l'ID del gateway di transito con l'ID del gateway privato virtuale.
Transit Gateway	Gateway virtuale privato con route propagate	Eliminazione dell'inst radamento contenente l'ID del gateway di transito.
Transit Gateway	Transit Gateway	Aggiornamento dell'inst radamento contenente l'ID del gateway di transito con l'ID del nuovo gateway di transito.

Fase 5: aggiorna l'instradamento del gateway di destinazione (condizionale)

Quando il nuovo gateway è un gateway di transito, modifica la tabella di routing del gateway di transito per consentire il traffico tra il VPC e la Site-to-Site VPN. Per ulteriori informazioni, consulta Tebelle di routing del gateway di transito in Gateway di transito di Amazon VPC.

Se hai eliminato le route statiche VPN, è necessario aggiungere le route statiche alla tabella di routing del gateway di transito.

A differenza di un gateway virtuale privato, un gateway di transito imposta lo stesso valore per il discriminatore multi-uscita (MED) in tutti i tunnel di un allegato VPN. Se si esegue la migrazione da un gateway virtuale privato a un gateway di transito e si fa affidamento sul valore MED per la selezione del tunnel, si consiglia di apportare modifiche al routing per evitare problemi di connessione. Ad esempio, puoi pubblicizzare percorsi più specifici sul tuo gateway di transito. Per ulteriori informazioni, consulta Tabelle di routing e priorità della route VPN.

Fase 6: aggiornamento dell'ASN del gateway del cliente (condizionale)

Quando l'ASN del nuovo gateway è diverso dall'ASN del vecchio gateway, è necessario aggiornare l'ASN sul dispositivo gateway del cliente in modo che faccia riferimento al nuovo ASN. Per ulteriori informazioni, consulta Opzioni di gateway del cliente per la connessione Site-to-Site VPN.

Modifica delle opzioni di connessione VPN site-to-site

Puoi modificare le opzioni per la connessione Site-to-Site VPN. È possibile modificare le seguenti opzioni:

- Il CIDR IPv4 varia sul lato locale (gateway cliente) e sul lato remoto (AWS) della connessione VPN che può comunicare attraverso i tunnel VPN. Il valore predefinito è `0.0.0.0/0` per entrambi gli intervalli.
- Il CIDR IPv6 varia sul lato locale (gateway cliente) e remoto (AWS) della connessione VPN che può comunicare attraverso i tunnel VPN. Il valore predefinito è `::/0` per entrambi gli intervalli.

Quando si modificano le opzioni di connessione VPN, gli indirizzi IP dell'endpoint VPN sul lato AWS non cambiano e le opzioni del tunnel non cambiano. La connessione VPN sarà temporaneamente non disponibile per un breve periodo mentre la connessione VPN viene aggiornata.

Per modificare le opzioni di connessione VPN utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione VPN e scegli Operazioni, Modifica le opzioni di connessione VPN.
4. Inserisci i nuovi intervalli CIDR in base alle esigenze.
5. Seleziona Salva modifiche.

Per modificare le opzioni tunnel VPN mediante la riga di comando o l'API

- modify-vpn-connection-options (AWS CLI)
- ModifyVpnConnectionOptions (API della query Amazon EC2)

Modifica delle opzioni del tunnel per Site-to-Site VPN

Puoi modificare le opzioni tunnel per i tunnel VPN nella connessione Site-to-Site VPN. Puoi modificare un tunnel VPN alla volta.

> **Important**
>
> Quando modifichi un tunnel VPN, la connettività sul tunnel viene interrotta per un massimo di alcuni minuti. Assicurati di prevedere il tempo di inattività previsto.

Per modificare le opzioni tunnel VPN mediante la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione VPN site-to-site e scegli Operazioni, Modifica delle opzioni del tunnel VPN.
4. In Indirizzo IP esterno del tunnel VPN, scegli l'IP dell'endpoint del tunnel VPN.
5. Scegli o immetti nuovi valori per le opzioni del tunnel in base alle esigenze. Per ulteriori informazioni, consulta Opzioni per tunnel VPN.
6. Seleziona Salva modifiche.

Per modificare le opzioni tunnel VPN mediante la riga di comando o l'API

- (AWS CLI) Utilizza describe-vpn-connections per visualizzare le opzioni correnti del tunnel e modify-vpn-tunnel-options per modificare le opzioni del tunnel.
- (API della query Amazon EC2) Utilizza DescribeVpnConnections per visualizzare le opzioni di tunnel correnti e ModifyVpnTunnelOptions per modificare le opzioni di tunnel.

Modifica degli instradamenti statici per una connessione VPN site-to-site

Per una connessione VPN Site-to-Site su un gateway virtuale privato configurata per il routing statico, puoi aggiungere o rimuovere i routing statici per la configurazione VPN.

Per aggiungere o rimuovere un instradamento statico mediante la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Selezione di una connessione VPN.
4. Seleziona Modifica instradamenti statici.
5. Aggiunta o rimozione di instradamenti in base alle esigenze.
6. Seleziona Salvataggio delle modifiche.
7. Se la propagazione della route per la tabella di routing non è stata abilitata, occorre aggiornare manualmente le route nella tabella di routing per riflettere i prefissi IP statici aggiornati nella connessione VPN. Per ulteriori informazioni, consulta (Gateway virtuale privato) Abilitazione della propagazione della route nella tabella di routing.
8. Per una connessione VPN su un gateway di transito, aggiungi, modifica o rimuovi gli instradamenti statici nella tabella di routing del gateway di transito. Per ulteriori informazioni, consulta Tebelle di routing del gateway di transito in Gateway di transito di Amazon VPC.

Per aggiungere una route statica utilizzando la riga di comando o l'API

- CreateVpnConnectionRoute(API di interrogazione Amazon EC2)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Per eliminare una route statica utilizzando la riga di comando o l'API

- DeleteVpnConnectionRoute(API di interrogazione Amazon EC2)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Modifica del gateway del cliente per una connessione VPN site-to-site

Puoi modificare il gateway del cliente della tua connessione Site-to-Site VPN utilizzando la console Amazon VPC o uno strumento a riga di comando.

Dopo aver modificato il gateway del cliente, la connessione VPN non sarà temporaneamente disponibile per un breve periodo durante il provisioning dei nuovi endpoint.

Per modificare il gateway del cliente mediante la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Selezione di una connessione VPN.
4. Scegli Operazioni, Modifica la connessione VPN.
5. In Tipo di destinazione, scegli Gateway del cliente.
6. Per Gateway del cliente di destinazione, scegli il nuovo gateway del cliente.
7. Seleziona Salva modifiche.

Per modificare il gateway del cliente utilizzando la riga di comando o l'API

- ModifyVpnConnection (API della query Amazon EC2)
- modify-vpn-connection (AWS CLI)

Sostituzione di credenziali compromesse per la connessione VPN site-to-site

Se ritieni che le credenziali del tunnel per la connessione Site-to-Site VPN siano state compromesse, puoi cambiare la chiave precondivisa IKE o modificare il certificato ACM. Il metodo da usare dipende dall'opzione di autenticazione scelta per i tunnel VPN. Per ulteriori informazioni, consulta Opzioni di autenticazione del tunnel Site-to-Site VPN.

Per modificare la chiave precondivisa IKE

Puoi modificare le opzioni del tunnel per la connessione VPN e specificare una nuova chiave IKE pre-condivisa per ogni tunnel. Per ulteriori informazioni, consulta Modifica delle opzioni del tunnel per Site-to-Site VPN.

In alternativa, puoi eliminare la connessione VPN. Per ulteriori informazioni, consulta Eliminazione di una connessione VPN. Non è necessario eliminare il VPC o il gateway virtuale privato. A questo punto, crea una nuova connessione VPN usando lo stesso gateway privato virtuale e configura le nuove chiavi sul dispositivo gateway del cliente. Puoi specificare le chiavi precondivise per i tunnel, o lasciare che AWS generi per te le nuove chiavi precondivise. Per ulteriori informazioni, consulta Create a VPN connection (Creazione di una connessione VPN). Gli indirizzi interni ed esterni del tunnel potrebbero cambiare quando crei nuovamente la connessione VPN.

Per modificare il certificato per il lato AWS dell'endpoint del tunnel

Ruotare il certificato. Per ulteriori informazioni, consulta Rotazione dei certificati dell'endpoint del tunnel VPN.

Per modificare il certificato sul dispositivo gateway del cliente

1. Creare un nuovo certificato. Per informazioni, consulta Rilascio e gestione dei certificati nella Guida per l'utente di AWS Certificate Manager.
2. Aggiungere il certificato al dispositivo gateway del cliente.

Rotazione dei certificati endpoint del tunnel VPN site-to-site

Puoi ruotare i certificati sugli endpoint del tunnel sul lato AWS utilizzando la console Amazon VPC. Quando il certificato di un endpoint del tunnel sta per scadere, AWS ruota automaticamente il

certificato utilizzando il ruolo collegato al ai servizi. Per ulteriori informazioni, consulta the section called “Ruoli collegati ai servizi”.

Per ruotare il certificato endpoint del tunnel Site-to-Site VPN utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Seleziona la connessione VPN site-to-site, quindi scegli Operazioni, Modifica del certificato del tunnel VPN.
4. Seleziona l'endpoint del tunnel.
5. Seleziona Salva.

Per ruotare il certificato endpoint del tunnel Site-to-Site VPN tramite la AWS CLI

Utilizza il comando modify-vpn-tunnel-certificate .

VPN IP privata con AWS Direct Connect

Con la VPN IP privata, puoi implementare la VPN IPSec AWS Direct Connect, crittografando il traffico tra la tua rete locale e AWS, senza l'uso di indirizzi IP pubblici o apparecchiature VPN aggiuntive di terze parti.

Uno dei principali casi d'uso di Private IP VPN over AWS Direct Connect è aiutare i clienti del settore finanziario, sanitario e federale a raggiungere gli obiettivi normativi e di conformità. Private IP VPN over AWS Direct Connect garantisce che il traffico tra le reti locali AWS e le reti locali sia sicuro e privato, consentendo ai clienti di rispettare i propri mandati normativi e di sicurezza.

Indice

- Creazione di una connessione VPN

Vantaggi della VPN IP privata

- Gestione e operazioni di rete semplificate: senza VPN IP privata, i clienti devono implementare VPN e router di terze parti per implementare VPN private sulle reti. AWS Direct Connect Grazie alla funzionalità VPN IP privata, i clienti non devono implementare e gestire la propria infrastruttura VPN. Ciò comporta operazioni di rete semplificate e costi ridotti.
- Migliore livello di sicurezza: in precedenza, i clienti dovevano utilizzare un'interfaccia AWS Direct Connect virtuale pubblica (VIF) per crittografare il traffico AWS Direct Connect, che richiedeva indirizzi IP pubblici per gli endpoint VPN. L'utilizzo di IP pubblici aumenta la probabilità di attacchi esterni (DOS) che, a loro volta, costringono i clienti a implementare dispositivi di sicurezza aggiuntivi per la protezione della rete. Inoltre, un VIF pubblico consente l'accesso tra tutti i servizi AWS pubblici e le reti locali dei clienti, aumentando la gravità del rischio. La funzionalità VPN IP privata consente la crittografia tramite VIF di AWS Direct Connect transito (anziché VIF pubblici), oltre alla possibilità di configurare IP privati. Ciò fornisce connettività end-to-end privata oltre alla crittografia, migliorando il livello di sicurezza generale.
- Scala di routing più elevata: le connessioni VPN IP private offrono limiti di routing più elevati (5000 rotte in uscita e 1000 rotte in entrata) rispetto alle AWS Direct Connect sole, che attualmente hanno un limite di 200 rotte in uscita e 100 in entrata.

Come funziona la VPN IP privata

La VPN Site-to-Site con IP privato funziona tramite AWS Direct Connect un'interfaccia virtuale di transito (VIF). Usa un gateway AWS Direct Connect e un gateway di transito per collegare le proprie reti locali con VPC AWS . Una connessione VPN IP privata presenta punti di terminazione sul gateway di transito sul AWS lato e sul dispositivo gateway del cliente sul lato locale. È necessario assegnare indirizzi IP privati sia al gateway di transito che all'estremità del dispositivo gateway del cliente dei tunnel IPSec. È possibile utilizzare indirizzi IP privati provenienti da intervalli di indirizzi IPv4 privati RFC1918 o RFC6598.

È possibile collegare una connessione IP VPN privata a un gateway di transito. È quindi possibile instradare il traffico tra l'allegato VPN e tutti i VPC (o altre reti) collegati anche al gateway di transito, associando una tabella di instradamento all'allegato VPN. Nella direzione inversa, puoi instradare il traffico dai tuoi VPC all'allegato VPN IP privato utilizzando le tabelle di instradamento associate ai VPC.

La tabella di routing associata all'allegato VPN può essere uguale o diversa da quella associata all'allegato sottostante. AWS Direct Connect In questo modo è possibile instradare contemporaneamente il traffico crittografato e non crittografato tra i VPC e le proprie reti on-premise.

Per maggiori dettagli sul percorso del traffico in uscita dalla VPN, consulta le politiche di routing dell'interfaccia virtuale privata e dell'interfaccia virtuale di transito nella Guida per l'AWS Direct Connect utente.

Prerequisiti

Per completare la configurazione di una VPN IP privata su AWS Direct Connect sono necessarie le seguenti risorse:

- Una AWS Direct Connect connessione tra la rete locale e AWS
- Un AWS Direct Connect gateway associato al gateway di transito appropriato
- Un gateway di transito con un blocco CIDR IP privato disponibile
- Un dispositivo gateway del cliente nella rete on-premise e un gateway del cliente AWS corrispondente

Crea il gateway del cliente

Un Customer Gateway è una risorsa in cui crei AWS. Rappresenta il dispositivo gateway del cliente nella rete on-premise. Quando crei un customer gateway, fornisci informazioni sul tuo dispositivo a AWS. Per ulteriori dettagli, consulta Gateway del cliente.

Per creare un gateway del cliente utilizzando la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Gateway del cliente.
3. Scegli Crea gateway del cliente.
4. (Facoltativo) In Name (Nome), inserire un nome per il gateway del cliente. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
5. In BGP ASN, inserire un Border Gateway Protocol (BGP) Autonomous System Number (ASN) del gateway del cliente.
6. Per Indirizzo IP, immettere l'indirizzo IP privato del dispositivo gateway del cliente.
7. (Opzionale) Per Device (Dispositivo), inserire un nome per il dispositivo che ospita questo gateway del cliente.

8. Scegli Crea gateway del cliente.

Per creare un gateway del cliente utilizzando l'API o la riga di comando

- CreateCustomerGateway (API di interrogazione Amazon EC2)
- create-customer-gateway (AWS CLI)

Preparazione del gateway di transito

Un Transit Gateway è un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti locali. È possibile creare un nuovo gateway di transito o utilizzarne uno esistente per la connessione VPN IP privata. Quando si crea il gateway di transito o si modifica un gateway di transito esistente, si specifica un blocco CIDR IP privato per la connessione.

> **Note**
>
> Quando si specifica il blocco CIDR del gateway di transito da associare alla VPN IP privata, assicurarsi che il blocco CIDR non si sovrapponga a nessun indirizzo IP per altri allegati di rete sul gateway di transito. Se alcuni blocchi IP CIDR si sovrappongono, potrebbero causare problemi di configurazione con il dispositivo gateway del cliente.

Per i passaggi specifici AWS della console per creare o modificare un gateway di transito da utilizzare per la VPN IP privata, consulta Transit gateway nella Amazon VPC Transit Gateways Guide.

Per creare un gateway di transito utilizzando l'API o la riga di comando

- CreateTransitGateway (API di interrogazione Amazon EC2)
- create-transit-gateway (AWS CLI)

Crea il gateway AWS Direct Connect

Crea un AWS Direct Connect gateway seguendo la procedura Creating a Direct Connect gateway nella Guida AWS Direct Connect per l'utente.

Per creare un AWS Direct Connect gateway utilizzando la riga di comando o l'API

- CreateDirectConnectGateway(API di AWS Direct Connect interrogazione)

- create-direct-connect-gateway (AWS CLI)

Creazione dell'associazione del gateway di transito

Dopo aver creato il AWS Direct Connect gateway, crea un'associazione di gateway di transito per il AWS Direct Connect gateway. Specificare il CIDR IP privato per il gateway di transito identificato in precedenza nell'elenco dei prefissi consentiti.

Per ulteriori informazioni, consulta Associazioni del gateway di transito nella Guida per l'utente di AWS Direct Connect .

Per creare un'associazione AWS Direct Connect gateway utilizzando la riga di comando o l'API

- CreateDirectConnectGatewayAssociazione (AWS Direct Connect Query API)
- create-direct-connect-gateway-association (AWS CLI)

Creazione di una connessione VPN

Creazione di una connessione VPN site-to-site utilizzando indirizzi IP privati

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Connessioni VPN site-to-site.
3. Scegli Create VPN Connection (Crea connessione VPN).
4. (Facoltativo) Per Name tag (Tag del nome) immetti un nome per la connessione Site-to-Site VPN. In questo modo viene creato un tag con una chiave di `Name` e il valore specificato.
5. Per Tipo di gateway di destinazione, scegli Gateway di transito. Quindi, scegli il gateway di transito identificato in precedenza.
6. Per Gateway del cliente, seleziona Esistente. Quindi, scegli il gateway del cliente creato in precedenza.
7. Selezionare una delle opzioni di routing a seconda che il dispositivo gateway del cliente supporti Border Gateway Protocol (BGP):
   - Se il dispositivo gateway del cliente supporta BGP, scegliere Dynamic (requires BGP) (Dinamico (richiede BGP)).
   - Se il dispositivo gateway del cliente non supporta BGP, scegliere Static (Statico).

8. Per Tunnel all'interno della versione IP, specifica se i tunnel VPN supportano il traffico IPv4 o IPv6.
9. (Facoltativo) Se hai specificato IPv4 per Tunnel inside IP Version, puoi facoltativamente specificare gli intervalli CIDR IPv4 per il gateway e AWS i lati del cliente autorizzati a comunicare tramite i tunnel VPN. Il valore predefinito è `0.0.0.0/0`.

   Se hai specificato IPv6 per la versione IP di Tunnel inside, puoi facoltativamente specificare gli intervalli CIDR IPv6 per il gateway e i lati del cliente autorizzati a comunicare tramite i tunnel VPN. AWS Il valore predefinito per entrambi gli intervalli è `::/0`.
10. Per Tipo di indirizzo IP esterno, scegli 4. PrivateIpv
11. Per Transport attachment ID, scegliete l'allegato del gateway di transito per il AWS Direct Connect gateway appropriato.
12. Scegliere Create VPN Connection (Crea connessione VPN).

> **Note**
>
> L’opzione Abilita accelerazione non è applicabile per le connessioni VPN su AWS Direct Connect.

Sicurezza nella VPN da AWS sito a sito

La sicurezza del cloud è la massima priorità. AWS In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano alla AWS VPN da sito a sito, AWS consulta Servizi nell'ambito del programma di conformità Servizi nell'ambito di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione facilita la comprensione dell'applicazione del modello di responsabilità condivisa quando si usa Site-to-Site VPN. I seguenti argomenti illustrano come configurare Site-to-Site VPN per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse VPN da sito a sito.

Indice

Protezione dei dati nella VPN da AWS sito a sito

Il modello di responsabilità AWS condivisa Modello di si applica alla protezione dei dati nella AWS VPN Site-to-Site. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutte le. Cloud AWS L'utente è responsabile del controllo

dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con una VPN da sito a sito o Servizi AWS altro utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Riservatezza del traffico Internet

Una connessione Site-to-Site VPN connette privatamente il VPC alla rete in locale. I dati trasferiti tra il VPC e la rete vengono instradati su una connessione VPN crittografata per proteggere la riservatezza e l'integrità dei dati in transito. Amazon supporta le connessioni VPN IPsec (Internet

Protocol security). IPsec è una suite di protocolli per la protezione delle comunicazioni IP mediante l'autenticazione e la crittografia dei singoli pacchetti IP in un flusso di dati.

Ogni connessione VPN da sito a sito è costituita da due tunnel VPN IPSec crittografati che collegano e collegano la rete. AWS Il traffico in ogni tunnel può essere crittografato con AES128 o AES256 e può utilizzare gruppi Diffie-Hellman per lo scambio delle chiavi, per fornire Perfect Forward Secrecy. AWS autentica con le funzioni hash SHA1 o SHA2.

Le istanze nel VPC non richiedono un indirizzo IP pubblico per connettersi alle risorse sul lato opposto della connessione Site-to-Site VPN. Le istanze possono instradare il traffico Internet attraverso la connessione Site-to-Site VPN alla rete locale. Possono quindi accedere a Internet tramite i punti di traffico in uscita esistenti e i dispositivi di sicurezza e monitoraggio della rete.

Per ulteriori informazioni, consultare i seguenti argomenti:

- Opzioni di tunnel per la connessione Site-to-Site VPN: fornisce informazioni sulle opzioni IPsec e IKE (Internet Key Exchange) disponibili per ogni tunnel.
- Opzioni di autenticazione del tunnel Site-to-Site VPN: fornisce informazioni sulle opzioni di autenticazione per gli endpoint del tunnel VPN.
- Requisiti per il dispositivo gateway del cliente: fornisce informazioni sui requisiti per il dispositivo gateway del cliente sul lato utente della connessione VPN.
- Fornire una comunicazione sicura tra siti utilizzando VPN CloudHub: Se disponi di più connessioni VPN da sito a sito, puoi fornire comunicazioni sicure tra i tuoi siti locali utilizzando la VPN. AWS CloudHub

Gestione delle identità e degli accessi per VPN da AWS sito a sito

AWS Identity and Access Management (IAM) è una soluzione Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (chi ha effettuato l'accesso) e autorizzato (chi dispone di autorizzazioni) a utilizzare le risorse. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità

- Gestione dell'accesso con policy
- Come funziona la AWS VPN da sito a sito con IAM
- Esempi di policy basate sull'identità per VPN da sito a sito AWS
- Risoluzione dei problemi relativi AWS all'identità e all'accesso alla VPN da sito a sito
- Ruolo collegato ai servizi di Site-to-Site VPN

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto nella VPN da sito a sito.

Utente del servizio: se utilizzi il servizio Cognito per eseguire il tuo lavoro, l'amministratore ti fornirà le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Site-to-Site VPN, consulta Risoluzione dei problemi relativi AWS all'identità e all'accesso alla VPN da sito a sito.

Amministratore del servizio: se sei il responsabile delle risorse presso la tua azienda, probabilmente disponi dell'accesso completo a . Il tuo compito è determinare le caratteristiche e le risorse Site-to-Site VPN a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con , consulta Come funziona la AWS VPN da sito a sito con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a . Per visualizzare policy basate su identità di di esempio che puoi utilizzare in IAM, consulta Esempi di policy basate sull'identità per VPN da sito a sito AWS.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se

accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione

`iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona la AWS VPN da sito a sito con IAM

Prima di utilizzare IAM per gestire l'accesso a Site-to-Site VPN, scopri quali funzionalità di IAM sono disponibili per l'uso con Site-to-Site VPN.

Funzionalità IAM che puoi utilizzare con la VPN da AWS sito a sito

Funzionalità IAM	Supporto di Site-to-Site VPN
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come la VPN Site-to-Site AWS e gli altri servizi funzionano con la maggior parte delle funzionalità IAM AWS , consulta i servizi che funzionano con IAM nella IAM User Guide.

Policy per Site-to-Site VPN basate su identità

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di criteri basate su identità di Site-to-Site VPN

Per visualizzare esempi di policy basate su identità Site-to-Site VPN, consulta Esempi di policy basate sull'identità per VPN da sito a sito AWS.

Policy basate sulle risorse all'interno di Site-to-Site VPN

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste

ulteriori policy basate su identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Azioni di policy di Site-to-Site VPN

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni VPN da sito a sito, consulta Azioni definite da VPN da sito a sito nel riferimento sull'autorizzazione AWS del servizio.

Le operazioni delle policy in utilizzano il seguente prefisso prima dell'operazione:

```
ec2
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Per visualizzare esempi di policy basate su identità Site-to-Site VPN, consulta Esempi di policy basate sull'identità per VPN da sito a sito AWS.

Risorse di policy per Site-to-Site VPN

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse VPN da sito a sito e dei relativi ARN, consulta Risorse definite dalla VPN da sito a sito nel Service Authorization AWS Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta Azioni definite dalla VPN da AWS Site-to-Site.

Per visualizzare esempi di policy basate su identità Site-to-Site VPN, consulta .Esempi di policy basate sull'identità per VPN da sito a sito AWS

Chiavi di Site-to-Site VPN

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali

che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di condizione VPN da sito a sito, consulta Chiavi di condizione per VPN da sito a sito nel riferimento di autorizzazione del AWS servizio. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni definite dalla AWS VPN da Site-to-Site.

Per visualizzare esempi di policy basate su identità Site-to-Site VPN, consulta Esempi di policy basate sull'identità per VPN da sito a sito AWS.

ACM nella Site-to-Site VPN

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Site-to-Site VPN

Supporta ABAC (tag nelle policy)	No

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Identity and Access Management con Site-to-Site VPN

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni di Site-to-Site VPN

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli collegati ai servizi per Site-to-Site VPN

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di Site-to-Site VPN. Modificare i ruoli del servizio solo quando Site-to-Site VPN fornisce le indicazioni per farlo.

Ruolo collegato ai servizi Site-to-Site VPN

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per VPN da sito a sito AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Site-to-Site VPN. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface () o l'API.AWS CLI AWS Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Site-to-Site VPN, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per la VPN da sito a sito nel Service Authorization AWS Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Site-to-Site VPN
- Descrivi connessioni VPN da sito a sito specifiche
- Crea e descrivi le risorse necessarie per una connessione AWS Site-to-Site VPN

Best practice per le policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse Site-to-Site VPN nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Site-to-Site VPN

Per accedere alla console AWS VPN da sito a sito, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse VPN Site-to-Site presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso o l'API. AWS CLI AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la console VPN da sito a sito, collega anche la VPN da sito a sito o la policy gestita alle entità. `AmazonVPCFullAccess` `AmazonVPCReadOnlyAccess` AWS Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Descrivi connessioni VPN da sito a sito specifiche

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": [
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-04d5cc9b88example",
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-903004f88example"
         ]
      }
   ]
}
```

Crea e descrivi le risorse necessarie per una connessione AWS Site-to-Site VPN

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
         "ec2:DescribeVpnConnections",
         "ec2:DescribeVpnGateways",
         "ec2:DescribeCustomerGateways",
         "ec2:CreateCustomerGateway",
         "ec2:CreateVpnGateway",
         "ec2:CreateVpnConnection"
         ],
         "Resource": [
            "*"
         ]
      },
   {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"s2svpn.amazonaws.com"
            }
         }
      }
   ]
}
```

Risoluzione dei problemi relativi AWS all'identità e all'accesso alla VPN da sito a sito

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di e di IAM.

Argomenti

- Non sono autorizzato a eseguire un'operazione in Site-to-Site VPN
- Non sono autorizzato a eseguire iam: PassRole

- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse VPN da sito a sito

Non sono autorizzato a eseguire un'operazione in Site-to-Site VPN

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `ec2:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `ec2:`*`GetWidget`*.

Se hai bisogno di assistenza, contatta il tuo amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, devi aggiornare le policy per poter passare un ruolo a Lambda.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` prova a utilizzare la console per eseguire un'operazione in Site-to-Site VPN. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse VPN da sito a sito

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Site-to-Site VPN supporta queste funzionalità, consulta Come funziona la AWS VPN da sito a sito con IAM.
- Per scoprire come fornire l'accesso alle tue risorse su Account AWS risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Ruolo collegato ai servizi di Site-to-Site VPN

AWS La VPN da sito a sito AWS Identity and Access Management utilizza ruoli collegati ai servizi (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a un Site-to-Site VPN. I ruoli collegati ai servizi sono predefiniti dalla VPN Site-to-Site e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione di Site-to-Site VPN perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Site-to-Site VPN definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo potrà assumere i

propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni del ruolo collegato ai servizi di Site-to-Site VPN

La VPN da sito a sito utilizza il ruolo collegato al servizio denominato AWSServiceRoleForVPCS2SVPN: Consenti alla VPN da sito a sito di creare e gestire risorse relative alle tue connessioni VPN.

Il ruolo AWSServiceRoleForVPCS2SVPN collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `AWS Certificate Manager`
- `AWS Private Certificate Authority`

La politica di autorizzazione dei ruoli denominata AWSVPCS2SVpnServiceRolePolicy consente alla VPN da Site-to-Site di completare le seguenti azioni sulle risorse specificate:

- Operazione: `acm:ExportCertificate` su `Resource: "*"`
- Operazione: `acm:DescribeCertificate` su `Resource: "*"`
- Operazione: `acm:ListCertificates` su `Resource: "*"`
- Operazione: `acm-pca:DescribeCertificateAuthority` su `Resource: "*"`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Site-to-Site VPN

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un gateway per i clienti con un certificato privato ACM associato nella AWS Management Console, o nell' AWS API AWS CLI, Site-to-Site VPN crea il ruolo collegato al servizio per te.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Site-to-Site VPN crea questo ruolo automaticamente quando crei un gateway del cliente con un certificato privato ACM associato.

Ruolo collegato ai servizi di AWS Site-to-Site VPN

La VPN da sito a sito non consente di modificare il ruolo collegato al servizio. AWSServiceRoleForVPCS2SVPN Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Site-to-Site VPN

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio Site-to-Site VPN utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse VPN da sito a sito utilizzate da AWSServiceRoleForVPCS2SVPN

Puoi eliminare questo ruolo collegato ai servizi solo dopo aver eliminato tutti i gateway del cliente che dispongono di un certificato privato ACM associato. Questo impedisce di rimuovere inavvertitamente l'autorizzazione per accedere ai certificati ACM in uso dalle connessioni Site-to-Site VPN.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForVPCS2SVPN servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Resilienza in AWS Site-to-Site VPN

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Oltre all'infrastruttura AWS globale, la VPN da sito a sito offre funzionalità che aiutano a supportare la resilienza dei dati e le esigenze di backup.

Due tunnel per connessione VPN

Una connessione VPN Site-to-Site è costituita da due tunnel, ciascuno terminato in una zona di disponibilità diversa, per fornire una maggiore disponibilità al VPC. Se si verifica un guasto del dispositivo interno AWS, la connessione VPN passa automaticamente al secondo tunnel in modo che l'accesso non venga interrotto. Di tanto in tanto, esegue AWS anche la manutenzione ordinaria della connessione VPN, che può disabilitare brevemente uno dei due tunnel della connessione VPN. Per ulteriori informazioni, consulta Sostituzioni degli endpoint del tunnel Site-to-Site VPN. Durante la configurazione del gateway del cliente, è pertanto importante configurare Entrambi i tunnel.

Ridondanza

Per proteggere da una perdita di connettività nel caso il gateway del cliente diventi non disponibile, puoi configurare una seconda connessione Site-to-Site VPN. Per ulteriori informazioni, consulta la seguente documentazione :

- Utilizzo di connessioni Site-to-Site VPN ridondanti per fornire il failover
- Opzioni di connettività di Amazon Virtual Private Cloud
- Creazione di un'infrastruttura di rete AWS multi-VPC scalabile e sicura

Sicurezza dell'infrastruttura nella VPN da AWS sito a sito

In quanto servizio gestito, la AWS VPN da sito a sito è protetta dalla sicurezza di rete globale. AWS Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere alla VPN da sito a sito attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Monitoraggio della connessione Site-to-Site VPN

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni della AWS Site-to-Site VPN connessione. È necessario raccogliere i dati sul monitoraggio da tutte le parti della soluzione per consentire un debug più facile di eventuali guasti in più punti. Tuttavia, prima di iniziare il monitoraggio della connessione Site-to-Site VPN, è opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

La fase successiva consiste nello stabilire una baseline per le prestazioni normali di VPN nell'ambiente, misurando le prestazioni in diversi momenti e con condizioni di carico differenti. Durante il monitoraggio della VPN, archivia i dati di monitoraggio storici per poterli confrontare con i dati sulle prestazioni correnti, per poter identificare i modelli di prestazioni normali e le anomalie E ideare metodi per risolvere i problemi.

Per stabilire una baseline, devi monitorare gli elementi seguenti:

- Lo stato dei tunnel VPN
- I dati in entrata nel tunnel
- I dati in uscita dal tunnel

Indice

Strumenti di monitoraggio

AWS fornisce diversi strumenti che è possibile utilizzare per monitorare una connessione VPN da sito a sito. Alcuni di questi strumenti possono essere configurati in modo che eseguano automaticamente il monitoraggio, mentre altri richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Strumenti di monitoraggio automatici

Per controllare una connessione Site-to-Site VPN e segnalare Eventuali problemi, puoi usare gli strumenti di monitoraggio automatici seguenti:

- Amazon CloudWatch Alarms: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica rispetto a una determinata soglia in diversi periodi di tempo. L'azione è una notifica inviata a un argomento di Amazon SNS. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per ulteriori informazioni, consulta Monitoraggio dei tunnel VPN tramite Amazon CloudWatch.
- AWS CloudTrail Monitoraggio dei log: condividi i file di CloudTrail registro tra account, monitora i file di registro in tempo reale inviandoli a CloudWatch Logs, scrivi applicazioni di elaborazione dei log in Java e verifica che i file di registro non siano cambiati dopo la consegna da parte di. CloudTrail Per ulteriori informazioni, consulta Logging API Calls Using AWS CloudTrail in Amazon EC2 API Reference e Working CloudTrail with log files nella Guida per AWS CloudTrail l'utente.
- AWS Health eventi: ricevi avvisi e notifiche relativi a cambiamenti nello stato dei tunnel VPN da sito a sito, consigli di configurazione basati sulle best practice o quando ti avvicini ai limiti di scalabilità. Utilizza gli eventi in Personal Health Dashboard per attivare i failover automatizzati, ridurre i tempi di risoluzione dei problemi o ottimizzare le connessioni per un'elevata disponibilità. Per ulteriori informazioni, consulta Monitoraggio delle connessioni VPN tramite eventi AWS Health.

Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio di una connessione VPN da sito a sito consiste nel monitorare manualmente gli elementi che CloudWatch gli allarmi non coprono. Le dashboard di Amazon VPC e CloudWatch console forniscono una at-a-glance visione dello stato del tuo ambiente. AWS

> **Note**
>
> Nella console Amazon VPC, i parametri di stato del tunnel VPN da sito a sito, come «Status» e «Last status change», potrebbero non riflettere cambiamenti di stato transitori o flap momentanei del tunnel. Si consiglia di utilizzare CloudWatch metriche e log per gli aggiornamenti granulari sulle modifiche dello stato del tunnel.

- Nel pannello di controllo di Amazon VPC sono visualizzate le seguenti informazioni:
  - Stato dei servizi per regione
  - Connessioni Site-to-Site VPN
  - Lo stato dei tunnel VPN. Nel riquadro di navigazione, scegli Site-to-Site VPN Connections (Connessioni VPN site-to-site), seleziona una connessione Site-to-Site VPN, quindi seleziona Tunnel Details (Dettagli tunnel).
- La CloudWatch home page mostra:
  - Stato e allarmi attuali
  - Grafici degli allarmi e delle risorse
  - Stato di integrità dei servizi

  Inoltre, è possibile utilizzare CloudWatch per effettuare le seguenti operazioni:
  - Crea pannelli di controllo personalizzati per monitorare i servizi di interesse.
  - Crea grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
  - Cerca e sfoglia tutte le metriche AWS delle tue risorse
  - Crea e modifica gli allarmi per ricevere le notifiche dei problemi.

AWS Site-to-Site VPN registri

AWS Site-to-Site VPN i log ti offrono una visibilità più approfondita sulle tue implementazioni VPN da sito a sito. Con questa caratteristica è possibile accedere ai registri di connessione VPN sito-sito che forniscono i dettagli relativi alla creazione del tunnel IP Security (IPSec), le negoziazioni Internet Key Exchange (IKE) e i messaggi di protocollo Dead Peer Detection (DPD).

I log VPN da sito a sito possono essere pubblicati su Amazon Logs. CloudWatch Questa caratteristica offre ai clienti un modo coerente per accedere e analizzare i registri dettagliati per tutte le connessioni VPN sito-sito.

Indice

Vantaggi dei registri VPN sito-sito

- Risoluzione dei problemi VPN semplificata: i log VPN da sito a sito aiutano a individuare le AWS discrepanze di configurazione tra il dispositivo gateway del cliente e a risolvere i problemi iniziali di connettività VPN. Le connessioni VPN possono funzionare in modo intermittente a causa della configurazione errata delle impostazioni (ad esempio timeout mal regolati), possono verificarsi problemi nelle reti di trasporto sottostanti (come il meteo Internet) o modifiche di routing o errori di percorso possono causare l'interruzione della connettività su VPN. Questa caratteristica consente di diagnosticare con precisione la causa degli errori di connessione intermittente e di mettere a punto la configurazione del tunnel di basso livello per un funzionamento affidabile.
- AWS Site-to-Site VPN Visibilità centralizzata: i log VPN da sito a sito possono fornire registri delle attività del tunnel per tutti i diversi modi in cui la VPN Site-to-Site è connessa: Virtual Gateway, Transit Gateway e, utilizzando sia Internet che come mezzo di trasporto. CloudHub AWS Direct Connect Questa caratteristica offre ai clienti un modo coerente per accedere e analizzare i registri dettagliati per tutte le connessioni VPN sito-sito.
- Sicurezza e conformità: i log VPN da sito a sito possono essere inviati ad CloudWatch Amazon Logs per un'analisi retrospettiva dello stato e dell'attività della connessione VPN nel tempo. Ciò consente di soddisfare i requisiti normativi e di conformità.

Restrizioni sulle dimensioni delle politiche relative alle risorse di Amazon CloudWatch Logs

CloudWatch Le politiche relative alle risorse di Logs sono limitate a 5120 caratteri. Quando CloudWatch Logs rileva che una policy si avvicina a questo limite di dimensione, abilita

automaticamente i gruppi di log che iniziano con. `/aws/vendedlogs/` Quando abiliti la registrazione, la VPN da Site-to-Site deve CloudWatch aggiornare la politica delle risorse Logs con il gruppo di log specificato. Per evitare di raggiungere il limite di dimensione della politica delle risorse CloudWatch Logs, inserisci come prefisso i nomi dei gruppi di log con. `/aws/vendedlogs/`

Contenuti dei registri VPN sito-sito

Le informazioni che seguono sono incluse nel registro delle attività del tunnel VPN sito-sito.

Campo	Descrizione
VpnLogCreationTimestamp	Timestamp di creazione del registro in formato leggibile dall'utente.
VpnConnectionId	L'identificatore di connessione VPN.
TunnelOutsideIndirizzo IP	L'IP esterno del tunnel VPN che ha generato la voce di registro.
TunnelDPDEnabled	Stato abilitato del protocollo Dead Peer Detection (True/False).
Tunnel CGW Natt DetectionStatus	NAT-T rilevato sul dispositivo gateway del cliente (True/False).
TunnelIKEPhase1State	Stato del protocollo IKE Fase 1 (Established | Rekeying | Negotiating | Down).
TunnelIKEPhase2State	Stato del protocollo IKE Fase 2 (Established | Rekeying | Negotiating | Down).
VpnLogDettaglio	Messaggi dettagliati per i protocolli IPSec, IKE e DPD.

Indice

Messaggi di errore IKEv1

Messaggio	Spiegazione
Il peer non risponde - Dichiarazione di peer morto	Peer non ha risposto ai messaggi DPD, imponendo un'azione di timeout DPD.
AWS la decrittografia del payload del tunnel non è riuscita a causa di una chiave precondiv isa non valida	La stessa chiave precondivisa deve essere configurata su entrambi i peer IKE.
Nessuna proposta corrispondente trovata da AWS	Gli attributi proposti per Fase 1 (crittografia, hashing e gruppo DH) non sono supportati da AWS VPN Endpoint, ad esempio 3DES
Nessuna corrispondenza proposta trovata. Notifica con "Nessuna proposta scelta"	Nessun messaggio di errore Proposta scelta viene scambiato tra peer per informare che è necessario configurare proposte/policy corrette per la fase 2 su IKE Peers.
AWS tunnel ha ricevuto DELETE per Phase 2 SA con SPI: xxxx	CGW ha inviato il messaggio Delete_SA per Fase 2
AWS tunnel ha ricevuto DELETE per IKE_SA da CGW	CGW ha inviato il messaggio Delete_SA per Fase 1

Messaggi di errore IKEv2

Messaggio	Spiegazione
AWS il tunnel DPD è scaduto dopo la ritrasmis sione di {retry_count}	Peer non ha risposto ai messaggi DPD, imponendo un'azione di timeout DPD.
AWS tunnel ha ricevuto DELETE per IKE_SA da CGW	Peer ha inviato il messaggio Delete_SA per Parent/IKE_SA
AWS tunnel ha ricevuto DELETE per Phase 2 SA con SPI: xxxx	Peer ha inviato il messaggio Delete_SA per CHILD_SA

Messaggio	Spiegazione
AWS il tunnel ha rilevato una collisione (CHILD_REKEY) come CHILD_DELETE	CGW ha inviato il messaggio Delete_SA per Active SA, che è in corso di identificazione.
AWS tunnel (CHILD_SA) una SA ridondante viene eliminata a causa della collisione rilevata	A causa della collisione, se vengono generati SA ridondanti, i peer chiuderanno SA ridondanti dopo aver abbinato i valori nonce come da RFC
AWS la Fase 2 del tunnel non è stata in grado di stabilire mantenendo la Fase 1	Peer non è stato in grado di stabilire CHILD_SA a causa di un errore di negoziazione, ad esempio proposta errata.
AWS: Selettore di traffico: TS_UNACCE TTABLE: ricevuto dal risponditore	Peer ha proposto selettori di traffico/dominio di crittografia errati. I peer devono essere configurati con CIDR identici e corretti.
AWS tunnel sta inviando AUTHENTIC ATION_FAILED come risposta	Il peer non è in grado di autenticare il peer verificando il contenuto del messaggio IKE_AUTH
AWS tunnel ha rilevato una mancata corrispon denza della chiave precondivisa con cgw: xxxx	La stessa chiave precondivisa deve essere configurata su entrambi i peer IKE.
AWS tunnel Timeout: eliminazione della fase 1 non stabilita IKE_SA con cgw: xxxx	L'eliminazione dell'IKE_SA semiaperto come peer non ha portato a termine le negoziazioni
Nessuna corrispondenza proposta trovata. Notifica con "Nessuna proposta scelta"	Nessun messaggio di errore Proposta scelta viene scambiato tra peer per informare che è necessario configurare proposte corrette su IKE Peers.
Nessuna proposta corrispondente trovata da AWS	Gli attributi proposti per la Fase 1 (Encryption, Hashing e DH Group) non sono supportati da AWS VPN Endpoint. ad esempio 3DES

Messaggi di negoziazione IKEv2

Messaggio	Spiegazione
AWS richiesta elaborata dal tunnel (id=xxx) per CREATE_CHILD_SA	AWS ha ricevuto la richiesta CREATE_CHILD_SA da CGW
AWS il tunnel sta inviando una risposta (id=xxx) per CREATE_CHILD_SA	AWS sta inviando la risposta CREATE_CHILD_SA a CGW
AWS il tunnel sta inviando una richiesta (id=xxx) per CREATE_CHILD_SA	AWS sta inviando la richiesta CREATE_CHILD_SA a CGW
AWS risposta elaborata dal tunnel (id=xxx) per CREATE_CHILD_SA	AWS ha ricevuto la risposta CREATE_CHILD_SA da CGW

Requisiti IAM per la pubblicazione nei CloudWatch registri

Affinché la funzionalità di registrazione funzioni correttamente, la policy IAM collegata al principale IAM utilizzata per configurare la funzionalità deve includere almeno le seguenti autorizzazioni. Ulteriori dettagli sono disponibili anche nella sezione Abilitazione della registrazione da determinati AWS servizi della Amazon CloudWatch Logs User Guide.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
```

```
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Visualizzazione della configurazione dei registri VPN sito-sito

Per visualizzare le impostazioni di registrazione correnti del tunnel

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Site-to-Site VPN Connections (Connessioni VPN site-to-site).
3. Selezionare la connessione VPN da visualizzare dall'elenco VPN connections (Connessioni VPN).
4. Selezionare la scheda Tunnel details (Dettagli tunnel).
5. Espandere le sezioni Tunnel 1 options (Opzioni tunnel 1) e Tunnel 2 options (Opzioni tunnel 2) per visualizzare tutti i dettagli della configurazione dei tunnel.
6. Puoi visualizzare lo stato attuale della funzionalità di registrazione nel registro di Tunnel VPN e il gruppo di log attualmente configurato (se presenteCloudWatch) nel gruppo di CloudWatch log.

Per visualizzare le impostazioni correnti di registrazione del tunnel su una connessione VPN da sito a sito utilizzando la riga di comando o l'API AWS

- DescribeVpnConnessioni (Amazon EC2 Query API)
- describe-vpn-connections (AWS CLI)

Abilitazione dei registri VPN sito-sito

> **Note**
>
> Quando abiliti i registri VPN sito-sito per un tunnel di connessione VPN esistente, la connettività su quel tunnel può essere interrotta per diversi minuti. Tuttavia, ogni connessione VPN offre due tunnel per la disponibilità elevata, in modo da poter abilitare la registrazione su un tunnel alla volta mantenendo inalterata la connettività sul tunnel. Per ulteriori informazioni, consulta Sostituzioni degli endpoint del tunnel Site-to-Site VPN.

Per abilitare la registrazione VPN durante la creazione di una nuova connessione VPN sito-sito

Seguire la procedura Fase 5: creazione di una connessione VPN. Durante la fase 9, Tunnel Options (Opzioni tunnel), è possibile specificare tutte le opzioni che si desidera utilizzare per entrambi i tunnel, tra cui le opzioni VPN logging (Registrazione VPN). Per ulteriori informazioni su queste opzioni, consulta Opzioni di tunnel per la connessione Site-to-Site VPN.

Per abilitare la registrazione del tunnel su una nuova connessione VPN da sito a sito utilizzando la riga di comando o l'API AWS

- CreateVpnConnessione (API di interrogazione Amazon EC2)
- create-vpn-connection (AWS CLI)

Per abilitare la registrazione del tunnel su una connessione VPN sito-sito

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Site-to-Site VPN Connections (Connessioni VPN site-to-site).
3. Selezionare la connessione VPN da modificare dall'elenco VPN connections (Connessioni VPN).
4. Selezionare Actions (Operazioni), Modify VPN tunnel options (Modifica opzioni tunnel VPN).
5. Selezionare il tunnel che si desidera modificare scegliendo l'indirizzo IP appropriato dall'elenco VPN tunnel outside IP address (Tunnel VPN esterno all'indirizzo IP).
6. In Tunnel activity log (Registro attività tunnel), selezionare Enable (Abilita).
7. In Amazon CloudWatch log group, seleziona il gruppo di CloudWatch log Amazon a cui desideri inviare i log.

8. (Facoltativo): in Output format (Formato di output), scegliere il formato desiderato per l'output del registro, json o testo.
9. Selezionare Save changes (Salva modifiche).
10. (Facoltativo): ripetere le fasi da 4 a 9 per l'altro tunnel, se lo si desidera.

Per abilitare la registrazione del tunnel su una connessione VPN Site-to-Site esistente utilizzando la riga di comando o l'API AWS

- ModifyVpnTunnelOptions(API di interrogazione Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Disabilitazione dei registri VPN sito-sito

Per disabilitare la registrazione del tunnel su una connessione VPN sito-sito

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione scegli Site-to-Site VPN Connections (Connessioni VPN site-to-site).
3. Selezionare la connessione VPN da modificare dall'elenco VPN connections (Connessioni VPN).
4. Selezionare Actions (Operazioni), Modify VPN tunnel options (Modifica opzioni tunnel VPN).
5. Selezionare il tunnel che si desidera modificare scegliendo l'indirizzo IP appropriato dall'elenco VPN tunnel outside IP address (Tunnel VPN esterno all'indirizzo IP).
6. In Tunnel activity log (Registro attività tunnel), deselezionare Enable (Abilita).
7. Selezionare Save changes (Salva modifiche).
8. (Facoltativo): ripetere le fasi da 4 a 7 per l'altro tunnel, se lo si desidera.

Per disabilitare la registrazione del tunnel su una connessione VPN da sito a sito utilizzando la riga di comando o l'API AWS

- ModifyVpnTunnelOptions(API di interrogazione Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Monitoraggio dei tunnel VPN tramite Amazon CloudWatch

Puoi monitorare i tunnel VPN utilizzando CloudWatch, che raccoglie ed elabora i dati grezzi del servizio VPN in metriche leggibili e quasi in tempo reale. Queste statistiche vengono registrate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web. I dati metrici della VPN vengono inviati automaticamente non appena diventano disponibili. CloudWatch

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Indice

Parametri e dimensioni VPN

Le seguenti CloudWatch metriche sono disponibili per le connessioni VPN da sito a sito.

Parametro	Descrizione
`TunnelState`	Lo stato dei tunnel. Per le VPN statiche, 0 indica DOWN e 1 indica UP. Per le VPN BGP, 1 indica ESTABLISHED e 0 viene utilizzato per tutti gli altri stati. Per entrambi i tipi di VPN, i valori compresi tra 0 e 1 indicano che almeno un tunnel non è UP. Unità: valore frazionario compreso tra 0 e 1
`TunnelDataIn` †	I byte ricevuti sul AWS lato della connessio ne attraverso il tunnel VPN da un gateway del cliente. Ciascun punto dati del parametro rappresenta il numero di byte ricevuti dopo il punto dati precedente. Utilizza la statistica Sum (Somma) per mostrare il numero totale di byte ricevuti durante il periodo.

Parametro	Descrizione
	Questo parametro conta i dati dopo la decrittografia. Unità: byte
`TunnelDataOut` †	I byte inviati dal AWS lato della connessione attraverso il tunnel VPN al gateway del cliente. Ciascun punto dati del parametro rappresenta il numero di byte inviati dopo il punto dati precedente. Utilizza la statistica Sum (Somma) per mostrare il numero totale di byte inviati durante il periodo. Questo parametro conta i dati prima della crittografia. Unità: byte

† Questi parametri possono segnalare l'utilizzo della rete anche quando il tunnel è inattivo. Ciò è dovuto ai controlli periodici dello stato eseguiti sul tunnel e alle richieste ARP e BGP in background.

Per filtrare i dati dei parametri, usa le seguenti dimensioni.

Dimensione	Descrizione
`VpnId`	Filtra i dati dei parametri metriche in base all'ID della connessione Site-to-Site VPN.
`TunnelIpAddress`	Consente di filtrare i dati dei parametri in base all'indirizzo IP del tunnel per il gateway privato virtuale.

Visualizzazione delle metriche VPN CloudWatch

Quando crei una connessione VPN da sito a sito, il servizio VPN invia le metriche sulla tua connessione CloudWatch VPN non appena diventano disponibili. Puoi visualizzare le metriche per le connessioni VPN come segue.

Per visualizzare le metriche utilizzando la console CloudWatch

I parametri vengono raggruppati prima in base allo spazio dei nomi del servizio e successivamente in base alle diverse combinazioni di dimensioni all'interno di ogni spazio dei nomi.

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. In All metrics (Tutti i parametri), scegliere il namespace parametro VPN.
4. Seleziona la dimensione per visualizzare le metriche (ad esempio Metriche tunnel VPN).

> **Note**
>
> Lo spazio dei nomi VPN non verrà visualizzato nella CloudWatch console fino a quando non sarà stata creata una connessione VPN da sito a sito nella regione che stai visualizzando. AWS

Per visualizzare le metriche utilizzando il AWS CLI

Al prompt dei comandi, utilizza il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Creazione di CloudWatch allarmi per monitorare i tunnel VPN

Puoi creare un CloudWatch allarme che invia un messaggio Amazon SNS quando l'allarme cambia stato. Un allarme controlla un singolo parametro in un periodo di tempo specificato e invia una notifica a un argomento Amazon SNS in base al valore del parametro relativo a una determinata soglia in periodi di tempo specificati.

Ad esempio, puoi creare un allarme che monitora lo stato di un tunnel VPN e inviare una notifica quando lo stato del tunnel è DOWN per 3 datapoint entro 15 minuti.

Per creare un allarme per lo stato del tunnelsingolo

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegli Allarmi, quindi Tutti gli allarmi.

3. Scegli Crea allarme, quindi Seleziona metrica.
4. Scegli VPN, quindi scegli Metriche tunnel VPN.
5. Seleziona l'indirizzo IP del tunnel desiderato, sulla stessa riga della TunnelStatemetrica. Scegli Select Metric (Seleziona parametro).
6. Per Whenever TunnelState is... , seleziona Inferiore, quindi inserisci «1" nel campo di immissione sotto a... .
7. In Configurazione aggiuntiva, imposta gli input “3 su 3” per i datapoint da attivare.
8. Seleziona Successivo.
9. Sotto Invia notifica ale seguente argomento SNS, seleziona un elenco notifche esistente o creane uno nuovo.
10. Seleziona Successivo.
11. Immetti un nome per l’allarme. Seleziona Successivo.
12. Controlla le impostazioni per l'avviso, quindi scegli Create alarm (Crea allarme).

Puoi creare un allarme per monitorare lo stato della connessione Site-to-Site VPN. Ad esempio, puoi creare un allarme che invia una notifica quando lo stato di uno o entrambi i tunnel è DOWN per un periodo di 5 minuti.

Per creare un allarme per lo stato della connessione Site-to-Site VPN

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegli Allarmi, quindi Tutti gli allarmi.
3. Scegli Crea allarme, quindi Seleziona metrica.
4. Scegliere VPN, quindi scegliere VPN Connection Metrics (Parametri connessione VPN).
5. Seleziona la tua connessione VPN da sito a sito e la metrica. TunnelState Scegli Select metric (Seleziona parametro).
6. Per Statistic (Statistica), specificare Maximum (Massimo).

   In alternativa, se la connessione Site-to-Site VPN è stata configurata affinché entrambi i tunnel siano attivi, è possibile specificare una statistica Minimum (Minimo) di modo che una notifica sia inviata quando un tunnel è inattivo.
7. In Whenever (Ogni volta che), scegli Lower/Equal (Minore di/Uguale a) (**<=**) e inserisci 0 (o 0.5 per quando almeno un tunnel è inattivo). Seleziona Successivo.

8. In Actions (Operazioni), selezionare un elenco di notifiche esistente oppure scegliere New list (Nuovo elenco) per creare uno nuovo. Seleziona Successivo.
9. Immettere un nome e una descrizione per l'allarme. Seleziona Successivo.
10. Controlla le impostazioni per l'avviso, quindi scegli Create alarm (Crea allarme).

Puoi anche creare allarmi che monitorano il volume di traffico in entrata o in uscita del tunnel VPN. Ad esempio, l'allarme seguente monitora la quantità di traffico dalla rete al tunnel VPN e invia una notifica quando viene raggiunta la soglia di 5.000.000 di byte durante un periodo di 15 minuti.

Per creare un allarme per il traffico di rete in entrata

1. Apri la console all'indirizzo https://console.aws.amazon.com/cloudwatch/ CloudWatch .
2. Nel pannello di navigazione, scegli Allarmi, quindi Tutti gli allarmi.
3. Scegli Crea allarme, quindi Seleziona metrica.
4. Scegli VPN, quindi scegli VPN Tunnel Metrics (Parametri tunnel VPN).
5. Seleziona l'indirizzo IP del tunnel VPN e la metrica TunnelDataIn. Scegli Select metric (Seleziona parametro).
6. Per Statistic (Statistica), specificare Sum (Somma).
7. Per Period (Periodo), selezionare 15 minutes (15 minuti).
8. Per Whenever (Ogni volta che), scegliere Greater/Equal (Maggiore di/Uguale a) (>=) e immettere 5000000. Seleziona Successivo.
9. In Actions (Operazioni), selezionare un elenco di notifiche esistente oppure scegliere New list (Nuovo elenco) per creare uno nuovo. Seleziona Successivo.
10. Immettere un nome e una descrizione per l'allarme. Seleziona Successivo.
11. Controlla le impostazioni per l'avviso, quindi scegli Create alarm (Crea allarme).

L'allarme seguente monitora il volume di traffico dal tunnel VPN alla rete E invia una notifica quando il numero di byte è inferiore a 1.000.000 durante un periodo di 15 minuti.

Per creare un allarme per il traffico di rete in uscita

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegli Allarmi, quindi Tutti gli allarmi.
3. Scegli Crea allarme, quindi Seleziona metrica.

4. Scegli VPN, quindi scegli VPN Tunnel Metrics (Parametri tunnel VPN).
5. Seleziona l'indirizzo IP del tunnel VPN e la metrica TunnelDataOut. Scegli Select metric (Seleziona parametro).
6. Per Statistic (Statistica), specificare Sum (Somma).
7. Per Period (Periodo), selezionare 15 minutes (15 minuti).
8. Per Whenever (Ogni volta che), scegliere Lower/Equal (Minore/Uguale) (<=) e immettere `1000000`. Seleziona Successivo.
9. In Actions (Operazioni), selezionare un elenco di notifiche esistente oppure scegliere New list (Nuovo elenco) per creare uno nuovo. Seleziona Successivo.
10. Immettere un nome e una descrizione per l'allarme. Seleziona Successivo.
11. Controlla le impostazioni per l'avviso, quindi scegli Create alarm (Crea allarme).

Per altri esempi di creazione di allarmi, consulta Creazione di CloudWatch allarmi Amazon nella Amazon CloudWatch User Guide.

Monitoraggio delle connessioni VPN tramite eventi AWS Health

AWS Site-to-Site VPN invia automaticamente notifiche a AWS AWS Health Dashboard(PHD), che è alimentato dall' AWS Health API. Questa dashboard non richiede alcuna configurazione ed è pronta per l'uso per gli utenti autenticati AWS . Puoi configurare più operazioni in risposta alle notifiche degli eventi tramite il AWS Health Dashboard.

AWS Health Dashboard Fornisce i seguenti tipi di notifiche per le connessioni VPN:

- Notifiche di sostituzione degli endpoint del tunnel
- Notifiche VPN a tunnel singolo

Notifiche di sostituzione degli endpoint del tunnel

Riceverai una notifica di sostituzione degli endpoint Tunnel AWS Health Dashboard quando uno o entrambi gli endpoint del tunnel VPN nella tua connessione VPN vengono sostituiti. Un endpoint del tunnel viene sostituito quando AWS esegue gli aggiornamenti del tunnel o quando modifichi la connessione VPN. Per ulteriori informazioni, consulta Sostituzioni degli endpoint del tunnel Site-to-Site VPN.

Quando la sostituzione di un endpoint del tunnel è completa, AWS invia la notifica di sostituzione dell'endpoint Tunnel tramite un evento. AWS Health Dashboard

Notifiche VPN a tunnel singolo

Una connessione Site-to-Site VPN è costituita da due tunnel per la ridondanza. Ti consigliamo vivamente di configurare entrambi i tunnel per la disponibilità elevata. Se la connessione VPN ha un tunnel attivo, ma l'altro è inattivo per più di un'ora al giorno, riceverai mensilmente una notifica VPN a tunnel singolo tramite un evento AWS Health Dashboard . Questo evento verrà aggiornato quotidianamente con tutte le nuove connessioni VPN rilevate come tunnel singolo, con notifiche inviate settimanalmente. Ogni mese verrà creato un nuovo evento che cancellerà tutte le connessioni VPN non più rilevate come tunnel singolo.

Quote di VPN sito-sito

Il tuo AWS account ha le seguenti quote, precedentemente denominate limiti, relative alla VPN da Site-to-Site. Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per richiedere un aumento delle quote per una quota regolabile, scegli Yes (Sì) nella colonna Adjustable. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente per Service Quotas.

Risorse Site-to-Site VPN

Nome	Predefinita	Adattabile
Gateway del cliente per regione	50	Sì
Gateway privati virtuali per regione	5	Sì
Connessioni VPN sito-sito per Regione	50	Sì
Connessioni VPN sito-sito per gateway virtuale privato	10	Sì
Connessioni VPN sito-sito accelerate per Regione	10	Sì
Connessioni VPN sito-sito per regione	10	Sì

> **Note**
>
> Sia le connessioni accelerate che quelle non associate vengono conteggiate nella quota totale delle connessioni VPN sito-sito per regione.

È possibile collegare un gateway virtuale privato alla volta a un VPC. Per collegare la stessa connessione Site-to-Site VPN a più VPC, ti consigliamo di utilizzare un gateway di transito. Per ulteriori informazioni, consulta Gateway di transito in Gateway di transito di Amazon VPC.

Le connessioni Site-to-Site VPN su un gateway di transito sono soggette al limite totale dei collegamenti del gateway di transito. Per ulteriori informazioni, consulta Quote di Transit gateway.

Route

Le origini delle route annunciate includono route VPC, altre route VPN e route delle interfacce virtuali AWS Direct Connect . Le route annunciate provengono dalla tabella di routing associata al collegamento VPN.

> **Note**
>
> Se utilizzi un gateway privato virtuale e la propagazione del routing è abilitata sulla tabella di routing VPC, verranno automaticamente aggiunti sia il routing dinamico che quello statico per la tua connessione VPN, fino al limite della tabella di routing del VPC. Per ulteriori dettagli, consulta le quote di Amazon VPC nella Guida per l'utente di Amazon VPC.

Nome	Predefinita	Adattabile
Route dinamiche annunciate da un dispositivo gateway del cliente a una connessione Site-to-Site VPN su un gateway virtuale privato	100	No
Route annunciate da una connessione Site-to-Site VPN su un gateway virtuale privato a un dispositivo gateway del cliente	1.000	No
Route dinamiche annunciate da un dispositivo gateway del cliente a una connessione Site-to-Site VPN su un transit gateway	1.000	No
Route annunciate da una connessione Site-to-Site VPN su un transit gateway per un dispositivo gateway del cliente	5.000	No
Route statiche da un dispositivo gateway del cliente a una connessione Site-to-Site VPN su un gateway virtuale privato	100	No

Larghezza di banda e throughput

Ci sono molti fattori che possono influenzare la larghezza di banda realizzata attraverso una connessione Site-to-Site VPN, tra cui, a titolo esemplificativo, la dimensione dei pacchetti, il mix di traffico (TCP/UDP), la definizione o la limitazione delle policy sulle reti intermedie, il meteo Internet e i requisiti specifici delle applicazioni.

Nome	Predefinita	Adattabile
Larghezza di banda massima per tunnel VPN	Fino a 1,25 Gb/s	No
Pacchetti al secondo (PPS) massimi per tunnel VPN	Fino a 140.000	No

Per le connessioni Site-to-Site VPN su un gateway di transito puoi utilizzare ECMP per ottenere una maggiore larghezza di banda VPN aggregando più tunnel VPN. Per utilizzare ECMP, la connessione VPN deve essere configurata per il routing dinamico. ECMP non è supportato nelle connessioni VPN che utilizzano routing statico. Per ulteriori informazioni, consulta Gateway di transito.

Unità di trasmissione massima (MTU)

La VPN Site-to-Site supporta un'unità di trasmissione massima (MTU) di 1446 byte e una corrispondente dimensione massima del segmento (MSS) di 1406 byte. Tuttavia, alcuni algoritmi che utilizzano intestazioni TCP più grandi possono ridurre efficacemente tale valore massimo. Per evitare la frammentazione, si consiglia di impostare MTU e MSS in base agli algoritmi selezionati. Per ulteriori dettagli su MTU, MSS e i valori ottimali, consulta Best practice per il dispositivo gateway del cliente.

I frame jumbo non sono supportati. Per ulteriori informazioni, consulta Jumbo frames nella Guida per l'utente di Amazon EC2.

Una connessione Site-to-Site VPN non supporta il rilevamento della MTU del percorso.

Risorse aggiuntive delle quote

Per le quote relative ai gateway di transito, incluso il numero di collegamenti su un gateway di transito, consulta Quote per i gateway di transito nella Guida dei gateway di transito di Amazon VPC.

Per informazioni sulle quote VPC aggiuntive, consulta Quote di Amazon VPC nella Guida per l'utente di Amazon VPC.

Cronologia dei documenti per la guida per l'utente della VPN site-to-site

La tabella seguente descrive gli aggiornamenti della Guida per l'utente di AWS Site-to-Site VPN.

Modifica	Descrizione	Data
Le informazioni VPN classiche sono state rimosse	Le informazioni sulla VPN classica sono state rimosse dalla guida.	19 gennaio 2023
Messaggi di esempio log VPN	Log di esempio aggiunti per connessione VPN sito-sito.	9 dicembre 2022
Utilità Download Configuration aggiornata	I clienti Site-to-Site VPN possono generare modelli di configurazione per i dispositivi Customer Gateway (CGW) compatibili, semplificando la creazione di connessioni VPN ad AWS. Questo aggiornamento aggiunge il supporto per i parametri Internet Key Exchange versione 2 (IKEv2) per molti dispositivi CGW popolari e include due nuove API - GetVpnConnectionDeviceTypes e GetVpnConnectionDeviceSampleConfiguration.	21 settembre 2021
Notifiche di connessione VPN	Site-to-Site VPN invia automaticamente le notifiche relative alla connessione VPN al AWS Health Dashboard.	29 ottobre 2020

Avvio tunnel VPN	È possibile configurare i tunnel VPN in modo che AWS richiama i tunnel.	27 agosto 2020
Modificare le opzioni di connessione VPN	Puoi modificare le opzioni per la connessione Site-to-Site VPN.	27 agosto 2020
Algoritmi di sicurezza aggiuntivi	È possibile applicare algoritmi di sicurezza aggiuntivi ai tunnel VPN.	14 agosto 2020
Supporto IPv6	I tunnel VPN possono supportare il traffico IPv6 all'interno dei tunnel.	12 agosto 2020
Unione di guide AWS Site-to-Site VPN	Questa versione unisce il contenuto della Guida per l'amministratore di rete AWS Site-to-Site VPN in questa guida.	31 marzo 2020
Connessioni di AWS Site-to-Site VPN accelerate	Puoi abilitare l'accelerazione per la connessione AWS Site-to-Site VPN.	3 dicembre 2019
Modifica delle opzioni tunnel AWS Site-to-Site VPN	Puoi modificare le opzioni per un tunnel VPN in una connessione AWS Site-to-Site VPN. Puoi inoltre configurare ulteriori opzioni tunnel.	29 agosto 2019
Supporto certificato privato AWS Private Certificate Authority	Puoi utilizzare un certificato privato da AWS Private Certificate Authority per autenticare la VPN.	15 agosto 2019

Nuova guida per l'utente di Site-to-Site VPN	In questa versione il contenuto di AWS Site-to-Site VPN (precedentemente noto come AWS Managed VPN) è separato dalla Guida per l'utente di Amazon VPC.	18 dicembre 2018
Modifica del gateway target	Puoi modificare il gateway target della connessione AWS Site-to-Site VPN.	18 dicembre 2018
ASN personalizzato	Quando crei un gateway virtuale privato, puoi specifica re un Autonomous System Number (ASN) privato per il lato Amazon del gateway.	10 Ottobre 2017
Opzioni per tunnel VPN	Puoi specificare blocchi CIDR per tunnel interni e chiavi già condivise personalizzate per i tunnel VPN.	3 ottobre 2017
Parametri VPN	Puoi visualizzare i parametri CloudWatch per le connessio ni VPN.	15 maggio 2017

Miglioramenti per VPN	Una connessione VPN ora supporta la funzione di crittografia AES a 256 bit, la funzione di hashing SHA-256, NAT Traversal e ulteriori gruppi Diffie-Hellman durante la Fase 1 e la Fase 2 di una connessione. Puoi inoltre utilizzare lo stesso indirizzo IP del gateway del cliente per ogni connessione VPN che utilizza lo stesso dispositivo gateway del cliente.	28 Ottobre 2015
Connessioni VPN che utilizzano la configurazione di routing statico	Puoi creare connessioni VPN IPsec con Amazon VPC utilizzando configurazioni di routing statico. In precedenza, le connessioni VPN richiedevano l'utilizzo del protocollo BGP (Border Gateway Protocol). Ora sono supportati entrambi i tipi di connessione E puoi stabilire la connettività da dispositivi che non supportano BGP, tra cui Cisco ASA e Microsoft Windows Server 2008 R2.	13 settembre 2012
Propagazione automatica delle route	Ora puoi configurare la propagazione automatica delle route dai collegamenti VPN e AWS Direct Connect alle tabelle di routing VPC.	13 settembre 2012

AWS VPN CloudHub e connessioni VPN ridondanti	Puoi comunicare in modo sicuro da un sito all'altro con o senza un VPC. Puoi inoltre utilizzare connessioni VPN ridondanti per fornire una connessione con tolleranza ai guasti al VPC.	29 settembre 2011

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.