AWS Decision Guide

Choosing an AWS networking and content delivery service

Choosing an AWS networking and content delivery service: AWS Decision Guide

Table of Contents

Introduction **1**
Understand 2
Consider 4
Choose 7
Use 9
Explore 19
Document history **20**

Choosing an AWS networking and content delivery service

Purpose:	Help determine which AWS networking and content delivery services are the best fit for your organization.
Last updated:	December 12, 2023
Covered services:	• Amazon API Gateway • AWS Client VPN • AWS Cloud WAN • Amazon CloudFront • AWS Direct Connect • Elastic Load Balancing • AWS Firewall Manager • AWS Global Accelerator • AWS Network Firewall • AWS PrivateLink • Amazon Route 53 • AWS Shield • AWS Site-to-Site VPN • AWS Transit Gateway • AWS Verified Access • Amazon VPC • Amazon VPC IPAM • Amazon VPC Lattice • AWS WAF

Deciding on an approach to cloud networking and content delivery can be complex, especially if you're used to managing and configuring networks with on-premises hardware. Fortunately, building networks in the cloud shares core concepts with building on-premises, such as IP addressing, load balancing, and routing. Familiarity with these concepts will help you understand what AWS services you need.

Amazon Web Services (AWS) offers 20+ purpose-built networking and content delivery services that you can use to build, operate, and secure your cloud networks across all your cloud environments and distributed cloud and edge locations globally. You can also build network infrastructure that extends your on-premises environment to AWS.

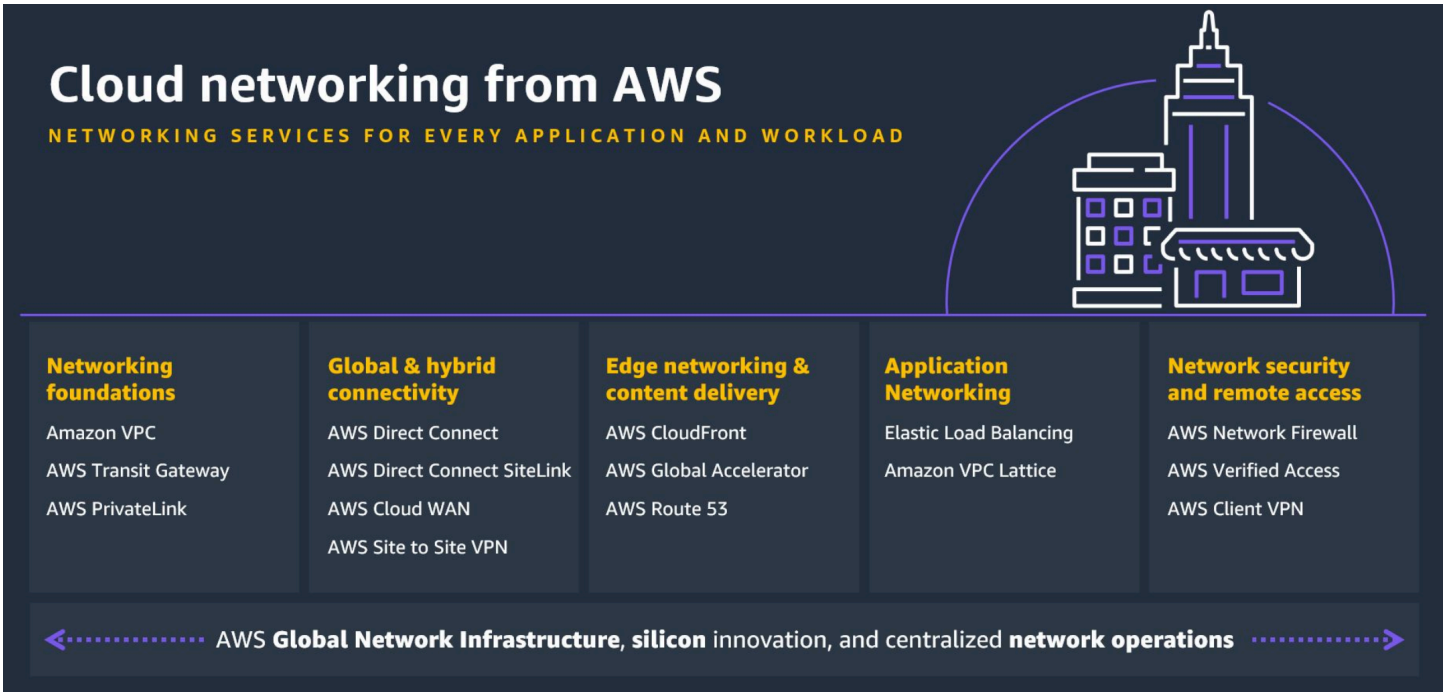
This decision guide will help you ask the right questions to choose the networking and content delivery services and tools that fit your needs.

This video provides a four-minute introduction to AWS networking.

Understand

What you build in AWS depends on your business needs. In this guide, we use the term *workloads* to refer to any collection of resources and code that delivers business value, such as a customer-facing application or a backend process.

Networking and content delivery services at AWS fall into four categories: networking foundations, global and hybrid connectivity, edge networking and content delivery, and application networking.



Networking foundations

In AWS, your workloads run inside one or more Amazon Virtual Private Cloud (VPCs). After your workloads are running in VPCs, you can connect the workloads to other VPCs—such as an AWS Transit Gateway—or you can connect them to software as a service (SaaS) services including other AWS services, such as AWS PrivateLink. Amazon VPC lets you provision a private, isolated section of the AWS Cloud where you can launch AWS resources in a virtual network using customer-defined IP address ranges. Amazon VPC gives you several options for connecting your AWS virtual networks with other remote networks.

Global and hybrid connectivity

You can use the services in this category to securely connect from on-premises networks to your workloads in the AWS Cloud. You can create a virtual private network (VPN) to connect remote users by using AWS Client VPN, connect on-premises networks using AWS Site-to-Site VPN, or build a global wide area network (WAN) with AWS Cloud WAN. You can also set up a direct, private connection to the AWS Cloud using AWS Direct Connect, providing a direct, secure connection to the cloud with predictable performance. You may also need to connect your on-premises data centers, remote sites, and the cloud. A hybrid network can connect these different environments.

Edge networking and content delivery

Services in this category help ensure higher performance through caching and optimized transport. A good example of this is Amazon CloudFront. You'll also want to see customer traffic optimally routed to provide availability using services such as Amazon Route 53. Additionally, it's important that customer traffic is routed to make the most of the AWS global infrastructure using services such as AWS Global Accelerator.

Application networking

As you increase adoption of the AWS Cloud, you'll want to consider how to connect workloads at scale, by using AWS App Mesh and Amazon VPC Lattice, integrate the workloads in your VPCs with APIs by using Amazon API Gateway, and manage the IP address usage of the resources running in your VPCs by using Amazon VPC IP Address Manager (IPAM). As customer demand increases, you can help ensure that the workloads in your VPCs can scale and provide high availability by using Elastic Load Balancing.

Networking security and remote access

While Amazon VPC helps you secure access to your workloads, the services in this category offer enhanced protection against threat actors and unauthorized users by using AWS Network Firewall,

AWS Shield, AWS Verified Access, and AWS WAF. To help ensure network security, consider using Amazon Route 53 DNS Firewall, AWS Network Firewall, AWS Firewall Manager, network access control lists, and security groups.

Consider

It's important that you choose the networking services that fit your business needs. The following are some of the criteria to consider when choosing networking services.

Business objectives

The networking services that you choose will depend on your business objectives. Assess where you are now and where you want to be when it comes to the security, reliability, accessibility, and performance of your workloads running in the AWS Cloud.

- Consider how the network services you use fit with your migration and integration strategies. A hybrid networking architecture can help you meet this need by integrating your on-premises data center and AWS.
- Review the networking and content delivery blogs in the *Let's architect!* AWS blog series to see what others are building in the AWS Cloud.
- Examine the third-party options available to help you accelerate your networking service adoption. The AWS Marketplace provides a curated digital catalog that you can use to find, buy, and deploy networking solutions.
- Decide if working with an AWS Partner that specializes in networking and content delivery would be beneficial. Members of the AWS Partner Network are strategic experts and experienced builders that can help you meet your needs with the AWS Cloud.
- Explore taking AWS networking online courses on AWS Skill Builder that cover services such as Amazon VPC, AWS Cloud WAN, and Amazon Route 53.

Workload characteristics

The networking services that you choose will depend on the characteristics of your workloads.

- Networking services each have a particular role. Services such as AWS Cloud WAN and AWS Transit Gateway are suited for connecting workloads that are running in VPCs. Amazon API Gateway creates public APIs so that your customers can connect to your workloads.

AWS Global Accelerator can help you improve the reliability, security, and latency of your workloads.

- As the internet continues to grow, so does the need for IP addresses for devices. The most common format for IP addresses is IPv4. The latest format for IP addresses is IPv6. IPv6 provides more address space and solves the problem of IPv4 address exhaustion. AWS services support for IPv6 includes support for dual stack configuration (IPv4 or IPv6) or IPv6 only configurations. The number of AWS services that support IPv6 is growing continuously. To view the current services that support IPv6, see AWS services that support IPv6.

Data protection

It's important to consider the protection of your data in the AWS Cloud.

- Businesses must protect customer data against evolving cyber risks. While Amazon VPC helps you to secure access to the workloads running in VPCs, consider enhanced data protection measures, such as AWS Network Firewall, AWS Shield, AWS WAF, and Amazon Route 53 Resolver DNS Firewall.
- It's recommended that you employ application-level encryption (TLS), irrespective of the transport, as a defense in depth measure to help ensure confidentiality end-to-end.
- If the workloads in your VPCs need to connect to other AWS services, you can connect to those services programmatically by using API endpoints over the public internet. However, if you want to send data over a private connection, use AWS PrivateLink. Many members of the AWS Partner Network offer their SaaS solutions through AWS PrivateLink.

Availability

Availability is an application's ability to maintain uptime. It's important that your customers can use the products and services that you build in your VPCs with minimal or no downtime.

- The AWS global infrastructure is built on AWS Regions and Availability Zones. When you deploy your workloads to your VPCs, you should deploy to multiple Availability Zones to ensure that your workload is still available in the event of a single Availability Zone failure.
- To improve the availability, scalability, security, and performance of the workloads running in your VPCs, consider load balancing (Elastic Load Balancing). You can use different types of load balancers depending on the needs of your applications. Each load balancer supports different types of traffic over different protocols and network layers aligned to the Open

Systems Interconnection (OSI) model. For more information about the differences between load balancer types, see product comparisons.

Performance

You can use networking services to optimize for the latency, throughput, and bandwidth requirements of your workloads running on the AWS global infrastructure.

- If you want to minimize latency to local customers using web applications around the globe, consider using Amazon CloudFront. CloudFront is a content delivery network that delivers content to customers with the lowest latency possible.
- If you're running gaming, Internet of Things (IoT), or Voice over IP (VoIP) workloads, consider using AWS Global Accelerator. This service helps you improve your workloads' availability and performance.
- If the workloads in your VPCs need to connect to other AWS Regions, you can connect to those services programmatically using public API endpoints.

Operational excellence

As you increase AWS Cloud adoption, you'll want to understand what is happening across your workloads at any time. Tools and services such as Reachability Analyzer and Amazon CloudWatch Internet Monitor can help you keep pace with changing business needs and priorities as your workloads grow.

- Managing IP addresses of workloads running in multiple VPCs can be difficult. Consider if you need to automate IP address management across your workloads (Amazon VPC IPAM).
- If you're using a microservice architecture, managing the connectivity, security, and monitoring between microservices can be a challenge. Consider if you need to automate microservice interaction (AWS App Mesh and Amazon VPC Lattice).

Connectivity

You can use networking services to connect to the AWS Cloud, connect workloads, or connect networks.

- Consider the following for connecting to the AWS Cloud:
  - If you want to securely connect remote users to your VPCs, consider using AWS Client VPN.

  - If you want to securely connect an entire on-premises network to your VPCs, consider using AWS Site-to-Site VPN.
  - If you require more consistent performance than the public internet can provide, consider a direct connection from your on-premises network to AWS (AWS Direct Connect).

- Consider the following for connecting networks:
  - If you operate in multiple AWS Regions, want to manage your own routing configurations, or prefer to use your own automation, consider using AWS Transit Gateway.
  - If you want to unify your data center, branch, and AWS networks with a WAN, consider using AWS Cloud WAN. It is also worth considering if you don't want to manage complex routing configurations or build your own automations for multi-Region connectivity.

Security

AWS provides a secure foundation for you to build and deploy your applications, but you are responsible for implementing your own security measures to protect your data, applications, and networking infrastructure, no differently than you would in an on-site data center.

- Review and understand the AWS Shared Responsibility Model and how it applies to security in the AWS Cloud.
- AWS security groups and network access control lists (NACLs) can be used together or on their own to secure a network, helping you to create a defense in depth security strategy.
- Businesses must protect their network applications against evolving cyber risks. Consider if you will need to protect your workloads against malicious attacks or malware (with AWS Network Firewall), distributed denial of service (DDoS) attacks (with AWS Shield), or SQL injection and cross-site scripting attacks (with AWS WAF).

  Amazon Route 53, AWS Firewall Manager, network access control lists, and security groups are also important to consider in ensuring network security.

Choose

Now that you know the criteria by which you will be evaluating your networking service options, you are ready to choose which services may be a good fit.

Service category	What is it optimized for?	AWS networking and content delivery services
Network foundations	Optimized for getting started with AWS networking services and connecting your VPCs securely.	Amazon VPC AWS PrivateLink AWS Transit Gateway
Global and hybrid connectivity	Optimized to ensure private, secure, and global network connectivity.	AWS Client VPN AWS Cloud WAN AWS Direct Connect AWS Site-to-Site VPN
Edge networking and content delivery	Optimized for low latency, reliable traffic routing to and from your workloads.	Amazon CloudFront AWS Global Accelerator Amazon Route 53
Application networking	Optimized to ensure that your workloads are highly available, adapt to demand, and can communicate with each other.	Amazon API Gateway Amazon VPC IPAM Amazon VPC Lattice Elastic Load Balancing
Network security and remote access	Optimized to protect your workloads against malware, DDoS, SQL injection, and cross-site scripting attacks.	AWS Firewall Manager AWS Network Firewall AWS Shield AWS Verified Access AWS WAF

Use

To explore how to use and learn more about each of the available AWS network services, we have provided a pathway to explore how each of the services work. The following section provides links to in-depth documentation, hands-on tutorials, and resources to get you started.

The following services cover global networking and VPC connectivity.

Amazon CloudFront

What is Amazon CloudFront?

Learn about speeding up content distribution.

Explore the guide

Getting started with Amazon CloudFront

Learn the basic steps to delivering content with CloudFront.

Explore the guide

Hosting on-demand streaming video with Amazon S3, Amazon CloudFront, and Amazon Route 53

Learn how to host videos for on-demand viewing in a secure and scalable way.

Get started with the tutorial

Deliver content faster with Amazon CloudFront

Learn how to decrease the end user latency of your web applications.

Get started with the tutorial

AWS Cloud WAN

What is AWS Cloud WAN?

Learn how to build, manage, and monitor a unified global network.

Explore the guide

Introducing AWS Cloud WAN

Learn about the main use cases for AWS Cloud WAN and how to get started.

Read the blog

Getting started with AWS Cloud WAN

Create your first global network and attach a VPC.

Get started with the tutorial

AWS Direct Connect

What is AWS Direct Connect?

Learn about connecting an on-premises network to AWS.

Explore the guide

Getting started with AWS Direct Connect

Watch a brief introduction to AWS Direct Connect and how to prepare your on-premises network to connect to AWS.

Watch the video

Connect your data center to AWS

Connect your data center to AWS using AWS Direct Connect.

Get started with the tutorial

AWS Global Accelerator

What is AWS Global Accelerator?

Learn about improving the performance of your workloads.

Explore the guide

Getting started with a standard accelerator

Create an accelerator to improve the network performance of a workload running on an EC2 instance.

Get started with the tutorial

Improve global application availability and performance for your traffic

Watch a brief demonstration on setting up AWS Global Accelerator to improve network performance.

Watch the video

AWS PrivateLink

What is AWS PrivateLink?

Learn how to privately connect your VPC to services.

Explore the guide

Get started with AWS PrivateLink

Send a request from an EC2 instance in a private subnet to Amazon CloudWatch using PrivateLink.

Get started with the tutorial

Expedite your IPv6 adoption with PrivateLink services and endpoints

Customers with large internet footprints feel the strain of public IPv4 address exhaustion. Learn how you can increase IPv6 usage within VPCs using PrivateLink.

Read the blog

Amazon Route 53

What is Amazon Route 53?

Learn about highly available and scalable domain name resolution.

Explore the guide

Amazon Route 53 use case tutorials

How to use Route 53 for use cases based on traffic and latency.

Get started with the tutorial

How to register a domain name with Amazon Route 53

This tutorial helps you register a new domain name for a web application.

Get started with the tutorial

Amazon Route 53 introduction

Watch a brief introduction to domain name resolution and Route 53.

Watch the video

AWS Site-to-Site VPN

What is AWS Site-to-Site VPN?

Getting started with AWS Site-to-Site VPN

AWS Site-to-Site VPN, choosing the right options to optimize performance

Learn about connecting remote users to AWS over VPN.

Explore the guide

Set up a Site-to-Site VPN connection between an on-premises device and AWS.

Get started with the tutorial

Choose the best options when setting up a VPN connection to AWS.

Read the blog

AWS Transit Gateway

What is a transit gateway?

Learn how to connect VPCs with transit gateways.

Explore the guide

Example transit gateway use cases

View common use cases for transit gateways.

Explore the guide

AWS Transit Gateway workshop

In this hands-on workshop, learn how to deploy Transit Gateway in single Region and single account, multi-account, and multi-Region setups.

Start the workshop

Amazon VPC

What is Amazon VPC?

Learn about virtual private clouds and the features of Amazon VPC.

Explore the guide

Get started with Amazon VPC

A guide to quickly getting started with Amazon VPC.

Explore the guide

Example VPC configura tions

View example VPC configura tions based on different use cases.

		Explore the guide
 **Modular and scalable VPC architecture** Build a virtual networking foundation based on AWS best practices for your AWS Cloud infrastructure. Get started with the tutorial		

Amazon VPC IPAM

 **What is IPAM?** Learn how to track and manage IP address usage. Explore the guide	 **Amazon VPC IP Address Manager (IPAM) best practices** Learn how to create a scalable IP address management plan. Read the blog	 **Creating pools to manage your IP space** Watch a brief video introduction to VPC IPAM. Watch the video

The following services relate to application level networking.

Amazon API Gateway

What is Amazon API Gateway?

Learn about creating APIs for your workloads.

Explore the guide

Building APIs with Amazon API Gateway

Learn how to get started building APIs in AWS.

Watch the video

Configuring private integrations with Amazon API Gateway HTTP APIs

Learn how to create an API to control private access to resources in a VPC.

Read the blog

AWS Client VPN

What is AWS Client VPN?

Learn about connecting networks to AWS over VPN.

Explore the guide

Getting started with AWS Client VPN

Download the AWS Client VPN application and connect to AWS over VPN.

Explore the guide

Scenarios and examples for AWS Client VPN

See examples for creating and configuring Client VPN access for your clients.

Explore the examples

Elastic Load Balancing

What is Elastic Load Balancing?

Learn about distributing incoming traffic across your workloads.

Explore the guide

Getting started with Elastic Load Balancing

Learn the difference between the different types of load balancers and create a load balancer.

Explore the guide

How to choose the right load balancer for your AWS workloads

Choose the right option to load balance traffic to your workloads.

Watch the video

AWS Firewall Manager

Getting started with AWS Firewall Manager policies

Learn how to use AWS Firewall Manager to enable a number of different types of security policies.

Explore the guide

How to continuously audit and limit security groups with AWS Firewall Manager

This blog post demonstra tes how to use AWS Firewall Manager to limit security groups to help ensure that only required ports are open.

Explore the guide

Use AWS Firewall Manager to deploy protection at scale in AWS Organizations

This post provides step-by-step instructions to deploy and manage security policies across your AWS Organizat ions implementation by using AWS Firewall Manager.

Explore the guide

AWS Network Firewall

What is AWS Network Firewall?

Getting started with AWS Network Firewall

AWS Network Firewall animated explainer video

Learn about network firewall and intrusion detection.

Explore the guide

Quickly create and manage a network firewall for a VPC.

Get started with the tutorial

Watch a brief video introduction to AWS Network Firewall.

Watch the video

AWS Shield

What is AWS Shield?

Learn about DDoS protectio n.

Explore the guide

Examples of basic DDoS resilient architectures

Learn about some common DDoS-resilient architectures.

Explore the guide

AWS Shield animated explainer video

Watch a brief video introduction to AWS Shield.

Watch the video

AWS Verified Access

Tutorial: Getting started with Verified Access

In this tutorial, you will learn how to create and configure Verified Access resources.

Explore the guide

AWS Verified Access Integration with third party identity providers

This blog post shows you how to integrate Verified Access (AVA) with the third party Okta identity provider.

Explore the guide

Integrating AWS Verified Access with device trust providers

This blog post discusses how to architect Zero Trust based remote connectivity on AWS.

Explore the examples

Amazon VPC Lattice

What is Amazon VPC Lattice?

Learn about connecting, securing, and monitoring the microservices in your workloads.

Explore the guide

Setting up Amazon VPC Lattice

Set up and launch VPC Lattice for the first time.

Explore the guide

Build secure multi-account multi-VPC connectivity for your applications with Amazon VPC Lattice

An introduction to how you can use VPC Lattice to solve VPC connectivity challenges.

Read the blog

Amazon VPC Lattice animated explainer

Watch a brief animated video about VPC Lattice.

Watch the video

AWS WAF

What is AWS WAF?

Learn about controlling access to your workloads.

Getting started with AWS WAF

Video introduction to AWS WAF

Explore the guide	Watch a brief video on how you can use AWS WAF to protect your workloads against web exploits and bots. Watch the video	Watch a brief video introduction to AWS WAF. Watch the video

Explore

Architecture diagrams	Whitepapers	AWS Solutions
Explore reference architecture diagrams to help you build your networking and content delivery architectures on AWS. Explore architecture diagrams	Explore whitepapers to help you get started, learn best practices, and understand your networking and content delivery options. Explore whitepapers	Explore vetted solutions and architectural guidance for common use cases for networking and content delivery. Explore AWS Solutions

Document history

The following table describes the important changes to this decision guide. For notifications about updates to this guide, you can subscribe to an RSS feed.

Change	Description	Date
Initial publication	Guide first published.	December 12, 2023