aws

아키텍처 다이어그램

보안 원격 작업자 환경

보안 원격 작업자 환경: 아키텍처 다이어그램

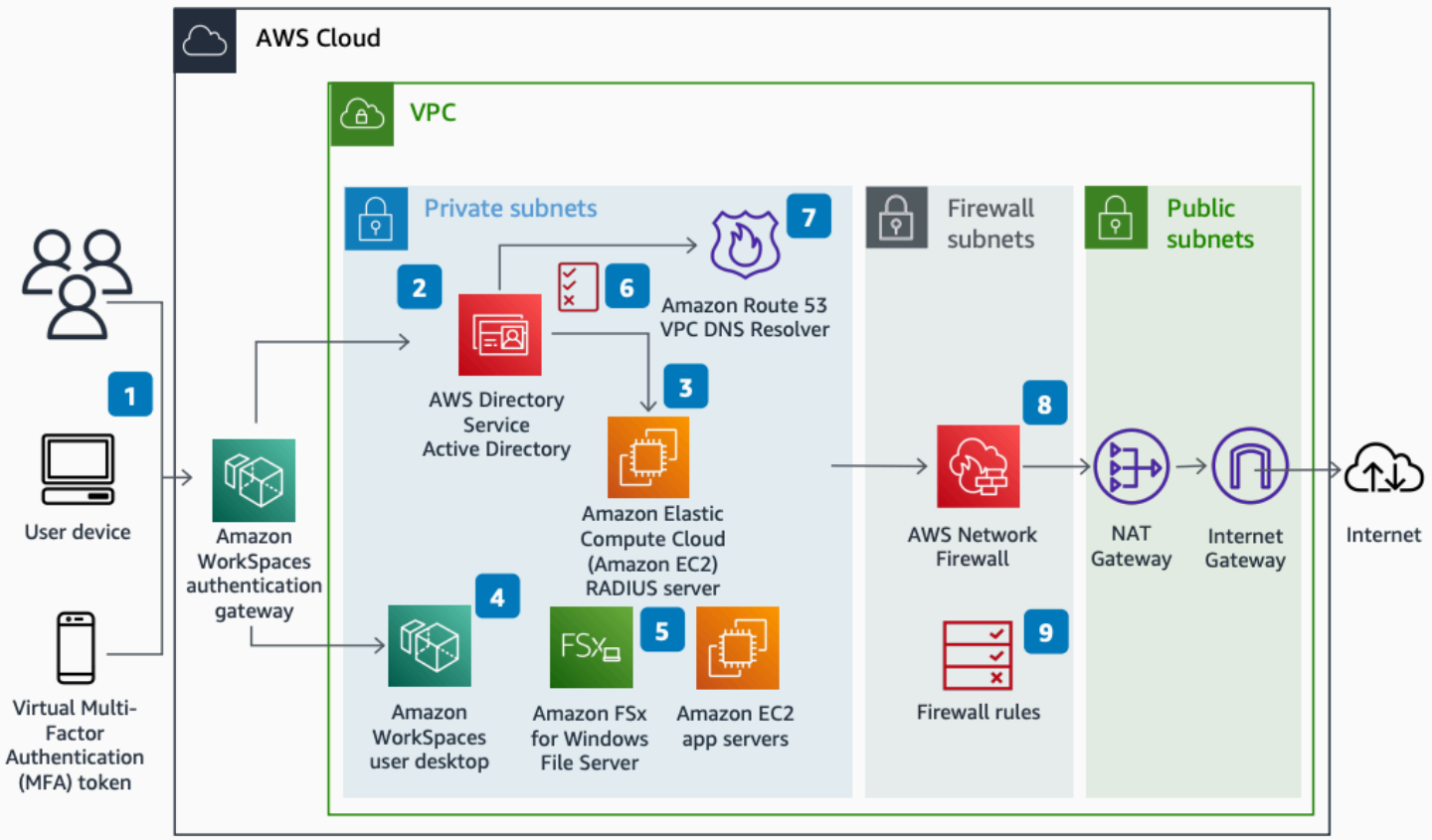
Table of Contents

보안 원격 작업자 환경

게시일: 2022년 1월 31일(다이어그램 기록)

이 아키텍처는 원격 작업자를 위한 안전한 데스크톱 환경을 구축하는 방법을 보여줍니다. 작업자는 주요 line-of-business 애플리케이션 및 데이터에 액세스할 수 있습니다.

보안 원격 작업자 환경



1. 사용자는 사용자 이름, 암호 및 MFA 코드와 함께 Amazon WorkSpaces 애플리케이션을 사용하여 데스크톱에 연결합니다.
2. Amazon WorkSpaces 인증 게이트웨이는 Amazon DynamoDB Streams에 대해 인증합니다.
3. MFA 코드는 MFA 서비스의 RADIUS 서버(예: OneLogin)에 대해 인증합니다.
4. 사용자는 Amazon WorkSpaces를 통해 데스크톱에 연결합니다.
5. 사용자는 Amazon Elastic Compute Cloud 및 Amazon FSx에서 호스팅되는 코어 시스템 및 파일에 액세스합니다.

6. Active Directory의 그룹 정책은 Amazon WorkSpaces에서 로컬 프린터로 인쇄하는 등 원치 않는 활동을 방지합니다.
7. 도메인 컨트롤러 DNS는 Route 53 Resolver DNS 방화벽 규칙을 적용하여 Route 53 VPC DNS 해석기로 전달합니다.
8. AWS Network Firewall는 아웃바운드 인터넷 트래픽을 필터링한 다음 NAT 게이트웨이와 인터넷 게이트웨이를 통해 퍼블릭 인터넷으로 라우팅합니다.
9. 방화벽 규칙은 원치 않는 사이트(예: 파일 공유 플랫폼)로의 아웃바운드 트래픽을 차단하여 데이터 유출을 방지합니다.

참조 자료

자세한 내용은 섹션을 참조하세요.

- AWS 아키텍처 아이콘
- AWS 아키텍처 센터
- AWS Well-Architected
- Amazon WorkSpaces 제품 페이지

다이어그램 기록

이 참조 아키텍처 다이어그램의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

변경 사항	설명	날짜
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2022년 1월 31일

> **Note**
>
> RSS 업데이트를 구독하려면 사용 중인 브라우저에 대해 RSS 플러그인이 활성화되어 있어야 합니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.