CONTROLLING REMOTE USER VPC ACCESS

"How do I implement VPC remote user access controls?"

Overview

Amazon Web Services (AWS) offers customers different methods for securing resources in their Amazon Virtual Private Cloud (Amazon VPC) networks. One important security measure is to effectively control remote user access in order to distinguish between authorized and unauthorized users. If internal resources are compromised, they can pose a threat to a larger network of resources—especially when attempting to steal sensitive data or communicate with command and control systems. This document provides AWS customers with best practices and common approaches for choosing a remote access solution as part of a holistic network security strategy. See the VPC Security Capabilities Solution Brief for broader network security recommendations.

The following sections assume basic knowledge of remote-network connectivity, virtual private networks (VPNs), user authentication, and networking.

General Best Practices

Consider the following universal network security principles when implementing a secure remote-access solution:

- Consider a solution that uses a two-factor authentication mechanism: a possession factor (something the user has) and a knowledge factor (something the user knows).
- Implement a solution that applies user- or profile-based policies rather than IP-based policies. User- or profile-based policies allow remote users to access internal resources from different IP addresses.
- Enable audit and access logging capabilities wherever available. Define log retention requirements and lifecycle policies early on, and plan to move log files to cost-efficient storage locations as soon as practical.

Application on AWS

The AWS Cloud provides low cost, elastic, and secure AWS services to control remote user access. In general, your authentication, authorization, auditing, availability, and scaling requirements will help determine the most appropriate configuration for your use case. The following sections describe common approaches that use a combination of native AWS services, open-source technologies, and third-party products for controlling remote user access.

Linux Bastion Hosts

Linux bastion hosts provide a secure way for you to connect to your Linux Amazon Elastic Compute Cloud (Amazon EC2) instances without exposing your Amazon VPCs to the internet. Bastion hosts also enable you to access other instances in your VPC using Secure Shell (SSH) on Linux. You can also configure security groups to provide fine-grain ingress control.

AWS offers a Quick Start that adds Linux bastion hosts to your new or existing AWS infrastructure for your Linux-based deployments. The bastion hosts provide secure access to Linux instances located in the private and public subnets of your virtual private cloud (VPC). The Quick Start sets up a Multi-AZ environment and deploys Linux bastion host instances into the public subnets to provide readily available administrative access to the environment. For more information, see the Linux Bastion Hosts Quick Start deployment guide.

Aviatrix User VPN Quick Start

For customers who want to implement a fully automated and prescriptive reference deployment, AWS offers the Aviatrix User VPN Quick Start. The Quick Start automatically deploys an Aviatrix Controller for a User VPN service in a new or existing Amazon VPC that enables your remote users to connect to your Amazon VPCs with enhanced security, and access your Amazon EC2 instances, applications, and services.

Aviatrix User VPN

The Quick Start leverages Aviatrix's User VPN, a cloud-native user VPN solution that enables secure remote access to AWS using Aviatrix SSL VPN. The solution is based on OpenVPN and is compatible with all OpenVPN clients. Aviatrix provides its own client that supports Security Assertion Markup Language (SAML) authentication directly from the client.

The Aviatrix User VPN features a point-and-click, centralized management console that you can use to implement changes and customizations quickly and easily. The solution supports many different authentication options including LDAP/AD, Duo, Okta, multi-factor authentication, and client SAML. It also allows you to assign users to profiles that provide granular access to network resources. For more information, see the Aviatrix User VPN Quick Start deployment guide.

Third-Party Solutions

The AWS Partner Network offers a variety of remote-access solutions that can help make it easier for companies of any size or stage of development provide secure remote access to their internal networks. When selecting a third-party product, look for a solution that is easy to configure, leverages your company's existing technologies, and meets your user management, configuration, patching, and upgrade requirements.

Cisco

The Cisco Adaptive Security Virtual Appliance (ASAv) is a virtual security solution that helps protect virtual and physical data center workloads that expand, contract, or shift their location over time. The Cisco ASAv delivers site-to-site, remote-access, and clientless VPN as a service in virtual domains or private cloud deployments. For more information, see the Cisco Adaptive Security Virtual Appliance (ASAv) webpage in the AWS Marketplace.

Palo Alto Networks

Palo Alto Networks VM-Series next-generation firewall is an AWS Network Competency and Security Competency approved solution that can be fully integrated into your AWS deployment workflow. With the VM-Series firewall, you can protect your remote users and reduce administrative effort and costs. For more information, see the Palo Alto Networks VM-Series Next-Generation Firewall Bundle 2 webpage in the AWS Marketplace.

Check Point

Check Point CloudGuard for AWS enables customers to meet their cloud security needs with flexible and manageable security options including: Firewall, VPN, Remote Access, IPS, Application Control, Antivirus, Anti-Bot. CloudGuard protects services in the public cloud from the most sophisticated threats as well as unauthorized access while preventing application layer denial of service attacks. For more information, see the CloudGuard IaaS webpage in the AWS Marketplace.

Sophos

Sophos Unified Threat Management (UTM) is a comprehensive security solution that helps you secure your infrastructure in AWS. Sophos UTM provides multiple security options including firewalls, IPS, advanced threat protection, and remote access. For more information, see the Sophos UTM webpage in the AWS Marketplace.

OpenVPN

OpenVPN Access Server is a full featured SSL VPN software solution that supports a wide range of configurations, including secure and granular remote access to internal network and/ or private cloud network resources and applications with fine-grained access control. For more information, see the OpenVPN Access Server webpage in the AWS Marketplace.

Resources

Amazon VPC	http://aws.amazon.com/vpc/

Amazon VPC Connectivity Options Whitepaper	https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/introduction.html AWS Whitepaper describing options for connecting to an Amazon Virtual Private Cloud.
Aviatrix User VPN AWS Quick Start	https://aws.amazon.com/quickstart/architecture/aviatrix-user-vpn/ AWS Quick Start that features a centralized controller and wizard for access control and configuration.
Linux Bastion Hosts AWS Quick Start	https://aws.amazon.com/quickstart/architecture/linux-bastion/ AWS Quick Start that creates bastion hosts for secure remote access in Linux-based deployments.