Secure Remote Worker for AWS

Design Guide

June 2021

Contents

Abstract

Today companies are investing in enabling their workforce to have a secure connection to the resources hosted in the Amazon Web Services (Public Cloud). This Cisco Validated Design guide (CVD) addresses a specific use case of secure remote workers covered in the Secure Remote Worker SAFE Design Guide. The secure remote worker solution uses the Cisco AnyConnect Secure Mobility Client, Cisco Duo, Cisco Umbrella, and Cisco Advanced Malware Protection (AMP) for Endpoints.

- **Cisco AnyConnect Secure Mobility Client:** Cisco AnyConnect Secure Mobility Client empowers remote workers with frictionless, highly secure access to the enterprise network from any device, at any time, in any location while protecting the organization. It provides a consistent user experience across devices, both on and off-premises, without creating a headache for your IT teams. Simplify management with a single agent
- **Cisco Duo:** Cisco Duo is a user-friendly, scalable way to keep business ahead of ever-changing security threats by implementing the Zero Trust security model. Multi-factor authentication from Duo protects the network by using a second source of validation, like a phone or token, to verify user identity before granting access. Cisco Duo is engineered to provide a simple, streamlined login experience for every remote user. As a cloud-based solution, it integrates easily with your existing technology and provides administrative, visibility, and monitoring
- **Cisco Umbrella Roaming Security Module:** Cisco Umbrella Roaming Security module for Cisco AnyConnect provides always-on security on any network, anywhere, any time – both on and off your corporate VPN. The Roaming Security module enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port. Umbrella provides real-time visibility into all internet activity per hostname both on and off your network or VPN
- **Cisco Advanced Malware Protection (AMP) Enabler:** Cisco AnyConnect AMP Enabler module is used as a medium for deploying Advanced Malware Protection (AMP) for Endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base. This approach provides AnyConnect user base administrators with an additional security agent that detects potential malware threats happening in the network, removes those threats, and protects the enterprise from compromise. It saves bandwidth and time taken to download, requires no changes on the portal side, and can be done without authentication credentials being sent to the endpoint. AnyConnect AMP Enabler protects the user both on and off the network or VPN

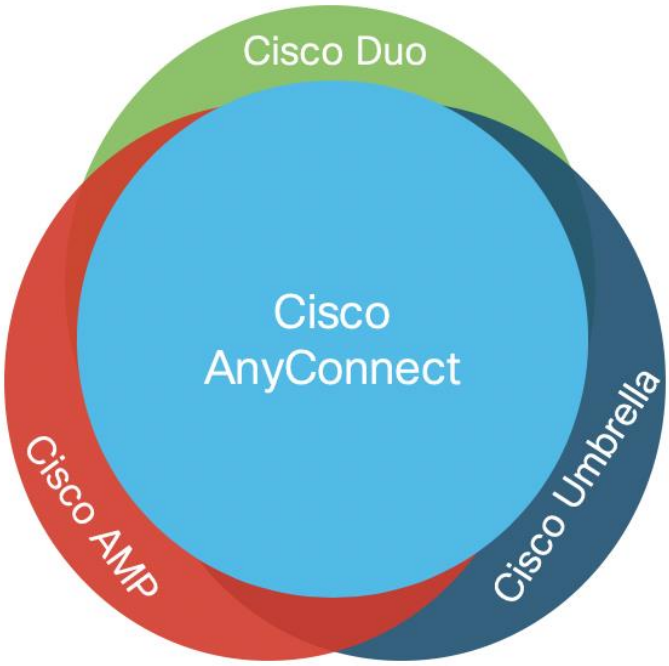


Figure 1. **Components of the Cisco secure remote worker solution**

Target Audience

This document provides best practices and recommended solutions for remote workers accessing resources hosted in the AWS cloud. This solution brings together a secure architecture that includes Anyconnect Mobility Client, Cisco Duo, Cisco Umbrella, and Cisco AMP for Endpoints to protect remote access workers even when the user is on an untrusted network. In addition to validated designs, this CVD also provides recommended step-by-step configuration.

The target audience for this CVD is Solutions Architect responsible for designing a secure environment for remote workers and the Implementation team responsible for deploying security.

Scope

Cisco Secure Remote Worker (SRW) design guide covers the following components:

- Cisco Secure Anyconnect Mobility Client
- Secure connection using remote access VPN termination on Cisco virtual appliances
  - Cisco Adaptive Security Virtual Appliance (Cisco ASAv)
- Authentication
  - LDAP
  - Duo (Two-factor authentication)
- Threat Protection
  - Cisco Umbrella Roaming Security Module (DNS Layer Security)
  - Cisco Advanced Malware Protection Enabler
- AWS Services

- Virtual Private Cloud (VPC)
- Transit Gateway (TGW)
- Internet Gateway (IGW)
- Route53
- Security Groups (SG)
- EC2 instances
- Elastic Network Interface (ENI)
- Elastic IP (EIP)
- Route Table (RT)

Out of scope

This document does not cover the following topics:

- Data Center connectivity (Hybrid Cloud): IPSec, SD-WAN, AWS direct connect enables hybrid cloud connectivity. These solutions are not part of this design guide
- Cisco ASA and NGFW authentication with DUO: Cisco ASA and NGFW support various types of authentication. This document covers LDAP authentication and Duo Integration on Cisco ASA
- This document does not cover the Cisco NGFWv VPN configuration and Cisco Defense Orchestrator (CDO)
- AWS Network Load balancer will not work properly with TLS and DTLS; this architecture uses AWS Route53 for DNS based VPN session load balancing
- This document covers “AWS Transit Gateway – TGW),” TGW is a regional construct. AWS supports inter-region TGW peering; this design guide does not cover TGW-TGW peering
- This architecture covers only VPN load-balancing; CVD does not focus on north-south and east-west traffic
- Cisco AnyConnect VPN auto-connect may not function because a new connection may land on another firewall when the VPN client initiates an auto-connect request

SAFE Architecture Introduction

Remote worker access enterprise resources using Internet connection protected by remote access VPN (RAVPN) or protected https session. Internet edge is an essential segment in the enterprise network, where the corporate network meets the public Internet. The SAFE Model identifies the Internet edge as one of the places in the network (PINs). SAFE simplifies complexity across the enterprise by implementing a model that focuses on the areas that a company must secure. This model treats each area holistically, focusing on today's threats and the capabilities needed to secure each area against those threats. Cisco has deployed, tested, and validated critical designs. These solutions provide guidance and best practices that ensure effective, secure remote access to the resources.

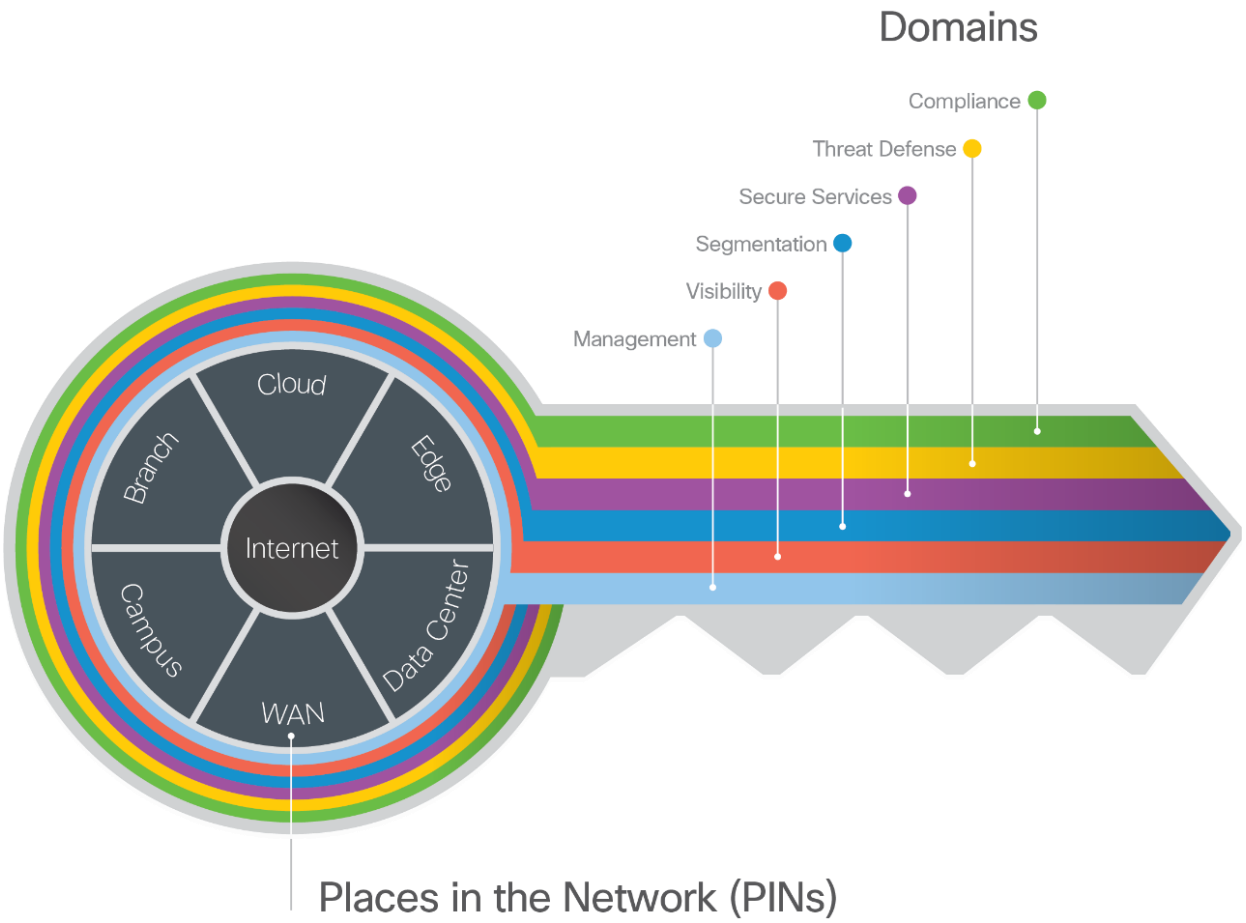


Figure 2. **key to SAFE organizes the complexity of holistic security into PINs & Secure Domain**

The Internet edge is the highest-risk PIN because it is the primary ingress for public traffic and the primary egress point to the Internet. Simultaneously, it is the critical resource that businesses need in today's Internet-based economy. SAFE matches up defensive capabilities against the categories of threats today. SAFE simplifies security by starting with business flows, then addressing their respective threats with corresponding security capabilities, architectures, and designs. SAFE provides guidance that is holistic and understandable.

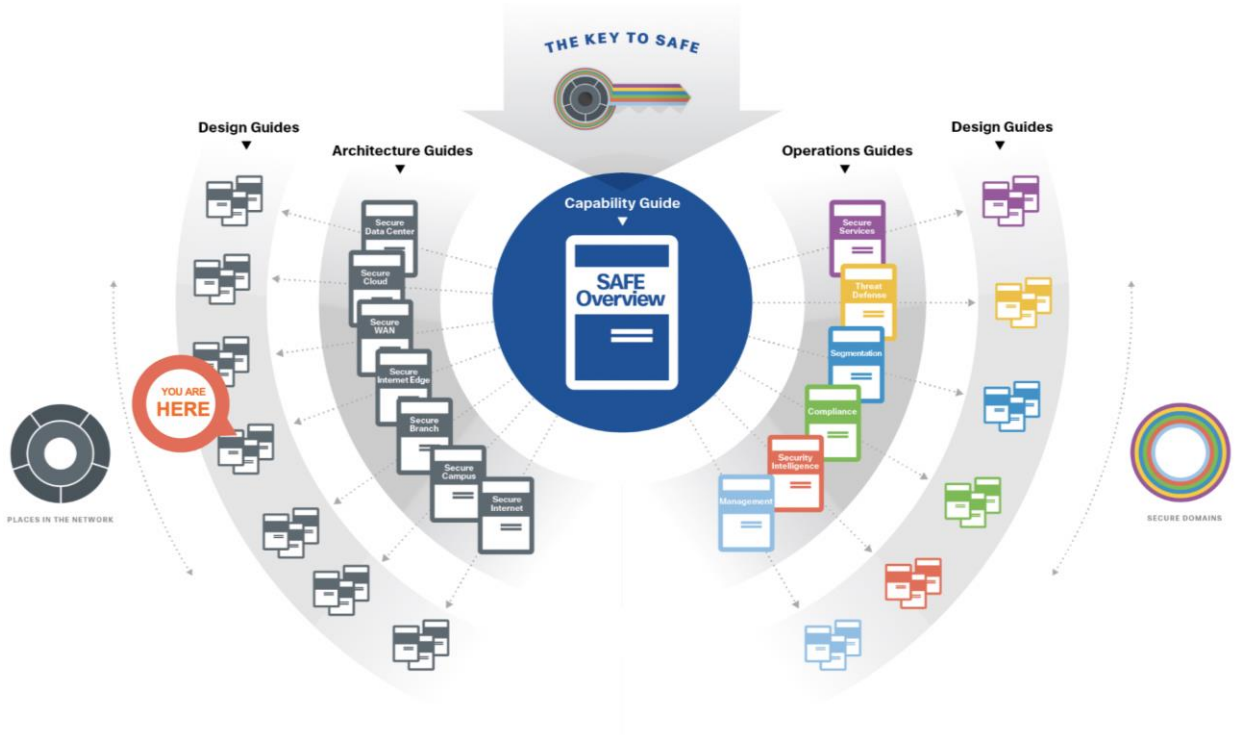


Figure 3. **SAFE Architecture and Design Guides**

More information about how Cisco SAFE simplifies security, along with this and other Cisco Validated Designs (CVD), can be found here.

Business Flow and Threat Capabilities

Business Flows: SAFE uses the concept of business flows to simplify the identification of threats, and this enables the selection of capabilities necessary to protect them. Secure Remote Worker has remote users accessing applications hosted in the secured environment.

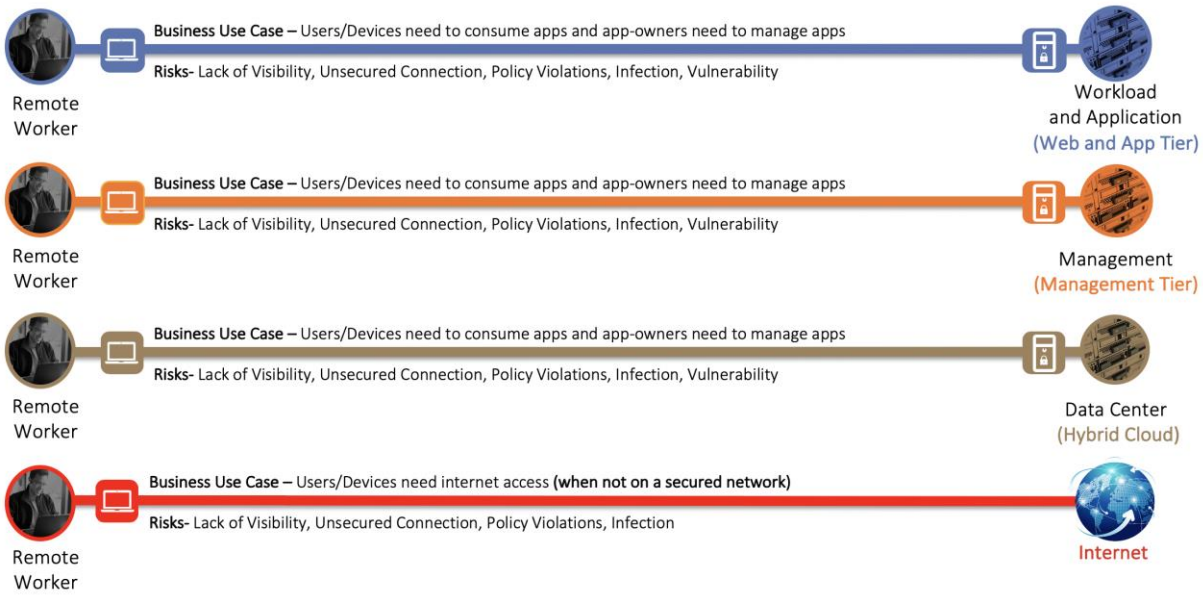


Figure 4. **The Secure Remote Worker (AWS) Business Flow**

Threat Capabilities: A secure remote worker is simplified using foundational, access, and business capability groups. Each flow requires the foundational group. Additional business activity risks need appropriate controls as shown in the Figure 5. User and Device capabilities are located where the flow originates from a remote worker to AWS VPC. For more information regarding capability groups, refer to the SAFE Overview Guide.

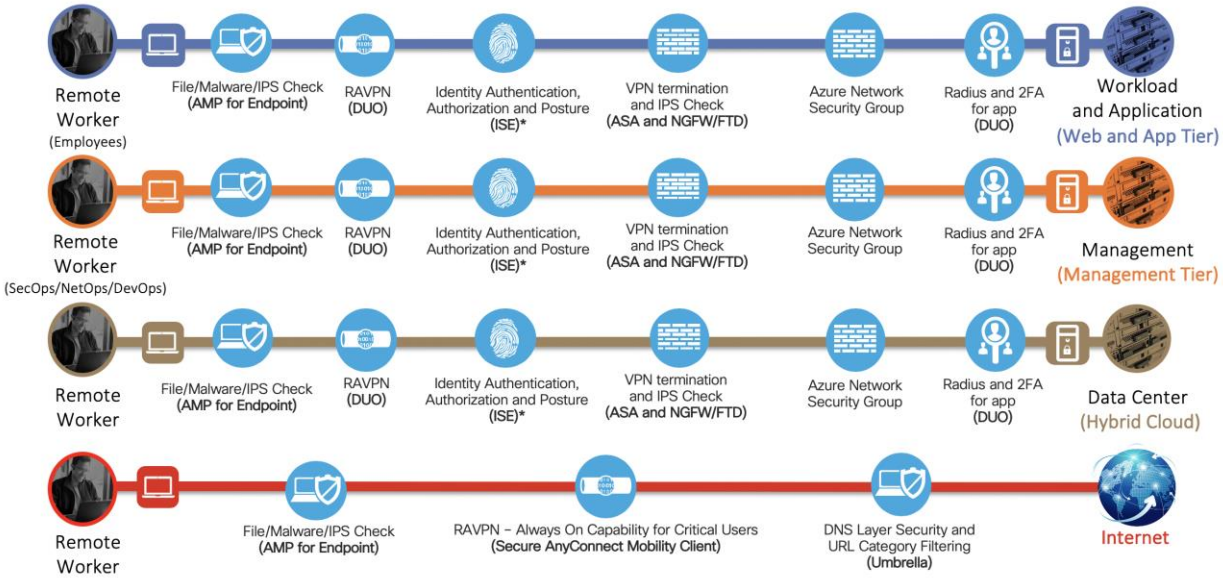


Figure 5. **Threat Capabilities for business flows**

*ISE is not part of this design guide

Cisco Overview

This Cisco validated design guide (CVD) covers the following devices and modules to extend security to remote workers.

Devices / Modules	Functionality
Cisco Secure AnyConnect Mobility Client	VPN Client for endpoints
Cisco Adaptive Security Appliance (Virtual) - ASAv	VPN Gateway / VPN concentrator
Cisco Firepower Next-Generation Firewall (Virtual) - NGFWv	VPN Gateway / VPN concentrator
Cisco Duo	Multi-factor authentication
Cisco Umbrella Roaming Security Module	DNS layer security
Cisco AMP Enabler	File/Malware/IPS Check

Cisco AnyConnect Secure Mobility Client: Cisco AnyConnect Secure Mobility Client is available for Windows, Mac, and Linux (64-bit) OS. It provides secure connectivity using TLS, DTLS, and IPSec VPN terminated on Cisco ASAv and Cisco NGFWv for remote access VPN (RAVPN)

Cisco Adaptive Security Virtual Appliance (ASAv): The Cisco adaptive security virtual appliance is a security appliance that protects the cloud environment. It provides users with highly secure access to cloud resources - anytime, anywhere. The remote users can use Cisco AnyConnect Secure Mobility Client on the endpoints to securely connect to the resources hosted in the Cloud. Cisco ASAv is available in AWS Marketplace and supports "Bring your own license (BYOL)" and "Pay-as-you-go (PAY-G)" licensing models

Cisco ASAv provides a wide range of license entitlement options:

ASAv Models
ASAv5, ASAv10, ASAv30, ASAv50, ASAv100

Cisco ASAv offers flexible management options:

Management Options	Detail
Command Line Interface (CLI)	On-box configuration
Adaptive Security Appliance Device Manager (ASDM)	On-box manager
Cisco Defense Orchestrator (CDO)	Cloud-based (multi-device manager)
Cisco Security Manager (CSM)	On-premise (multi-device manager)
Application Programing Interface (API)	Configuration, monitoring and orchestration

Cisco Next-Generation Firewall Virtual / Firepower Threat Defense Virtual (NGFWv): The Cisco Firepower NGFW Virtual (NGFWv) helps you prevent breaches, get visibility to stop threats fast, and automate operations to save time. A next-generation firewall virtual is a network security device that provides capabilities beyond a traditional, stateful firewall by adding capabilities like virtual private network (VPN) application visibility and control (AVC), Next-Generation IPS (NGIPS), URL filtering, and Advanced Malware Protection (AMP). Cisco

NGFWv is available in AWS Marketplace and supports "Bring your own license (BYOL)" and "Pay-as-you-go (PAY-G)" licensing models.

Cisco NGFWv has the following flexible management and configuration options:

Management Options	Detail
Firepower management center (FMC)	Centralized Manager
Firepower Device Manager (FDM)	On-box manager
Cisco Defense Orchestrator (CDO)	Cloud-based (multi-device manager)
Application Programing Interface (API)	Configuration, monitoring and orchestration

Cisco Duo: Cisco Duo integrates with Cisco ASA or Cisco Firepower Threat Defense (FTD) VPN to add two-factor authentication for AnyConnect logins. Duo supports two-factor authentication in a variety of ways:

- **ASA-SSL VPN using SAML:** With this configuration, end-users experience the interactive Duo prompt when using the Cisco AnyConnect Mobility Client for VPN. The interactive MFA prompt gives users the ability to view all available authentication device options and select which one to use. This administrator gets insight into the devices connecting to the VPN and applies Duo policies such as health requirements or access policies for different networks (authorized networks, anonymous networks, or geographical locations as determined by IP address) when using the AnyConnect Mobility Client. Primary authentication and Duo MFA occur at the identity provider, not at the ASA itself
- **ASA SSL VPN using RADIUS:** With this configuration, end-users receive an automatic push or phone call for multi-factor authentication after submitting their primary credentials using the AnyConnect Mobility Client or clientless SSL VPN via browser. This configuration supports Duo policies for different networks (authorized networks, anonymous networks, or geographical locations as determined by IP address) when using the AnyConnect client
- **ASA SSL VPN using LDAPS:** Using this option with the clientless SSL VPN, end-users experience the interactive Duo prompt in the browser. The AnyConnect client does not show the Duo prompt and instead adds a second password field to the regular AnyConnect login screen where the user enters the word “push” for Duo Push, the word “phone” for a phone call, or a one-time passcode. This configuration does not support IP-based network policies or device health requirements when using the AnyConnect client
- **FTD VPN using RADIUS:** Choose this option for Cisco Firepower Threat Defense (FTD) Remote Access VPN. With this configuration, end-users receive an automatic push or phone call for multi-factor authentication after submitting their primary credentials using the AnyConnect Mobility Client or clientless SSL VPN via browser. Users may append a different factor selection to their password entry. This configuration supports Duo policies for different networks (authorized networks, anonymous networks, or geographical locations as determined by IP address) when using the AnyConnect client

For detailed information on the above authentication methods, checkout the following links:

https://duo.com/docs/cisco

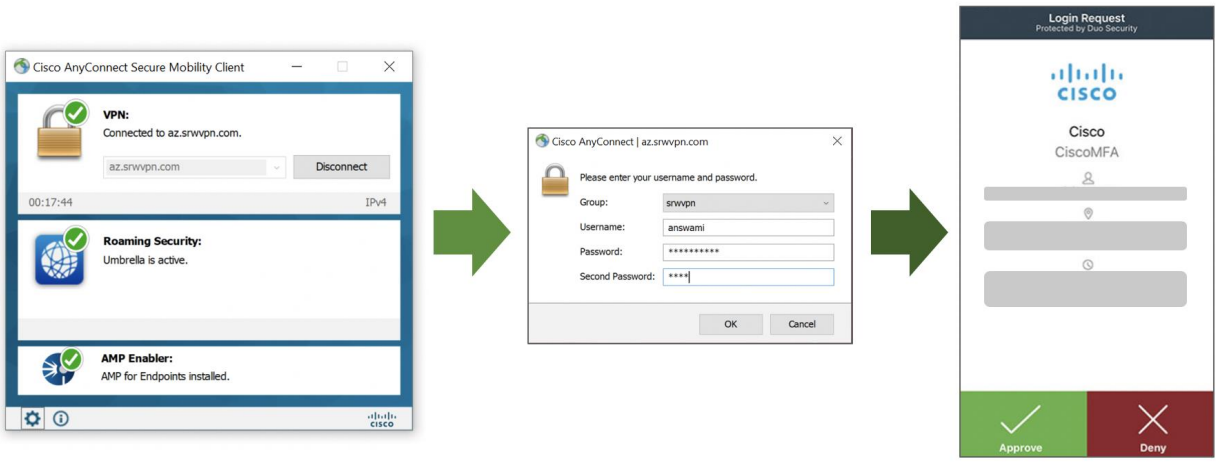


Figure 6. **Cisco Duo**

Cisco Umbrella Roaming Security Module: The Cisco Umbrella Roaming Security module for Cisco AnyConnect provides always-on security on any network, anywhere, any time – both on and off VPN. The Roaming Security module enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port. Umbrella provides real-time visibility into all internet activity per hostname both on and off your network or VPN.

License requirement to enable Umbrella Roaming Security Module:

License	Functionality
Cisco Umbrella Roaming service	Basic DNS-layer security

The same Umbrella Roaming Security module is used regardless of the subscription. Subscription is required to enable features.

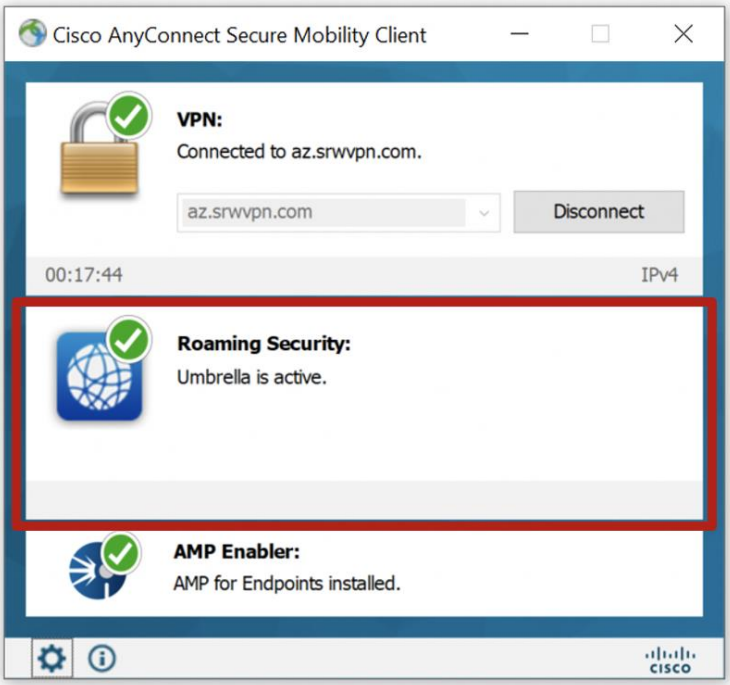


Figure 7. **Cisco Umbrella Roaming Security Module**

Cisco AnyConnect AMP Enabler: Cisco AnyConnect AMP Enabler is used as a medium for deploying Advanced Malware Protection (AMP) for Endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base. This approach provides AnyConnect user base administrators with an additional security agent that detects potential malware threats happening in the network, removes those threats, and protects the enterprise from compromise. It saves bandwidth and time taken to download, requires no changes on the portal side, and can be done without authentication credentials being sent to the endpoint. AnyConnect AMP Enabler protects the user both on and off the network or VPN.

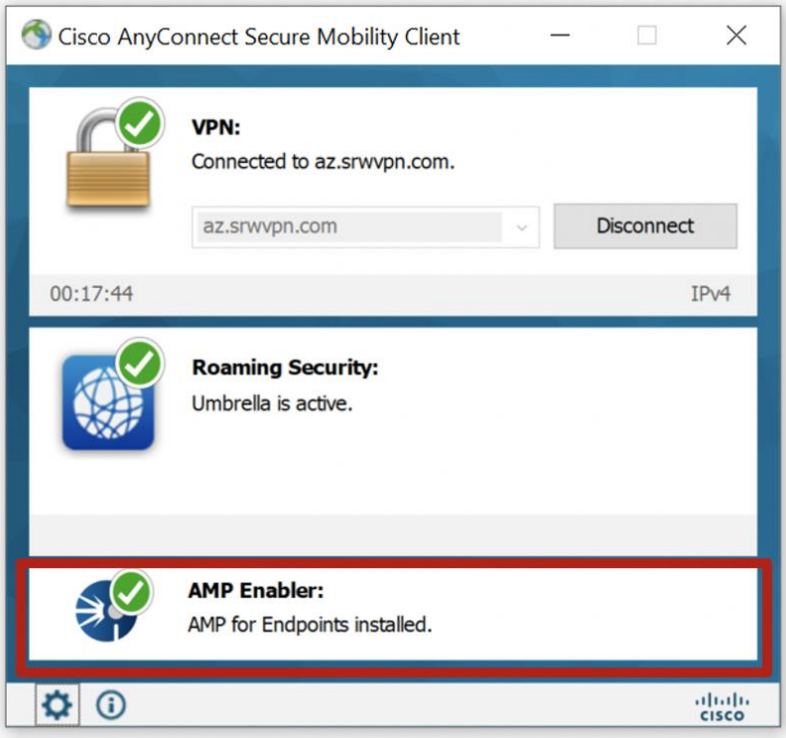


Figure 8. **Cisco AMP Enabler**

License requirement to enable AMP Enabler:

https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/package-comparison.html

Product	License
Cisco AMP license	Essential, Advantage or Premier

Security Integration

Let's look at the security integration covered in this design guide. We will start with a VPN configuration on the firewall. Once firewalls are ready to accept VPN connection, we will then integrate the Cisco firewall with the following security controls to get the desired security, visibility, and threat protection.

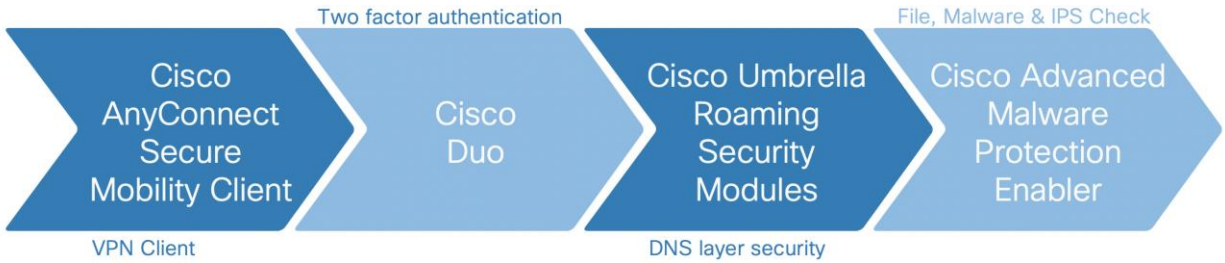


Figure 9. **Cisco Security Integration for Secure Remote Worker**

It is essential to configure the AWS network before implementing the above security controls—the design implementation section has detailed information on Network Integration.

NOTE: Cisco Duo, Umbrella, and AMP offer EU based locations for customers having to follow EU rules.

Amazon Web Services Overview

Amazon Web Services (AWS) is a public cloud service provider for building, testing, deploying, managing applications and services. AWS is amongst few leaders in a public cloud provider that offers infrastructure as a service (IaaS), platform as a service (PaaS), container as a service (CaaS), function as a service (FaaS), and software as a service (SaaS). This document covers how a remote access VPN user securely access the cloud resources using Cisco AnyConnect secure mobility client and other security modules.

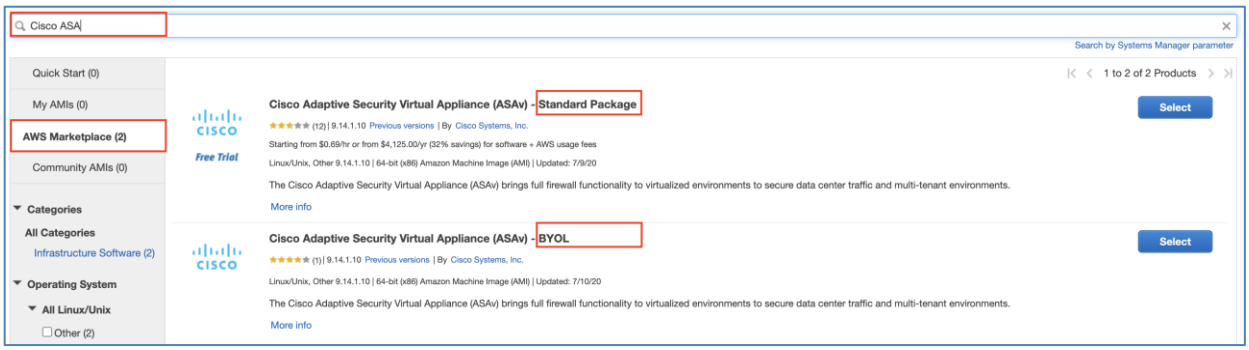
Before we dive into the secure architecture, it is essential to define the importance of network-related services used in the document. AWS offers a wide range of network services that will integrate with the Cisco security portfolio to provide an unmatched secure remote worker experience. This Cisco validated design guide (CVD) covers the following AWS services to build a highly secure and resilient architecture for Cisco Secure Remote Worker.

- **AWS Virtual Private Cloud (VPC):** AWS VPC is a logically isolated section of the AWS cloud. It provides complete control over the virtual networking environment, including selection of your customized IP address range, creation of subnets, and configuration of route tables and network gateways (AWS Documentation)
- **AWS Availability Zone (AZ):** AWS locations are composed of Regions and Availability Zones. Each Region is a separate geographic area. Each Region has multiple, isolated locations known as Availability Zones. Availability Zone is a separate data center with separate network connection, power and cooling (AWS Documentation)
- **AWS Route Table (RT):** A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed (AWS Documentation)
- **AWS Internet Gateway (IGW):** An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet (AWS Documentation)
- **AWS Transit Gateway (TGW):** AWS transit gateway acts as a cloud router that connects VPCs and on-premises networks through a central hub. (AWS Documentation)
- **AWS Security Group (SG):** AWS security group (SG) acts as a virtual firewall for your EC2 instance to control inbound and outbound traffic. AWS security group controls traffic on five-tuple information (AWS Documentation)
- **AWS EC2 instance (EC2):** Amazon Elastic Compute Cloud is a virtual machine in AWS (AWS Documentation)
- **AWS Elastic Network Interface (ENI):** An elastic network interface is a logical networking component in a VPC that represents a virtual network card (AWS Documentation)
- **AWS Elastic IP (EIP):** AWS EIP is a public IP address mapped to the EC2 instance (AWS Documentation)
- **AWS Route53:** AWS Route 53 is a highly available and scalable cloud DNS service. It is designed to integrate with AWS services (AWS Documentation)

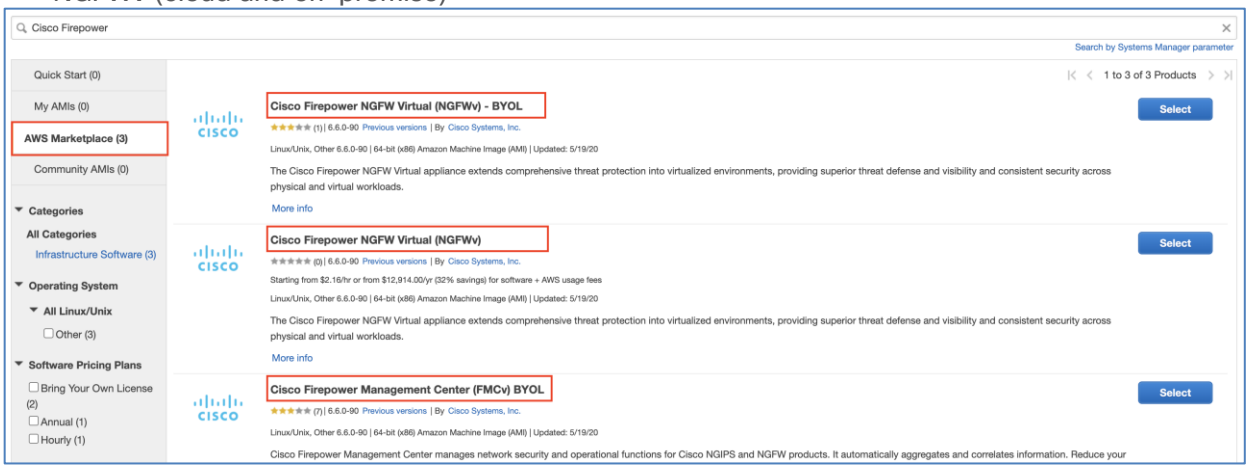
AWS Marketplace Listing

Cisco offers Cisco ASAv, NGFWv, and FMCv in AWS Marketplace.

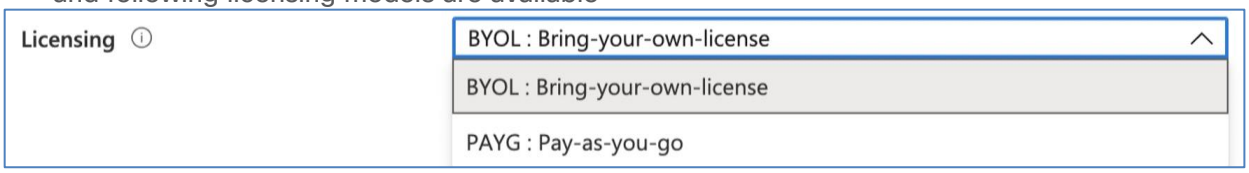
- Cisco Adaptive Security Appliance Virtual (ASAv): ASAv has two listings (Standalone and High Availability); this CVD covers multiple standalone devices for VPN load balancing



- Cisco Firepower Next-Generation Firewall Virtual (NGFWv) & Cisco Firepower Management Center Virtual (FMCv): Cisco NGFWv and FMCv are available in the AWS market, Cisco FMCv can manage up to 25 NGFWv (cloud and on-premise)



- Supported Licensing Model for ASAv and FTDv instance: Instances are licenses using Cisco smart licensing and following licensing models are available



- Bring-your-own-license (BYOL): Customers can use licenses available in their smart account on cisco firewalls deployed in AWS
- Pay-as-you-go (PAYG): This option enables a full-featured firewall, and customers are billed directly by AWS for compute and device licenses

Cisco ASAv and NGFWv supported instance type

Cisco ASAv supports the following mentioned instance types only (ASAv datasheet) enable license to support throughput.

AWS Instance Size	Supported License Entitlement
c3.large, c4.large, c5.large, m4.large	ASAv5
c3.large, c4.large, c5.large, m4.large	ASAv10
c3.xlarge, c4.xlarge, c5.xlarge, m4.xlarge	ASAv30

AWS Instance Size	Supported License Entitlement
c3.2xlarge, c4.2xlarge, c5.2xlarge, m4.2xlarge	ASAv50
c5.4xlarge, c5n.4xlarge	ASAv100

Cisco Firepower Next-Generation Firewall supports the following mentioned instance types only (NGFWv datasheet) enable license to support throughput and the maximum number of VPN endpoints.

AWS Instance Size	Device
c3.xlarge, c4.xlarge, c5.xlarge, c5.2xlarge, c5.4xlarge	NGFWv

Note: c5.2xlarge and c5.4xlarge can have upto eight interfaces.

Cisco Firepower Management Center (FMCv) supports management of NGFWv provisioned in AWS or outside AWS.

AWS Instance Size	Device	Maximum NGFWv firewall management support
c3.4xlarge, c4.4xlarge, c5.4xlarge	NGFWv	25

Note: Refer to our datasheets for updated VPN numbers and throughput.

Cisco Secure Remote Worker Architecture for AWS

Today more and more organizations are consuming services, workloads, and applications hosted in AWS. AWS provides a wide range of services that offer ease of usability, orchestration, and management. Customers are embracing these services, but this resource consumption model opens another attack surface. Using Cisco Security controls, customers can provide a secure connection to the AWS cloud infrastructure.

This remote access VPN architecture protects multi-VPC, multi-AZ (availability zone) by extending the Cisco Secure Remote Worker solution. This Architecture brings together Cisco Security and AWS Infrastructure-as-a-service (IaaS) and extends remote access VPN capabilities with Duo, Umbrella, and AMP Enabler.

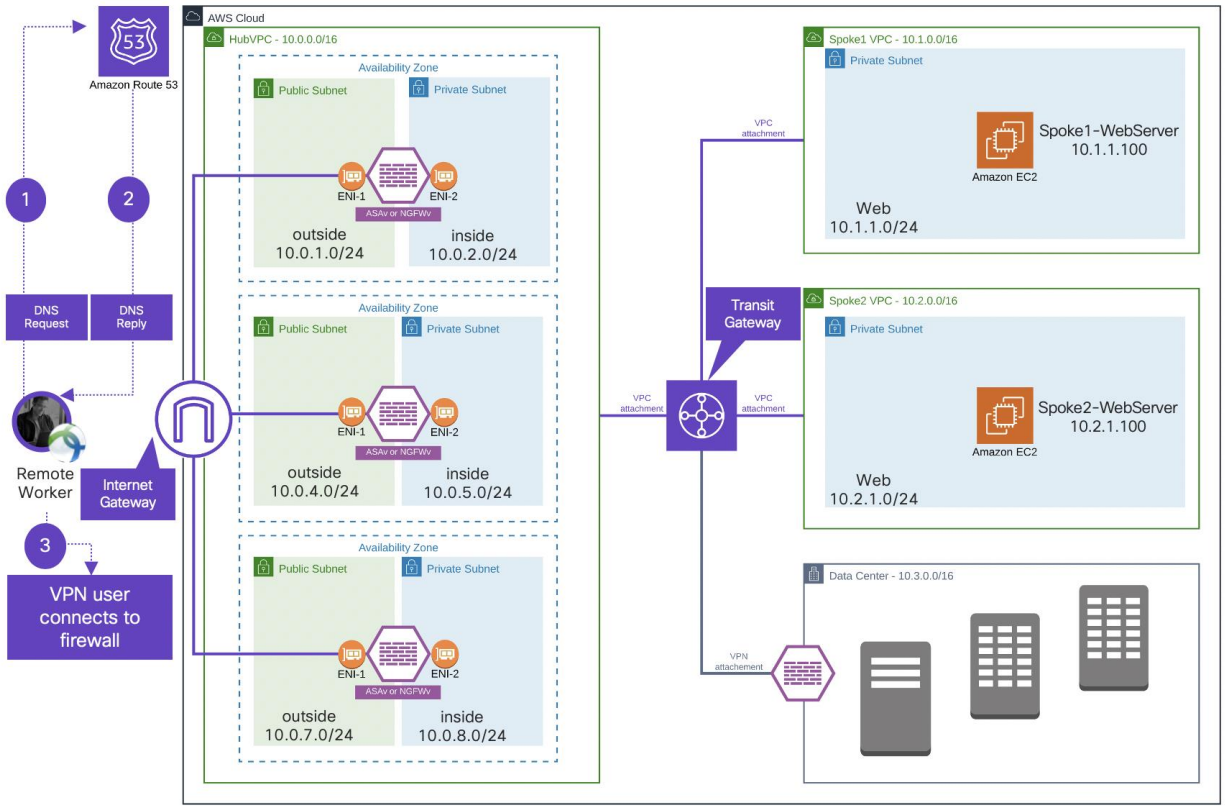


Figure 10. **Secure Remote Worker architecture for multi-VPC, multi-availability zone**

The above network design has the following components and services:

- Cisco ASAv or Cisco NGFWv for SSL VPN termination (TLS and DTLS)
- Cisco Secure Anyconnect Mobility Client on the endpoints
- Authentication
  - Microsoft Windows 2019 Active Directory (LDAP)
- Threat protection
  - Umbrella Security Roaming Module (DNS layer security)
  - AMP Enabler (File, IPS, and Malware policies)
- AWS Hub and Spoke model
  - AWS transit gateway to connect VPCs

- AWS Route53 to load balance remote access VPN (RAVPN)
- AWS Security Group on workloads for micro-segmentation
- AWS availability Zone for fault domains
- AWS Internet Gateway for internet connectivity
- AWS route table for routing
- AWS transit gateway for connection to the Data Center (not in scope)

Traffic Flow

North-South traffic flow (VPN traffic): AWS blocks layer-2 visibility required for native HA and VPN load balancing. To enable resiliency and VPN load balancing, one must rely on the native cloud services such as AWS Route 53 and AWS route table. In this architecture, VPN users send a DNS query to AWS Route 53 and receive the Cisco Firewall's IP address, then make an SSL VPN connection to the firewall. AWS route 53 tracks all the firewalls using health-checks, and it load-balances VPN connection endpoints (Cisco Firewalls).

- Each Cisco Firewall would have separate VPN pool CIDR
- To maintain symmetry, AWS route in subnet sends traffic back to the correct firewall
- Traffic uses AWS transit gateway to reach the spoke VPC
- Each AZ should have multiple firewalls

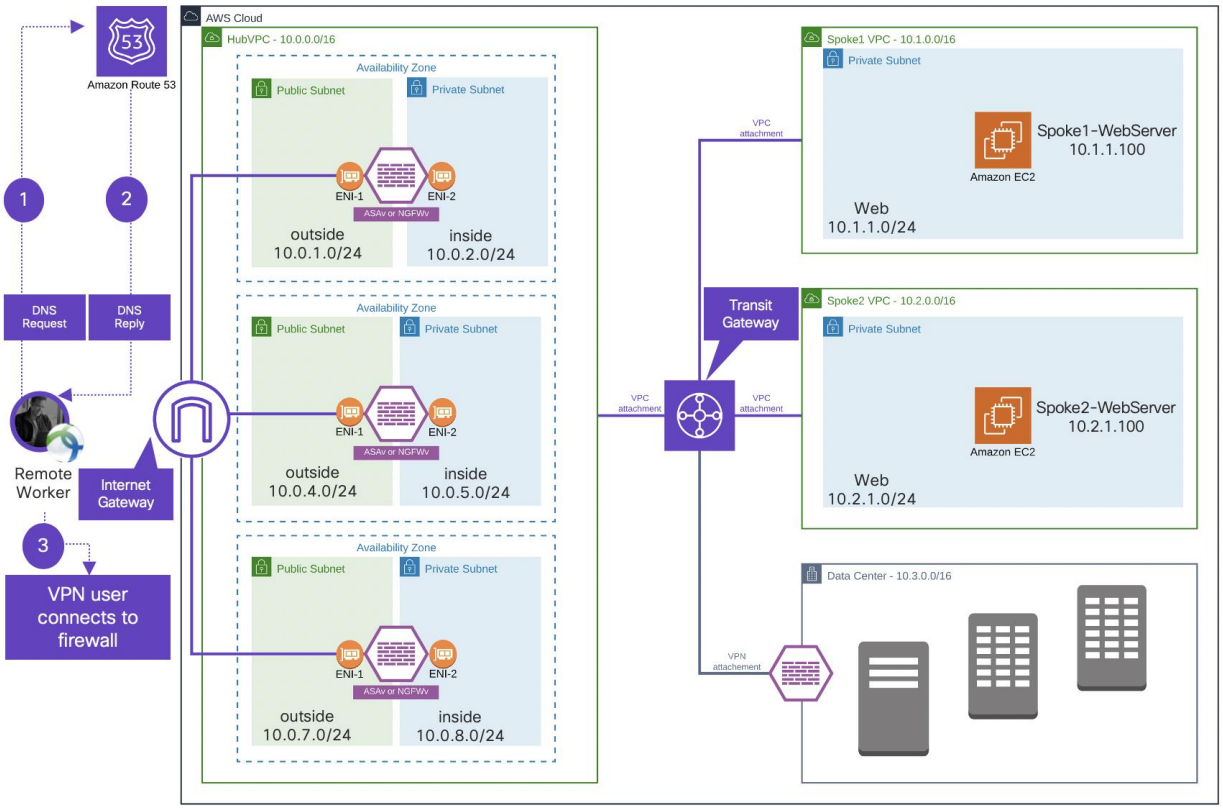


Figure 11. **North-South traffic flow (VPN)**

Inbound traffic flow (non-VPN traffic): For inbound non-VPN traffic, we used AWS Network Load Balancer (NLB). NLB keeps monitor the health of each firewall in the backend pool. Traffic lands on NLB using NLB's

DNS/FQDN, then NLB load balances traffic to the firewall, and all ingress traffic is translated to inside interfaces so that return traffic will come back to the same firewall.

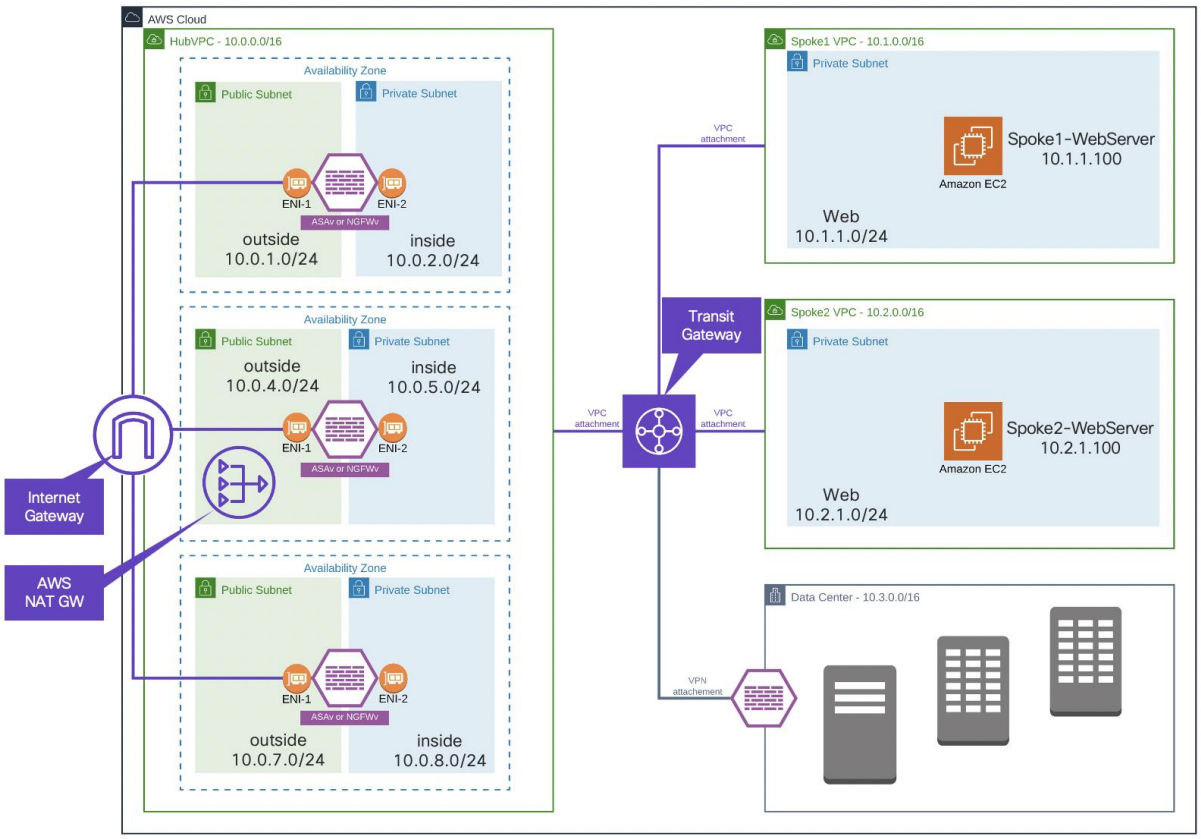


Figure 12. **Figure12. Inbound traffic flow (non-VPN traffic)**

Outbound traffic flow (non-VPN traffic): For outbound non-VPN traffic, we used AWS NAT gateway (NAT GW). Here is the detailed traffic flow:

- Route table associated with Spoke1/2 VPC has a default route that points to AWS Transit Gateway
- Transit Gateway route table has a default route that points to HubVPC
- Private subnet in HubVPC has a route-table which contains a default route that points to NAT gateway
- Public subnet is HubVPC has a route-table that contains routes for spoke-VPCs that points to AWS transit gateway

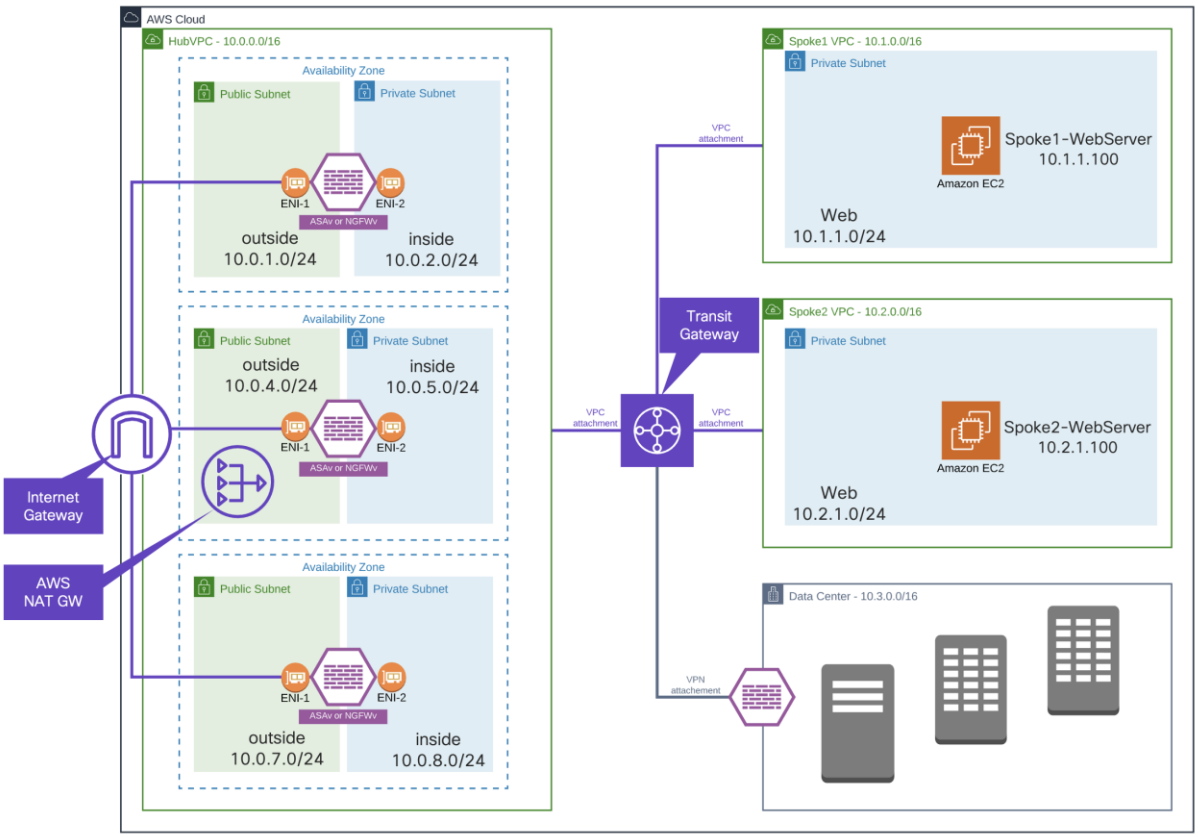


Figure 13. **Outbound traffic (non-VPN traffic) uses AWS NAT gateway**

Remote access VPN key capabilities for traffic and threat management

Static Split Tunnel versus Dynamic Split Tunnel

The default behavior of a VPN client is to tunnel all traffic. The client sends everything through the tunnel unless the split tunnel is defined. Split tunnels are of two types static and dynamic.

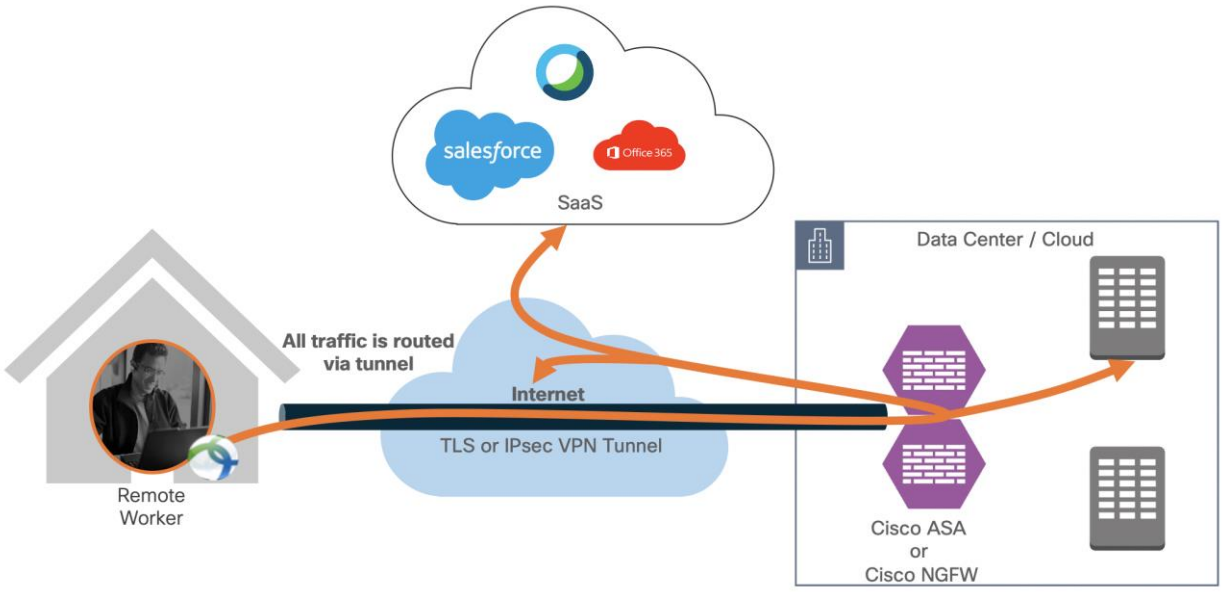


Figure 14. **Remote employee accessing resources hosted in the data center (tunnel-all)**

Static Split Tunnel

Static split tunneling involves defining the IP addresses of hosts and networks that should be included in or excluded from the remote access VPN tunnel. The limitation of the static split tunnel is that it is based on IP addresses defined in the split tunnel ACL. You can enhance split tunneling by defining dynamic split tunneling.

```
access-list stunnel standard permit IP 10.82.0.0 255.255.0.0
group-policy vpn-user attributes
split-tunnel-network-list value stunnel
```

The above configuration pushes the route for 10.1.0.0 255.255.0.0 network to the VPN client. The VPN client only sends traffic for 10.1.0.0/16 through the tunnel. Traffic not destined for 10.1.0.0/16 network is not part of the VPN tunnel.

FTD configuration example for split tunnel: Link

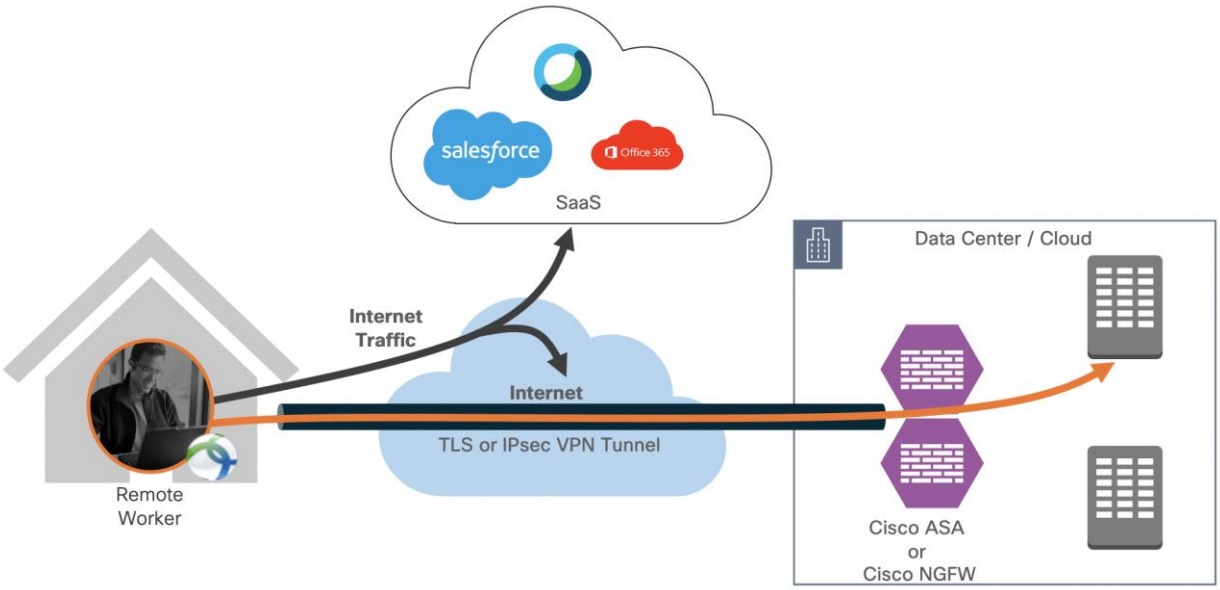


Figure 15. **Traffic destined for 10.1.0.0/16 is sent through the VPN tunnel, other traffic is exempted from VPN tunnel**

Dynamic Split Tunnel

With dynamic split tunneling, you can fine-tune split tunneling based on DNS domain names. Because the IP addresses associated with full-qualified domain names (FQDN) can change or simply differ based on region, defining split tunneling based on DNS names provides a more dynamic definition of which traffic should, or should not, be included in the remote access VPN tunnel. If any addresses returned for excluded domain names are within the address pool included in the VPN, those addresses will then be excluded. Excluded domains are not blocked. Instead, traffic to those domains is kept outside the VPN tunnel.

Example: you could send traffic to Cisco WebEx, salesforce and Office365 on the public Internet, thus freeing bandwidth in your VPN tunnel for traffic that is targeted to servers within your protected network.

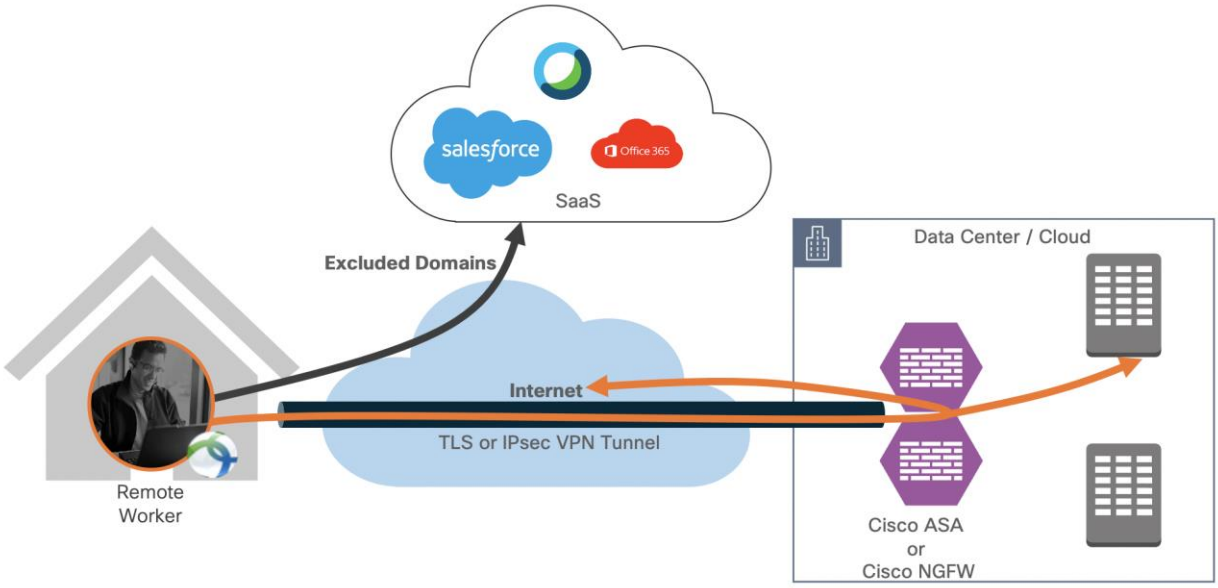


Figure 16. **Dynamic split tunnel applied (exclude traffic destined to exclude domains)**

Cisco ASA natively supports a "dynamic split-tunnel" feature. On the Cisco Next-Generation firewall, the dynamic split tunnel feature is configured using Flex-Config.

VPN always on

Always-On operation prevents access to Internet resources when the computer is not on a trusted network, unless a VPN session is active. Enforcing the VPN to always be on in this situation protects the computer from security threats.

When Always-On is enabled, it establishes a VPN session automatically after the user logs in and upon detection of an untrusted network. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer (specified in the ASA group policy) expires. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.

When Always-On is enabled in the VPN Profile, AnyConnect protects the endpoint by deleting all the other downloaded AnyConnect profiles and ignores any public proxies configured to connect to the ASA.

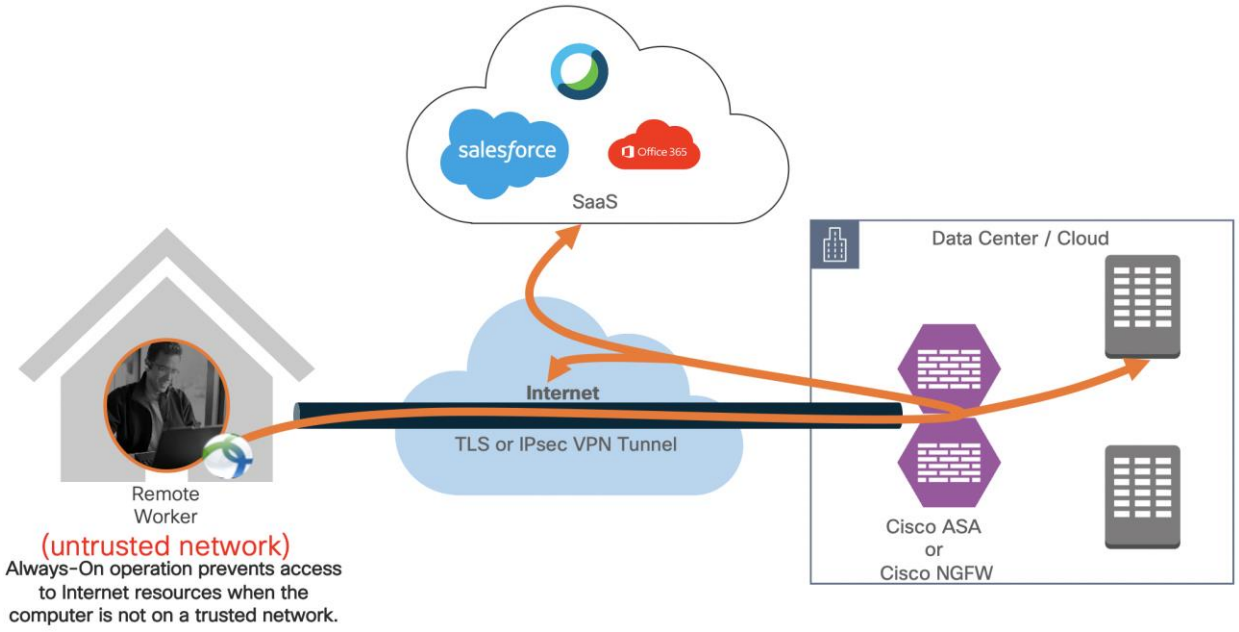


Figure 17. **VPN always on feature**

A remote worker is protected by the solutions mentioned above when the remote worker is on or off the VPN connection.

No VPN connection – Cisco AnyConnect modules provide protection when users are not on a VPN.

- Cisco Umbrella Roaming Module continues to provide DNS layer security
- Cisco AMP enabler continues to protect against the threats
- Cisco Duo continues to provide MFA for SaaS applications

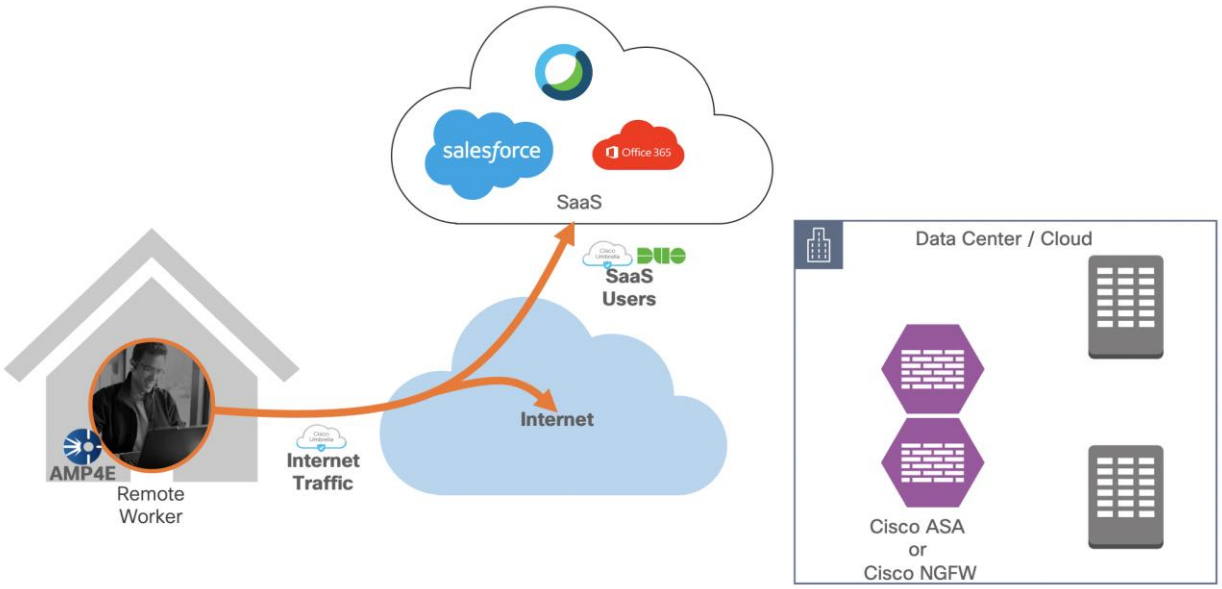


Figure 18. **Remote worker is not connected to VPN**

VPN without a split tunnel – Cisco AnyConnect modules provide protection when users are on a VPN and split tunnel is not enabled.

- Cisco Umbrella Roaming Module continues to provide DNS layer security

- Cisco AMP enabler continues to protect against the threats
- Cisco Duo continues to provide MFA for SaaS and Cloud applications

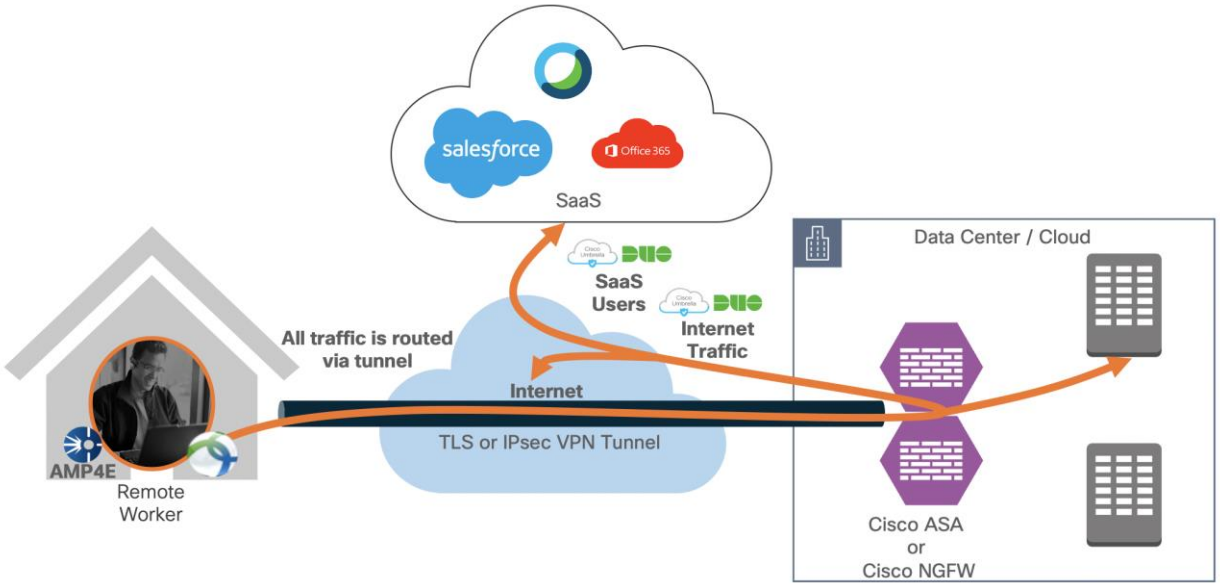


Figure 19. **Remote worker is on VPN (no split tunnel)**

VPN with a split tunnel – Cisco AnyConnect modules provide protection when users are on a VPN with a split tunnel enabled.

- Cisco Umbrella Roaming Module continues to provide DNS layer security
- Cisco AMP enabler continues to protect against the threats
- Cisco Duo continues to provide MFA for SaaS and Cloud applications

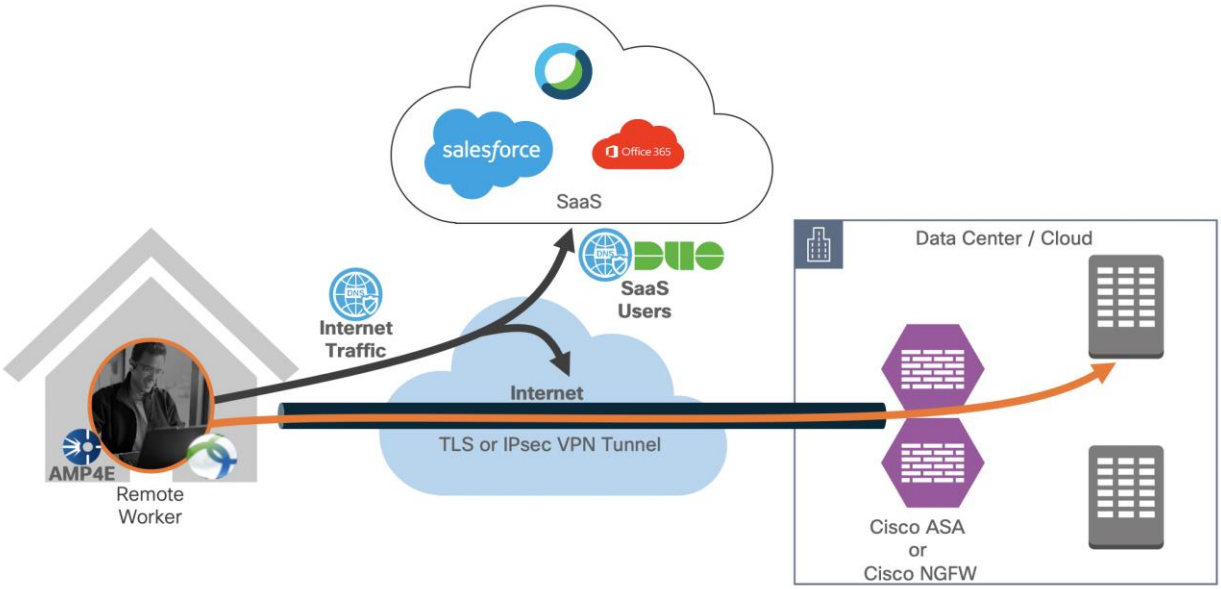


Figure 20. **Remote worker is on VPN (split tunnel)**

VPN with a dynamic split tunnel – Cisco AnyConnect modules provide protection when users are on a VPN with a dynamic tunnel enabled.

- Cisco Umbrella Roaming Module continues to provide DNS layer security

- Cisco AMP enabler continues to protect against the threats
- Cisco Duo continues to provide MFA for SaaS and Cloud applications
- Excluded domains are excluded from VPN encryption but still protected by Umbrella, and AMP

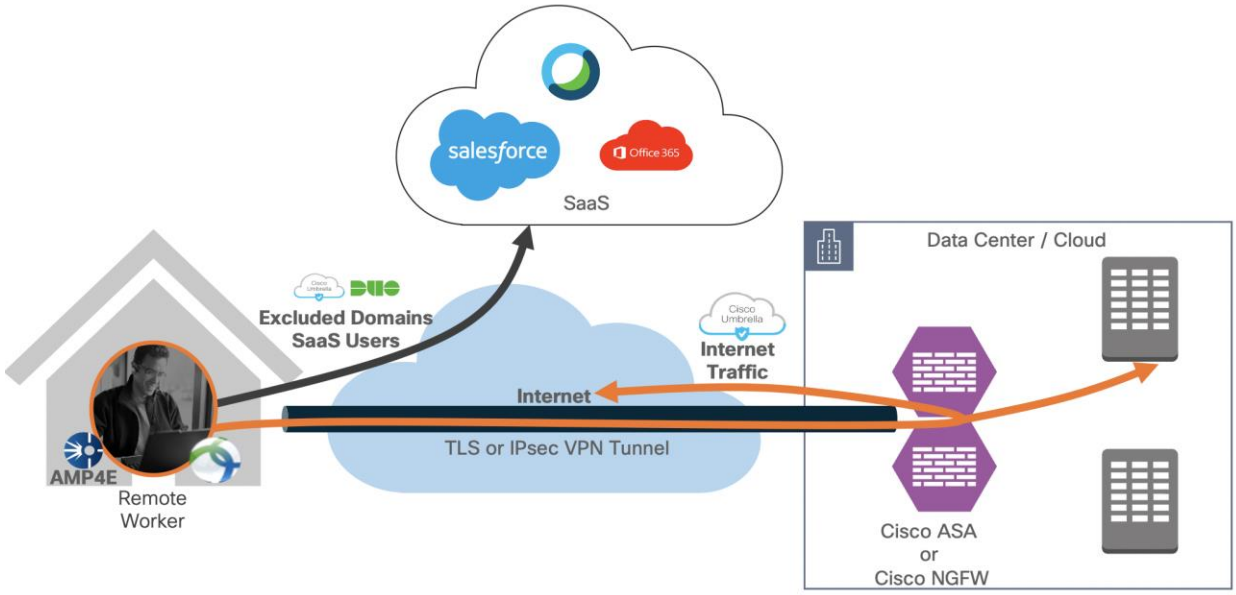


Figure 21. **Remote worker is on VPN (Dynamic split tunnel – exclude domain)**

VPN with always on VPN feature enabled - Cisco AnyConnect modules provide protection when users are on a VPN and split tunnel is not enabled.

- Cisco Umbrella Roaming Module continues to provide DNS layer security
- Cisco AMP enabler continues to protect against the threats
- Cisco Duo continues to provide MFA for SaaS and Cloud applications

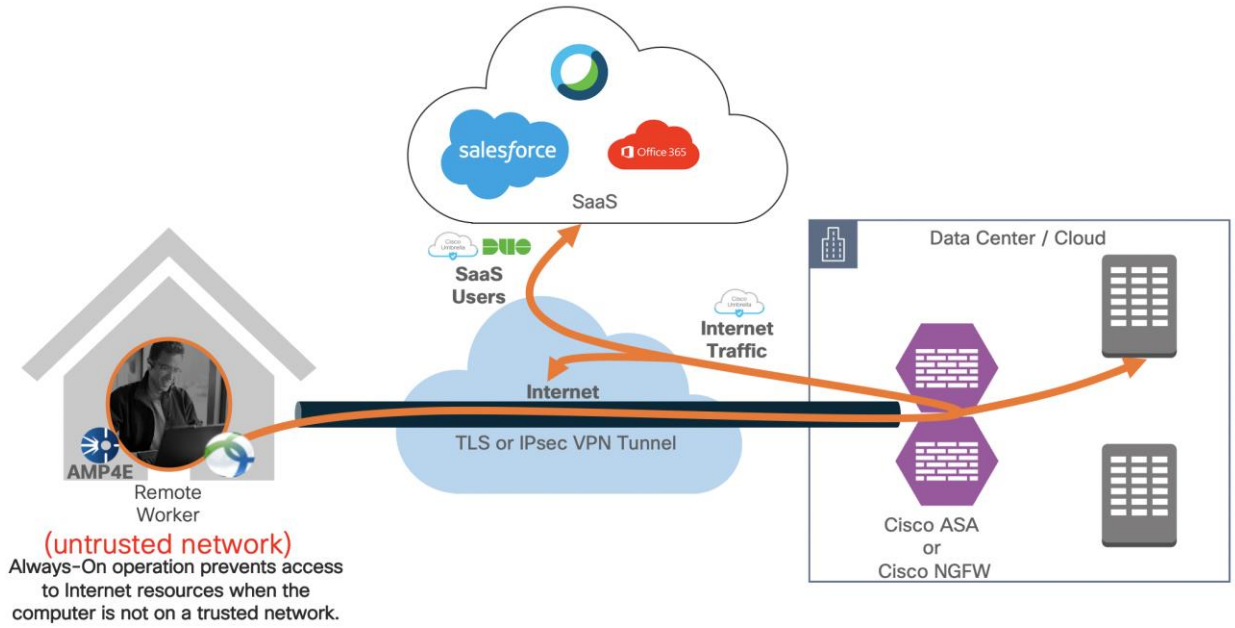


Figure 22. **Remote worker is on the trusted network (always-on-VPN)**

Non-VPN Remote worker (Duo Network Gateway)

Remote workers without Cisco Secure AnyConnect Mobility Client can use Cisco Duo Network Gateway to securely access internal web applications from any device, using any browser, from anywhere in the world. Users can also remotely SSH to configured hosts through Duo Network Gateway after installing Duo's connectivity tool, providing server access without a VPN.

Users first authenticate to Duo Network Gateway and approve a two-factor authentication request before they may access your different protected services. Session awareness minimizes repeated MFA prompts as users access additional services and hosts via your gateway.

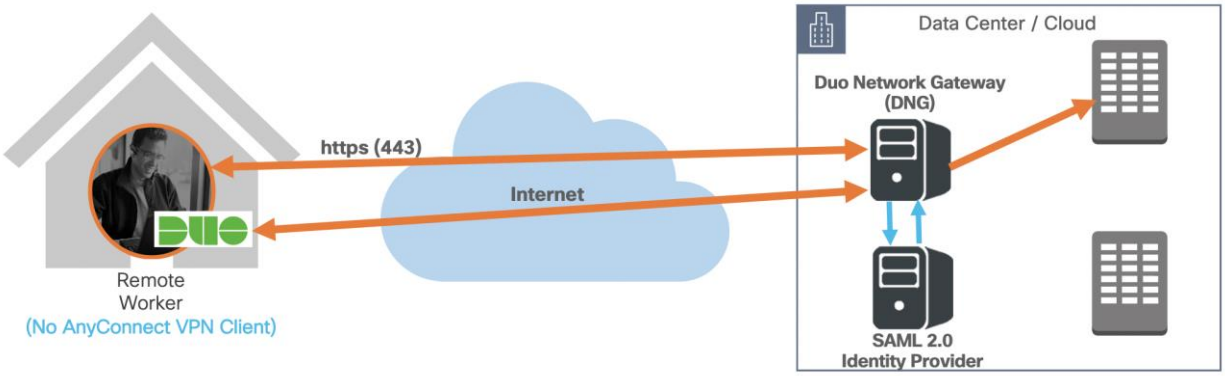


Figure 23. **Non-VPN remote worker (Duo Network Gateway)**

Duo Network Gateway: [DNG Documentation]

Design Implementation

Since we have covered the design specifics, we will begin implementing and setting up the AWS environment. We will start by setting up the AWS VPCs as per the design shown in the below diagram. Once VPCs are ready, we will attach an internet gateway to HubVPC, followed by a transit gateway attachment. Once our base network is ready, we will deploy ASAs and add ASAs in AWS route53 to load balance VPN sessions.

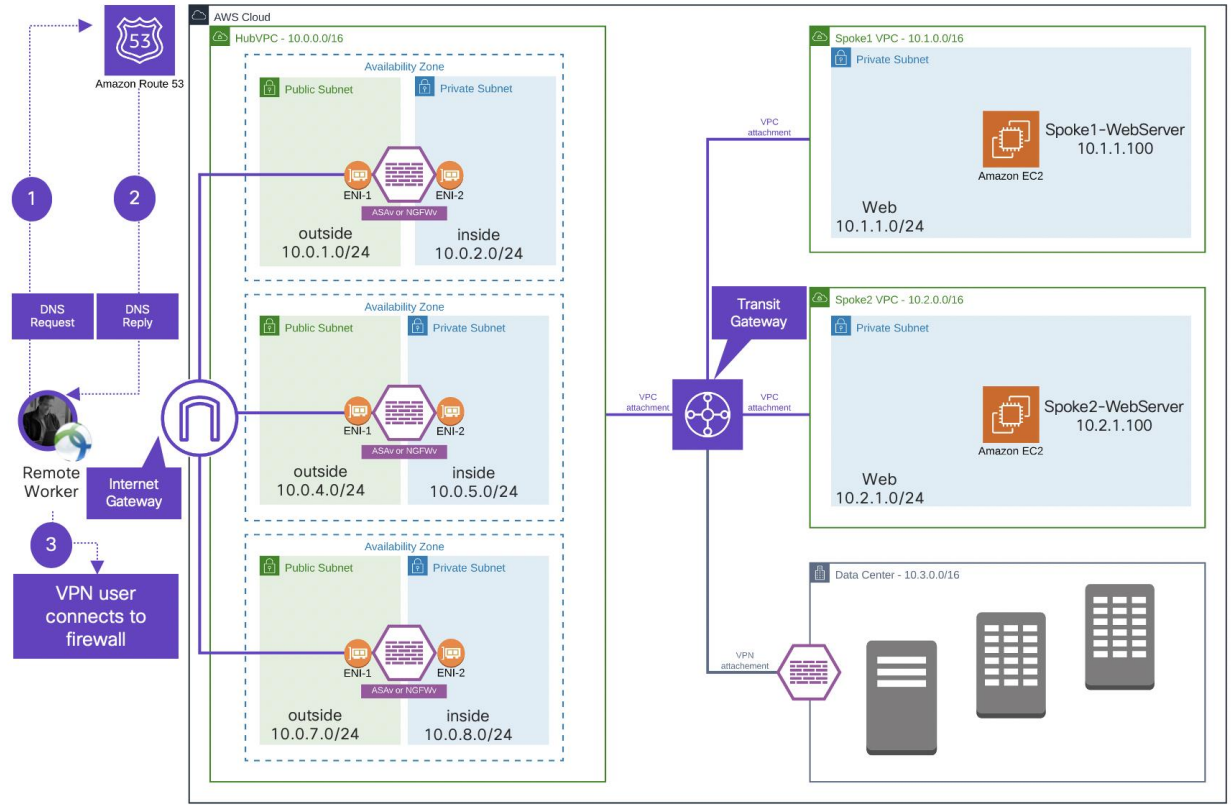


Figure 24. **Secure Remote Worker architecture for multi-VPC, multi-AZ**

Network Implementation Overview

- Set up the Infrastructure
  - Create VPCs and Subnets
  - Create Internet Gateway and attach internet gateway to the HubVPC
  - Deploy Transit Gateway and add VPCs
  - Deploy and Cisco Firewall (ASAv) in AZ1, AZ2, and AZ3
- Configure routing and VPN load balancing
  - Create and associate route tables
  - Configure VPN ASAs (HubASA1, HubASA2, and HubASA3)
  - Create and configure AWS route 53

Figure 25. **Network Implementation**

Security Implementation Overview

- Configure Cisco ASAv (enable VPN configuration)
- Integrate Cisco Duo for two-factor authentication
- Integrate Cisco Umbrella Roaming Security Module
- Integrate Cisco AMP Enabler

Figure 26. **Security Implementation**

Set up the AWS Infrastructure

In this section, we will create new AWS VPCs and configure all the associated components that we need for our deployment.

Implementation procedure:

- **Infrastructure Deployment**
  - **Step 1.** Create the VPCs
  - **Step 2.** Create the Subnets in each VPC
  - **Step 3.** Create Internet Gateway and attach it to the HubVPC
  - **Step 4.** Create Transit Gateway and attach VPCs
  - **Step 5.** Deploy ASAs and Workloads in VPCs
  - **Step 6.** Create, configure and associate route tables
  - **Step 7.** Configure VPN ASAs (HubASA01, HubASA02, and HubASA03)
  - **Step 8.** Configure AWS route53 for VPN load balancing
- **Authentication**
  - Configure LDAP authentication for RAVPN
    - **Step 1.** Add aaa-server group on ASAVs
    - **Step 2.** Edit aaa-server settings
    - **Step 3.** Change primary authentication in Anyconnect Connection Profile
  - **Enable two-factor authentication with Duo (LDAP with Duo)**
    - **Step 1.** Setup use on Duo portal
    - **Step 2.** Add Application on Duo portal
    - **Step 3.** Configure aaa-server (LDAP-Duo)
    - **Step 4.** Edit Duo-LDAP and add servers in the selected server group
    - **Step 5.** Edit AnyConnect VPN profile and add LDAP-Duo for two-factor authentication
    - **Step 6.** Download and install certificates on all ASAVs

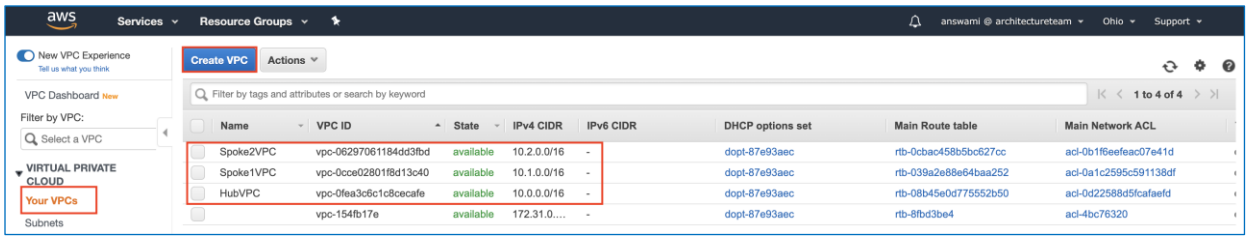
Step 7. Download and install Cisco Duo package on all ASAVs for clientless VPN

- **Threat Protection**
  - Umbrella Roaming Security Module
    - **Step 1.** Download Umbrella Roaming Security Module
    - **Step 2.** Setup AnyConnect Client Profile
    - **Step 3.** Enable Umbrella Roaming Security Profile
    - **Step 4.** Enable Umbrella DNS Security
  - **AMP** Enabler
    - **Step 1.** Create Endpoint Group for RAVPN users
    - **Step 2.** Create Endpoint Group policy for RAVPN users
    - **Step 3.** Download connectors for MAC, Windows, Linux, and Android
    - **Step 4.** Add AMP Enabler Service Profile
    - **Step 5.** Edit the Group-Policy to Download the AnyConnect AMP Enabler

Infrastructure Deployment

Step 1. Create the VPCs - Log on to the AWS console and search for 'VPC' service. Click on "Your VPCs" then click create VPC for each of the VPCs in the table below.

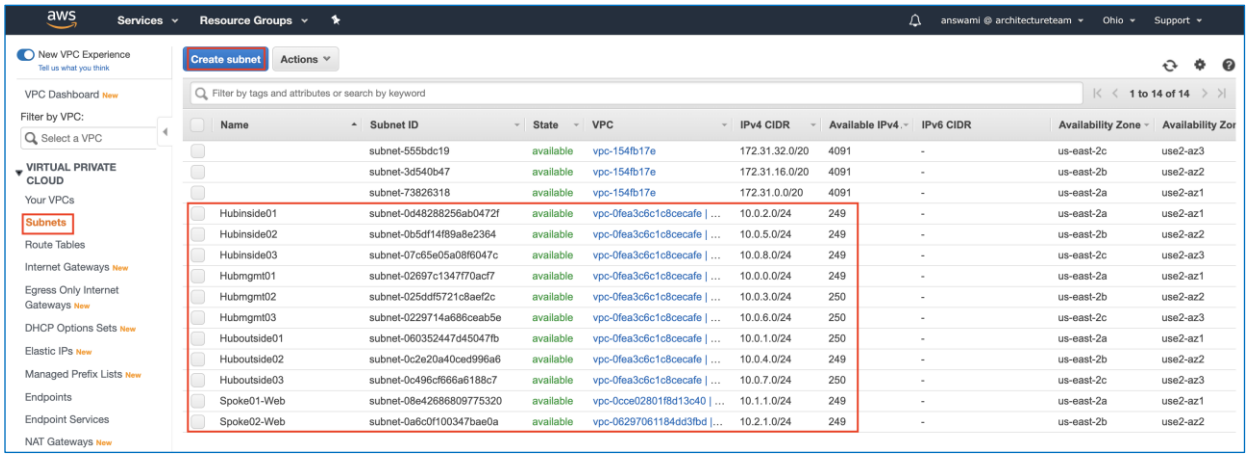
VPC Name	Subnets	Purpose
HubVPC	10.0.0.0/16	Hub
Spoke1VPC	10.1.0.0/16	Spoke1
Spoke2VPC	10.2.0.0/16	Spoke2



Step 2. Create Subnets in each VPC - Click on the VPC → Subnets → Create Subnets and create subnets in the table below.

VPC Name	CIDR	Name
HubVPC	10.0.0.0/24	Hubmgmt01
	10.0.3.0/24	Hubmgmt02
	10.0.6.0/24	Hubmgmt03
	10.0.1.0/24	Huboutside01

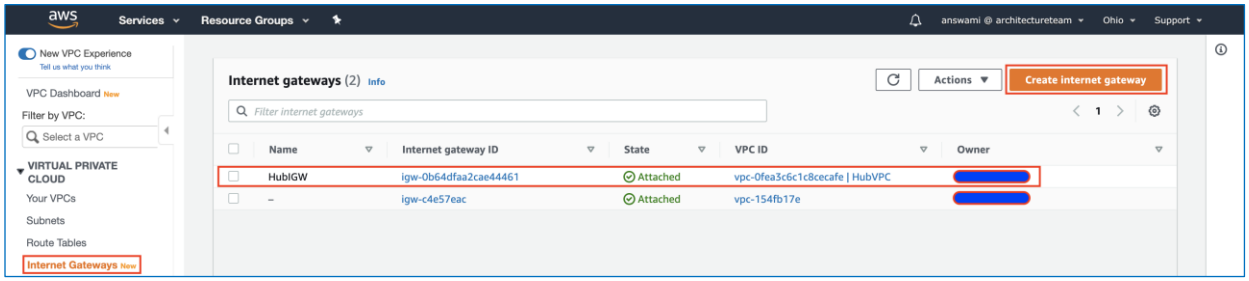
VPC Name	CIDR	Name
	10.0.4.0/24	Huboutside02
	10.0.7.0/24	Huboutside03
	10.0.2.0/24	Hubinside01
	10.0.5.0/24	Hubinside02
	10.0.8.0/24	Hubinside03
Spoke1VPC	10.1.1.0/24	Spoke01-Web
Spoke2VPC	10.2.1.0/24	Spoke02-Web



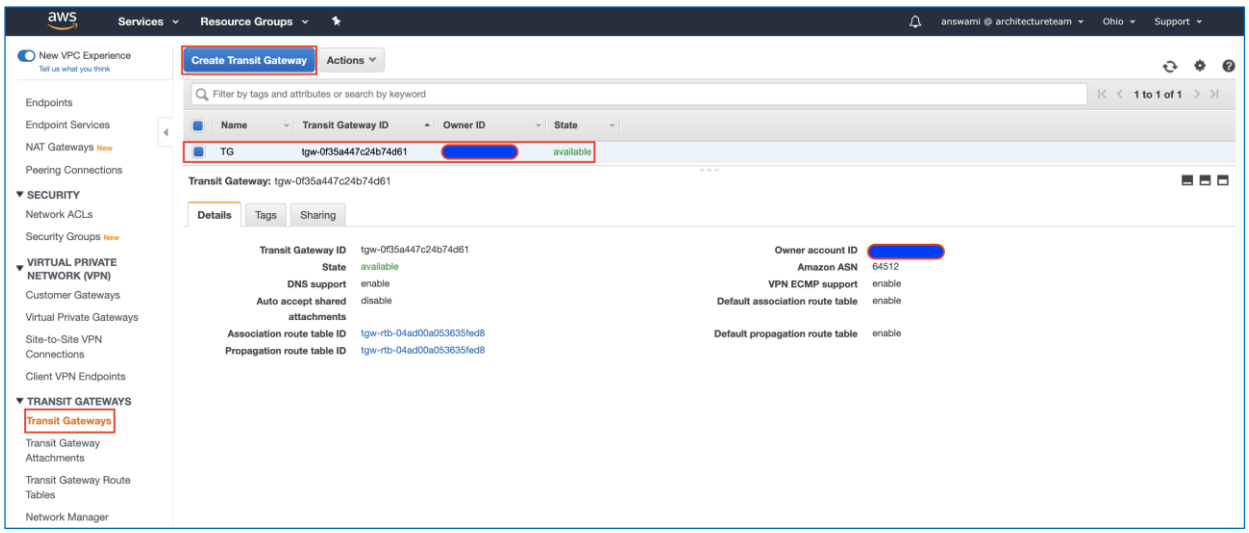
HubVPC has ASAs and it connects with Spoke1VPC and Spoke2VPC using the AWS transit gateway.

- HubASA1, HubASA2, and HubASA3
- Spoke01-Web01 (10.1.1.100)
    - Spoke1VPC has a Linux machine for testing
- Spoke02-Web02 (10.2.1.100)
    - Spoke2VPC has a Linux machine for testing

Step 3. Create Internet Gateway and attach it to HubVPC - Access AWS VPC service → click Internet Gateway → Create Internet Gateway and once created attach it to HubVPC

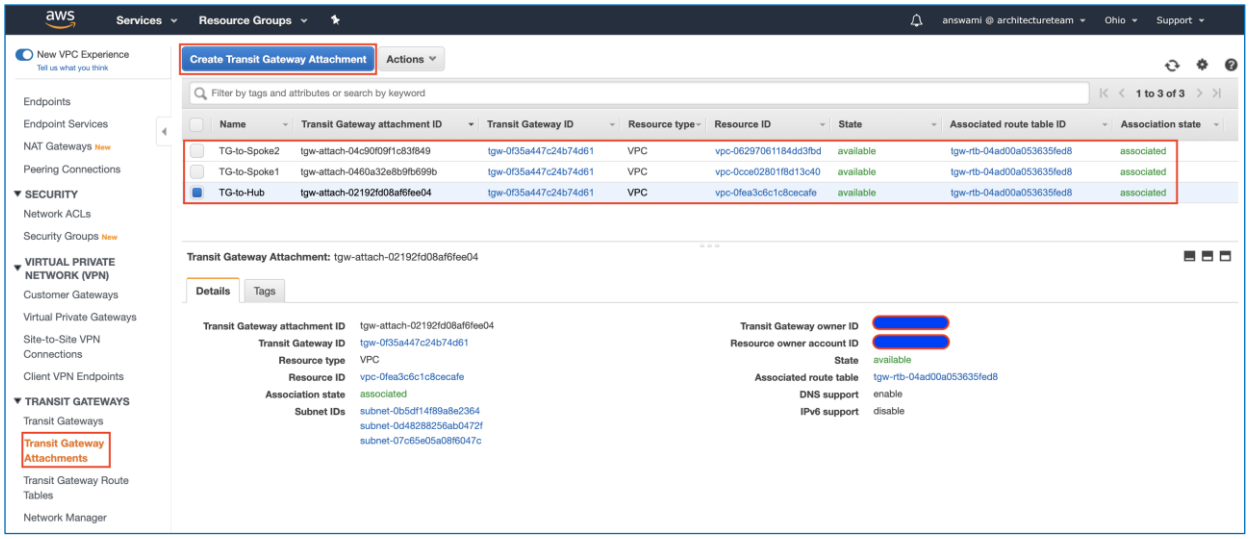


Step 4. Create Transit Gateway and attach VPCs - Access AWS VPC service → Transit Gateways → Create Transit Gateway



Create the three Transit Gateway attachment for hub and spoke model

TG name	VPC Name	Attachment Type	Subnets Associated
TG-to-Hub	HubVPC	VPC attachment	Hubinside01, Hubinside02, and Hubinside03
TG-to-Spoke1	Spoke1VPC	VPC attachment	Spoke01-Web
TG-to-Spoke2	Spoke2VPC	VPC attachment	Spoke02-Web

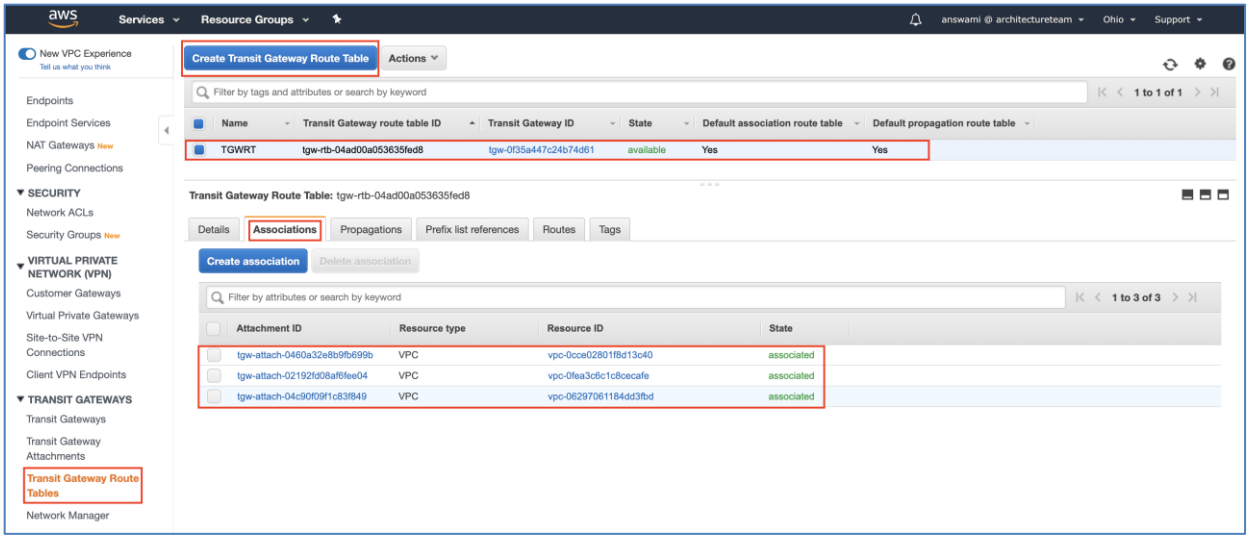


Subnets for Transit Gateway attachment

VPC Name	Attachment Type
TG-to-Hub	Hubinside01, Hubinside02, and Hubinside03
TG-to-Spoke1	Spoke01-Web
TG-to-Spoke2	Spoke02-Web

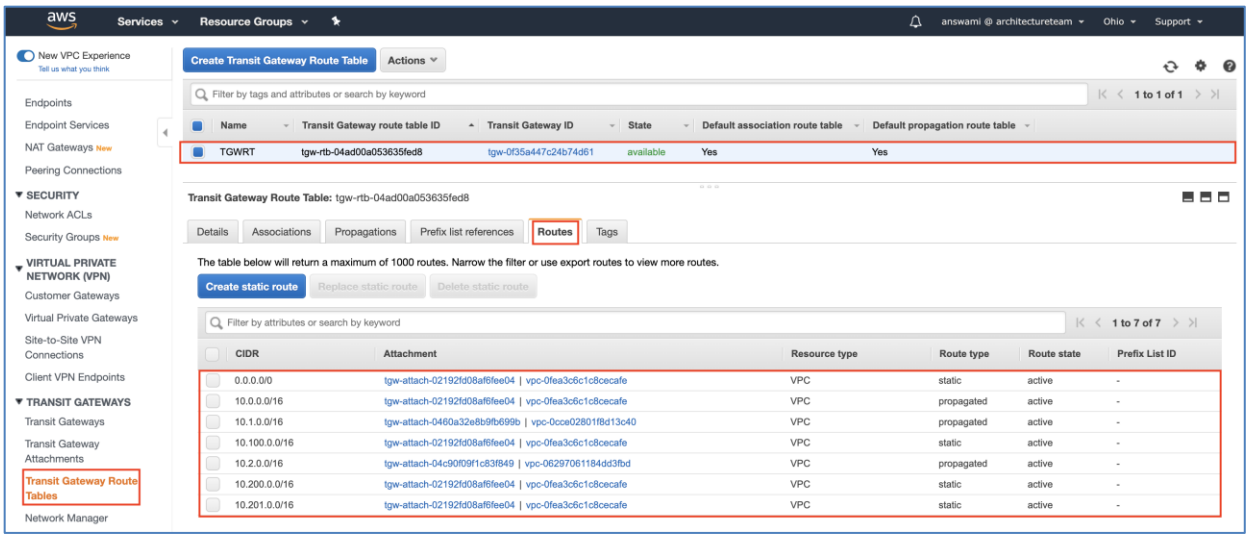
Create route-table in Transit Gateway and associate route table with HubVPC, Spoke1VPC, and Spoke2VPC

VPC Name	Attachment Type
HubVPC	VPC attachment
Spoke1VPC	VPC attachment
Spoke2VPC	VPC attachment



Add routes in the route table associated to the transit gateway, the route table has routes for the following subnets:

Subnet Name	Subnet	VPC Attachment
HubASA1 VPN pool	10.100.0.0/16	HubVPC
HubASA2 VPN pool	10.200.0.0/16	HubVPC
HubASA3 VPN pool	10.201.0.0/16	HubVPC
Spoke1VPC	10.1.0.0/16	Spoke1VPC
Spoke2VPC	10.2.0.0/16	Spoke2VPC
Default Route	0.0.0.0/0	HubVPC



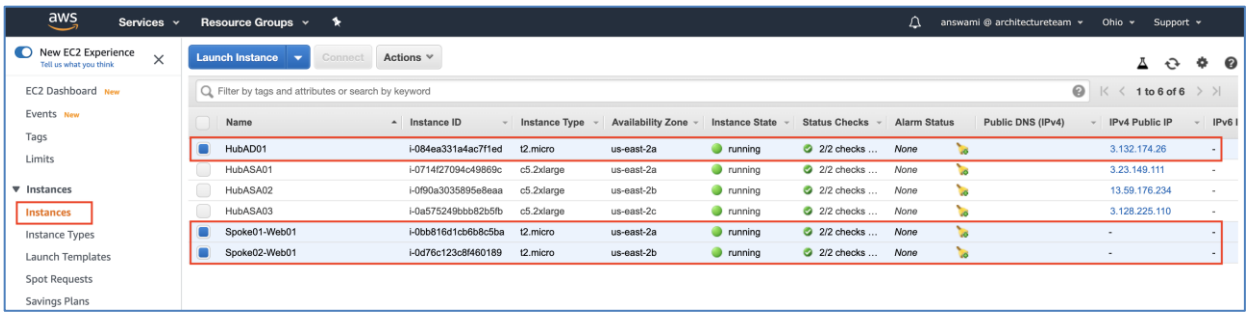
Step 5: Deploy ASAs and Workloads in VPCs – Deploy the following workloads in AWS VPCs and allow traffic in the AWS security group. Three ASAs are deployed in this architecture, each AZ has one ASAv, but we recommend using multiple ASAs per AZ.

Deploy Workloads in HubVPC, Spoke1VPC, and Spoke2VPC

- Access AWS marketplace and search for Microsoft Window Server 2016 or 2019 and Cent OS and deploy instances.

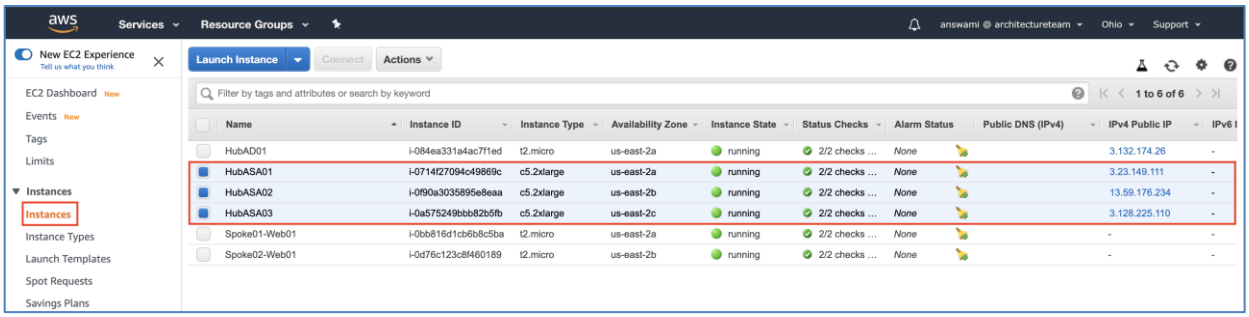
VM Name	VNet Name	Subnet Name	IP address	Port	OS
HubAD01	HubVPC	Hubmgmt01	10.0.0.55	TCP 389	Windows Server 2019
Spoke01-Web01	Spoke1VPC	Spoke01-Web	10.1.1.100	TCP 80	CentOS 7.5
Spoke02-Web01	Spoke2VPC	Spoke01-Web	10.2.1.100	TCP 80	CentOS 7.5

- Active Directory Server:
  - Deploy MS Windows Server 2016 or 2019 from AWS Marketplace
  - Install AD services, create a domain, and add users
  - Ensure Windows firewalls, and AWS security allows TCP 389 (LDAP), and ICMP traffic
- Red HAT VMs:
  - Deploy Red HAT from AWS Marketplace
  - Install httpd service and start httpd
  - Ensure iptables, and AWS Security Group allows TCP 80 traffic, and ICMP traffic

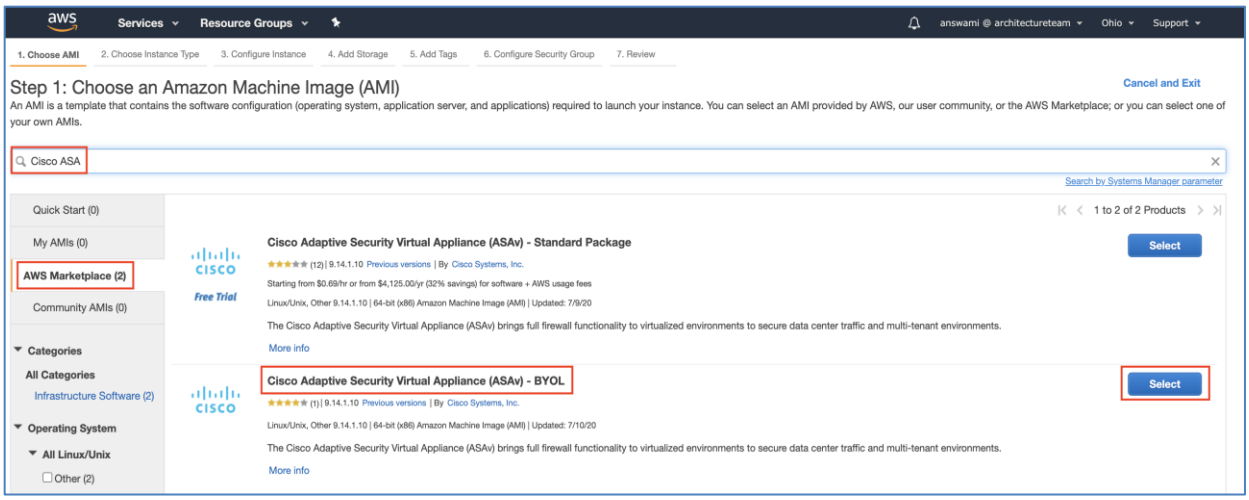


Step 5. Deploy Cisco ASAVS – Deploy ASAs in HubVPC – Access AWS marketplace and search Cisco ASA and deploy BYOL offering

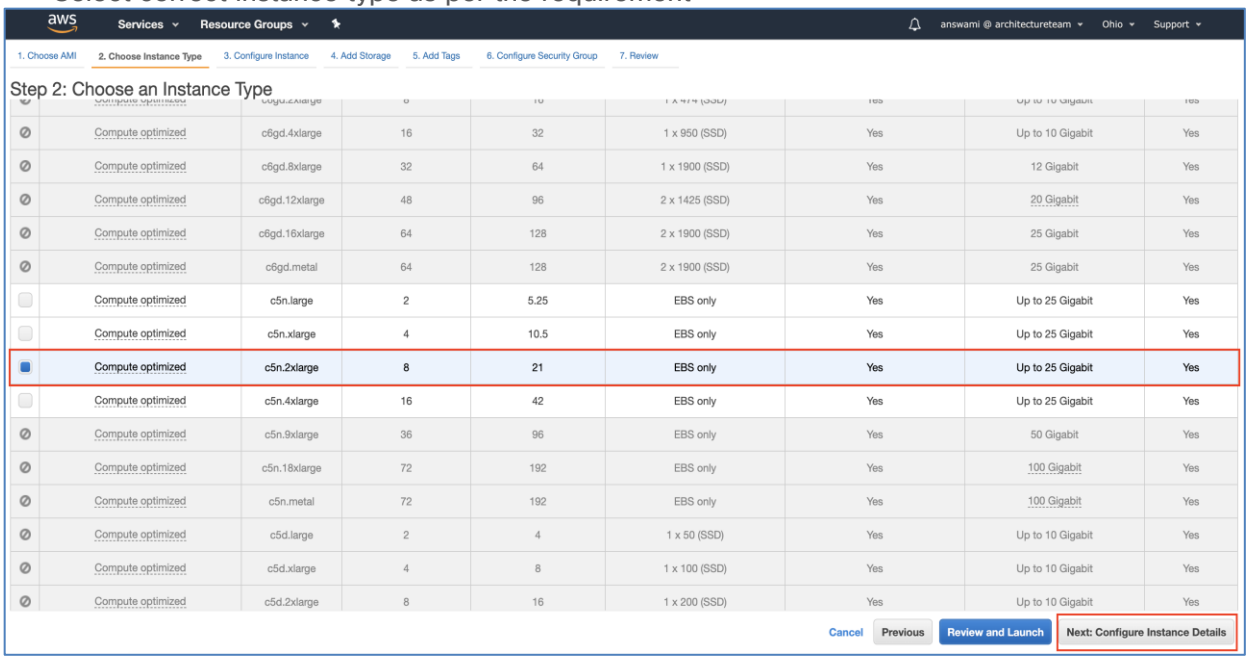
VM Name	VNet Name	Subnet Name	IP address	Port	OS
HubASA01	HubVPC	Hubmgmt01 Huboutside01 Hubinside01	10.0.0.10 10.0.1.10 10.0.2.10	TCP 22, 80 & 443	ASAv 9.14.x
HubASA02	HubVPC	Hubmgmt02 Huboutside02 Hubinside02	10.0.3.10 10.0.4.10 10.0.5.10	TCP 22, 80 & 443	ASAv 9.14.x
HubASA03	HubVPC	Hubmgmt03 Huboutside03 Hubinside03	10.0.6.10 10.0.7.10 10.0.8.10	TCP 22, 80 & 443	ASAv 9.14.x



- Access AWS console, click EC2 → Launch Instance → Click AWS Marketplace → Search for Cisco ASA and click Cisco ASA BYOL offering to deploy ASAv (you can also use Standard (PAY-G) offering)



- Read pricing information and click continue
- Select correct instance type as per the requirement



Click configure instance details, on instance details screen add the following information:

- VPN – HubVPC
- Subnet Information for ASA01:
    - First Subnet/vNIC – Hubmgmt01
    - Second Subnet/vNIC – Huboutside01
    - Third Subnet/vNIC – Hubinside01

Leave default storage setting and click add Tags

In Tags mention – Name – HubASA01

Select Security Group that allows traffic (22, 80, and 443)

Click on launch and select key to deploy this instance

Now deploy HubASA02 and HubASA03 using the following subnets:

- HubASA02
  - First Subnet/vNIC – Hubmgmt02
  - Second Subnet/vNIC – Huboutside02
  - Third Subnet/vNIC – Hubinside02
- HubASA03
  - First Subnet/vNIC – Hubmgmt03
  - Second Subnet/vNIC – Huboutside03
  - Third Subnet/vNIC – Hubinside03

Now move m0/0 to management only and add default route on the outside interfaces; this step is optional and added to segregate management and data traffic. Interface management0/0 can be used as a data interface, by default ASA is configured with "no management-only" command. Use jump-box do add change management interface configuration.

On ASA1 (HubASA01)

```
Interface m0/0
 ip address 10.0.0.10 255.255.255.0
 management-only
!
route management 0.0.0.0 0.0.0.0 10.0.0.10
route outside 0.0.0.0 0.0.0.0 10.0.1.10
```

On ASA2 (HubASA02)

```
Interface m0/0
 ip address 10.0.3.10 255.255.255.0
 management-only
!
route management 0.0.0.0 0.0.0.0 10.0.3.1
route outside 0.0.0.0 0.0.0.0 10.0.4.1
```

On ASA2 (HubASA03)

```
Interface m0/0
 ip address 10.0.6.10 255.255.255.0
 management-only
!
```

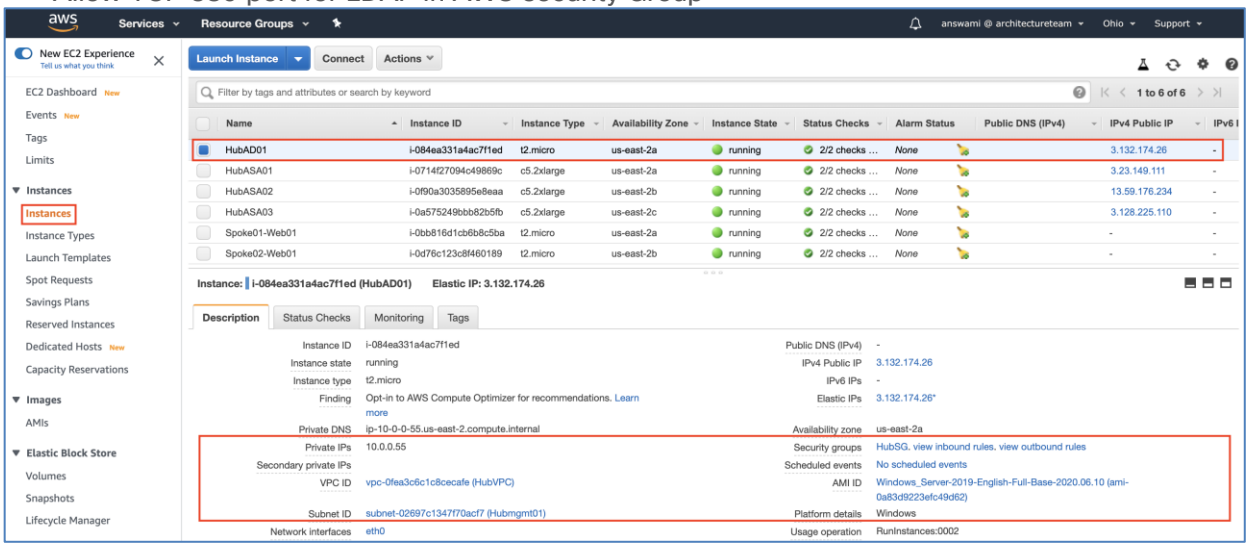
route management 0.0.0.0 0.0.0.0 10.0.6.1

route outside 0.0.0.0 0.0.0.0 10.0.7.1

Now map EIP on eth0 and eth1 of allow ASAs (eth0 is management and eth1 is outside)

Deploy Active Directory HubVPC – Access AWS marketplace and search for Microsoft Window Server 2016 deploy instance (HubAD01) in Hubmgmt01 subnet

- Once AD is deployed, install AD service
- Disable windows firewall
- Add a test user
- Allow TCP 389 port for LDAP in AWS security Group



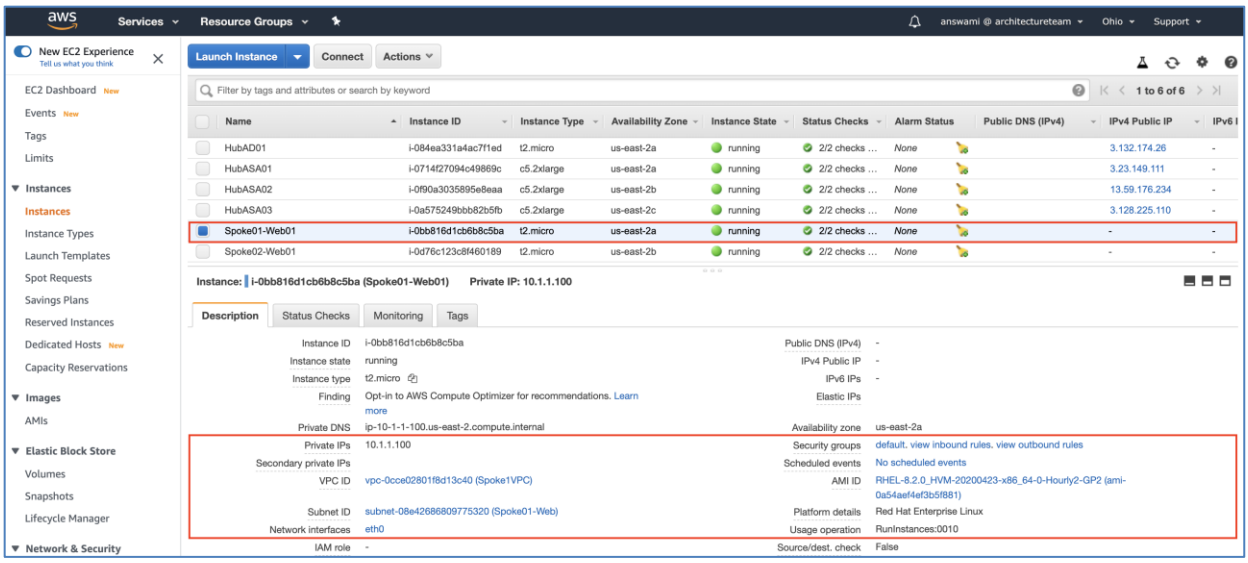
Deploy Web Servers

Access AWS marketplace and search for red hat instances and deploy in Spoke01VPC and Spoke02VPC

- **Spoke01-Web01** in Spoke1VPC
- **Spoke02-Web01** in Spoke2VPC
- Install httpd service and start it
- Allow port 80, 443 and ICMP traffic in AWS Security Group

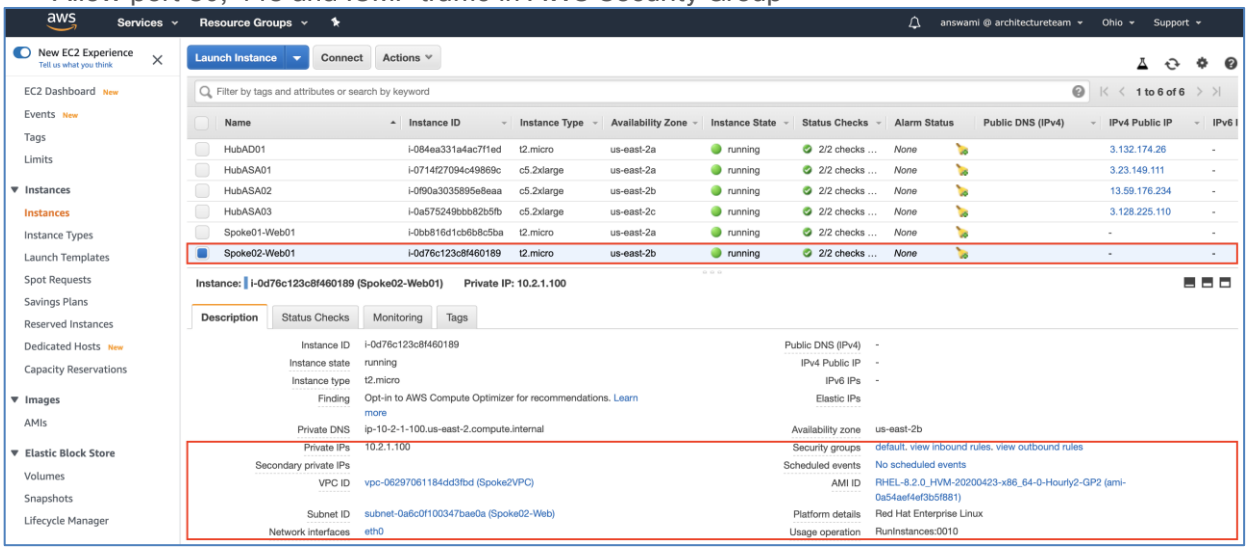
Spoke01-Web01

- Deploy in Spoke1VPC
- Install httpd service and start it
- Allow port 80, 443 and ICMP traffic in AWS Security Group

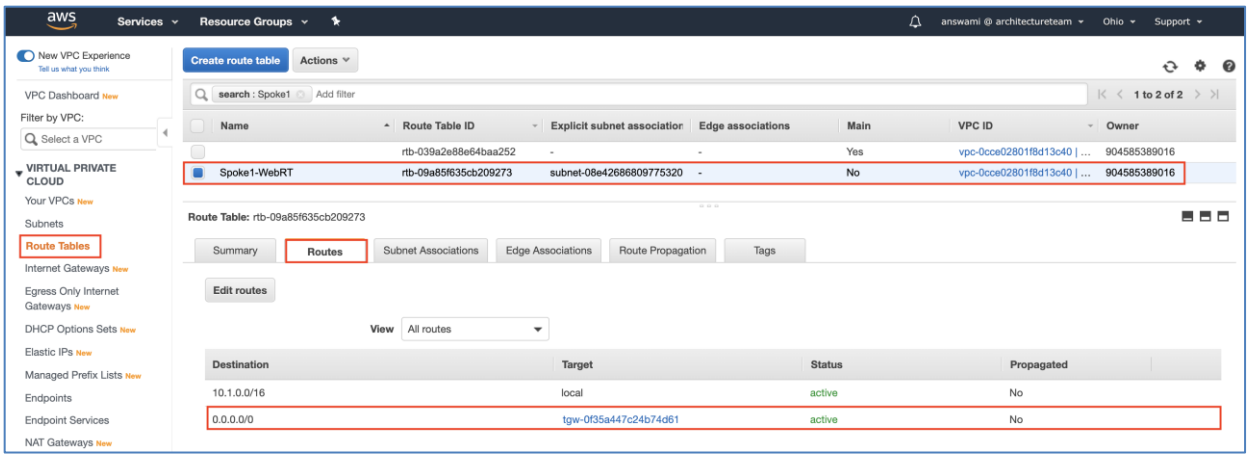


Spoke02-Web01

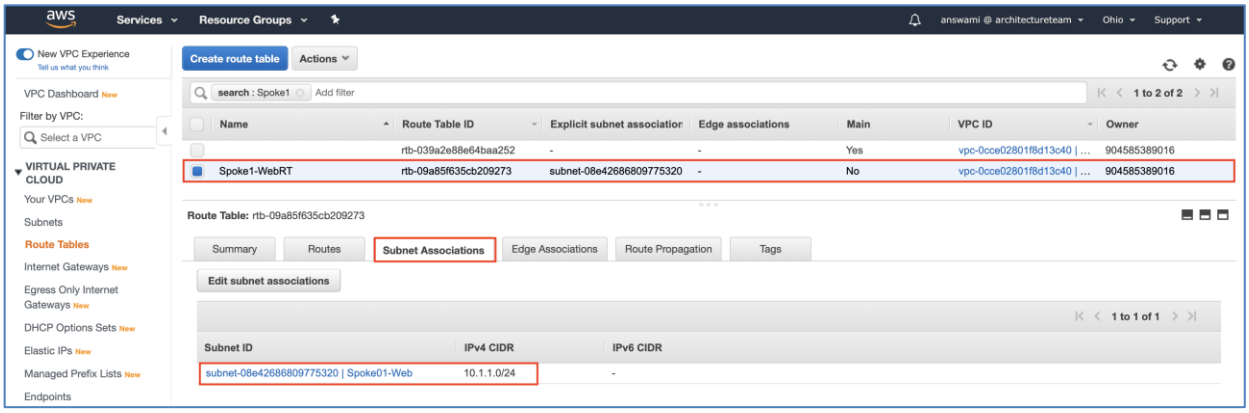
- Deploy in Spoke1VPC
- Install httpd service and start it
- Allow port 80, 443 and ICMP traffic in AWS Security Group



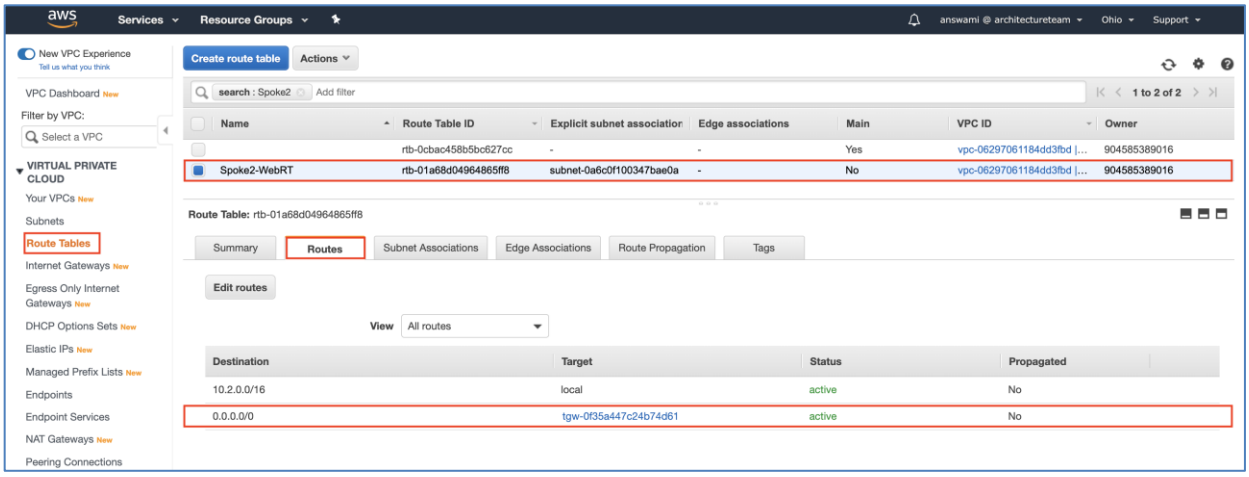
Step 6: **Create, configure and associate route tables –** Create route tables to route traffic. **Spoke1-WebRT** has a default route pointing to AWS Transit Gateway.



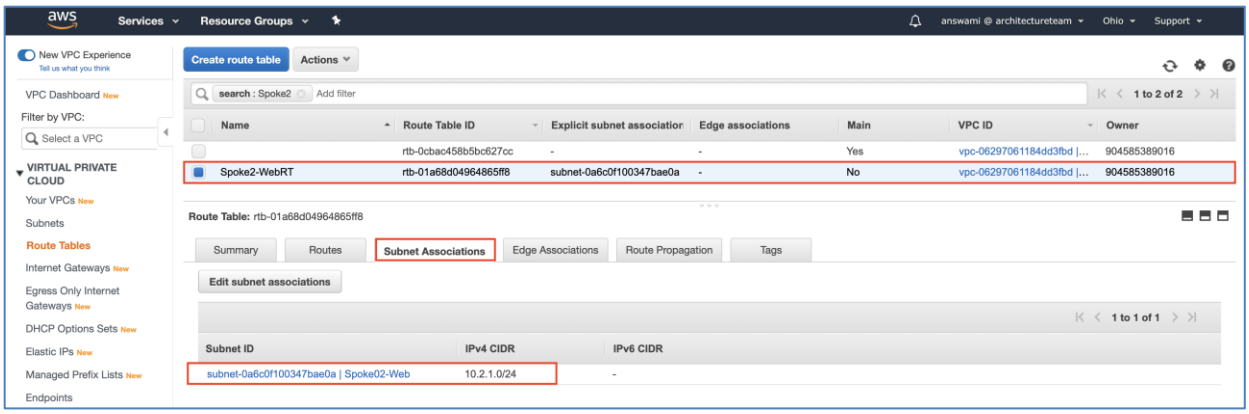
Spoke1-WebRT is associated to **Spoke01-Web**.



Spoke2-WebRT has a default route pointing to AWS Transit Gateway.



Spoke2-WebRT is associated to **Spoke02-Web**.

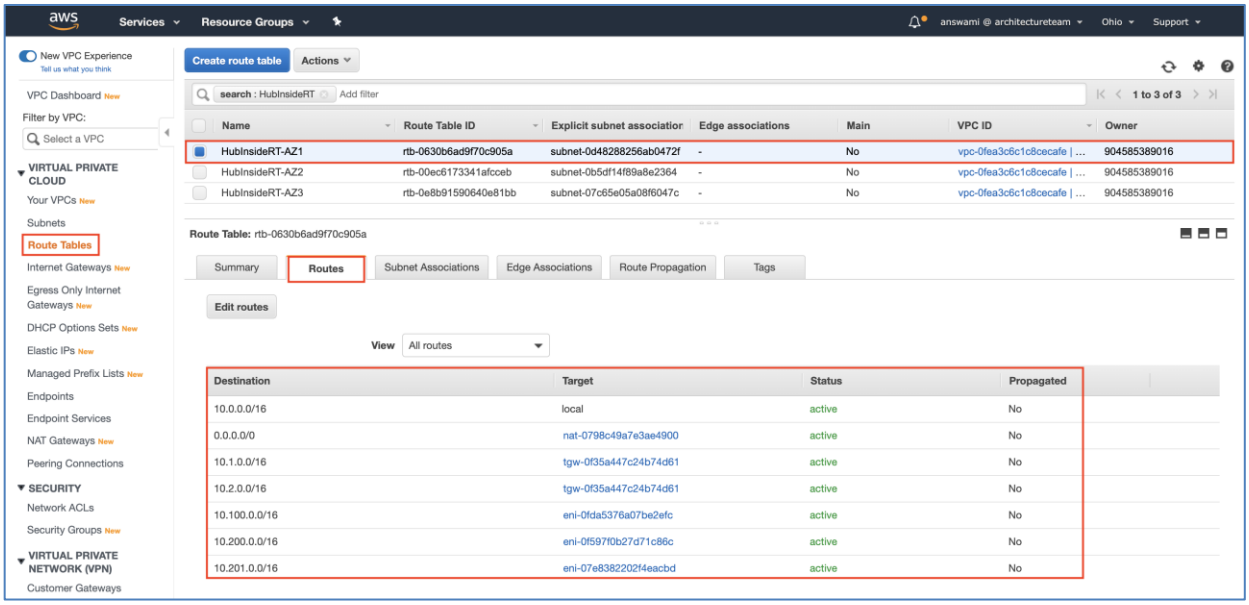


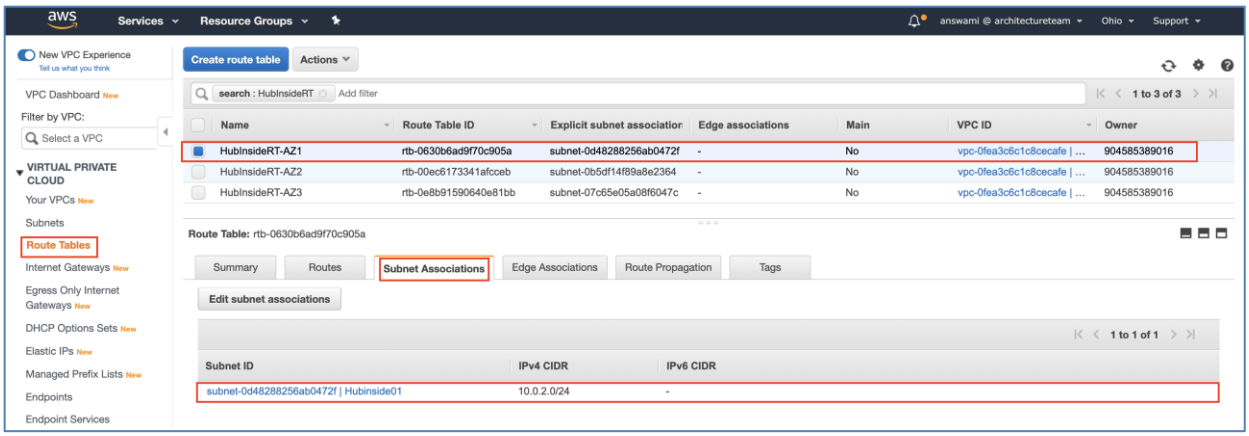
HubinsideRT-AZ1 has the following routes:

- Default-Route points to the NAT Gateway
- Route for Spoke1VPC and Spoke2VPC points to the Transit Gateway
- Route for VPN pools points to respective ASA ENIs
    - 10.100.0.0/16 – HubASA1 (eth2 ENI)
    - 10.200.0.0/16 – HubASA2 (eth2 ENI)
    - 10.201.0.0/16 – HubASA1 (eth2 ENI)

HubinsideRT-AZ1 is associated to Hubinside01

Note: Same route table can be applied to Hubinside02 and Hubinside03. As a best practice we have HubinsideRT-AZ2 and HubinsideRT-AZ3 with similar routes





HubinsideRT-AZ2 has the following routes:

- Default-Route points to the NAT Gateway
- Route for Spoke1VPC and Spoke2VPC points to the Transit Gateway
- Route for VPN pools points to respective ASA ENIs
    - 10.100.0.0/16 – HubASA1 (eth2 ENI)
    - 10.200.0.0/16 – HubASA2 (eth2 ENI)
    - 10.201.0.0/16 – HubASA1 (eth2 ENI)

HubinsideRT-AZ2 is associated to Hubinside02

HubinsideRT-AZ3 has the following routes:

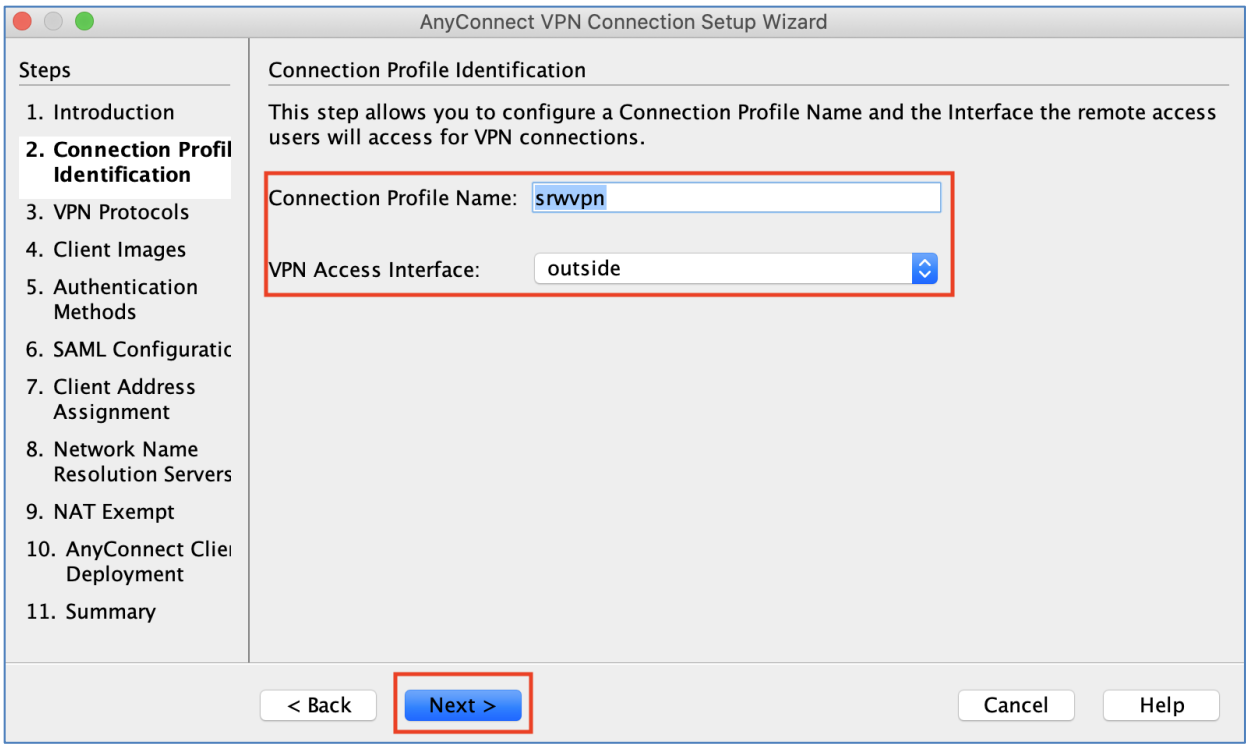
- Default-Route points to the NAT GW
- Route for Spoke1VPC and Spoke2VPC points to the TGW
- Route for VPN pools points to respective ASA ENIs
    - 10.100.0.0/16 – HubASA1 (eth2 ENI)
    - 10.200.0.0/16 – HubASA2 (eth2 ENI)
    - 10.201.0.0/16 – HubASA1 (eth2 ENI)

HubinsideRT-AZ3 is associated to Hubinside03

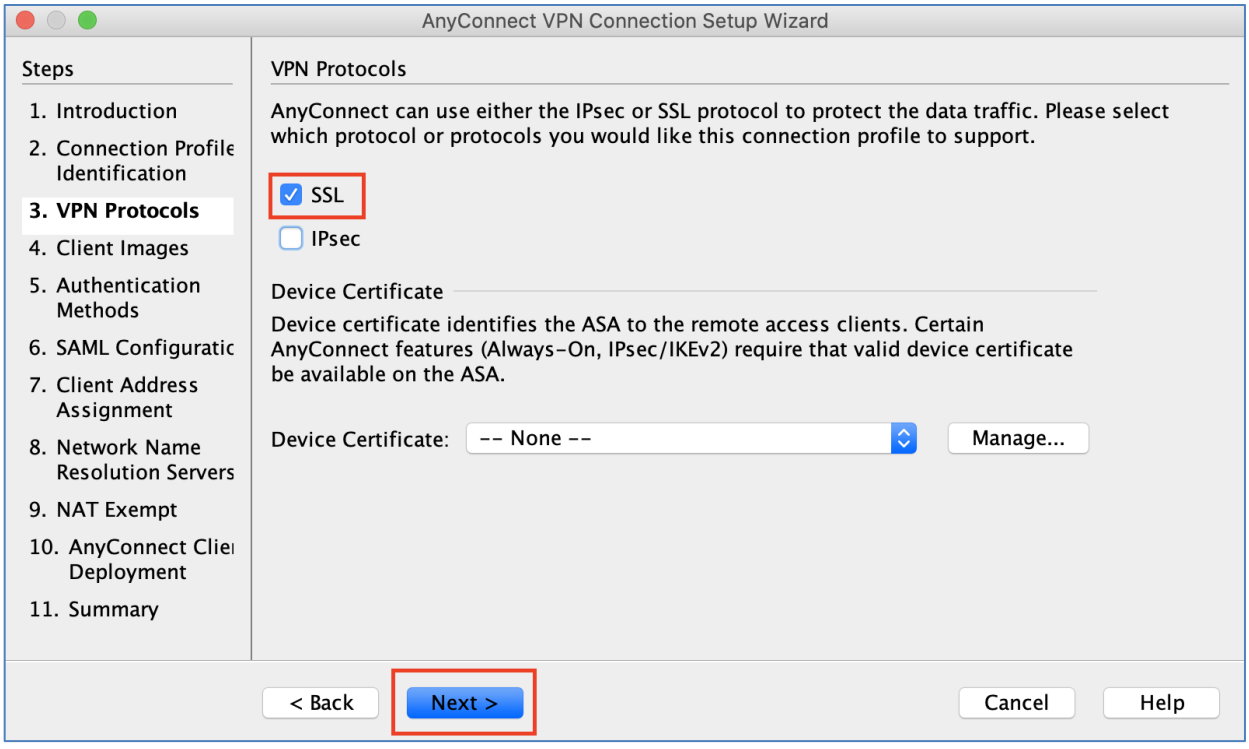
Step 7: Configure RAVPN ASAVs (HubASA01, HubASA02, and HubASA03) - Now we have our base infrastructure ready, let's configure RAVPN using Cisco Adaptive Security Device Manager (ASDM). Cisco VPN wizard configuration guide (Cisco Documentation).

Device Name	VPN Profile Name	VPN Pool	VPN Type
HubASA01	srwvpn	10.100.0.0/16	RAVPN (SSL)
HubASA02	srwvpn	10.200.0.0/16	RAVPN (SSL)
HubASA03	srwvpn	10.201.0.0/16	RAVPN (SSL)

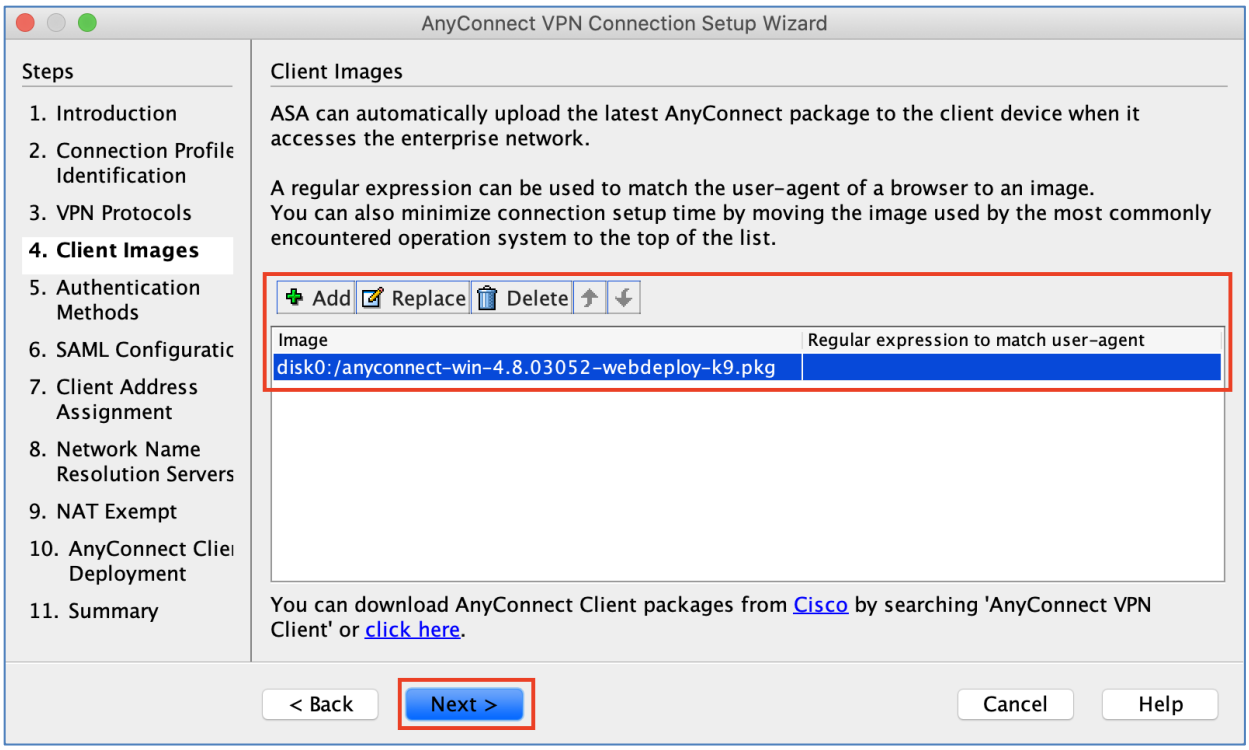
Launch ASDM, click on Wizards → VPN Wizards → AnyConnect VPN Wizard. Click next on the introduction page. Now add vpn profile name as “srwvpn” and select outside interface.



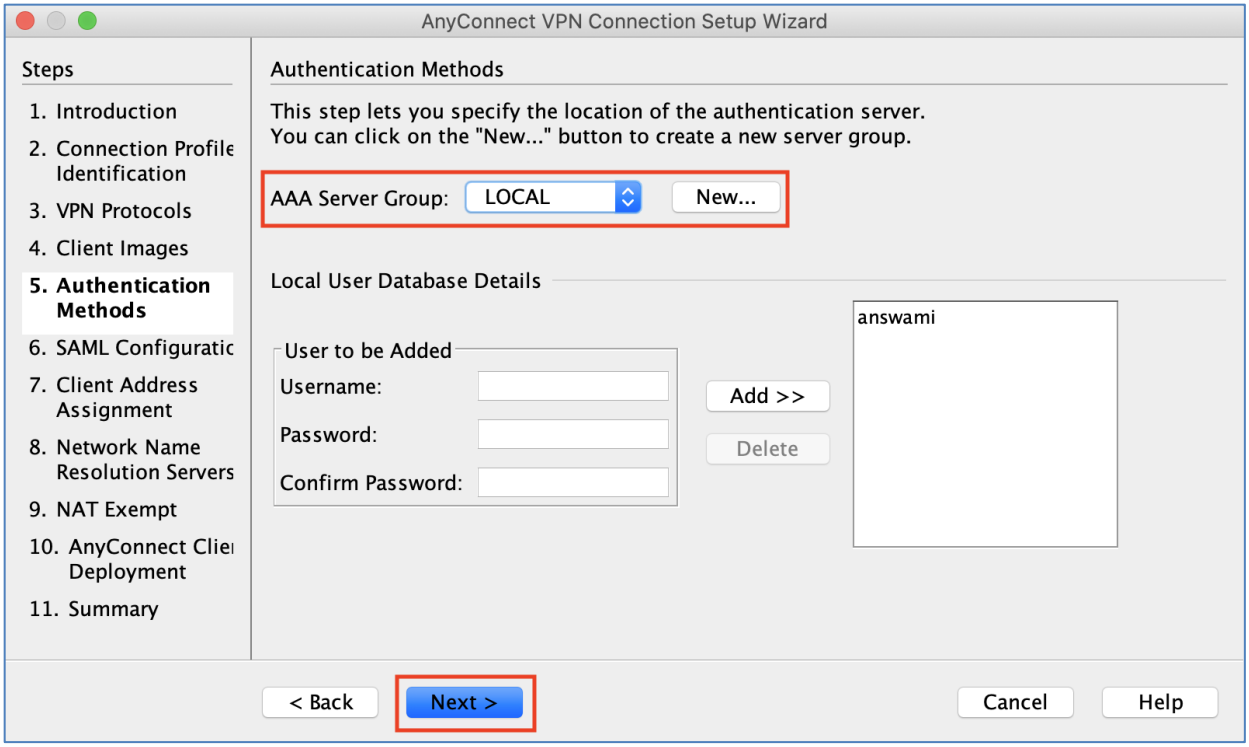
Under the VPN protocol, select SSL and then click next.



Now upload and point to the latest AnyConnect, click next

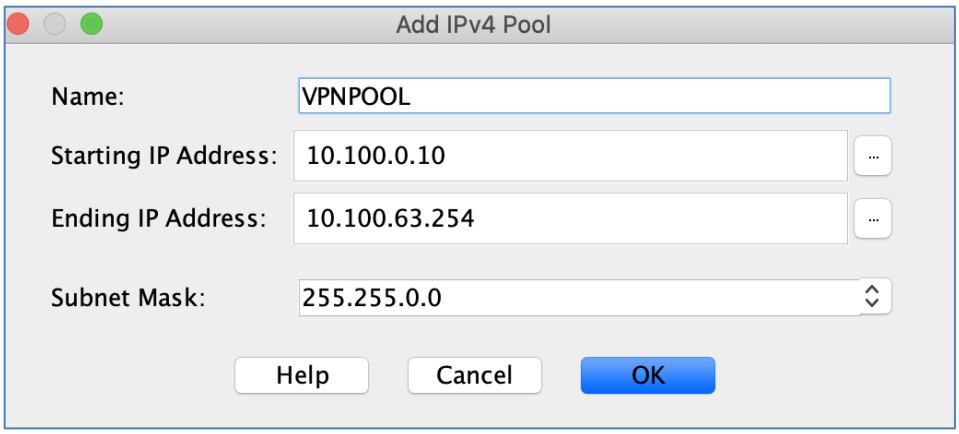


Select LOCAL authentication and click next.

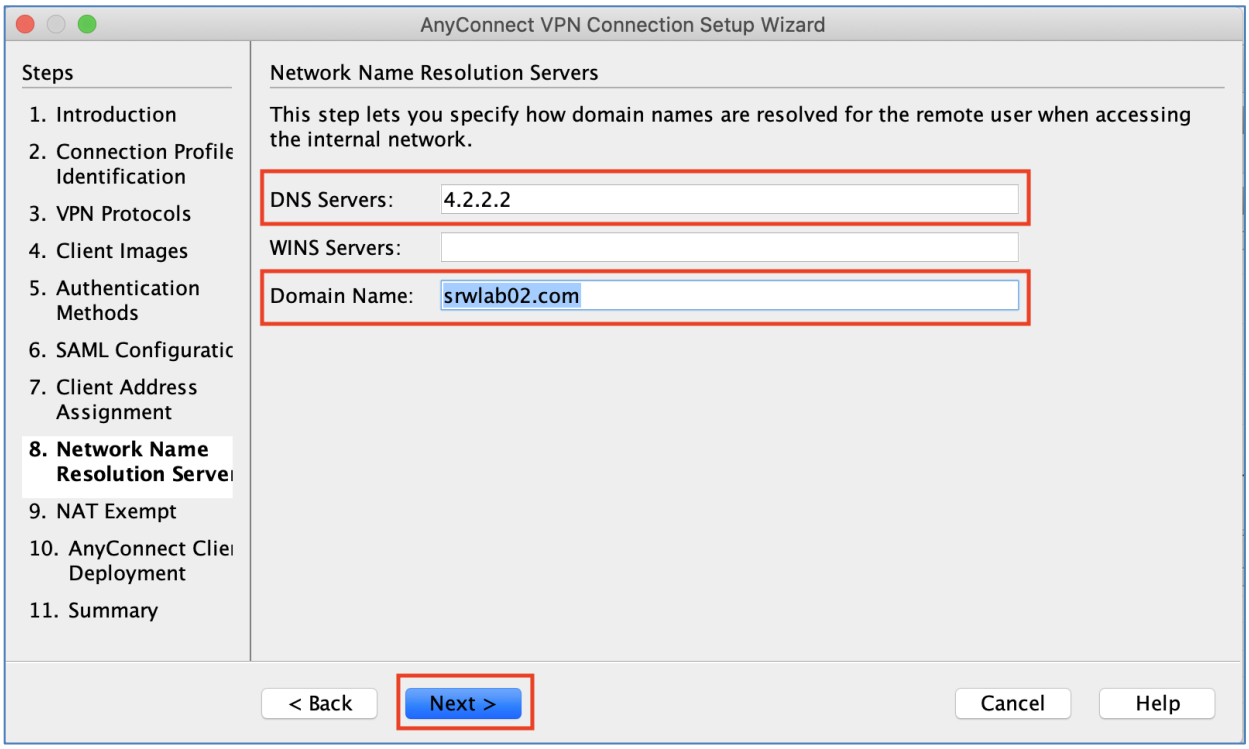


On SAML configuration leave default settings and click next.

Now add a VPN pool (refer to the above table for pool information – Each ASA has a different pool).



Add DNS and Domain information, click next.



Enable NAT exempt for VPN traffic, then click next on AnyConnect Client Deployment page.

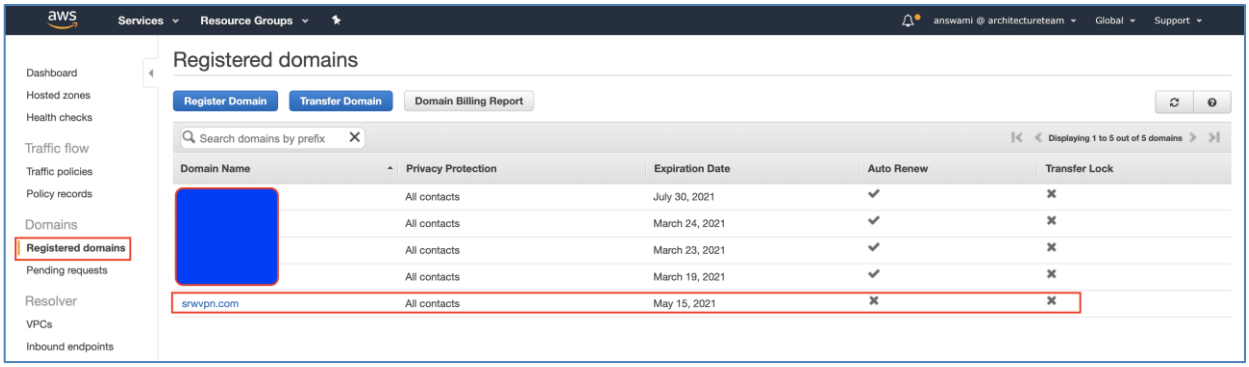
Click finish to deploy.

Repeat VPN setup steps for HubASA02 and HubASA03, use the following VPN pool.

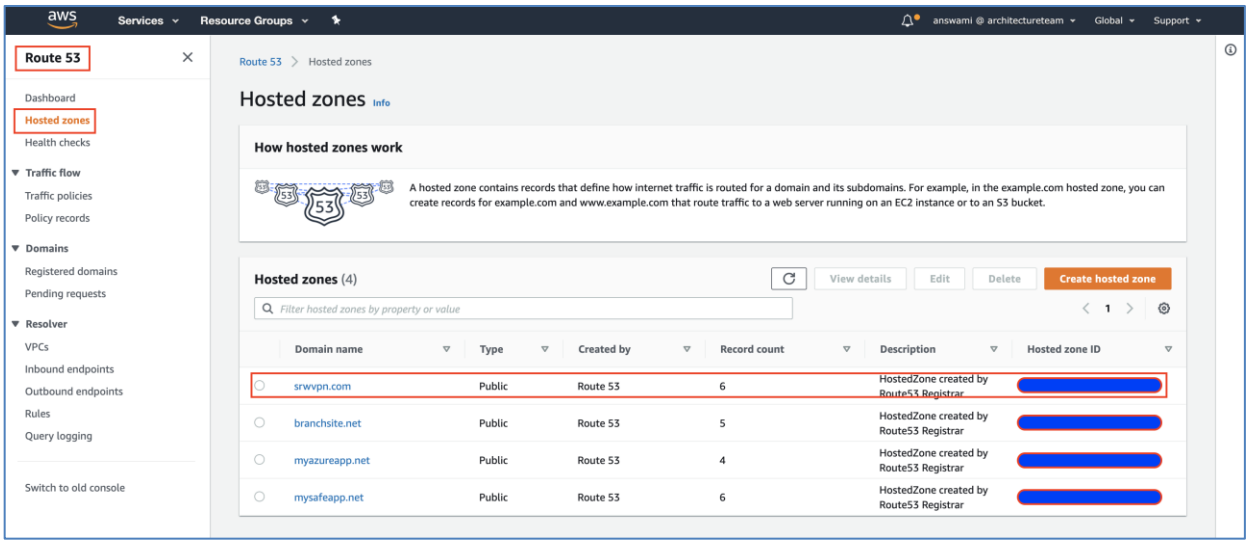
Device Name	VPN Profile Name	VPN Pool	VPN Type
HubASA02	srwvpn	10.200.0.0/16	RAVPN (SSL)
HubASA03	srwvpn	10.201.0.0/16	RAVPN (SSL)

Step 8: Configure AWS route53 for VPN load balancing - AWS route53 provides a way to load balance remote access VPN sessions

Register domain using Route53 (example: srwvpn.com): Access Route53 and click register domains→ Register Domain. Add the required information and register domain for Anyconnect VPN.



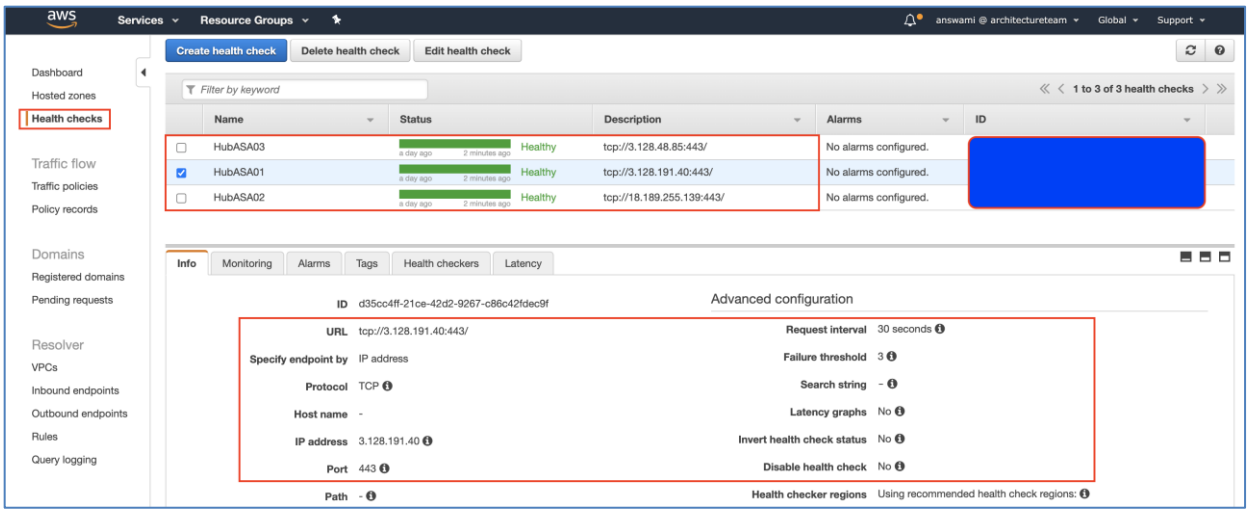
Create a public hosted zone: Click AWS Router 53 → Hosted Zones → Create Hosted Zone. Now add a public hosted zone for srwvpn.com.



Create health-checks for HubASA01, HubASA02, and HubASA03: Use EIP associated with eth2 of HubASA01, HubASA02, and HubASA03 in health-checks.

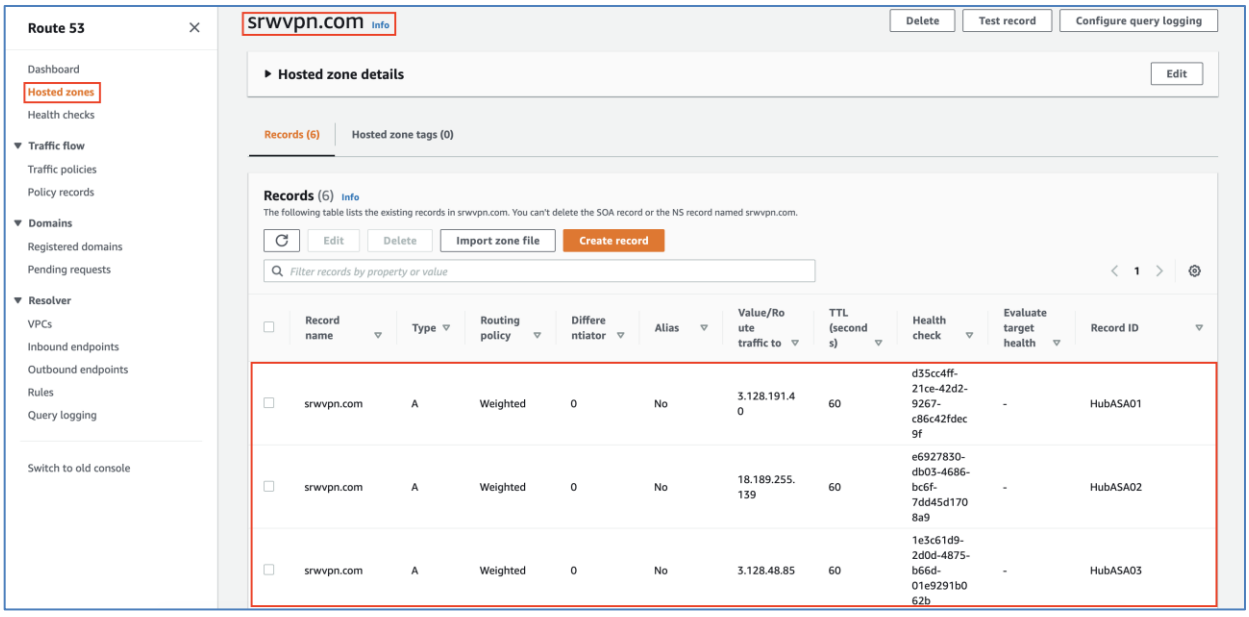
- Use URL as tcp://EIP:443
- Protocol TCP
- Port 443

Note: Add health-check for HubASA01, HubASA02, and HubASA03 using their respective EIPs



Add "A-records" in hosted zone: Now add three "A" records, one for each ASA and use the following properties:

- Type: A record
- Routing Policy: Weighted
- Differentiator/Weight: 0 (zero is required for equal distribution)
- Value: eth2 EIP of ASA
- TTL: 60
- Record ID: HubASA01
- Health-Check: HubASA01



Note: Add "A records" for HubASA02, HubASA03, and associate health-check as well.

Authentication

Configure LDAP Authentication for RAVPN

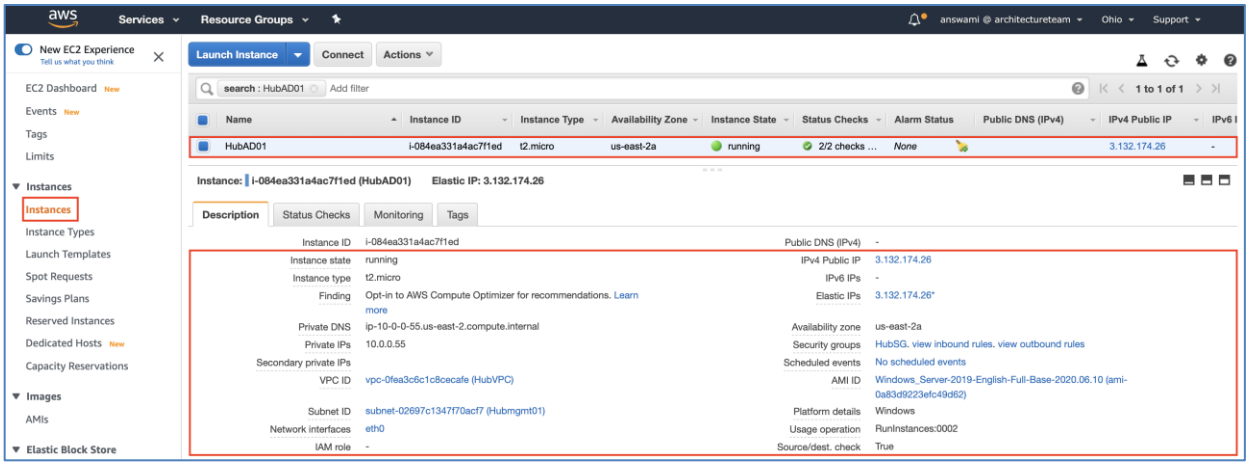
Step 1. Add aaa-server group on ASAs

Step 2. Edit aaa-server settings

Step 3. Change primary authentication in Anyconnect Connection Profile

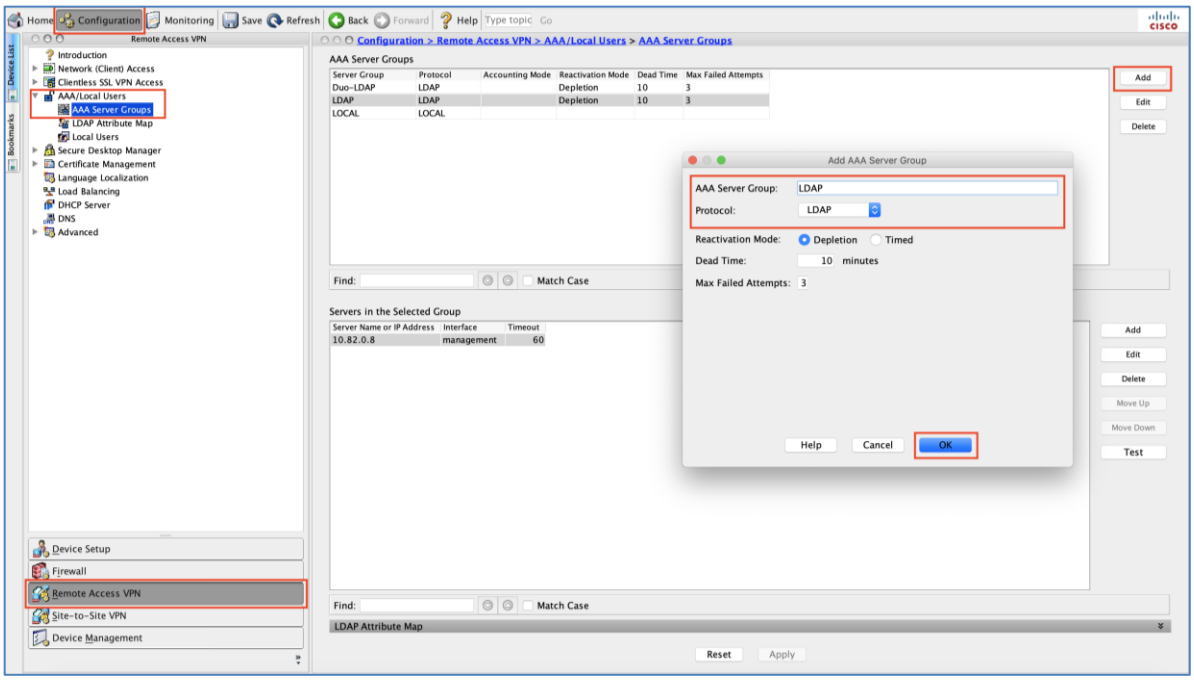
Now we have our base infrastructure ready, and we are all set to integrate LDAP authentication. Once LDAP authentication is enabled, we will modify the AnyConnect VPN profile to use LDAP for RAVPN user authentication. Active directory server is deployed in HubVPC.

VM Name	VPC/subnet	IP address	OS
HubAD01	HubVPC/Hubmgmt01	10.0.0.55	Windows Server 2019 Data Center

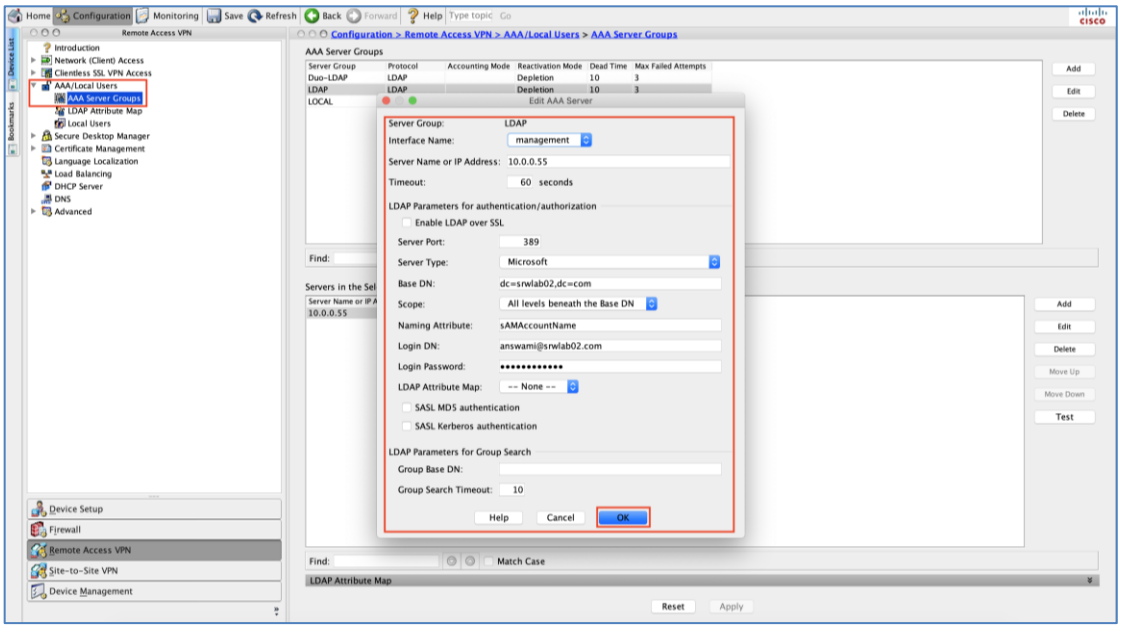


AWS Security Group associated with this VM has rules to allow RDP (TCP 3389), and LDAP (389) port. Cisco ASAs (HubASA01, HubASA02, and HubASA03) uses a management interface to reach HubAD01 (Active Directory Domain Controller)

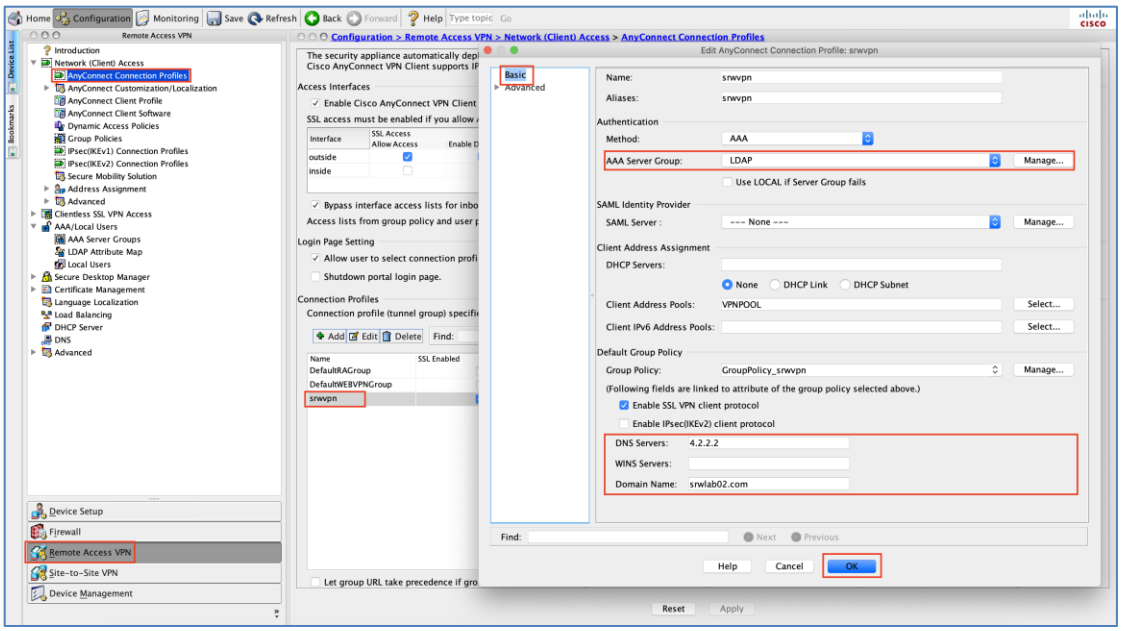
Step 1. Add aaa-server group on ASAVs - In ASDM, go to configuration -> Remote Access VPN -> AAA server group. Click on add, give it a name and then select LDAP from the drop-down menu and click ok.



Step 2. Edit aaa-server settings - Select aaa-server added in step1, click on add and then add LDAP server information as soon in the following screenshot.



Step 3. Change primary authentication in Anyconnect Connection Profile - Now change primary authentication in AnyConnect VPN profile to LDAP.



Duo integration (Two-factor-authentication): We now have our primary authentication setup, and it uses the LDAP server. Duo provides two-factor-authentication for RAVPN; let's integrate with Duo (Duo documentation).

Enable two-factor authentication with Duo (LDAP with Duo)

Step 1. Setup use on Duo portal

Step 2. Add Application on Duo portal

Step 3. Configure aaa-server (LDAP-Duo)

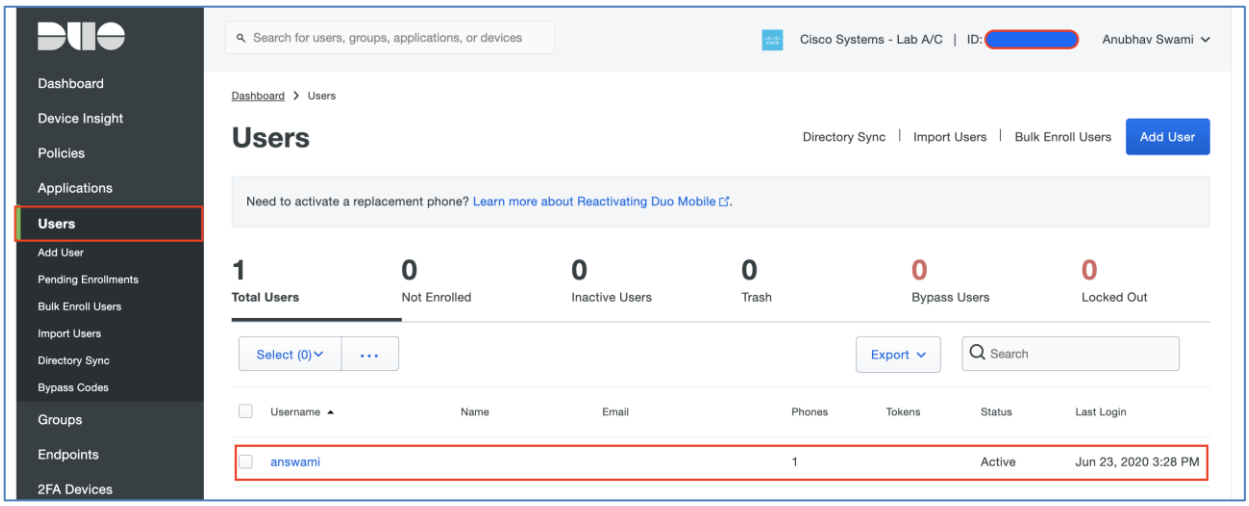
Step 4. Edit Duo-LDAP and add servers in the selected server group

Step 5. Edit AnyConnect VPN profile and add LDAP-Duo for two factor authentication

Step 6. Download and install certificates on all ASAs

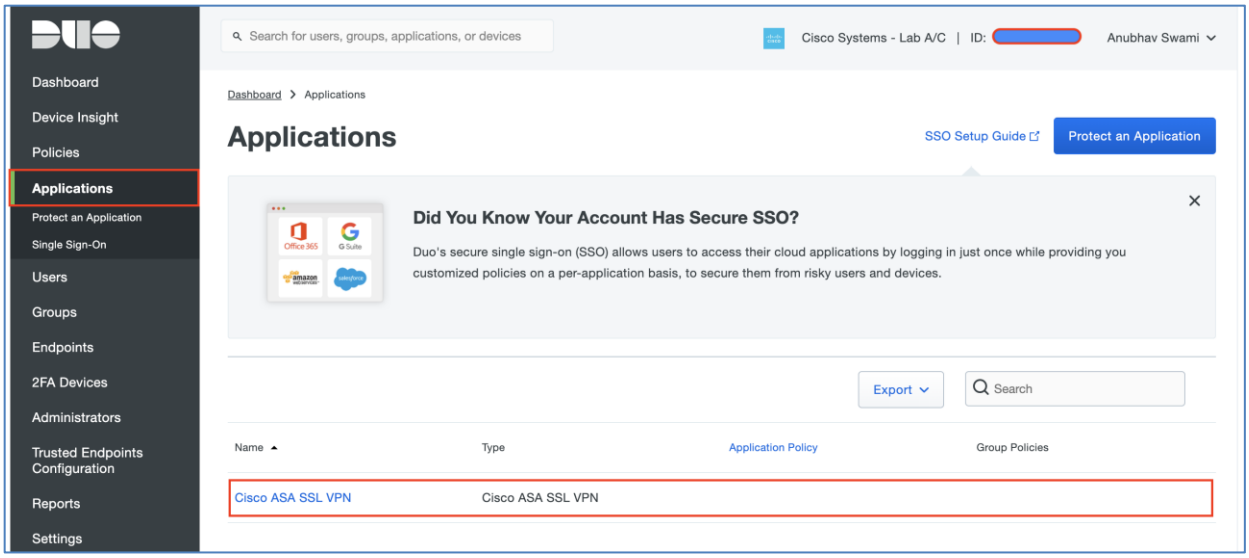
Step 7. Download and install Cisco Duo package on all ASAs for clientless VPN

Step 1. Setup use on Duo portal - Add a user on the Duo portal and have the user enroll for push, call, or text for two-factor authentication.

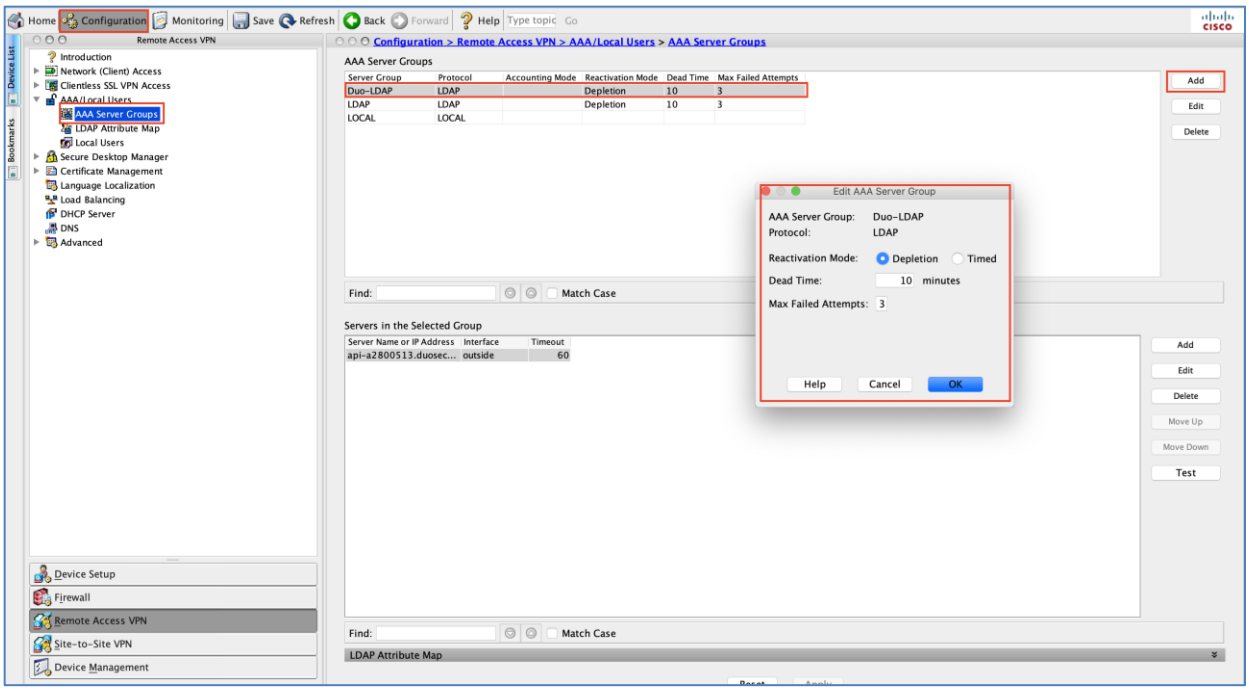


Note: Ask users to enroll for push, call, or text for second-factor authentication.

Step 2. Add a user on the Duo portal (Search for Cisco ASA SSL VPN and click protect), Copy integration key, secret key, and API hostname. This information will be used on ASA to integrate Duo two-factor-authentication (2FA).

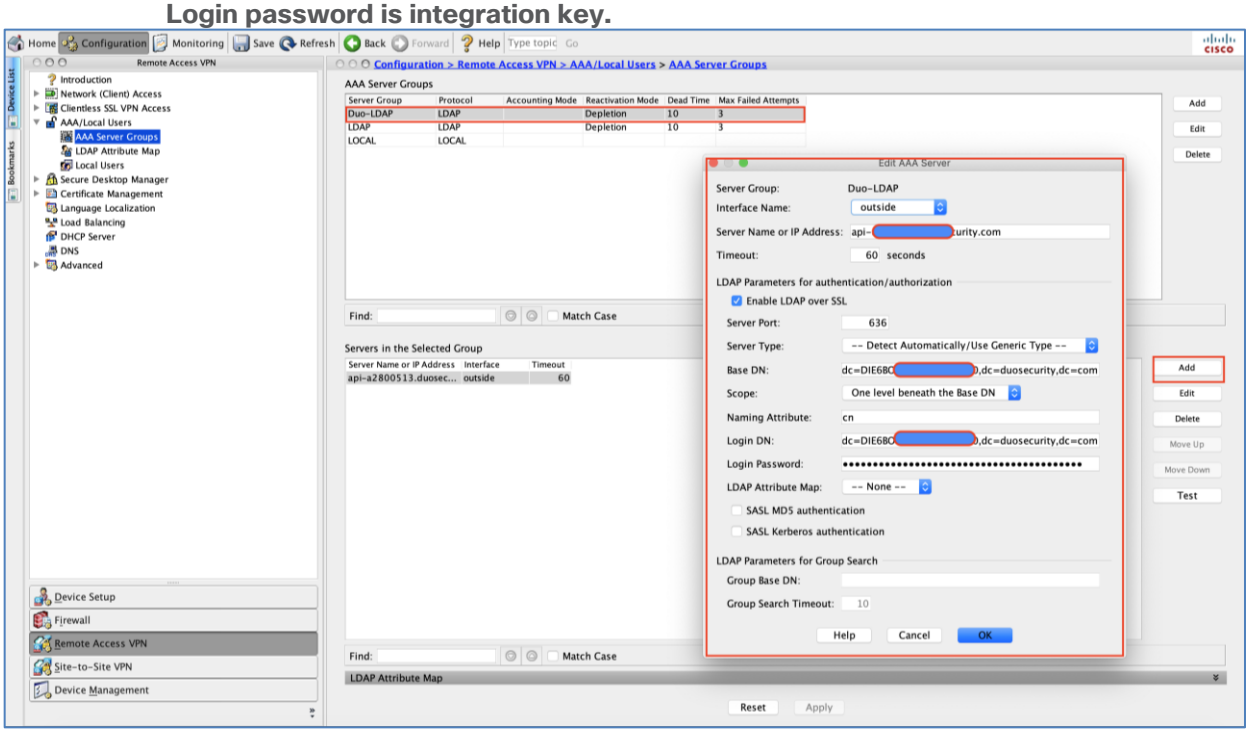


Step 3. Configure aaa-server (LDAP-Duo) - Use integration key, secret key, and API hostname for Duo integration.

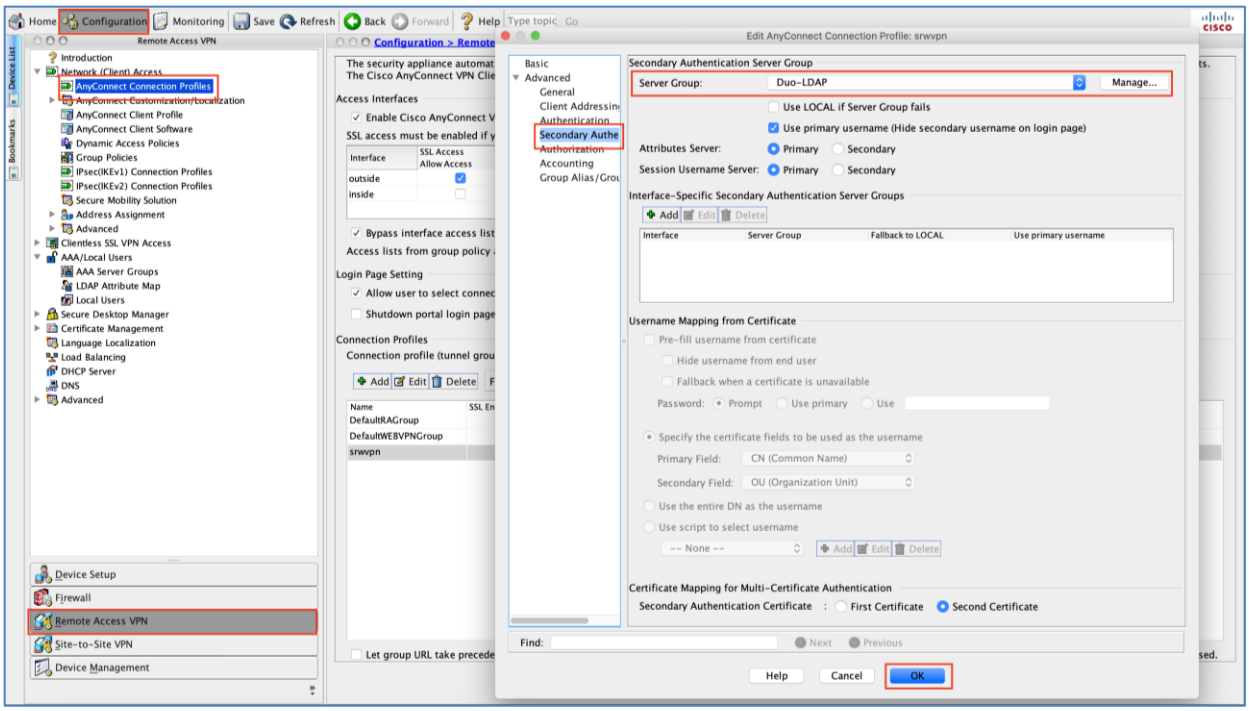


Step 4. Edit Duo-LDAP and add servers in the selected server group (timeout should be 60).

Server or IP address is API hostname
Base DN is dc=Integration_key,dc=duosecurity,dc=com
Login DN is same as Base DN
Login password is integration key.



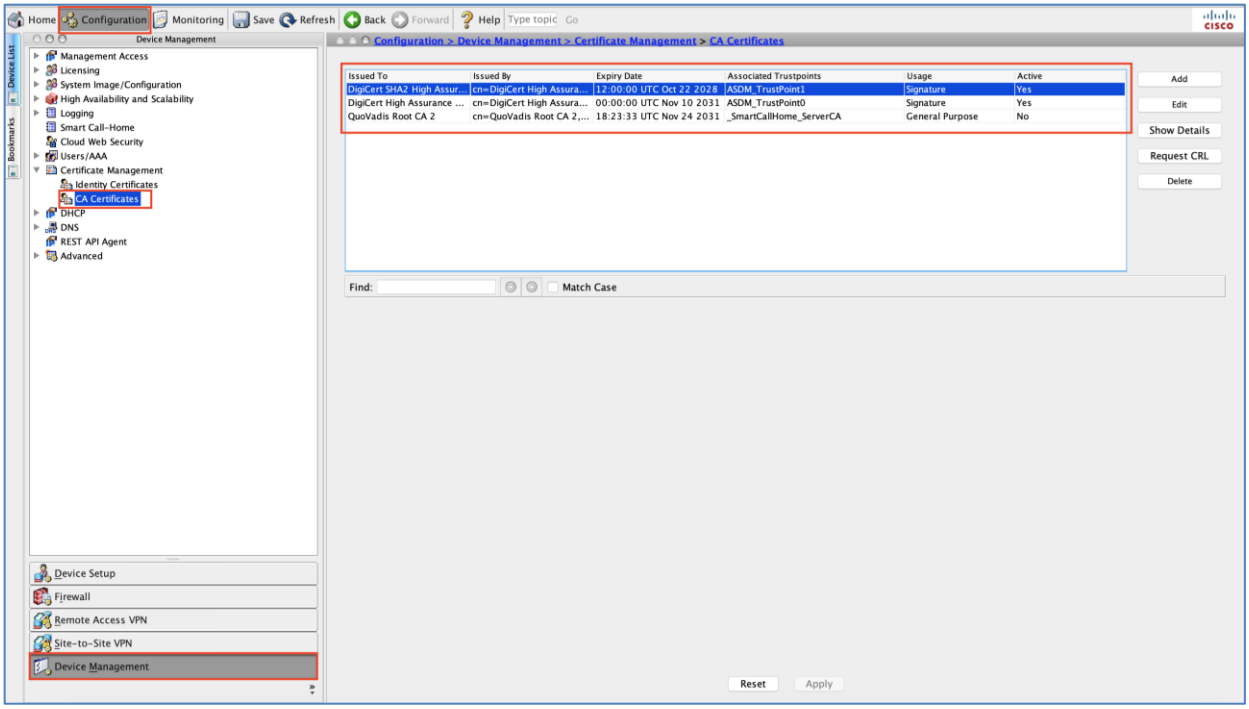
Step 5. Edit AnyConnect VPN profile and add LDAP-Duo for two factor authentication - Make sure that "Use primary username" is checked.



Step 6. Download and install certificates on all ASAVs (hubasa1, hubasa2, and hubasa3) – Click the configuration tab and then click Device management. Navigate to certificate management → CA certificates. Import the following certificates on all ASAVs.

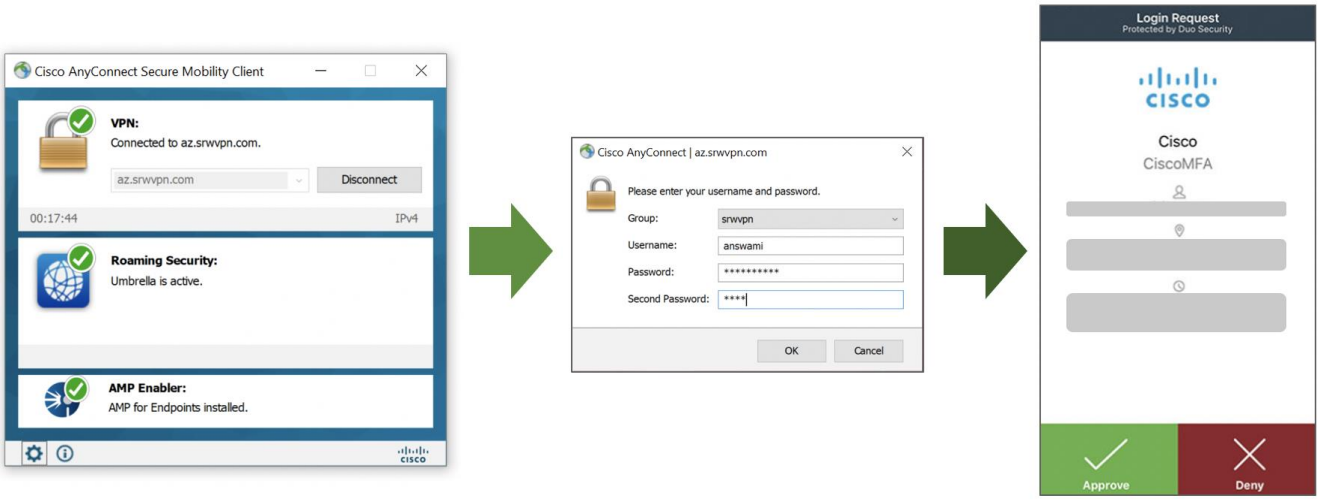
Cert1: https://dl.cacerts.digicert.com/DigiCertHighAssuranceEVRootCA.crt

Cert2: https://dl.cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt



Step 7. Download and install Cisco Duo package on all ASAVs (hubasa1, hubasa2, and hubasa3) for clientless VPN – Checkout Duo documentation (step 4)

Access Cisco Secure AnyConnect Mobility Client (Server: srwvpn.com, username, password, and secondary password). In secondary password as push, call, or text to get Duo challenge on the enrolled device.



By default, the user will get a certificate error, to avoid certificate error install trusted certificates on ASAVs. (Cisco Documentation)

Threat Protection

Cisco Umbrella Roaming Security Module

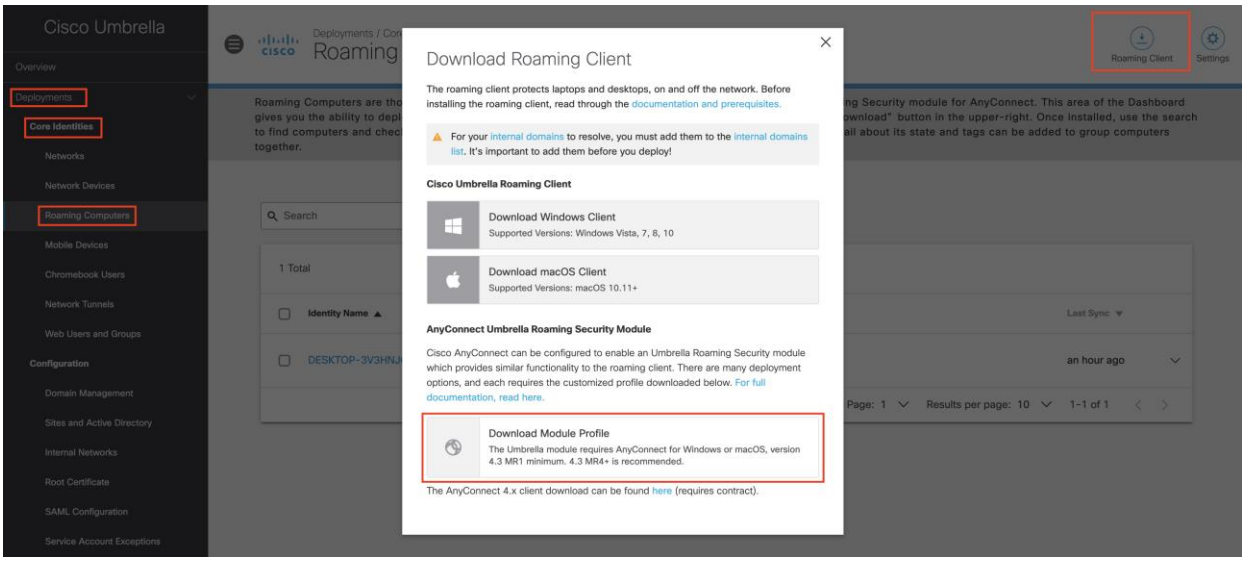
Step 1. Download Umbrella Roaming Security Module

Step 2. Setup AnyConnect Client Profile

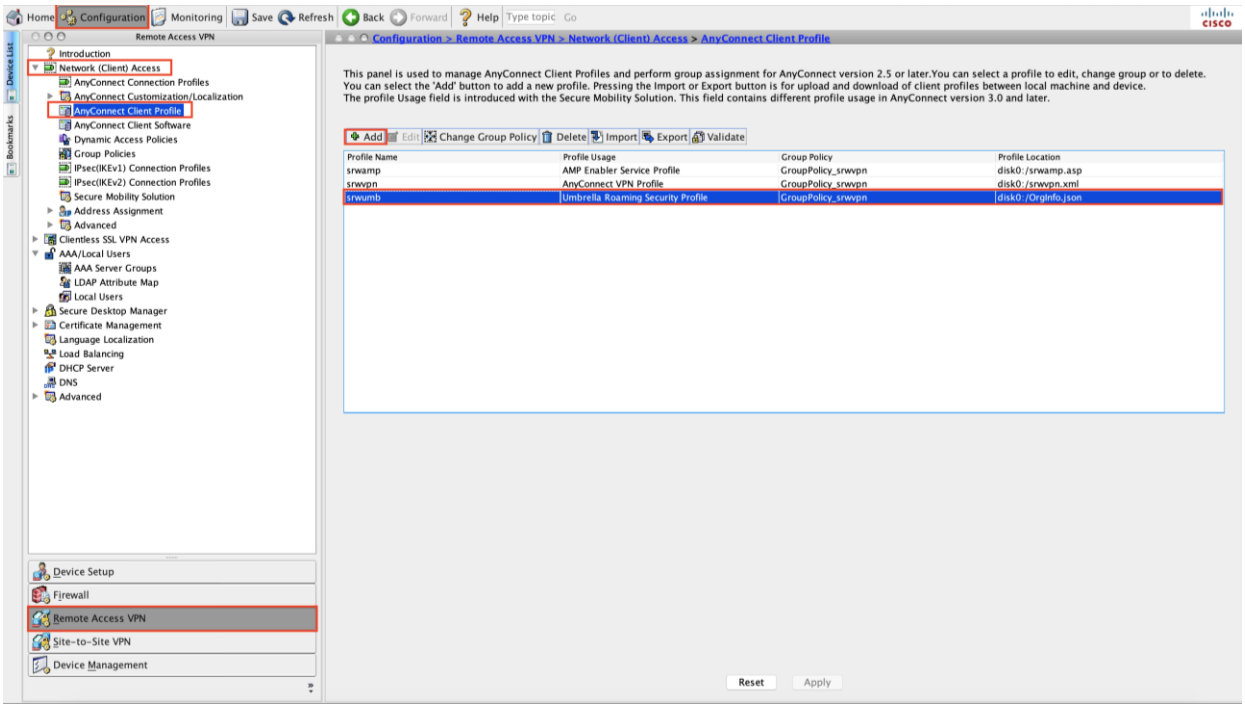
Step 3. Enable Umbrella Roaming Security Profile

Step 4. Enable Umbrella DNS Security

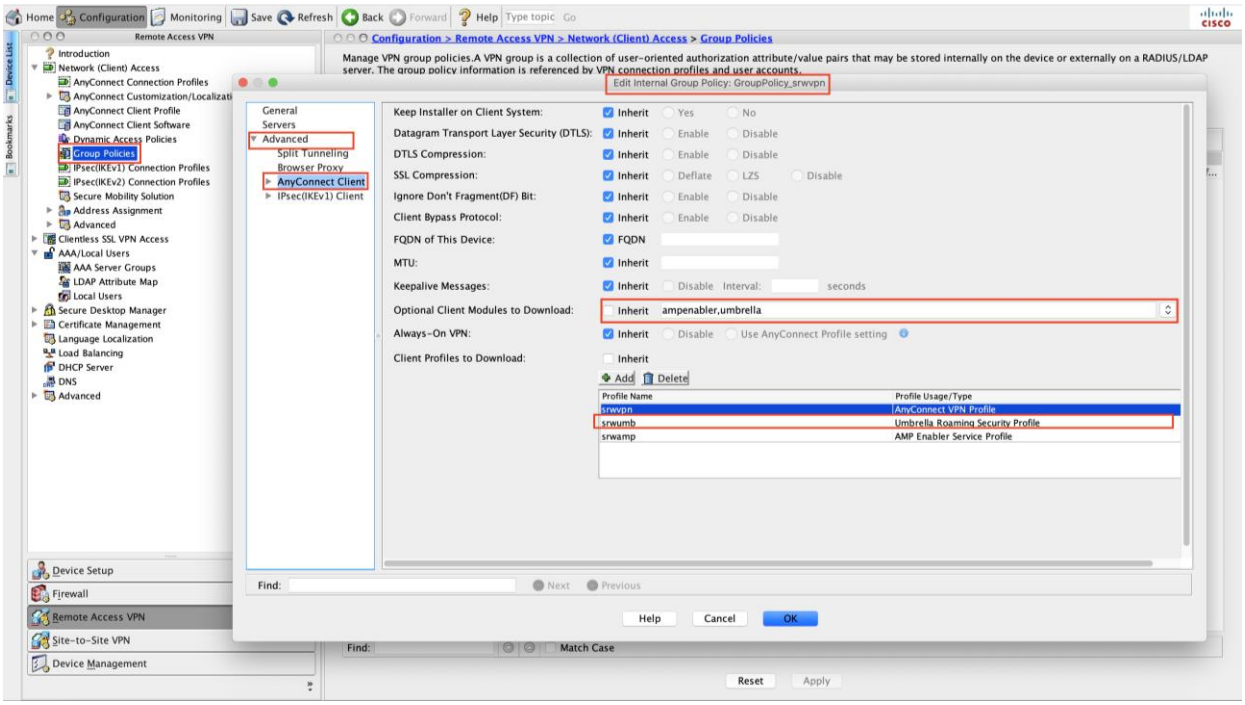
Step 1. Download Umbrella Roaming Security Module: - Access Cisco Umbrella portal, navigate to Deployments → Core Identities → Roaming Computers, and click Roaming Client. Download module profile (OrgInfo.json). (Cisco Umbrella Documentation)



Step 2. Setup AnyConnect Client Profile - In ADSM, navigate to Configuration → Remote Access VPN → Network (Client) Access → AnyConnect Client Profile → Click add. Now let's upload OrgInfo.json file to Cisco ASA and map it with AnyConnect VPN profile, Umbrella roaming security profile, and Group Policy.

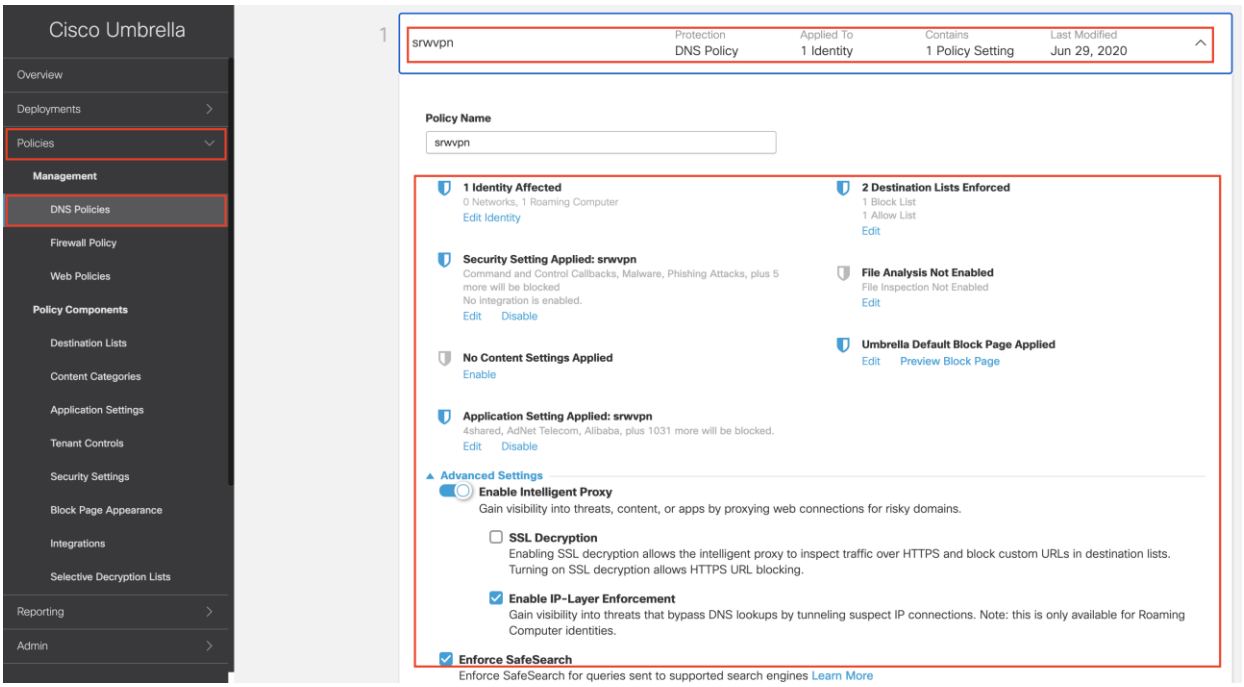


Step 3. Enable Umbrella Roaming Security Profile: Navigate to Configuration → Remote Access VPN → Network (Client) Access → Group Policy → select Group_Policy, now ensure it has Umbrella Roaming Security Profile enabled



Note: Uncheck Inherit and select umbrella from the drop-down menu.

Step 4. Enable Cisco Umbrella Security - Access Umbrella portal and navigate to Policies → DNS policies -> Create DNS policy to enable DNS layer security. This policy blocks users from accessing malicious websites.



Cisco AMP Enabler

Cisco AMP Enabler – Now we have Cisco AnyConnect is integrated with Cisco Duo, and Cisco Umbrella Roaming Security Module. Let's integrate Cisco Secure Anyconnect Mobility Client with Cisco AMP (Cisco AMP enabler documentation)

Step 1. Create Endpoint Group for RAVPN users

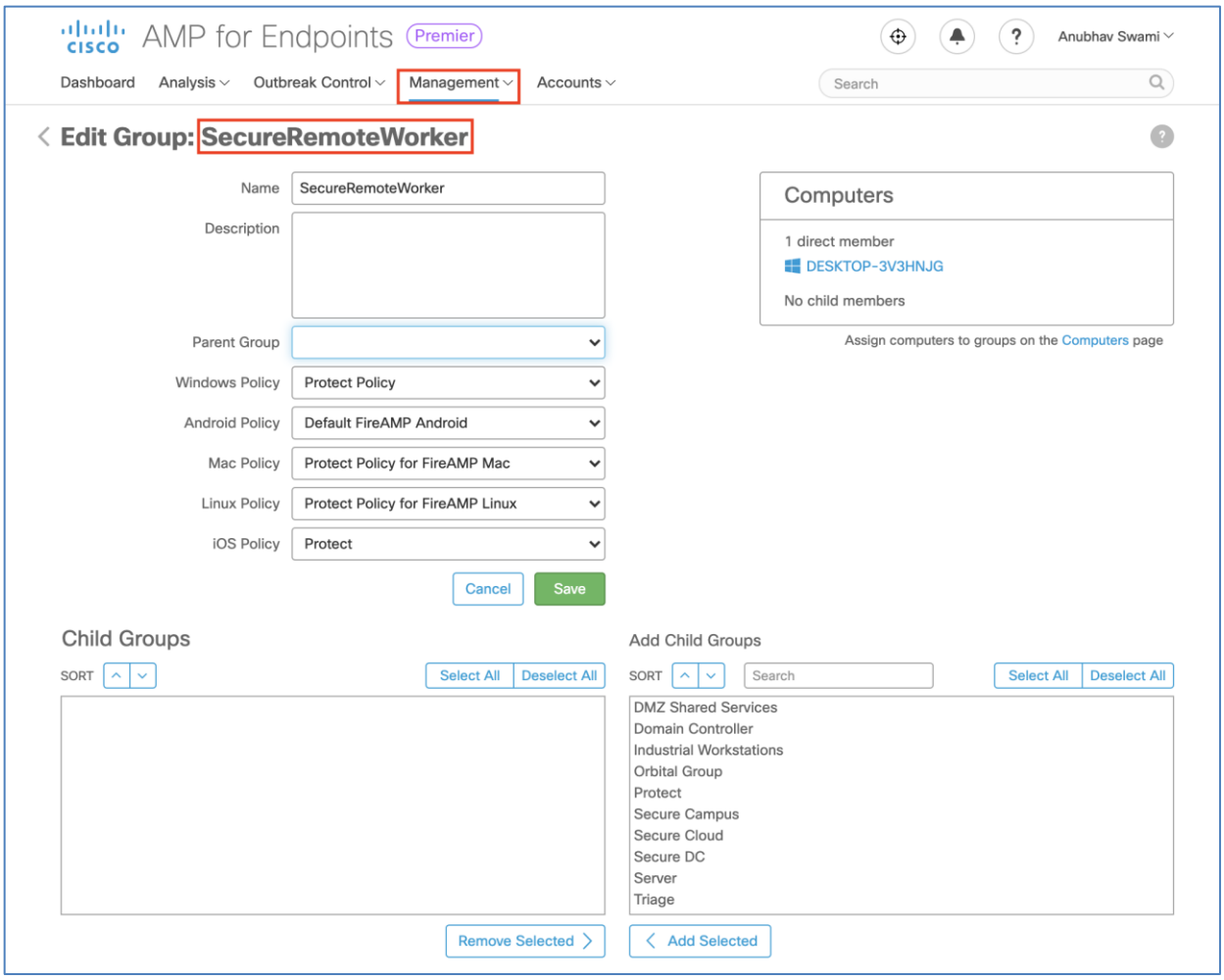
Step 2. Create Endpoint Group policy for RAVPN users

Step 3. Download connectors for MAC, Windows, Linux, and Android

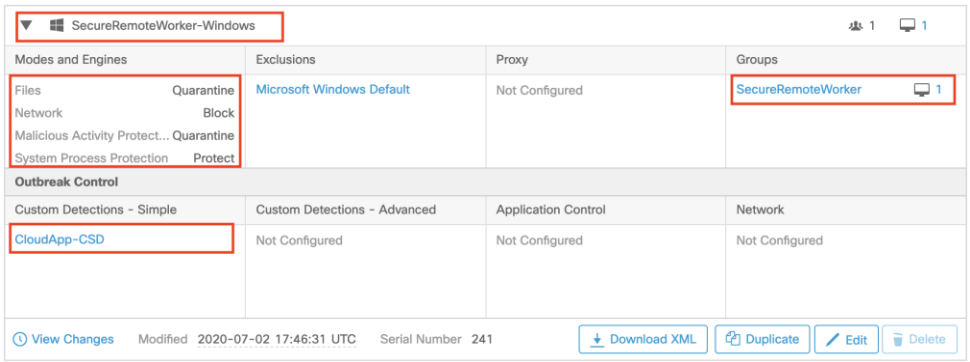
Step 4. Add AMP Enabler Service Profile

Step 5. Edit the Group-Policy to Download the AnyConnect AMP Enabler

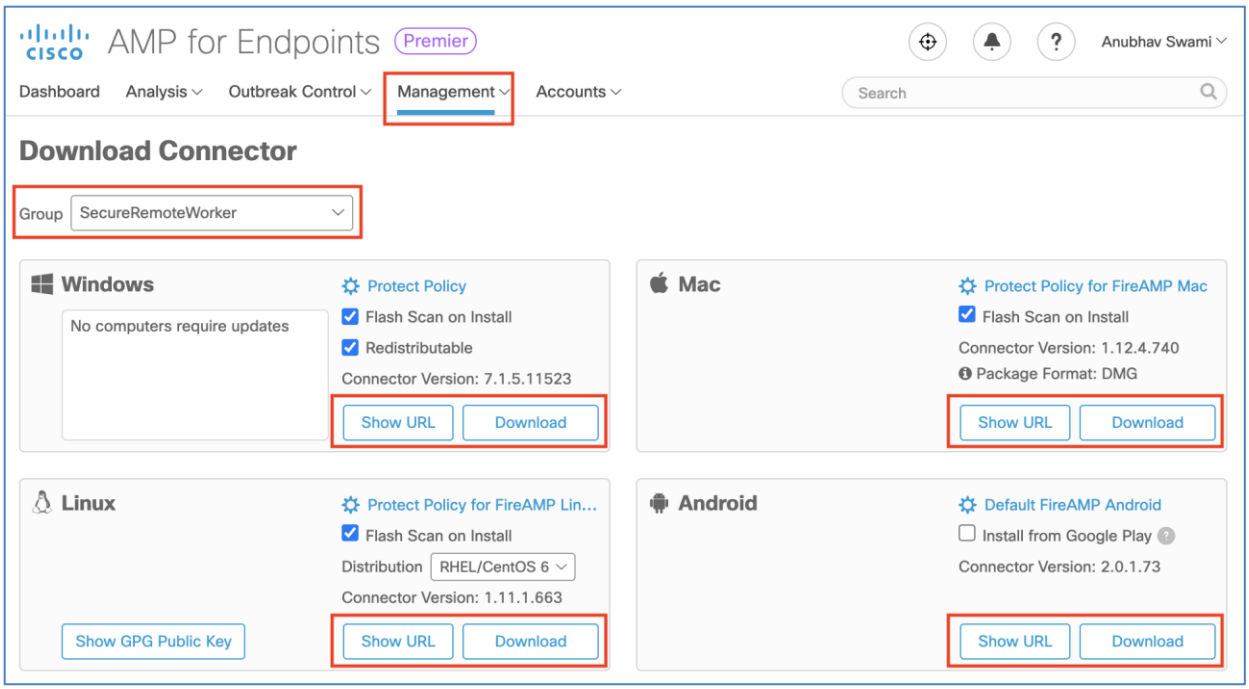
Step 1. Create Endpoint Group for RAVPN users - Access Cisco AMP portal, navigate to management → groups → create group



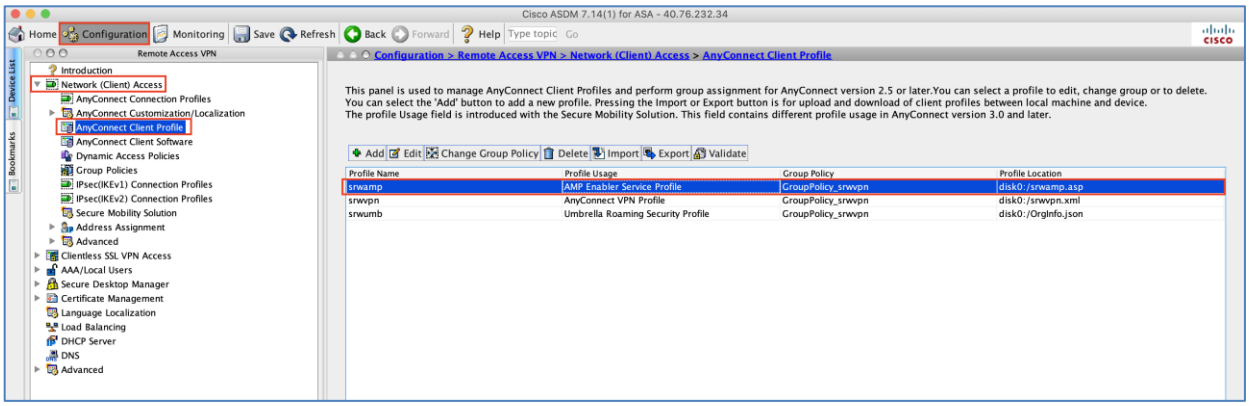
Step 2. Create Endpoint Group policy for RAVPN users – Create a policy for windows endpoint and attach it to the “SecureRemoteWorker” Group. Also, configure "custom detection" to block specific hash value.



Step 3. Download connectors for MAC, Windows, Linux, and Android – Access Cisco AMP portal, navigate to management → download connector → select SecureRemoteWorker from the drop-down menu. You can also use URLs and use URLs in firewalls configuration. If firewall reports error with URL, download connectors and host connectors in AWS S3 bucket.

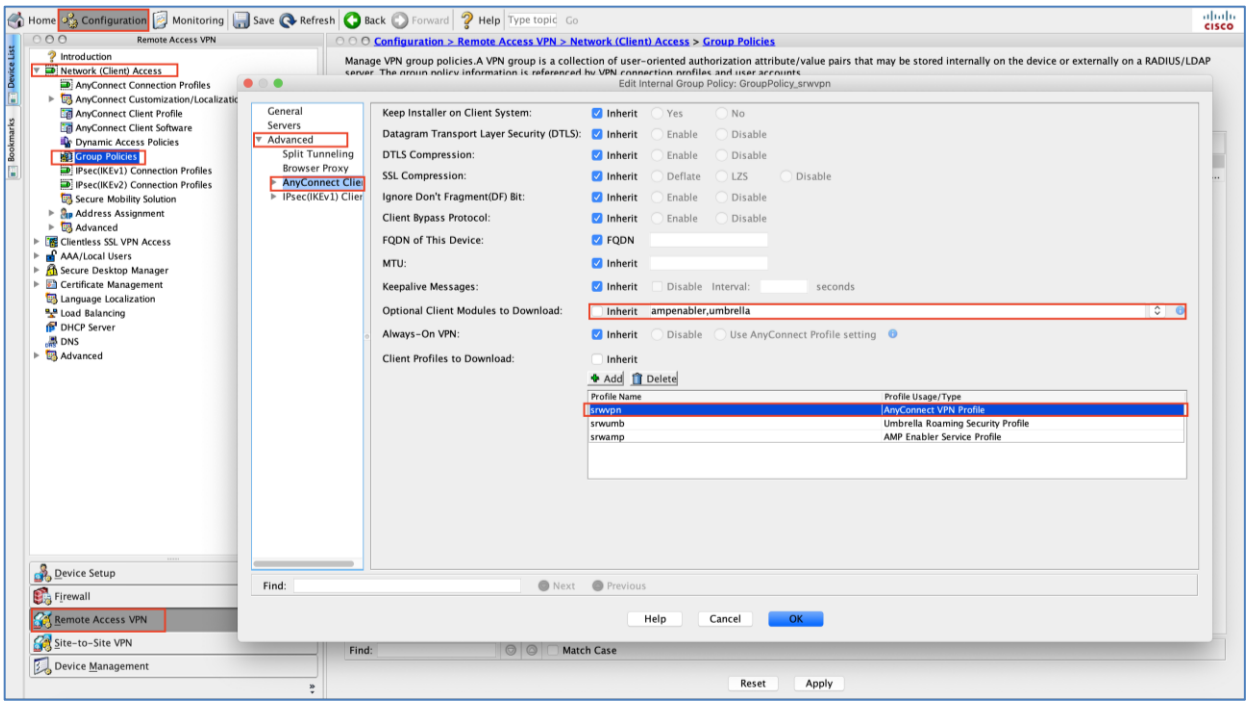


Step 4. Add AMP Enabler Service Profile -Navigate to Configuration → Remote Access VPN → Network (Client) Access → AnyConnect Client Profile. Add the AMP Enabler Service Profile, point to connect URL shown in **step 3**.



Step 5. Edit the Group-Policy to Download the AnyConnect AMP Enabler

- Navigate to **Configuration → Remove Access VPN → Group Policies → Edit**
- Go to Advanced → AnyConnect Client → Optional Client Modules to Download
- Choose **AnyConnect AMP Enabler**

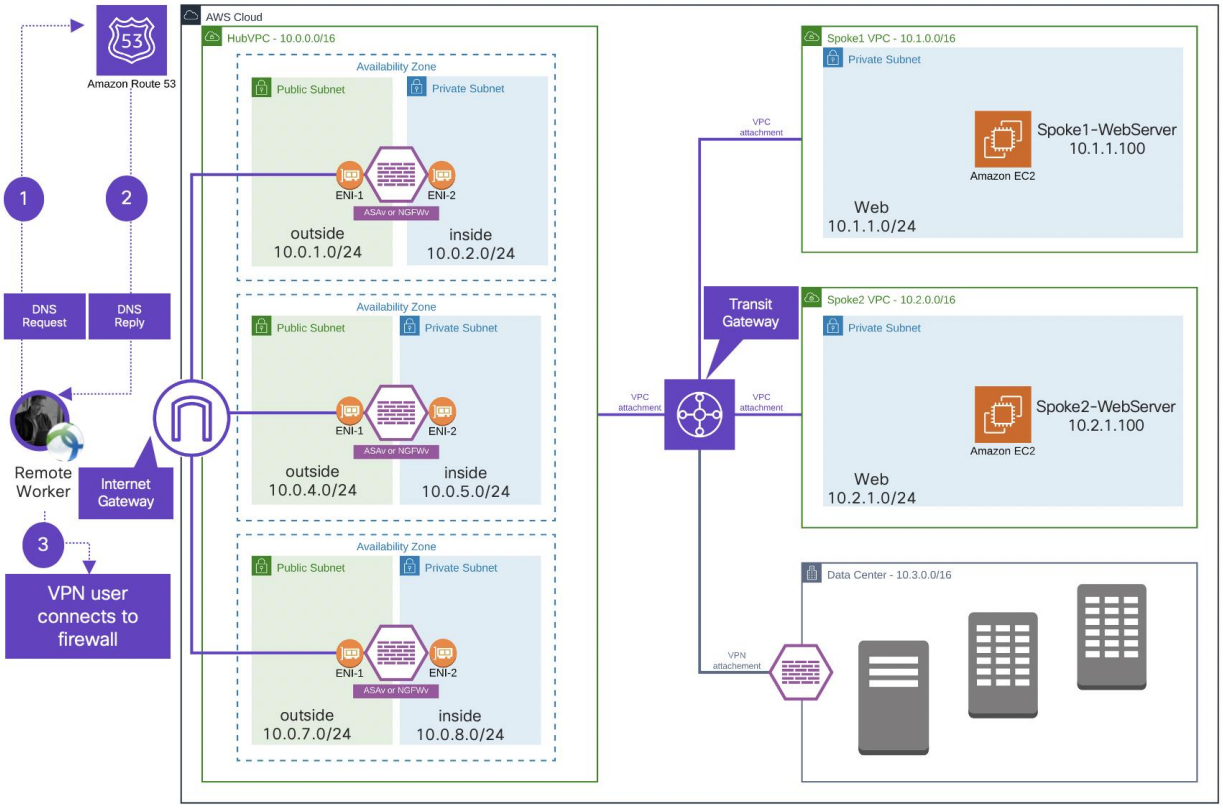


Validation Testing

Test Case 1 – Cisco AnyConnect Remote Access VPN load balancing using AWS route 53

The secure remote worker initiates a connection to srwvpn.com (srwvpn.com mapped HubASA01, HubASA02, and HubASA03 in endpoints. AWS route 53 keeps track of Cisco firewalls on TCP 443, as long as the firewall responds to these probes firewall is marked as online.

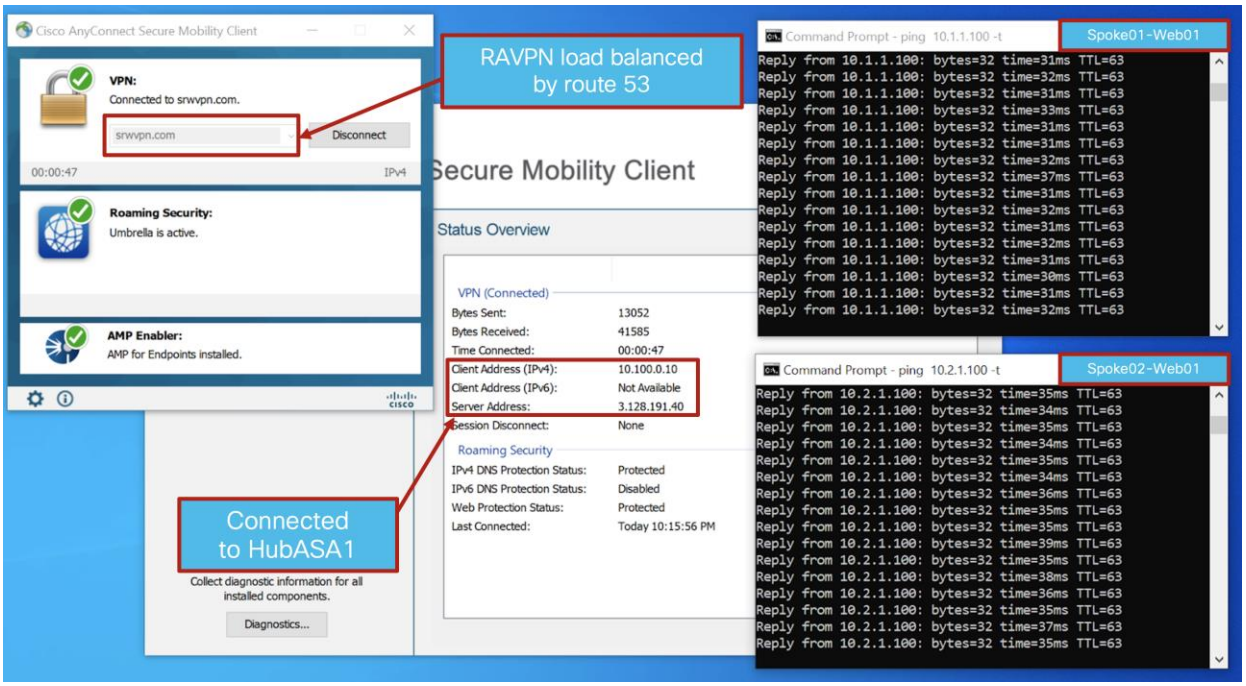
The AWS route 53 is responsible for load balancing SSL VPN across HubASA01, HubASA02, and HubASA03.



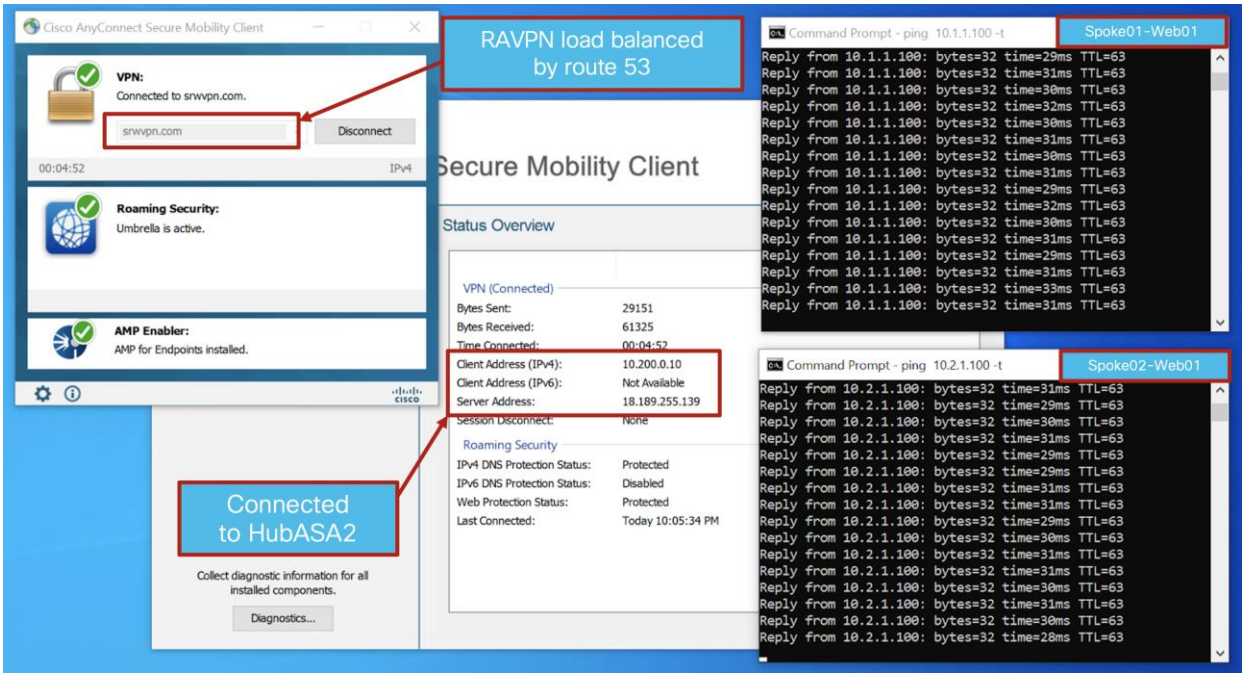
The AWS route 53 endpoint configuration ensure equal load distribution of SSL RAVPN.

Record name	Type	Routing policy	Differentiator	Alias	Value/Route traffic to	TTL (seconds)	Health check	Evaluate target health	Record ID
srwvpn.com	A	Weighted	0	No	3.128.191.40	60	d35cc4ff-21ce-42d2-9267-c86c42fdec9f	-	HubASA01
srwvpn.com	A	Weighted	0	No	18.189.255.139	60	e6927830-db03-4686-bc6f-7dd45d1708a9	-	HubASA02
srwvpn.com	A	Weighted	0	No	3.128.48.85	60	1e3c61d9-2d0d-4875-b66d-01e9291b062b	-	HubASA03

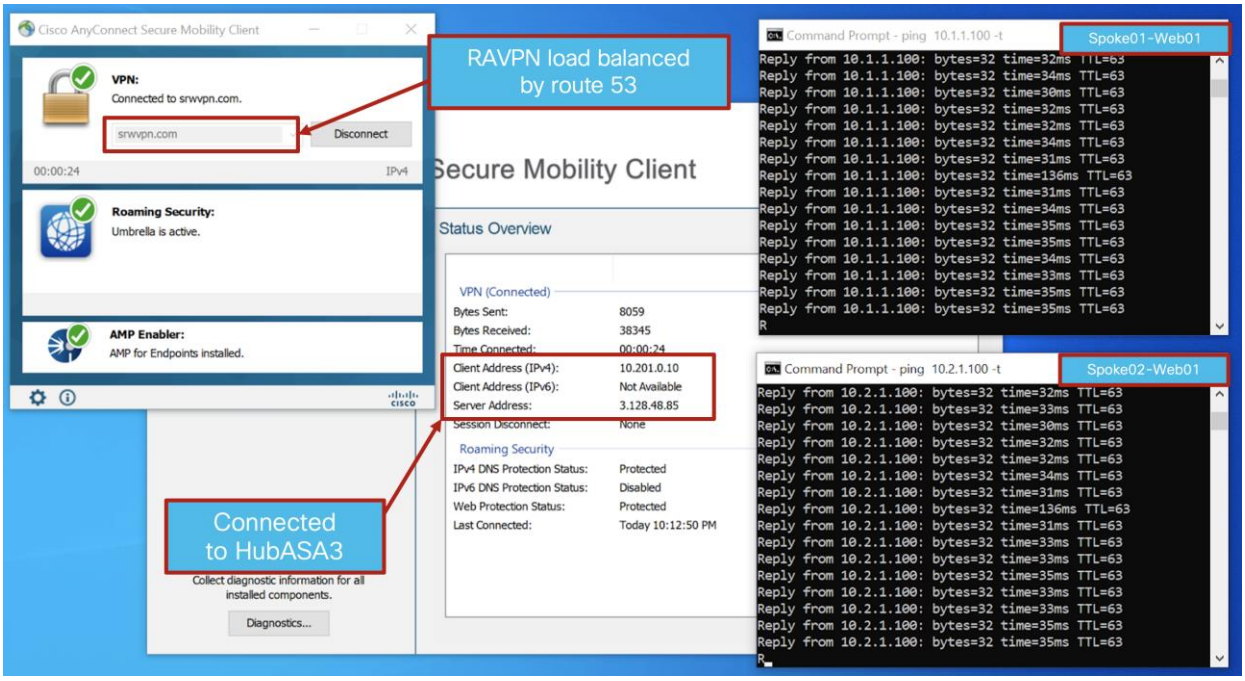
Remote worker is connected to srwvpn.com and session is terminated on HubASA01 (firewall 1). User is able to access workloads in Spoke1VPC and Spoke2VPC.



Remote worker is connected to srwvpn.com and session is terminated on HubASA2 (firewall 2). User is able to access workloads in Spoke1VPC and Spoke2VPC.



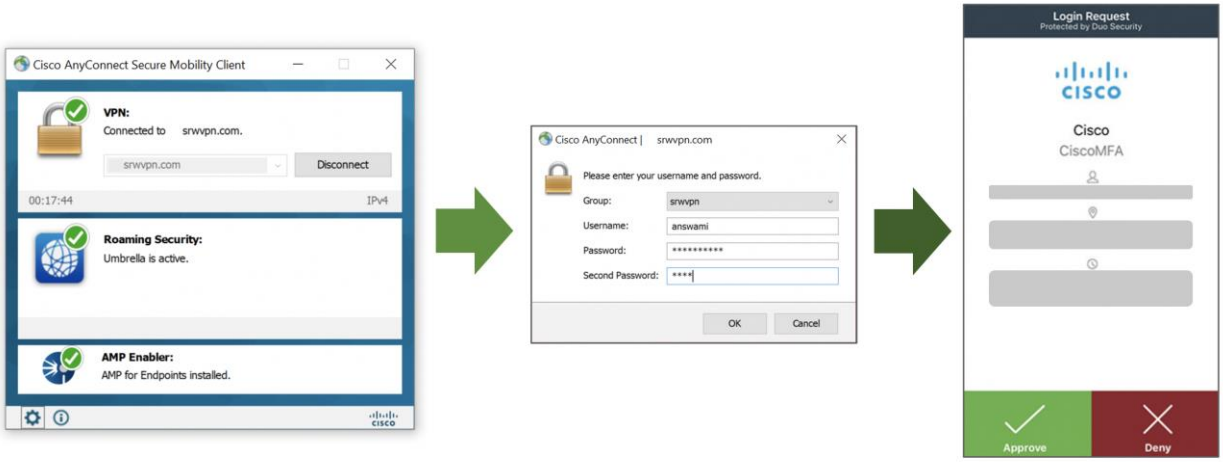
Remote worker is connected to srwvpn.com and session is terminated on HubASA3 (firewall 3). User is able to access workloads in Spoke1VPC and Spoke2VPC



Test Case 2 – Cisco Duo two-factor authentication (2FA)

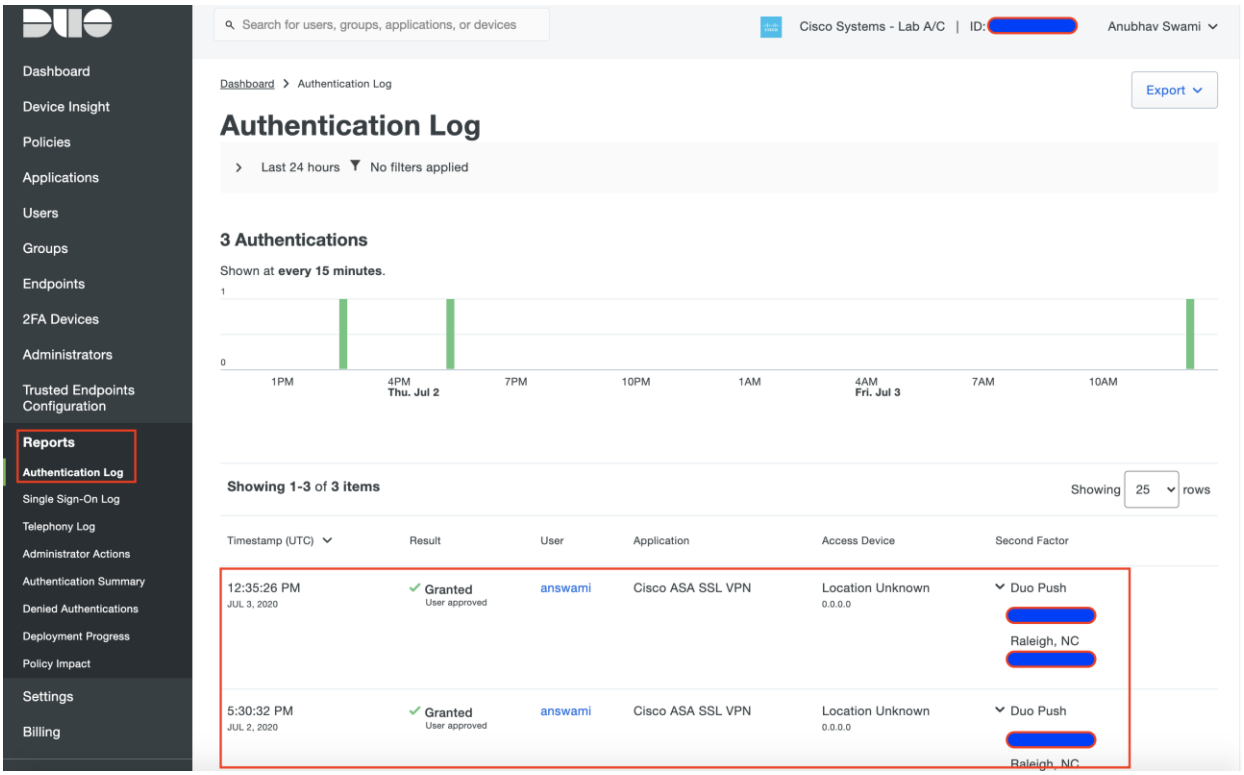
When a remote access VPN user connects to the secure network, the user is challenged to enter a primary and secondary password. RAVPN user must provide the primary password as configured on the LDAP server, and in the secondary password, the user can enter "push, text, or call". Duo sends a challenge for two-factor authentication post-primary authentication is successful.

AnyConnect VPN client user experience



Cisco Duo portal shows information about authenticated users; it provides the IP address, enrollment information, and timestamp.

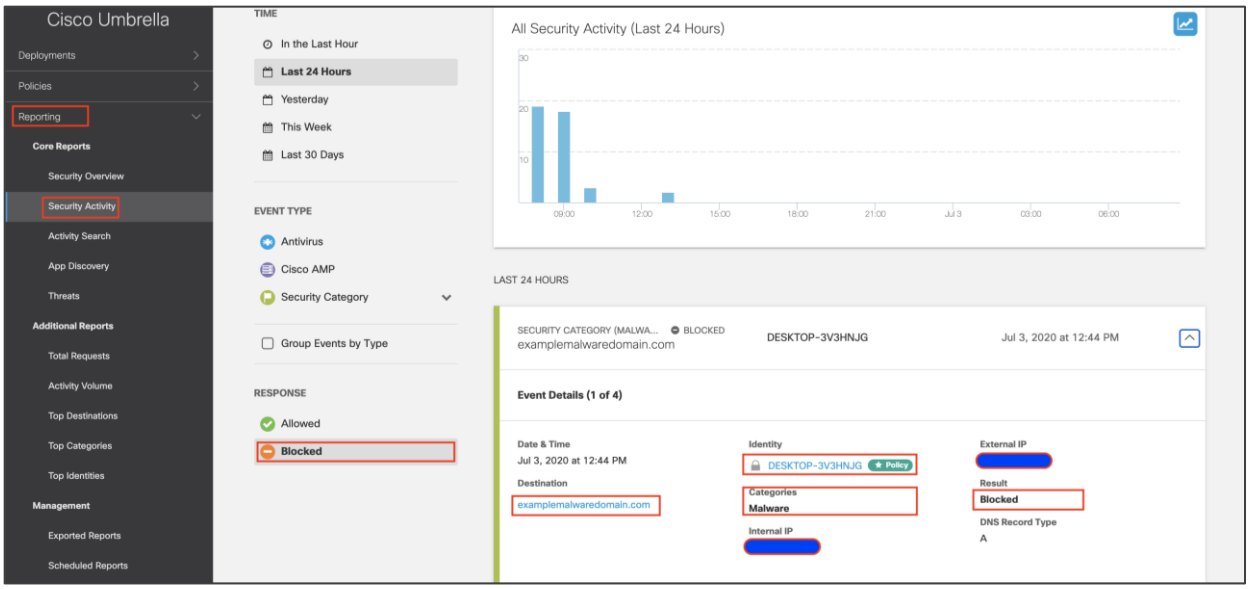
Access Duo admin portal and navigate to Navigate Reports → Authentication Logs.



Test Case 3 – Cisco Umbrella Roaming Security Module (DNS layer protection)

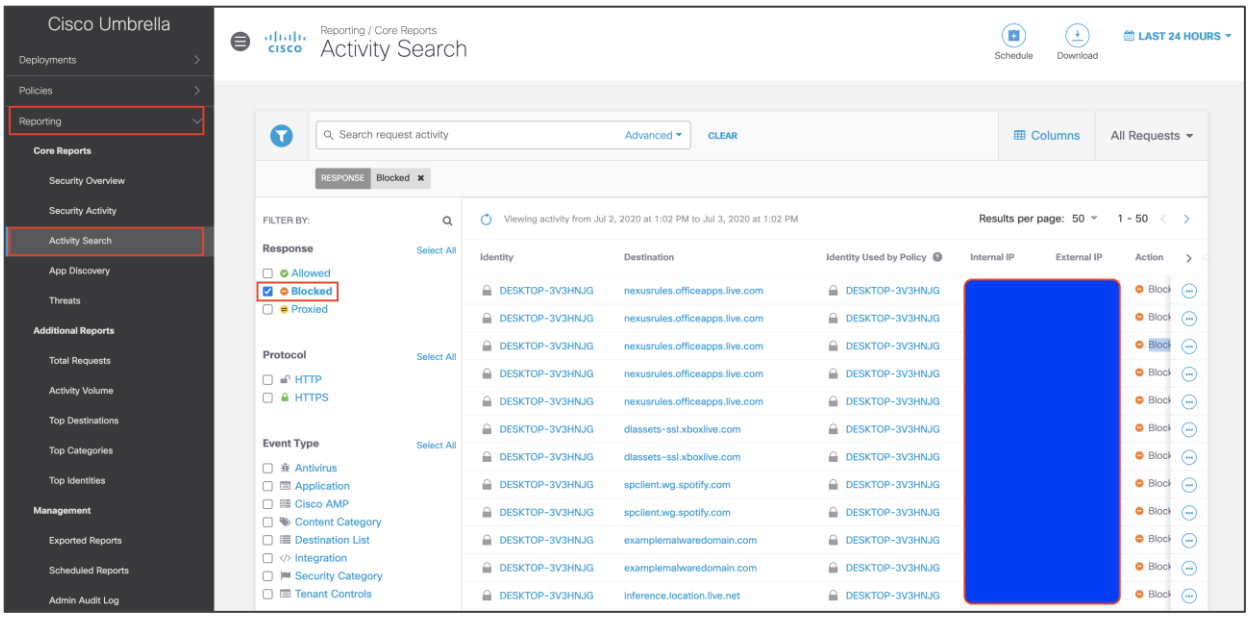
Cisco Umbrella Roaming Security Module for Cisco Secure AnyConnect Mobility Client enforces DNS layer security. Administrators can enforce DNS policies configured for the on-premise users to RAVPN users also regardless of whether remote access VPN users is connected to the secure network or not. In the deployment section, we added a DNS policy that blocks traffic to malicious sites. On the RAVPN client, we access "examplemalwaredomain.com," and Umbrella drops traffic, and the user sees the Umbrella block page.

To view logs access Cisco Umbrella portal and navigate to reporting → core reporting → security activity

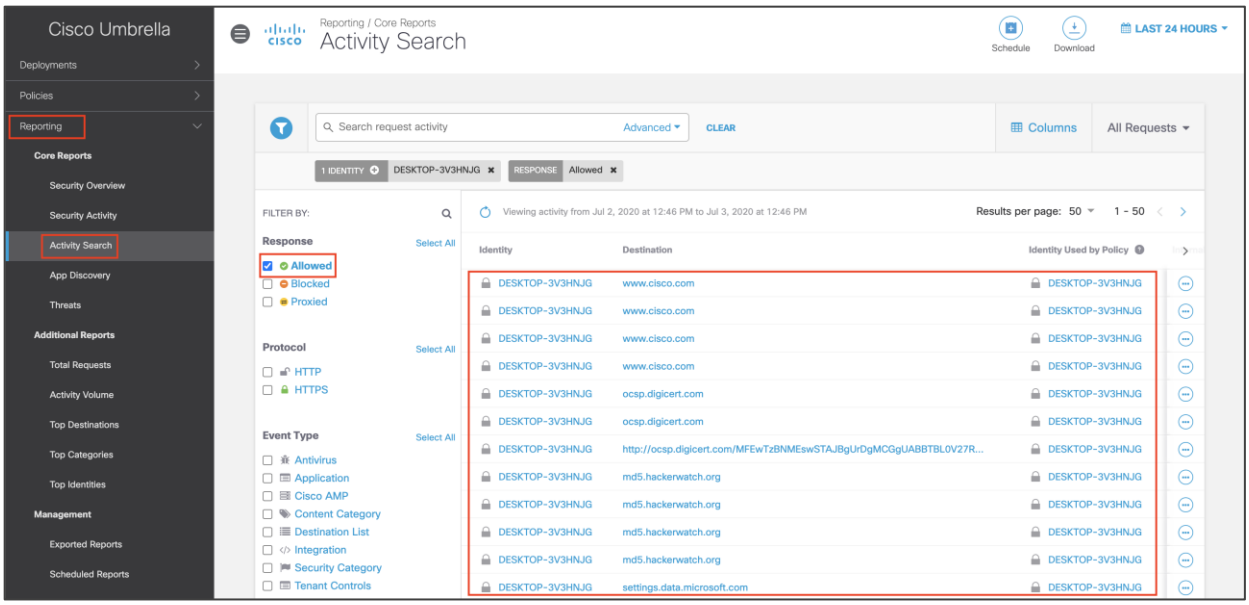


To search activity logs access Cisco Umbrella admin portal and navigate to reporting → activity search

Blocked Sessions

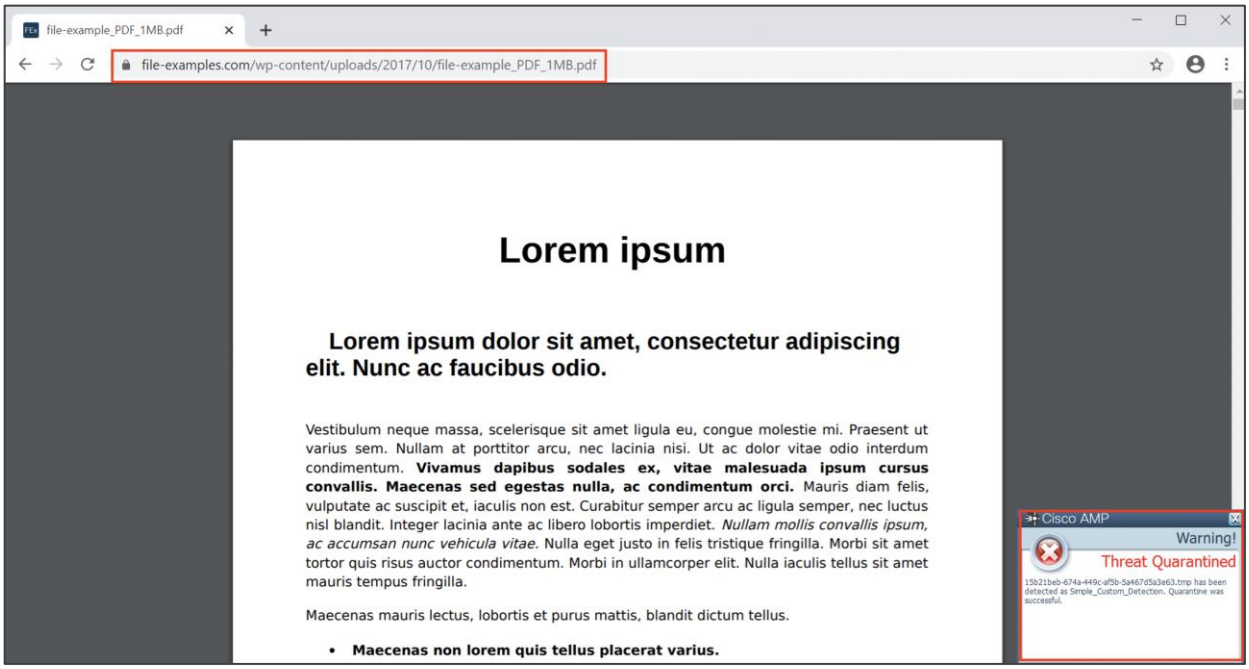


Allowed sessions

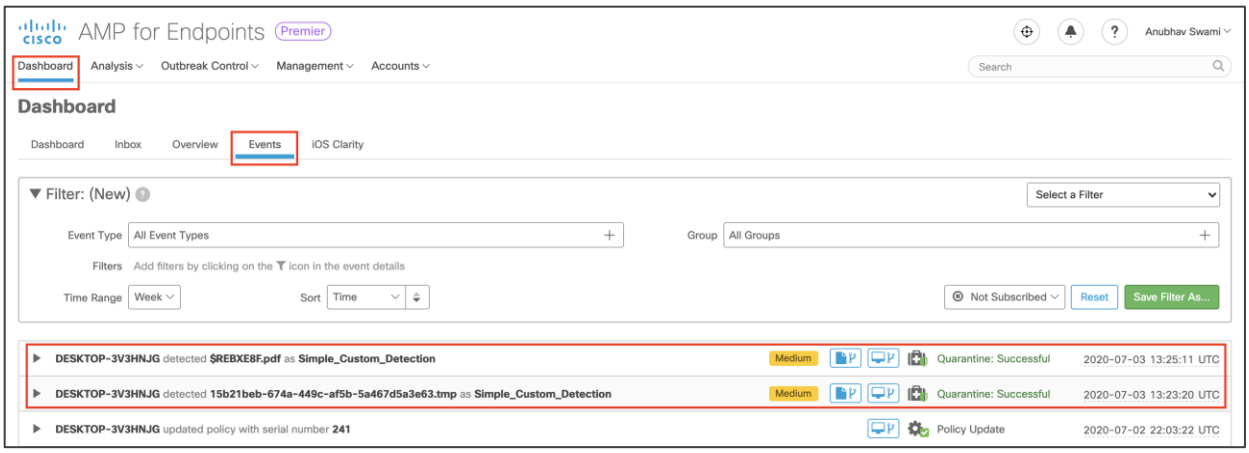


Test Case 4 – Cisco AMP enabler (File blocking)

Cisco Secure AnyConnect Mobility Client provides integration with the AMP enabler module. AMP enabler ensures that the remote access user stays protected from malware. In the deployment section, we integrated the AnyConnect client with AMP enabler and configured a policy to block the file with a specific hash value. On the RAVPN user tries to download a blocked file.



To search activity logs access Cisco AMP portal and navigate to dashboard → events.



Appendix

Appendix A - Summary

Cisco Secure Remote Worker Architecture outlines the design principle for a highly scalable and resilient design for remote access VPN. Today remote workers are the majority of the workforce, and an organization must provide unmatched security to the remote workers. This design guide provides detailed information on validated designs for RAVPN and positioning firewalls in AWS.

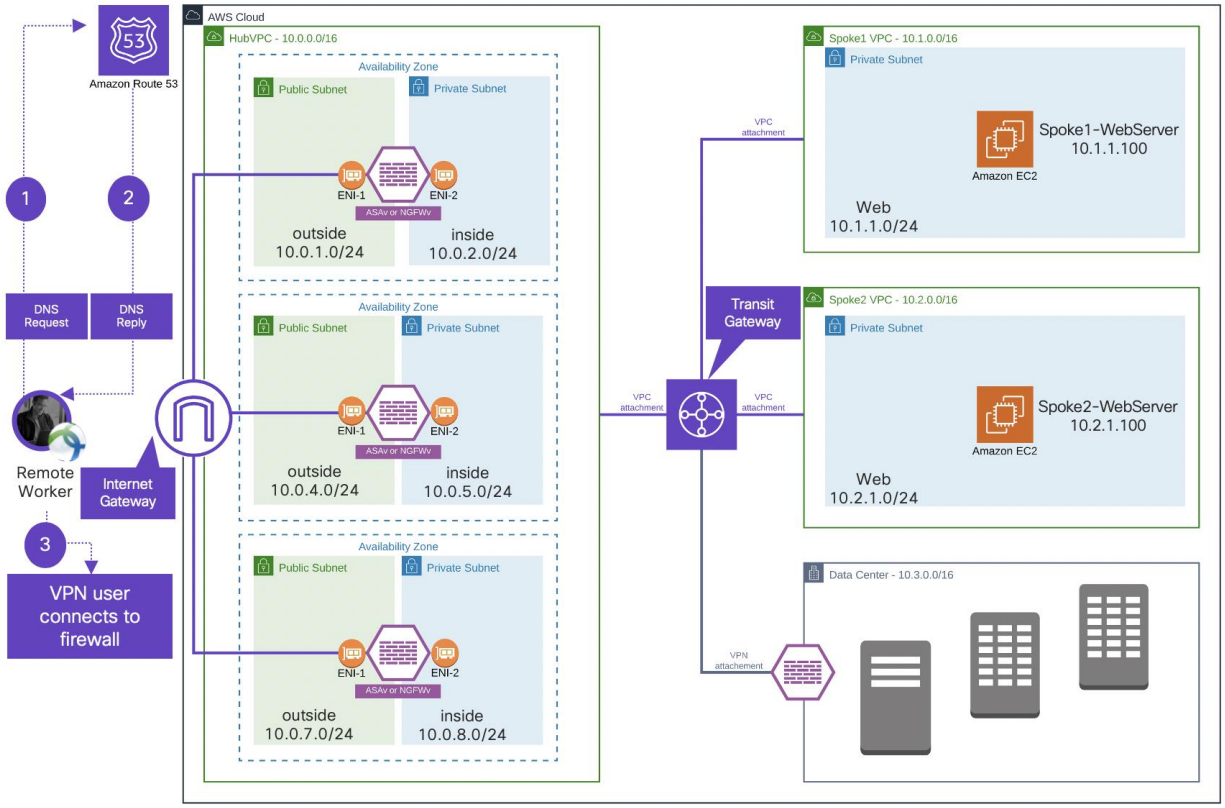


Figure 27. **Components of the Cisco secure remote worker solution**

This document describes how to load balancing RAVPN connection, scaleout when required. In addition to scalability, cisco integrates with other security modules for better visibility and threat management.

- Cisco Duo (Two-factor Authentication)
- Cisco Umbrella Roaming Security Module (DNS layer security)
- Cisco AMP enabler (Malware protection)

Appendix B - Maximum RAVPN sessions support on ASA and NGFW

The maximum number of remote access VPN sessions supported on the Cisco ASA and Cisco Next-Generation Firewall.

Cisco ASAv datasheet: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/datasheet-c78-733399.html

Cisco NGFWv datasheet: https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/datasheet-c78-742858.html

Appendix C - Licensing information

This section defines the packaging structure and licensing information for the Cisco AnyConnect secure mobility client. The following AnyConnect VPN licenses are available:

- Plus subscription license
- Plus perpetual license
- Apex subscription license
- VPN only perpetual license

Subscription licenses are term-based licenses available in terms of 12 to 60 months.

Perpetual licenses are permanent licenses.

Plus license includes basic VPN services such as device and per-application VPN, trusted network detection, basic device context collection, FIPS compliance, Network Access Manager 802.1X supplicant, the Cloud Web Security module, and the Cisco Umbrella Roaming module. The existing AnyConnect customers should think of AnyConnect Plus as similar to the previous AnyConnect Essentials.

Apex license includes more advanced services such as endpoint posture checks (hostscan through ASA VPN, or ISE Posture through the Cisco Identity Services Engine), network visibility, next-generation VPN encryption, and clientless remote access VPN as well as all the capabilities of AnyConnect Plus. The existing AnyConnect customers should think of AnyConnect Apex as similar to previous AnyConnect Premium and Premium Shared Licenses.

- Clientless (browser-based) VPN termination on the Cisco Adaptive Security Appliance
- VPN compliance and posture agent in conjunction with the Cisco Adaptive Security Appliance
- Unified compliance and posture agent in conjunction with the Cisco Identity Services Engine 1.3 or later
- Next-generation encryption (Suite B) with AnyConnect and third-party (non-AnyConnect) IKEv2 VPN clients
- Network Visibility Module
- ASA multi-context mode remote access
- SAML Authentication (new in 4.4 with ASA 9.7.1 or later)
- All Plus services described above

VPN-only licenses are perpetual based, clientless, and may only be used on a single ASA. The web security module, cisco umbrella roaming, ISE posture, network visibility is not supported. VPN-only license provides the following functionality:

- VPN functionality for PC and mobile platforms, including per-application VPN on mobile platforms, Cisco phone VPN, and third-party (non-AnyConnect) IKEv2 VPN clients
- Clientless (browser-based) VPN termination on the Cisco Adaptive Security Appliance
- VPN-only compliance and posture agent in conjunction with the Cisco Adaptive Security Appliance
- FIPS compliance
- Next-generation encryption (Suite B) with AnyConnect and third-party (non-AnyConnect) IKEv2 VPN clients
- SAML Authentication (new in AnyConnect 4.4 with ASA 9.7.1 or later)

The Anyconnect Secure Mobility Licenses are supported on the following platforms:

- Cisco Adaptive Security Appliance (Physical and Virtual)
- Cisco Next-Generation Firewall (Physical and Virtual)
- Licensing information

Appendix D - Acronyms Defined

ACL – Access Control List
AD – Active Directory
AMP – Advanced Malware Protection
AMP4E – Advanced Malware Protection for Endpoints
ASAv – Adaptative Security Virtual Appliance
ASDM – Adaptive Security Appliance Device Manager
AVC – Application Visibility and Control
AZ – Availability Zone
CDO – Cisco Defense Orchestrator
CFT – CloudFormation Template
CVD – Cisco Validated Design
ELB – External Load Balancer or Elastic Load balancer
ENI – Elastic Network Interface
FDM – Firepower Device Manager
FMC – Firepower Management Center
FQDN - Fully Qualified Domain Name / DNS Name
FTD – Firepower Threat Defense
IGW – Internet Gateway
ILB – Internal Load Balancer
MFA - Multi Factor Authentication
NGW – NAT Gateway
NGFWv – Next-Generation Firewall Virtual
NGIPS – Next Generation Intrusion Prevention System
NVA – Network Virtual Appliance
PIN – Place in network

RAVPN – Remote Access VPN
Route53 – DNS Services
RT – Route Table
SG – Security Group
TGW – Transit Gateway
VPC – Virtual Private Cloud
VPN – Virtual private network

Appendix E - References

This section will list all the references:

SAFE Secure Internet Edge Architecture Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-architecture-guide-pin-secure-internet-edge.pdf

SAFE Secure Internet Architecture Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-internet-architecture-guide.pdf

SAFE Edge Remote Access VPN with DDoS Design Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-design-guide-edge-remote-access-vpn-ddos.pdf

SAFE Secure Cloud for AWS Design Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/secure-aws-design.pdf

Cisco AnyConnect VPN: https://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html

Cisco Anyconnect VPN Ordering Guide: https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

Cisco Adaptive Security Appliance (ASA): https://www.cisco.com/go/asa

Cisco Next-Generation Firewall (NGFW): https://www.cisco.com/go/ngfw

Cisco Anyconnect Secure Mobility License Ordering Guide: https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

Cisco Umbrella Roaming Security Module: https://docs.umbrella.com/deployment-umbrella/docs/anyconnect-umbrella-roaming-security-client-administrator-guide

Cisco ASAv Datasheet: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/datasheet-c78-733399.html

Cisco NGFWv Datasheet: https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/datasheet-c78-742858.html

Duo configuration Guide (ASA and FTD): http://duo.com/docs/

Cisco Duo Network Gateway: https://duo.com/docs/dng

AWS Documentation: https://docs.aws.amazon.com/

AWS Security Group: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

AWS Network Access List: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

AWS VPC: https://aws.amazon.com/vpc/

AWS Transit Gateway: https://aws.amazon.com/transit-gateway/

AWS Internet Gateway: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

AWS Elastic Load Balancer: https://aws.amazon.com/elasticloadbalancing/

AWS Route Table: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

AWS Route 53 (DNS): https://aws.amazon.com/route53/

AWS CloudFormation Template (CFT): https://aws.amazon.com/cloudformation/resources/templates/

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.