

Secure Remote Worker for Azure

Design Guide

June 2021

Contents

Abstract	3
Target Audience	4
Scope	4
Out of scope	5
SAFE Architecture Introduction	5
Business Flow and Threat Capabilities	7
Cisco Overview	8
Security Integration	12
Azure Overview	13
Azure Marketplace Listing	14
Cisco ASA v and NGFW v supported instance type	15
Cisco Secure Remote Worker Architecture for Azure	16
Traffic Flow	18
Remote access VPN key capabilities for traffic and threat management	23
Non-VPN Remote worker (Duo Network Gateway)	30
Design Implementation	30
Network Implementation Overview	30
Security Implementation Overview:	31
Set up the Azure Infrastructure	31
Authentication	51
Threat Protection	57
Validation Testing	62
Test Case 1 - Cisco AnyConnect Remote Access VPN load balancing using Azure Traffic Manager	62
Test Case 2 - Cisco Duo two-factor authentication (2FA)	64
Test Case 3 - Cisco Umbrella Roaming Security Module (DNS layer protection)	65
Test Case 4 - Cisco AMP enabler (File blocking)	67
Appendix	68
Appendix A - Summary	68
Appendix B - Maximum RAVPN sessions support on ASA and NGFW	69
Appendix C - Licensing information	69
Appendix D - Acronyms Defined	71
Appendix E - References	72

Abstract

Today companies are investing in enabling their workforce to have a secure connection to the resources hosted in the Azure (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

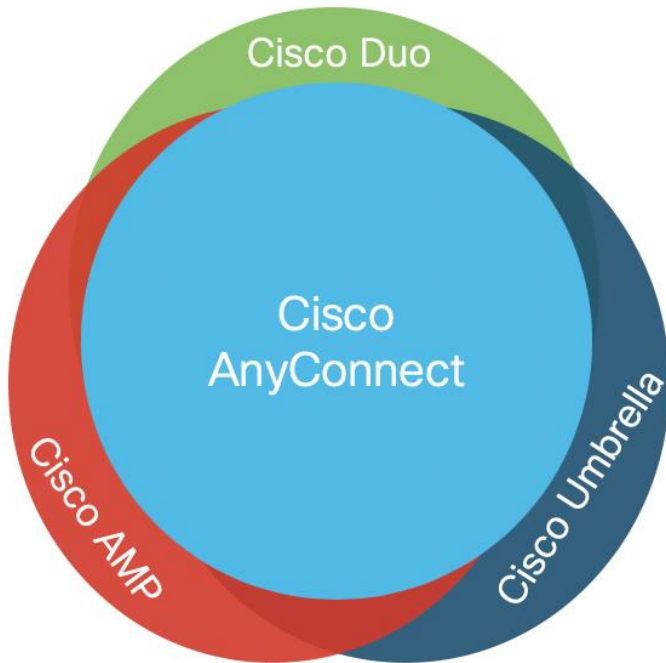


Figure 1. **Components of the Cisco secure remote worker solution**

Target Audience

This document provides best practices and recommended solutions for remote workers accessing resources hosted in the Azure 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 ASA)
- Authentication
 - LDAP
 - Duo (Two-factor authentication)
- Threat Protection
 - Cisco Umbrella Roaming Security Module (DNS Layer Security) and IP Layer Enforcement
 - Cisco Advanced Malware Protection Enabler
- Azure Services

- Virtual Network (VNet)
- VNet peering
- Route Table (UDR)
- Traffic Manager
- Azure DNS
- Network Security Group

Out of scope

This document does not cover the following topics:

- Data Center connectivity (Hybrid Cloud): IPsec, SD-WAN, Azure express route 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)
- Azure DNS or Azure Traffic based load balancing supports TLS and DTLS based load balancing, IPsec RAVPN is out of scope
- This document covers “Azure VNet peering,” i.e., the connection between VNets in the same region. “Global VNet peering” can also be used. Azure VNet peering is covered in Azure overview section in the document
- Cisco ASAv High Availability is not covered as VPN load balancing requires active/active architecture
- Custom ARM template to deploy firewalls is not part of this design guide; the user can use ARM templates uploaded in [GitHub](#) as their base ARM template and add availability zone or availability set attributes. Sample ARM template used in this guide is available in [Github](#)
- 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.

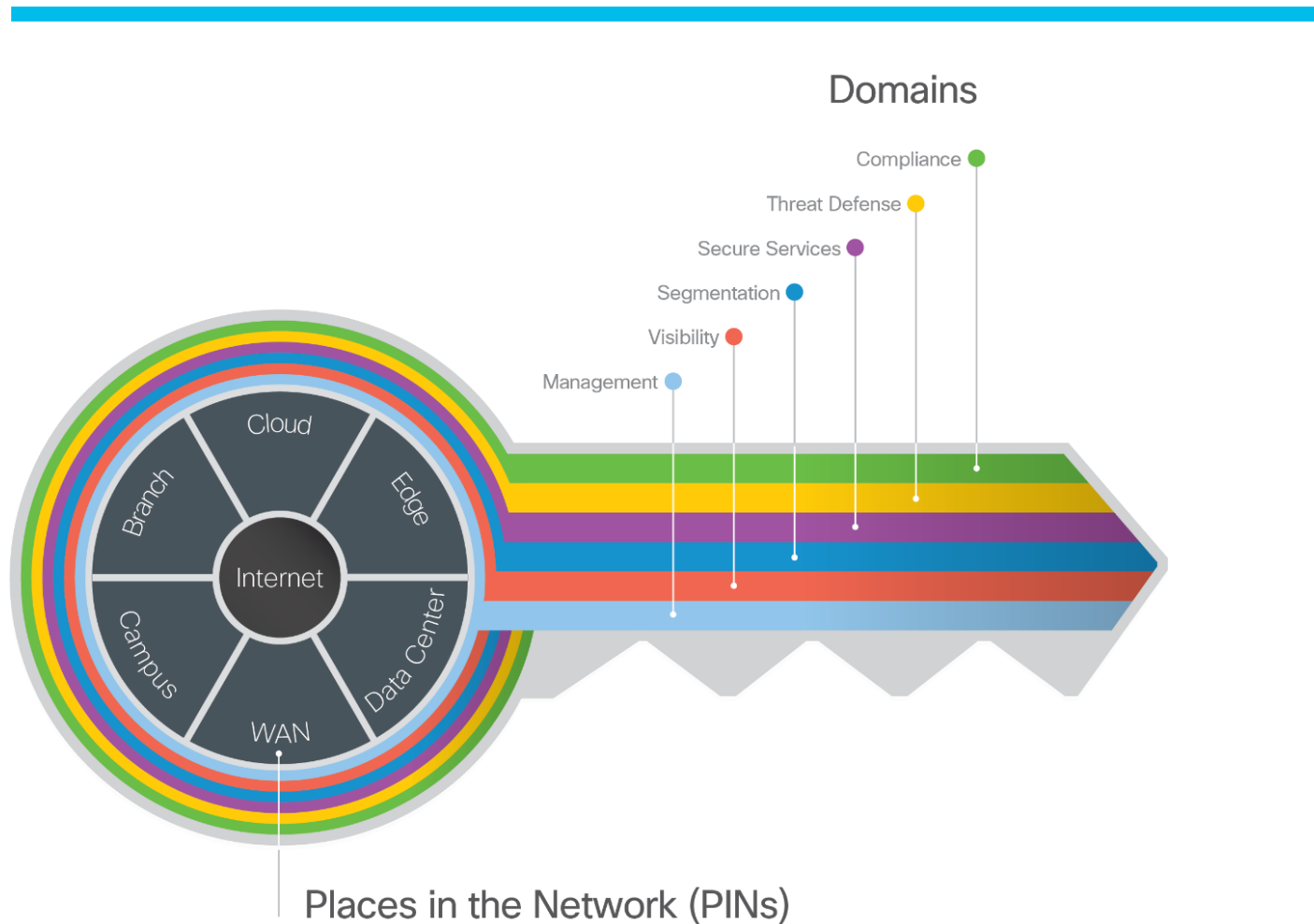


Figure 2. **key to SAFE organizes the complexity of holistic security into PINs & Secure Domain**
 The Internet edge is the highest-risk PIN because it is the primary ingress for public traffic and the primary egress point to the Internet. Simultaneously, it is the critical resource that businesses need 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.

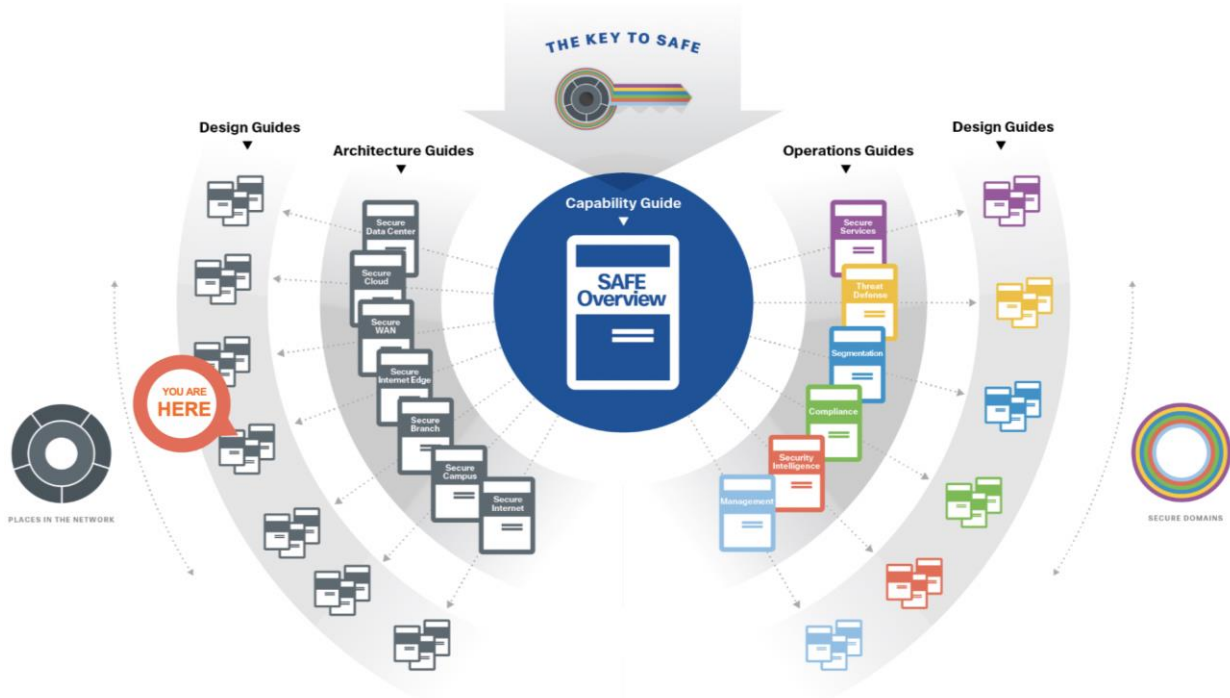


Figure 3. **SAFE Architecture and Design Guides**

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 Flow: 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.

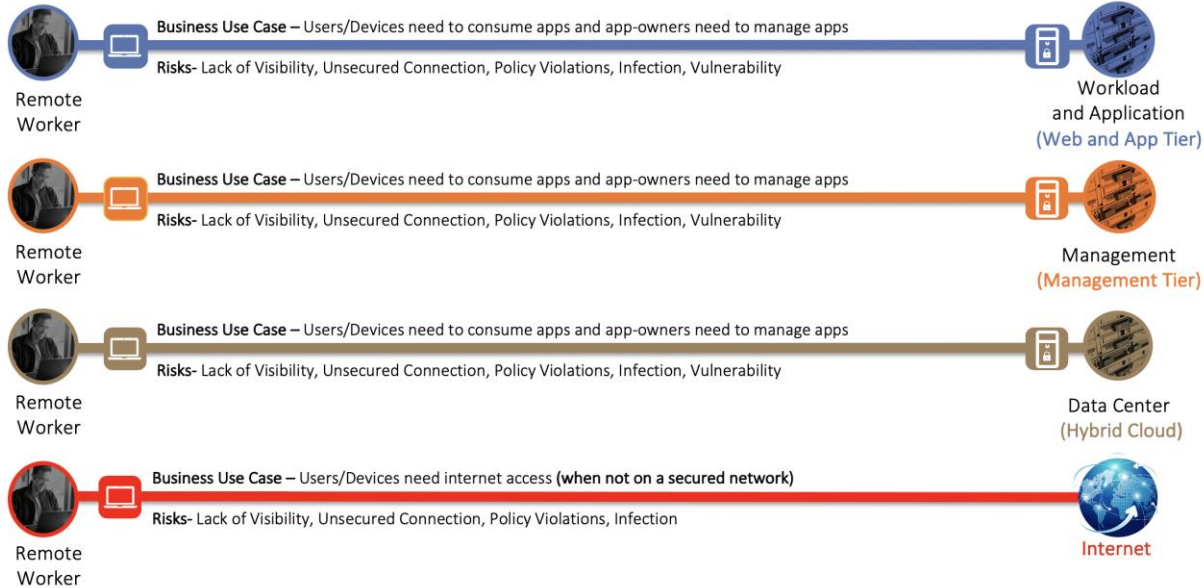


Figure 4. **The Secure Remote Worker (Azure) Business Flow**

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 Azure VNet. For more information regarding capability groups, refer to the [SAFE Overview Guide](#).

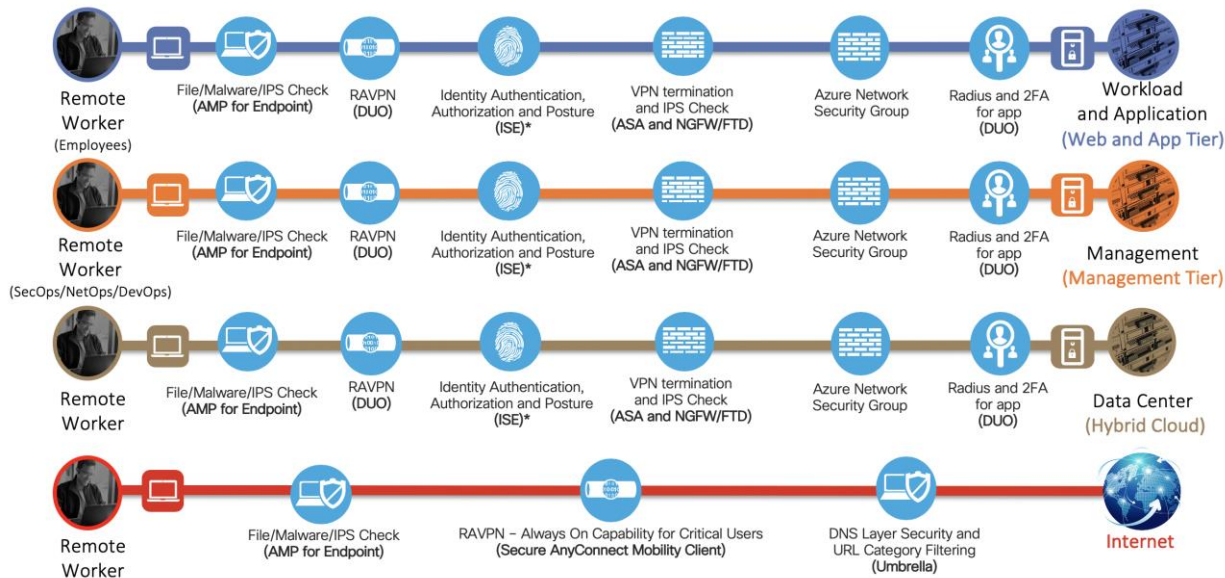


Figure 5. **Threat Capabilities for business flows**

*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) - ASA v	VPN Gateway / VPN concentrator
Cisco Firepower Next-Generation Firewall (Virtual) - NGFW v	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 ASA v and Cisco NGFW v for remote access VPN (RAVPN)

Cisco Adaptive Security Virtual Appliance (ASA v): 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 Programming 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 Programming 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>

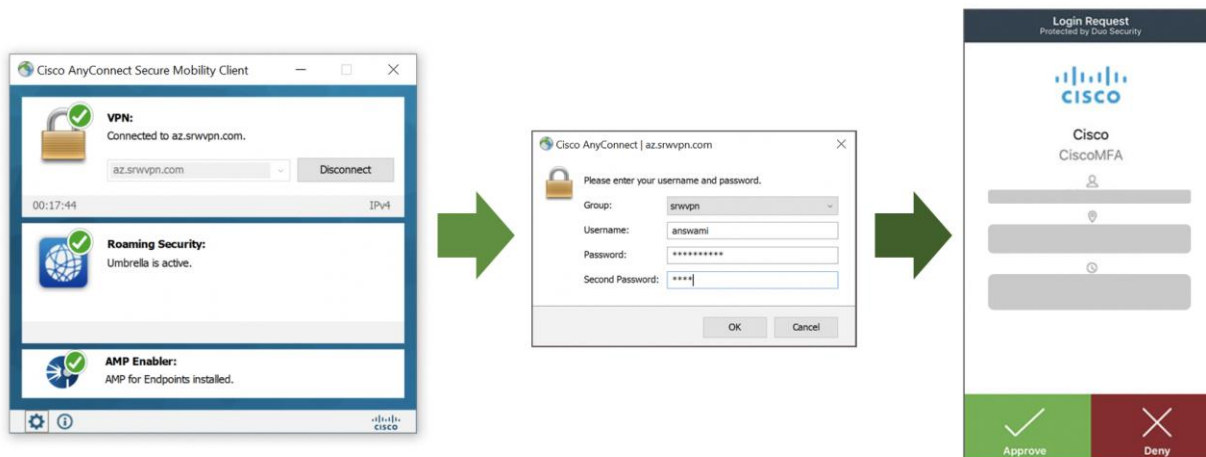


Figure 6. Cisco Duo

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.

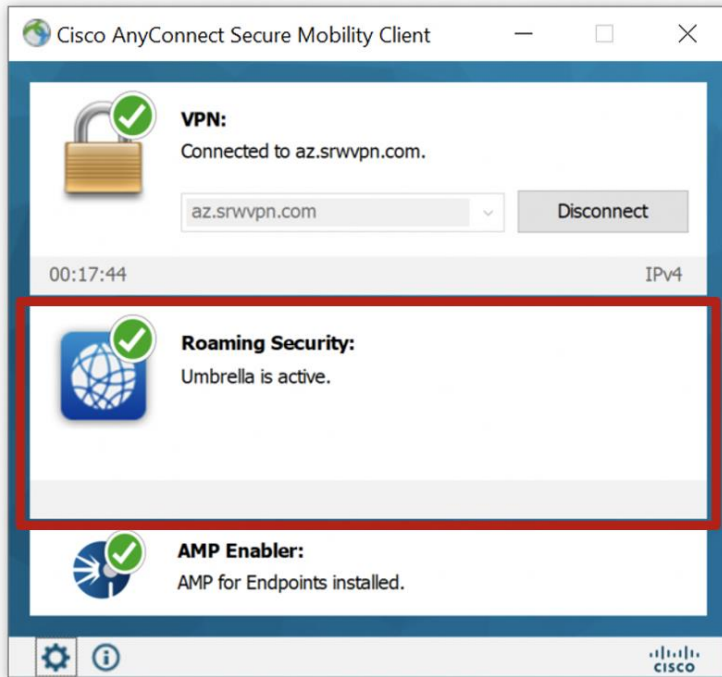


Figure 7. **Cisco Umbrella Roaming Security Module**

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

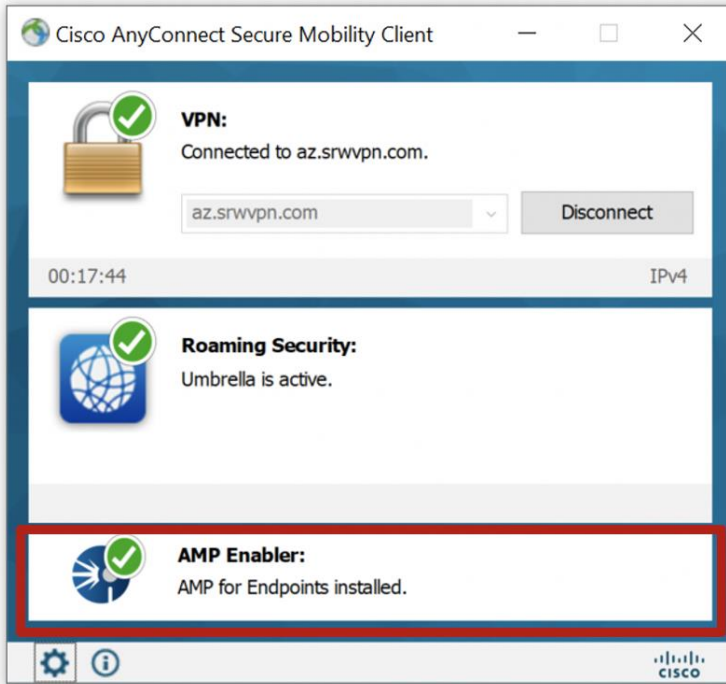


Figure 8. **Cisco AMP Enabler**
License requirement to enable AMP Enabler:

<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.

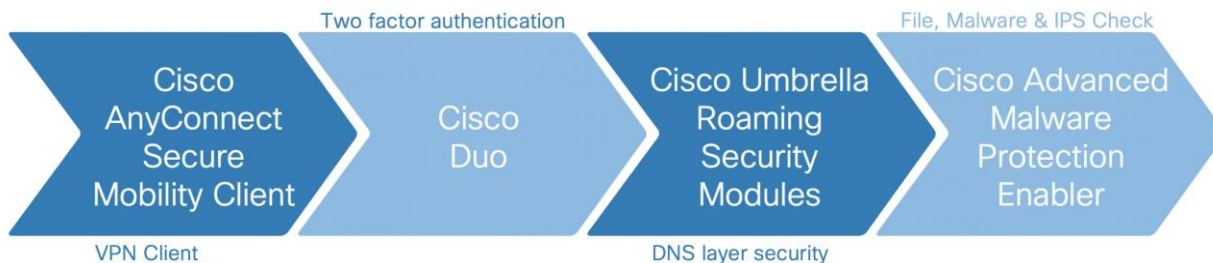


Figure 9. **Cisco Security Integration for Secure Remote Worker**

It is essential to configure the Azure 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.

Azure Overview

Microsoft Azure is a public cloud service provided for building, testing, deploying, managing applications and services through Microsoft managed data centers. Azure 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 again securely accesses 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. Azure 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 Azure services to build a highly secure and resilient architecture for Cisco Secure Remote Worker.

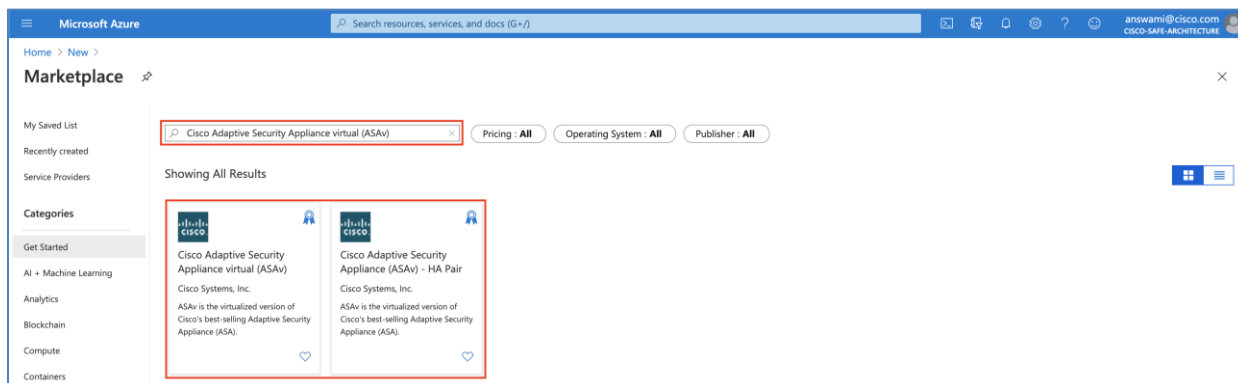
- **Azure Resource Group (RG):** Azure Resource Group is a container that holds related resources for an Azure solution. Typically, users group related resources for a resource group ([Azure Documentation](#)).
- **Azure Virtual Network (VNet):** Azure Virtual Network (VNet) is a building block of a private network in Azure. VNet provides a way to control address space, subnets, virtual machines, routes tables, load balancers, and gateway ([Azure Documentation](#)).
- **Azure VNet Peering:** VNet peering enables a seamless connection between VNets in Azure. Traffic uses Microsoft's private network when routed via VNet peering ([Azure Documentation](#)). Azure supports the following types of peering:
 - **Virtual network peering: Connect virtual networks within the same Azure region.**
 - **Global virtual network peering: Connecting virtual networks across Azure regions.**
- **Azure Route Table (UDR):** Azure Route Table is a flexible way to route traffic in Azure VNets. User Defined Route (UDR) takes precedence over the system routes. UDR supports various next-hop options such as network virtual appliance (NVA), VNet, Internet, and none ([Azure Documentation](#)).
- **Azure Network Security Group (NSG):** Azure network security group is similar to access-control-list; it filters network traffic from and to Azure resources in VNet. Security rules in NSG that can allow or deny inbound and outbound traffic. NSG is a layer four construct; you can specify source and destination, port, and protocol ([Azure Documentation](#)).
- **Azure Network Virtual Appliance (NVA):** Azure defined third party network and security appliance as NVA. Azure UDR lets you forward traffic to NVA for security and routing. Cisco ASA, and NGFW are also available in the Azure marketplace.
- **Azure Availability Zone (AZ):** Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures ([Azure Documentation](#)).
- **Azure Availability Set (AVS):** Availability sets are another datacenter configuration to provide VM redundancy and availability. This configuration within a datacenter ensures that at least one virtual machine is available during either a planned or unplanned maintenance event ([Azure Documentation](#) – This document applies to Cisco ASA and Cisco NGFW as well).

- **Azure Internal Load Balancer (ILB):** Azure Internal Balancer operates at layer four, and it distributes traffic flows that arrive at the load balancer's frontend IP to backend pool instances. The load balancing rule defines how traffic should be load balanced to the backend instances. ILB provides the flexibility of enabling health probes to track the health of the backend instances. For the scalable and resilient design, ILB load balances traffic to multiple Cisco Instances ([Azure Documentation](#)). In order to add NVA in the backend pool NVA be in Availability Set or Availability Zone.
- **Azure External Load Balancer (ELB):** Azure Public Load Balancer or External Load Balancer operates at layer four, and it distributes traffic flows that arrive at the load balancer's frontend IP to backend pool instances. The load balancing rule defines how traffic should be load balanced to the backend instances. ELB provides the flexibility of enabling health probes to track the health of the backend instances. For the scalable and resilient design, ELB load balances traffic to multiple Cisco Instances ([Azure Documentation](#)). In order to add NVA in the backend pool NVA be in Availability Set or Availability Zone.
- **Azure Traffic Manager (ATM):** Azure Traffic Manager is a DNS-based traffic load balancer that enables traffic distribution in global Azure regions. Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint. Traffic Manager engages a variety of load balancing methods and service endpoint health probe ([Azure Documentation](#)).
- **Azure Resource Manager Template (ARM Template):** Azure Resource Manager (ARM) templates provide a flexible way to implement infrastructure as code in the Azure environment. ARM template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration ([Azure Documentation](#)). Cisco Live Breakout Session covers how to create ARM templates ([BRKSEC-3093](#) – Search BRKSEC-3093, Cisco Live Login Required).
- **Azure Marketplace:** Azure Marketplace third party application that can be used by Azure Customers hosts, Cisco provide wide range of NVA and services in Azure marketplace ([Azure Documentation](#)).

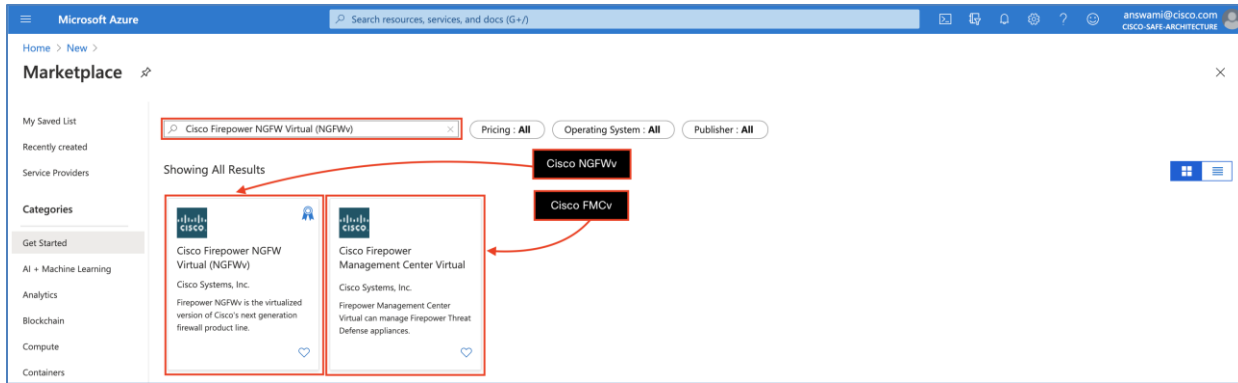
Azure Marketplace Listing

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

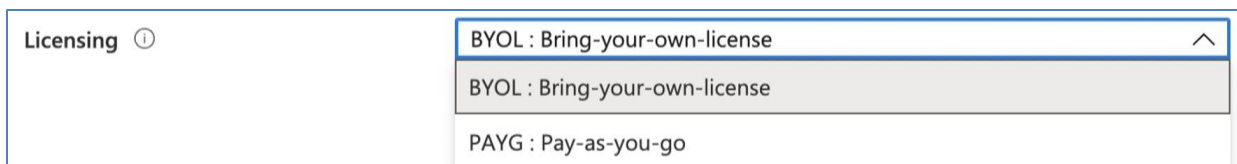
- **Cisco Adaptive Security Appliance Virtual (ASAv):** ASAv has two listings (Standalone and High Availability); this CVD covers multiple standalone devices for VPN load balancing.



- **Cisco Firepower Next-Generation Firewall Virtual (NGFWv) & Cisco Firepower Management Center Virtual (FMCv):** Cisco NGFWv and FMCv are available in the Azure 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 Azure.
- **Pay-as-you-go (PAYG):** This option enables a full-featured firewall, and customers are billed directly by Azure for compute and device licenses.

Note: Cisco ASAv supports only BYOL.

Cisco ASAv and NGFWv supported instance type

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

Azure Instance Size	Supported License Entitlement
F4, F4s, D3, D3_v2, DS3, DS3_V2	ASAv5
F4, F4s, D3, D3_v2, DS3, DS3_V2	ASAv10
F4, F4s, D3, D3_v2, DS3, DS3_V2	ASAv30
F8, F8s, D8_v3, D4, D4_v2, DS4, DS4_v2	ASAv50

Cisco Firepower Next-Generation Firewall supports the following mentioned instance types only ([NGFWv datasheet](#))

Azure Instance Size	Device
D3, D3_v2	NGFWv
D4_v2, D5_v2	NGFWv

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

Azure Instance Size	Device	Maximum NGFWv firewall management support
D4_v2	NGFWv	25

Note: Refer to Cisco ASA v and NGFWv datasheets for updated VPN numbers and throughput.

Cisco Secure Remote Worker Architecture for Azure

Today more and more organizations are consuming services, workloads, and applications hosted in Azure. Azure 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 Azure cloud infrastructure.

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

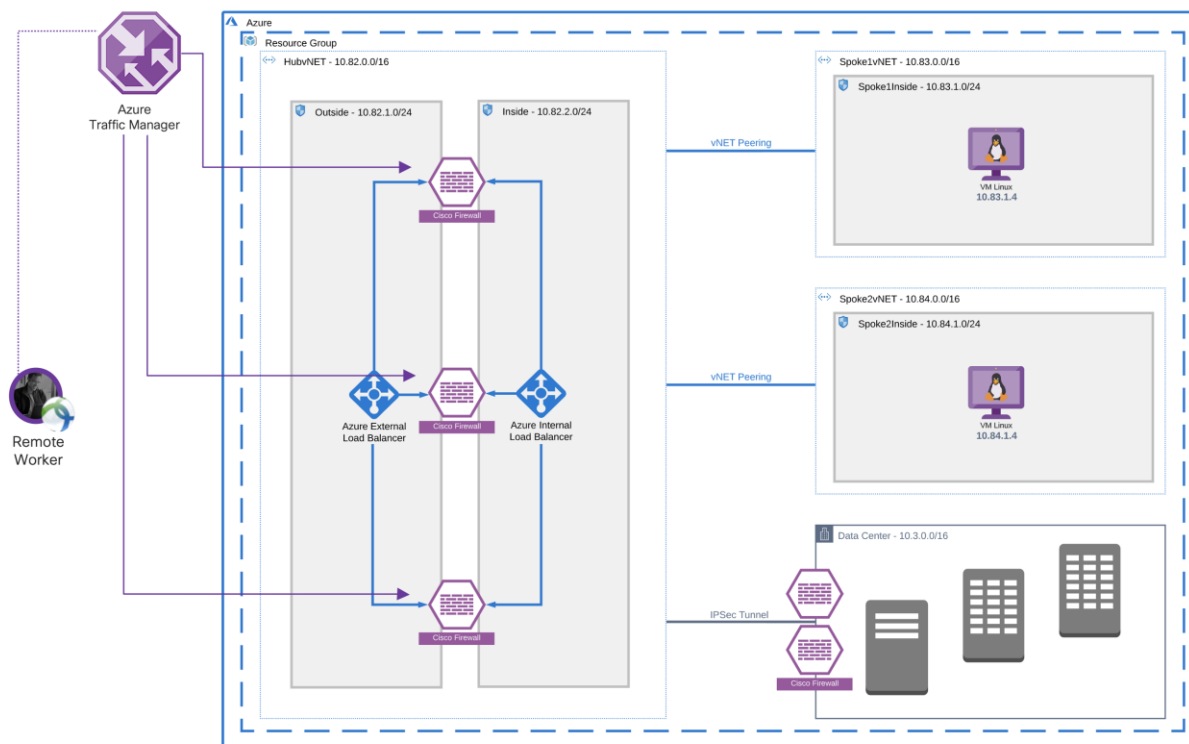


Figure 10. **Secure Remote Worker architecture for multi-VNet, single-availability zone**

The above network design has the following components and services:

- Cisco ASA v 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 & IP layer enforcement)**

- AMP Enabler (File, IPS, and Malware policies)
- Azure Hub and Spoke model
 - VNet peering to peer VNets to the HubVNet
 - Azure Internal load balancer (standard) for east-west traffic protection and outbound traffic protection
 - Azure External load balancer (standard) for inbound north-south traffic
 - Azure Traffic Manager for load balancing remote access VPN (RAVPN) to Cisco firewall
 - Azure Network Security Group on workloads for micro-segmentation
 - Azure virtual network gateway or Azure express route connection back to the Data Center (not in scope)
 - Azure availability set (AVS) for fault domains

Network Architecture (VPN only and no E/W traffic)

This Architecture brings together Cisco Security and Azure Infrastructure-as-a-service (IaaS) and extends remote access VPN capabilities with Duo, Umbrella, and AMP Enabler. This architecture is only for VPN; hence no-load balancer is added.

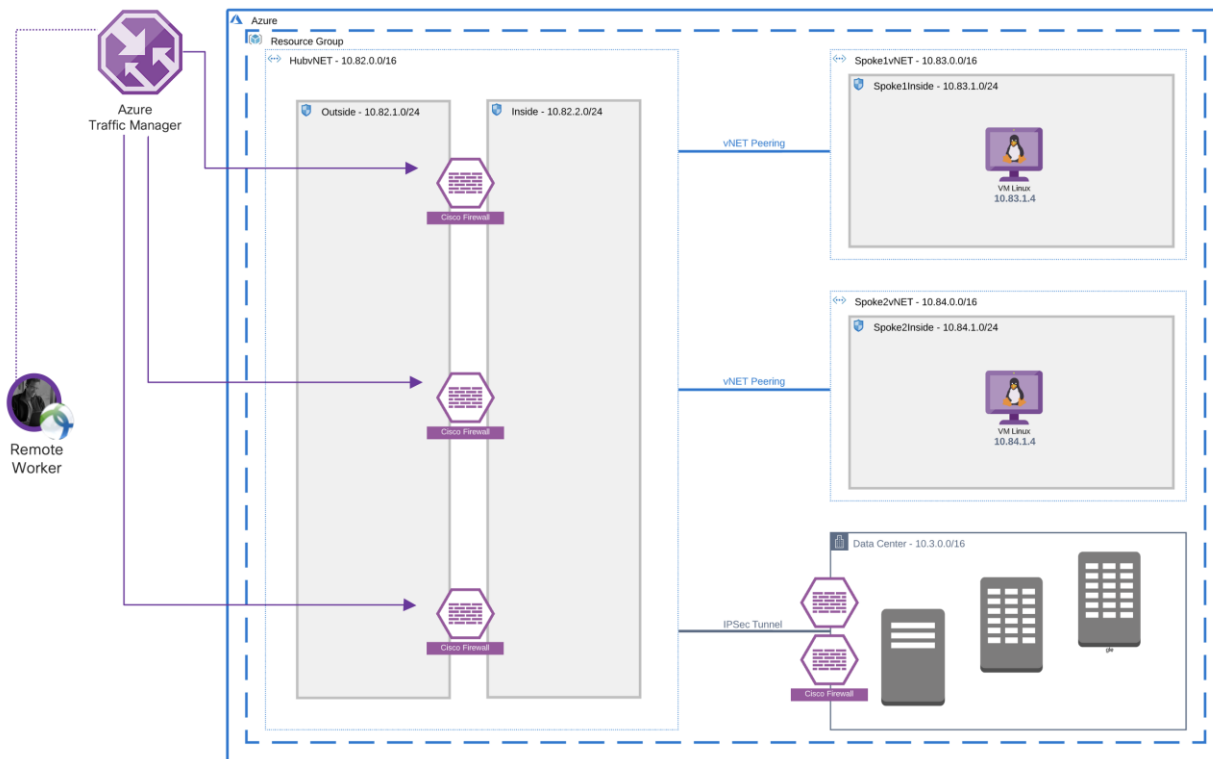


Figure 11. Secure Remote Worker architecture for multi-VNet, single-availability zone (VPN only)

Network Architecture with Multi Availability Zone

This architecture shows the deployment of multi firewalls in a multi availability zone; the multi-AZ design provides a resilient architecture.

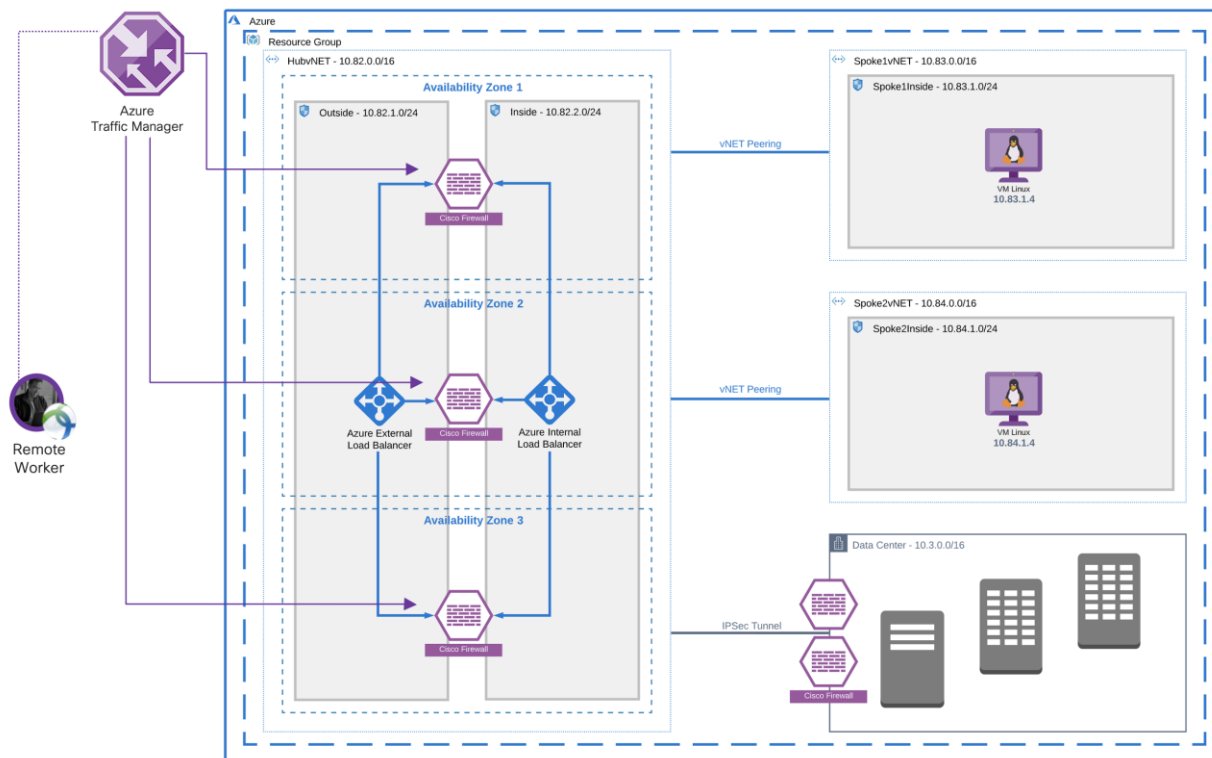


Figure 12. **Secure Remote Worker architecture for multi-VNet, multi-AZ**

The network design shown in the above diagram is similar to the single availability zone architect, but this architecture adds multiple availability zones to provide data center level VM resiliency.

To deploy Cisco firewalls in an availability set or availability zone, an ARM template deployment is required. Here are few sample templates available on GitHub:

Template1: Deploys ASA in Azure Availability Set ([GitHub](#)). Sample ARM template used for this testing is available in [Github](#).

Template2: Deploys NGFWv in a load balancer sandwich model, once deployed add Azure Traffic Manager for RAVPN ([GitHub](#))

Note:

- Each network is different, and we recommend using the above templates as an example and customize your templates
- ARM template provides a way to deploy firewalls in multi-az architecture (show in deployment steps)
- HubvNET should only have firewalls, Active Directory, Duo proxy and other security services. HubvNET should not have workloads and applications

Traffic Flow

North-South traffic flow (VPN traffic): Azure 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 Azure Traffic Manager (ATM), DNS, and UDR. In this architecture, VPN users send VPN traffic to the Azure Traffic Manager. ATM tracks all the firewalls using probes, and it load-balances VPN connection endpoints (Cisco Firewalls).

- Each Cisco Firewall would have separate VPN pool CIDR
- To maintain symmetry, UDR in subnet sends traffic back to the correct firewall
- Traffic uses VNet peering to reach the spoke VNets
- Each AZ should have multiple firewalls
- VPN traffic can work without load balancers, non-VPN traffic needs ILB and ELB

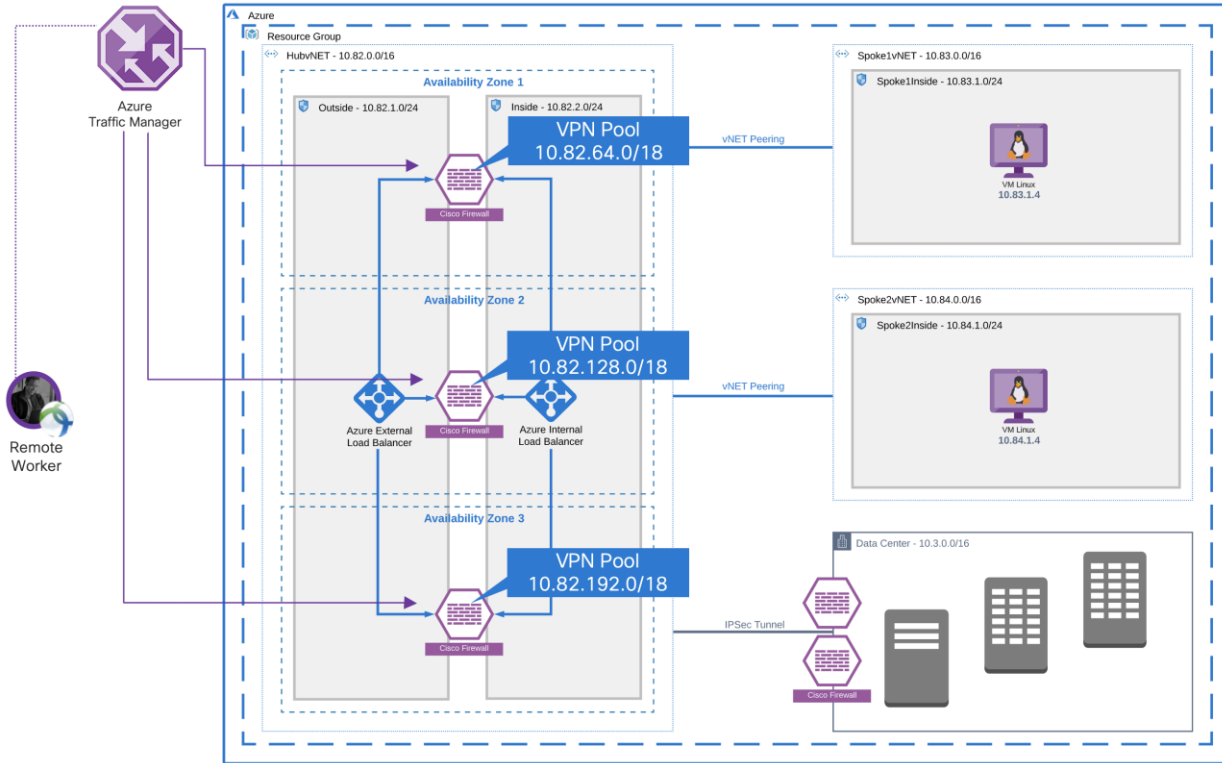


Figure 13. **North-South traffic flow**

Azure DNS zone could potentially replace Azure Traffic Manager for VPN load balancing, but Azure DNZ zone does not health probe capability. Also, Azure DNS is not DNS registrar.

Customers can still purchase DNS from a third-party DNS registrar and point to the Azure DNS zone.

Note: Since Azure DNS does not support health probes, VPN load-balancing would not work correctly if a firewall failed. Azure DNS will keep on forwarding VPN connections to the failed firewall.

East-West traffic flow (non-VPN traffic) – Firewalls in the HubvNET inspects east-west traffic, each subnet in the spoke VNet has a route-table that has a user-defined route (UDR) pointing to Azure ILB "virtual-IP-address". Traffic lands on ILB and ILB forward it to the firewall. The firewall inspects the traffic; if traffic is allowed, it is sent to the destination VNet using VNet peer. Return traffic is forwarded back to the ILB because of the similar UDR is applied on destination VNet also. ILB maintains the state and sends traffic back to the same firewall that processed the initial packet flow.

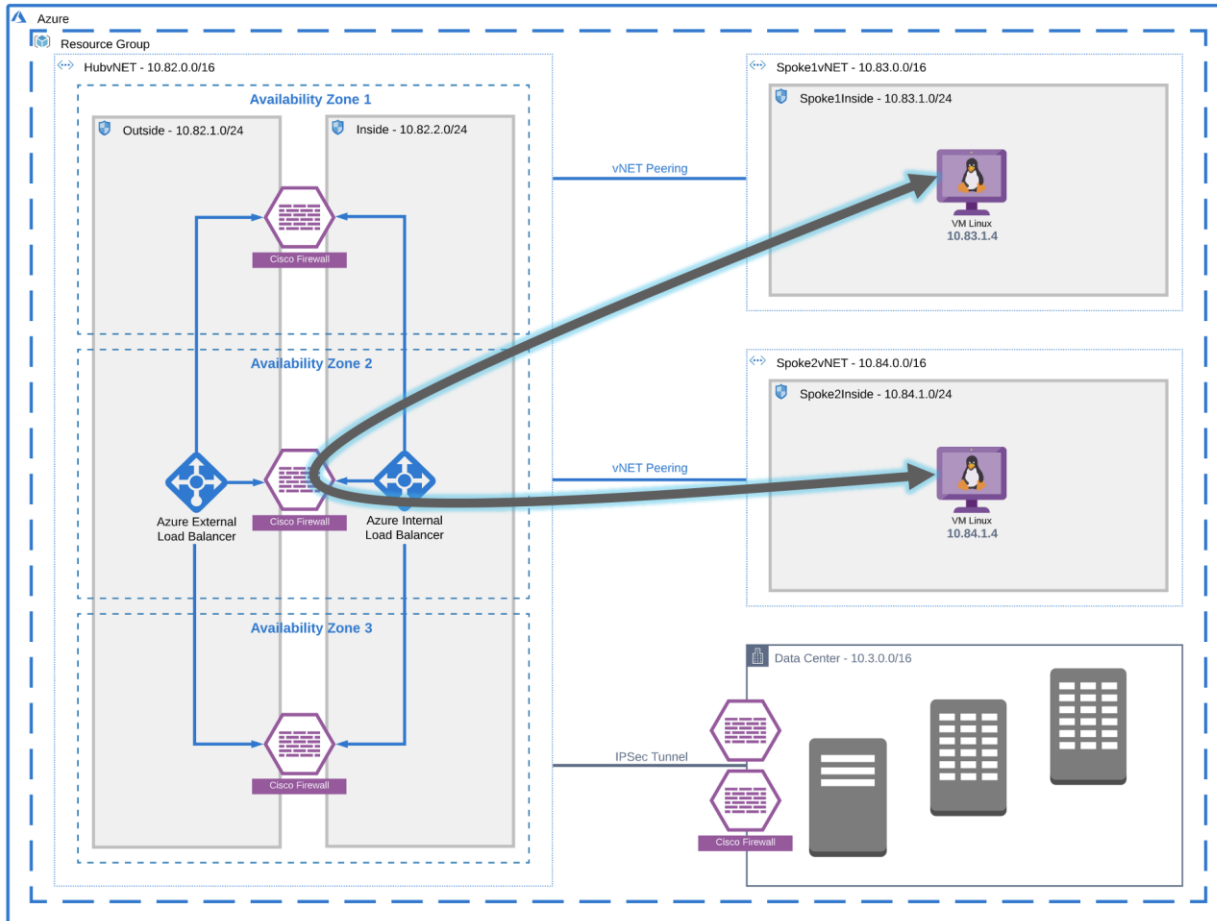


Figure 14. East-West traffic flow (non-VPN traffic)

Outbound traffic flow (non-VPN traffic): Each spoke subnet has a route-table associated with it. UDR controls traffic routing, and it has a default route that points to ILB's virtual IP (VIP). HubvNET has ILB, and ILB points to firewalls for internet connectivity. Internet traffic is load-balanced on the perimeter firewall, and traffic is SNATed to the outside interface IP address.

Outbound traffic does not hit external load balancer because a public IP mapped to the outside interface of the firewall and UDR on the outside subnet used 10.82.1.1 as a default gateway.

Azure ILB used in this architecture is a standard SKU that requires explicit Azure NSG to allow traffic on firewalls (backend devices). There is an azure NSG applied to inside and outside interfaces of firewalls; this NSG has allow-all rule applied, but you can restrict traffic according to your Infosec policy.

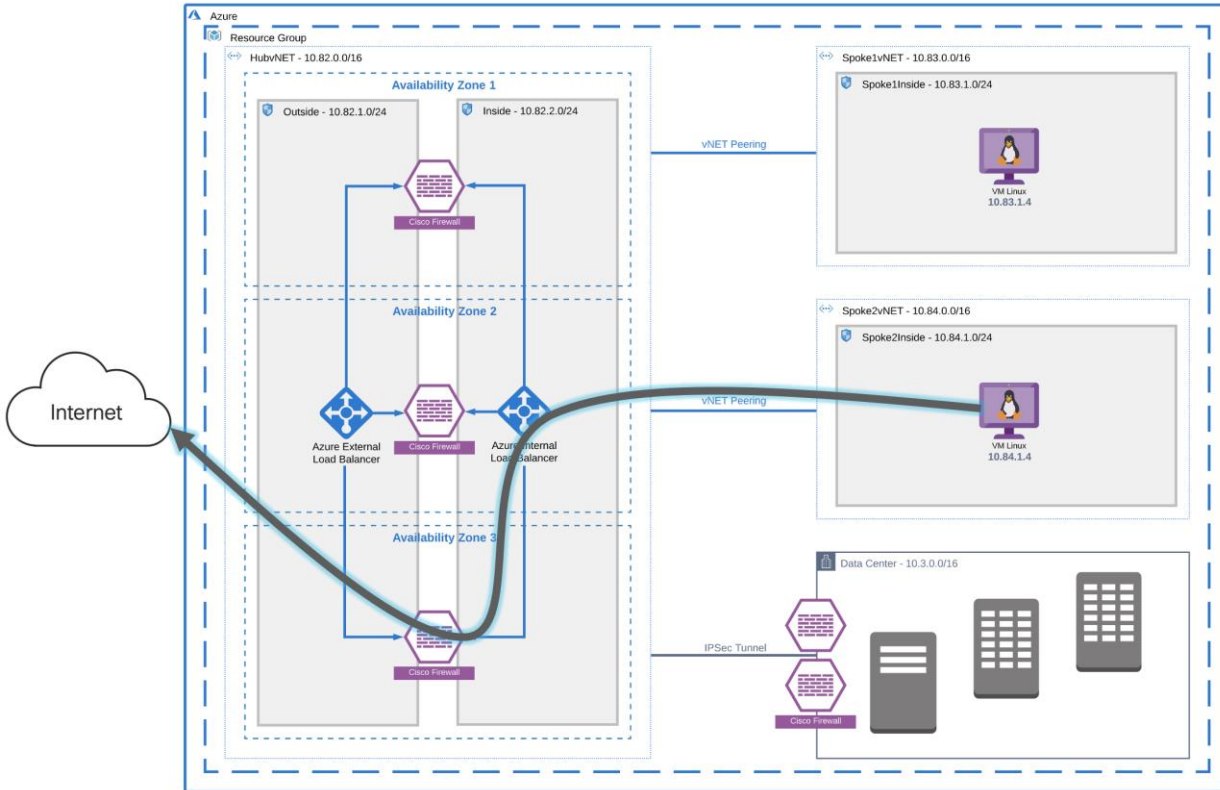


Figure 15. **Outbound traffic flow (non-VPN)**

Inbound traffic flow (non-VPN traffic): External users would access frontend IP on the Azure public load balancer (ELB), ELB has external interfaces in the backend pool. ELB is responsible for load balancing incoming non-VPN traffic, ELB sends traffic to the firewall if allowed traffic is SNATed to inside interface to maintain traffic symmetry.

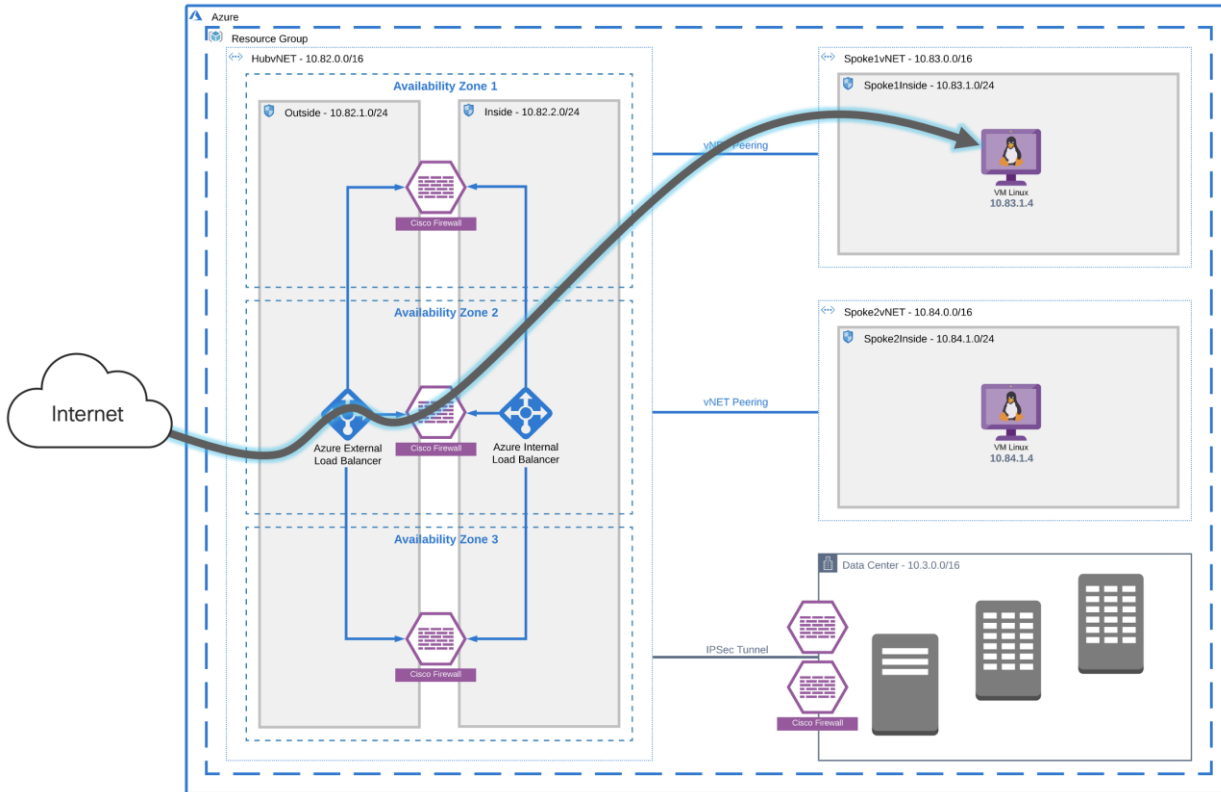


Figure 16.
Inbound traffic flow (non-VPN)

Data Center Connectivity (out-of-scope of this document): The connection between the Data Center and the Azure cloud is a critical component of hybrid cloud deployment. The variety of connection options are available:

- **Azure Express Route**
- **IPsec tunnel terminated on Azure VNG (Virtual Network Gateway)**
- **IPsec tunnel terminated on ASA/FTDv (Azure)**
- **IPsec tunnel terminated on CSR (Azure)**

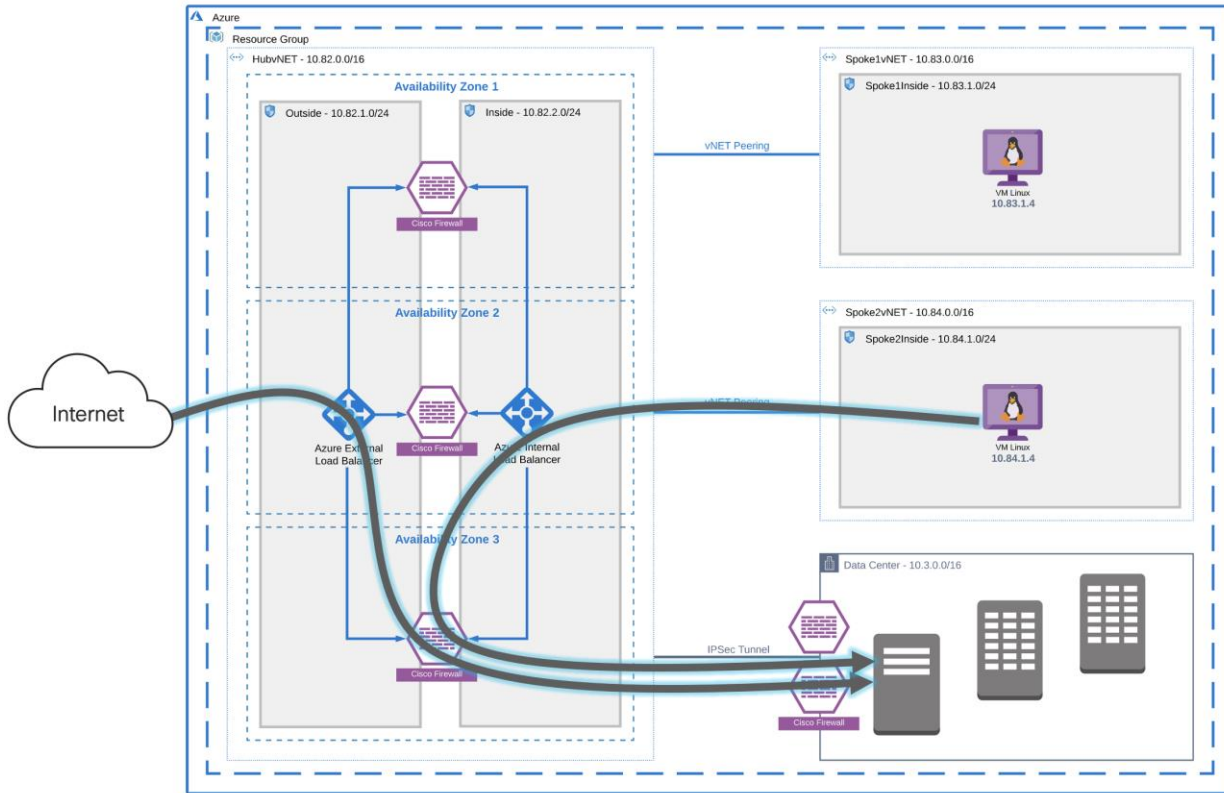


Figure 17. Azure Cloud and Data Center Connectivity

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.

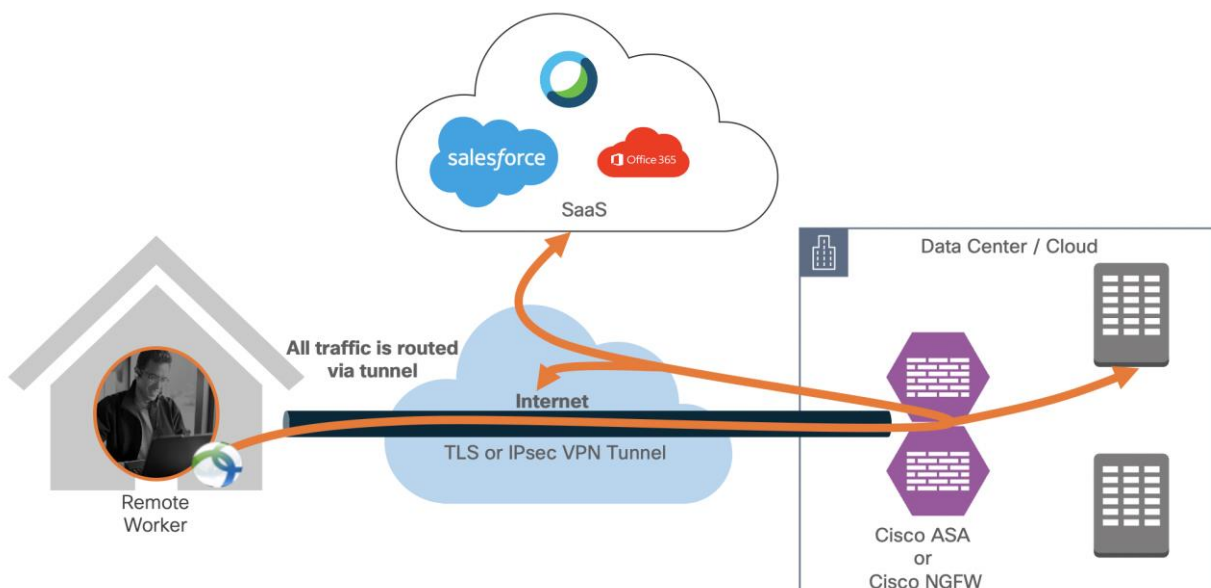


Figure 18. Remote employee accessing resources hosted in the data center (tunnel-all)

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](#)

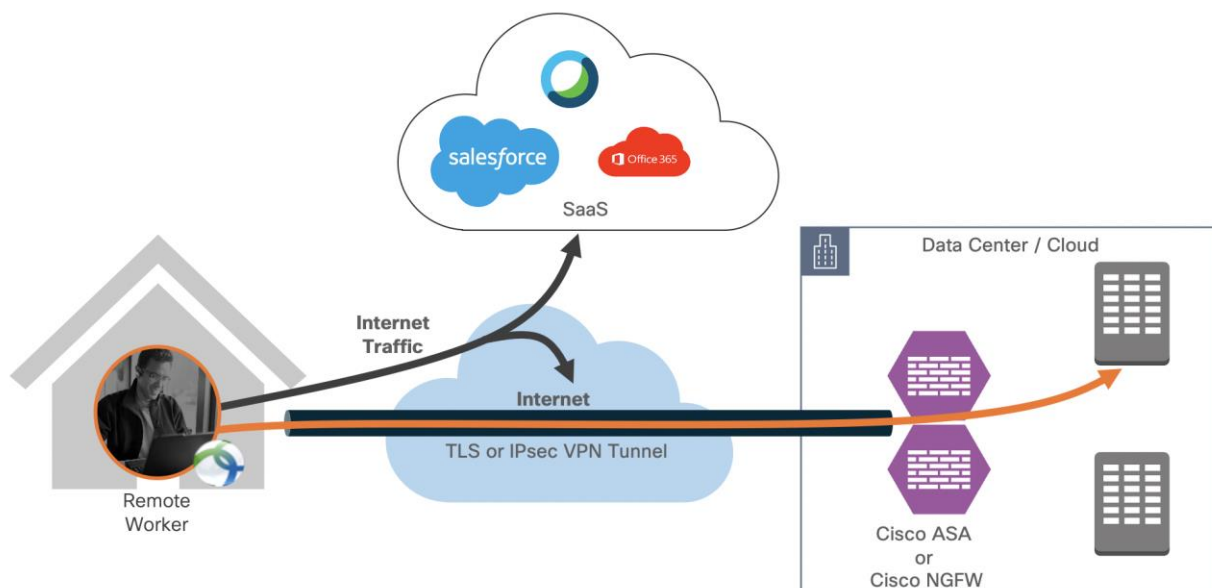


Figure 19. Traffic destined for 10.1.0.0/16 is sent through the VPN tunnel, other traffic is exempted from VPN tunnel

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.

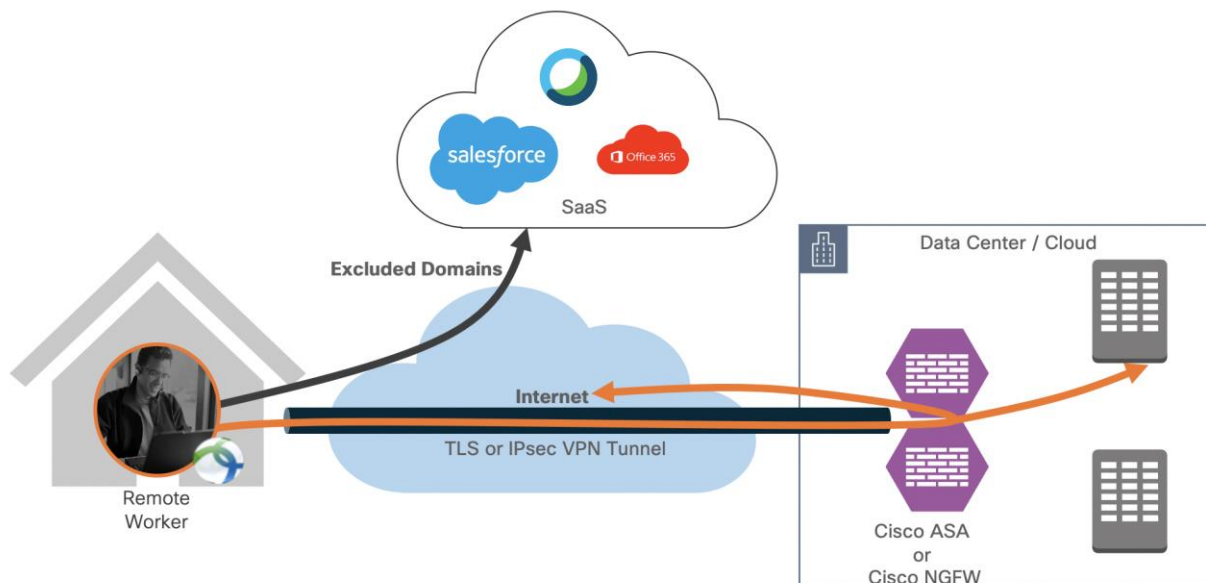


Figure 20. **Dynamic split tunnel applied (exclude traffic destined to exclude domains)**

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.

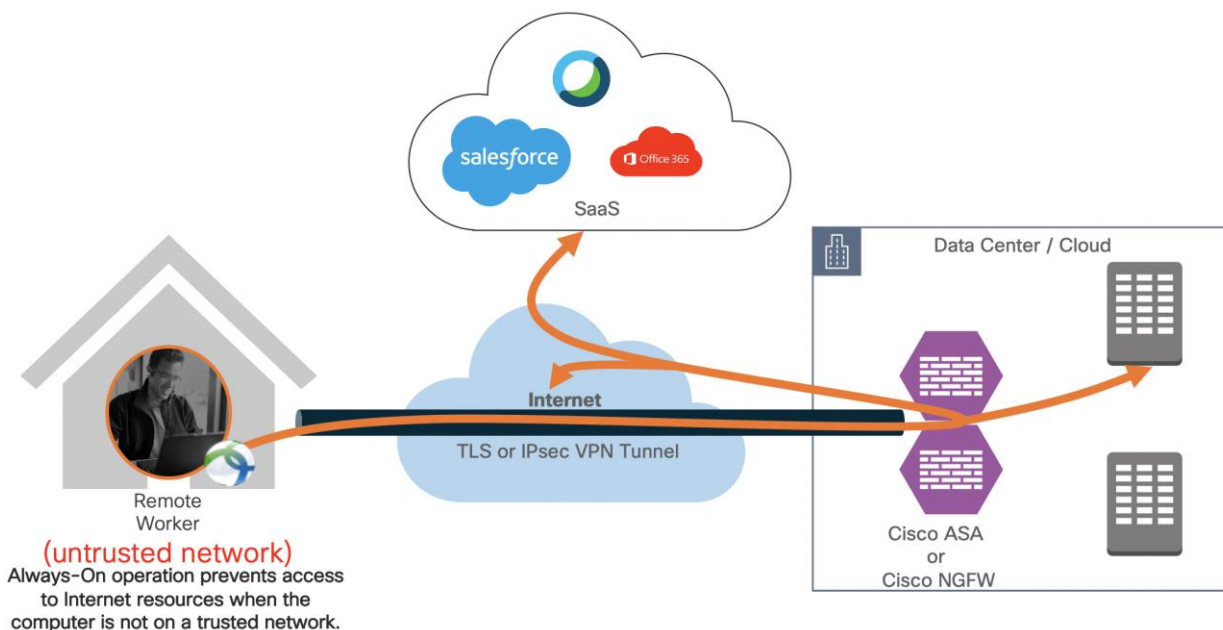


Figure 21. **VPN always on feature**

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 & IP layer enforcement
- Cisco AMP enabler continues to protect against the threats
- Cisco Duo continues to provide MFA for SaaS applications

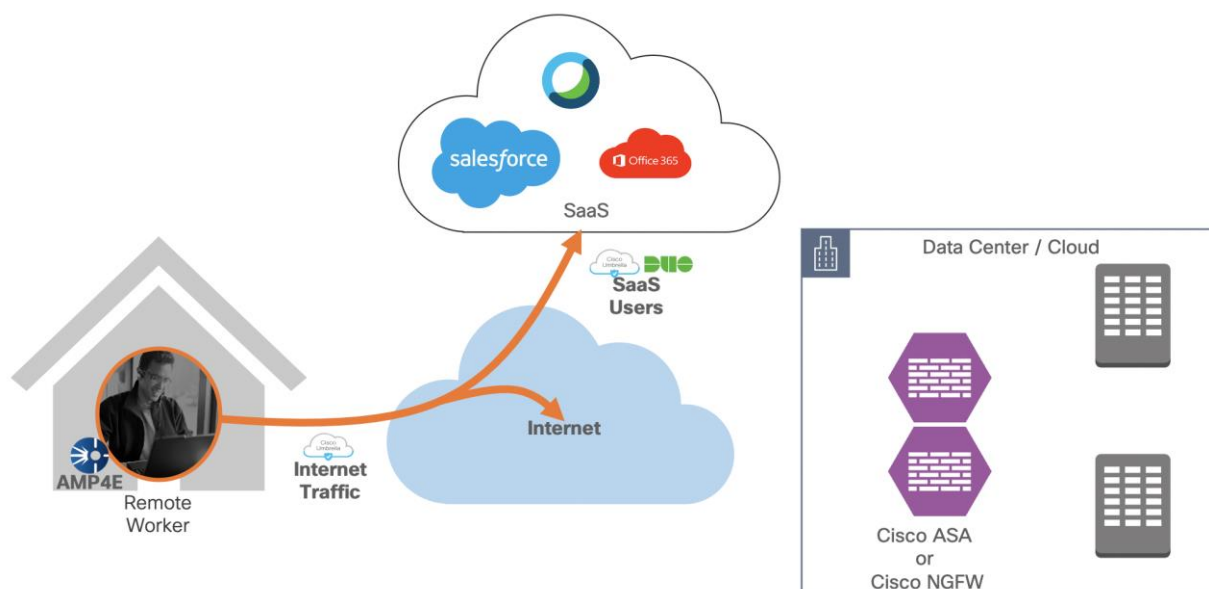


Figure 22. **Remote worker is not connected to VPN**

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

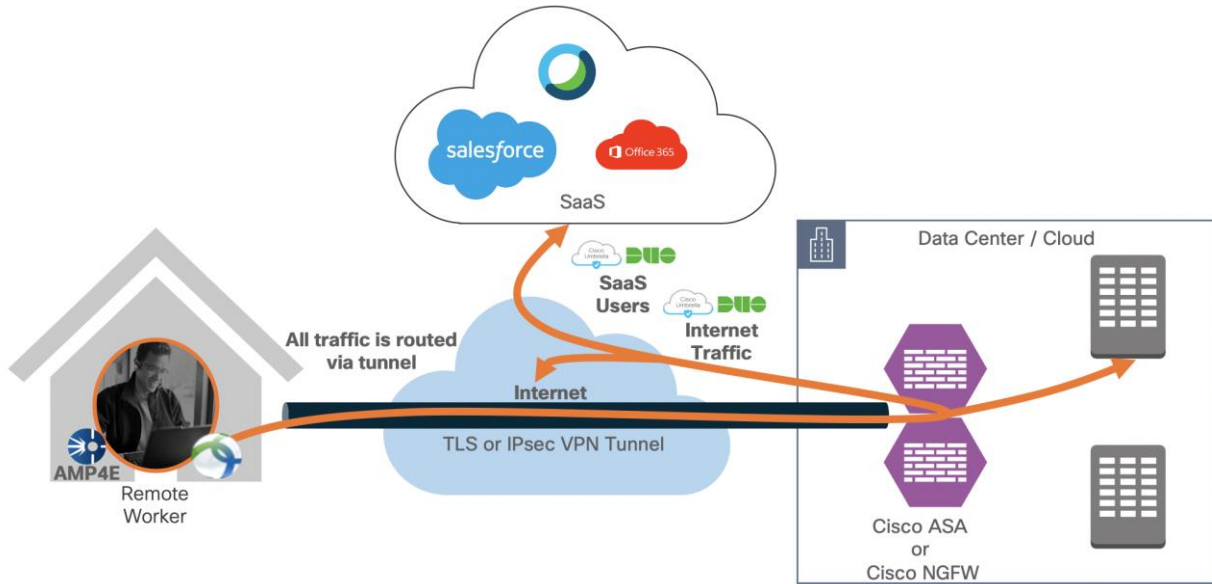


Figure 23. Remote worker is on VPN (no split tunnel)

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

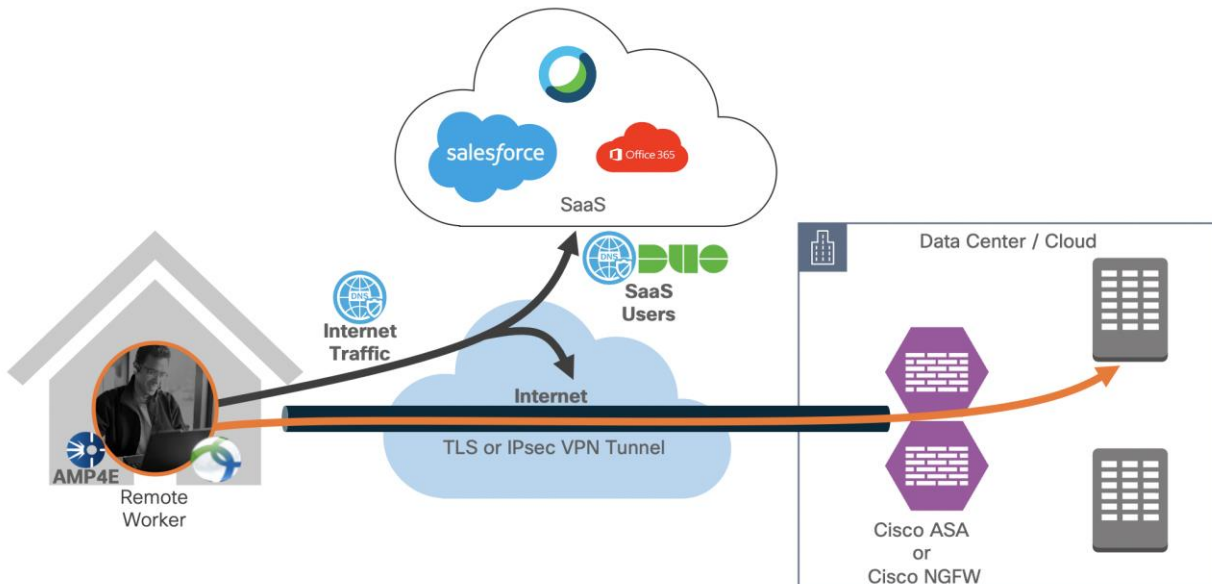


Figure 24. Remote worker is on VPN (split tunnel)

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 and IP layer enforcement
- 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

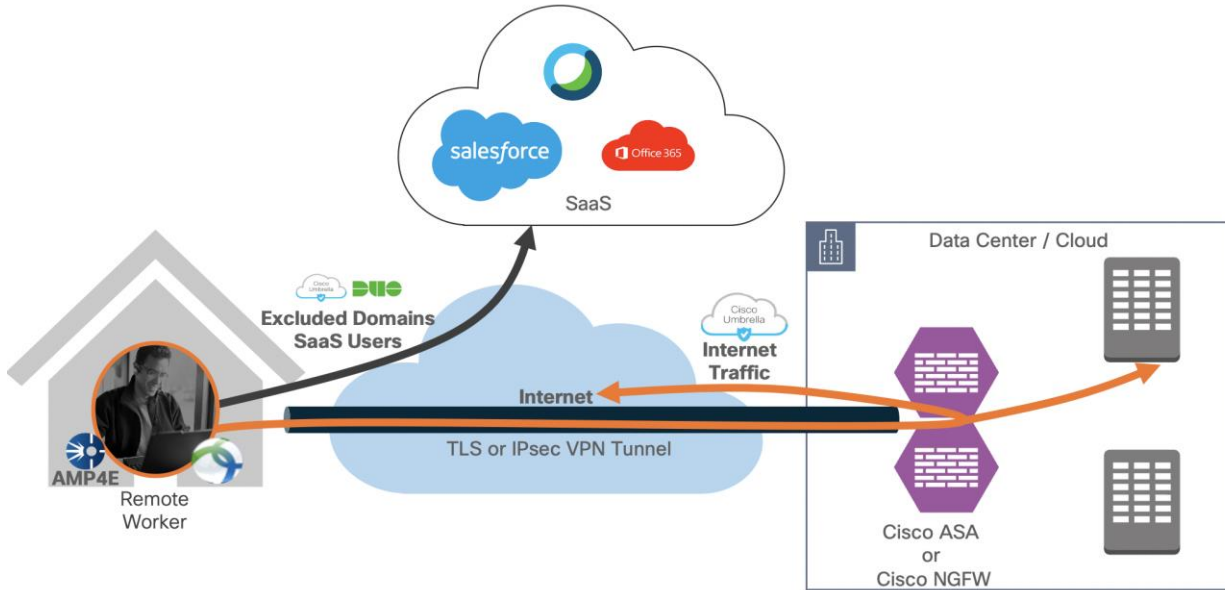


Figure 25. **Remote worker is on VPN (Dynamic split tunnel - exclude domain) VPN with always on VPN feature enabled** - Cisco AnyConnect modules provide protection when users are on a VPN and split tunnel is not enabled.

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

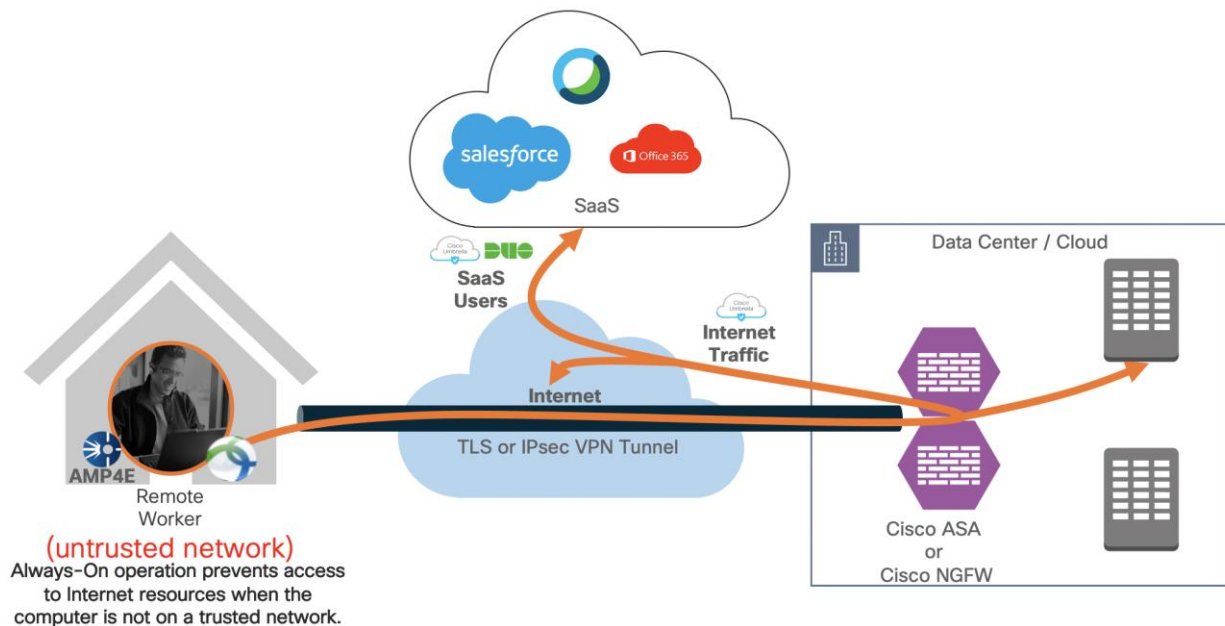


Figure 26. **Remote worker is on the trusted network (always-on-VPN)**

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.

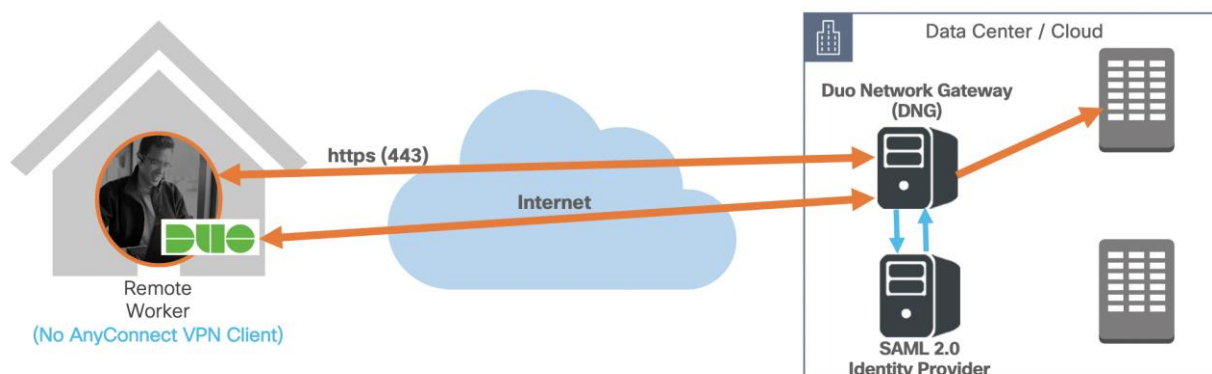


Figure 27. **Non-VPN remote worker (Duo Network Gateway)**

Duo Network Gateway: [DNG Documentation](#)

Design Implementation

Since we have covered the design specifics, we will begin implementing and setting up our Azure environment. We will start by setting up the Azure VNet (Virtual Network) as per the design shown in the above diagram. Once our VNets are ready, we will deploy firewalls (ASAv), followed by Azure LB and UDR deployment. Once we have our network ready, we will create the Azure Traffic Manager for RAVPN load balancing. Lastly, we will configure ASAs for VPN and integrate ASAs with Duo, Umbrella, and AMP.

Implementation process overview:

Network Implementation Overview

- Set up the Azure Virtual Network
 - Create VNets
 - Create VNet peering
 - Deploy workloads in VNets
 - Deploy and Cisco Firewall (ASAv) in AZ1, AZ2, and AZ3
- Setup Azure Load Balancers
 - Create and configure Azure Internal Load balancer (ILB)
 - Create and configure Azure Public/External Load balancer (ELB)

- Configure routing and VPN load balancing
 - Create and associate Azure Route Table (UDR)
 - Configure VPN ASAs (hubasa1, hubasa2, and hubasa3)
 - Create and create an Azure Traffic Manager



Figure 28. 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 29. Security Implementation

Set up the Azure Infrastructure

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

Implementation procedure:

- **Infrastructure Deployment**
 - Step 1.** Create the VNets
 - Step 2.** Create Subnets in each VNet
 - Step 3.** Create VNet Peering
 - Step 4.** Deploy workloads in VNets
 - Step 5.** Deploy ASAVs
 - Step 6.** Deploy and configure Azure Internal Load Balancer
 - Step 7.** Deploy and configure Azure External/Public Load Balancer
 - Step 8.** Configure Azure Route Table (UDRs)
 - Step 9.** Configure RAVPN on ASAVs
 - Step 10.** Configure Azure Traffic Manager and enable RAVPN 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

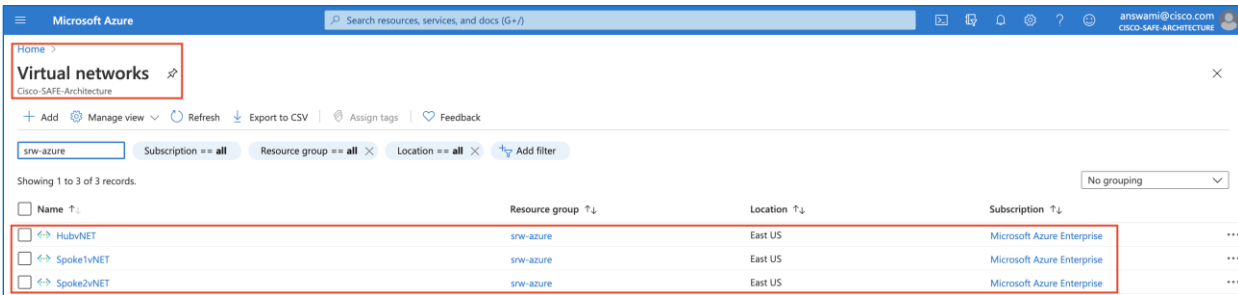
- **AMP Enabler**

- 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 VNets - Log on to the Azure portal and search for 'Virtual Networks' service. Add a new VNet in the 'Resource Group' and region of your choice. We had created a new 'Resource Group: srw-azure' for this specific implementation but you can use an existing one.

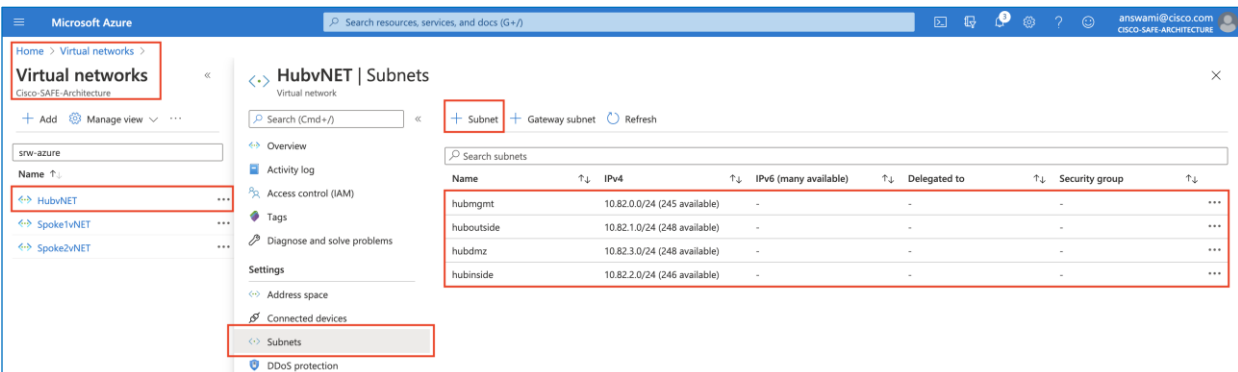
VNet Name	Subnets	Purpose
HubvNET	10.82.0.0/16	Hub VNet
Spoke1vNET	10.83.0.0/16	Spoke1
Spoke2vNET	10.84.0.0/16	Spoke2



Step 2. Create Subnets in each VNet - Click on the VNet name and create subnets as soon in the below table.

VNet Name	CIDR	Name
HubvNET	10.82.0.0/24	hubmgmt
	10.82.1.0/24	huboutside
	10.82.2.0/24	hubinside
	10.82.3.0/24	hubdmz (un-used)
Spoke1vNET	10.83.0.0/24	spoke1mgmt
	10.83.1.0/24	spoke1inside
Spoke2vNET	10.84.0.0/24	spoke2mgmt
	10.84.1.0/24	spoke2inside

- HubvNET (subnets – hubmgmt, huboutside, hubinside and hubdmz)



- Spoke1vNET (subnets – spoke1mgmt and spoke1inside)

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Virtual networks' sidebar is visible, with 'Spoke1vNET' selected. The main content area displays the 'Spoke1vNET | Subnets' configuration page. A table lists the subnets:

Name	IPv4	IPv6 (many available)	Delegated to	Security group
spoke1mgmt	10.83.0.0/24 (251 available)	-	-	-
spoke1inside	10.83.1.0/24 (250 available)	-	-	-

- Spoke2vNET (subnets - spoke2mgmt and spoke2inside)

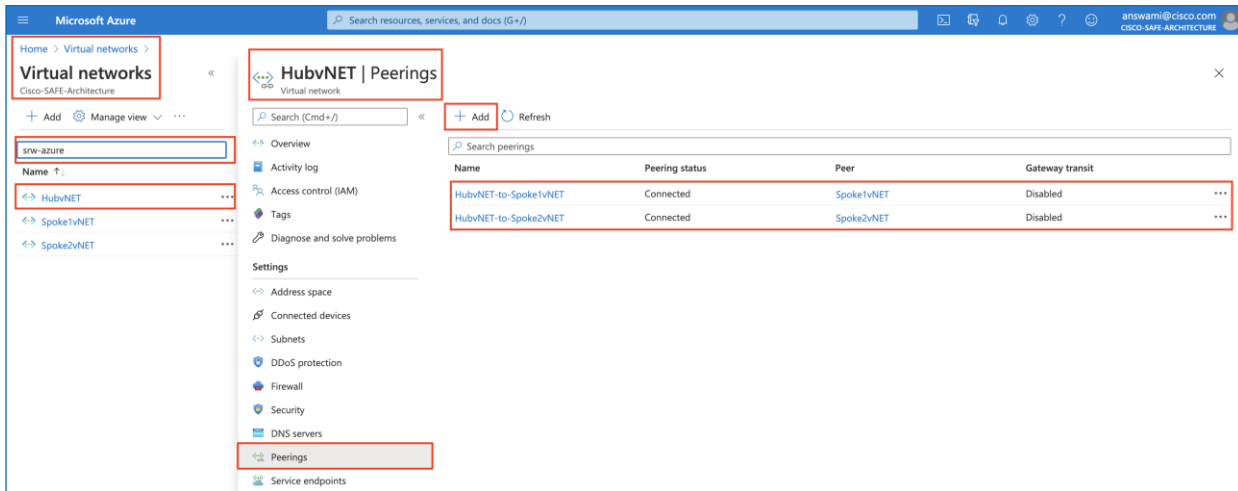
The screenshot shows the Microsoft Azure portal interface. On the left, the 'Virtual networks' sidebar is visible, with 'Spoke2vNET' selected. The main content area displays the 'Spoke2vNET | Subnets' configuration page. A table lists the subnets:

Name	IPv4	IPv6 (many available)	Delegated to	Security group
spoke2mgmt	10.84.0.0/24 (251 available)	-	-	-
spoke2inside	10.84.1.0/24 (250 available)	-	-	-

Step 3. Create VNet Peering – Click on VNet name and then click peering and then click add to create following peerings

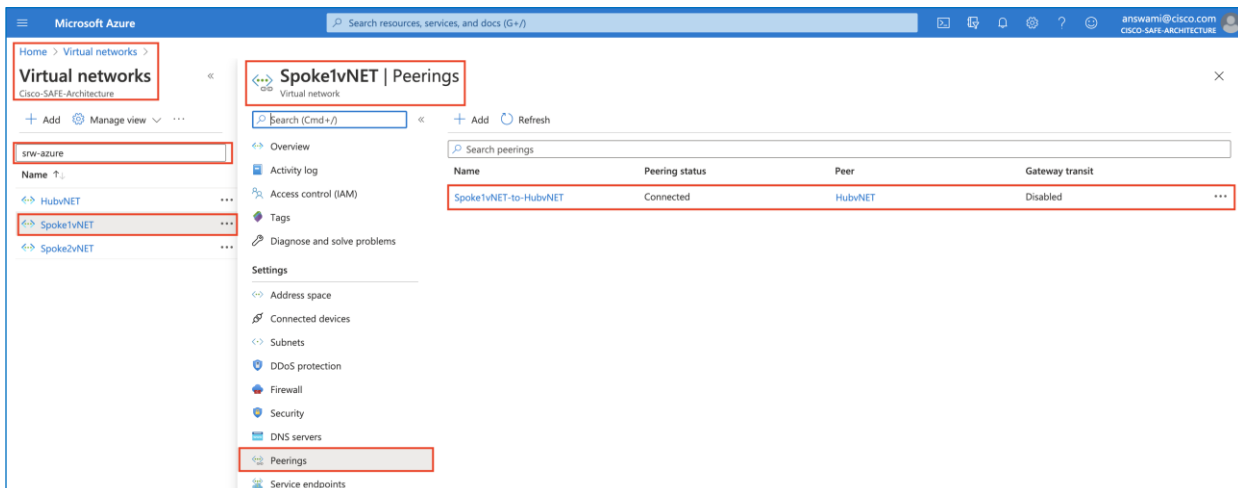
- **HubvNET peerings:** Create two peering from HubvNET, one going to Spoke1vNET and other one going to Spoke2vNET. (Note: Ensure Allow forwarded traffic from Spoke1vNET, Spoke2vNET to HubvNET should be enabled)

VNet Peer Name	Hub	Spoke
HubvNET-to-Spoke1vNET	Hub VNet	Spoke1 VNet
HubvNET-to-Spoke2vNET	Hub VNet	Spoke2 VNet

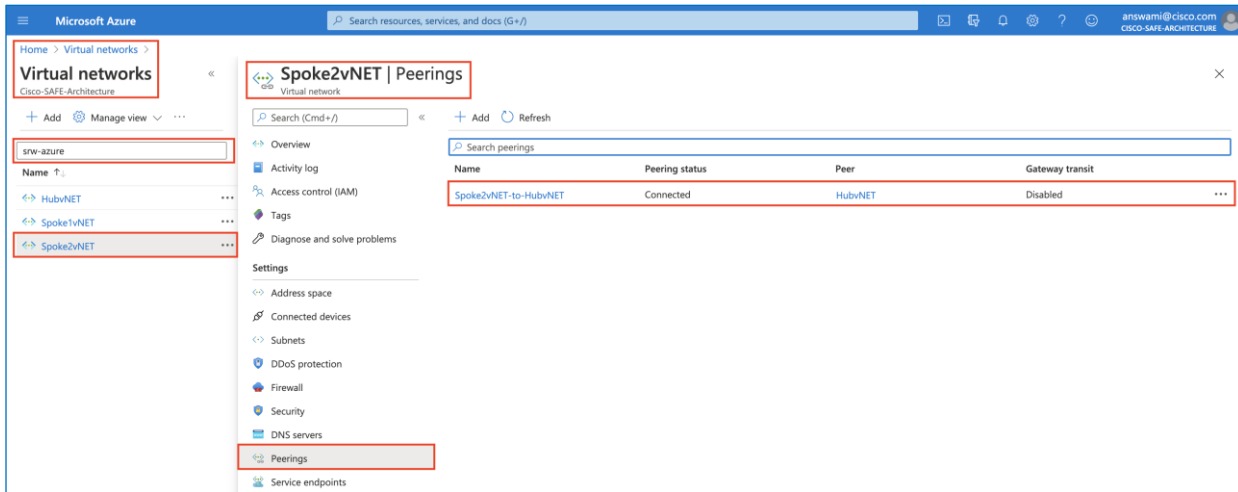


- **Spoke1vNET peering:** Spoke1vNET would have one peering to HubvNET, click on this peering and enable “allow forwarded traffic from HubvNET to spoke1vNET”

VNet Peer Name	Spoke	Hub
Spoke1vNET-to-HubvNET	Spoke1 VNet	Hub VNet



- **Spoke2vNET peering:** Spoke 2vNET would have one peering to HubvNET, click on this peering and enable “allow forwarded traffic from HubvNET to spoke1vNET”



VNet Peer Name	Spoke	Hub
Spoke2vNET-to-HubvNET	Spoke2 VNet	Hub VNet

Step 4. Deploy workloads in VNets – Deploy the following workloads in Azure and allow traffic in the network security group.

VM Name	VNet Name	Subnet Name	IP address	Port	OS
srw-ad	HubvNET	hubmgmt	10.82.0.6	TCP 389	Windows Server 2019
srw-spoke1jb01	Spoke1vNET	spoke1inside	10.83.1.4	TCP 80	CentOS 7.5
srw-spoke2jb01	Spoke2vNET	spoke2inside	10.84.1.4	TCP 80	CentOS 7.5

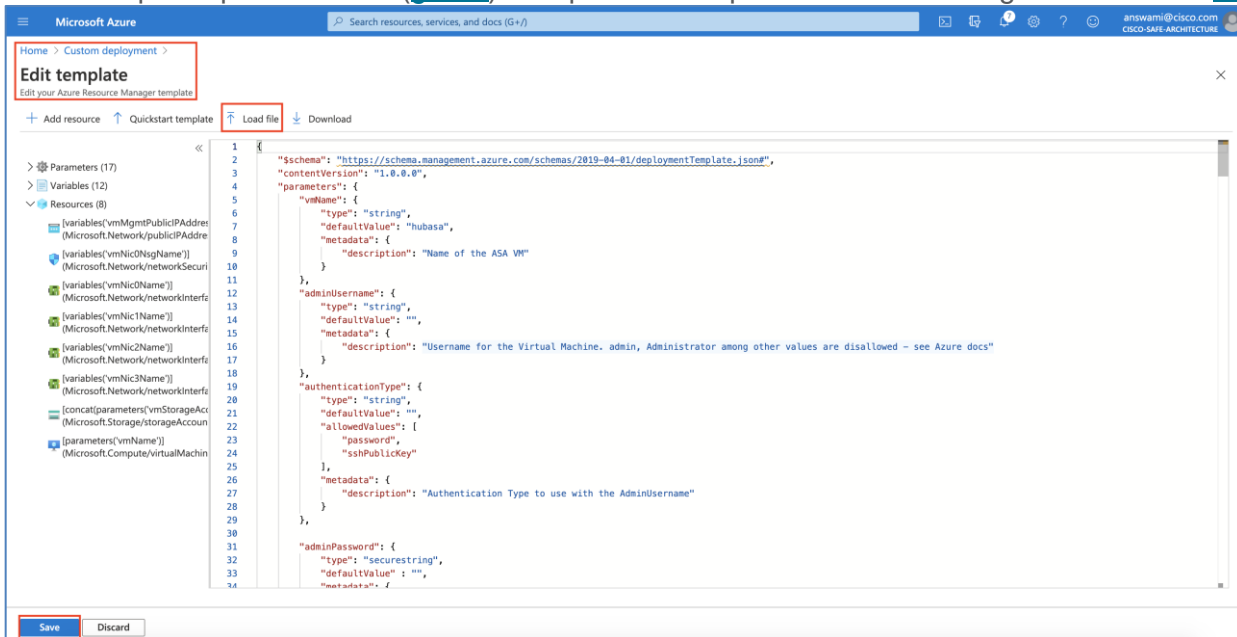
- Active Directory Server:
 - Deploy MS Windows Server 2016 or 2019 from Azure Marketplace
 - Install AD services, create a domain, and add users
 - Ensure Windows firewalls, and Azure NSG allows TCP 389 (LDAP), and ICMP traffic
- CentOS VMs:
 - Deploy CentOS 7.5 or higher from Azure Marketplace
 - Install httpd service and start httpd
 - Ensure iptables, and Azure NSG allows TCP 80 traffic, and ICMP traffic

Step 5. Deploy Cisco ASAVs – Deploy three ASAs with following IP configuration using Azure ARM template.

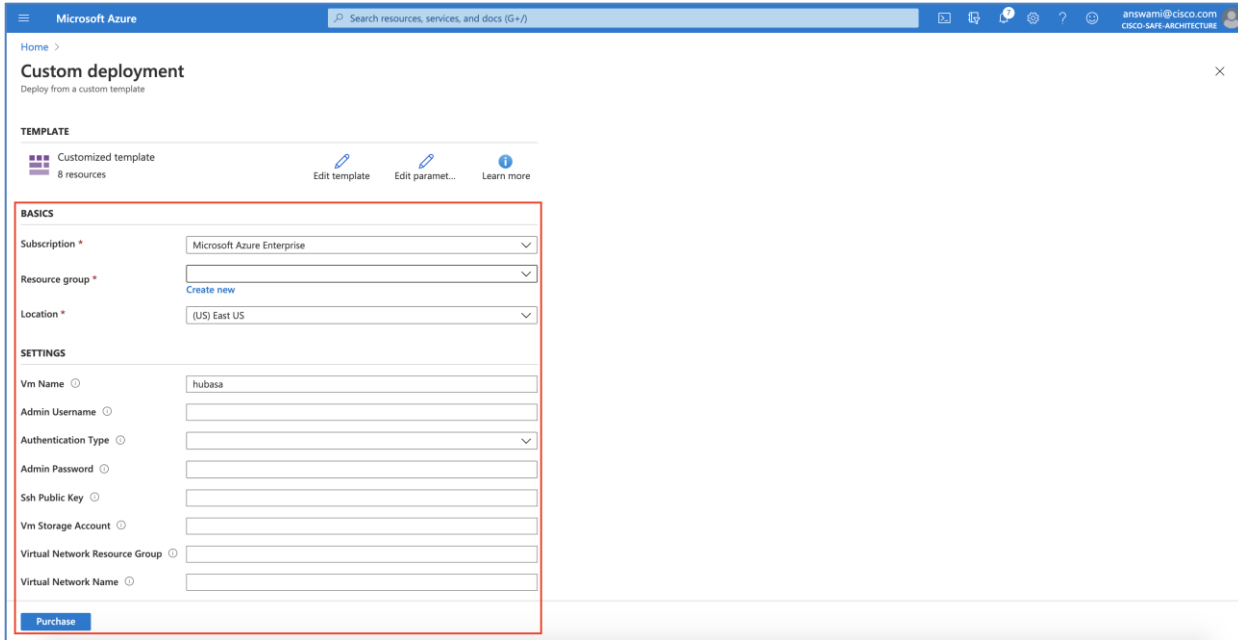
VM Name	Management	Outside	Inside	DMZ	Public IP on Interfaces
hubasa01	10.82.0.10	10.82.1.10	10.82.2.10	10.82.3.10	M0/0 and G0/1
hubasa02	10.82.0.11	10.82.1.11	10.82.2.11	10.82.3.11	M0/0 and G0/1
hubasa03	10.82.0.12	10.82.1.12	10.82.2.12	10.82.3.12	M0/0 and G0/1

Note: Adding a sample ARM template for reference, ASAs can be deployed using the Azure marketplace default deployment template (supported model). ARM templates make it easy to add firewalls in the availability-set or availability-zone.

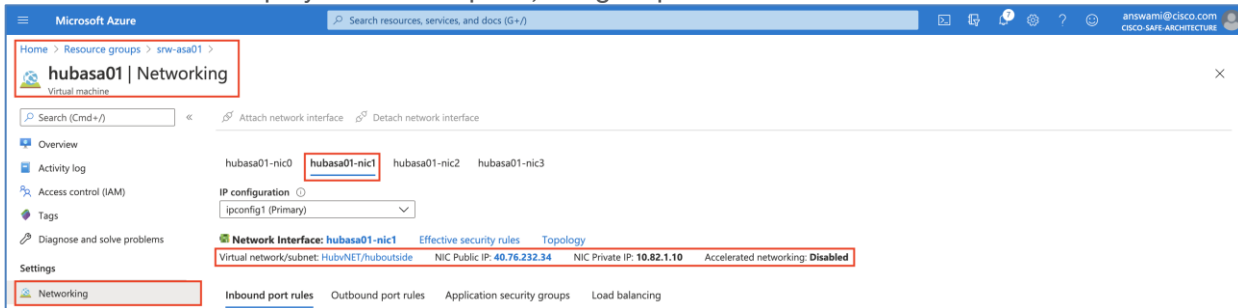
- In Azure search bar, search for custom deployment and click on custom deployment
- Click on load file and point to the ARM template that has Azure Availability Set for single availability zone and availability zone information for multiple availability zone deployment. You can customize ARM templates provided here ([github](#)). Sample ARM template used in this design is available in [Github](#).



- Now add required information to deploy ASA (hubasa1) and click purchase to deploy hubasa1



- When ASA deployment is complete, assign a public IP address on nic1 for RAVPN termination



- Deploy all three ASAs (hubasa1, hubasa2, and hubasa3) using steps shown above
- Now access ASA console connection and configure the following IP addresses on the interfaces:

VM Name	Management	Outside	Inside	DMZ	Public IP on Interfaces
hubasa01	10.82.0.10	10.82.1.10	10.82.2.10	10.82.3.10	M0/0 and G0/1
hubasa02	10.82.0.11	10.82.1.11	10.82.2.11	10.82.3.11	M0/0 and G0/1
hubasa03	10.82.0.12	10.82.1.12	10.82.2.12	10.82.3.12	M0/0 and G0/1

- 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

On ASA1 (hubasa1)

```
Interface m0/0
ip address 10.82.0.10 255.255.255.0
management-only
```

!

```
route management 0.0.0.0 0.0.0.0 10.82.0.1
route outside 0.0.0.0 0.0.0.0 10.82.1.1
```

On ASA2 (hubasa2)

```
Interface m0/0
 ip address 10.82.0.11 255.255.255.0
 management-only
!
route management 0.0.0.0 0.0.0.0 10.82.0.1
route outside 0.0.0.0 0.0.0.0 10.82.1.1
```

On ASA3 (hubasa3)

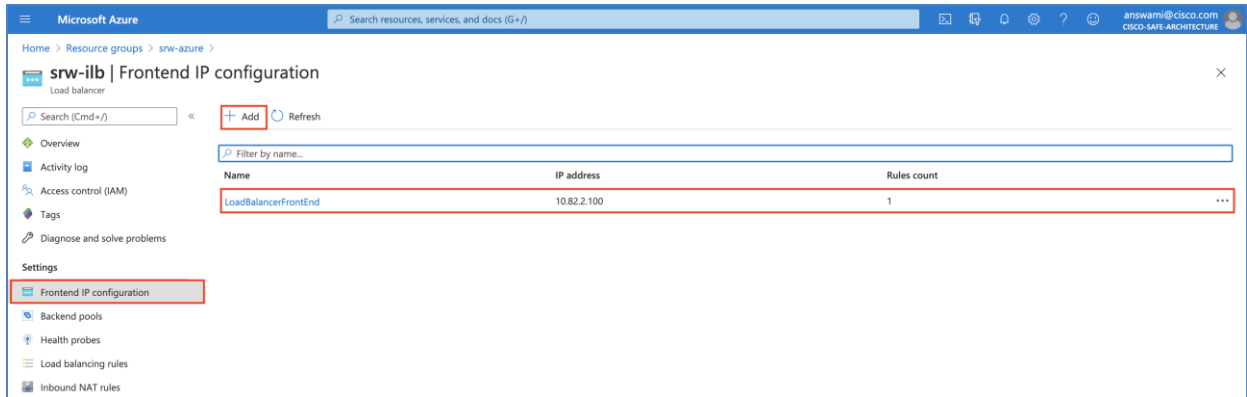
```
Interface m0/0
 ip address 10.82.0.12 255.255.255.0
 management-only
!
route management 0.0.0.0 0.0.0.0 10.82.0.1
route outside 0.0.0.0 0.0.0.0 10.82.1.1
```

Note: By default, management0/0 is configured to receive an IP address from DHCP; management interface cannot be configured as a “management-only” interface until the DHCP IP address is changed to a static IP address on management0/0 interface. The management interface can be used as a data interface if there is a strict requirement of separating management and data interfaces. Cisco ASA can be accessed using the console from Azure port, and the DHCP address on the management0/0 interface can be replaced with the same static IP address.

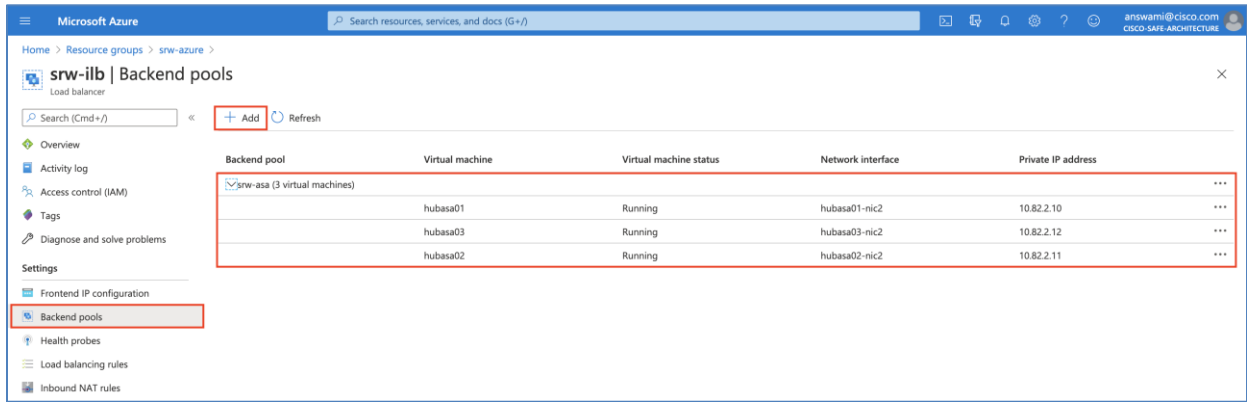
Step 6. Deploy and Configure Azure Internal Load Balancer (ILB) - In the Azure portal, search for 'Load Balancers' service; click on "+Add" button. Create an Internet Load Balancer srw-ilb using the following information.

ilb Name	Resource Group	type	SKU	Public IP	Availability Zone
srw-ilb	srw-azure	internal	Standard	Create new Name: srw-ilb-ip	Zone- redundant

- Click Review + create to deploy Azure ILB
- The next step is to add "Frontend IP - VIP" on ILB, click on "frontend IP configuration" then click on "+ Add" button. On the new screen, add frontend IP name as "LoadBalancerFrontEnd", use static IP address (10.82.2.100), and select the "hubinside" network. Finally click add

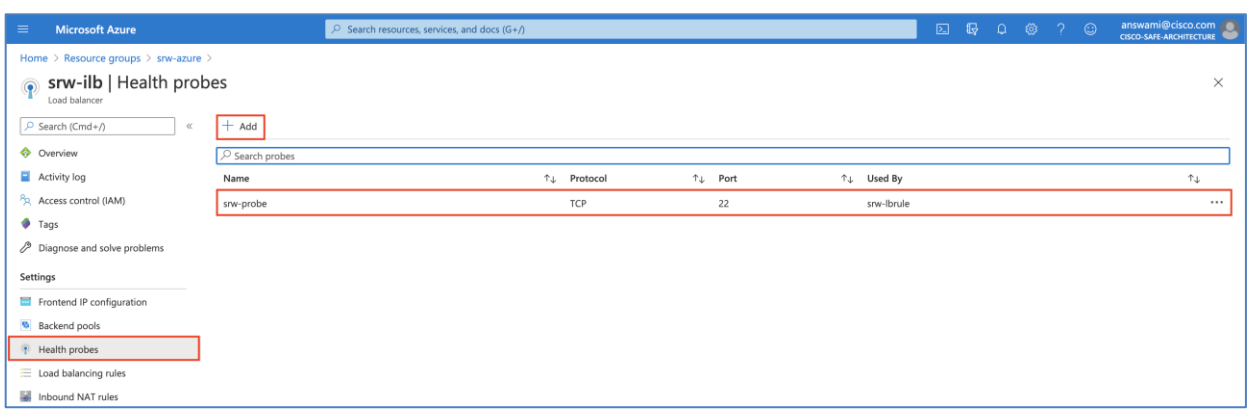


- Now add firewalls (ASA's inside interface IPs in the backend pool) - Click backend pools and click "+add" button. Ensure ILB points to the inside interface of all three firewalls (hubasa1, hubasa2, and hubasa3)



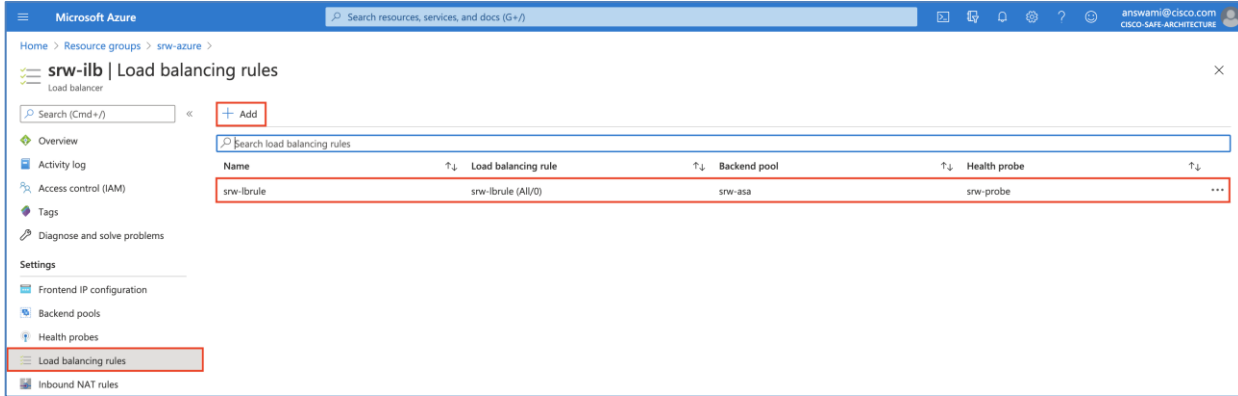
- The next step is to add health probe, click health probes and then click "+ add"

Probe Name	Protocol	Port
srw-probe	TCP	22



- The next step is to add load balancing rule, click on load balancing rules and then click "+ add". Ensure "HA port" checkbox is checked

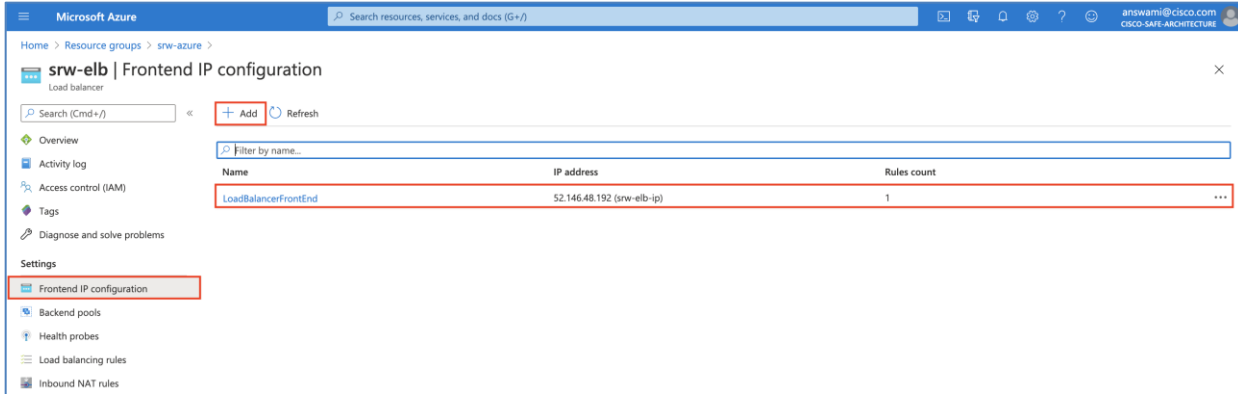
Load balancing rule name	LB port	Backend pool	Probe
srw-lbrule	HA port	srw-asa	srw-probe



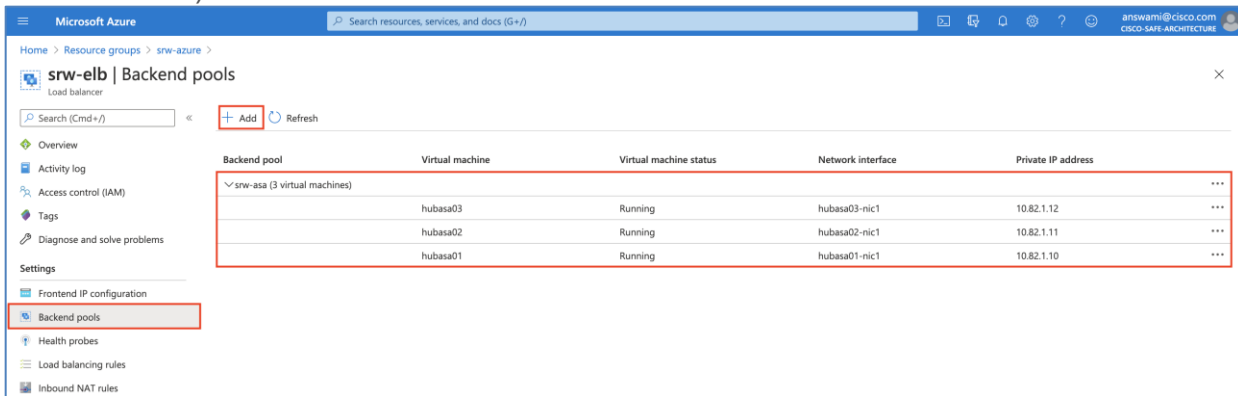
Step 7. Deploy and Configure Azure Public/External Load Balancer (ELB) - In the Azure portal, search for 'Load Balancers' service; click on "+ Add" button. Create an Internet Load Balancer srw-elb using the following information.

LB Name	Resource Group	type	SKU	Public IP	Availability Zone
srw-elb	srw-azure	public/external	Standard	Create new Name: srw-elb-ip	Zone-redundant

- Click Review + create to deploy Azure ILB.
- The next step is to add "Frontend IP - VIP" on ELB, click on "frontend IP configuration" then click on "+ Add" button. On the new screen, add frontend IP name as "LoadBalancerFrontEnd", use new public ip address (srw-elb-ip).

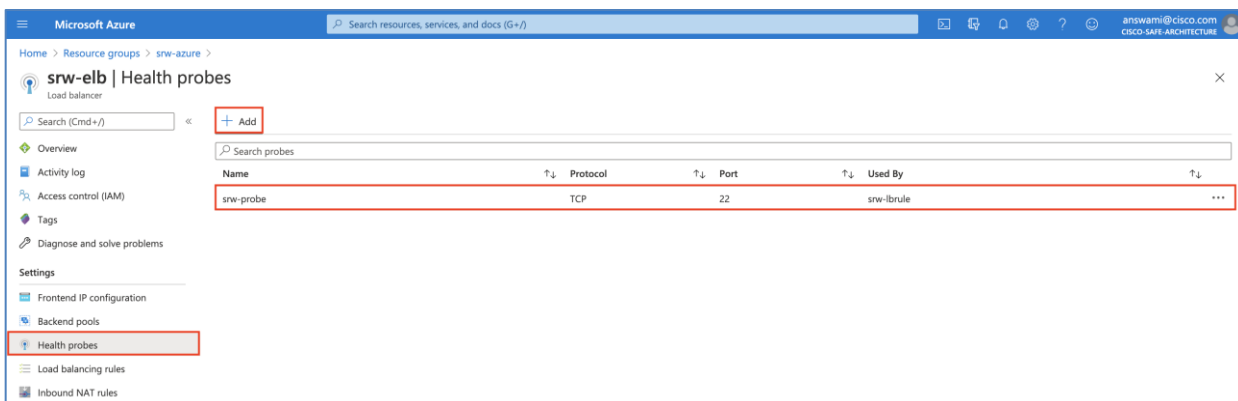


- Now add firewalls (ASA's outside interface IPs in the backend pool) - Click backend pools and click "+add" button. Ensure ELB points to the outside interface of all three firewalls (hubasa1, hubasa2, and hubasa3).



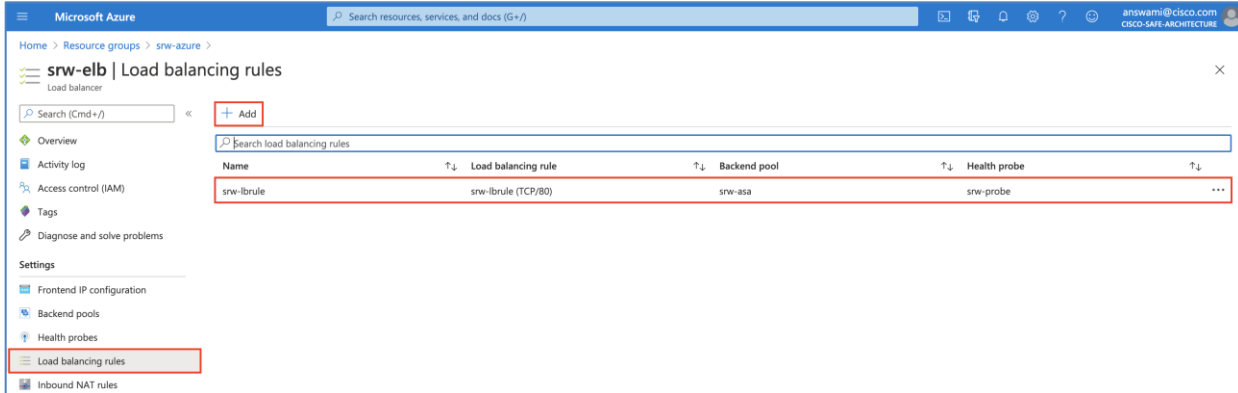
- The next step is to add health probe, click health probes and then click "+ add"

Probe Name	Protocol	Port
srw-probe	TCP	22



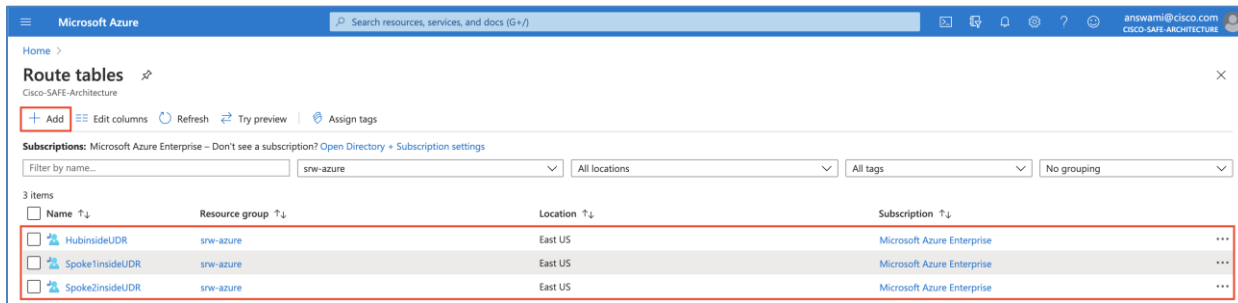
- The next step is to add load balancing rule, click on load balancing rules and then click "+ add". Ensure "HA port" checkbox is checked

Load balancing rule name	LB port	Backend pool	Probe
srw-lbrule	HA port	srw-asa	srw-probe



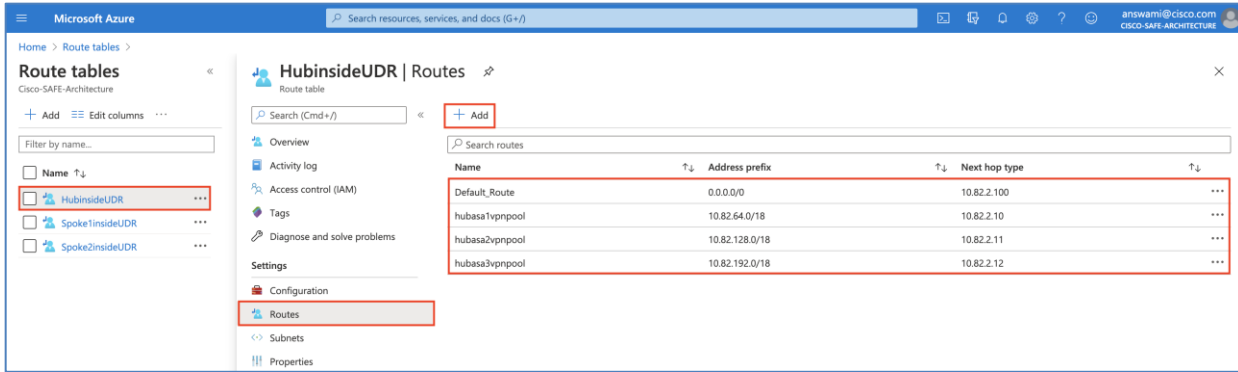
Step 8. Configure Azure Route Table (User Defined Route - UDR) - In the Azure portal, search for route tables service; click on "+ Add" button and create three route tables:

- Route tables - Three UDR's used in this architecture.



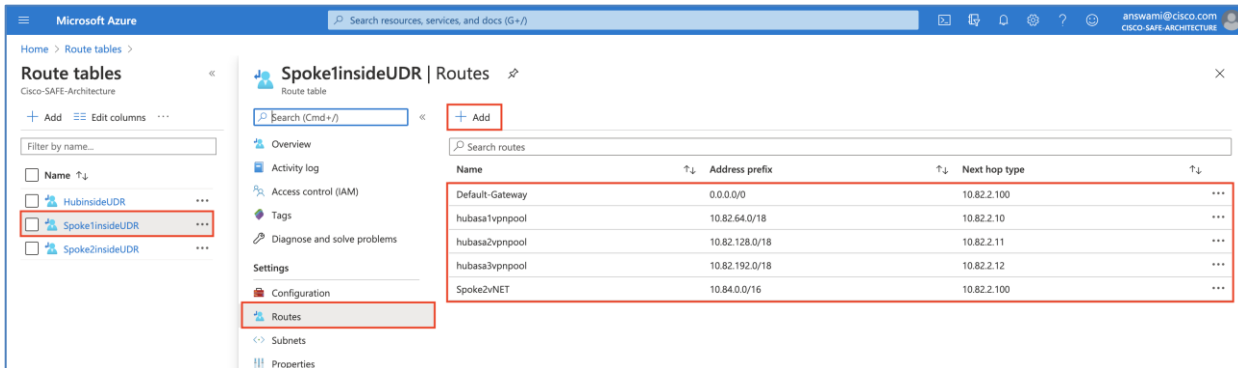
- HubinsideUDR - This Azure route table is associated to hubinside subnet

Route Table Name	Subnet Association	Route
HubinsideUDR	hubinside	Default Route → 10.82.2.100 (srw-ilb VIP) VPN pool1 (10.82.64.0/18) → 10.82.2.10 (hubasa1 inside) VPN pool2 (10.82.128.0/18) → 10.82.2.11 (hubasa2 inside) VPN pool2 (10.82.192.0/18) → 10.82.2.12 (hubasa3 inside)



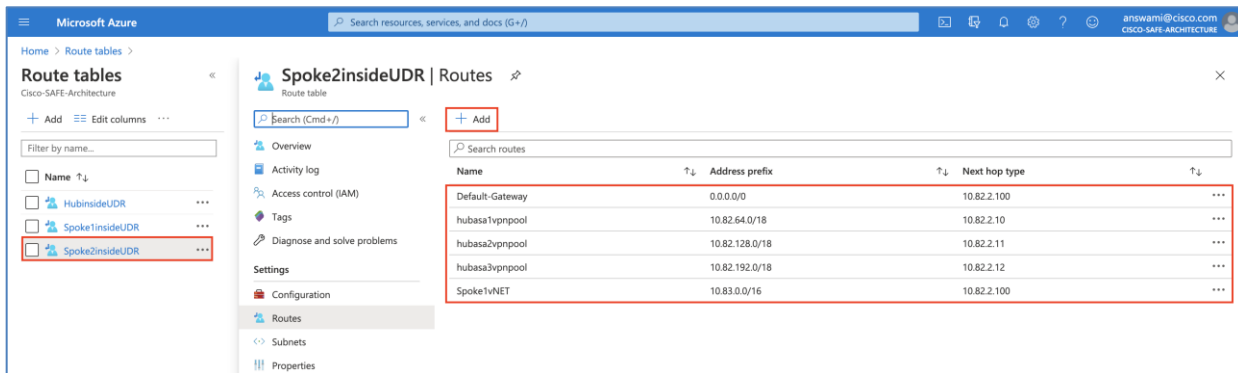
- Spoke1insideUDR – This Azure route table is associated to Spoke1inside subnet

Route Table Name	Subnet Association	Route
Spoke1insideUDR	spoke1inside	Default Route → 10.82.2.100 (srw-ilb VIP) VPN pool1 (10.82.64.0/18) → 10.82.2.10 (hubasa1 inside) VPN pool2 (10.82.128.0/18) → 10.82.2.11 (hubasa2 inside) VPN pool2 (10.82.192.0/18) → 10.82.2.12 (hubasa3 inside) Spoke2vNET (10.84.0.0/16) → 10.82.2.100 (srw-ilb VIP)



- Spoke2insideUDR – This Azure route table is associated to Spoke1inside subnet

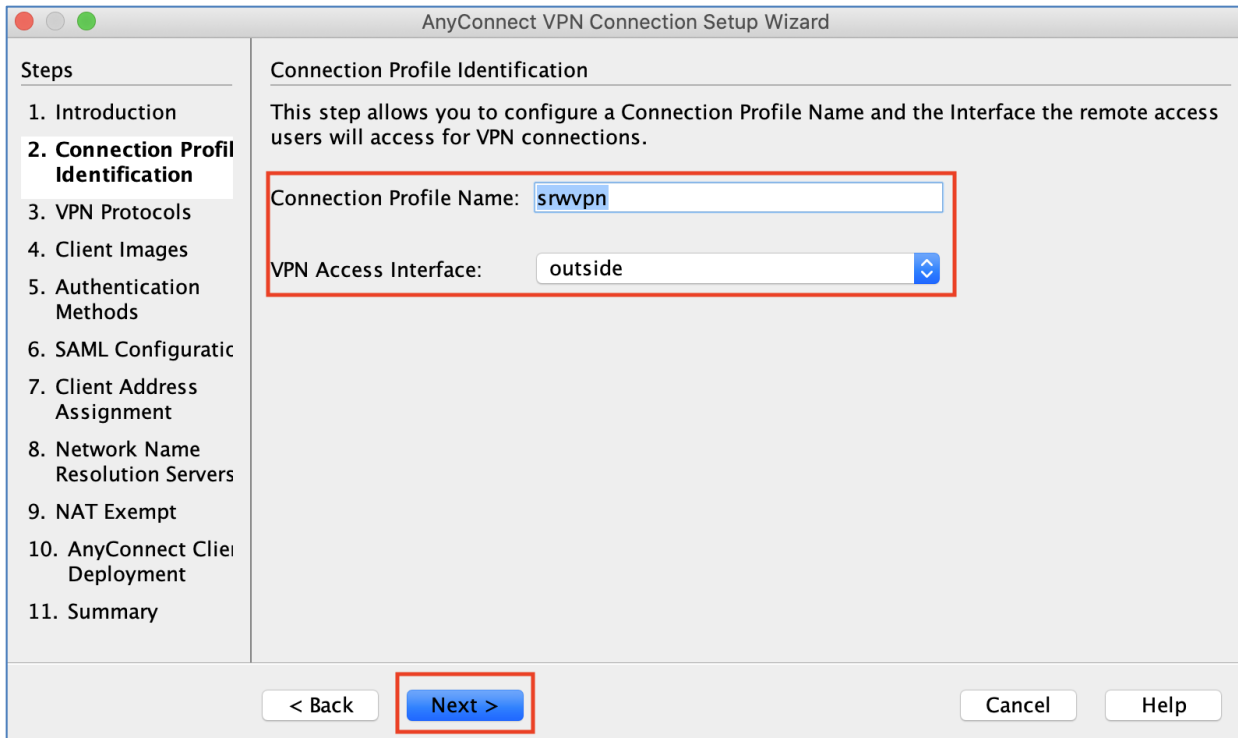
Route Table Name	Subnet Association	Route
Spoke2insideUDR	spoke2inside	Default Route → 10.82.2.100 (srw-ilb VIP) VPN pool1 (10.82.64.0/18) → 10.82.2.10 (hubasa1 inside) VPN pool2 (10.82.128.0/18) → 10.82.2.11 (hubasa2 inside) VPN pool2 (10.82.192.0/18) → 10.82.2.12 (hubasa3 inside) Spoke1vNET (10.83.0.0/16) → 10.82.2.100 (srw-ilb VIP)



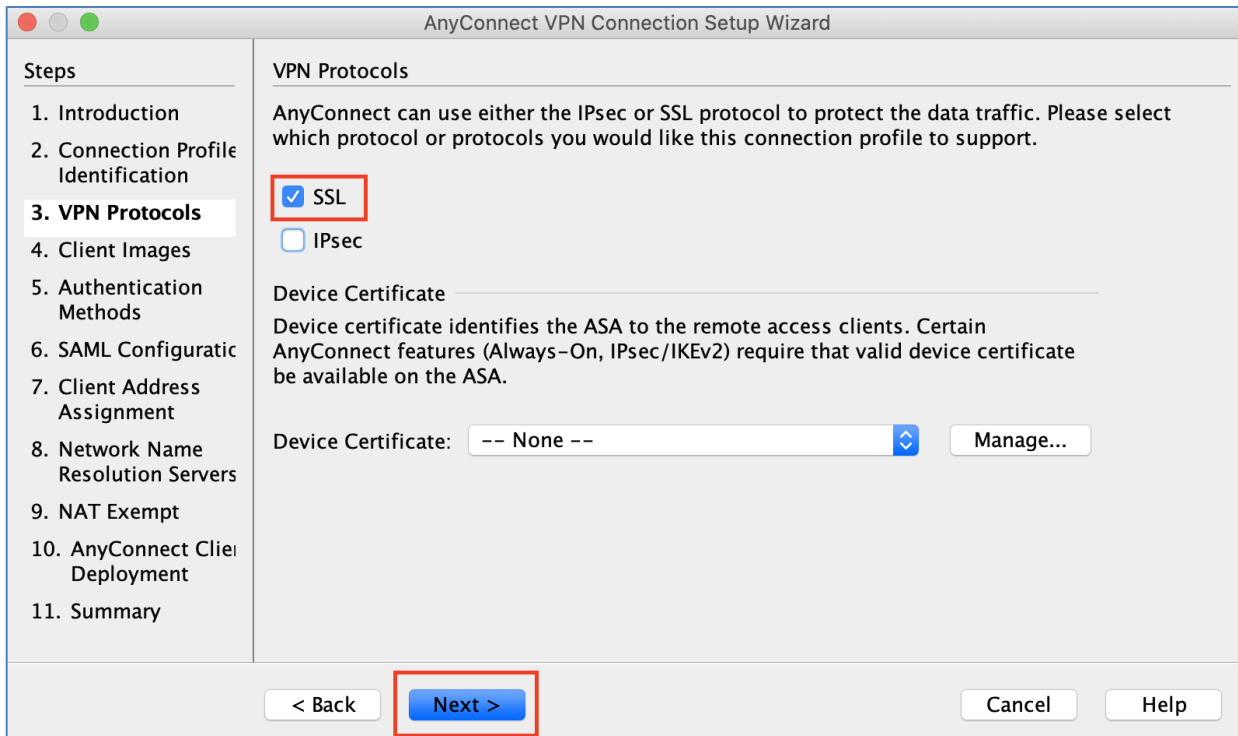
Step 9. Configure RAVPN on ASAVs (hubasa1, hubasa2, and hubasa3): Now we have our base infrastructure ready, let's configure RAVPN using Cisco Adaptive Security Device Manager (ASDM). Cisco VPN wizard configuration guide ([Cisco Documentation](#))

Device Name	VPN Profile Name	VPN Pool	VPN Type
hubasa1	srwvpn	10.82.64.0/18	RAVPN (SSL)
hubasa2	srwvpn	10.82.128.0/18	RAVPN (SSL)
hubasa3	srwvpn	10.82.192.0/18	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

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
- 4. Client Images**
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignment
8. Network Name Resolution Servers
9. NAT Exempt
10. AnyConnect Client Deployment
11. Summary

Client Images

ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.

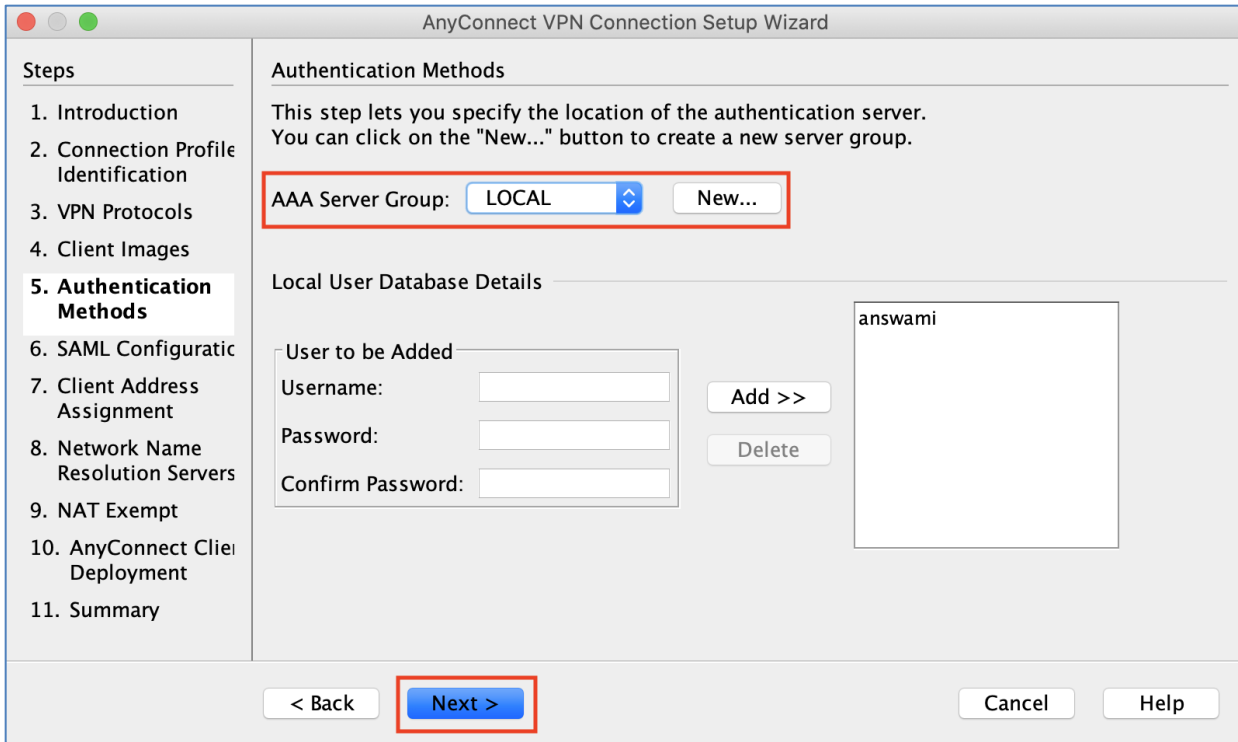
A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg	

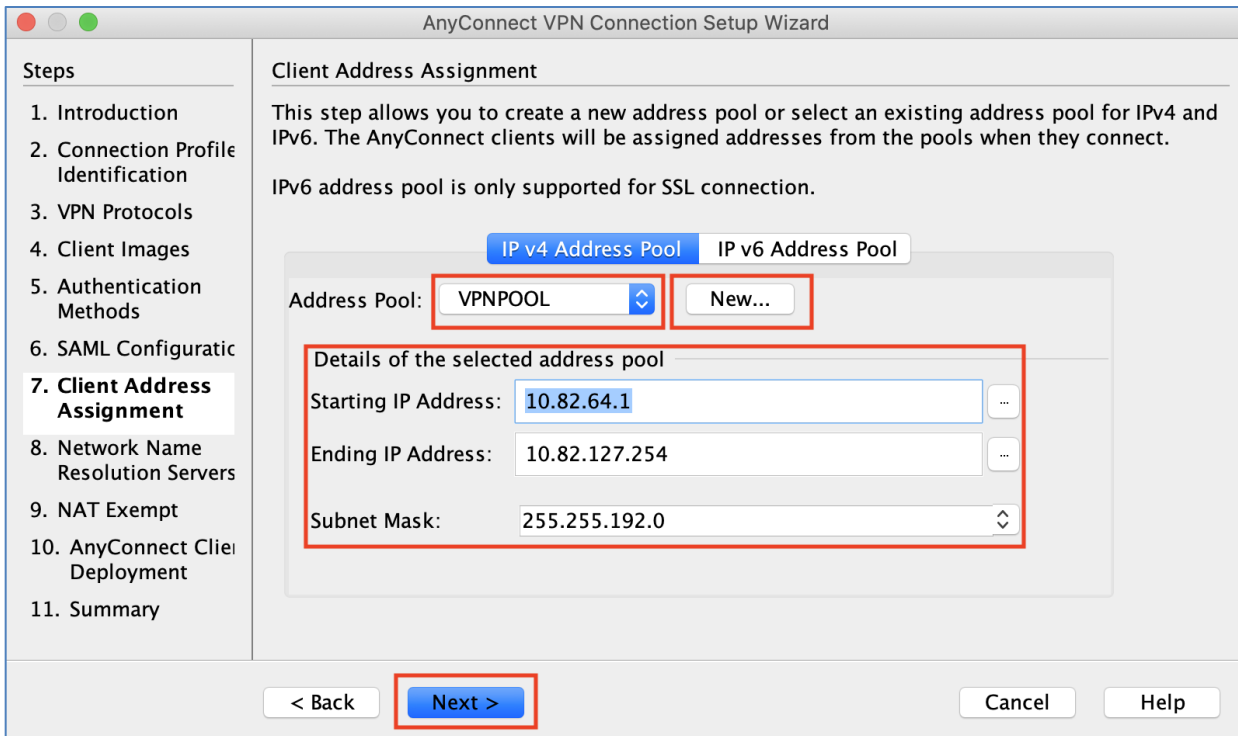
You can download AnyConnect Client packages from [Cisco](#) by searching 'AnyConnect VPN Client' or [click here](#).

< Back **Next >** Cancel Help

- 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

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. SAML Configuration
7. Client Address Assignment
- 8. Network Name Resolution Servers**
9. NAT Exempt
10. AnyConnect Client Deployment
11. Summary

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 168.63.129.16, 4.2.2.2

WINS Servers:

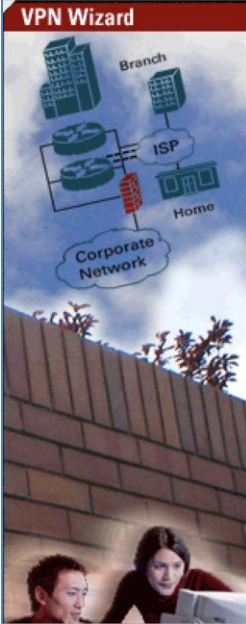
Domain Name: srwlab01.com

< Back **Next >** Cancel Help

- Enable NAT exempt for VPN traffic, then click next on AnyConnect Client Deployment page
- Click finish to deploy

AnyConnect VPN Connection Setup Wizard

VPN Wizard



Summary

Here is the summary of the configuration.

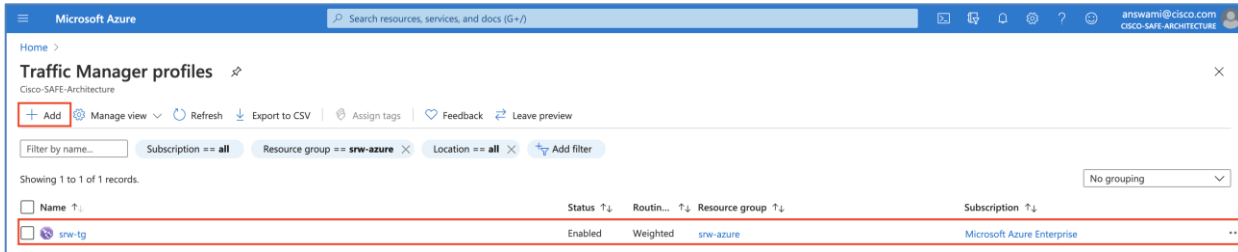
Name	Value
▼ Summary	
Name/Alias of the Connection Profile	srwvpn
VPN Access Interface	outside
Device Digital Certificate	-- none --
VPN Protocols Enabled	SSL only
AnyConnect Client Images	1 package
Authentication Server Group	LOCAL
SAML	Server: Authentication Method: aaa
Address Pool for the Client	10.82.64.1 – 10.82.127.254
DNS	Server: Domain Name:
Network Address Translation	The protected traffic can be subjected to network address translation

< Back **Finish** Cancel Help

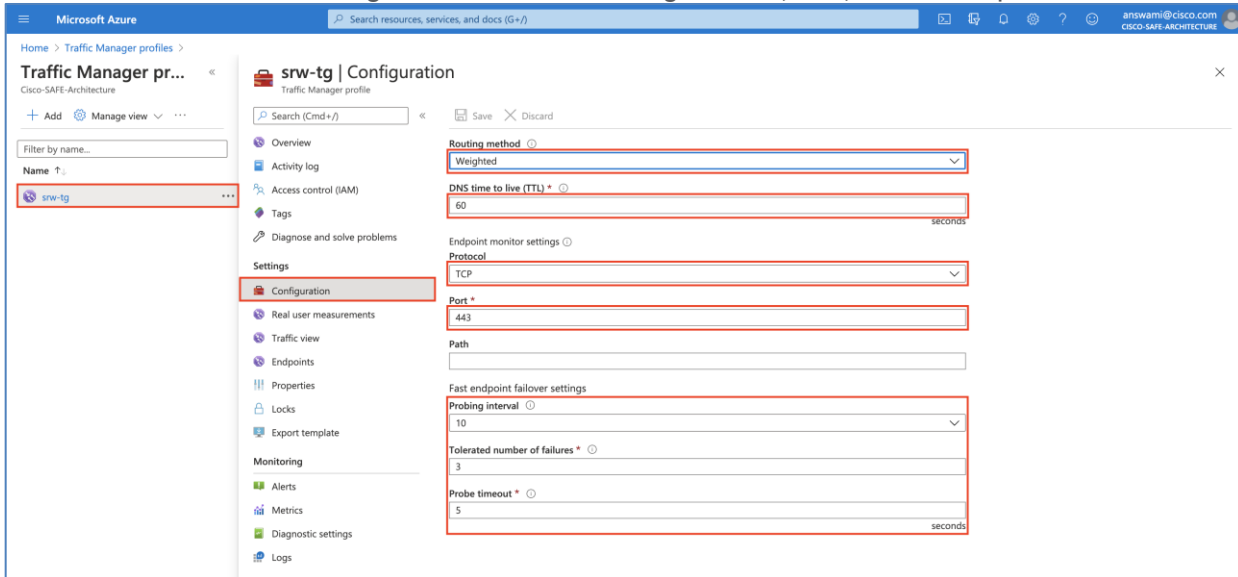
- Repeat VPN setup steps for hubasa2 and hubasa3, use the following VPN pool.

Device Name	VPN Profile Name	VPN Pool	VPN Type
hubasa1	srwvpn	10.82.64.0/18	RAVPN (SSL)
hubasa2	srwvpn	10.82.128.0/18	RAVPN (SSL)
hubasa3	srwvpn	10.82.192.0/18	RAVPN (SSL)

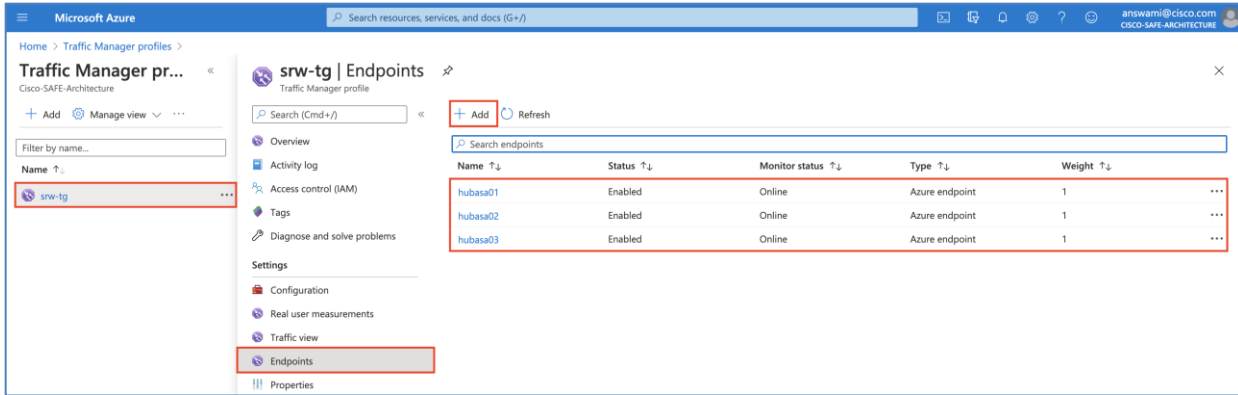
Step 10. Configure Azure Traffic Manager and enable RAVPN load balancing - In the Azure portal and search for 'Azure Traffic Manager Profiles' service. Click on "+add" to add a new Azure Traffic Manager.



- Once traffic manager profile is created, click on traffic manager profile (srw-tg)
- Now click on the configuration to define routing method, TTL, and health probe



- The next step is to add public IP addresses mapped to the outside interface of firewalls (hubasa1, hubasa2, and hubasa3) and select weight for all firewalls as 1.



Authentication

Configure LDAP Authentication for RAVPN

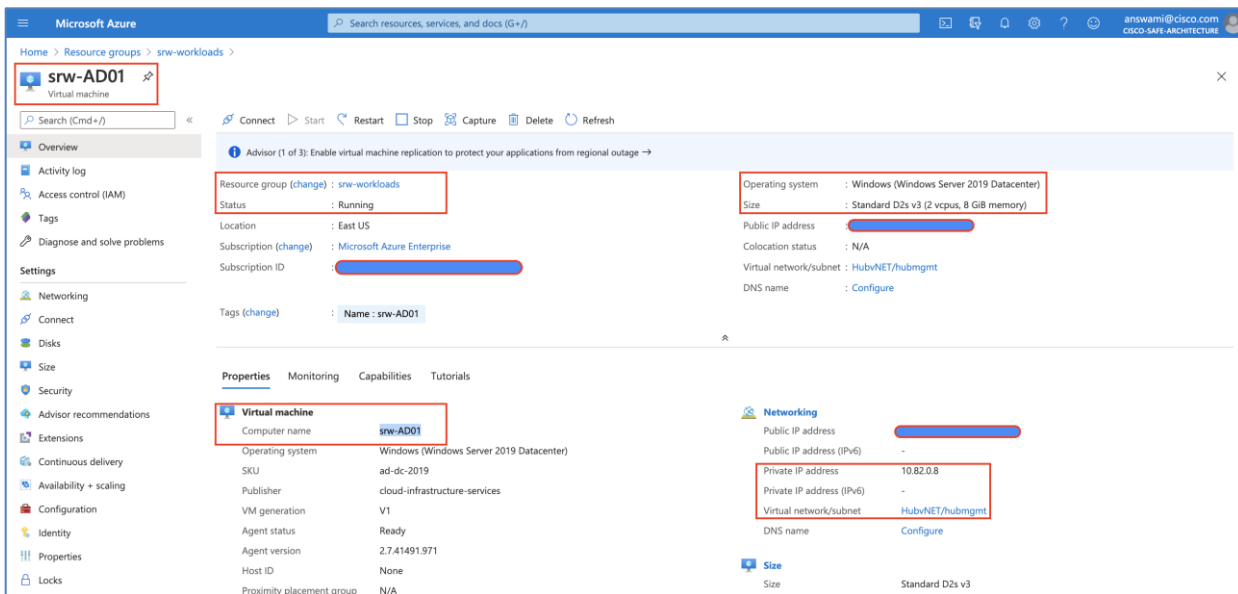
Step 1. Add aaa-server group on ASAs

Step 2. Edit aaa-server settings

Step 3. Change primary authentication in Anyconnect Connection Profile

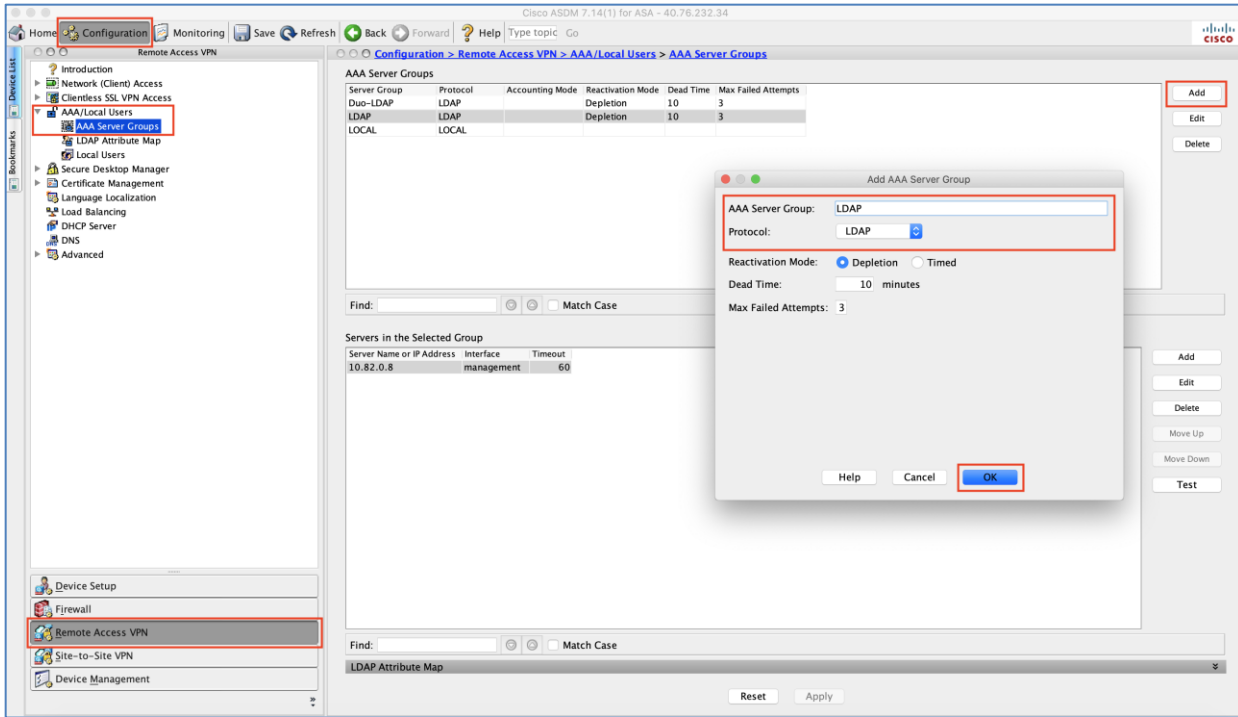
Now we have our base infrastructure ready, and we are all set to integrate LDAP authentication. Once LDAP authentication is enabled, we will modify the AnyConnect VPN profile to use LDAP for RAVPN user authentication. Active directory server is deployed in HubvNET.

VM Name	VNet/subnet	IP address	OS
srw-AD01	HubvNET/hubmgmt	10.82.0.8	Windows Server 2019 Data Center

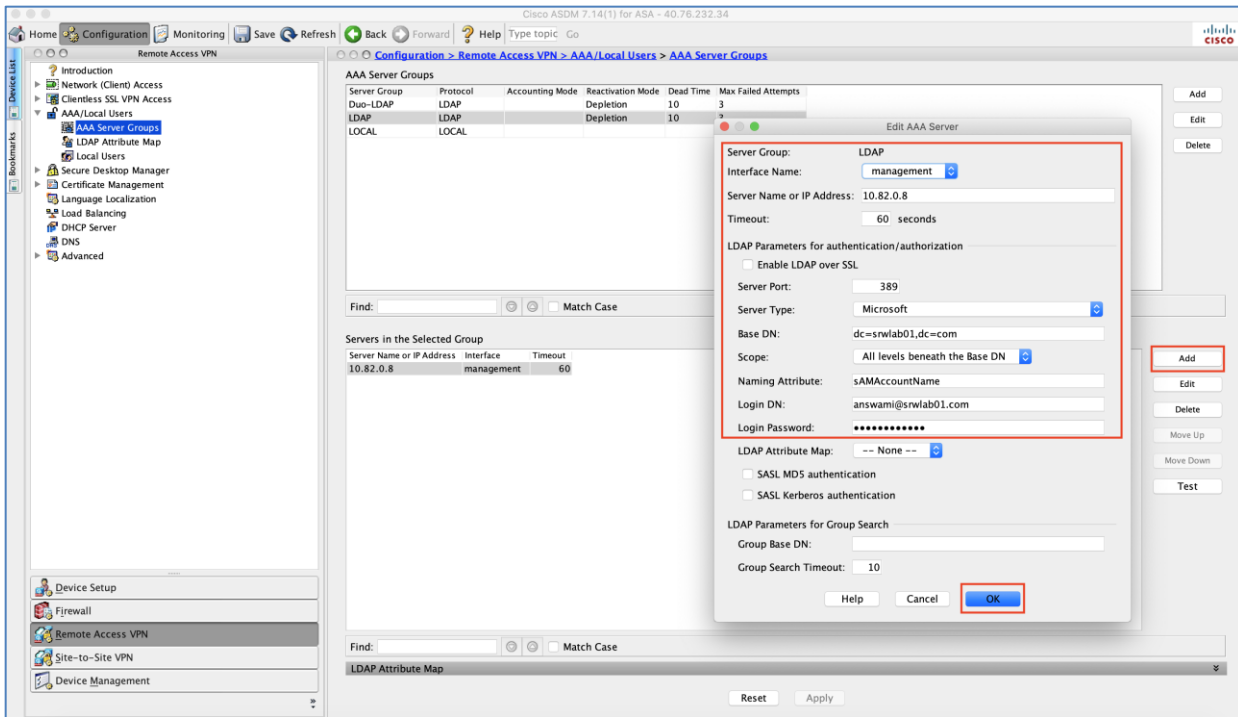


NSG associated with this VM has rules to allow RDP (TCP 3389), and LDAP (389) port. Cisco ASAs (hubasa1, hubasa2, and hubasa3) uses a management interface to reach srw-AD01 (Active Directory Domain Controller).

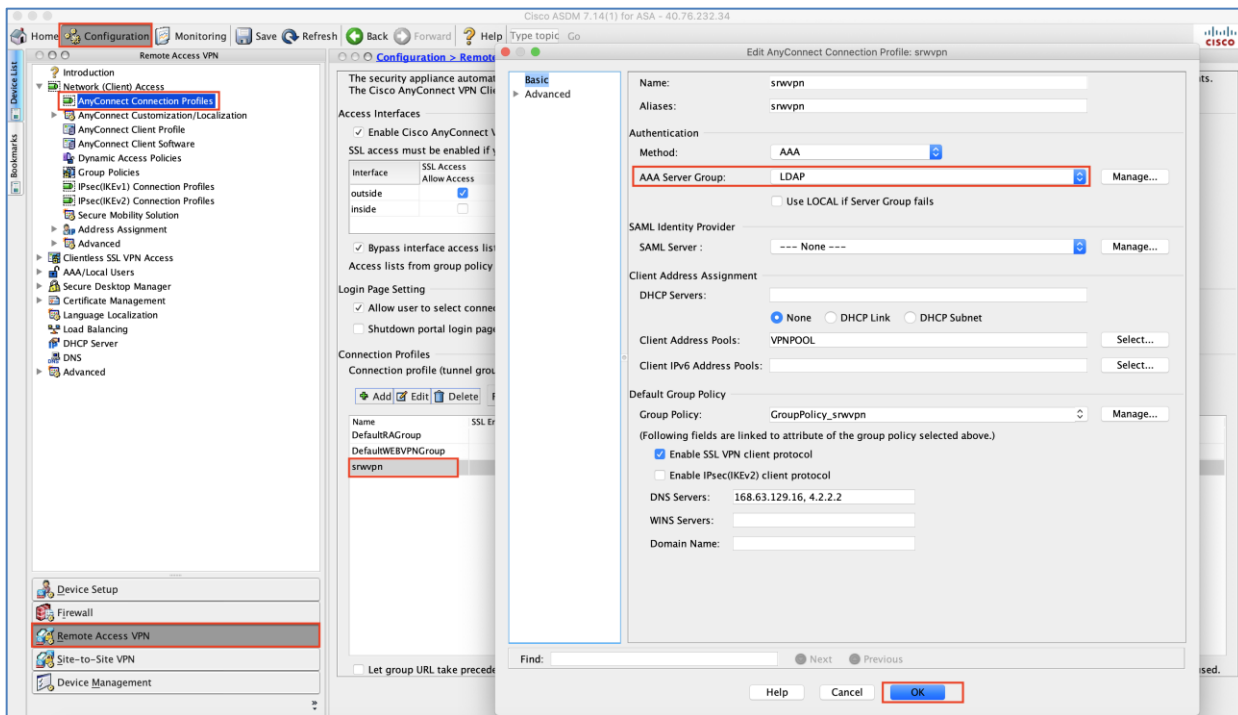
Step 1. Add aaa-server group on ASAVs - In ASDM, go to configuration -> Remote Access VPN -> AAA server group. Click on add, give it a name and then select LDAP from the drop-down menu and click ok.



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.

Search for users, groups, applications, or devices

Cisco Systems - Lab A/C | ID: [redacted] Anubhav Swami

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users | [Add User](#)

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

1 Total Users **0** Not Enrolled **0** Inactive Users **0** Trash **0** Bypass Users **0** Locked Out

[Select \(0\)](#) [Export](#)

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>	answami			1		Active	Jun 23, 2020 3:28 PM

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

Step 2. Add Application on Duo portal - 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).

Search for users, groups, applications, or devices

Cisco Systems - Lab A/C | ID: [redacted] Anubhav Swami

Dashboard > Applications

Applications

[SSO Setup Guide](#) | [Protect an Application](#)

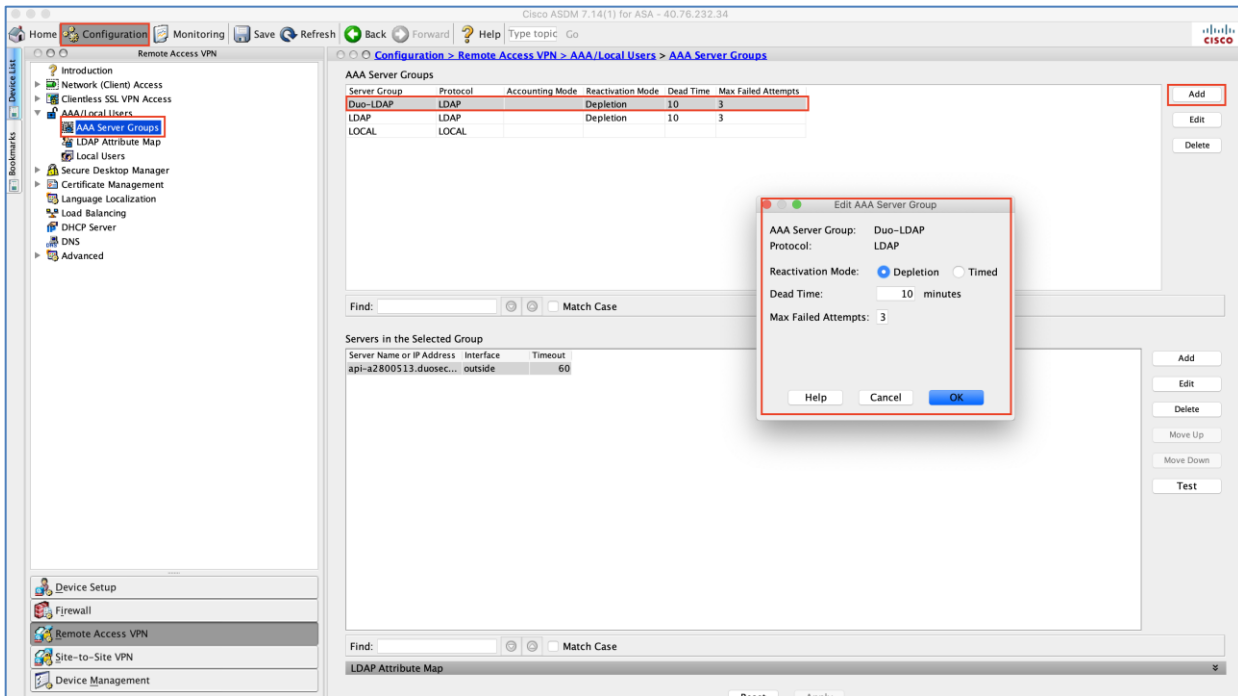
Did You Know Your Account Has Secure SSO?

Duo's secure single sign-on (SSO) allows users to access their cloud applications by logging in just once while providing you customized policies on a per-application basis, to secure them from risky users and devices.

[Export](#)

Name	Type	Application Policy	Group Policies
Cisco ASA SSL VPN	Cisco ASA SSL VPN		

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



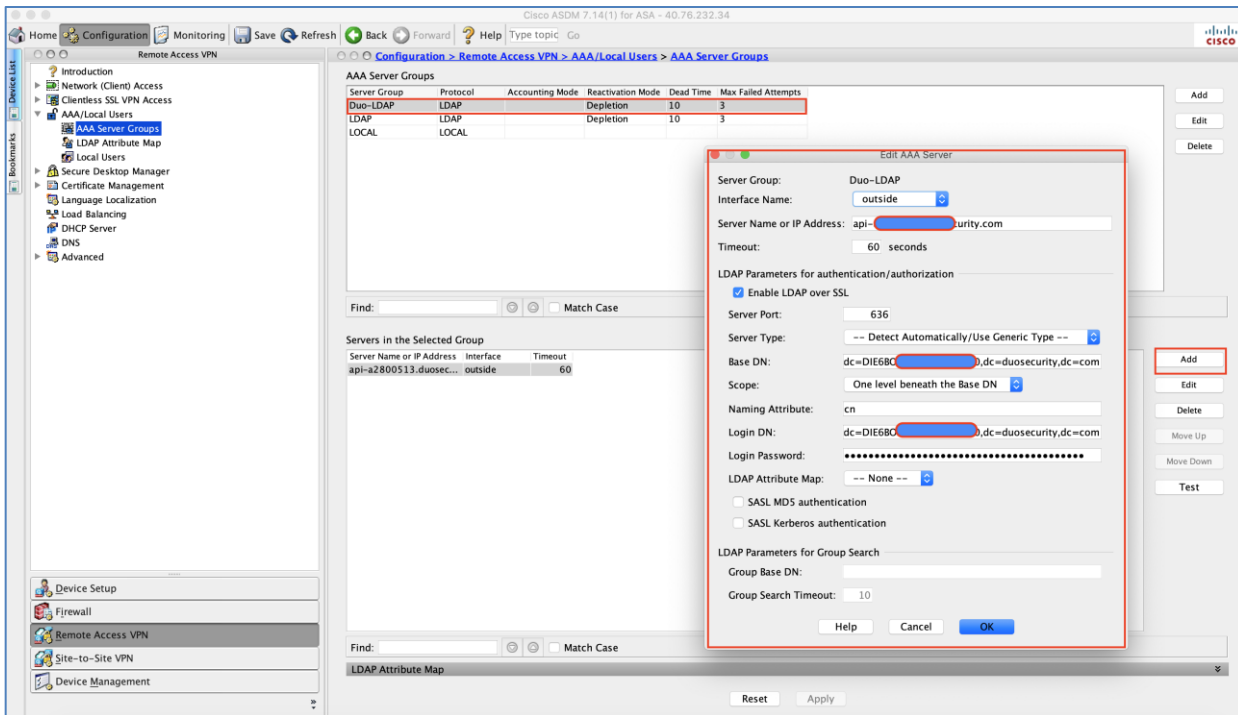
Step 4. Edit Duo-LDAP and add servers in the selected server group (timeout should be 60).

Server or IP address is API hostname

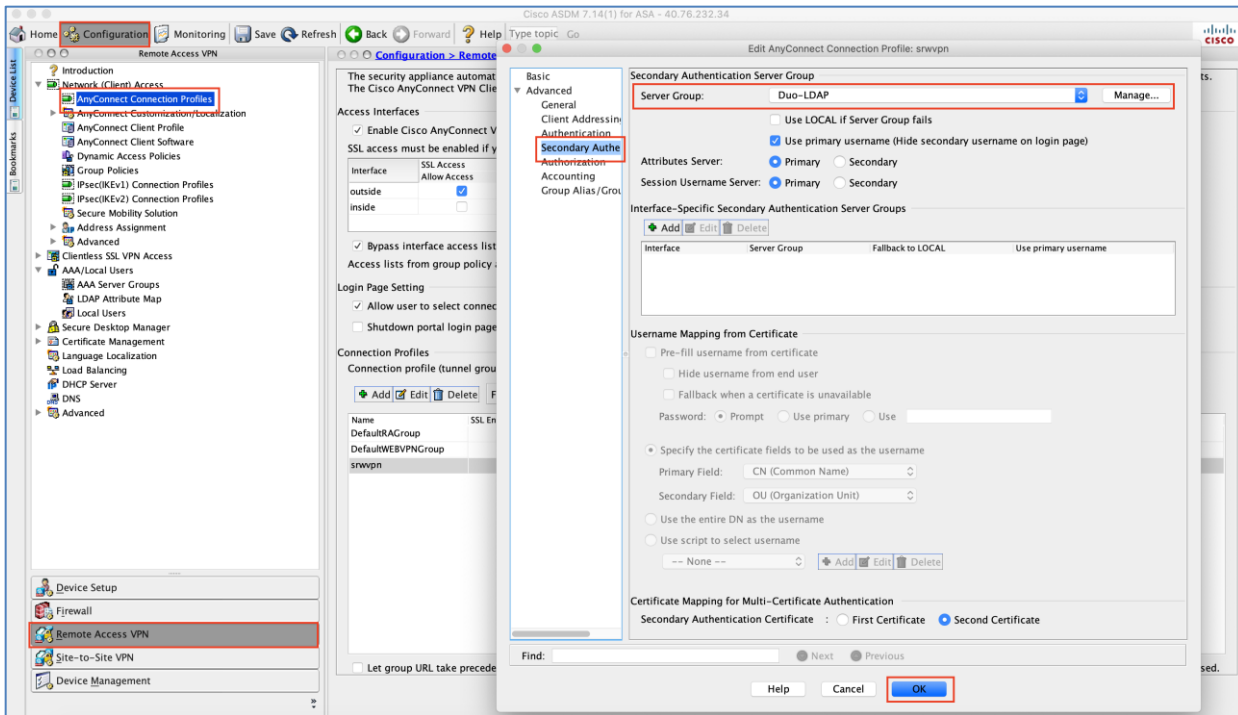
Base DN is dc=Integration_key,dc=duosecurity,dc=com

Login DN is same as Base DN

Login password is integration key.



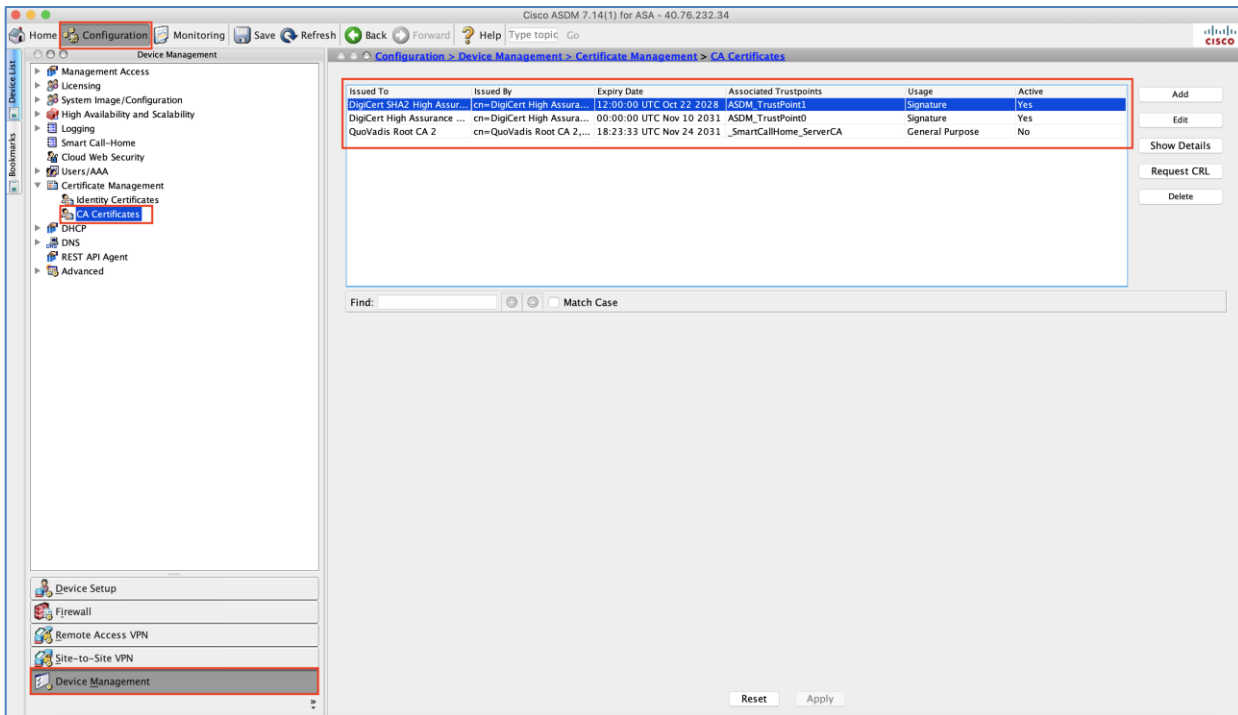
Step 5. Edit AnyConnect VPN profile and add LDAP-Duo for two factor authentication - Make sure that "Use primary username" is checked.



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.

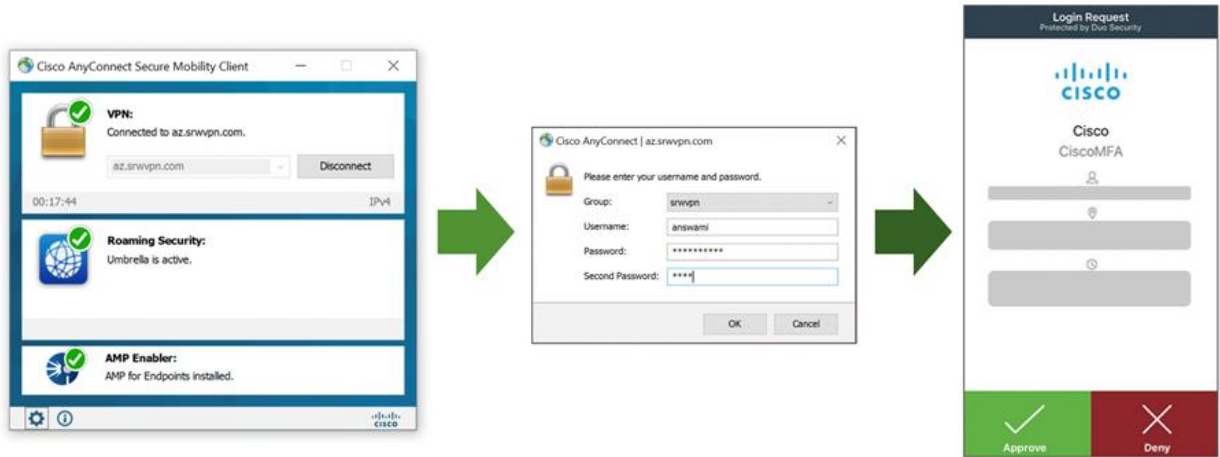
Cert1: <https://dl.cacerts.digicert.com/DigiCertHighAssuranceEVRootCA.crt>

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: az.srvwpn.com, username, password, and secondary password). In secondary password as push, call, or text to get Duo challenge on the enrolled device.



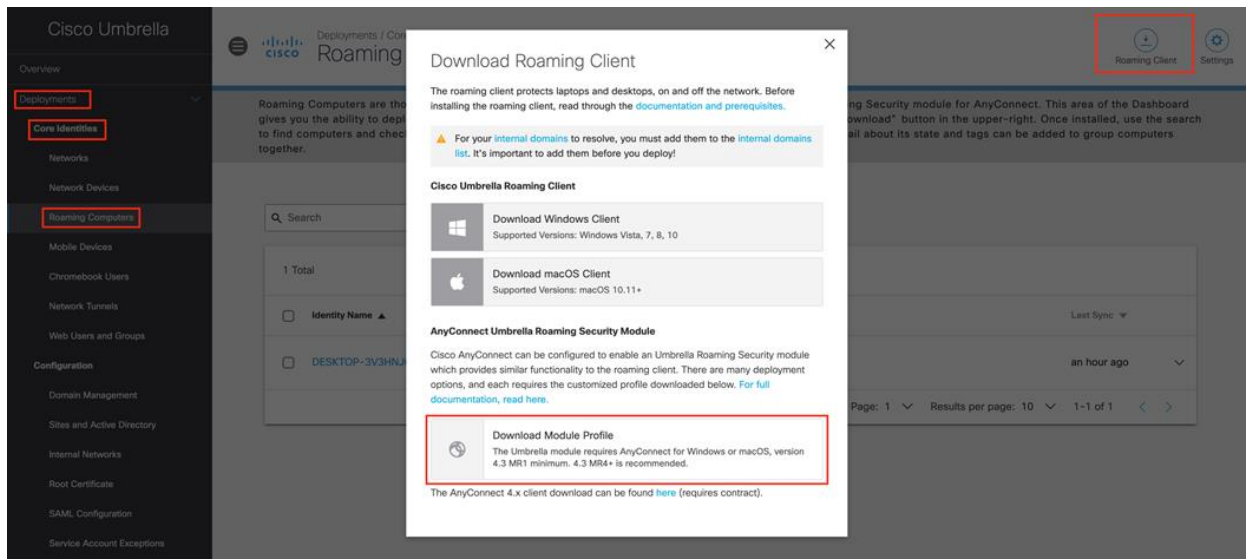
By default, the user will get a certificate error, to avoid certificate error install trusted certificates on ASAVs. (Cisco Documentation)

Threat Protection

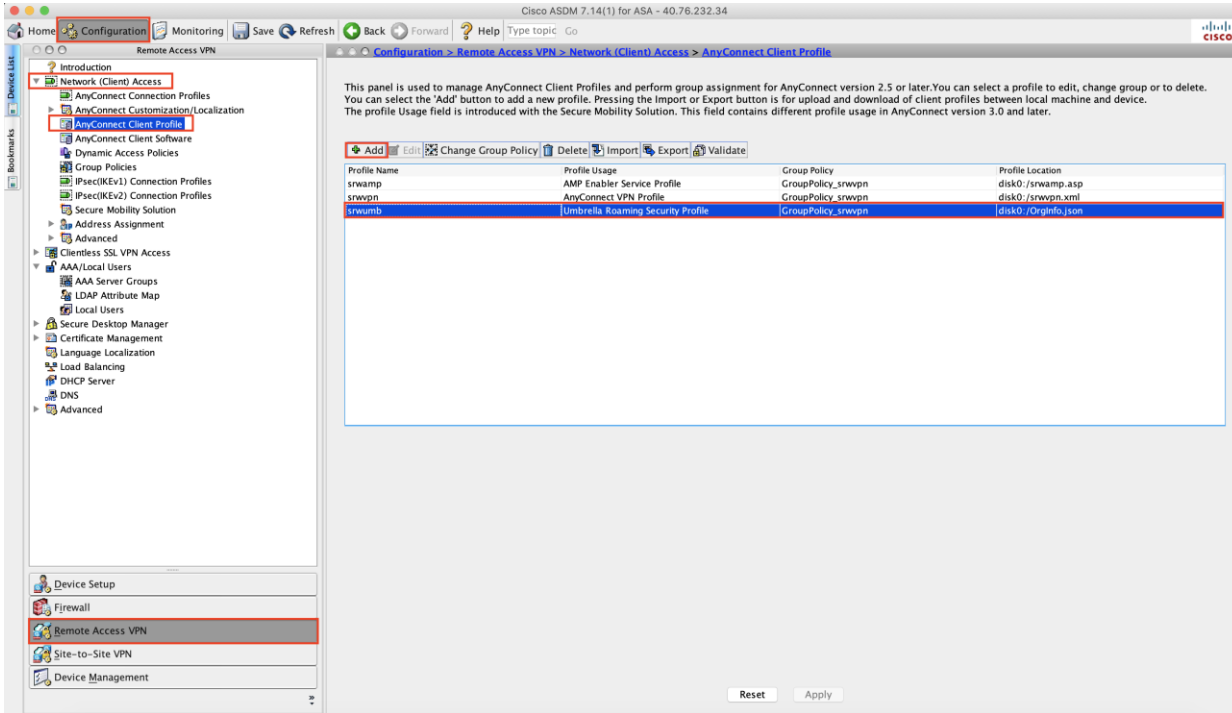
Cisco Umbrella Roaming Security Module

- 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

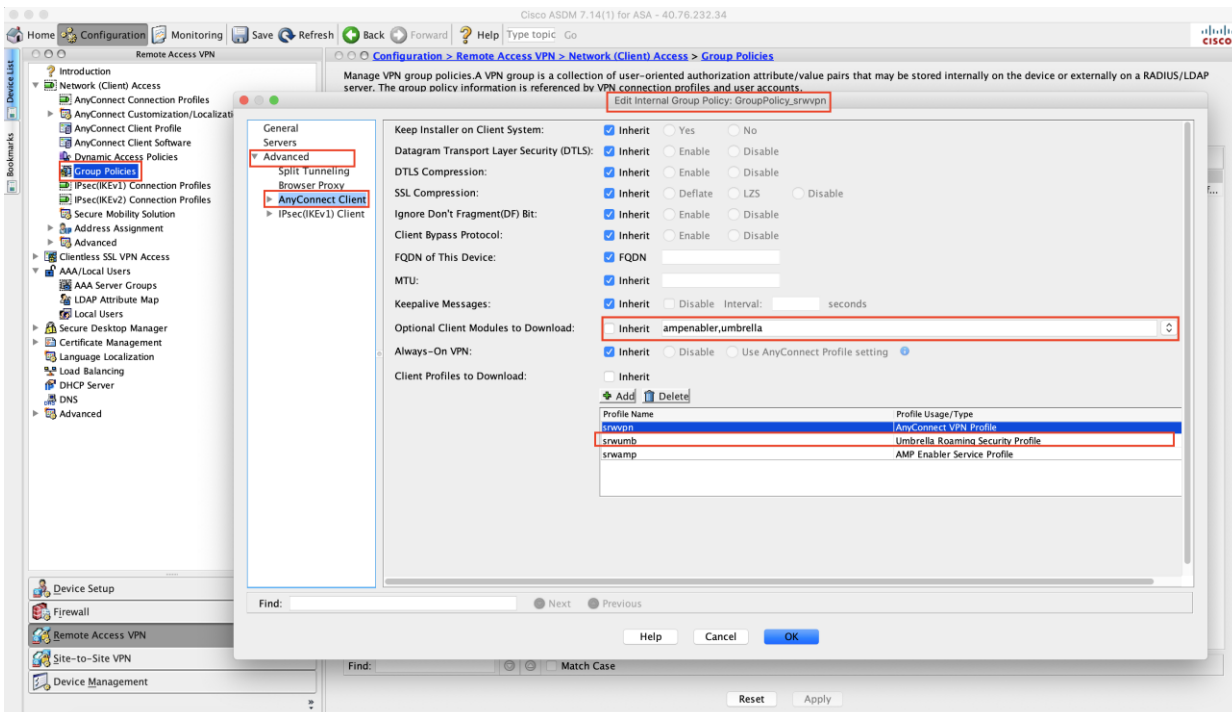
Step 1. Download Umbrella Roaming Security Module: - Access Cisco Umbrella portal, navigate to Deployments → Core Identities → Roaming Computers, and click Roaming Client. Download module profile (OrgInfo.json). ([Cisco Umbrella Documentation](#))



Step 2. Setup AnyConnect Client Profile - In ASDM, 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.

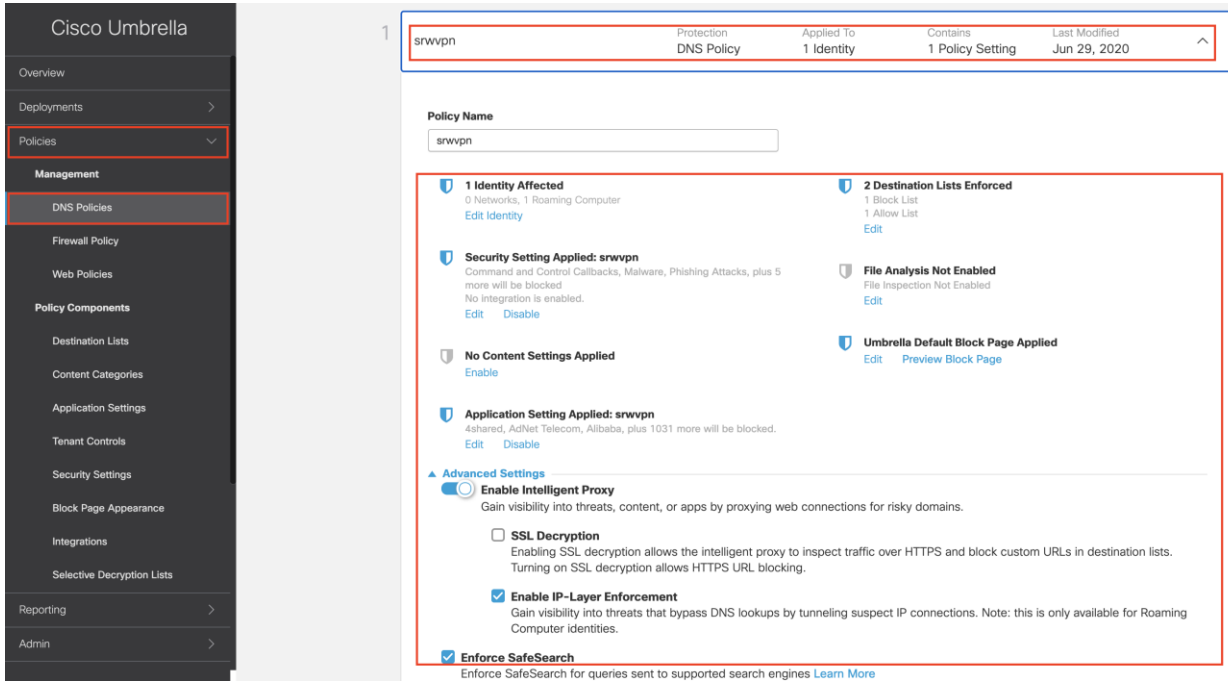


Step 3. Enable Umbrella Roaming Security Profile: Navigate to Configuration → Remote Access VPN → Network (Client) Access → Group Policy → select Group_Policy, now ensure it has Umbrella Roaming Security Profile enabled



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

The screenshot shows the 'Edit Group' configuration page for 'SecureRemoteWorker' in the Cisco AMP for Endpoints Management console. The 'Management' menu is highlighted. The group name is 'SecureRemoteWorker'. The configuration includes various policies: Windows Policy (Protect Policy), Android Policy (Default FireAMP Android), Mac Policy (Protect Policy for FireAMP Mac), Linux Policy (Protect Policy for FireAMP Linux), and iOS Policy (Protect). There are 'Cancel' and 'Save' buttons. On the right, the 'Computers' section shows 1 direct member (DESKTOP-3V3HNJG) and no child members. Below, the 'Child Groups' section is empty, and the 'Add Child Groups' list includes DMZ Shared Services, Domain Controller, Industrial Workstations, Orbital Group, Protect, Secure Campus, Secure Cloud, Secure DC, Server, and Triage.

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.

The screenshot shows the configuration for the 'SecureRemoteWorker-Windows' endpoint group. The group is associated with the 'SecureRemoteWorker' group. The configuration includes Modes and Engines (Files: Quarantine, Network: Block, Malicious Activity Protection: Quarantine, System Process Protection: Protect), Exclusions (Microsoft Windows Default), Proxy (Not Configured), and Groups (SecureRemoteWorker). Under Outbreak Control, Custom Detections - Simple includes CloudApp-CSD. The configuration was modified on 2020-07-02 17:46:31 UTC with Serial Number 241. Action buttons include View Changes, Download XML, Duplicate, Edit, and Delete.

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 Azure storage.

The screenshot shows the Cisco AMP for Endpoints Premier Management interface. The 'Management' menu is selected. The 'Group' dropdown is set to 'SecureRemoteWorker'. There are four panels for different operating systems: Windows, Mac, Linux, and Android. Each panel has configuration options and 'Show URL' and 'Download' buttons.

Operating System	Protect Policy	Flash Scan on Install	Redistributable	Connector Version	Package Format
Windows	Protect Policy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7.1.5.11523	-
Mac	Protect Policy for FireAMP Mac	<input checked="" type="checkbox"/>	-	1.12.4.740	DMG
Linux	Protect Policy for FireAMP Lin...	<input checked="" type="checkbox"/>	-	1.11.1.663	-
Android	Default FireAMP Android	<input type="checkbox"/>	-	2.0.1.73	-

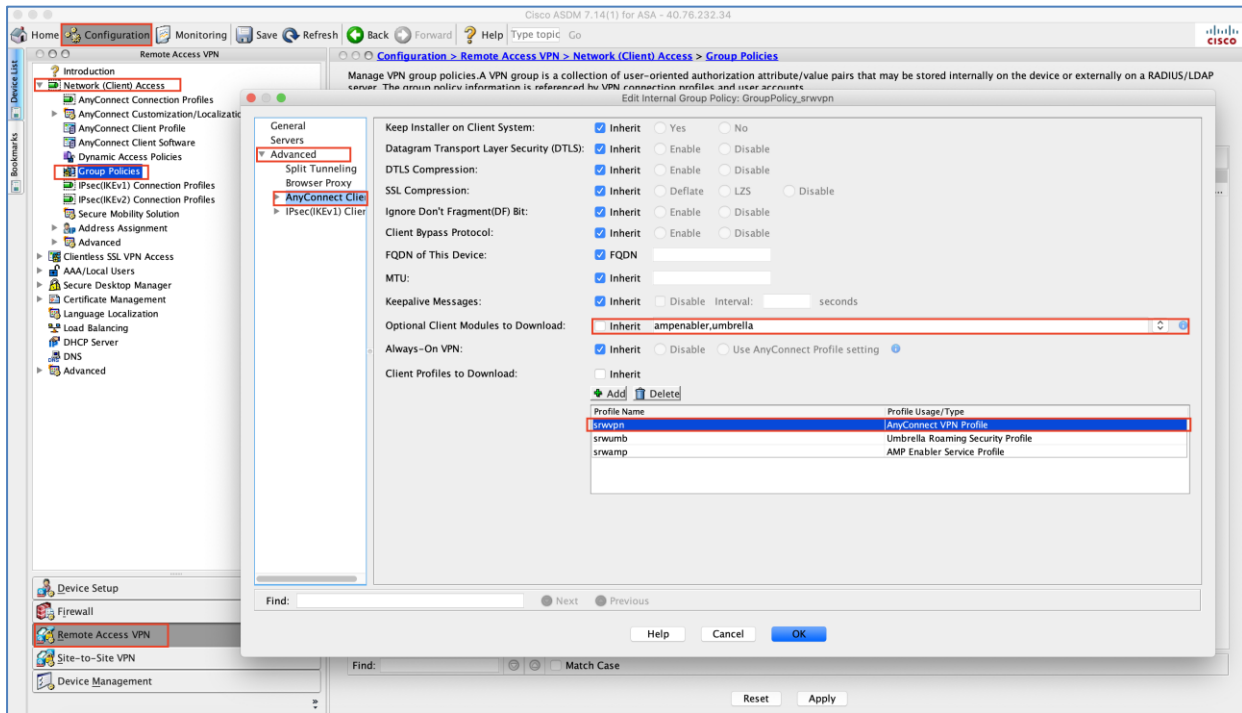
Step 4. Add AMP Enabler Service Profile -Navigate to Configuration → Remote Access VPN → Network (Client) Access → AnyConnect Client Profile. Add the AMP Enabler Service Profile, point to connect URL shown in **step 3**.

The screenshot shows the Cisco ASDM Configuration page for AnyConnect Client Profile. The 'AnyConnect Client Profile' is selected in the left-hand navigation pane. The main pane shows a table of profiles with columns for Profile Name, Profile Usage, Group Policy, and Profile Location.

Profile Name	Profile Usage	Group Policy	Profile Location
Anyamp	AMP Enabler Service Profile	GroupPolicy_srswpn	disk0:/srwmpa1.tfp
srwvpn	AnyConnect VPN Profile	GroupPolicy_srswpn	disk0:/srwvpn.xml
srwumb	Umbrella Roaming Security Profile	GroupPolicy_srswpn	disk0:/OrgInfo.json

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

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

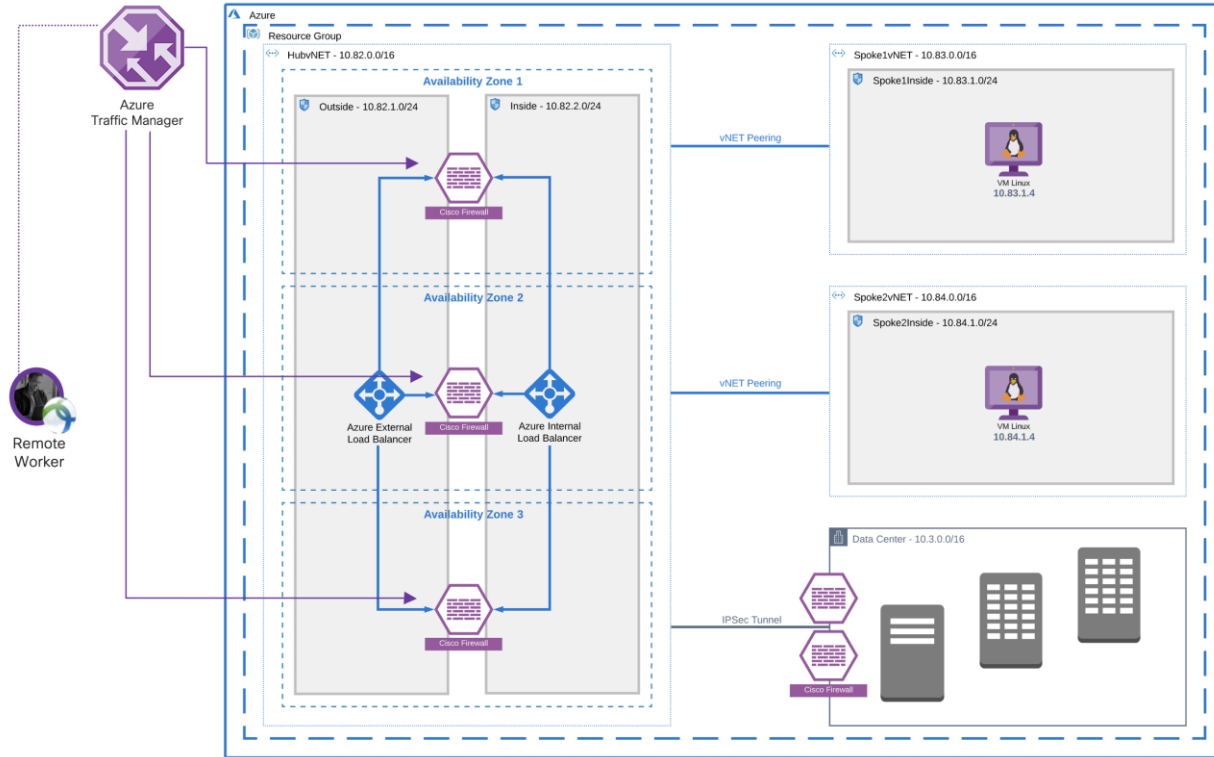


Validation Testing

Test Case 1 - Cisco AnyConnect Remote Access VPN load balancing using Azure Traffic Manager

The secure remote worker initiates a connection to az.srwvpn.com (cname mapped to Azure traffic manager's FQDN), Azure traffic manager has hubasa1, hubasa2, and hubasa3 in endpoints. Azure probes Cisco firewalls on TCP 443, as long as firewall responds to these probes firewall is marked as online. ATM load balances traffic to the endpoints on a weighted average (Weight for each firewall is 1).

The Azure Traffic Manager is responsible for load balancing SSL VPN across hubasa1, hubasa2, and hubasa3.

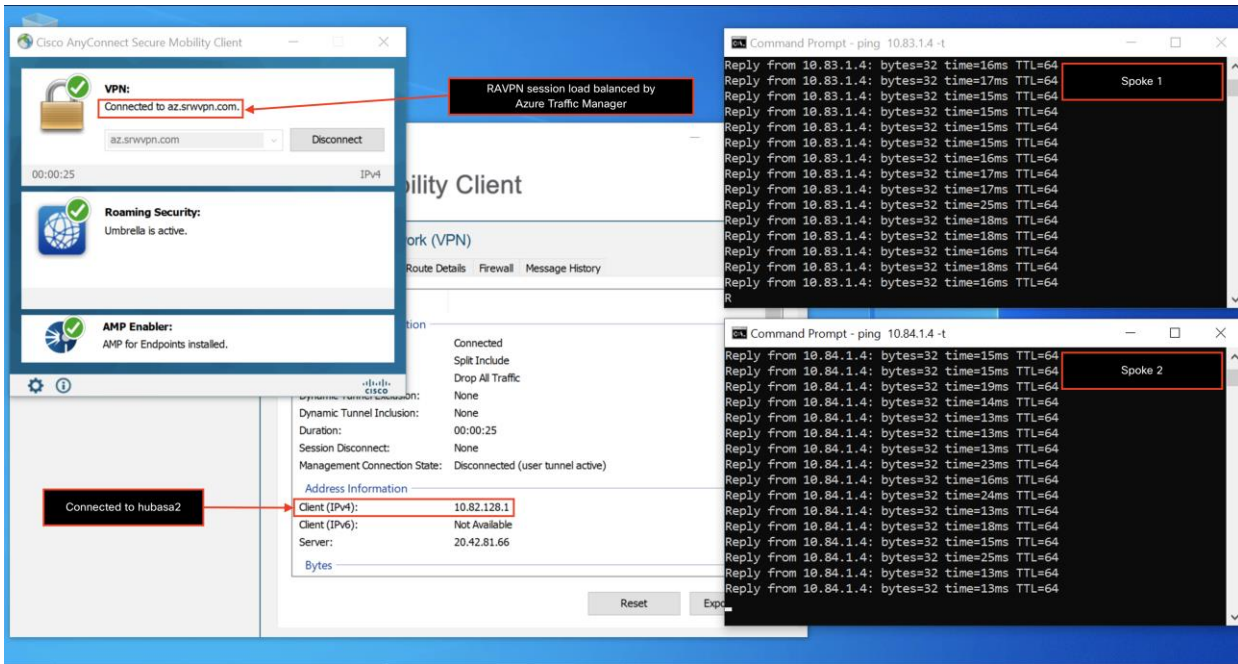


- ATM endpoint configuration ensure equal load distribution of SSL RAVPN.

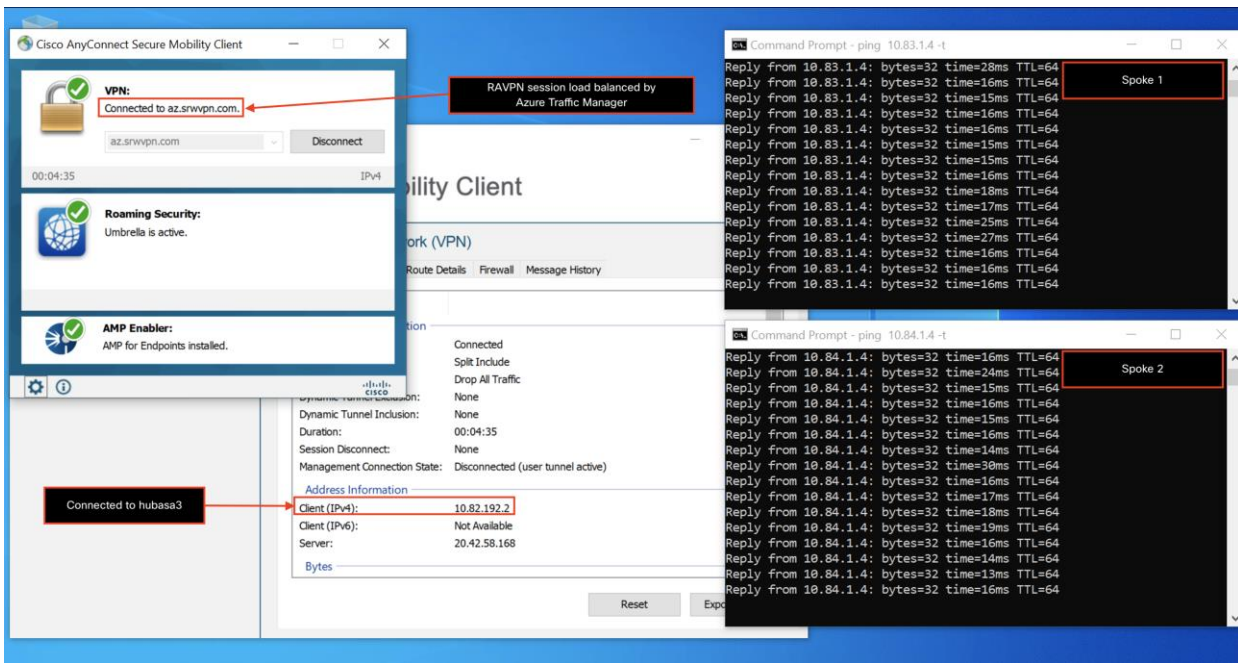
Name	↑↓ Status	↑↓ Monitor status	↑↓ Type	↑↓ Weight
hubasa01	Enabled	Online	Azure endpoint	1
hubasa02	Enabled	Online	Azure endpoint	1
hubasa03	Enabled	Online	Azure endpoint	1

Remote worker is connected to az.srvvpn.com and session is terminated on hubasa1 (firewall 1). User is able to access workloads in Spoke1vNET and Spoke2vNET.

Remote worker is connected to az.srvvpn.com and session is terminated on hubasa2 (firewall 2). User is able to access workloads in Spoke1vNET and Spoke2vNET.



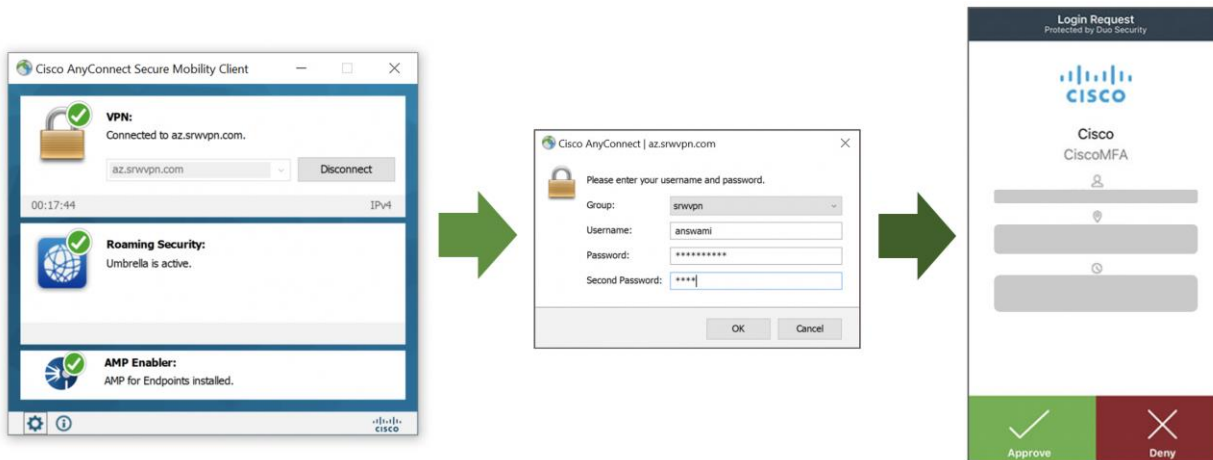
Remote worker is connected to az.srvvpn.com and session is terminated on hubasa3 (firewall 3). User is able to access workloads in Spoke1vNET and Spoke2vNET.



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.

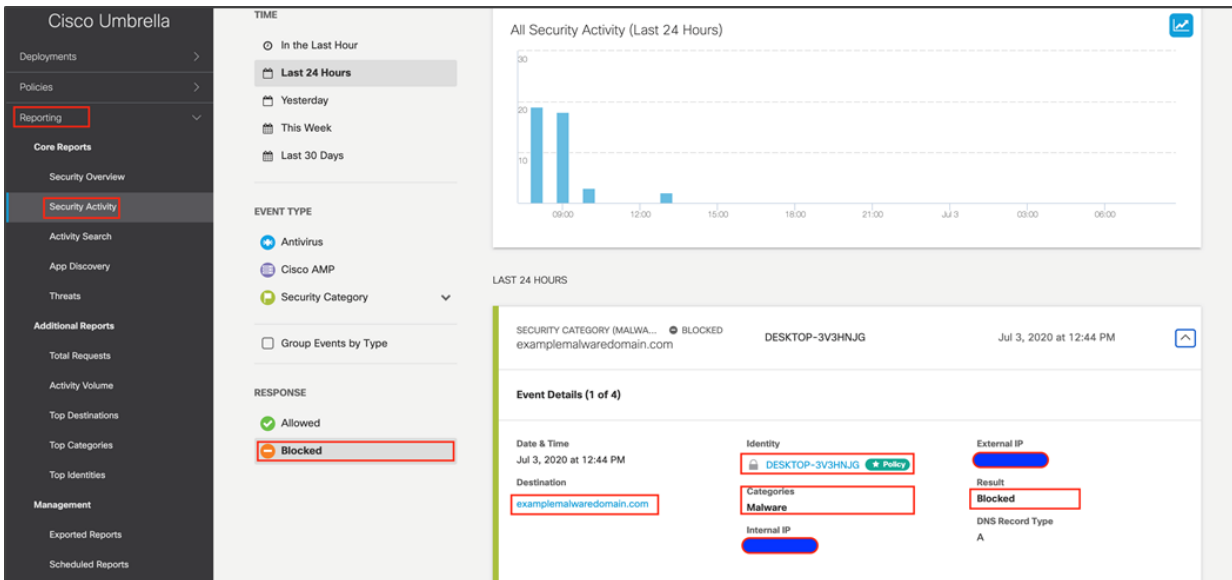
Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
12:35:26 PM JUL 3, 2020	✓ Granted User approved	answami	Cisco ASA SSL VPN	Location Unknown 0.0.0.0	Duo Push Raleigh, NC
5:30:32 PM JUL 2, 2020	✓ Granted User approved	answami	Cisco ASA SSL VPN	Location Unknown 0.0.0.0	Duo Push Raleigh, NC

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 "examplemalware.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

The screenshot shows the Cisco Umbrella Activity Search interface. The left sidebar has 'Reporting' and 'Activity Search' highlighted. The main panel shows a search for 'Blocked' requests. The table lists various requests with columns for Identity, Destination, Identity Used by Policy, Internal IP, External IP, and Action. The 'Internal IP' column is redacted with a blue box. The 'Response' filter is set to 'Blocked'.

Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action
DESKTOP-3V3HNJG	nexusrules.officeapps.live.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	nexusrules.officeapps.live.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	nexusrules.officeapps.live.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	nexusrules.officeapps.live.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	nexusrules.officeapps.live.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	dlassets-ssl.xboxlive.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	dlassets-ssl.xboxlive.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	spclient.wg.spotify.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	spclient.wg.spotify.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	examplemalwaredomain.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	examplemalwaredomain.com	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block
DESKTOP-3V3HNJG	inference.location.live.net	DESKTOP-3V3HNJG	[Redacted]	[Redacted]	Block

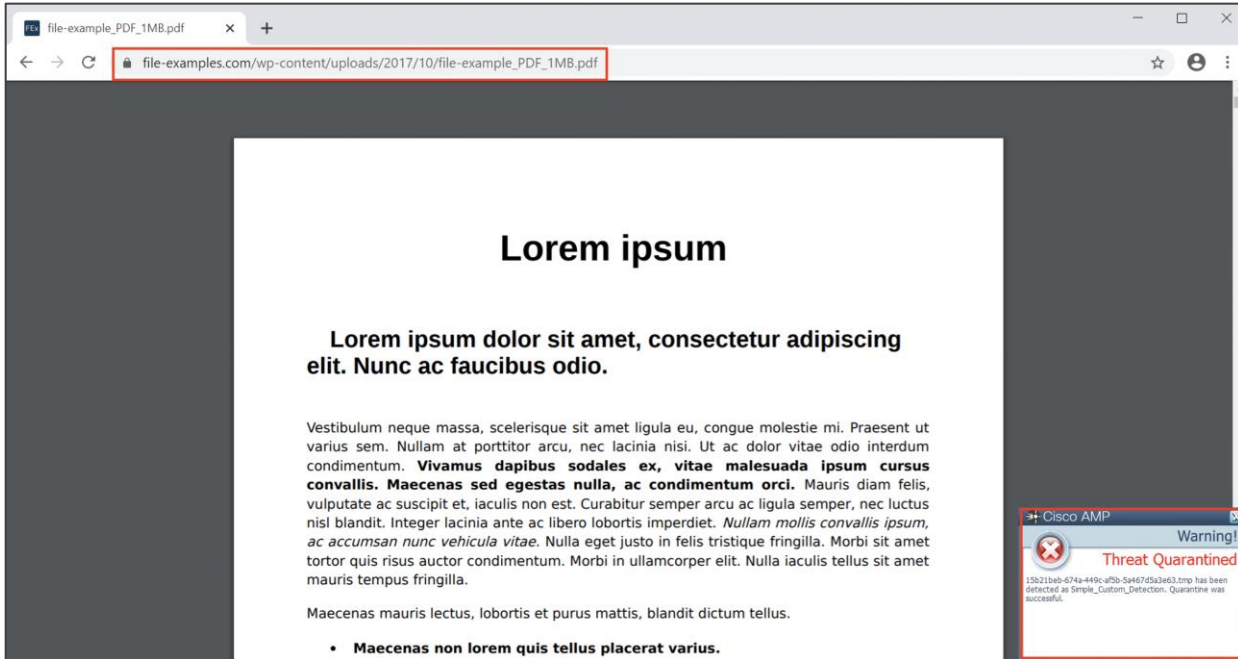
Allowed sessions

The screenshot shows the Cisco Umbrella Activity Search interface with filters set to 'Identity: DESKTOP-3V3HNJG' and 'Response: Allowed'. The table lists various requests to www.cisco.com and other domains. The 'Response' filter is set to 'Allowed'.

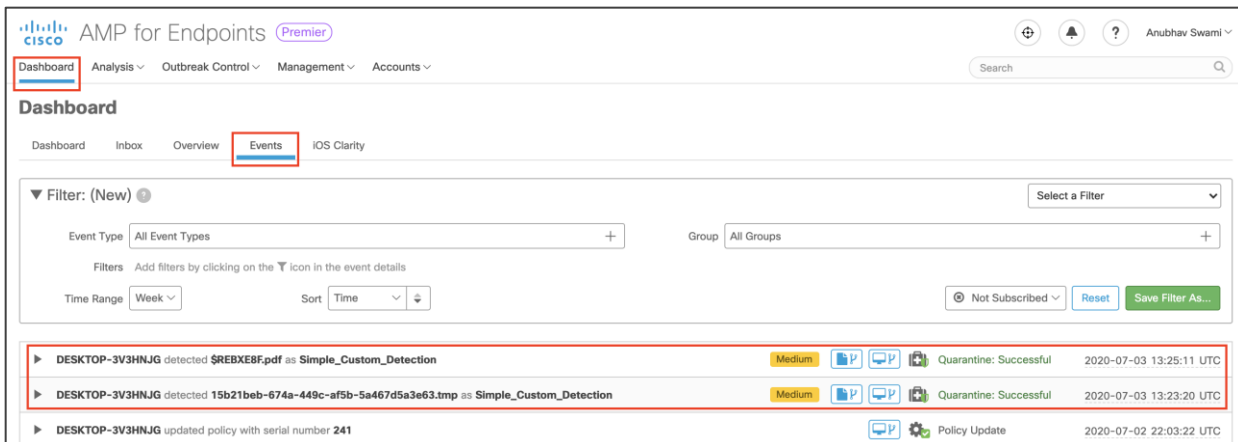
Identity	Destination	Identity Used by Policy
DESKTOP-3V3HNJG	www.cisco.com	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	www.cisco.com	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	www.cisco.com	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	www.cisco.com	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	ocsp.digicert.com	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	ocsp.digicert.com	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	http://ocsp.digicert.com/MFEwTzBNMEswSTAjBgUrDgMCGgUABBTBLOV2R...	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	md5.hackerwatch.org	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	md5.hackerwatch.org	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	md5.hackerwatch.org	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	md5.hackerwatch.org	DESKTOP-3V3HNJG
DESKTOP-3V3HNJG	settings.data.microsoft.com	DESKTOP-3V3HNJG

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 Azure.

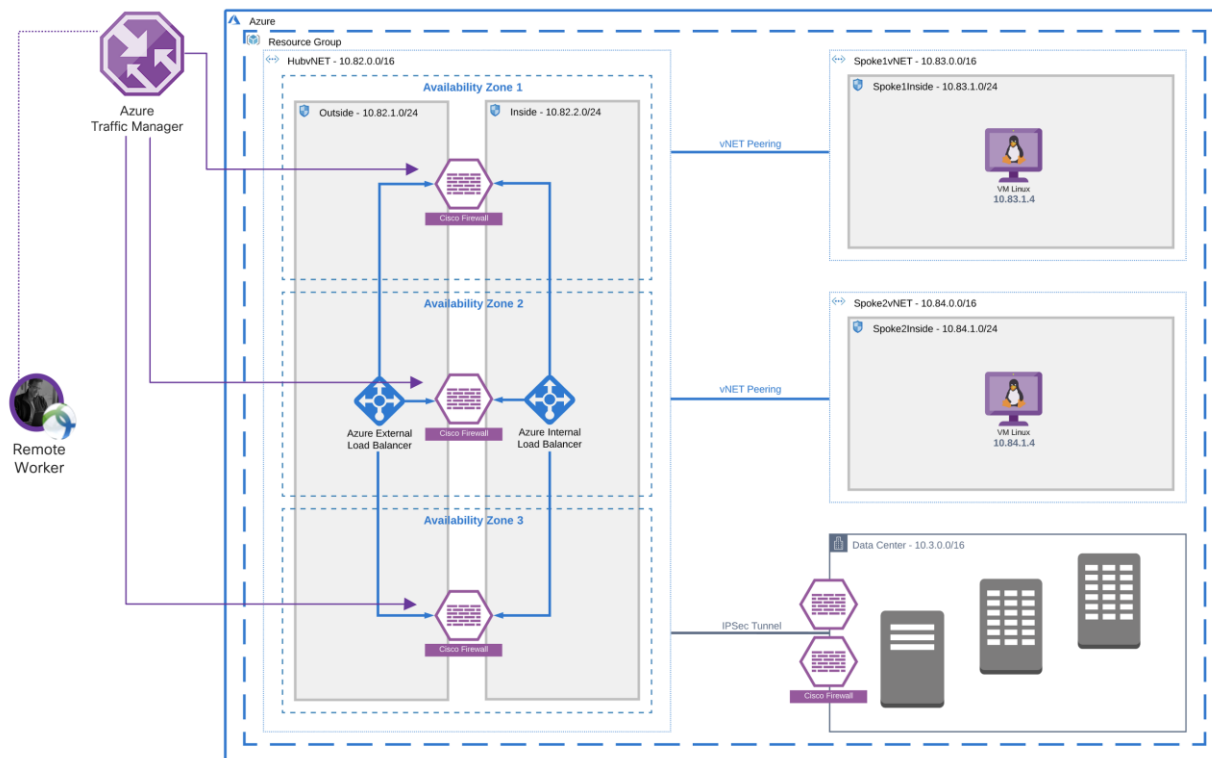


Figure 30.
Components of the Cisco secure remote worker solution

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 ASA v datasheet: <https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/datasheet-c78-733399.html>

Cisco NGFW v 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

ARM - Azure Resource Manager

ASA_v - Adaptative Security Virtual Appliance

ASDM - Adaptive Security Appliance Device Manager

AVC - Application Visibility and Control

CDO - Cisco Defense Orchestrator

CVD - Cisco Validated Design

ELB - External Load Balancer

FDM - Firepower Device Manager

FMC - Firewall Management Center

FQDN - Fully Qualified Domain Name / DNS Name

FTD - Firepower Threat Defense

ILB - Internal Load Balancer

MFA - Multi Factor Authentication

NGFW_v - Next-Generation Firewall Virtual

NGIPS - Next Generation Intrusion Prevention System

NSG - Network Security Group

NVA - Network Virtual Appliance

PIN - Place in network

RAVPN - Remote Access VPN

RG - Resource Group

TM - Traffic Manager

UDR - User Defined Route

VNet - Virtual Network

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>

ARM yourself using NGFWv and ASAv (Azure) - BRKSEC-3093 (Cisco Live Login required) - Search BRKSEC-3093 in the filter bar

<https://www.ciscolive.com/global/on-demand-library.html?#/>

Azure Documentation:

<https://docs.microsoft.com/en-us/azure/?product=featured>

Azure Resource Group:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>

Azure Network Security Group:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

Azure Virtual Network (VNet):

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>

Azure VNet Peering:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

Azure Load Balancer:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

Azure Routing:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

Azure DNS Zone:

<https://docs.microsoft.com/en-us/azure/dns/dns-zones-records>

Azure Traffic Manager:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>

Azure Resource Manager (ARM):

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>

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>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)