

Secure Remote Worker for On-Prem

Design Guide

October, 2021

Contents

Scope	3
In Scope	3
Out of scope	3
Introduction	4
Secure Remote Worker Architecture	4
Secure Remote Worker Business Flows	6
Solution Overview	7
Remote access VPN key capabilities for traffic and threat management	7
Target Audience	11
Product Overview	11
Security Integrations	13
Policy Setup for Secure VPN Client Modules	14
Umbrella	14
Secure Endpoint	21
Remote Worker Deployment	22
Version Information	22
Network Topology	23
Cisco Firepower Threat Defense	23
Cisco Secure Access by Duo	35
Cisco Secure VPN	37
Cisco Umbrella Roaming Security module	49
Cisco Secure Endpoint Connector	54
Validation Testing	57
Test Case 1- Cisco Duo two-factor authentication (2FA)	57
Test Case 2 - Cisco Umbrella Roaming Security Module (DNS layer protection)	59
Test Case 3 - Cisco Secure Endpoint AMP enabler (File blocking)	60
Test Case 4 - Geolocation blocking	62
Appendix	62
Appendix A - Licensing information	62
Appendix B - Acronyms	63
Appendix C - References	64
Appendix D - Feedback	64

Scope

In Scope

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

- Cisco Secure VPN (formerly known as AnyConnect Mobility Client)
- Secure connection using remote access VPN termination on Cisco hardware appliances
 - Secure Firewall (Firepower Threat Defense on Firepower 4100)
- Authentication
 - LDAP
 - Duo (Two-factor authentication)
- Threat Protection
 - Cisco Umbrella Roaming Security Module
 - Cisco Secure Endpoint (AMP) Enabler (formerly AMP for Endpoints)

Out of scope

This document does not cover the following topics:

- Firepower Threat Defense (FTD) Installation
- Firepower Management Console (FMC) Installation
- Identity Services Engine (ISE)
- Windows Server setup
- Initial Duo installation
- VPNless access to private applications (Duo Network Gateway)
- Policy Enforcement in Cisco Umbrella
- Cisco Meraki MX
- Cisco Adaptive Security Appliance (ASA)

Introduction

Today's distributed workforce continues to grow, and new challenges arise for businesses of all sizes. The need to have secure remote workers access cloud, private data centers, and public internet resources is even more important now than it has been in the past. While the benefits of these resources are immense, so are the risks that come with using them.

The IT teams need to be able to trust that their users can access all these resources with minimal interactions, while being as secure as possible. To do this, we need to protect the endpoints users will be on, the connection from these devices, validate their identity, and protect data from threats.

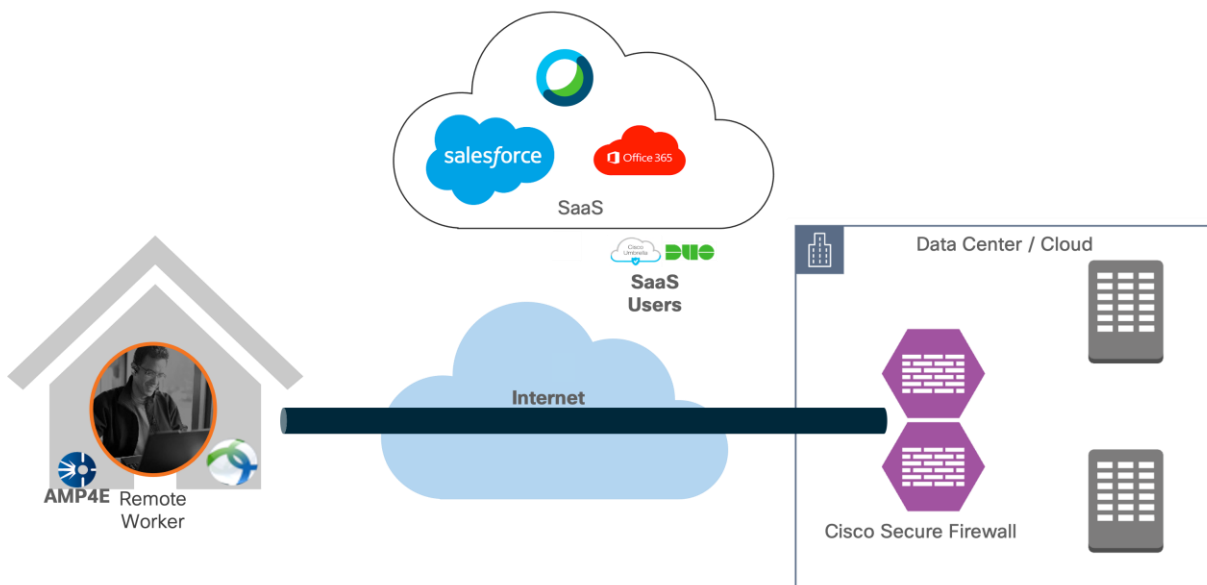


Figure 1. Cisco Remote Access VPN on premises with Cisco Secure Firewall

Secure Remote Worker Architecture

Remote workers access enterprise resources using Internet connections protected by remote access VPN (RAVPN). 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.

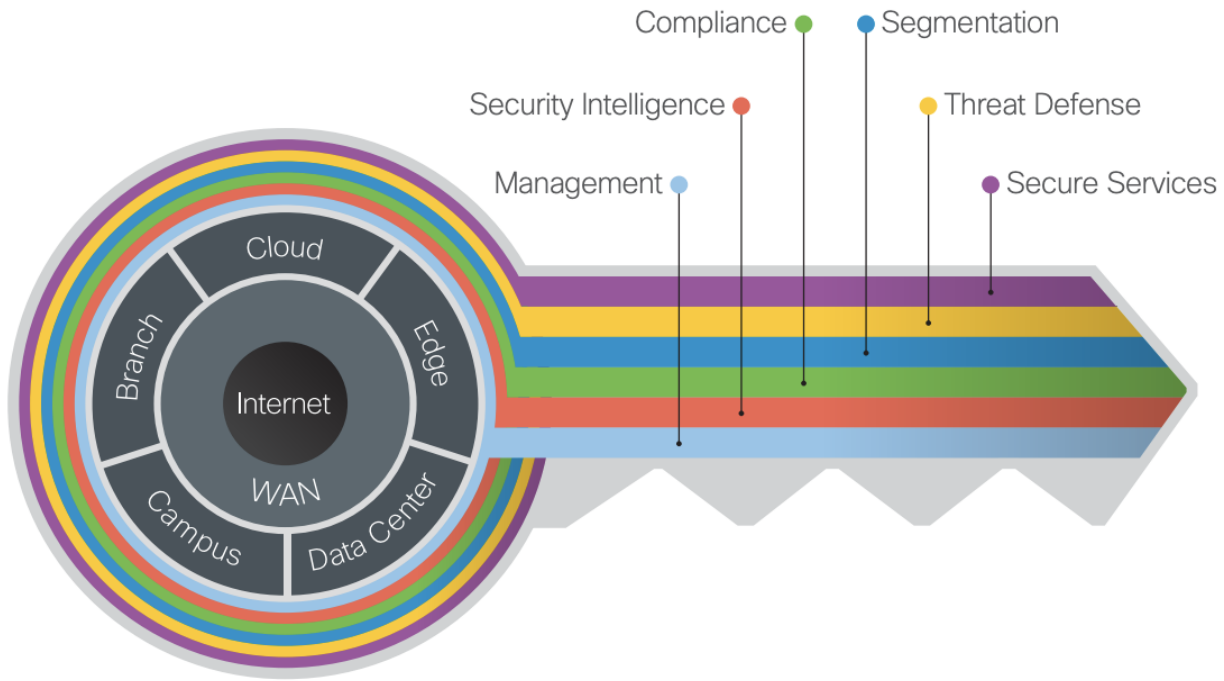


Figure 2. Key to SAFE organizes the complexity of holistic security into PINs & Secure Domain

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.

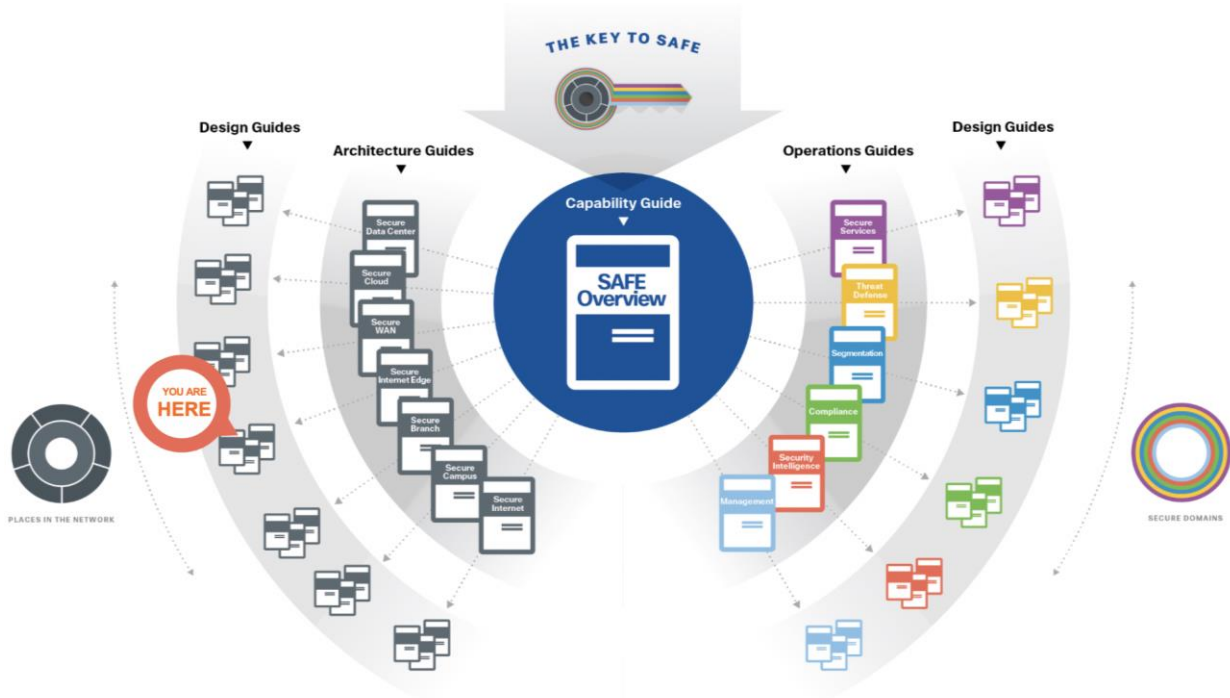


Figure 3. SAFE Architecture and Design Guides

More information about how Cisco SAFE simplifies security, along with other CVDs, can be found [here](#).

Secure Remote Worker Business Flows

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. The Secure Remote Worker design guide focuses on remote users accessing applications hosted in a secured environment. There is a secondary focus on securing the user when accessing internet resources, however, more in depth details are explored in the [Cisco Secure Access Service Edge \(SASE\) Design Guide](#).

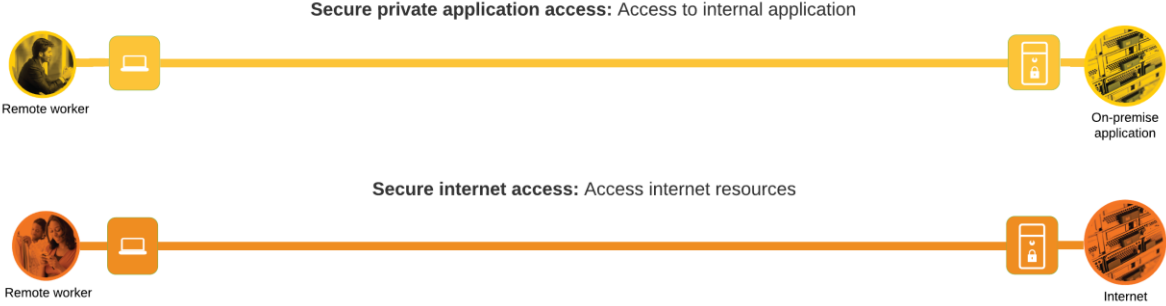


Figure 4. Remote Access VPN Business Flows

Threat Capabilities: Not all business flows have the same requirements. Some use cases are subject to a smaller attack vector and therefore require less security. Some have multiple vectors and require more.

Evaluating the business flow by analyzing the attack surfaces provides the information needed to determine and apply the correct capabilities for flow specific and effective security. This process also allows for the application of capabilities to address risk and administrative policy requirements. For more information regarding SAFE capabilities, refer to the [SAFE Overview Guide](#).

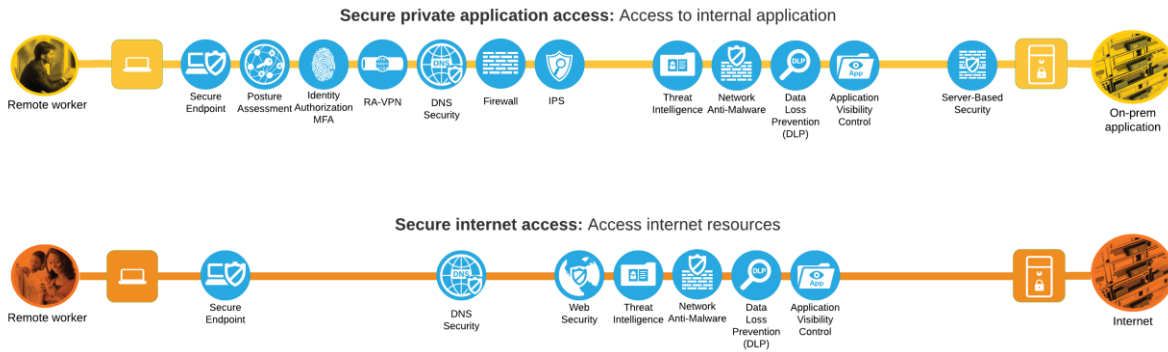


Figure 5. Threat Capabilities for business flows

Solution Overview

Today’s companies are investing in enabling their workforce to have a secure remote connection to the resources hosted in their private data centers. 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 Secure VPN, Cisco Secure Firewall, Cisco Secure Access by Duo, Cisco Umbrella, and Cisco Secure Endpoint.

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.

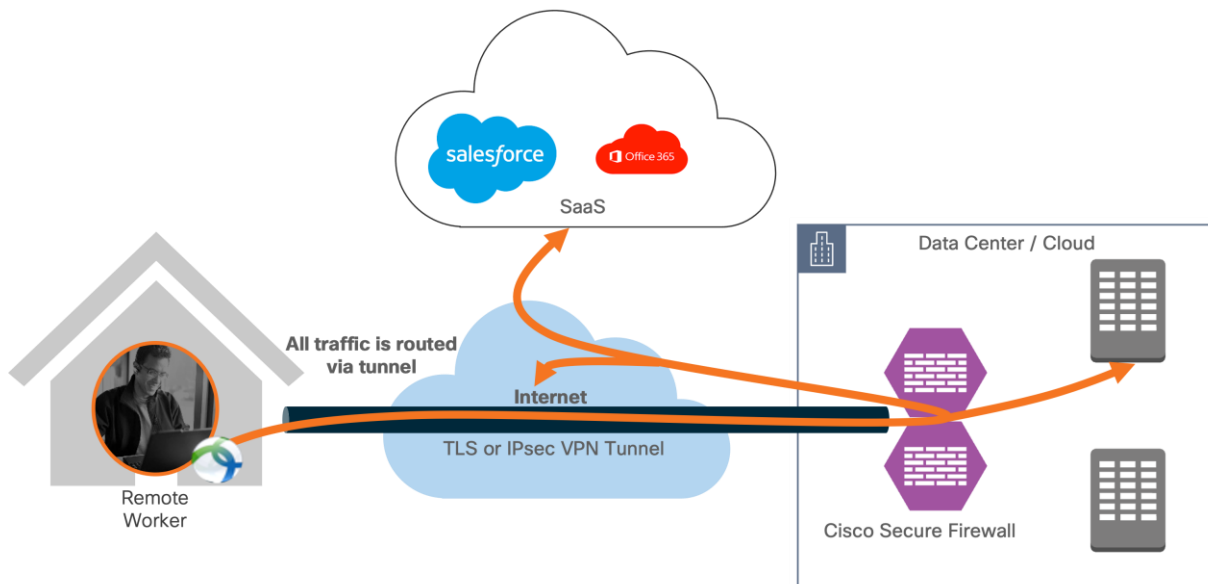


Figure 6. Remote employee accessing resources hosted in the data center (tunnel-all)

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.

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.

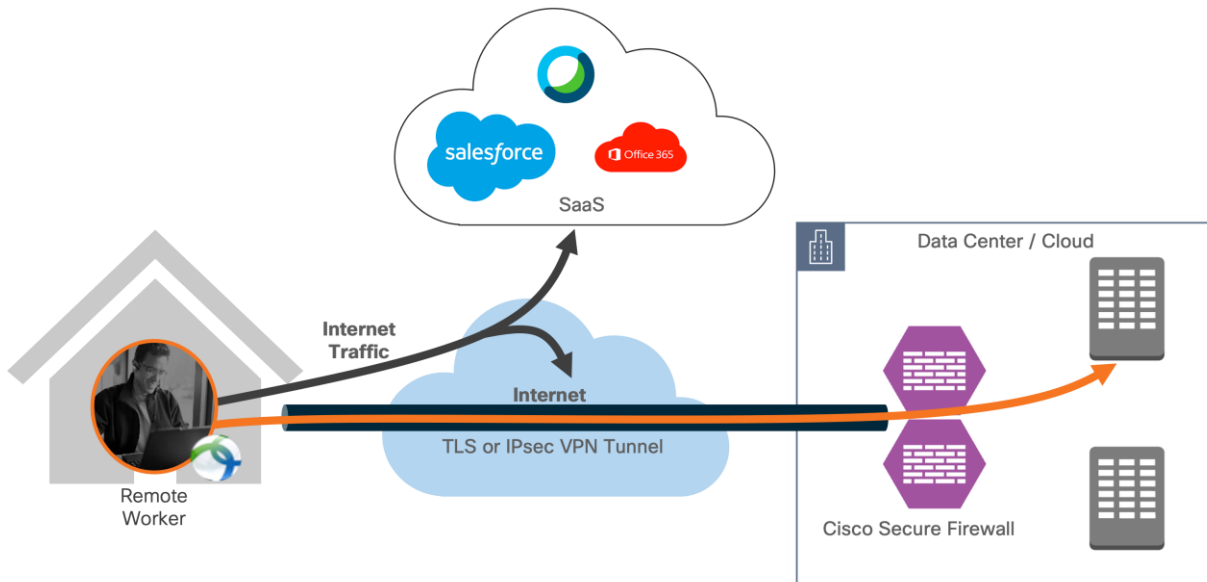


Figure 7. Traffic destined for private subnets/domains are sent through the VPN tunnel, other traffic goes direct to the Internet

VPN with a split tunnel

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

- Cisco Umbrella Roaming Module continues to provide cloud delivered security through Cisco Umbrella to traffic not destined for the VPN tunnel
- Cisco Secure Endpoint enabler continues to provide anti-virus and malware protection
- Cisco Secure Access by Duo continues to provide MFA for applications

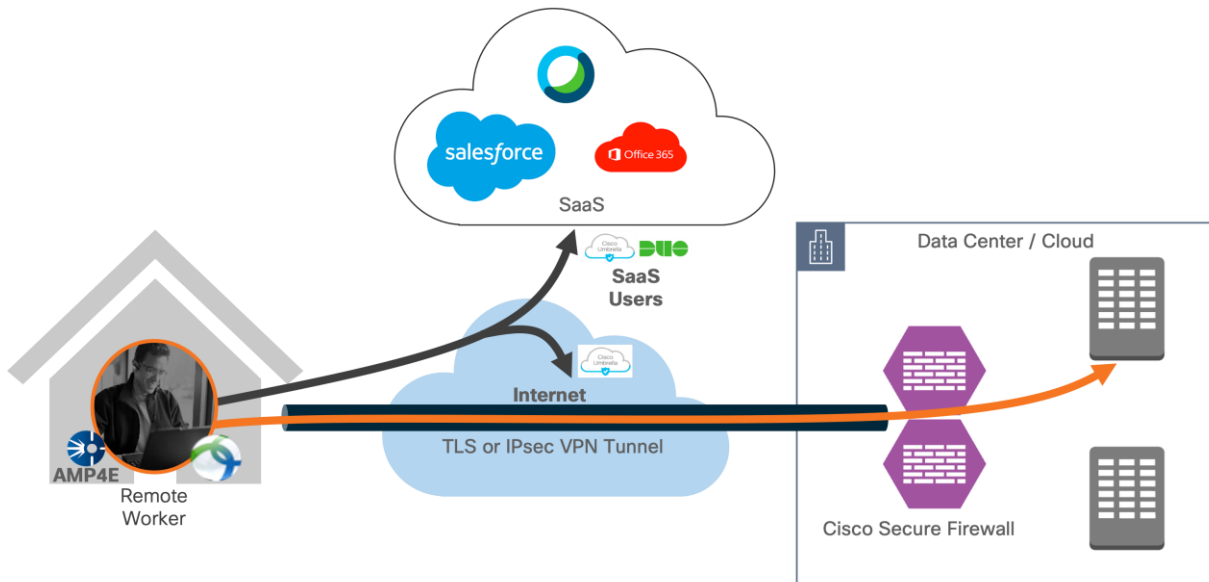


Figure 8. Remote worker is on VPN (split tunnel)

No VPN connection

Cisco Secure VPN modules provide protection when users are not on a VPN.

- Cisco Umbrella Roaming Module continues to provide cloud delivered security through Cisco Umbrella
- Cisco Secure Endpoint continues to provide anti-virus and malware protection
- Cisco Secure Access by Duo continues to provide MFA for applications

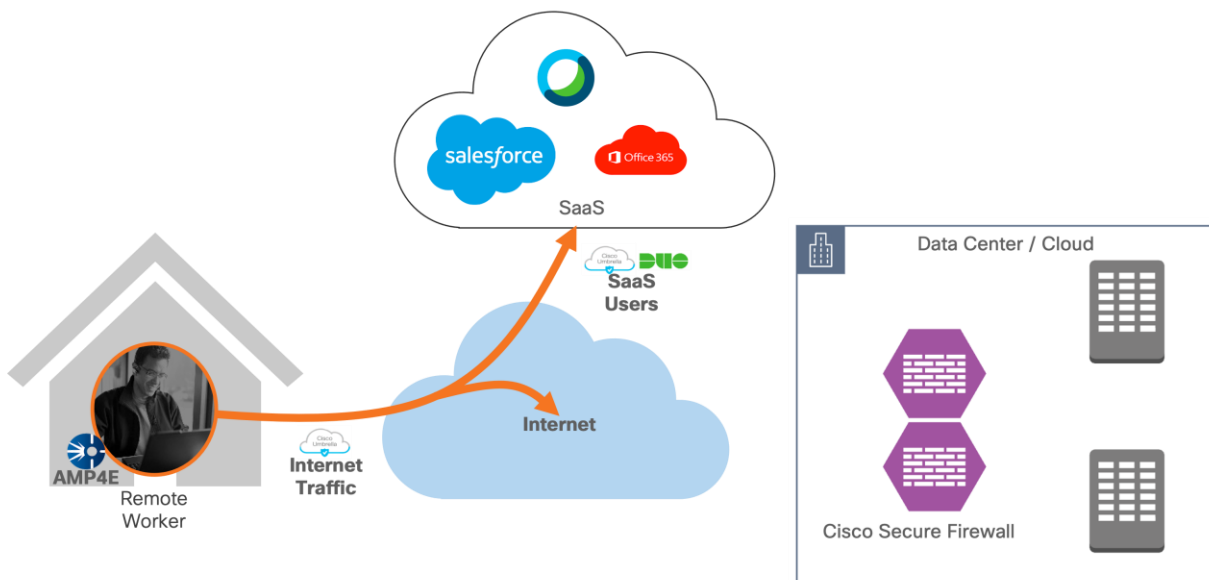


Figure 9. Remote worker is not connected to VPN

Target Audience

This document provides best practices and recommended solutions for remote workers accessing resources hosted in on-prem infrastructures. This solution brings together a secure architecture that includes Cisco Secure VPN Mobility Client, Cisco Secure Access by Duo, Cisco Umbrella, and Cisco Secure Endpoint to protect remote access workers even when the user is on an untrusted network. In addition to validated designs, this Cisco Validated Design (CVD) also provides recommended step-by-step configurations.

The target audience for this CVD are Solution Architects responsible for designing a secure environment for remote workers and the implementation team responsible for deploying security.

Product Overview

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

Devices / Modules	Functionality
Cisco Secure VPN Mobility Client	VPN Client for endpoints
Cisco Secure Firewall (FTD)	VPN Gateway / VPN concentrator
Cisco Secure Access by Duo	Multi-factor authentication
Cisco Umbrella Roaming Security Module	Cloud delivered security
Cisco Secure Endpoint Enabler	Anti-Virus and Malware protection for endpoints

Cisco Secure Access by Duo

Cisco Secure Access by Duo is a user-friendly, scalable way to keep business ahead of ever-changing security threats by implementing part of 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. 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 administration, visibility, and monitoring.

Cisco Secure Access by Duo integrates with Cisco FTD VPN to add two-factor authentication for Secure VPN logins. Duo supports two-factor authentication for FTD using RADIUS authentication. With this configuration, end-users receive an automatic push or phone call for multi-factor authentication after submitting their primary credentials using the Secure VPN Mobility Client. Users may append a different factor selection to their password entry.

Cisco Secure VPN (formerly AnyConnect Secure Mobility Client)

Cisco Secure VPN 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.

Note: Strong encryption license is required in smart account

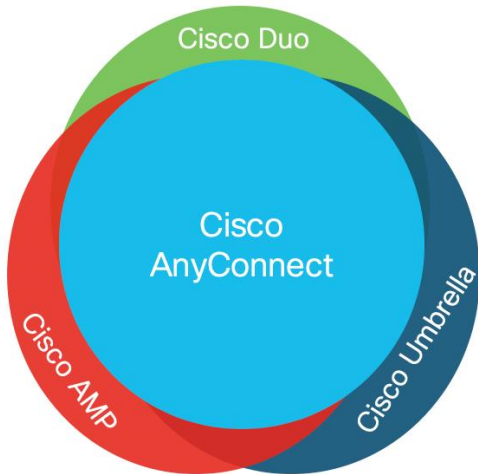


Figure 10. Components of the Cisco Secure VPN Client

Cisco Umbrella Roaming Security Module

Cisco Umbrella Roaming Security module for Cisco Secure VPN provides always-on security on any network, anywhere, any time. The Roaming Security module enforces security through Umbrella’s Secure Internet Gateway (SIG). Cisco Umbrella SIG unifies multiple functions in a single solution that traditionally required a set of on-premises security appliances (firewalls, proxies, gateways) or single function cloud-based security solutions. Umbrella provides real-time visibility and control for all internet activity both on and off your network or VPN.

License requirement to enable Umbrella Roaming Security Module:

License	Functionality
Cisco Umbrella Roaming service	Enable Umbrella connectivity to roaming clients

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

[Cisco Umbrella Packages](#)

Cisco Secure Endpoint (AMP) Enabler

Cisco Secure VPN AMP Enabler module is used as a medium for deploying Cisco Secure Endpoint, formerly Advanced Malware Protection (AMP). This approach provides the roaming workforce with an additional security agent that acts as an anti-virus and malware protection system. It detects potential malware threats, removes those threats, and protects the devices from compromise. Cisco Secure Endpoint protects the user both on and off the network or VPN.

[Secure Endpoint License Comparison](#)

Product	License
Cisco Secure Endpoint license	Essential, Advantage or Premier

Cisco Secure Firewall

The Cisco Secure Firewall running Firepower Threat Defense (FTD) helps you prevent breaches, get visibility to stop threats fast, and automate operations to save time. A next-generation firewall 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. Cisco FTD is available on hardware and as a virtual appliance.

Cisco FTD 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

This design guide makes use of Cisco FMC to configure the firewalls.

Note: Licensing requirements for RAVPN can be found in Appendix A. The FTDs in this environment use AnyConnect Plus licenses.

Security Integrations

Each product in the Cisco product portfolio has a unique role to play when deploying an RAVPN solution. A key component of this deployment guide is to provide guidance on the integration of these products into a cohesive security solution. In this guide:

- Cisco FTDs are configured to accept VPN connections from Cisco Secure VPN clients
- Cisco Secure Access by Duo is installed to validate the identity of connections from Cisco Secure VPN clients
- Upon successful connection to the VPN, the Cisco Umbrella Roaming Security module is delivered to the clients for cloud security protection when not using the VPN tunnel
- Upon successful connection to the VPN, the Cisco Secure Endpoint package is delivered to the clients for anti-virus and malware protection

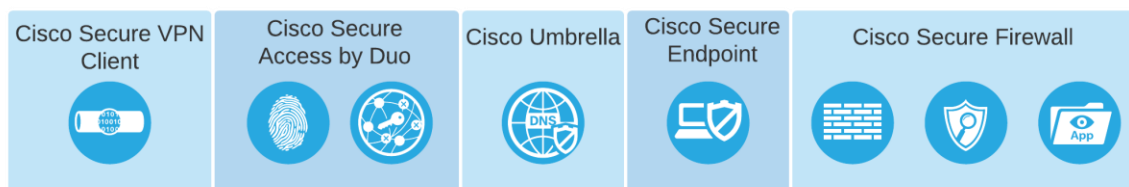


Figure 11. Cisco Security Integration for Secure Remote Worker

Note: Cisco Secure Access by Duo, Umbrella, and Secure Endpoint offer EU (European Union) based locations for customers having to follow EU rules.

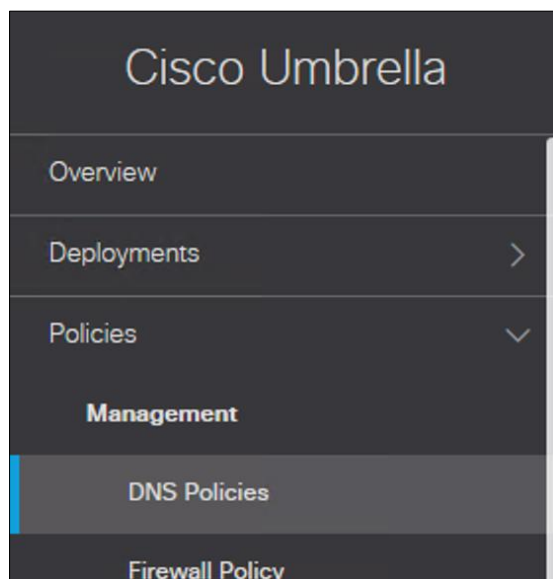
Policy Setup for Secure VPN Client Modules

Before doing the Remote Worker deployment steps, the policies for the VPN modules need to be set up first. This will reduce the number of steps in the deployment section and remove unnecessary overhead during that process.

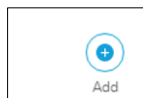
Umbrella

This policy will be applied to any remote workers that are roaming. For this guide, only Umbrella DNS will be used. For a more in-depth Umbrella solution, including Web security, Data Loss Prevention and Remote Browser Isolation see the Cisco Umbrella Security Policy details [here](#).

Step 1. Go to **Policies** -> **Management** -> **DNS Policies**



Step 2. Add a new policy on the top right



Step 3. Leave everything as the default and click **next**

How would you like to be protected?

Choose which type of access control or threats to block. Your selection will determine what features are available to the policy, what level of visibility is provided in your reports, and should match how Umbrella is deployed in your environment. For more information, click [here](#).

Select Your Protection:

- Access Control**
Restrict access with broad category based blocking and/or surgical block and allow destination lists.
 - Content Category Blocking**
Block access to destinations based on content category.
 - Apply Destination Lists**
Create or modify lists to explicitly block or allow destinations. Note: global block and global allow destination lists are applied by default.
 - Application Control**
Block or allow access to applications individually or by group.

- Block Threats**
Secure your network and endpoints using a variety of antimalware engines and threat intelligence.
 - Security Category Blocking**
Ensure domains are blocked when they host malware, command and control, phishing, and more.
 - File Analysis**
Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).
 - IP-Layer Enforcement**
Block threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for roaming computer identities.

[▶ Advanced Settings](#)

CANCEL

NEXT

Note: For more information on Umbrella best practices for policy creation, go [here](#).

Step 4. Add roaming computers to the policy and click **next**

What would you like to protect?

Select Identities

Search Identities

All Identities

- G Suite OUs
- G Suite Users
- Mobile Devices
- Network Devices 2 >
- Networks 3 >
- Roaming Computers 5 >
- Sites 5 >
- Tags 1 >

5 Selected REMOVE ALL

- Roaming Computers 5

CANCEL
PREVIOUS
NEXT

Note: For more information on Umbrella Policy precedence, go [here](#).

Step 5. Leave the next page with all the defaults and click **next**

Security Settings









Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

Select Setting

Default Settings ▾

Categories To Block

EDIT

-  Malware
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.
-  Newly Seen Domains
Domains that have become active very recently. These are often used in new attacks.
-  Command and Control Callbacks
Prevent compromised devices from communicating with attackers' infrastructure.
-  Phishing Attacks
Fraudulent websites that aim to trick users into handing over personal or financial information.
-  Dynamic DNS
Block sites that are hosting dynamic DNS content.
-  Potentially Harmful Domains
Domains that exhibit suspicious behavior and may be part of an attack.
-  DNS Tunneling VPN
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
-  Cryptomining
Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

▶ INTEGRATIONS

CANCEL

PREVIOUS

NEXT

Note: For more information on Umbrella Security Categories, go [here](#).

Step 6. Change the **Content Access** to **Moderate** and click **next**

Limit Content Access

Select content categories to block identity access to websites that serve content of that type. Select a preset level of control or add a custom setting. For more information, see For more information about categories, [Umbrella's Help](#).

High
Blocks adult, illegal activity, social networking, and file sharing websites.

Moderate
Blocks adult and illegal activity websites.

Low
Blocks pornography, tasteless, and proxy websites.

Custom
Blocks manually selected content categories.

Categories - Moderate

These are the categories we will block. Note: if you want to make changes create a custom setting

Adware	Alcohol
Dating	Illegal Drugs
Gambling	Child Abuse Content
Hate Speech	Internet Watch Foundation
Lingerie and Swimsuits	Non-sexual Nudity
Pornography	Filter Avoidance
Sexuality	Extreme
Terrorism	Weapons

CANCEL

PREVIOUS

NEXT

Note: For more information on managing Umbrella Content categories go [here](#).

Step 7. The **Control Applications** section can be left as is, click on **next**

Control Applications
Select applications or application categories you'd like to block or allow for the users in your organization

Application Settings

Default Settings ▾

Applications To Control

Search for an application

- > Ad Publishing
- > Anonymizer
- > Application Development and Testing
- > Backup & Recovery
- > Business Intelligence
- > Cloud Carrier
- ▾ Cloud Storage

CANCEL PREVIOUS NEXT

Note: For more information on Umbrella Application categories, go [here](#).

Step 8. Apply a Destination List to your roaming users. For this design guide, the destination list has been left as default. Click **next**

Apply Destination Lists [ADD NEW LIST](#)

Search for and apply the appropriate block or allow Destination Lists for this policy. Click Add New List to create a Destination List.

Q Search...

Select All Showing: All Lists ▾ 4 Total

All Destination Lists

<input type="checkbox"/>	4shared	1 >
<input checked="" type="checkbox"/>	Global Allow List	1 >
<input checked="" type="checkbox"/>	Global Block List	0 >
<input type="checkbox"/>	vpn	1 >

1 Allow Lists Applied

<input checked="" type="checkbox"/>	Global Allow List	1
-------------------------------------	-------------------	---

1 Block Lists Applied

<input checked="" type="checkbox"/>	Global Block List	0
-------------------------------------	-------------------	---

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

Note: For more information on managing Umbrella Destination Lists, go [here](#).

Step 9. **File Analysis** in Umbrella is out of scope for this design guide and therefore is disabled. Click **next**

File Analysis

Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

File Inspection
Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

Note: For more information on Umbrella File analysis, go [here](#).

Step 10. Leave the block page as the default

Set Block Page Settings
 Define the appearance and bypass options for your block pages.

Use Umbrella's Default Appearance
[Preview Block Page »](#)

Use a Custom Appearance

› **BYPASS USERS** _____

› **BYPASS CODES** _____

Note: For more information on Umbrella Block pages, go [here](#).

Step 11. On the policy summary page, give the policy a meaningful name and click on **Save**

Policy Summary

Policy Name

Secure Endpoint

A Secure Endpoint group needs to be created for an AnyConnect module to be created. These steps go over creating that group.

Step 1. Go to **Management -> Groups**

Secure Endpoint Premier

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

Groups

Quick Start
 Computers
Groups

Search

Step 2. Click on create group on the right side

[View All Changes](#)

Step 3. Give the new group a meaningful name and leave everything as the default, then **Save**

New Group

Name	<input type="text" value="remoteWorkers"/>
Description	<input type="text"/>
Parent Group	<input type="text" value=""/>
Windows Policy	<input type="text" value="Default Policy (Protect Policy)"/>
Android Policy	<input type="text" value="Default Policy (Default FireAMP Android)"/>
Mac Policy	<input type="text" value="Default Policy (Audit Policy for FireAMP M)"/>
Linux Policy	<input type="text" value="Default Policy (Audit Policy for FireAMP L)"/>
Network Policy	<input type="text" value="Default Policy (Default Network)"/>
iOS Policy	<input type="text" value="Default Policy (Audit)"/>

Cancel

Save

Remote Worker Deployment

Version Information

Product	Version
Cisco Firepower Threat Defense	7.0
Cisco Secure VPN	4.10.03
Cisco Umbrella	N/A
Cisco Secure Endpoint Connector	7.2.11
Cisco Secure Access by Duo	N/A

Network Topology

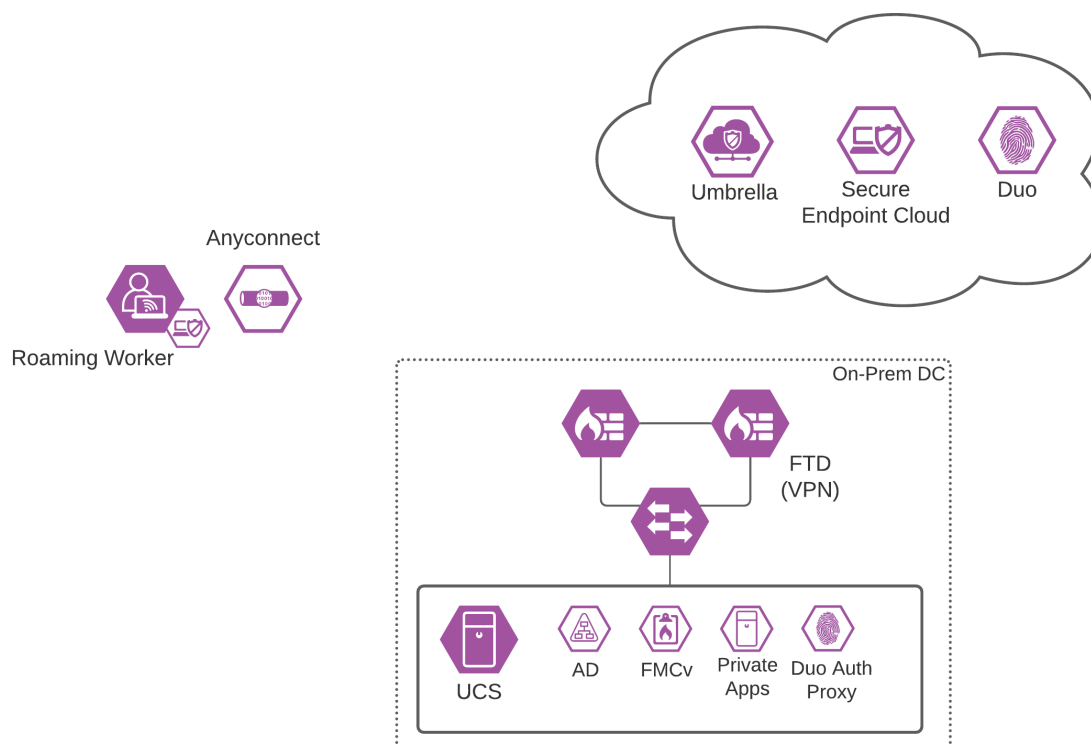


Figure 12. Cisco Remote Access VPN On-Prem Architecture

Cisco Firepower Threat Defense

The deployment steps in this design guide assume that the FTD devices are managed by FMC, have been deployed as a High Availability Pair and are accessible over the WAN network. For installation and deployment guides:

[Firewall Management Center Virtual Getting Started Guide](#)

[Cisco Firepower 4100 Getting Started Guide](#)

[Cisco Firepower Split Tunneling Configuration](#)

[High Availability for Firepower Threat Defense](#)

Note: This design guide uses the Firepower 4110 for testing and validation. The version needed for your environment may change depending on access requirements. For performance information see the [Cisco Firepower 4100 Series Data Sheet](#).

Once they have been installed, the interfaces, routing, NAT (Network Address Translation), and policy can be applied to the devices.

Interfaces

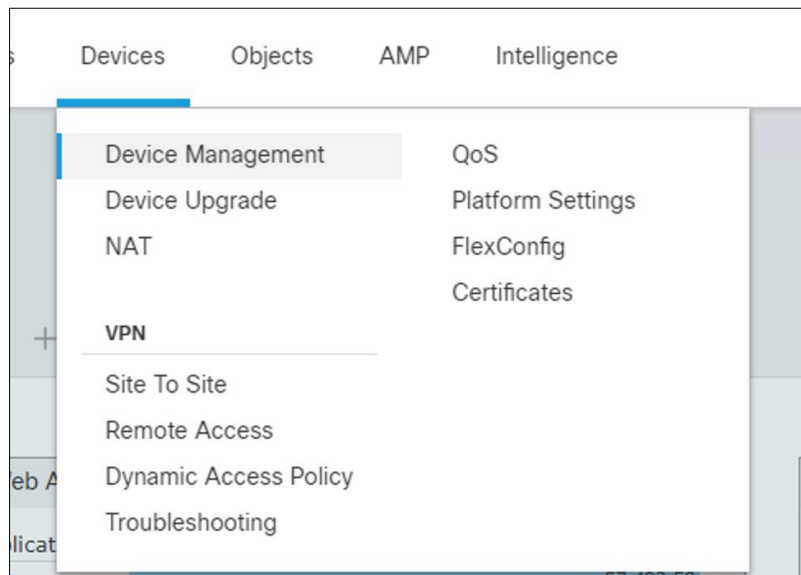
Typically, a minimum of two interfaces must be configured to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organizations network(s). For this design guide, the *outside* interface is used as the

ingress interface for VPN connections and the *inside* interface is used to denote the link to the rest of the network.

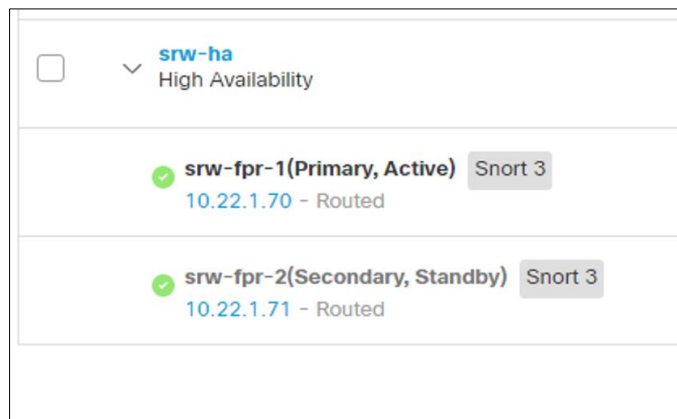
For more information on the configuration of Interfaces in Firewall Management Center go [here](#).

Outside Interface

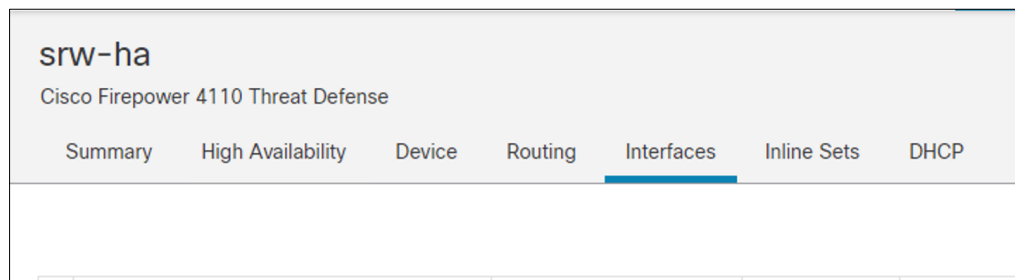
Step 1. Go to **Devices** -> **Device Management** in the FMC



Step 2. Click on the FTD or HA (High Availability) pair name



Step 3. Go to the **Interfaces** tab



Step 4. **Edit** the interface that is going to the outside using the pencil icon on the right side. In this case it is port-channel1.

Step 5. Give it a meaningful name. This guide uses **outside**.

Edit Ether Channel Interface

General IPv4 IPv6 Advanced

Name:
outside

Enabled

Step 6. In the **security zone** section, open the dropdown and create a new zone

Step 7. Give it a meaningful name. This guide uses **outside**. Click **OK**. This will create a new zone.

New Security Zone

Enter a name...
outside

Cancel OK

Step 8. Verify that the new zone was created and is filled in on the dropdown

Security Zone:
outside

MTU:

Step 9. Go to the **IPv4** tab

Edit Ether Channel Interface

General IPv4 IPv6 Advanced

IP Type:
Use Static IP

IP Address:

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Step 10. Fill in the publicly addressable IP address for your company with a netmask of 255.255.255.254.

Edit Ether Channel Interface

General **IPv4** IPv6 Advanced

IP Type:
Use Static IP ▼

IP Address:

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Step 11. Click **OK**. Verify the interface information is on the device interface page.

Port-channel1 outside EtherChannel outside /255.255.255.224(Static) Global

Step 12. Click on **Save** on the top right to save this configuration

You have unsaved changes **Save** **Cancel**

Inside Interface

Step 1. For the inside interface, repeat the same steps taken for the outside interface.

Edit Ether Channel Interface

General **IPv4** IPv6 Advanced

Name:

Enabled
 Management Only

Description:

Mode:
 ▼

Security Zone:
 ▼

MTU:

(64 - 9184)

Propagate Security Group Tag:

Ether Channel ID *:

Step 2. Set the internal IP address to be the gateway for all the internal IPs.

Edit Ether Channel Interface

General **IPv4** IPv6 Advanced

IP Type:
Use Static IP

IP Address:
10.3.1.10/255.255.255.0
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Step 3. Click **Ok**, verify the information is in the interfaces tab and then **save** the configuration on the top right.

Routing

Cisco FTD supports several Internet protocols for routing:

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP)
- Border Gateway Protocol (BGP)

This design guide was validated using static routing, however, more details on setting up dynamic routing on Firewall Management Center can be found [here](#).

Step 1. Go to **Devices** -> **Device Management** in the FMC

Devices **Objects** AMP Intelligence

Device Management QoS
Device Upgrade Platform Settings
NAT FlexConfig
Certificates

VPN

Site To Site
Remote Access
Dynamic Access Policy
Troubleshooting

Step 2. Click on the FTD or HA pair name

srw-ha
 High Availability

srw-fpr-1(Primary, Active) Snort 3
 10.22.1.70 - Routed

srw-fpr-2(Secondary, Standby) Snort 3
 10.22.1.71 - Routed

Step 3. Go to the **Routing** tab then to the **Static Route** section

srw-ha
 Cisco Firepower 4110 Threat Defense

Summary High Availability Device **Routing** Interfaces Inline Sets DHCP

Manage Virtual Routers
 Global

- Virtual Router Properties
- OSPF
- OSPFv3
- RIP
- BGP
 - IPv4
 - IPv6
 - Static Route**
- Multicast Routing
 - IGMP

Network ▲	Interface	Leak Route
▼ IPv4 Routes		
▼ IPv6 Routes		

Step 4. Click on **Add Route**

Step 5. Select the outside interface, then create a new **Available Network**

Step 6. Give it a meaningful name, this guide will use **internet**, change the network radio button to **Network**, fill in 0.0.0.0/0 and **Save**

New Network Object

Name
internet

Description

Network
 Host Range Network FQDN

0.0.0.0/0

Allow Overrides

Cancel Save

Step 7. Add the network that was created to the **Selected Network** section using the **Add** button

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network

Search

- any-ipv4
- ESXi-VLAN200
- ESXi-VLAN201
- InsideGateway
- internet**
- InternetGateway

Add

Selected Network

- internet

Step 8. Create a new gateway by pressing the plus (+) symbol

Step 9. Give it a meaningful name. This guide uses **internetGw**. Fill in the host box with the outside interfaces next hop and click **Save**

New Network Object ?

Name

Description

Network
 Host Range Network FQDN

Allow Overrides

Step 10. Verify the information is in the static route page and **save** the config on the top right of FMC

internet	outside	Global	internetGw	false	1	
----------	---------	--------	------------	-------	---	--

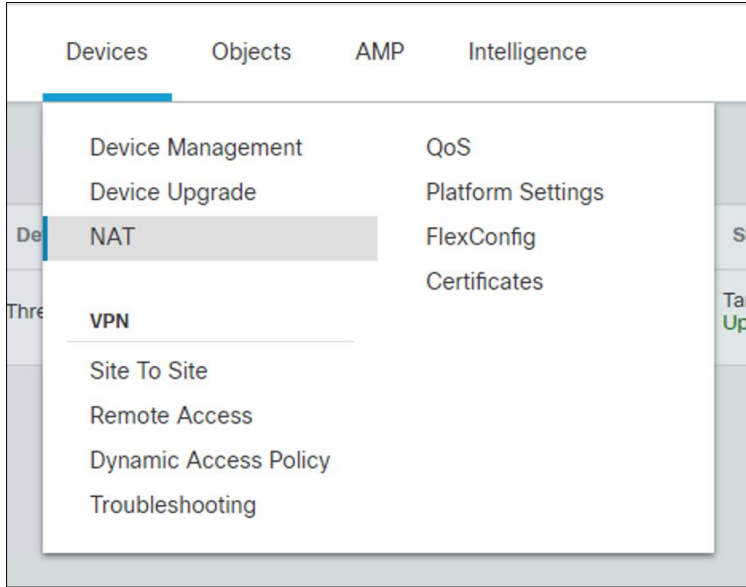
NAT

For this design guide, it is assumed that the Cisco FTD pair used for VPN access is also being used as the Internet Edge for the network. To facilitate this, NAT must be deployed for all internal traffic to reach the Internet. This will be used for application updates, on-site workers, FMC, and any other needs of different applications that may need the Internet.

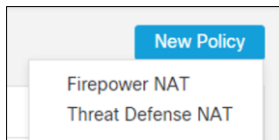
Note: If the Internet edge is located in another part of the network, skip this step, and create a route between the VPN firewall and the edge router(s).

For additional information on NAT go [here](#).

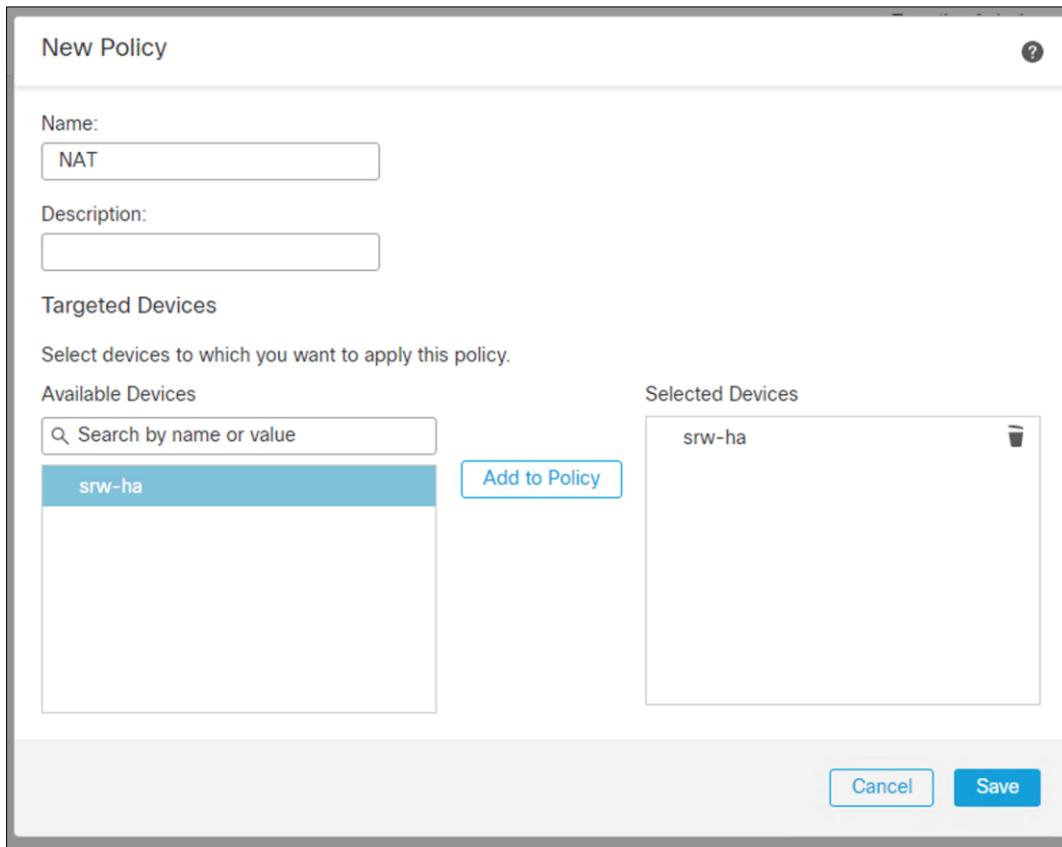
Step 1. Go to **Devices** -> **NAT**



Step 2. Create a new policy using the **Threat Defense NAT** option

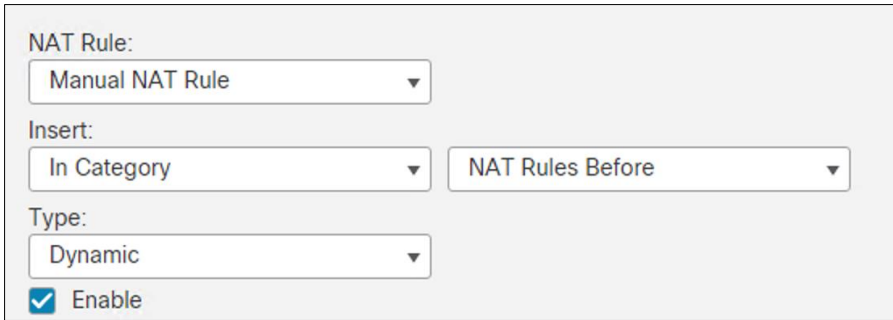


Step 3. Add a meaningful **Name** to the policy, **Add** the FTD device to the **Selected Devices** section, and click **Save**



Step 4. Edit the new NAT policy using the pencil icon and create a new rule on the right side

Step 5. Make the NAT rule a **Manual NAT Rule** with a Type **Dynamic**



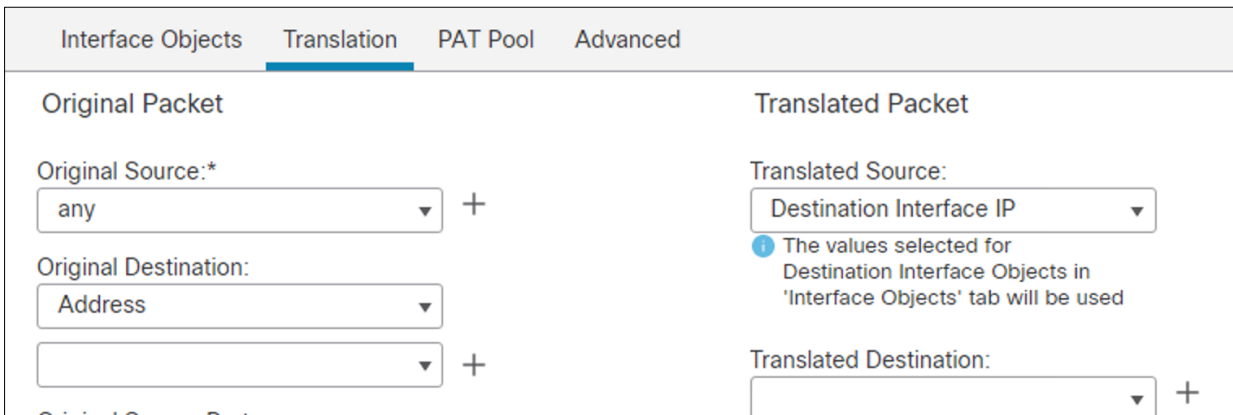
NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Dynamic

Enable

Step 6. In the **Translation** tab, change the **Original Source** to **any**, **Original Destination** to **Address** and **Translated Source** to **Destination Interface IP**



Interface Objects Translation PAT Pool Advanced

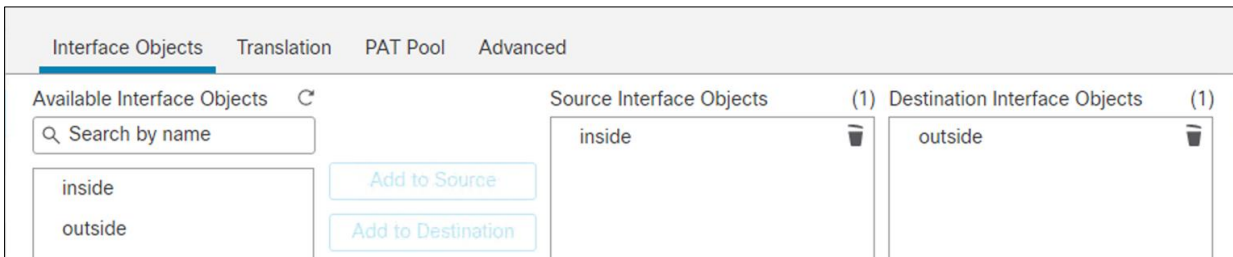
Original Packet Translated Packet

Original Source:* any + Translated Source: Destination Interface IP

Original Destination: Address + Translated Destination: +

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Step 7. In the **Interface Objects** tab, add **inside** to **Source Interface Objects** and **outside** to the **Destination Interface Objects**, then **Save**



Interface Objects Translation PAT Pool Advanced

Available Interface Objects Search by name

Source Interface Objects (1) Destination Interface Objects (1)

inside outside

Add to Source Add to Destination

Step 8. Verify the rule is in the rule list and click **Save** on the top right



NAT Rules Before

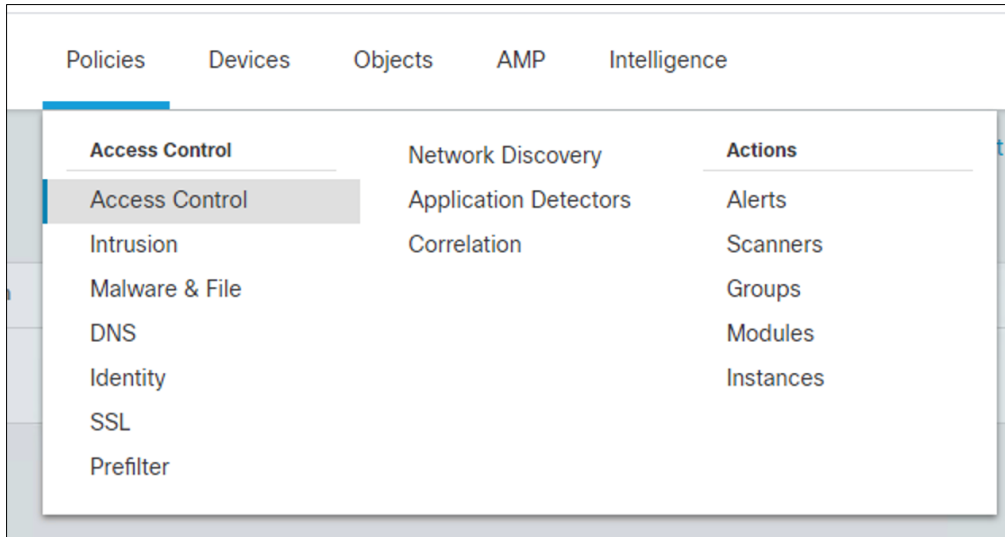
ID	Name	Type	Original Source	Original Destination	Translated Source	Translated Destination	Enabled
1	Dy...	Interface	inside	outside	any		<input checked="" type="checkbox"/>

Policy

If you created a basic Block all traffic access control policy when you registered the FTD with the FMC, then you need to add rules to the policy to allow traffic through the device. If NAT was configured in the previous section, this procedure will show you how to create a rule that allows internal devices to communicate to the Internet, Policies to allow traffic from the VPN subnet to the internal network will be shown later in the document.

For more advanced security rules, see the [Firewall Management Center Configuration Guide](#).

Step 1. Go to **Policies -> Access Control**



Step 2. Create a new policy on the right and give it a meaningful name. Add the FTD device to the selected devices and click **Save**.

New Policy ?

Name:

Description:

Select Base Policy:

Default Action:

- Block all traffic
- Intrusion Prevention
- Network Discovery

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices:

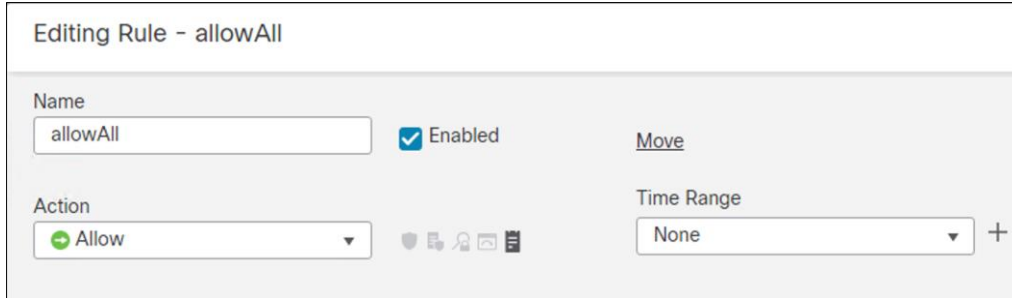
Selected Devices:

Step 3. Edit the new policy using the pencil icon and click **+ Add Rule**

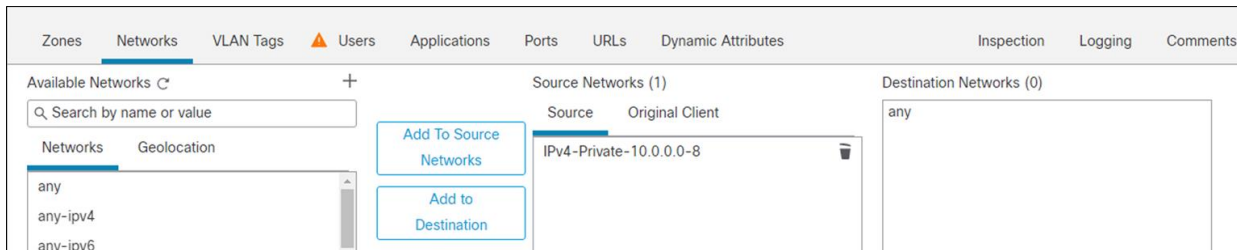
Default Prefilter Policy SSL Policy: None Identity Policy: None

Show Rule Conflicts ?

Step 4. Add a meaningful **Name** to the policy, with the action **Allow**



Step 5. On the Networks tab, **Add** your internal address scheme to the **Source Networks**. **Save** the rule

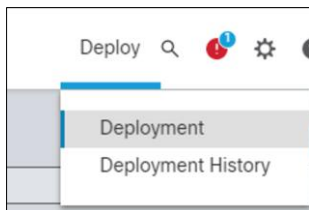


Step 6. Verify there are two rules, a default deny and an allow for all internal traffic to get out. **Save** this policy

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	
Mandatory - srw-acp (1-1)															
1	allowAll	Any	Any	IPv4-Private-1	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	
Default - srw-acp (2-2)															
2	defaultBlock	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block	

Deploy

Step 1. Go to **Deploy** -> **Deployment**



Step 2. Verify there is the FTD pending a deployment

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input type="checkbox"/> srw-ha	admin		FTD		Sep 22, 2021 4:53 PM		Pending

Step 3. Select the FTD and **deploy**

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> srw-ha	admin		FTD		Sep 22, 2021 4:53 PM		In Progress... (5%) Deployment has been initiated.

Step 4. FTD initial setup is finished once it has successfully deployed

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
> <input checked="" type="checkbox"/> srw-ha	admin		FTD		Sep 22, 2021 4:53 PM		Completed

Cisco Secure Access by Duo

To install the authentication proxy, please follow the [Cisco Firepower Threat Defense VPN with AnyConnect](#) document.

Auth Proxy

The auth proxy config should look like this:

```
[ad_client]
host=10.22.1.50
service_account_username=administrator
service_account_password=*****
search_dn=DC=srwlabs03,DC=com

[radius_server_auto]
ikey=DIxxxxxxxxxxxx
skkey=Dbxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-XXXXXXXXX.duosecurity.com
radius_ip_1=0.0.0.0/0
radius_secret_1=*****
failmode=safe
client=ad_client
port=1812
```

Directory Sync

So that we do not need to make a new user each time someone needs to login, we can make use of the Duo Directory Sync. This allows Duo to get the users and groups from the AD server using the authentication proxy. You can setup the Directory Sync using these [directions](#).

Note: Since the authentication proxy has already been installed, you can add a new cloud section to the configuration instead of installing a second authentication proxy.

The authentication proxy configuration file should now look like this:

```
[ad_client]
host=10.22.1.50
service_account_username=administrator
service_account_password=*****
search_dn=DC=srwlab03,DC=com

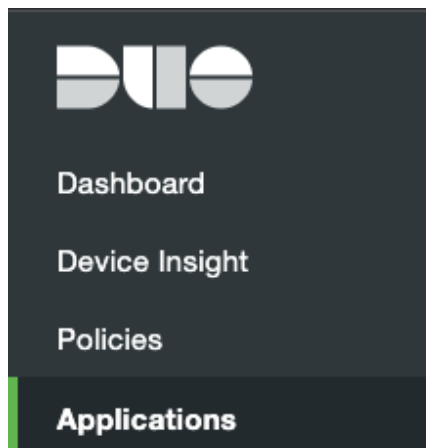
[radius_server_auto]
ikey=DIxxxxxxxxxxxxx
skey=Dbxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-XXXXXXXXX.duosecurity.com
radius_ip_1=0.0.0.0/0
radius_secret_1=*****
failmode=safe
client=ad_client
port=1812

[cloud]
ikey=DXXXXXXXXXXXXXXXXXXXXX
skey=iAXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXXX.duosecurity.com
service_account_username=administrator
service_account_password=*****
```

Duo Security Policy

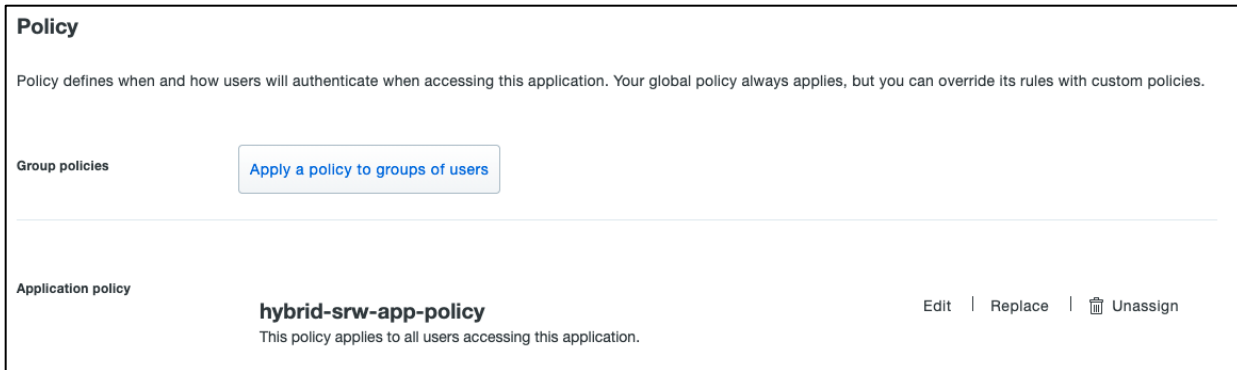
We will change the policy for the FTD VPN application was created in Duo so that it will only allow connections from specific IP addresses and block all others.

Step 1. In the Duo administration dashboard go to **Applications**



Step 2. Select the application that is used to protect VPN connection to the FTD

Step 3. Go to **Policy** and in the **Application Policy** section, click **edit**



Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies Apply a policy to groups of users

Application policy **hybrid-srw-app-policy** Edit | Replace | Unassign
This policy applies to all users accessing this application.

Step 4. Under **User Location**, click the search bar and choose the countries that will be enabled for VPN access. Next to **All other countries**, choose **Deny access**.



User location

Duo will do a country lookup on the host IP address and can apply actions based on the country.

+

Note: Access attempts from internal IPs (some applications don't report the user's IP) and unknown countries will default to "No action."

Step 5. Click **Save Policy**.

Cisco Secure VPN

Cisco Secure VPN allows employees to access a company's internal resources while remote and ensures those connections are secure.

The following deployment steps will cover:










- Downloading the Secure VPN files and adding them to FMC
- Navigating the Remote Access VPN wizard, including the integrations of Umbrella, Duo and Secure Endpoint.

File Download

Step 1. Download the Secure VPN (AnyConnect) files:
<https://software.cisco.com/download/home/286281283/type/282364313/release/4.10.03104>

Note: For this design guide the windows and mac headend files are used, however, download any others you may need for your specific needs.

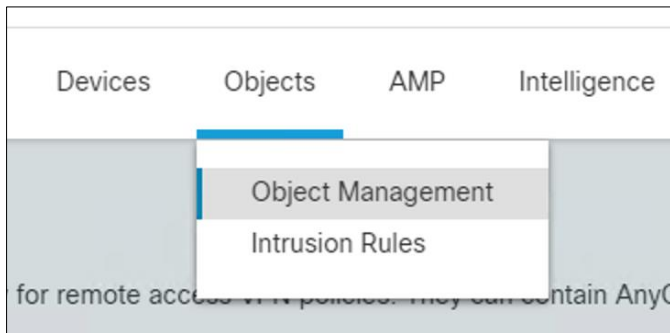
Step 2. Additionally, download the Profile Editor (Windows only) to make modifications to the Secure VPN package that will be attached to FMC.

AnyConnect Headend Deployment Package (Mac OS) anyconnect-macos-4.10.03104-webdeploy-k9.pkg Advisories	23-Sep-2021	83.55 MB	  
AnyConnect Headend Deployment Package (Windows) anyconnect-win-4.10.03104-webdeploy-k9.pkg Advisories	23-Sep-2021	76.47 MB	  
Profile Editor (Windows) tools-anyconnect-win-4.10.03104-profileeditor-k9.msi Advisories	23-Sep-2021	11.49 MB	  

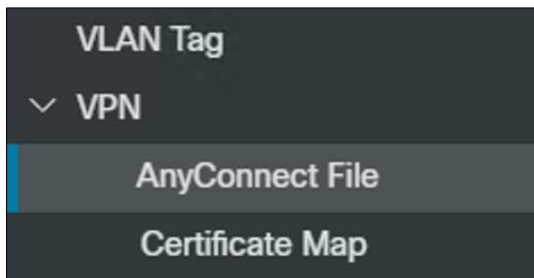
Step 3. Upload to

Upload Files to FMC

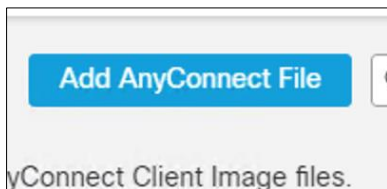
Step 1. Go to **Objects** -> **Object Management**



Step 2. Go to **VPN** -> **AnyConnect File**



Step 3. Click **Add AnyConnect File**



Step 4. Provide a meaningful **Name** to the file.

Step 5. Click **Browse** and add the windows headend file that was downloaded in the previous section.

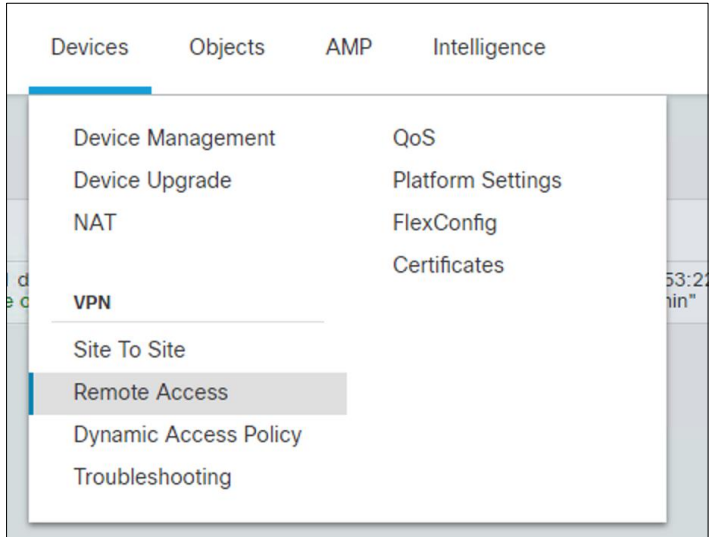
Step 6. Select **AnyConnect Client Image** as the file type.

Step 7. Click **Save**.

Step 8. Repeat as necessary for each of the operating systems that was downloaded.

Remote Access Policy Wizard

Step 1. Go to **Devices** -> **Remote Access**



Step 2. Click **Add** on the top right, bringing you to a RA VPN Wizard

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

Description:

Be
 Before
 elemer
 VPN P
 Authe
 Config
 or SSC
 AnyC

Step 3. Give the policy a meaningful name. Check the protocols you would like to use (this guide is using SSL) and add the FTD device to the **Selected Devices** section. Go to the next page

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Q Search"/> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px; background-color: #0070c0; color: white;">srw-ha</div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> srw-ha 🗑️ </div>

Step 4. In the **Connection Profile** make sure the authentication method is AAA Only, the authentication server is set to the Duo Authentication proxy that was created earlier.

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

i This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: ▼

Authentication Server:* ▼ +
(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: ▼ +
(Realm or RADIUS)

[Configure LDAP Attribute Map](#)

Step 5. In the **Client Address Assignment**, edit the IPv4 pool and add a new one

Add IPv4 Pool ?

Name*

IPv4 Address Range*

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Step 6. Give the address pool a meaningful name. Enter a network range and netmask to be assigned to your remote users. Click **Save**

Add IPv4 Pool

Name*

IPv4 Address Range*

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across

Step 7. Add the newly created pool to the **Selected IPv4 Pools** section. Click **Ok**

Address Pools

Available IPv4 Pools ↻ +

Selected IPv4 Pools

srw-pool 🗑


srw-pool Add


Step 8. Leave everything else as is and click **next**

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. selected, IP address assignment is tried in the order of AAA server, DHCP server and IP

Use AAA Server (Realm or RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to a connection is established. Select or create a Group Policy object.

Group Policy:* ▼ +

[Edit Group Policy](#)

Step 9. Select the AnyConnect images that were downloaded in the previous section. Click **Next**

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	mac-head	anyconnect-macos-4.10.01075-webdeploy...	Mac OS ▼
<input checked="" type="checkbox"/>	windows-head	anyconnect-win-4.10.01075-webdeploy-k9...	Windows ▼

Step 10. Set the network interface to outside

AAA

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* ▼ +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Step 11. In the **Device Certificates** section, add a new certificate

Note: Obtaining a certificate for the FTD, also known as PKI enrollment, is explained in [Firepower Threat Defense Certificate-Based Authentication](#). This chapter contains a full description of configuring, enrolling, and maintaining certificates in FMC.

Step 12. Give the certificate a meaningful **Name**. This design guide makes use of a PKCS12 File from Active Directory. Add the certificate option that best suits your network from the note above. Click **Save**

The screenshot shows the 'Add Cert Enrollment' dialog box. The 'Name*' field contains 'srwCA'. The 'Description' field is empty. The 'Enrollment Type' dropdown is set to 'PKCS12 File'. The 'PKCS12 File*' field contains 'keyStore.p12' and has a 'Browse PKCS12 File' button next to it. The 'Passphrase' field is empty. There is an unchecked checkbox labeled 'Skip Check for CA flag in basic constraints of the CA Certificate'. At the bottom right, there are 'Cancel' and 'Save' buttons. The dialog has tabs for 'CA Information', 'Certificate Parameters', 'Key', and 'Revocation', with 'CA Information' being the active tab.

Step 13. Click **Next**

AAA

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Step 14. Verify the information is correct on the last page and click **finish**

Split Tunneling

In this guide only traffic that is destined for our internal network will be sent down the VPN tunnel

Step 1. Go to **Devices -> Remote Access** and edit the VPN profile that was created in the previous section

Step 2. Edit the group policy and go to the **Split Tunneling** section

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Step 3. Change the IPv4 and IPv6 split tunneling dropdowns to **tunnel networks specified below**.

IPv4 Split Tunneling:
 Tunnel networks specified below ▼

IPv6 Split Tunneling:
 Tunnel networks specified below ▼

Split Tunnel Network List Type:
 Standard Access List Extended Access List

Standard Access List:
 [Empty dropdown menu] +

DNS Request Split Tunneling
 DNS Requests:
 Send DNS requests as per split tunneling ▼

Domain List:
 [Empty text area]

Step 4. Create a new **Standard Access List** by clicking on the plus sign

Step 5. Give it a meaningful name and click on the **Add** button.

New Standard Access List Object

Name

▼ Entries (0)

Add

Step 6. Leave it as an allow and add the subnet(s) for your internal network into the **Selected Network** box.

Add Standard Access List Entry ?

Action:

Network:

Available Network ↻ +

- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918
- IPv6-to-IPv4-Relay-Anycast
- mgmtGateway

Selected Network

IPv4-Private-10.0.0.0-8 🗑

Inline

Step 7. Click on **Add**, then **Save** the configuration

Step 8. The new ACL that was created should fill in the access list box

IPv4 Split Tunneling:

IPv6 Split Tunneling:

Split Tunnel Network List Type:
 Standard Access List Extended Access List

Standard Access List:
 +

DNS Request Split Tunneling

DNS Requests:

Domain List:

Step 9. Save the group policy, save the VPN profile, and save the policy.

Step 10. Go to **Policies** -> **Access Control** and edit the policy attached to the VPN FTD

Step 11. Create a new allow rule and give it a meaningful name

Name

allowVPNusers Enabled

Action

Allow

Step 12. Add the **outside** zone to the source zones and **inside** zone to the destination zones.

Source Zones (1)

outside

Destination Zones (1)

inside

Step 13. On the **Networks** tab, add the VPN address pool to the source networks and the internal net to destination address.

Source Networks (1)

Source	Original Client
srw-pool	

Destination Networks (1)

IPv4-Private-10.0.0.0-8

Enter an IP address

Enter an IP address

Step 14. Click **Save**

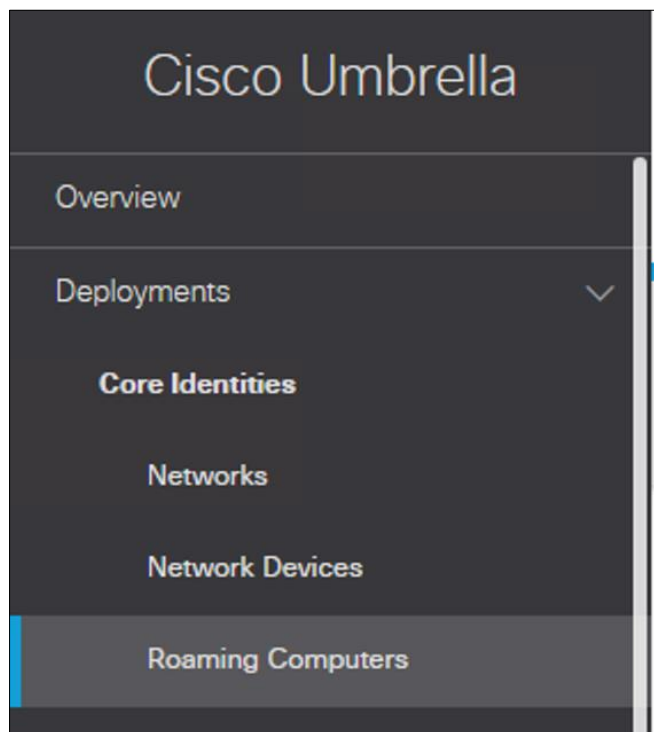
Cisco Umbrella Roaming Security module

The Cisco Umbrella Roaming Security module will be used to protect users while on or off the VPN

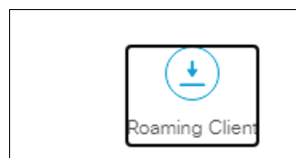
Download umbrella roaming security profile

Step 1. Login into your umbrella account at dashboard.umbrella.com

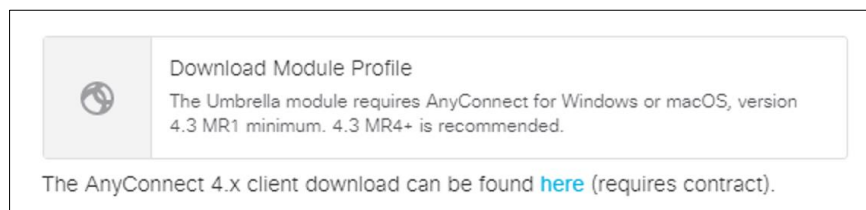
Step 2. Go to **Deployments** -> **Roaming Computers**



Step 3. Click on the **Roaming Client** download button



Step 4. Download the module profile at the bottom of the download window



Step 5. It should download as OrgInfo.json



Add profile to VPN profile

Step 6. On the FMC, go to **Devices** -> **Remote Access VPN** and edit the VPN policy created previously

Step 7. Edit the connection profile that was created in the previous steps, then edit the **Group Policy**

Firepower Management Center Overview

Devices / VPN / Edit Connection Profile

srwUsers

Connection Profile Access Interfaces Advanced

Name

DefaultWEBVPNGroup

srwUsers

Edit Group Policy

Name:*
DfltGrpPolicy

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:
Specify the VPN tunnel must be configured for

SSL

IPsec-IKEv2

Step 8. Go to the **AnyConnect** tab and then to **Client Modules**

General **AnyConnect** Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

Download optional client modules to the endpoint. AnyConnect client requests download from the FTD of only the modules that are configured here.

Client Module	Profile	Download	
No records to display			

+

Step 9. Click the **plus sign** to add a new module

Add Client Module ?

Client Module

▼ !

Profile to download

▼ +

Enable module download

Cancel Add

Step 10. Change the **Client Module** to **Umbrella Roaming Security**

Client Module

▼

Profile to download

Step 11. Then click on the **plus sign** to add a **new profile**

Add AnyConnect File ?

Name:*

File Name:*
 !

File Type:*
Umbrella Roaming Security Profile ▼

Description:

Step 12. Give it a meaningful name and browse to the OrgInfo.json file. Click **Save**

Add AnyConnect File ?

Name:*

File Name:*

File Type:*
Umbrella Roaming Security Profile ▼

Description:

Step 13. Make sure the profile is the new one that was created with the Umbrella orgInfo file and check the **Enable Module Download** box

Add Client Module ?

Client Module

Umbrella Roaming Security ▼

Profile to download

ac-umbrella-roam.json ▼ +

Enable module download

Cancel Add

Step 14. Click **Add**

Cisco Secure Endpoint Connector

Secure Endpoint connector will be used to secure the roaming client from malicious files and activity.

Download Connector

Step 1. Go to **Management** -> **Download Connector**

Secure Endpoint Premier

Dashboard Analysis ▼ Outbreak Control ▼ Management ▼ Accounts ▼

Download Connector

Group Select a Group ▼

Windows

Flash Scan

Mac

Quick Start
Computers
Groups
Policies
Exclusions
Download Connector

Step 2. Select the group that was created earlier in this guide

Download Connector

Group: remoteWorkers

Windows

No computers require updates

Protect Policy

- Flash Scan on Install
- Redistributable

Connector Version: 7.1.5.11523

[Show URL](#) [Download](#)

Mac

Audit Policy for FireAMP Mac

- Flash Scan on Install

Connector Version: 1.16.1.851

Package Format: DMG

[Show URL](#) [Download](#)

Linux

Audit Policy for FireAMP Linux

- Flash Scan on Install

Distribution: RHEL/CentOS 6

Connector Version: 1.16.1.783

[Show GPG Public Key](#) [Show URL](#) [Download](#)

Android

Default FireAMP Android

- Install from Google Play

Connector Version: 2.2.0.14

[Show URL](#) [Download](#)

Step 3. Show the URL for the windows and mac connectors, then copy them to a notepad file for future use

Download URL

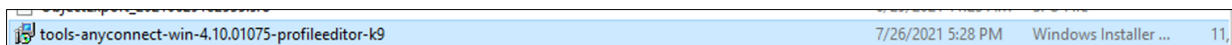
You can email this URL to users so they can download and install the Connector

https://console.amp.cisco.com/install_packages/ad256018-946a-46a8-b921-81671a774c73/download?product=WindowsProduct

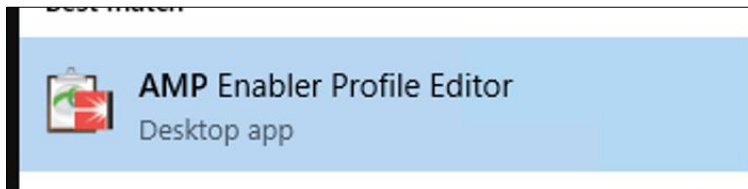
[Copy URL](#)

Create AMP Profile

Step 1. Install the **AnyConnect profile editor** that was downloaded in the AnyConnect headend file steps



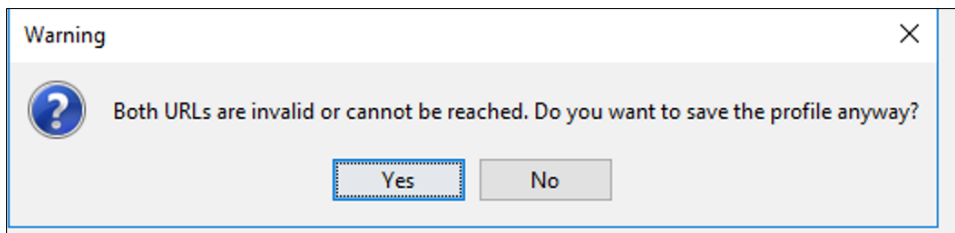
Step 2. After it has been installed, open the **AMP Enabler Profile Editor**



Step 3. Leave the radio on **Install AMP Enabler** and put the two URLs (uniform resource locators) for the connectors in their respective boxes

Note: If the check fails, paste the URL into a browser and see if it downloads. If it does, then you may save this configuration

Step 4. **Save** the profile and accept the message about the URLs (uniform resource locators) being invalid

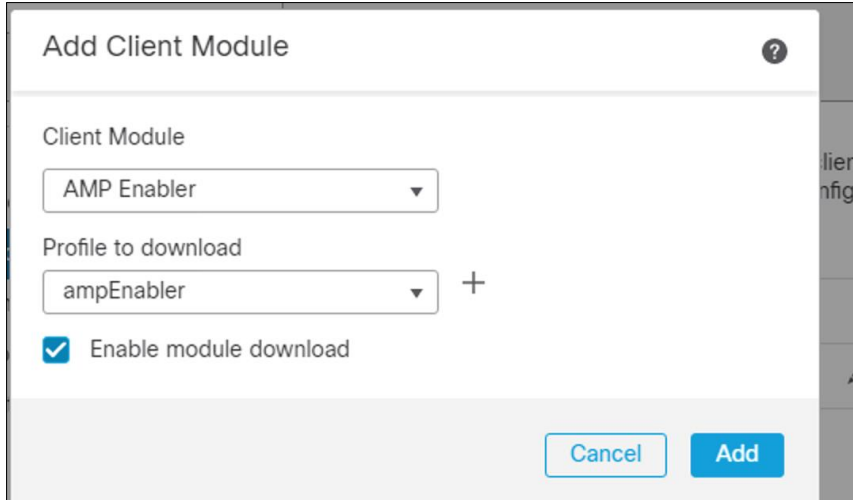


Step 5. The file should now be saved as **amp-enabler.xml** in your documents folder



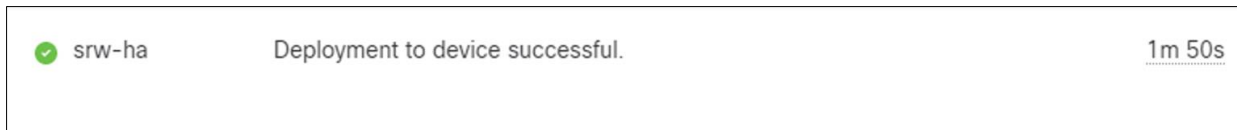
Add AMP enabler to the RA VPN profile

- Step 1.** Go back to the RAVPN for **Client Modules** on the **FMC**
- Step 2.** Click the **plus sign** to add a **New Module**
- Step 3.** Change the client module to **AMP Enabler** and add a new profile.
- Step 4.** Give it a meaningful name and upload the amp-enabler xml file. Click **Save**
- Step 5.** Check the **Enable Module Download** box and click on **Add**.

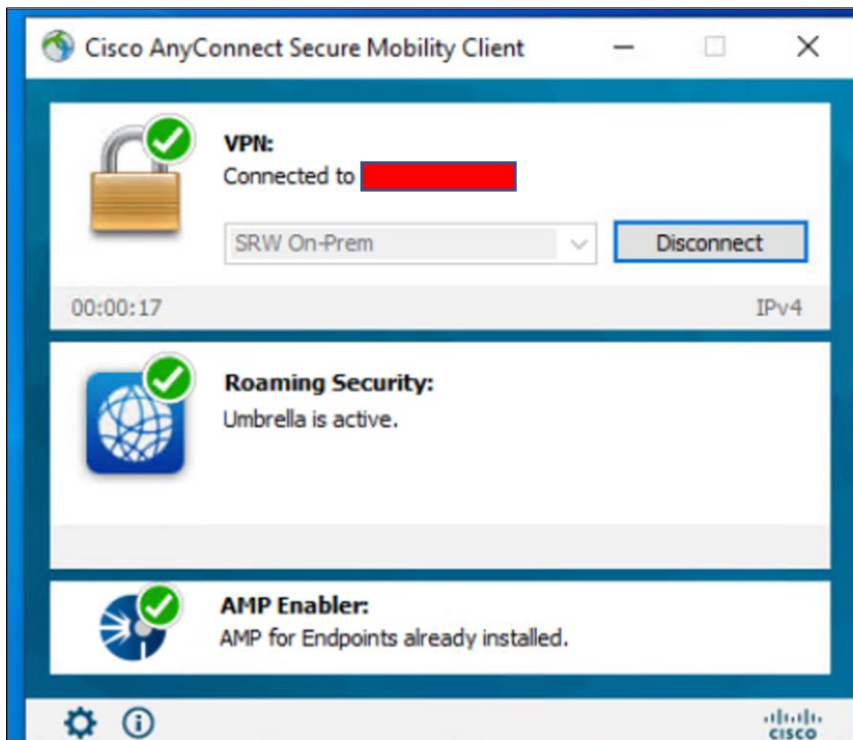


Step 6. Click on **Save**, **Save**, and **Save** once more

Step 7. **Deploy** these changes



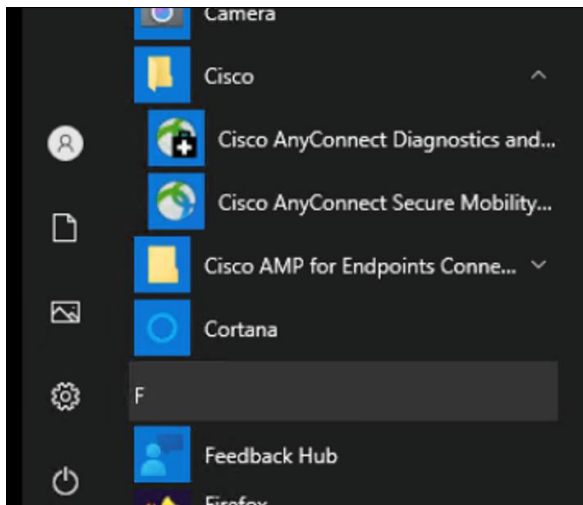
Step 8. Connect to the VPN and make sure the modules get installed



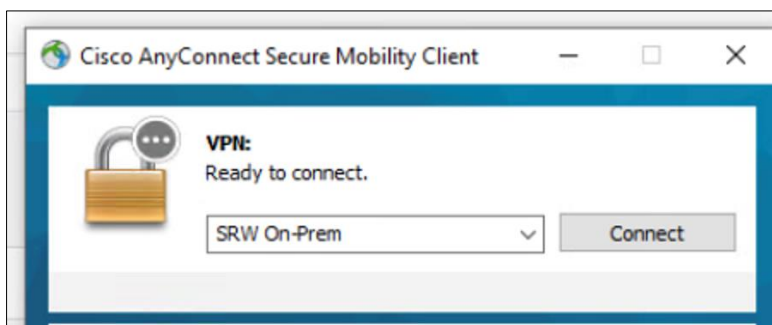
Validation Testing

Test Case 1- Cisco Duo two-factor authentication (2FA)

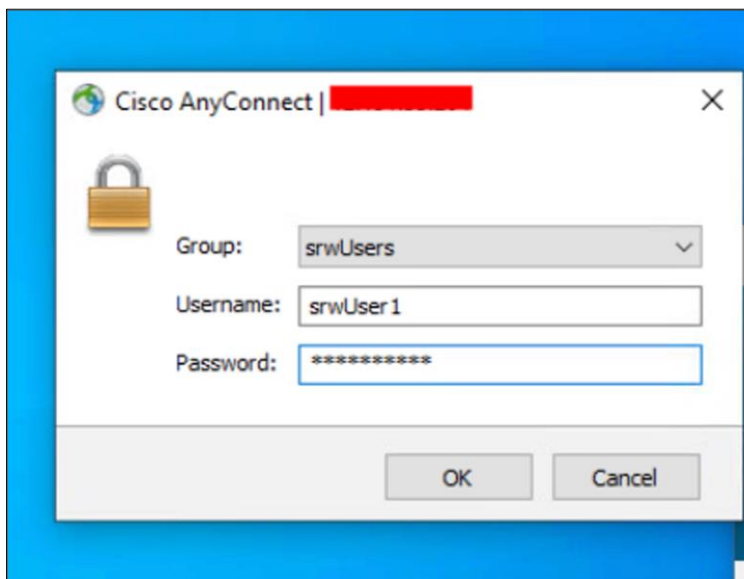
Step 1. On a roaming device, open AnyConnect Secure Mobility Client



Step 2. Select the network to be connected to and press **Connect**.



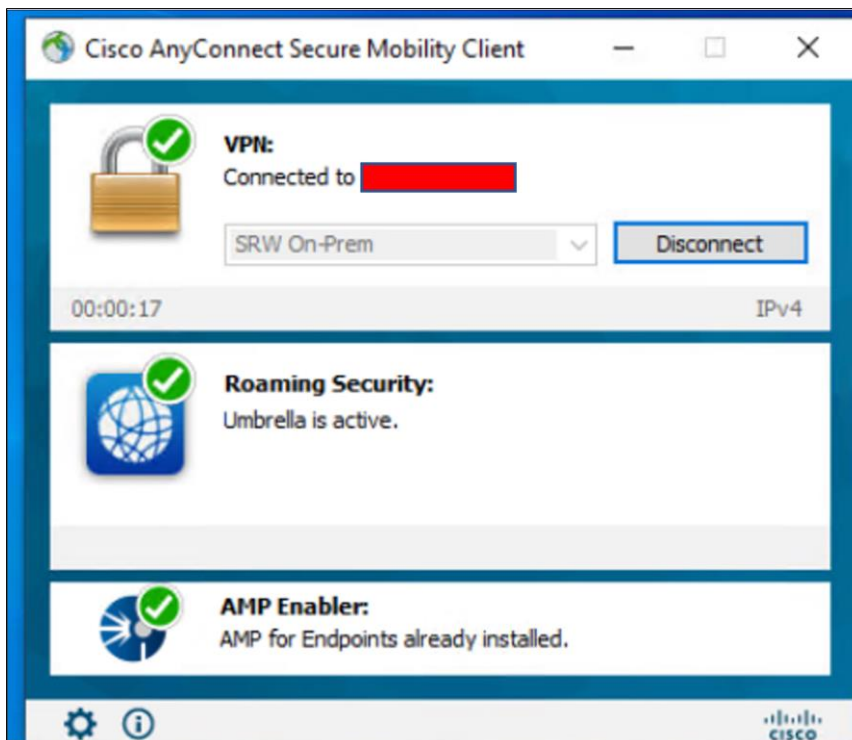
Step 3. Enter the credentials for a valid user and press **OK**.



Step 4. If configured correctly, you will get a Duo push notification

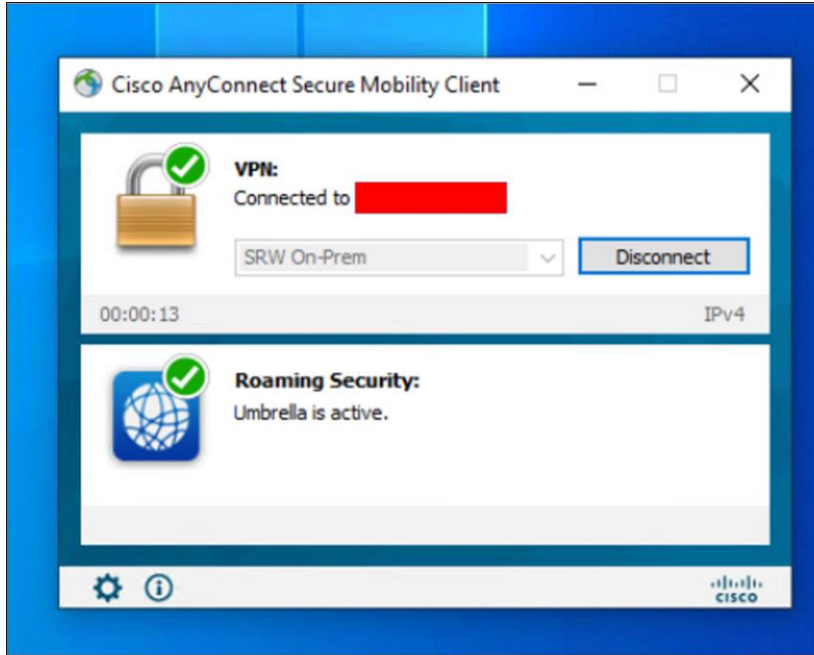


Step 5. Approve the request and finish the connection

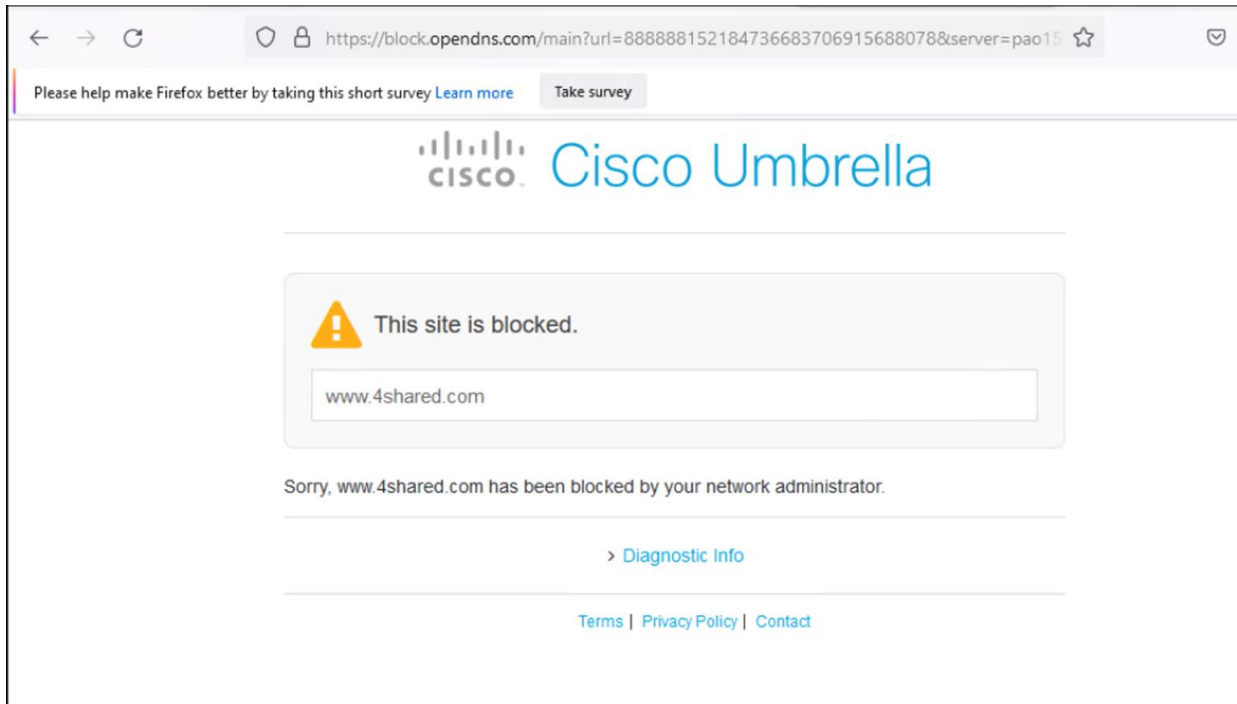


Test Case 2 - Cisco Umbrella Roaming Security Module (DNS layer protection)

Step 1. Open AnyConnect Secure Mobility Client and verify the **Roaming Security** module is active

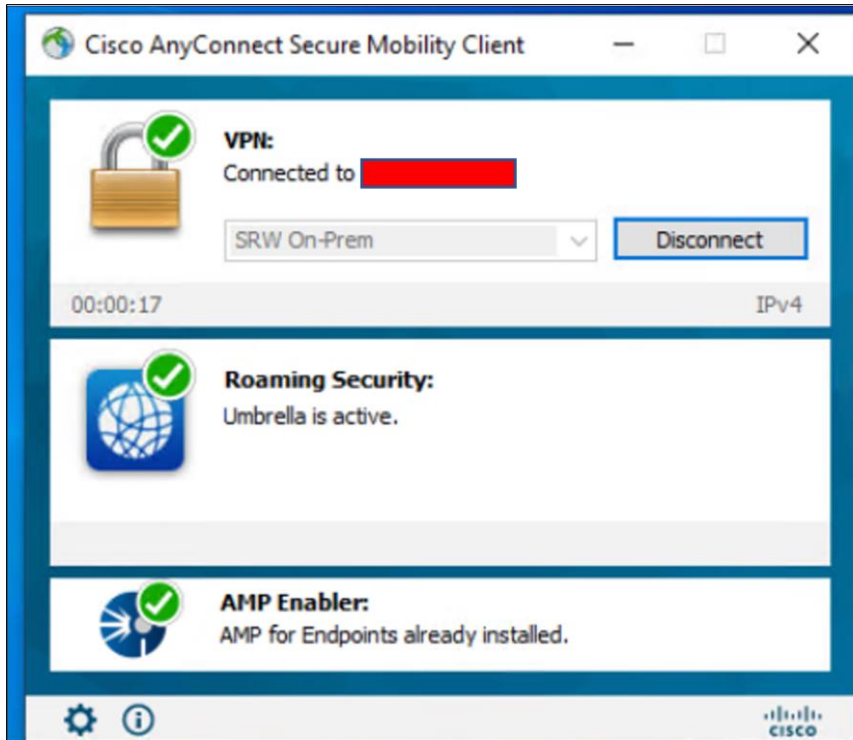


Step 2. Open any browser and connect to **4shared.com**. Verify it has been blocked.

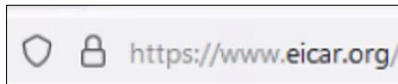


Test Case 3 - Cisco Secure Endpoint AMP enabler (File blocking)

Step 1. Verify the AMP enabler is installed



Step 2. Go to eicar.org



Step 3. Download the eicar.com file



Step 4. After saving the file, it should either fail or be removed immediately



Step 5. In the Secure Endpoint Dashboard, navigate to the **Analysis -> Event** page

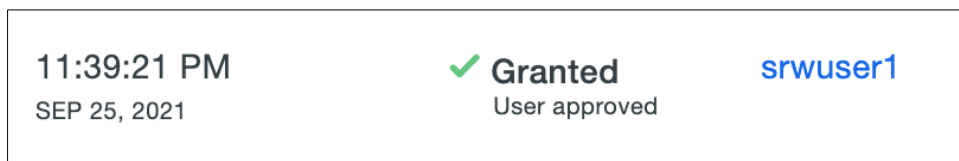
Step 6. There should be a block for the file in the events



Test Case 4 - Geolocation blocking

This test will validate that the geo block in Duo is successfully blocking connection attempts from devices outside of the geographical range set in Duo.

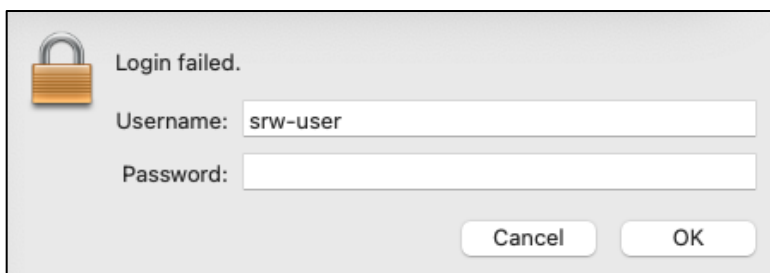
- Step 1.** Connect to the VPN from a region that is allowed to connect and login.
- Step 2.** A Duo prompt should be pushed to the device and allow access
- Step 3.** Check the Duo reports page, there should be a User approved connection



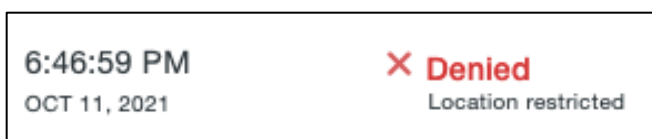
- Step 4.** Disconnect and attempt to connect from a region that has not been enabled by your organization.

Note: If you do not have a means of testing with a device outside of your region, temporarily change the allow list to block the current region you are in to test that a region block will be successful.

- Step 5.** A Duo prompt should not come up and it should continue to ask for login information.



- Step 6.** Check the Duo reports page, there should be a block with a reason of Location restricted



Appendix

Appendix A - Licensing information

This section defines the packaging structure and licensing information for the Cisco Secure VPN. The following Secure 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 (about 5 years).

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 Secure VPN customers should think of AnyConnect Plus like the previous AnyConnect Essentials.

Apex license includes more advanced services such as endpoint posture checks (host scan through FTD 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 Secure VPN customers should think of AnyConnect Apex like the 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 Secure VPN and third-party (non-Secure VPN) IKEv2 VPN clients
- Network Visibility Module
- All Plus services described above

VPN-only licenses are perpetual based, clientless, and may only be used on a single FTD. 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-Secure VPN) 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 Secure VPN and third-party (non-Secure VPN) IKEv2 VPN clients

The Secure VPN Licenses are supported on the following platforms:

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

Appendix B - Acronyms

Acronym	Definition
ACL	Access control list
AD	Active Directory
AMP	Advanced Malware Protection
AMP4E	Advanced Malware Protection for Endpoints
ASAav	Adaptive Security Virtual Appliance

Acronym	Definition
ASDM	Adaptive Security Appliance Device Manager
AVC	Application Visibility and Control
CDO	Cisco Defense Orchestrator
CVD	Cisco Validated Design
FDM	Firepower Device Manager
FMC	Firewall Management Center
FQDN	Fully Qualified Domain Name / Domain Name System (DNS) Name
FTD	Firepower Threat Defense
MFA	Multi Factor Authentication
PIN	Place in network
RAVPN	Remote Access Virtual Private Network
VPN	Virtual Private Network

Appendix C - References

[Secure Remote Worker for AWS Design Guide](#)

[Secure Remote Worker for Azure Design Guide](#)

[Cisco Secure Firewall](#)

[Cisco Firepower 4100 Series Data Sheet](#)

[Cisco Firepower 9300 Series Data Sheet](#)

[Firewall Management Center Virtual Getting Started Guide](#)

[Cisco Firepower 4100 Getting Started Guide](#)

[Cisco Firepower 9300 Getting Started Guide](#)

[Cisco Firepower Split Tunneling Configuration](#)

[High Availability for Firepower Threat Defense](#)

[Cisco AnyConnect Secure Mobility Client](#)

[Cisco AnyConnect Secure Mobility License Ordering Guide](#)

[Cisco Umbrella Module for AnyConnect](#)

[Duo for Cisco AnyConnect VPN with ASA or Firepower](#)

Appendix D - Feedback

If you have feedback on this design guide or any of the Cisco Security design guides, please send an email to ask-security-cvd@cisco.com

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)