You make **possible**

Deploying AnyConnect with Firepower Threat Defense with posture and MFA

Mark Stephens – Cyber Security Technical Solutions Architect
@216stephens

BRKSEC-2348

Barcelona | January 27-31, 2020

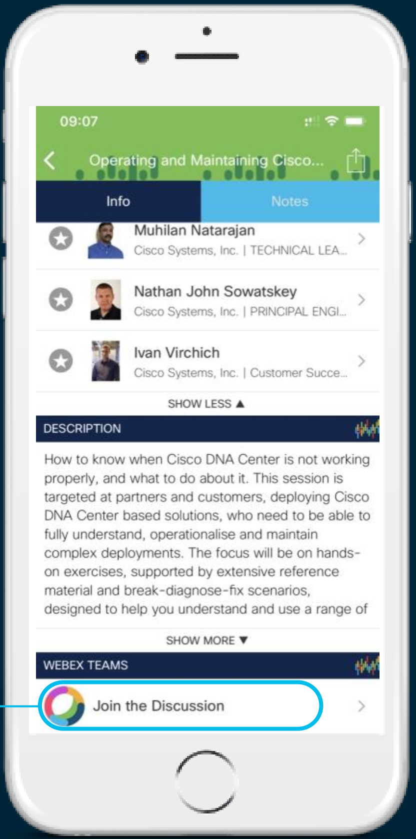
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

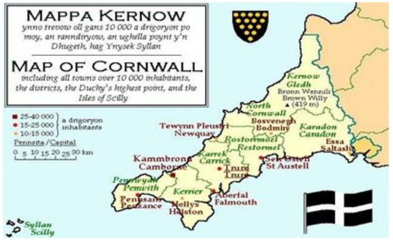
Abstract

- This session will enable attendees to deploy FTD to securely support remote access users with AnyConnect, leveraging ISE integration for posture and Duo integration for MFA. The breakout will cover the steps for success and address the integrations of the bigger Cisco architecture and TrustSec.   The attendee will leave the session confident of the capabilities of FTD, the configuration procedures and the tools for troubleshooting. This is a must attend session for those existing AnyConnect customers wanting to move to Firepower.

Agenda

- Introduction
- The Big Picture Architecture
- Platform Drill Down
- Steps for success
- Configuration Down and Dirty
- TrustSec Integration
- Conclusion

About your speaker



- Cyber Technical Solutions Architect
- GPEN, CISSP and former CCIE
- 21+ year Cisco veteran (Joined September 1998)
- Enterprise SE, 9 years
- Security TSA (Enterprise & Commercial) 12 years
- Grew up in Cornwall, England
- Live in Cleveland, Ohio, US
- Wife, Nadine and 4 teenagers
- Fun: Photography, reading, travel, school sports and dance and budding sailor

Mark Stephens: mstephen@cisco.com

#216stephens

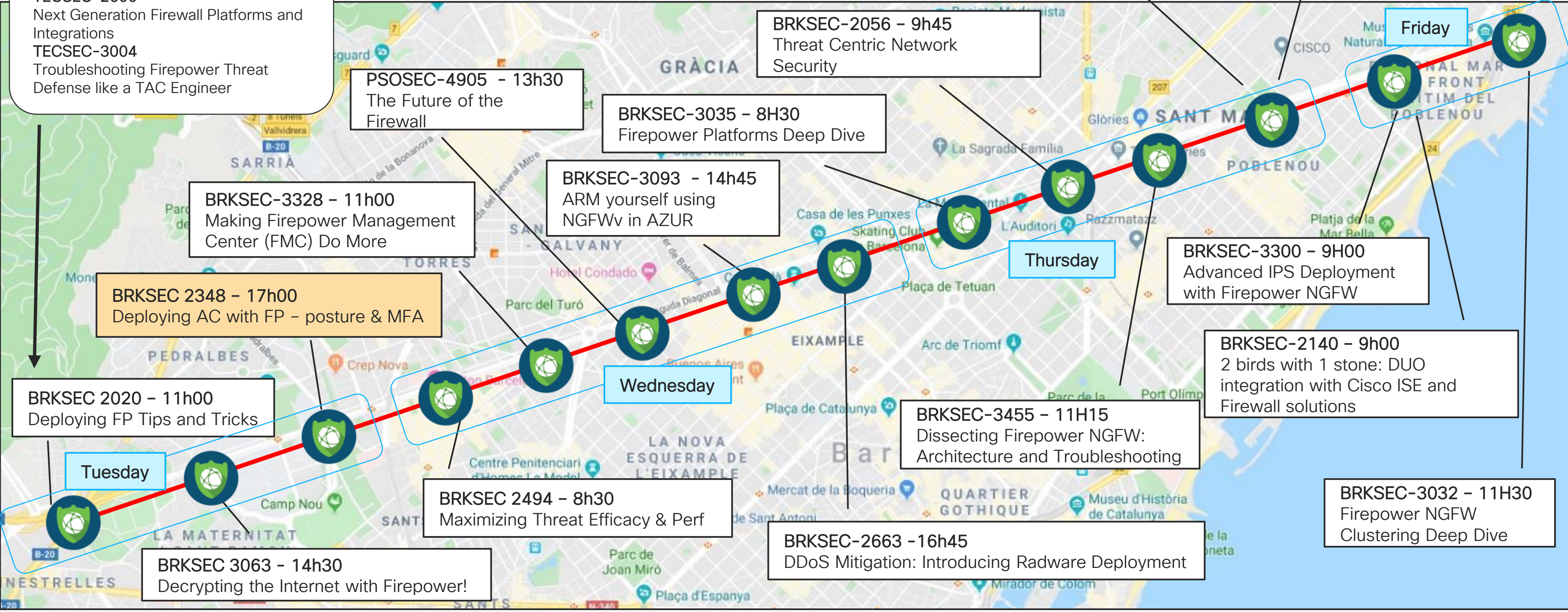
Introduction

What not covered in this session

Not intending to *boil the ocean*

This is a solutions approach

Firepower Diagonal Learning Map



Monday – 8h30
TECSEC-2600
Next Generation Firewall Platforms and Integrations
TECSEC-3004
Troubleshooting Firepower Threat Defense like a TAC Engineer

BRKSEC 2020 – 11h00
Deploying FP Tips and Tricks

BRKSEC 3063 - 14h30
Decrypting the Internet with Firepower!

BRKSEC 2348 – 17h00
Deploying AC with FP – posture & MFA

BRKSEC 2494 – 8h30
Maximizing Threat Efficacy & Perf

BRKSEC-3328 – 11h00
Making Firepower Management Center (FMC) Do More

PSOSEC-4905 - 13h30
The Future of the Firewall

BRKSEC-3093 - 14h45
ARM yourself using NGFWv in AZUR

BRKSEC-3035 – 8H30
Firepower Platforms Deep Dive

BRKSEC-2663 -16h45
DDoS Mitigation: Introducing Radware Deployment

BRKSEC-2056 – 9h45
Threat Centric Network Security

BRKSEC-3455 – 11H15
Dissecting Firepower NGFW: Architecture and Troubleshooting

BRKSEC 3629 – 14h45
Designing IPSec VPNs with Firepower Threat Defense integration for Scale and High Availability

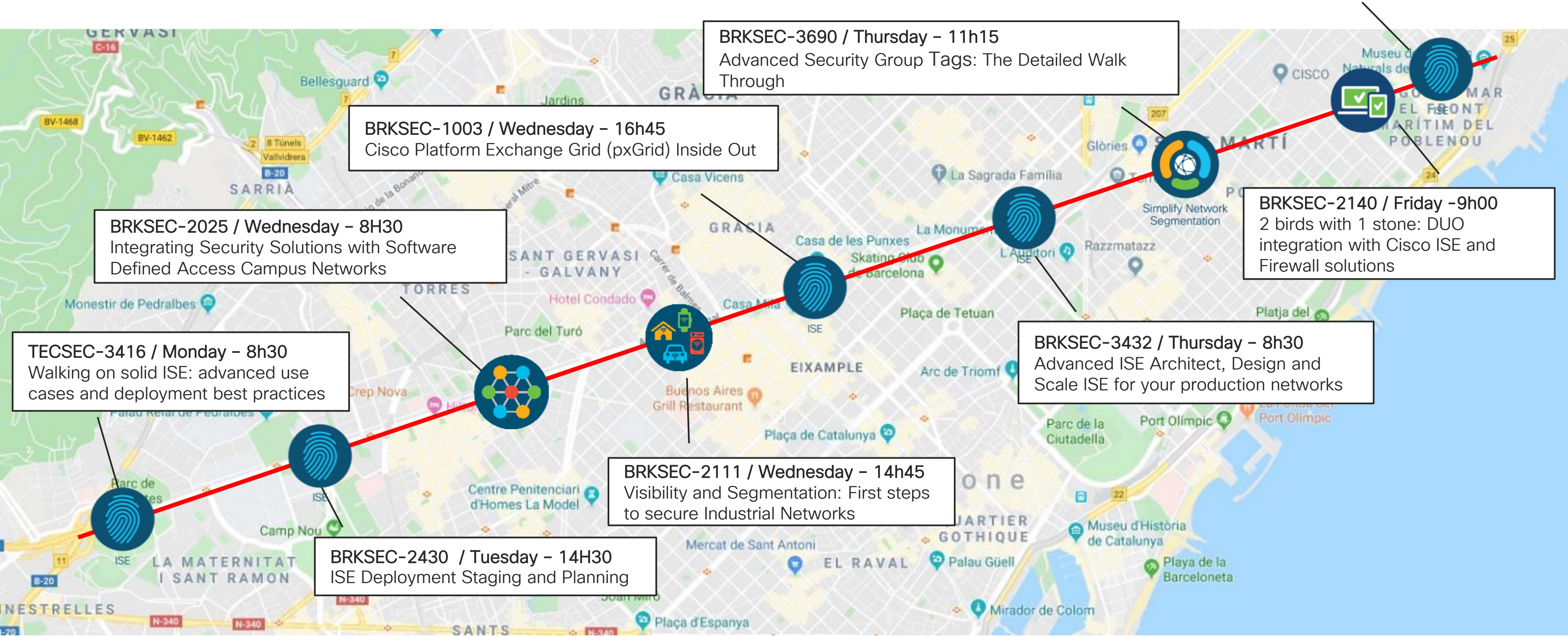
Thursday BRKSEC-2034 -14h45
Cloud Management of Firepower and ASA with Cisco Defense Orchestrator

BRKSEC-3300 – 9H00
Advanced IPS Deployment with Firepower NGFW

BRKSEC-2140 – 9h00
2 birds with 1 stone: DUO integration with Cisco ISE and Firewall solutions

BRKSEC-3032 – 11H30
Firepower NGFW Clustering Deep Dive

ISE Diagonal Learning Map



TECSEC-3416 / Monday – 8h30
Walking on solid ISE: advanced use cases and deployment best practices

BRKSEC-2430 / Tuesday – 14H30
ISE Deployment Staging and Planning

BRKSEC-2025 / Wednesday – 8H30
Integrating Security Solutions with Software Defined Access Campus Networks

BRKSEC-2111 / Wednesday – 14h45
Visibility and Segmentation: First steps to secure Industrial Networks

BRKSEC-1003 / Wednesday – 16h45
Cisco Platform Exchange Grid (pxGrid) Inside Out

BRKSEC-3690 / Thursday – 11h15
Advanced Security Group Tags: The Detailed Walk Through

BRKSEC-3432 / Thursday – 8h30
Advanced ISE Architect, Design and Scale ISE for your production networks

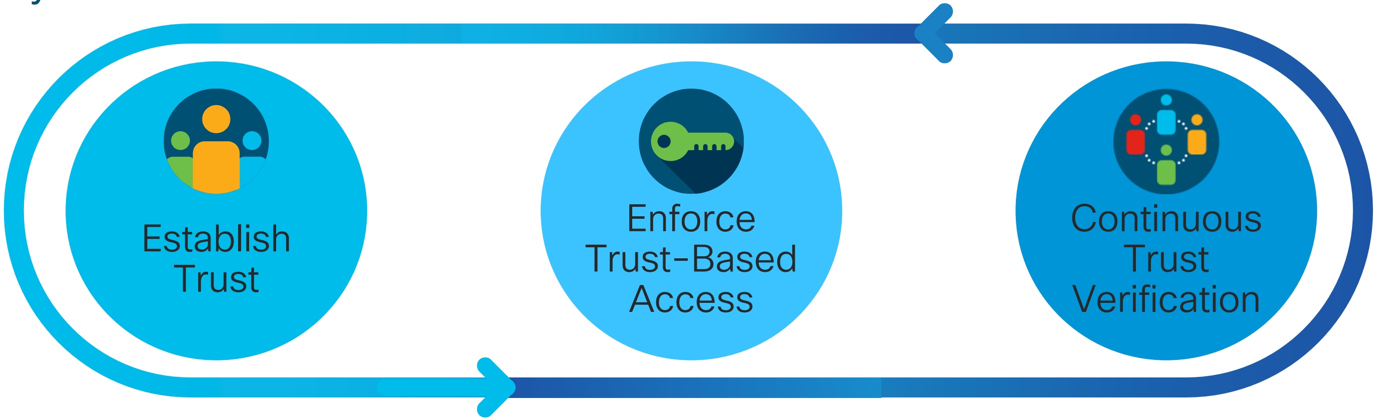
BRKSEC-2140 / Friday -9h00
2 birds with 1 stone: DUO integration with Cisco ISE and Firewall solutions

BRKSEC-3229 / Friday 9h00
ISE under magnifying glass.
How to troubleshoot ISE

The Big Picture Architecture

How to Implement Cisco Zero Trust

3 Step Cyclical Process



We establish trust by verifying:

- Multi-factors of User Identity
- Device context and Identity
- Device posture & health
- Location
- Relevant attributes and context

We enforce least privilege access to:

- Networks
- Applications
- Resources
- Users & Things

We continuously verify:

- Original tenets used to establish trust are still true
- Traffic is not threat traffic
- Behavior for any risky, anomalous or malicious actions
- If compromised, then the trust is broken

Solution Components

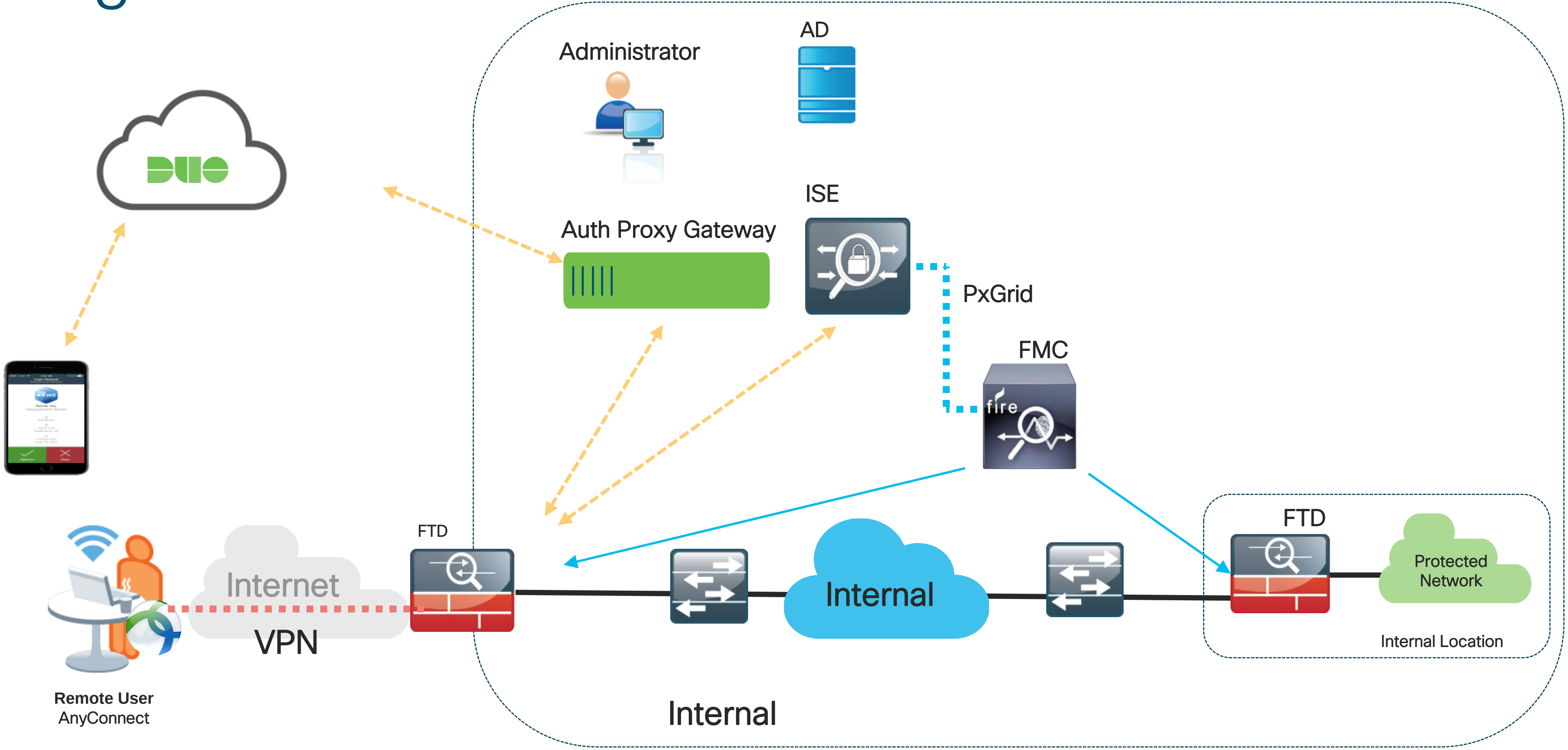
Establish Trust

Enforce Trust-Based Access

Continuous Trust Verification

Multi Factor Authentication	DUO	Verify identity of users
Policy Control and Management	ISE FMC	Ensure trustworthiness of devices
Infrastructure	FTD	Enforce risk-based and adaptive access policies

Big Picture Architecture

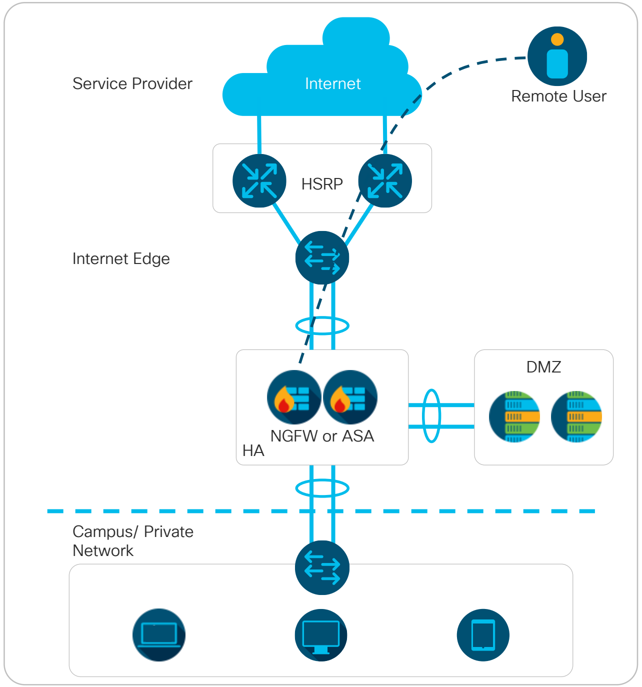


Platform Drill Down

FTD

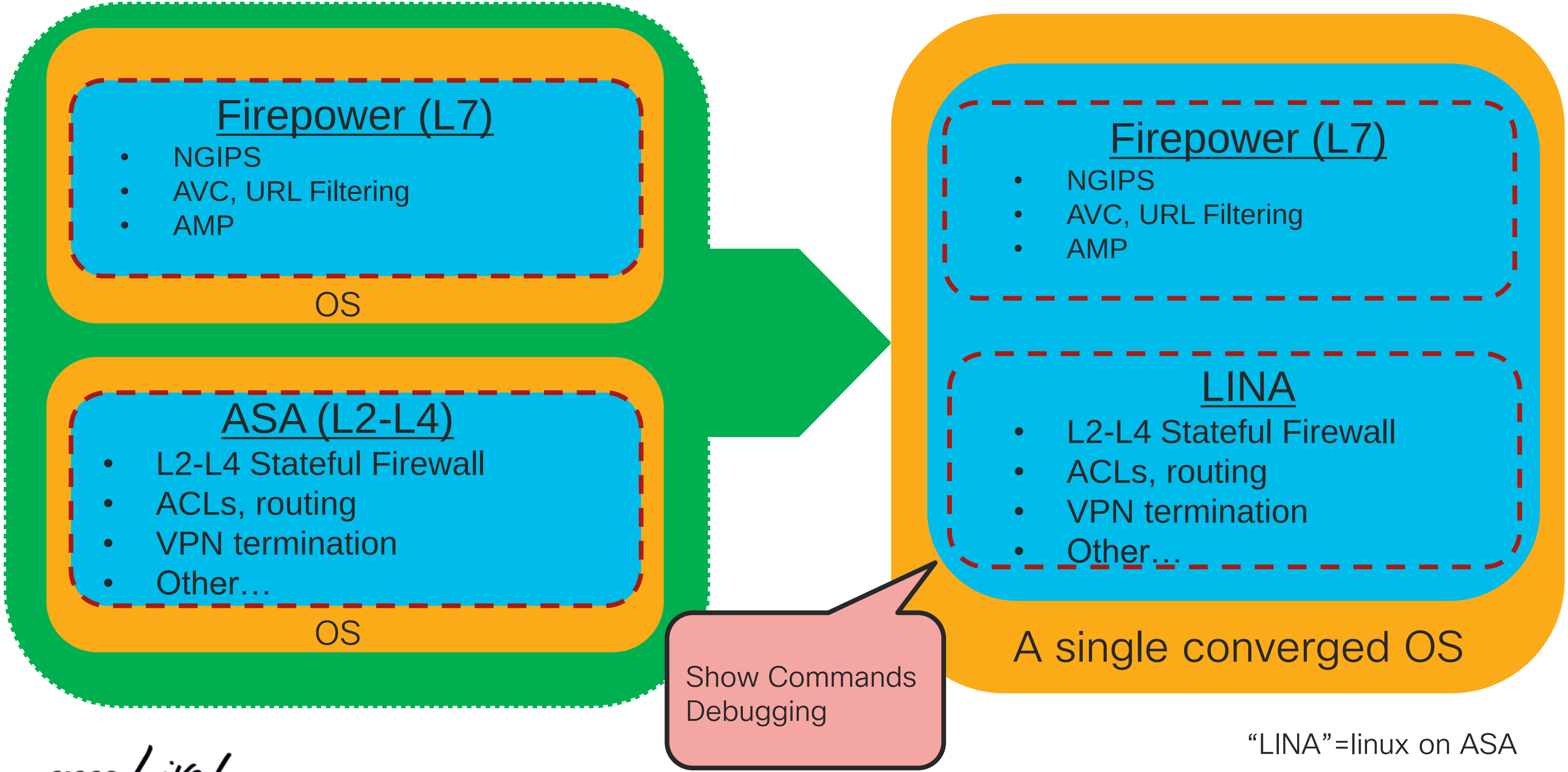
FTD For Remote Access VPN

Key Functions	Key Capabilities
Resilience (and scalability)	VPN load balancing
Advanced Access Control	IPSEC and SSL
Block access to malicious IP's, URL's, DNS	**Talos Security Intelligence**
Dynamic NAT/PAT and Static NAT	AD, LDAP and Radius
Remote Access VPN	IKEv1 and IKEv2
Site to Site VPN	RADIUS CoA
Detecting malicious network traffic	**Snort IPS**
Visibility and tracking of file transfers, Blocking of malicious files	**Advanced Malware Protection**
Dynamic analysis of unknown files	**Threat Grid Integration**



Use-case: RAVPN

Firepower Threat Defense (FTD)



Firepower (L7)

- NGIPS
- AVC, URL Filtering
- AMP

OS

ASA (L2-L4)

- L2-L4 Stateful Firewall
- ACLs, routing
- VPN termination
- Other…

OS

Firepower (L7)

- NGIPS
- AVC, URL Filtering
- AMP

LINA

- L2-L4 Stateful Firewall
- ACLs, routing
- VPN termination
- Other…

A single converged OS

Show Commands
Debugging

“LINA”=linux on ASA

Cisco FTD NGFW Portfolio

FPR-1010

650 Mbps AVC
650 Mbps AVC+IPS

FPR-1120
FPR-1140
FPR-1150

1.5-2.2 Gbps AVC
1.5-2.2 Gbps AVC+IPS

FPR-2110
FPR-2120
FPR-2130
FPR-2140

2-8.5 Gbps AVC
2-8.5 Gbps
AVC+IPS

New!
FPR-4115
FPR-4125
FPR-4145

FPR-4110
FPR-4120
FPR-4140
FPR-4150

Stand alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS 6

Six node cluster
Up to 254 Gbps AVC
Up to 226 Gbps
AVC+IPS

New!
FPR9K-SM-40
FPR9K-SM-48
FPR9K-SM-56

FPR9K-SM-24
FPR9K-SM-36
FPR9K-SM-44

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS

Six node (2 chassis) cluster
Up to 336 Gbps AVC
Up to 307 Gbps AVC+IPS

Remote Access VPN Sizing and Throughput

Firepower Platform	**1010**	**1120**	**1140**	**1150**	**2110**	**2120**	**2130**	**2140**
Max VPN Peers	75	150	400	800	1500	3500	7500	10,000
IPsec VPN Throughput	300 Mbps	1 Gbps	1.2 Gbps	1.4 Gbps	500 Mbps	700 Mbps	1 Gbps	2 Gbps
Firepower Platform	**4110**	**4115**	**4120**	**4125**	**4140**	**4145**	**4150**	
Max VPN Peers	10,000	15,000	15,000	20,000	20,000	20,000	20,000	
IPsec VPN Throughput	6 Gbps	8 Gbps	10 Gbps	14 Gbps	13 Gbps	18 Gbps	14 Gbps	

Note: Remote Access throughput approximately minus 10% of IPSec VPN S2S numbers shown

Remote Access VPN Sizing and Throughput

Firepower Platform	SM-24	SM-36	SM-40	SM-44	3xSM-44	SM-48	SM-56	3xSM-56
Max VPN Peers	20,000	20,000	20,000	20,000	60,000	20,000	20,000	60,000
IPsec VPN Throughput	13 Gbps	16 Gbps	20 Gbps	17 Gbps	51 Gbps	25 Gbps	27 Gbps	81 Gbps*
Firepower Platform	**NGFWv 4 vCPU**	**NGFWv 8 vCPU**	**NGFWv 12 vCPU**					
Max VPN Peers	250	250	750					
IPsec VPN Throughput	761 Mbps	1.3 Gbps	2.4 Gbps					

Note: Remote Access throughput approximately minus 10% of IPSec VPN S2S numbers shown

*In unclustered configuration

Management Designed for the User

Flexibility of cloud or on-premises options

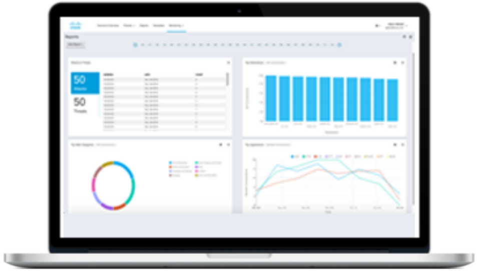
Security Integrations

Cisco Firepower Management Center (FMC)

On premise Centralized Manager
SecOps Focused

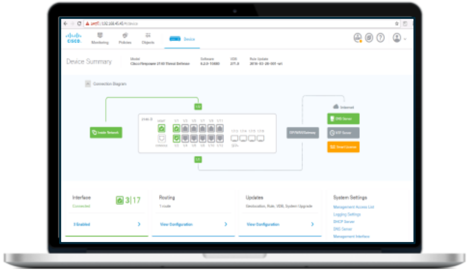
Common APIs

Cisco Defense Orchestrator (CDO)



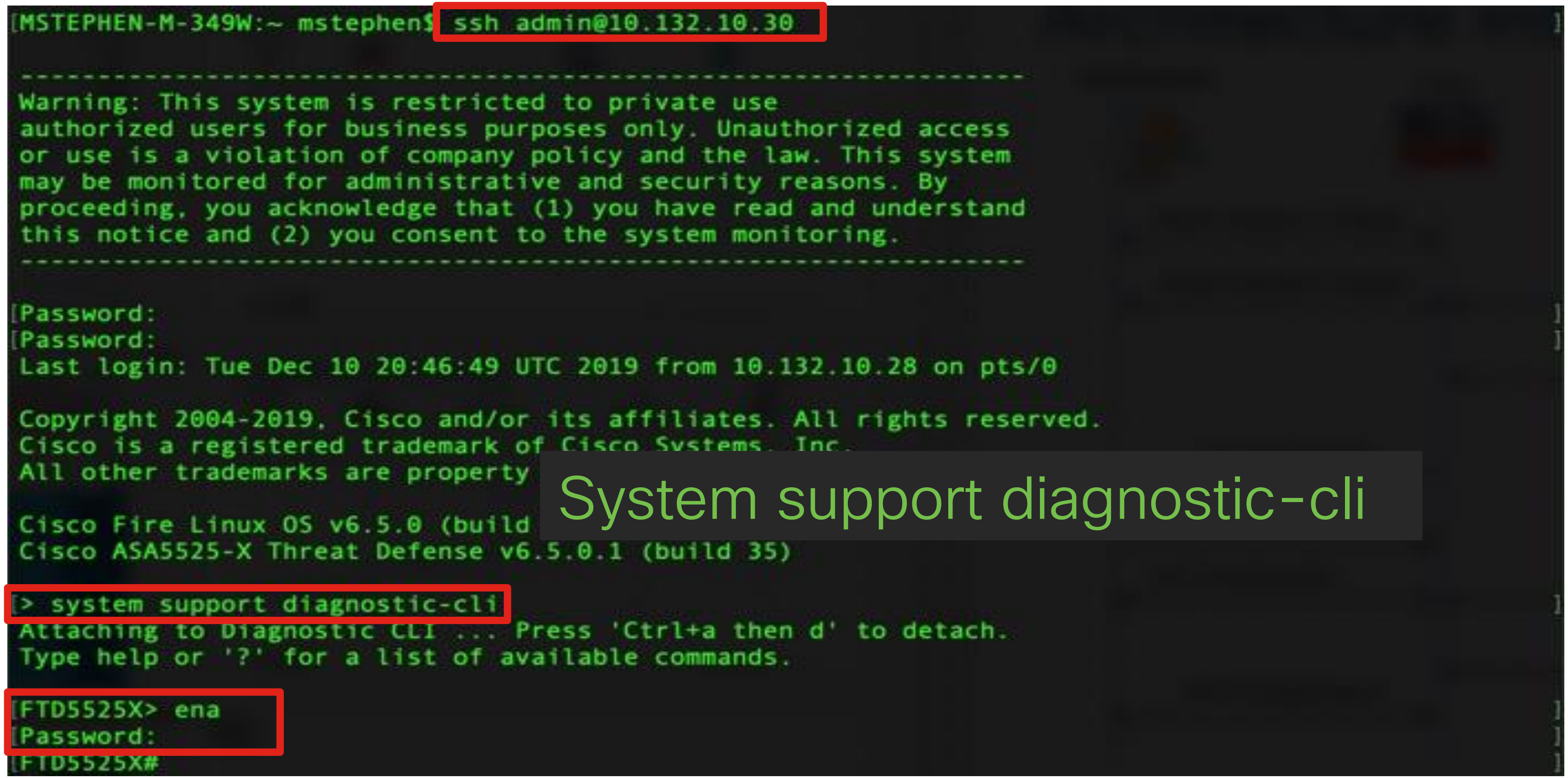
Cloud Based Centralized Manager
NetOps Focused

Cisco Firepower Device Manager (FDM)



On-box Manager
NetOps Focused

Accessing the LINA (cli)



```
[MSTEPHEN-M-349W:~ mstephen$ ssh admin@10.132.10.30

 ---------------------------------------------------------------
 Warning: This system is restricted to private use
 authorized users for business purposes only. Unauthorized access
 or use is a violation of company policy and the law. This system
 may be monitored for administrative and security reasons. By
 proceeding, you acknowledge that (1) you have read and understand
 this notice and (2) you consent to the system monitoring.
 ---------------------------------------------------------------

[Password:
[Password:
 Last login: Tue Dec 10 20:46:49 UTC 2019 from 10.132.10.28 on pts/0

 Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
 Cisco is a registered trademark of Cisco Systems, Inc.
 All other trademarks are property

 Cisco Fire Linux OS v6.5.0 (build
 Cisco ASA5525-X Threat Defense v6.5.0.1 (build 35)

[> system support diagnostic-cli
 Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
 Type help or '?' for a list of available commands.

[FTD5525X> ena
[Password:
[FTD5525X#
```

System support diagnostic-cli

FTD Software Versions

6.3.X

- RA VPN: RADIUS Dynamic Authorization or Change of Authorization (CoA)
- RA VPN: Two-Factor Authentication

6.4.X

- RA VPN: Secondary authentication

FDM

- RA VPN: Radius servers and COA
- Multiple Connection profiles
- Authentication Certs, MFA, etc
- Redundant ISE servers

6.5.X

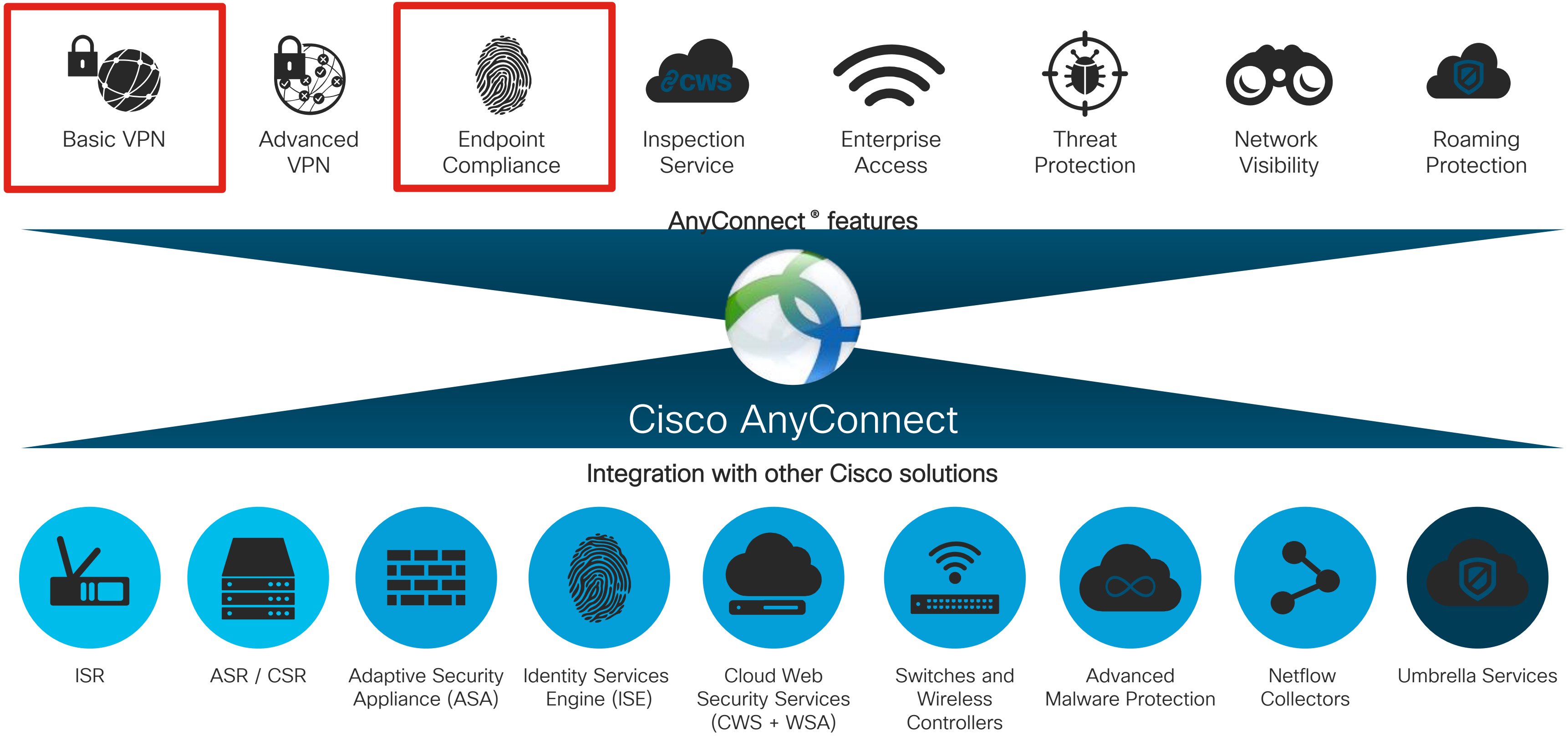
- FPR1150 Support

FDM

- Remote access VPN two-factor authentication using Duo LDAP.

AnyConnect

Cisco AnyConnect® – Way more than VPN



Basic VPN

Advanced VPN

Endpoint Compliance

Inspection Service

Enterprise Access

Threat Protection

Network Visibility

Roaming Protection

AnyConnect® features

Cisco AnyConnect

Integration with other Cisco solutions

ISR

ASR / CSR

Adaptive Security Appliance (ASA)

Identity Services Engine (ISE)

Cloud Web Security Services (CWS + WSA)

Switches and Wireless Controllers

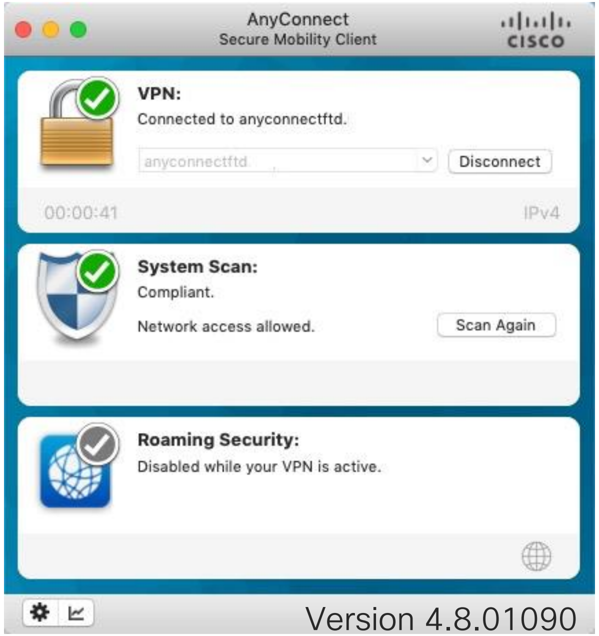
Advanced Malware Protection

Netflow Collectors

Umbrella Services

AnyConnect Secure Mobility Client

- TLS/IPSec IKEv2 Client
- IPv4, IPv6
- Windows, MAC OS X, Linux Intel
- Mobile devices IOS/Android
- Strong and NG encryption
- Authentication Options
- Consistent User Experience
- And more…



AnyConnect
Secure Mobility Client

VPN:
Connected to anyconnectftd.

anyconnectftd

00:00:41 IPv4

System Scan:
Compliant.
Network access allowed.

Roaming Security:
Disabled while your VPN is active.

Version 4.8.01090

https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/datasheet-c78-733184.html

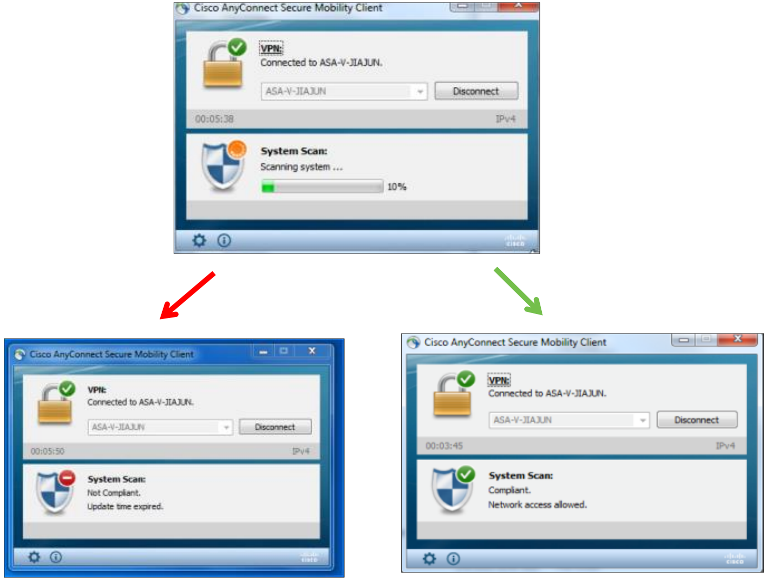
System Scan Module

ISE Posture

Supports device posture and authorization across multiple access methods

Simplifies management with only one agent to manage

Prevents noncompliant devices from accessing the network


Cisco AnyConnect Secure Mobility Client
ASA-V-JIAJUN
Disconnect
00:05:38
IPv4
10%
Cisco AnyConnect Secure Mobility Client
ASA-V-JIAJUN
Disconnect
00:05:50
IPv4
Cisco AnyConnect Secure Mobility Client
ASA-V-JIAJUN
Disconnect
00:03:45
IPv4

VPN:
Connected to ASA-V-JIAJUN.

System Scan:
Scanning system ...

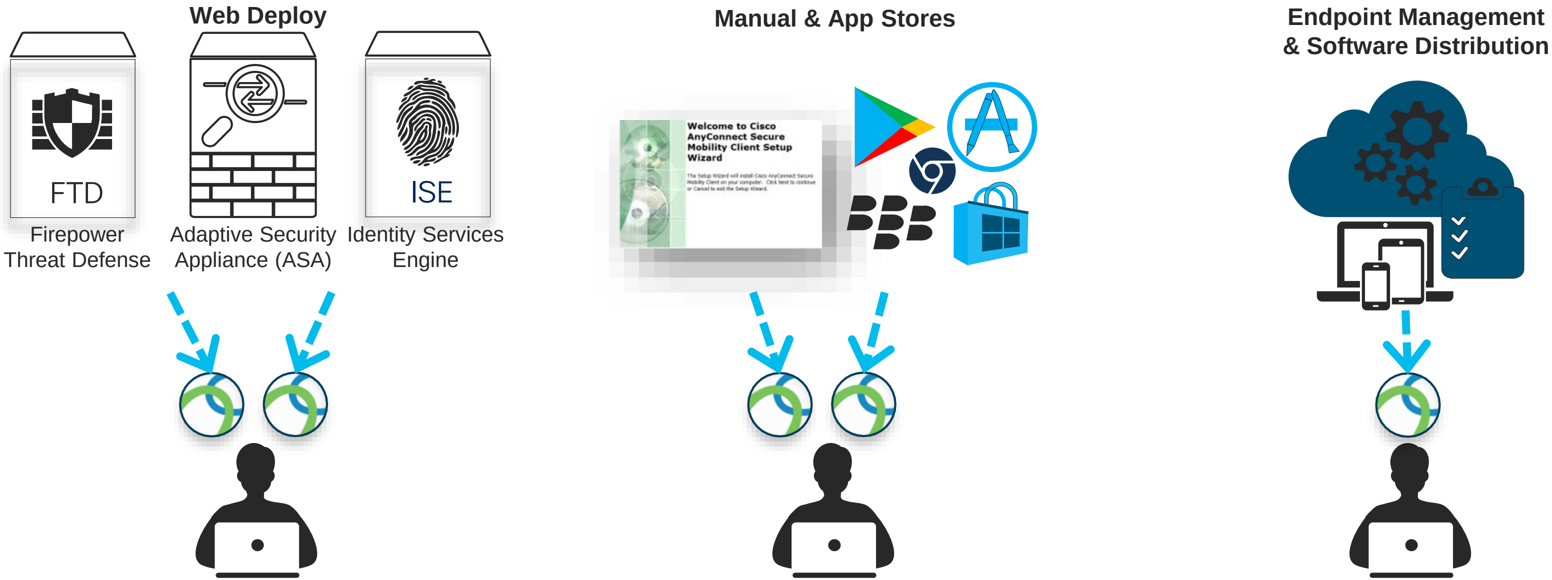
VPN:
Connected to ASA-V-JIAJUN.

System Scan:
Not Compliant.
Update time expired.

VPN:
Connected to ASA-V-JIAJUN.

System Scan:
Compliant.
Network access allowed.

Get Users Connected Quickly and Easily



Welcome to Cisco AnyConnect Secure Mobility Client Setup Wizard

The Setup Wizard will install Cisco AnyConnect Secure Mobility Client on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Benefits

- Flexible Options for Deployments
- Greater Control over Correct Versions
- Dynamically Update Policies on Endpoint
- Simple to add / remove / change AC Modules

Capabilities

- Headend Deployment from ASA, FTD and/or ISE
- AC Installed with Software Managers (SMS/SCCM)
- Manual Install per OS
- Mobile Users can install from App Stores

Cisco Identity Services Engine (ISE)

Cisco ISE overview

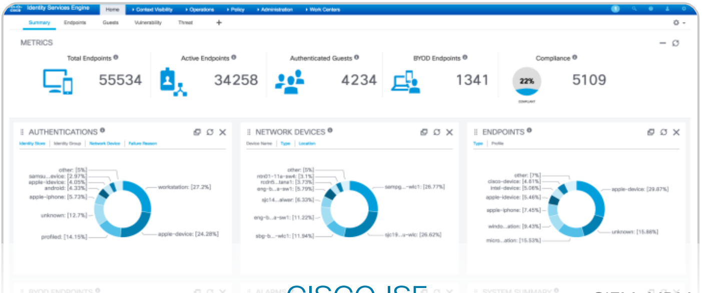
Release 2.6.0 ⭐

Cisco Identity Services Engine (ISE) is an industry leading, Network Access Control and Policy Enforcement platform, that lets you,

See
Users, endpoints and applications

Secure
By controlling network access and segmentation

Share
Context with partners for enhanced operations



Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Summary | Endpoints | Guests | Vulnerability | Threat

METRICS

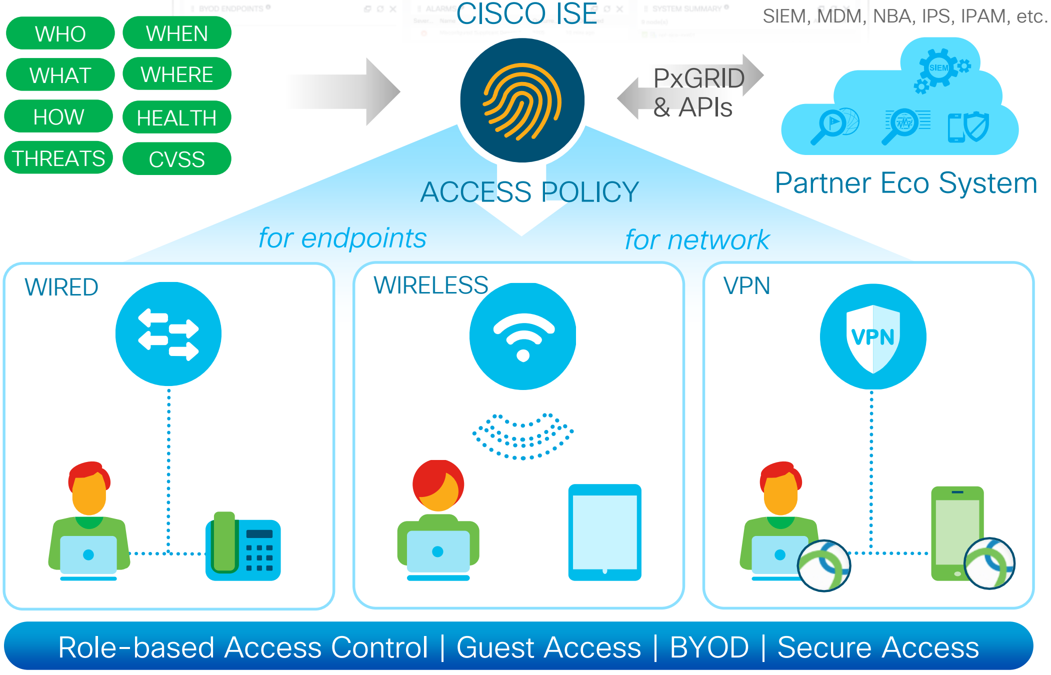
Total Endpoints 55534

Active Endpoints 34258

Authenticated Guests 4234

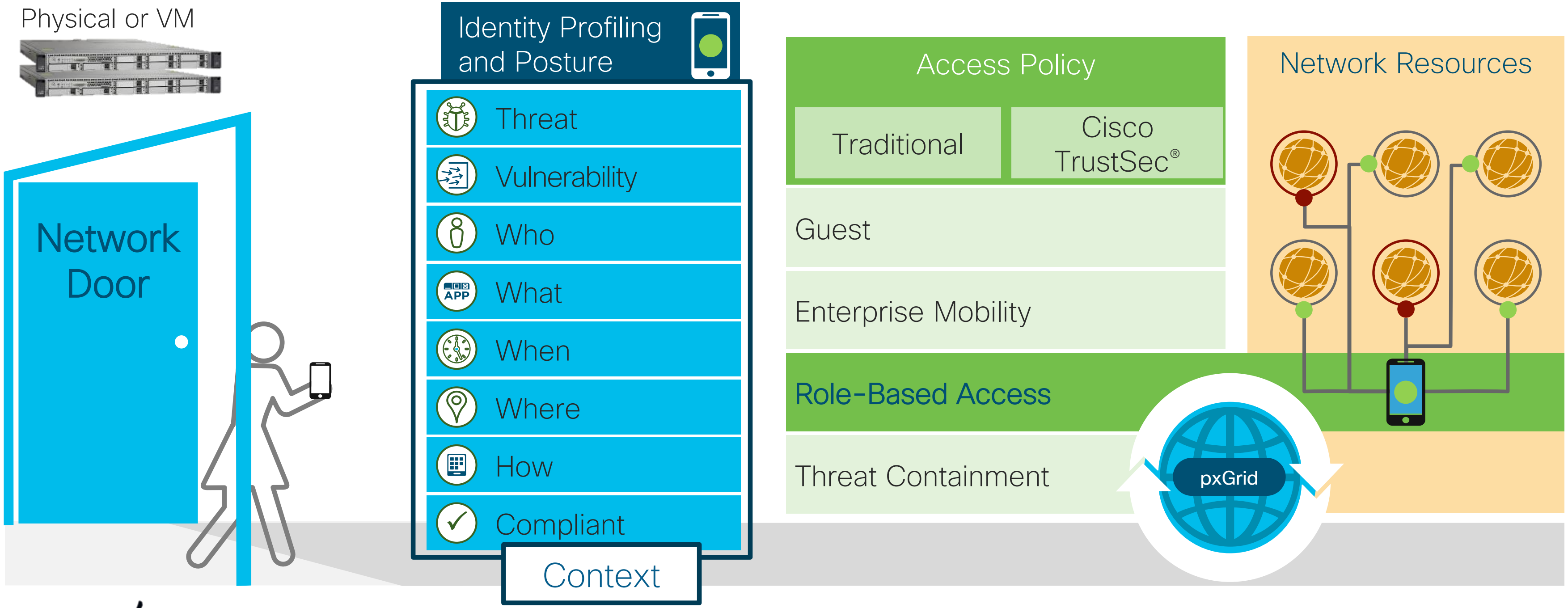
BYOD Endpoints 1341

Compliance 5109



Cisco Identity Services Engine (ISE)

A centralized security solution that automates context-aware access to network resources and shares contextual data



Physical or VM

Network Door

Identity Profiling and Posture

- Threat
- Vulnerability
- Who
- What
- When
- Where
- How
- Compliant

Context

Access Policy

- Traditional
- Cisco TrustSec®
- Guest
- Enterprise Mobility
- Role-Based Access
- Threat Containment

Network Resources

Cisco Duo Multi-Factor Authentication and the Authentication Proxy

Multi-Factor Authentication (MFA)

How it works:

A user logs in using primary authentication (something they know = username + password).

Duo prompts the user with secondary authentication (something they have = push notification sent via Duo Mobile app on their smartphone).

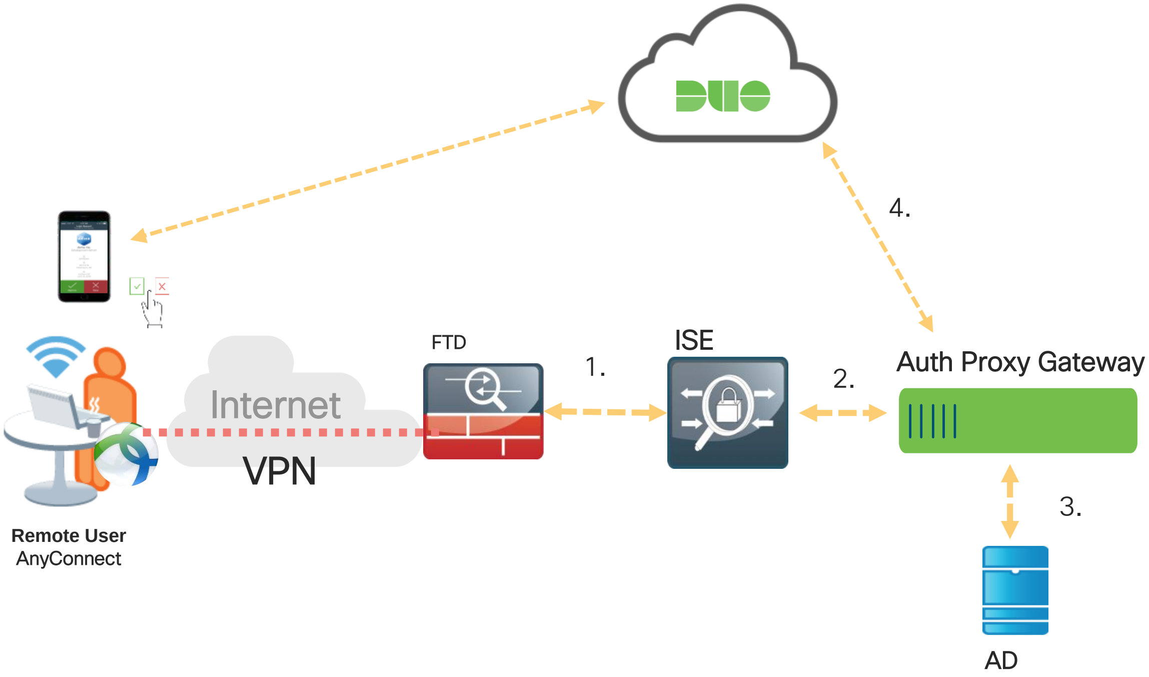
What this does:

- ✓ Prevents identity-based attacks.
- ✓ Thwarts attackers using stolen or compromised passwords.
- ✓ Provides zero-trust access for applications.
- ✓ Creates less reliance on passwords alone.

https://signup.duo.com/

Why is a Secondary Authentication Needed?

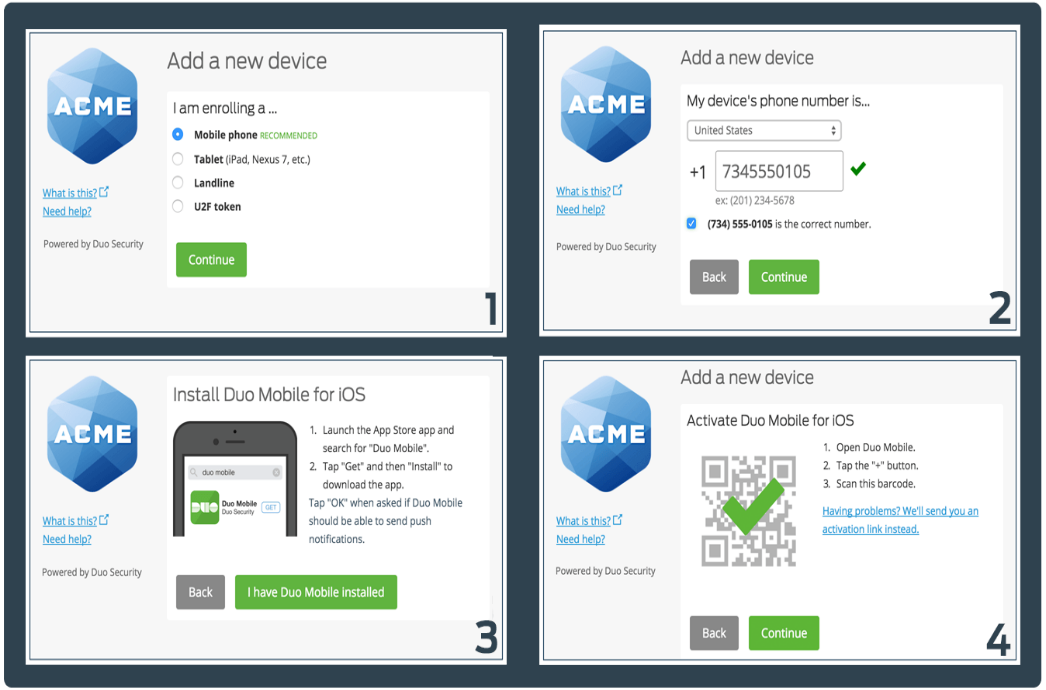
1. Primary authentication initiated to Cisco ISE
2. Cisco ISE sends authentication request to the Duo Authentication Proxy
3. Primary authentication using Active Directory or RADIUS
4. Duo Authentication Proxy connection established to Duo Security over TCP port 443
5. Duo authentication proxy receives authentication response
6. Cisco ISE access granted



Duo User Enrollment

- Automatic enrollment via AD Sync allows Admins to add a group of users and then send them activation links that the user follows to complete their enrollment. Users are created in Duo immediately.
- End User Guide – https://guide.duo.com/enrollment
- Enrollment Documentation – https://duo.com/docs/enrolling-users#overview

- Auto-enrollment
- Self-enrollment
- Manual Enrollment



1

Add a new device

I am enrolling a ...

- ● Mobile phone RECOMMENDED
- ○ Tablet (iPad, Nexus 7, etc.)
- ○ Landline
- ○ U2F token

Continue

What is this? Need help? Powered by Duo Security

2

Add a new device

My device's phone number is...

United States

+1 7345550105 ✓

ex: (201) 234-5678

☑ (734) 555-0105 is the correct number.

Back Continue

3

Install Duo Mobile for iOS

1. Launch the App Store app and search for "Duo Mobile".
2. Tap "Get" and then "Install" to download the app.

Tap "OK" when asked if Duo Mobile should be able to send push notifications.

Back I have Duo Mobile installed

4

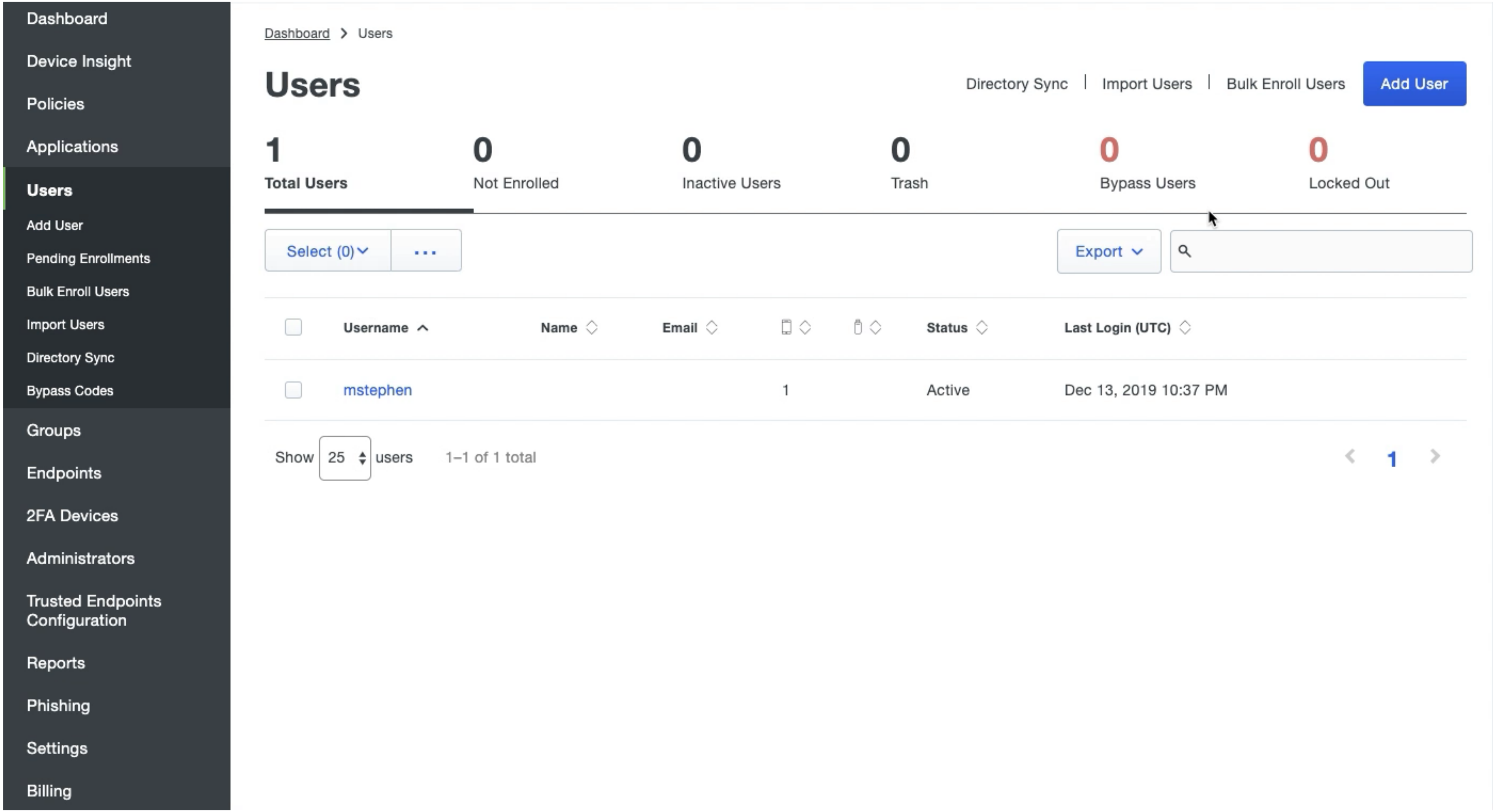
Add a new device

Activate Duo Mobile for iOS

1. Open Duo Mobile.
2. Tap the "+" button.
3. Scan this barcode.

Having problems? We'll send you an activation link instead.

Back Continue



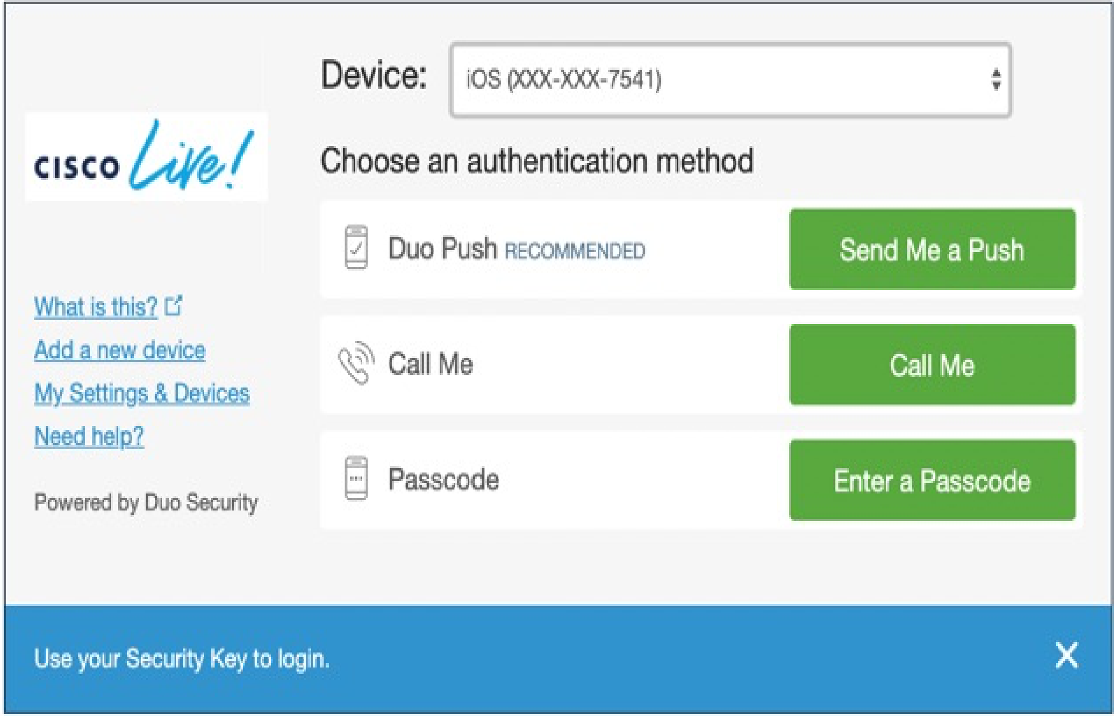
Users

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

□	Username	Name	Email	📱	🔌	Status	Last Login (UTC)
□	mstephen			1		Active	Dec 13, 2019 10:37 PM

Show 25 users 1–1 of 1 total

End User Verification for auth method



Device: iOS (XXX-XXX-7541)

Choose an authentication method

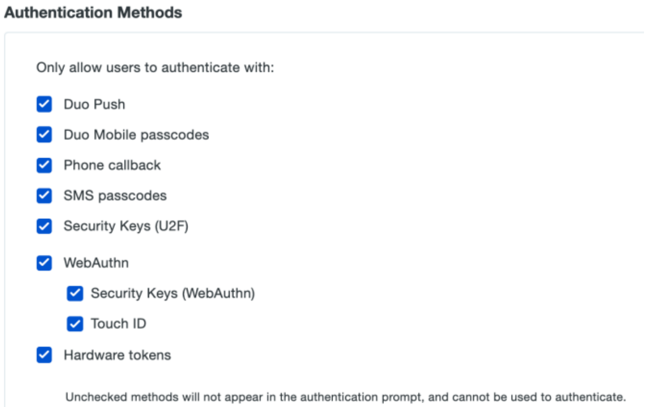
Duo Push RECOMMENDED

Call Me

Passcode

Powered by Duo Security

Use your Security Key to login.



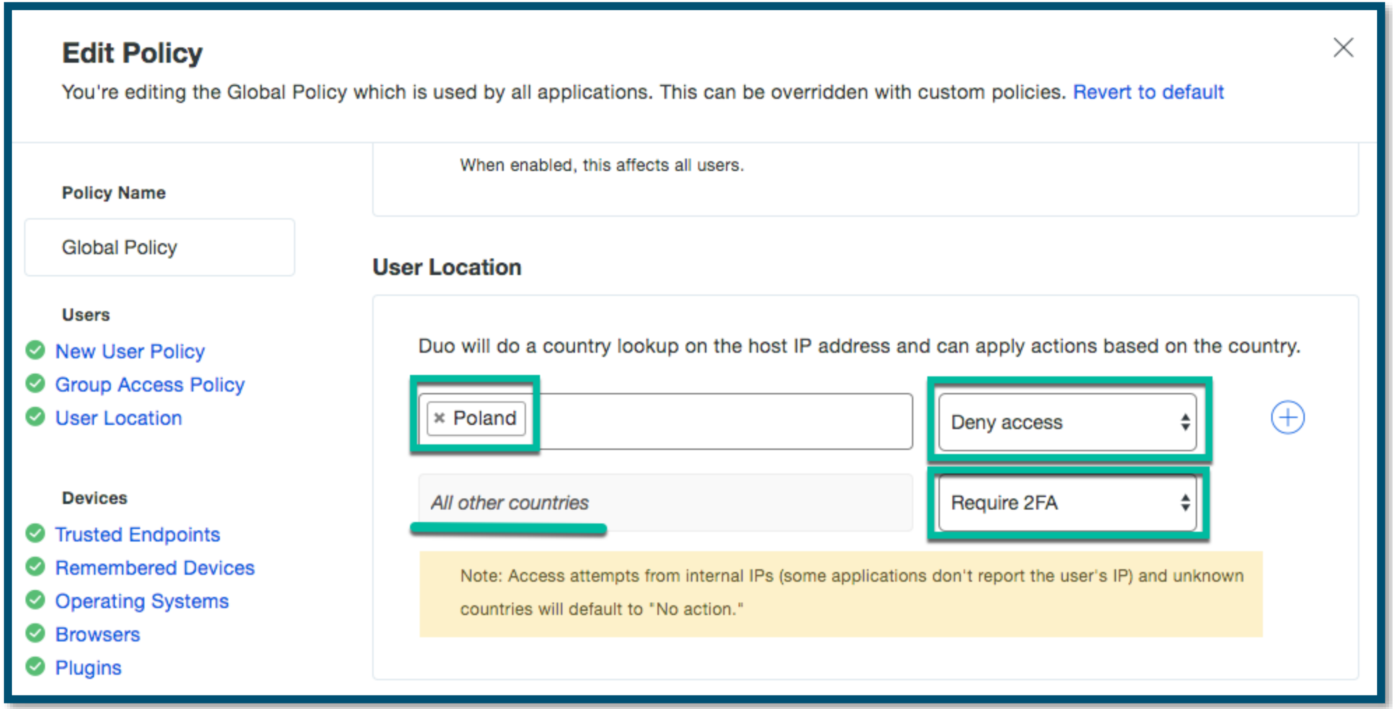
Authentication Methods

Only allow users to authenticate with:

- ☑ Duo Push
- ☑ Duo Mobile passcodes
- ☑ Phone callback
- ☑ SMS passcodes
- ☑ Security Keys (U2F)
- ☑ WebAuthn
  - ☑ Security Keys (WebAuthn)
  - ☑ Touch ID
- ☑ Hardware tokens

Unchecked methods will not appear in the authentication prompt, and cannot be used to authenticate.

Cisco Duo Geo Location Policy



Edit Policy

You're editing the Global Policy which is used by all applications. This can be overridden with custom policies. Revert to default

Policy Name

Global Policy

Users

- ✓ New User Policy
- ✓ Group Access Policy
- ✓ User Location

Devices

- ✓ Trusted Endpoints
- ✓ Remembered Devices
- ✓ Operating Systems
- ✓ Browsers
- ✓ Plugins

When enabled, this affects all users.

User Location

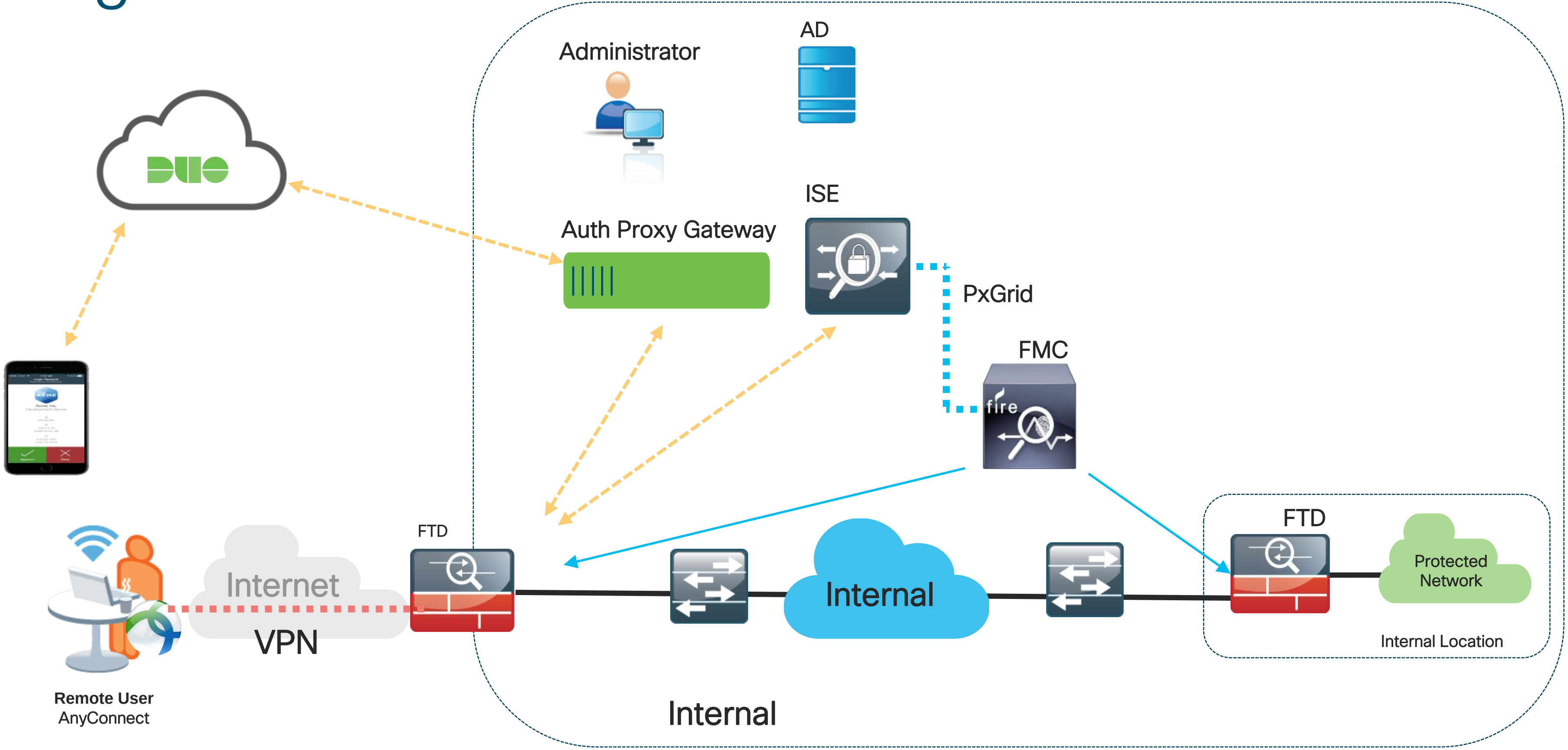
Duo will do a country lookup on the host IP address and can apply actions based on the country.

× Poland	Deny access
All other countries	Require 2FA

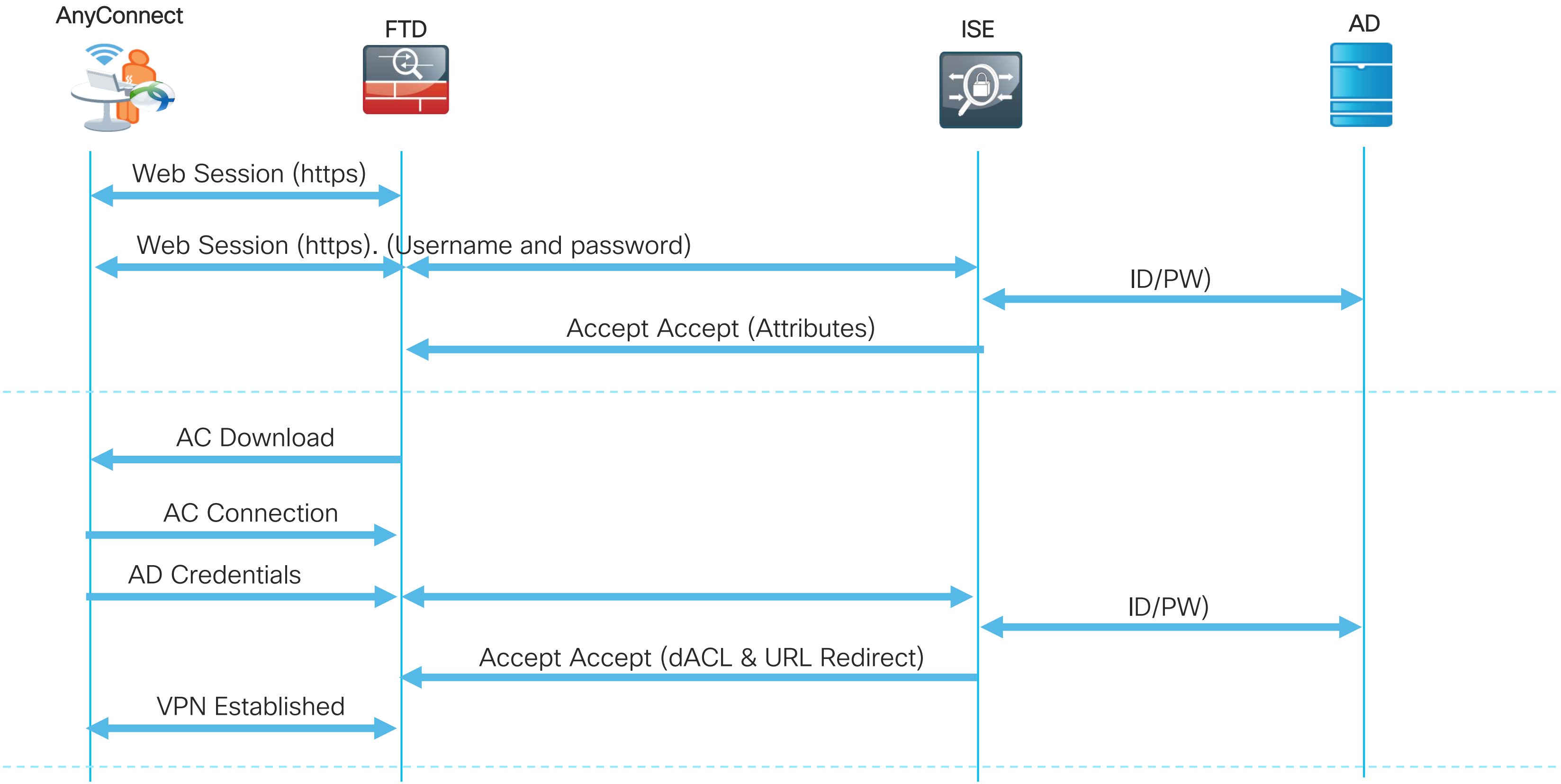
Note: Access attempts from internal IPs (some applications don't report the user's IP) and unknown countries will default to "No action."

Steps for success

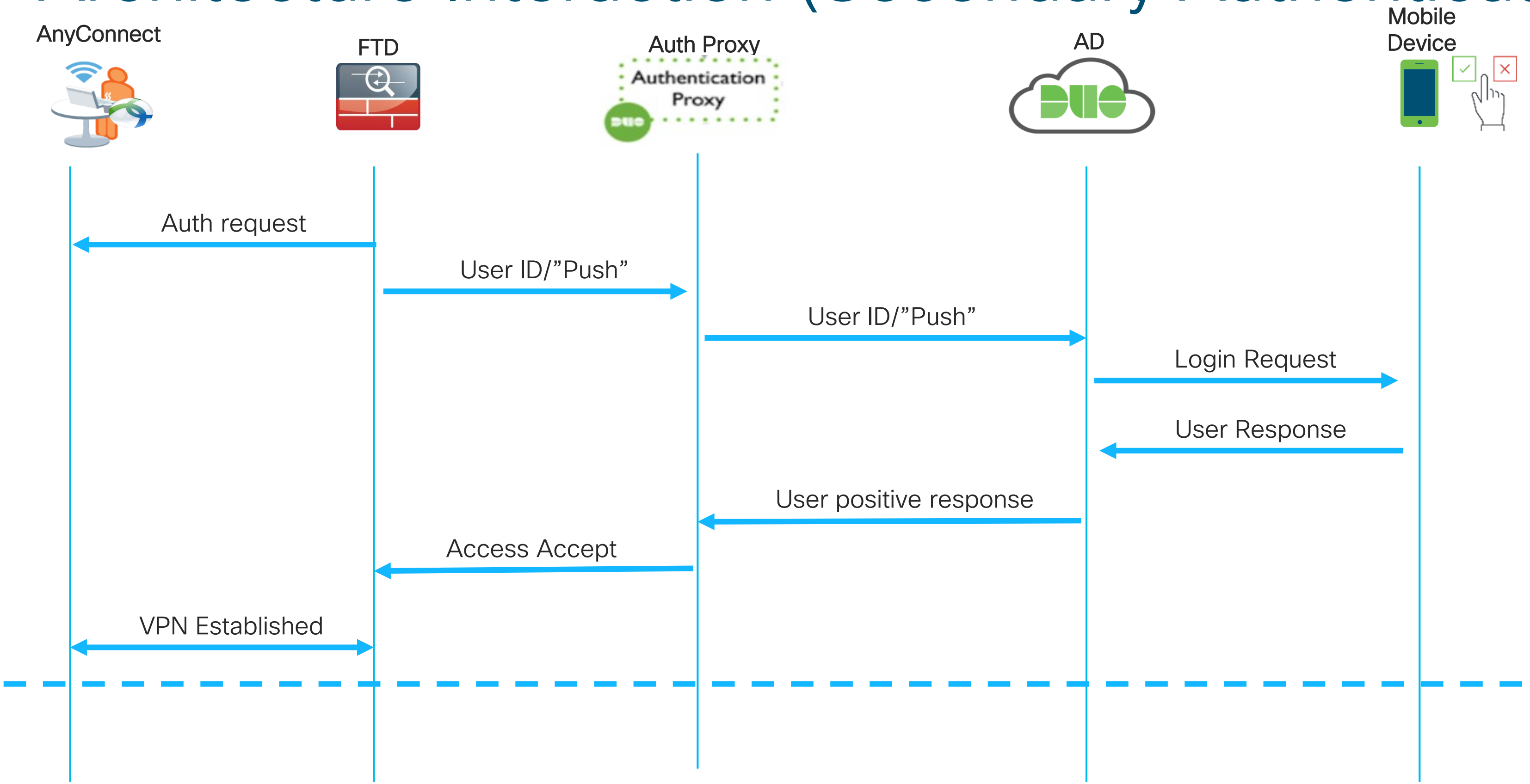
Big Picture Architecture



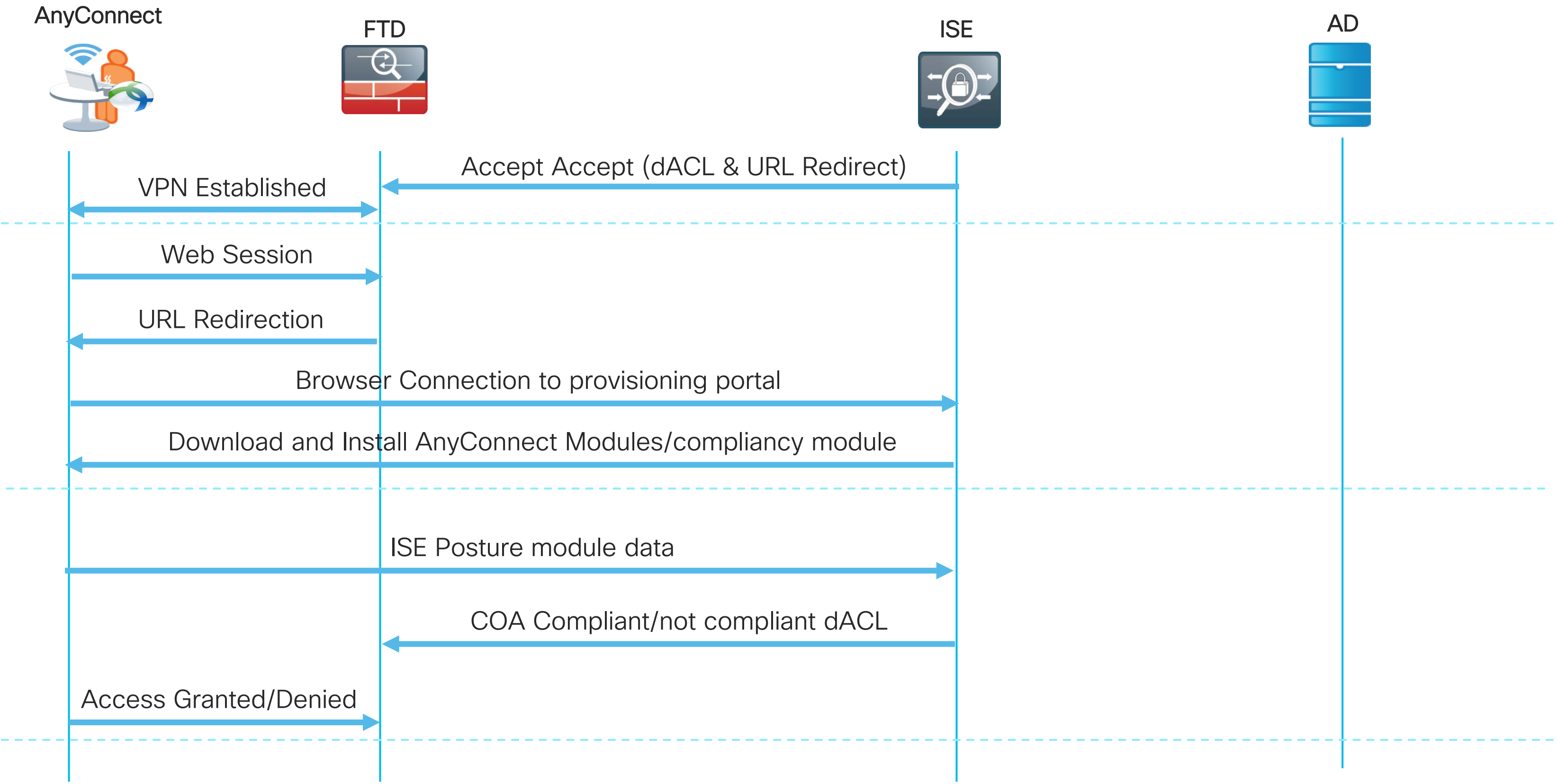
Architecture Interaction


AnyConnect
FTD
ISE
AD
Web Session (https)
Web Session (https). (Username and password)
ID/PW)
Accept Accept (Attributes)
AC Download
AC Connection
AD Credentials
ID/PW)
Accept Accept (dACL & URL Redirect)
VPN Established

Architecture Interaction (Secondary Authentication)



Architecture Interaction

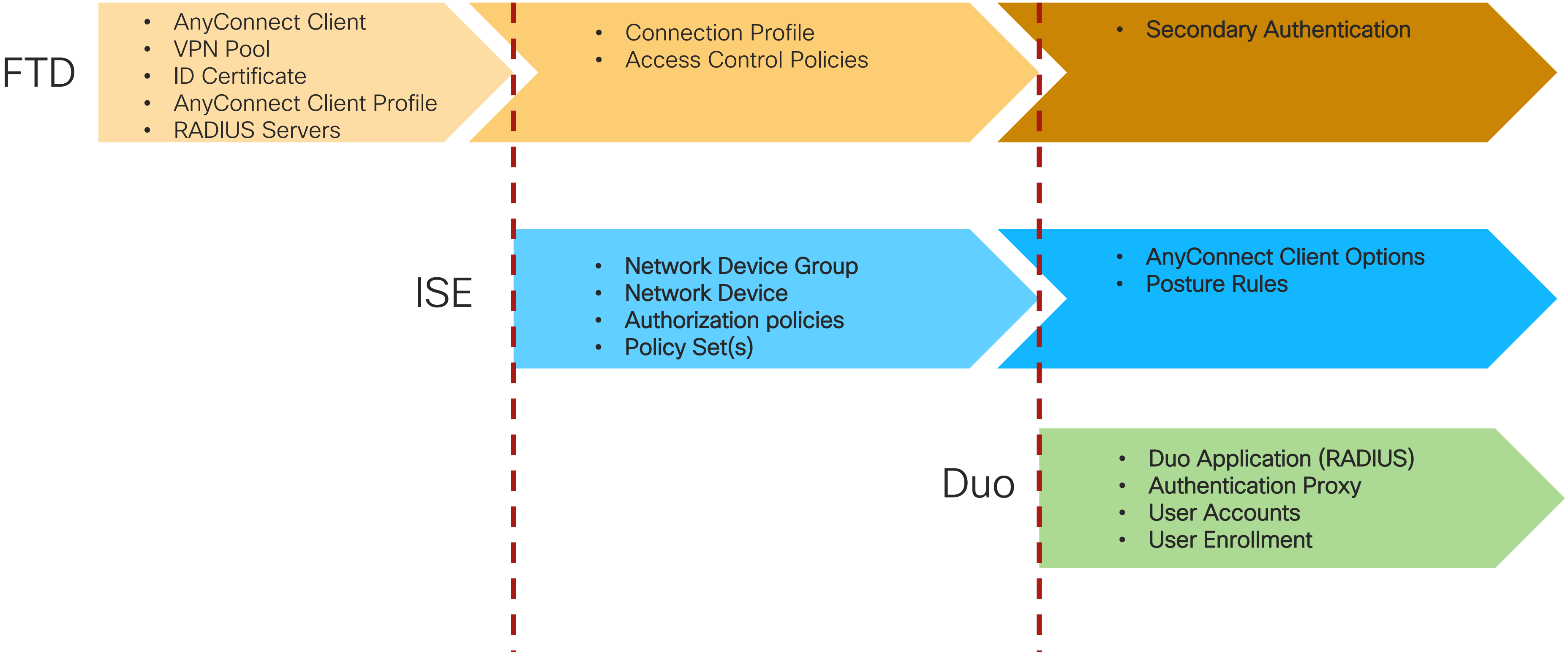

AnyConnect
FTD
ISE
AD
Accept Accept (dACL & URL Redirect)
VPN Established
Web Session
URL Redirection
Browser Connection to provisioning portal
Download and Install AnyConnect Modules/compliancy module
ISE Posture module data
COA Compliant/not compliant dACL
Access Granted/Denied

Configuration Down and Dirty

A journey of a 1000 miles starts with one step

Lao Tzu

Roadmap to configuring



FTD

- AnyConnect Client
- VPN Pool
- ID Certificate
- AnyConnect Client Profile
- RADIUS Servers

- Connection Profile
- Access Control Policies

- Secondary Authentication

ISE

- Network Device Group
- Network Device
- Authorization policies
- Policy Set(s)

- AnyConnect Client Options
- Posture Rules

Duo

- Duo Application (RADIUS)
- Authentication Proxy
- User Accounts
- User Enrollment

Polzeath Beach

Licensing the whole solution

AnyConnect

FTD

ISE

Duo MFA

Licensing the whole solution

AnyConnect – Plus License

- **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
- Basic endpoint context collection
- IEEE 802.1X Windows supplicant
- Cisco Cloud Web Security agent for Windows and Mac OS X platforms (Cloud Web Security services are licensed separately.)
- Cisco Umbrella Roaming agent for Windows and Mac OS X platforms (Umbrella Roaming services are licensed separately.)
- FIPS compliance

Cisco AnyConnect

Ordering Guide

March 2017

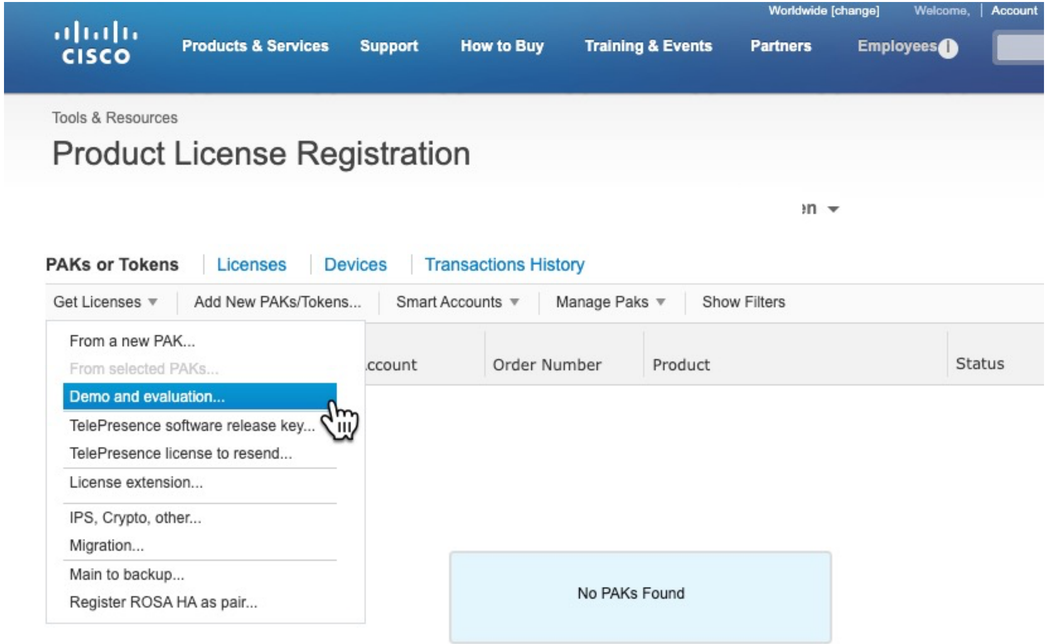
Term License: L-AC-PLS-LIC= 1,3 or 5 years

https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

Licensing the whole solution

Requesting Demo licenses

https://www.cisco.com/go/license



Worldwide [change] Welcome, | Account

Products & Services Support How to Buy Training & Events Partners Employees

Tools & Resources

Product License Registration

PAKs or Tokens | Licenses | Devices | Transactions History

Get Licenses ▾ | Add New PAKs/Tokens... | Smart Accounts ▾ | Manage Paks ▾ | Show Filters

- From a new PAK...
- From selected PAKs...
- Demo and evaluation...
- TelePresence software release key...
- TelePresence license to resend...
- License extension...
- IPS, Crypto, other...
- Migration...
- Main to backup...
- Register ROSA HA as pair...

ccount | Order Number | Product | Status

No PAKs Found

If the above link is not available, you may send an email to:

licensing@cisco.com

Licensing the whole solution

AnyConnect –Apex License

- 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 multicontext-mode remote access
- SAML Authentication (new in 4.4 with ASA 9.7.1 or later)
- All Plus services described above

Cisco AnyConnect

Term License: L-AC-APX-LIC= 1,3 or 5 years

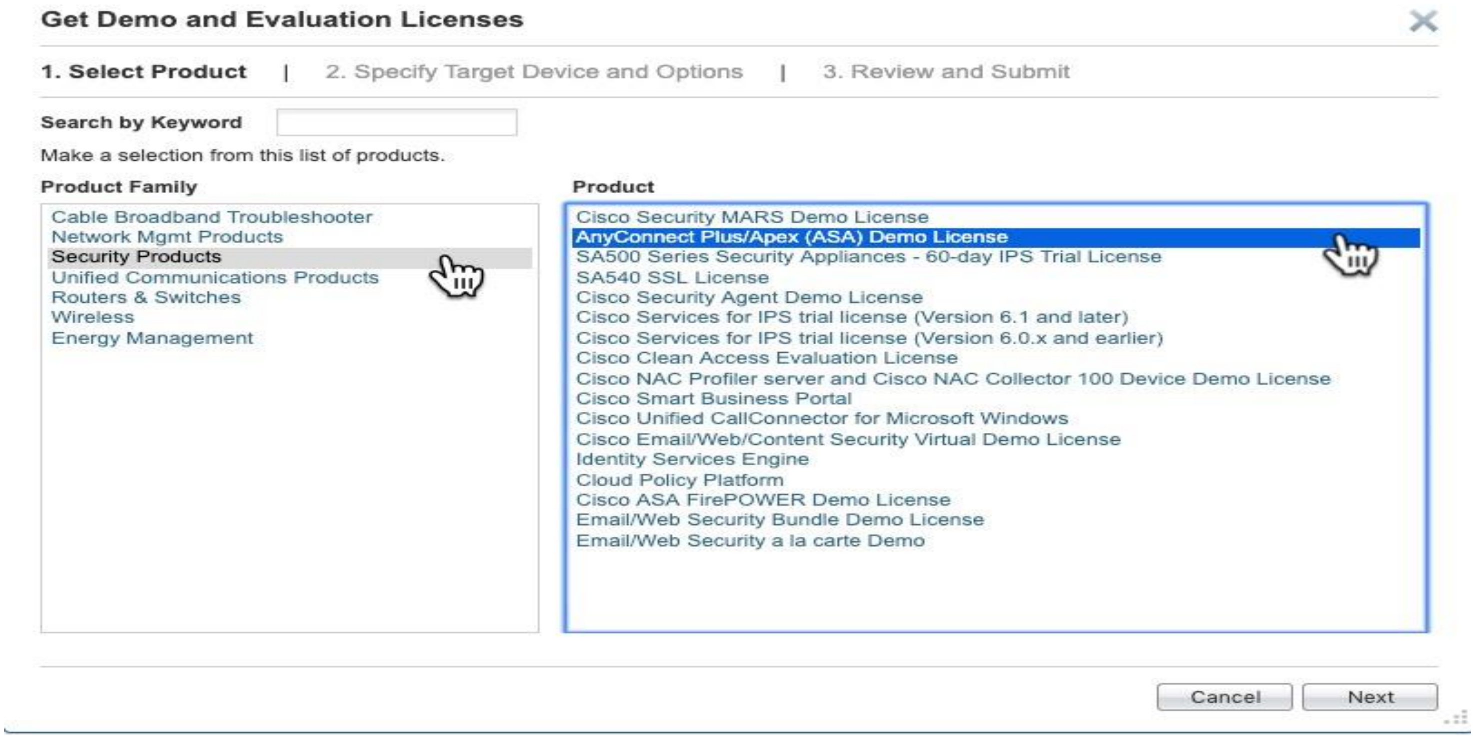
Ordering Guide

https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

March 2017

Licensing the whole solution

Requesting Demo licenses



Get Demo and Evaluation Licenses

1. Select Product | 2. Specify Target Device and Options | 3. Review and Submit

Search by Keyword

Make a selection from this list of products.

Product Family

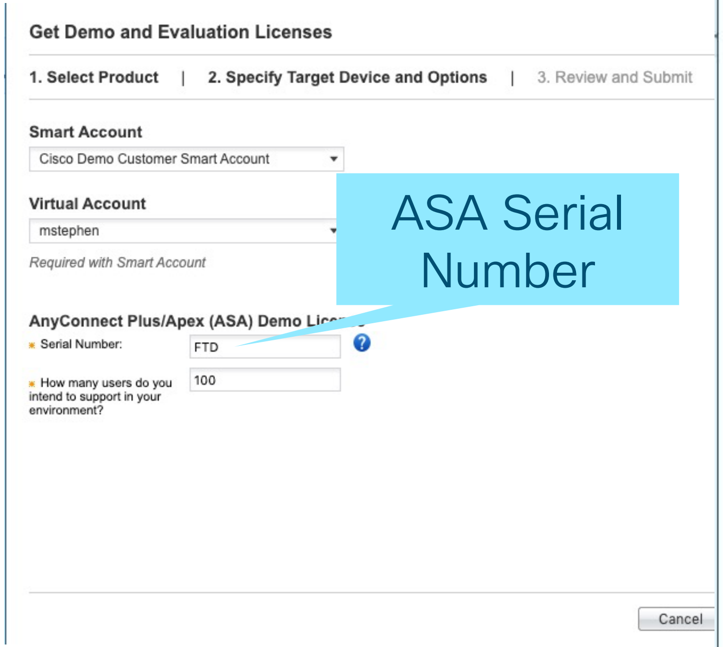
- Cable Broadband Troubleshooter
- Network Mgmt Products
- Security Products
- Unified Communications Products
- Routers & Switches
- Wireless
- Energy Management

Product

- Cisco Security MARS Demo License
- AnyConnect Plus/Apex (ASA) Demo License
- SA500 Series Security Appliances - 60-day IPS Trial License
- SA540 SSL License
- Cisco Security Agent Demo License
- Cisco Services for IPS trial license (Version 6.1 and later)
- Cisco Services for IPS trial license (Version 6.0.x and earlier)
- Cisco Clean Access Evaluation License
- Cisco NAC Profiler server and Cisco NAC Collector 100 Device Demo License
- Cisco Smart Business Portal
- Cisco Unified CallConnector for Microsoft Windows
- Cisco Email/Web/Content Security Virtual Demo License
- Identity Services Engine
- Cloud Policy Platform
- Cisco ASA FirePOWER Demo License
- Email/Web Security Bundle Demo License
- Email/Web Security a la carte Demo

Licensing the whole solution

Requesting Demo licenses



Get Demo and Evaluation Licenses

1. Select Product | **2. Specify Target Device and Options** | 3. Review and Submit

Smart Account

Cisco Demo Customer Smart Account ▾

Virtual Account

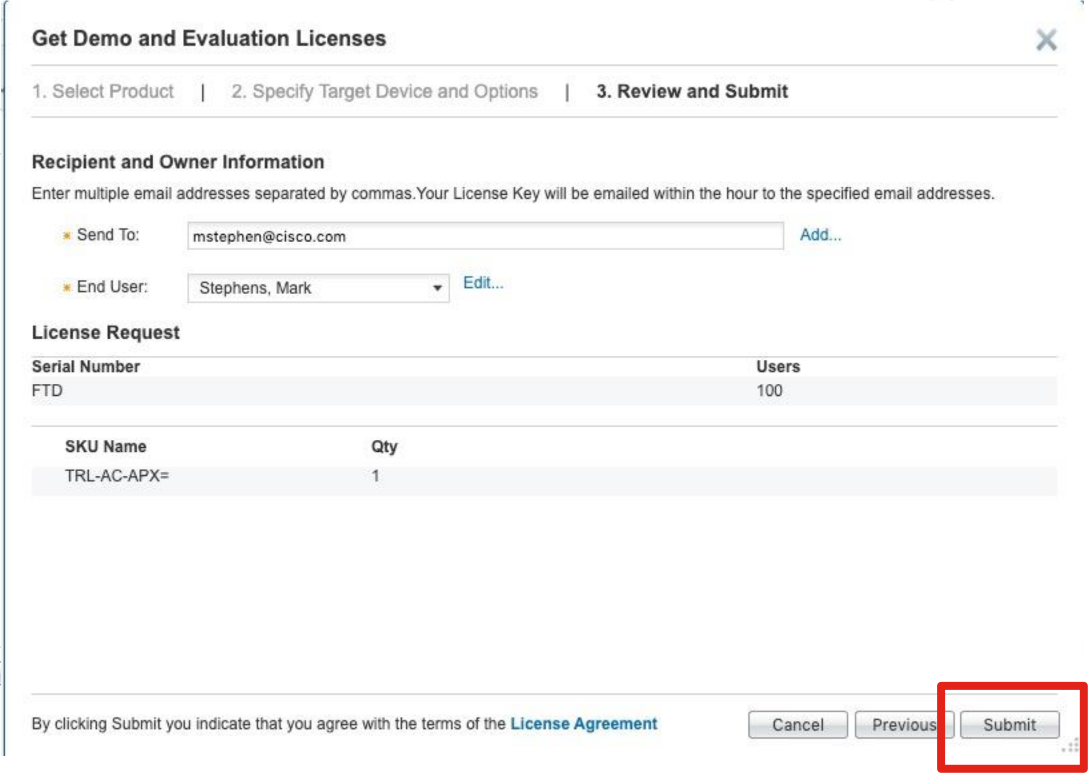
mstephen ▾

Required with Smart Account

AnyConnect Plus/Apex (ASA) Demo Lic

* Serial Number:	FTD
* How many users do you intend to support in your environment?	100

ASA Serial Number



Get Demo and Evaluation Licenses

1. Select Product | 2. Specify Target Device and Options | **3. Review and Submit**

Recipient and Owner Information

Enter multiple email addresses separated by commas.Your License Key will be emailed within the hour to the specified email addresses.

* Send To: mstephen@cisco.com

* End User: Stephens, Mark ▾

License Request

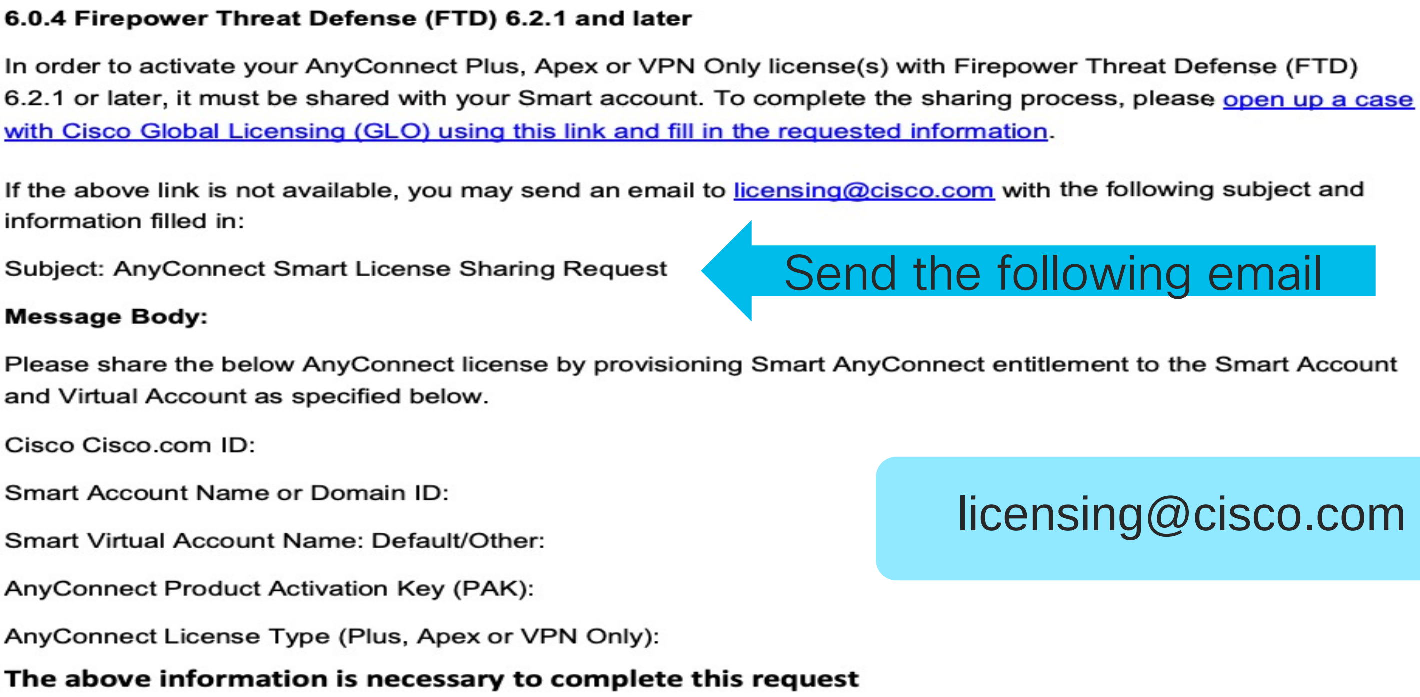
Serial Number	Users
FTD	100

SKU Name	Qty
TRL-AC-APX=	1

By clicking Submit you indicate that you agree with the terms of the **License Agreement**

Licensing the whole solution

Firepower Threat Defense (FTD)



6.0.4 Firepower Threat Defense (FTD) 6.2.1 and later

In order to activate your AnyConnect Plus, Apex or VPN Only license(s) with Firepower Threat Defense (FTD) 6.2.1 or later, it must be shared with your Smart account. To complete the sharing process, please open up a case with Cisco Global Licensing (GLO) using this link and fill in the requested information.

If the above link is not available, you may send an email to licensing@cisco.com with the following subject and information filled in:

Subject: AnyConnect Smart License Sharing Request

Message Body:

Please share the below AnyConnect license by provisioning Smart AnyConnect entitlement to the Smart Account and Virtual Account as specified below.

Cisco Cisco.com ID:

Smart Account Name or Domain ID:

Smart Virtual Account Name: Default/Other:

AnyConnect Product Activation Key (PAK):

AnyConnect License Type (Plus, Apex or VPN Only):

The above information is necessary to complete this request

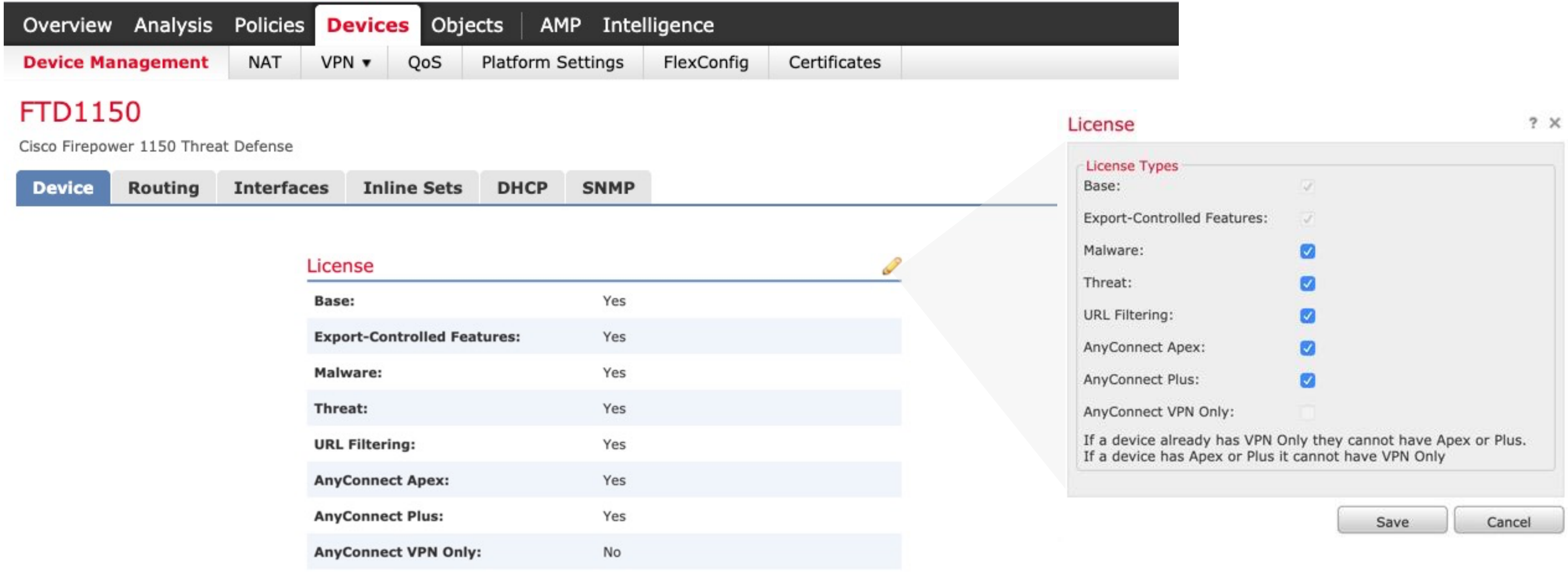
Send the following email

licensing@cisco.com

Licensing the whole solution

Firepower Threat Defense

Devices>Device management>Device



FTD1150

Cisco Firepower 1150 Threat Defense

License

Base:	Yes
Export-Controlled Features:	Yes
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes
AnyConnect Apex:	Yes
AnyConnect Plus:	Yes
AnyConnect VPN Only:	No

License

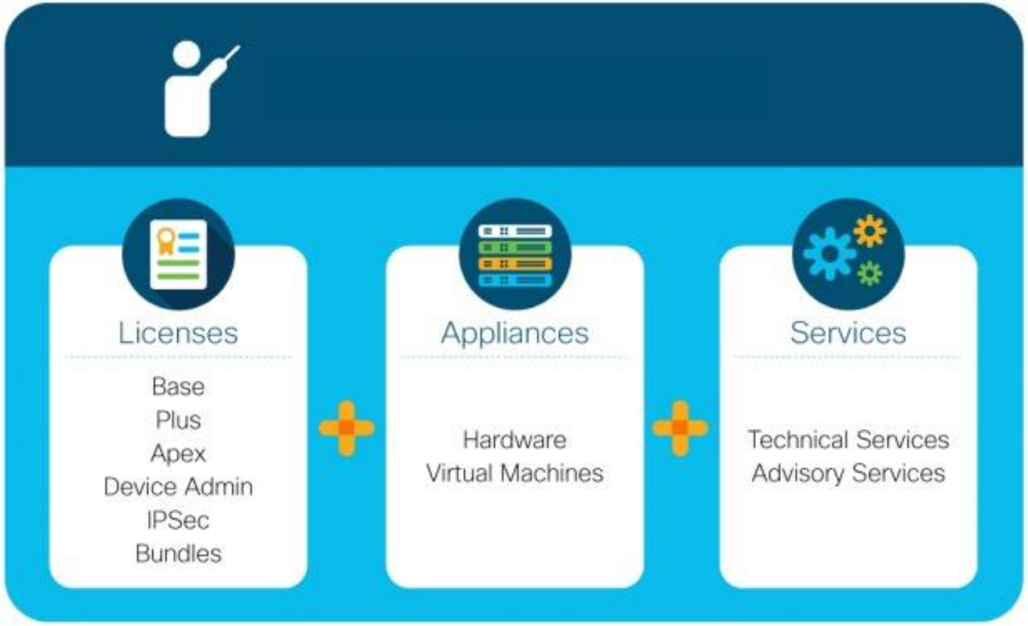
License Types

Base:	☑
Export-Controlled Features:	☑
Malware:	☑
Threat:	☑
URL Filtering:	☑
AnyConnect Apex:	☑
AnyConnect Plus:	☑
AnyConnect VPN Only:	□

If a device already has VPN Only they cannot have Apex or Plus.
If a device has Apex or Plus it cannot have VPN Only

Licensing the whole solution

ISE



Licenses

Base
Plus
Apex
Device Admin
IPSec
Bundles

Appliances

Hardware
Virtual Machines

Services

Technical Services
Advisory Services

Cisco Identity Services Engine

Ordering Guide

November 2019

☑ Base licensing User

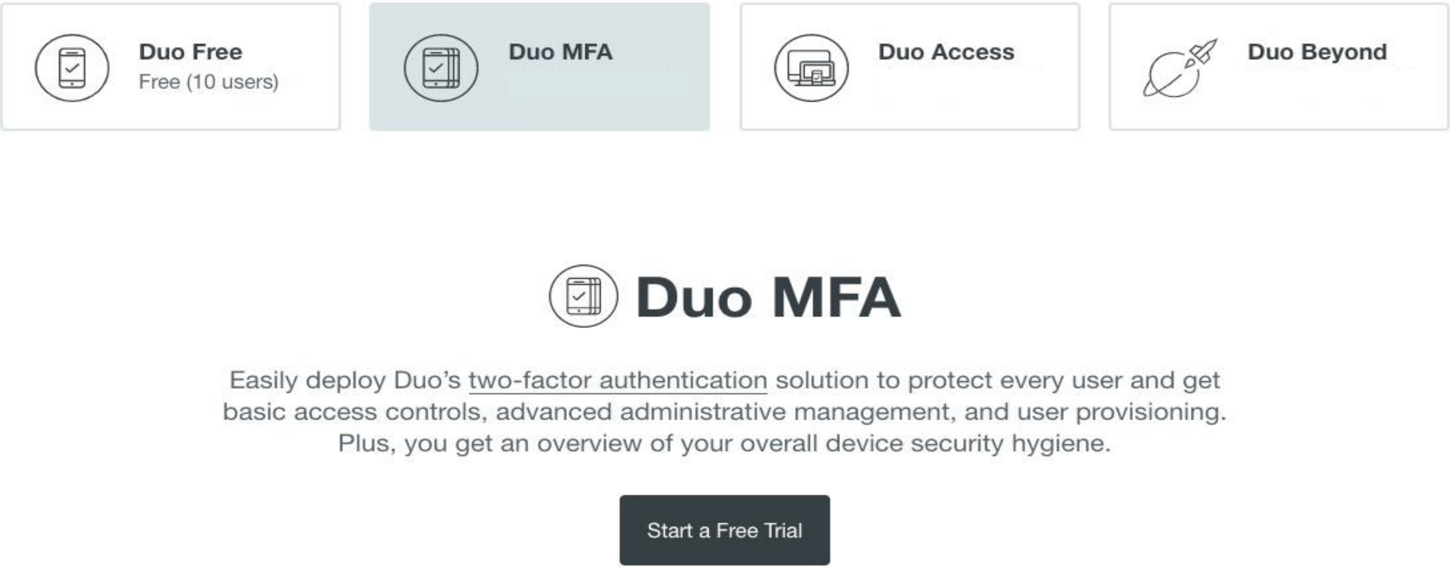
☑ Plus licensing PxGrid

☑ Apex licensing Posture

https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/guide_c07-656177.pdf

Licensing the whole solution

Duo



Duo MFA

Easily deploy Duo's two-factor authentication solution to protect every user and get basic access controls, advanced administrative management, and user provisioning. Plus, you get an overview of your overall device security hygiene.

https://duo.com/pricing/duo-mfa

Licensing the whole solution

AnyConnect

FTD

ISE

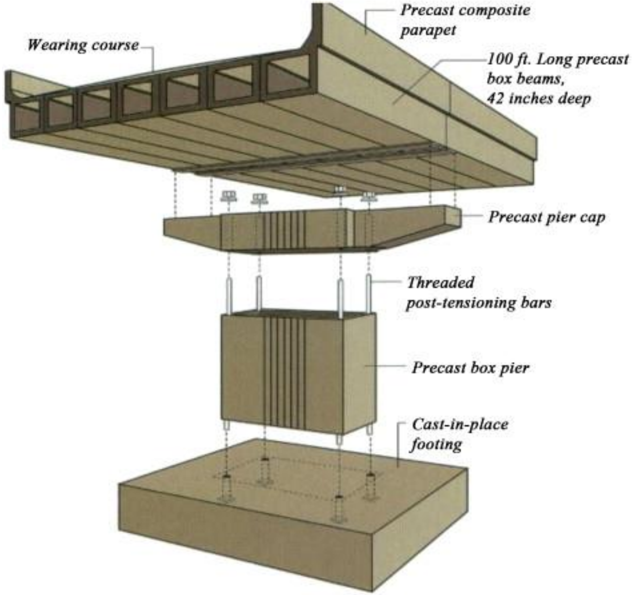
Duo MFA

Polzeath Beach

FTD Configuration

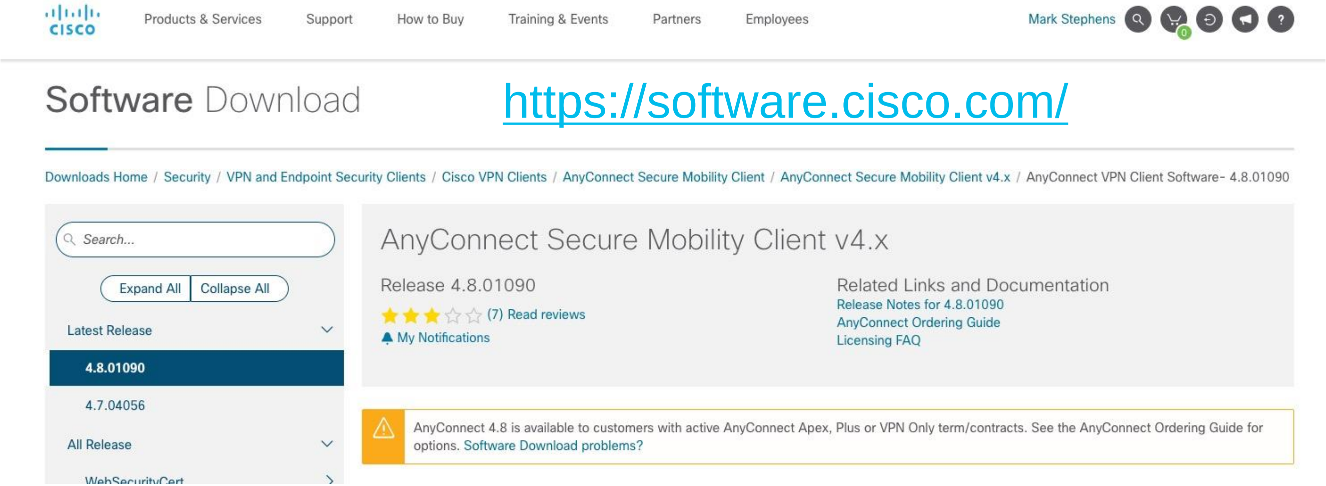
FMC Building Blocks

- AnyConnect Clients
- VPN Pool
- ID Certificate
- AnyConnect Client Profile
- Redirect ACL
- RADIUS Servers


Precast composite parapet
Wearing course
100 ft. Long precast box beams, 42 inches deep
Precast pier cap
Threaded post-tensioning bars
Precast box pier
Cast-in-place footing

FMC Building Blocks

AnyConnect Client



Software Download

https://software.cisco.com/

Downloads Home / Security / VPN and Endpoint Security Clients / Cisco VPN Clients / AnyConnect Secure Mobility Client / AnyConnect Secure Mobility Client v4.x / AnyConnect VPN Client Software- 4.8.01090

AnyConnect Secure Mobility Client v4.x

Release 4.8.01090

★★★☆☆ (7) Read reviews

My Notifications

Related Links and Documentation

Release Notes for 4.8.01090

AnyConnect Ordering Guide

Licensing FAQ

AnyConnect 4.8 is available to customers with active AnyConnect Apex, Plus or VPN Only term/contracts. See the AnyConnect Ordering Guide for options. Software Download problems?

anyconnect-macos-4.8.01090-webdeploy-k9.pkg

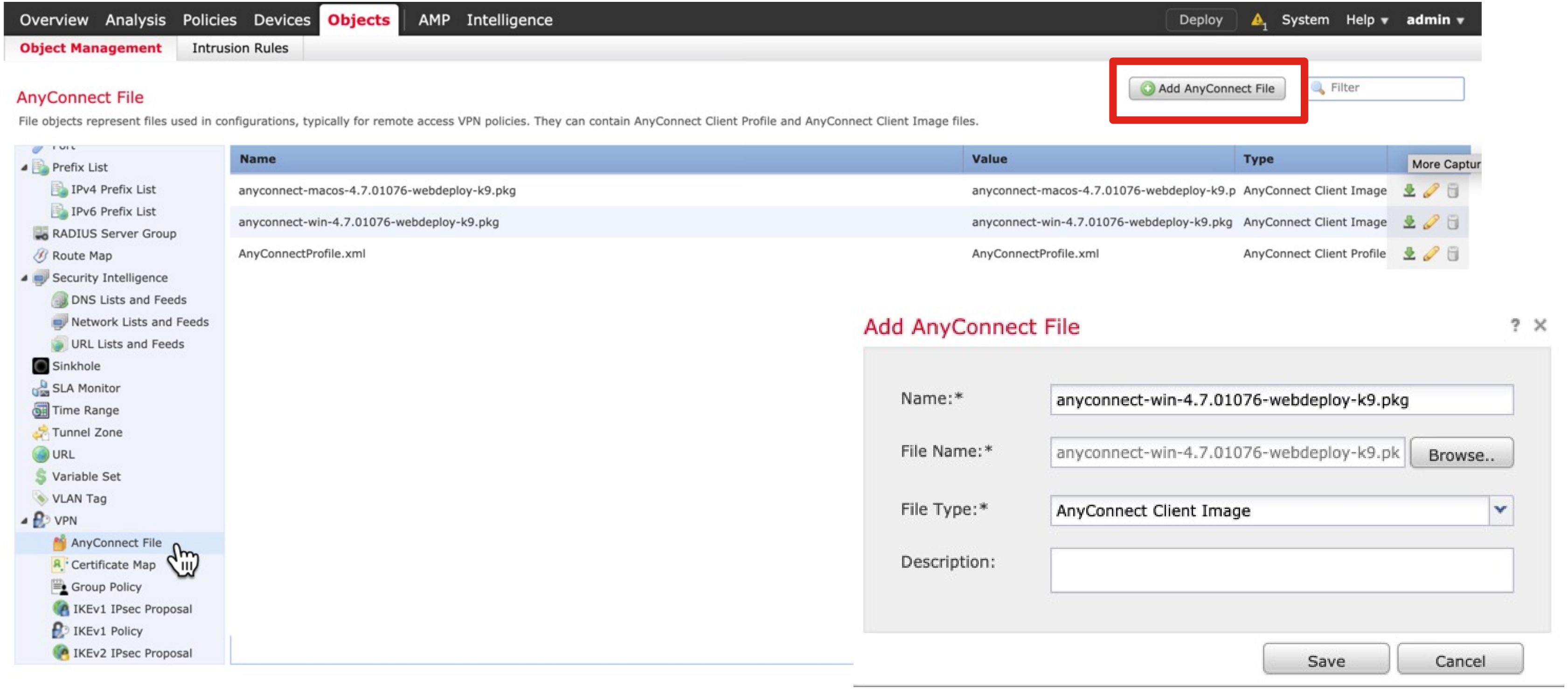
anyconnect-linux64-4.8.01090-webdeploy-k9.pkg

anyconnect-win-4.8.01090-webdeploy-k9.pkg

FMC Building Blocks

AnyConnect Client

Objects>Object Management>VPN>AnyConnect File



AnyConnect File

File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.

Name	Value	Type
anyconnect-macos-4.7.01076-webdeploy-k9.pkg	anyconnect-macos-4.7.01076-webdeploy-k9.p	AnyConnect Client Image
anyconnect-win-4.7.01076-webdeploy-k9.pkg	anyconnect-win-4.7.01076-webdeploy-k9.pkg	AnyConnect Client Image
AnyConnectProfile.xml	AnyConnectProfile.xml	AnyConnect Client Profile

Add AnyConnect File

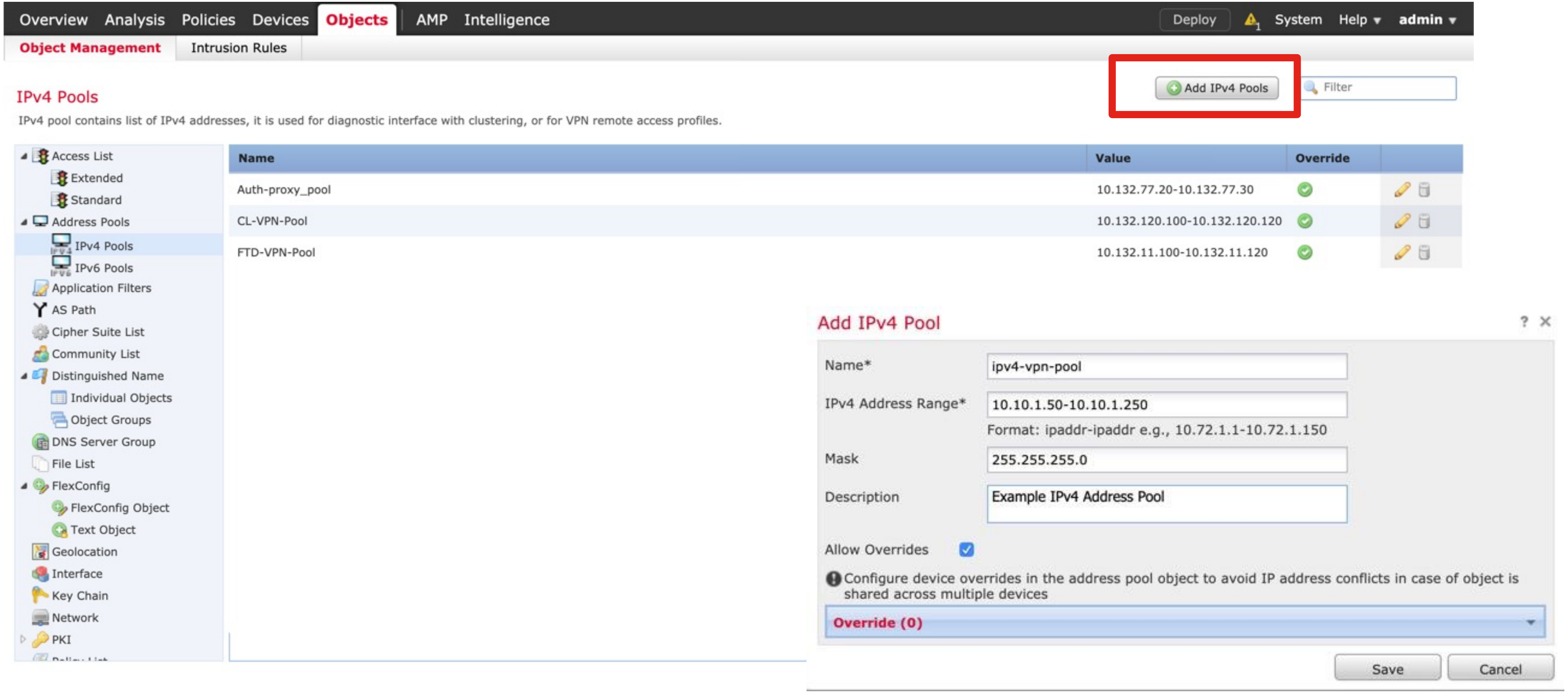
Name:*	anyconnect-win-4.7.01076-webdeploy-k9.pkg
File Name:*	anyconnect-win-4.7.01076-webdeploy-k9.pk Browse..
File Type:*	AnyConnect Client Image
Description:	

Save Cancel

FMC Building Blocks

VPN Pool

Objects>Object Management>Address Pool>IPv4 Pools



IPv4 Pools

IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.

Name	Value	Override
Auth-proxy_pool	10.132.77.20-10.132.77.30	✓
CL-VPN-Pool	10.132.120.100-10.132.120.120	✓
FTD-VPN-Pool	10.132.11.100-10.132.11.120	✓

Add IPv4 Pool

Name*	ipv4-vpn-pool
IPv4 Address Range*	10.10.1.50-10.10.1.250
	Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150
Mask	255.255.255.0
Description	Example IPv4 Address Pool
Allow Overrides	☑

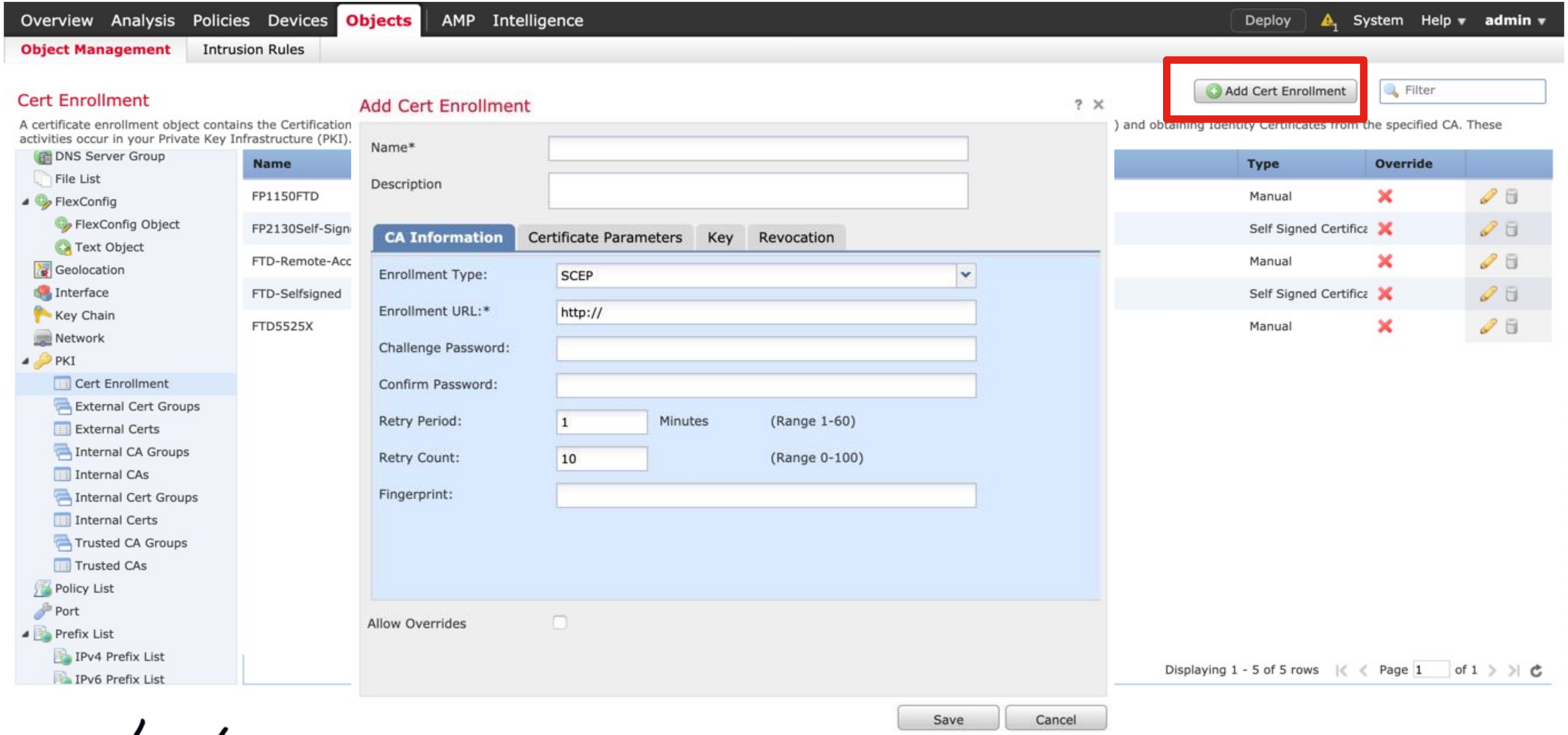
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

FMC Building Blocks

ID Certificate

Objects>Object Management>PKI>Cert Enrollment



Cert Enrollment

A certificate enrollment object contains the Certification ...) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override
FP1150FTD	Manual	✗
FP2130Self-Sign	Self Signed Certifica	✗
FTD-Remote-Acc	Manual	✗
FTD-Selfsigned	Self Signed Certifica	✗
FTD5525X	Manual	✗

Displaying 1 - 5 of 5 rows   Page 1 of 1

Add Cert Enrollment

Name*:

Description:

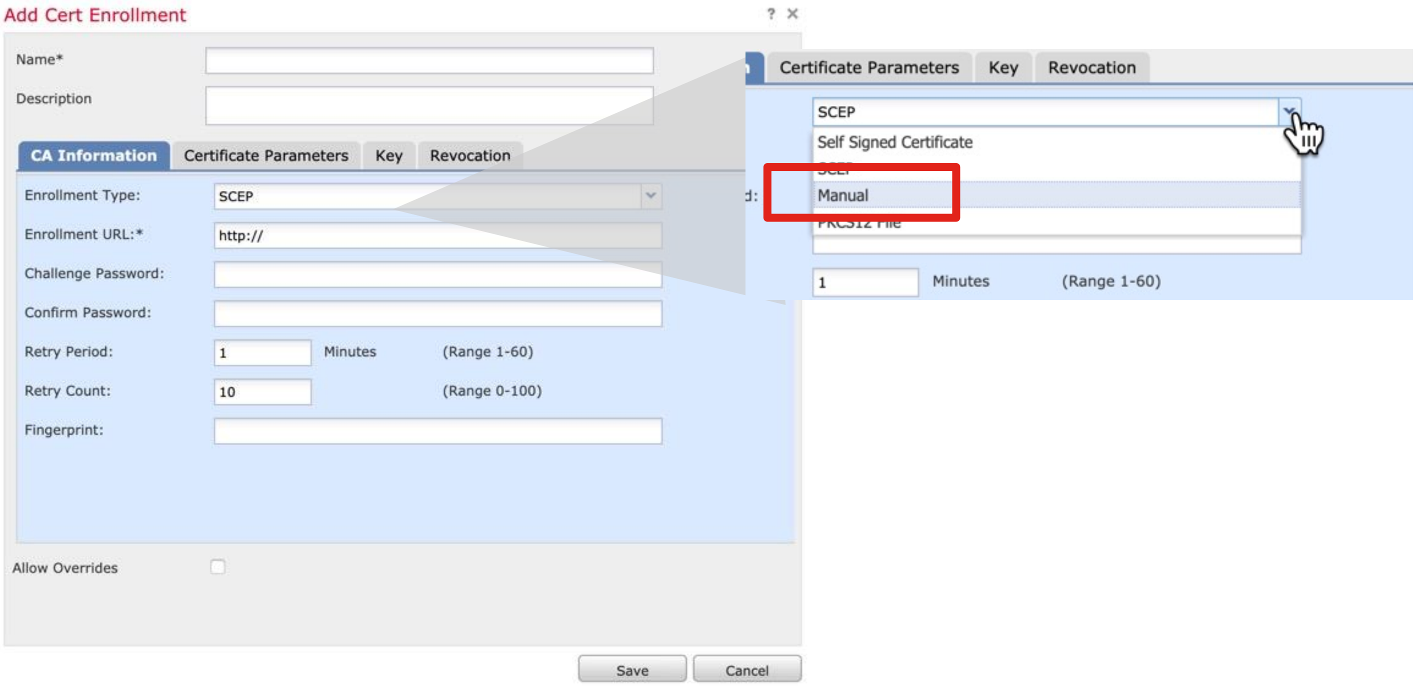
Enrollment Type:	SCEP		
Enrollment URL:*	http://		
Challenge Password:			
Confirm Password:			
Retry Period:	1	Minutes	(Range 1-60)
Retry Count:	10		(Range 0-100)
Fingerprint:			

Allow Overrides □

FMC Building Blocks

ID Certificate

Objects>Object Management>PKI>Cert Enrollment



Add Cert Enrollment

Name*

Description

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type: SCEP

Enrollment URL:* http://

Challenge Password:

Confirm Password:

Retry Period: 1 Minutes (Range 1-60)

Retry Count: 10 (Range 0-100)

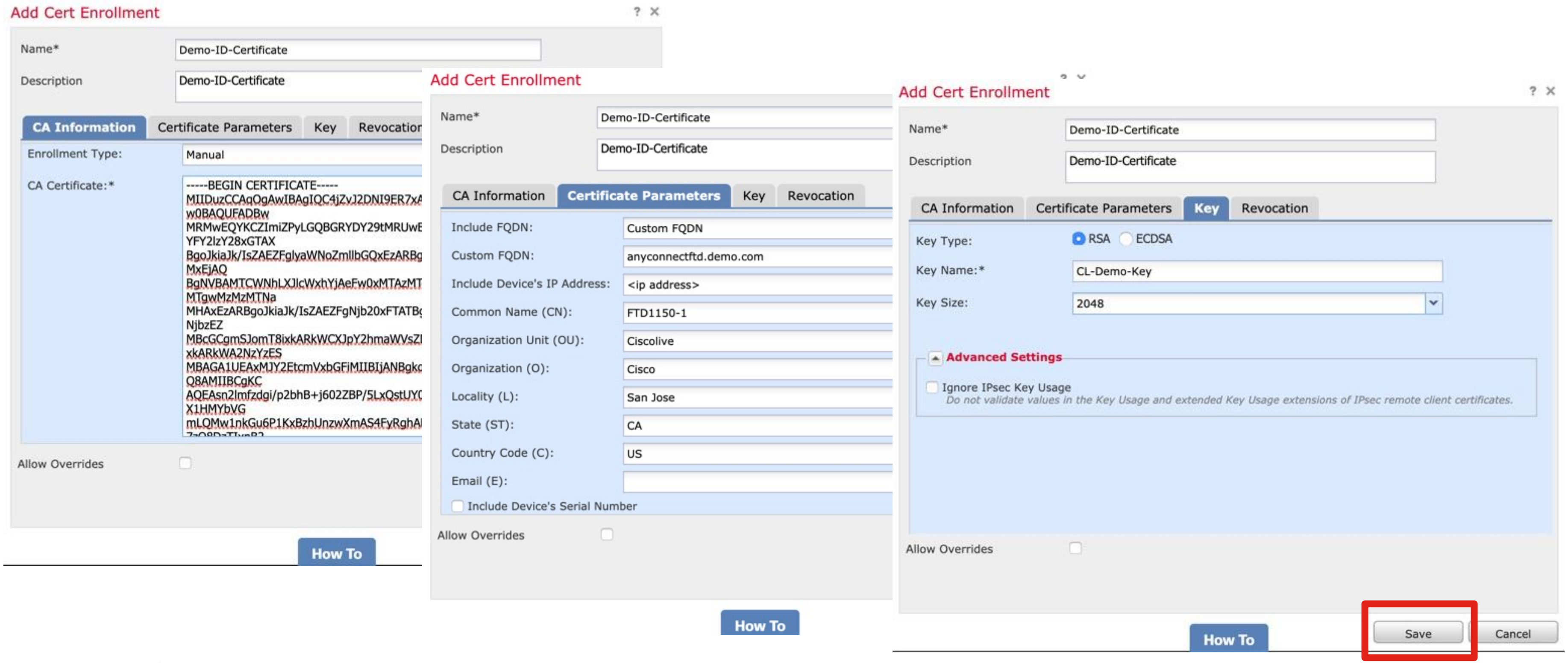
Fingerprint:

Allow Overrides □

FMC Building Blocks

ID Certificate

Objects>Object Management>PKI>Cert Enrollment



Add Cert Enrollment

Name*: Demo-ID-Certificate

Description: Demo-ID-Certificate

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type: Manual

CA Certificate:*

```
-----BEGIN CERTIFICATE-----
MIIDuzCCAqOgAwIBAgIQC4jZvJ2DNI9ER7xA
w0BAQUFADBw
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwE
YFY2lzY28xGTAX
BgoJkiaJk/IsZAEZFglyaWNoZmllbGQxEzARBg
MxEjAQ
BgNVBAMTCWNhLXJlcWxhYjAeFw0xMTAzMT
MTgwMzMzMTNa
MHAxEzARBgoJkiaJk/IsZAEZFgNjb20xFTATBg
NjbzEZ
MBcGCgmSJomT8ixkARkWCXJpY2hmaWVsZI
xkARkWA2NzYzES
MBAGA1UEAxMJY2EtcmVxbGFiMIIBIjANBgkq
Q8AMIIBCgKC
AQEAsn2lmfzdgi/p2bhB+j602ZBP/5LxQstUY0
X1HMYbVG
mLQMw1nkGu6P1KxBzhUnzwXmAS4FyRghAl
```

Allow Overrides □

How To

Add Cert Enrollment

Name*: Demo-ID-Certificate

Description: Demo-ID-Certificate

CA Information | Certificate Parameters | Key | Revocation

Include FQDN: Custom FQDN

Custom FQDN: anyconnectftd.demo.com

Include Device's IP Address: <ip address>

Common Name (CN): FTD1150-1

Organization Unit (OU): Ciscolive

Organization (O): Cisco

Locality (L): San Jose

State (ST): CA

Country Code (C): US

Email (E):

□ Include Device's Serial Number

Allow Overrides □

How To

Add Cert Enrollment

Name*: Demo-ID-Certificate

Description: Demo-ID-Certificate

CA Information | Certificate Parameters | Key | Revocation

Key Type: ● RSA ○ ECDSA

Key Name:* CL-Demo-Key

Key Size: 2048

Advanced Settings

□ Ignore IPsec Key Usage

Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides □

How To

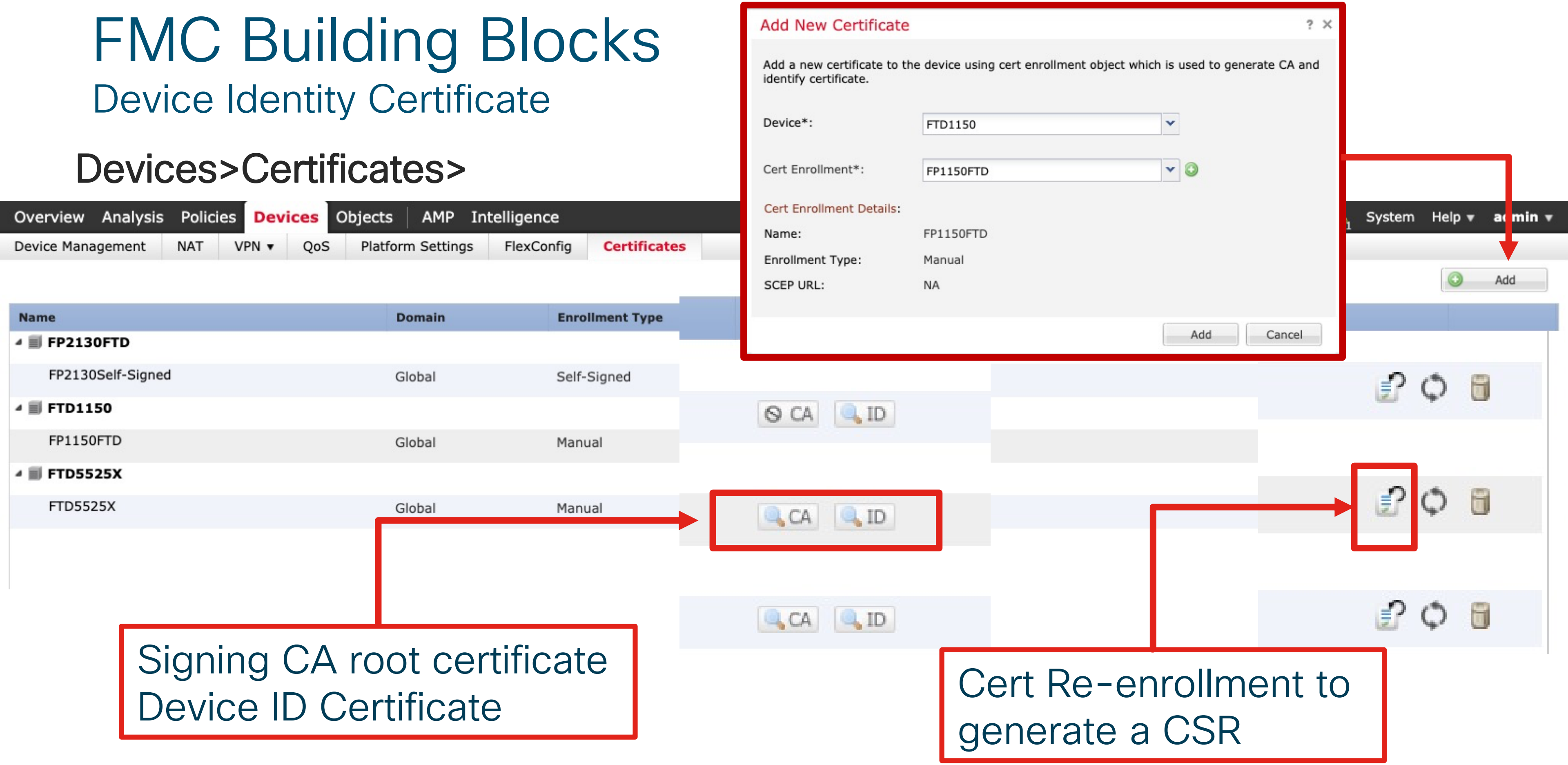
Save

Cancel

FMC Building Blocks

Device Identity Certificate

Devices>Certificates>



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:	FTD1150
Cert Enrollment*:	FP1150FTD

Cert Enrollment Details:

Name:	FP1150FTD
Enrollment Type:	Manual
SCEP URL:	NA

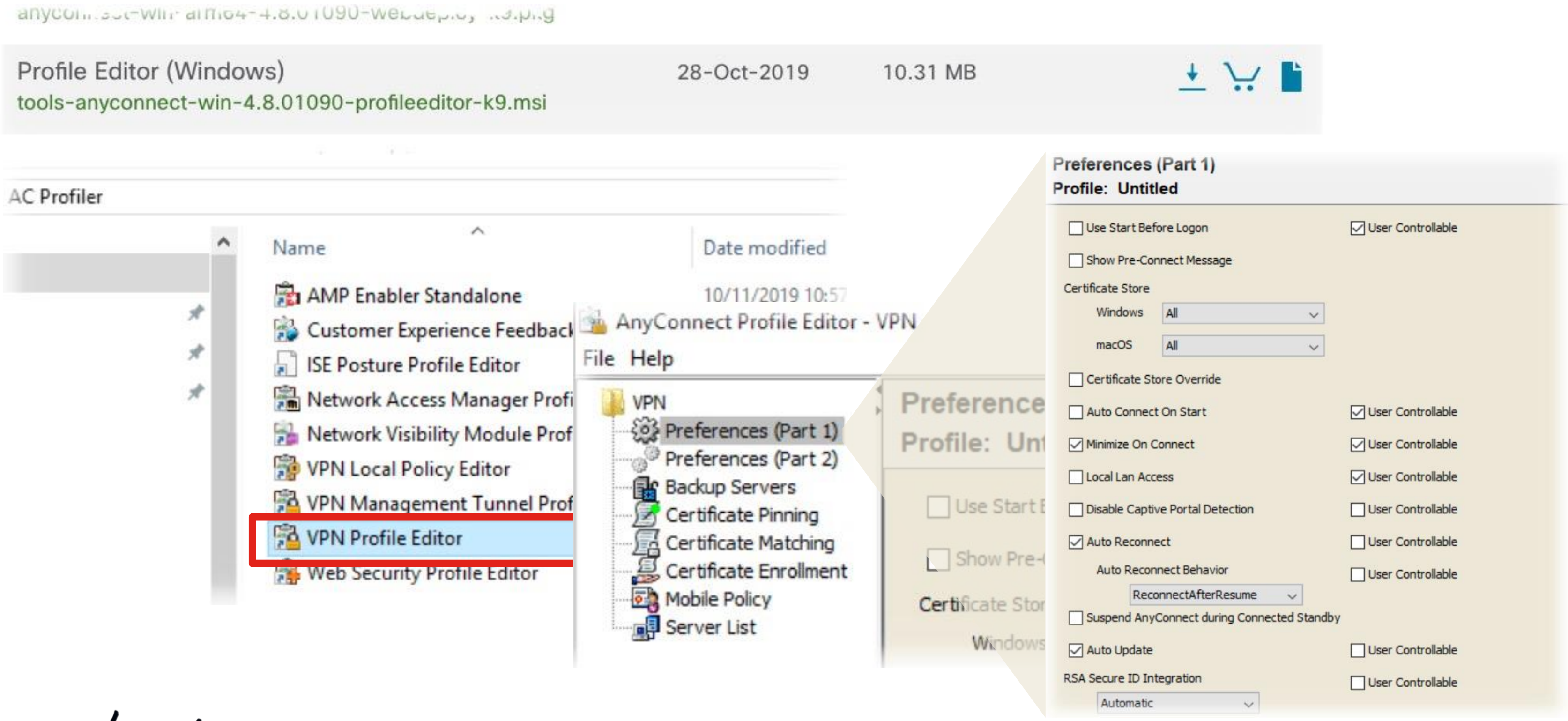
Name	Domain	Enrollment Type
FP2130FTD		
FP2130Self-Signed	Global	Self-Signed
FTD1150		
FP1150FTD	Global	Manual
FTD5525X		
FTD5525X	Global	Manual

Signing CA root certificate Device ID Certificate

Cert Re-enrollment to generate a CSR

FMC Building Blocks

AnyConnect Client Profile Editor



Profile Editor (Windows) 28-Oct-2019 10.31 MB
tools-anyconnect-win-4.8.01090-profileeditor-k9.msi

AC Profiler

Name	Date modified
AMP Enabler Standalone	10/11/2019 10:57
Customer Experience Feedback	
ISE Posture Profile Editor	
Network Access Manager Profi	
Network Visibility Module Prof	
VPN Local Policy Editor	
VPN Management Tunnel Prof	
VPN Profile Editor	
Web Security Profile Editor	

AnyConnect Profile Editor - VPN

File Help

- VPN
  - Preferences (Part 1)
  - Preferences (Part 2)
  - Backup Servers
  - Certificate Pinning
  - Certificate Matching
  - Certificate Enrollment
  - Mobile Policy
  - Server List

Preferences (Part 1)
Profile: Untitled

☐ Use Start Before Logon ☑ User Controllable

☐ Show Pre-Connect Message

Certificate Store

Windows: All

macOS: All

☐ Certificate Store Override

☐ Auto Connect On Start ☑ User Controllable

☑ Minimize On Connect ☑ User Controllable

☐ Local Lan Access ☑ User Controllable

☐ Disable Captive Portal Detection ☐ User Controllable

☑ Auto Reconnect ☐ User Controllable

Auto Reconnect Behavior ☐ User Controllable

ReconnectAfterResume

☐ Suspend AnyConnect during Connected Standby

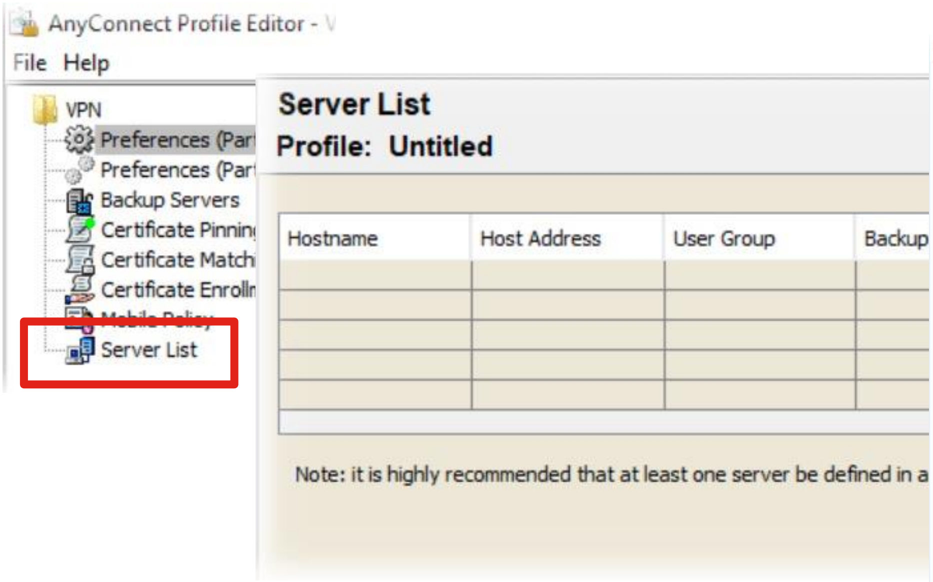
☑ Auto Update ☐ User Controllable

RSA Secure ID Integration ☐ User Controllable

Automatic

FMC Building Blocks

AnyConnect Client Profile Editor (cont)



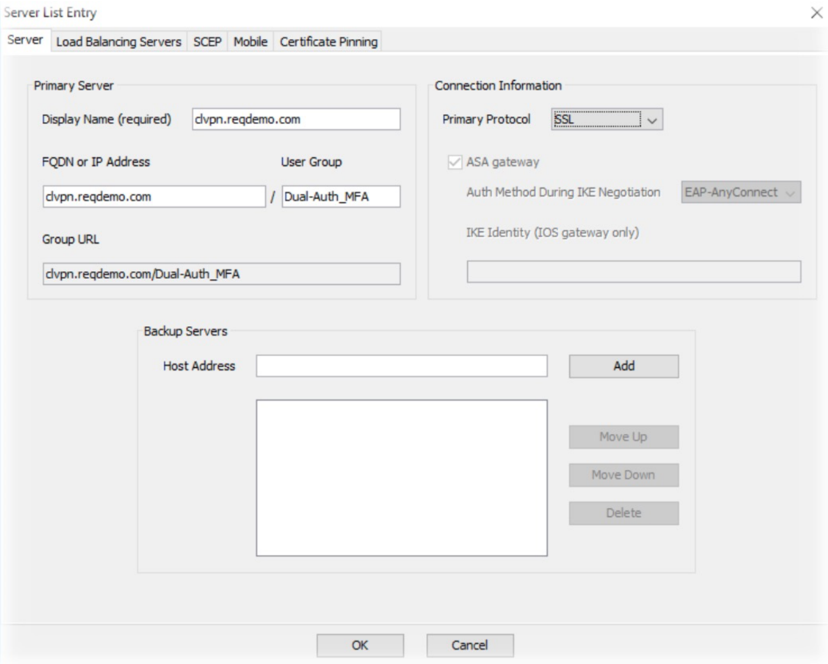
AnyConnect Profile Editor - V

Server List

Profile: Untitled

Hostname	Host Address	User Group	Backup

Note: it is highly recommended that at least one server be defined in a



Server List Entry

Primary Server

Display Name (required): dlvpn.reqdemo.com

FQDN or IP Address / User Group: dlvpn.reqdemo.com / Dual-Auth_MFA

Group URL: dlvpn.reqdemo.com/Dual-Auth_MFA

Connection Information

Primary Protocol: SSL

☑ ASA gateway

Auth Method During IKE Negotiation: EAP-AnyConnect

IKE Identity (IOS gateway only):

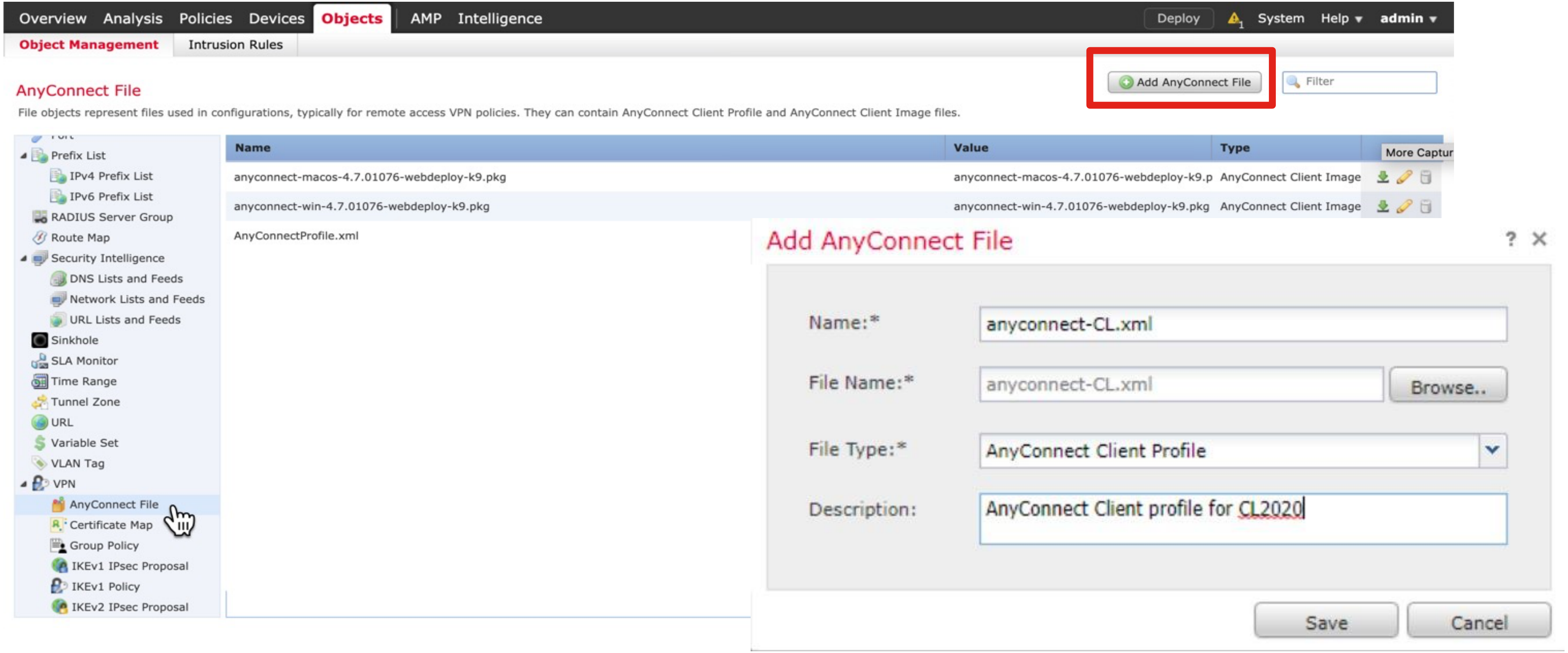
Backup Servers

Host Address:

FMC Building Blocks

AnyConnect Client Profile

Objects>Object Management>VPN>AnyConnect File



AnyConnect File

File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.

Name	Value	Type
anyconnect-macos-4.7.01076-webdeploy-k9.pkg	anyconnect-macos-4.7.01076-webdeploy-k9.p	AnyConnect Client Image
anyconnect-win-4.7.01076-webdeploy-k9.pkg	anyconnect-win-4.7.01076-webdeploy-k9.pkg	AnyConnect Client Image
AnyConnectProfile.xml		

Add AnyConnect File

Name:* anyconnect-CL.xml

File Name:* anyconnect-CL.xml Browse..

File Type:* AnyConnect Client Profile

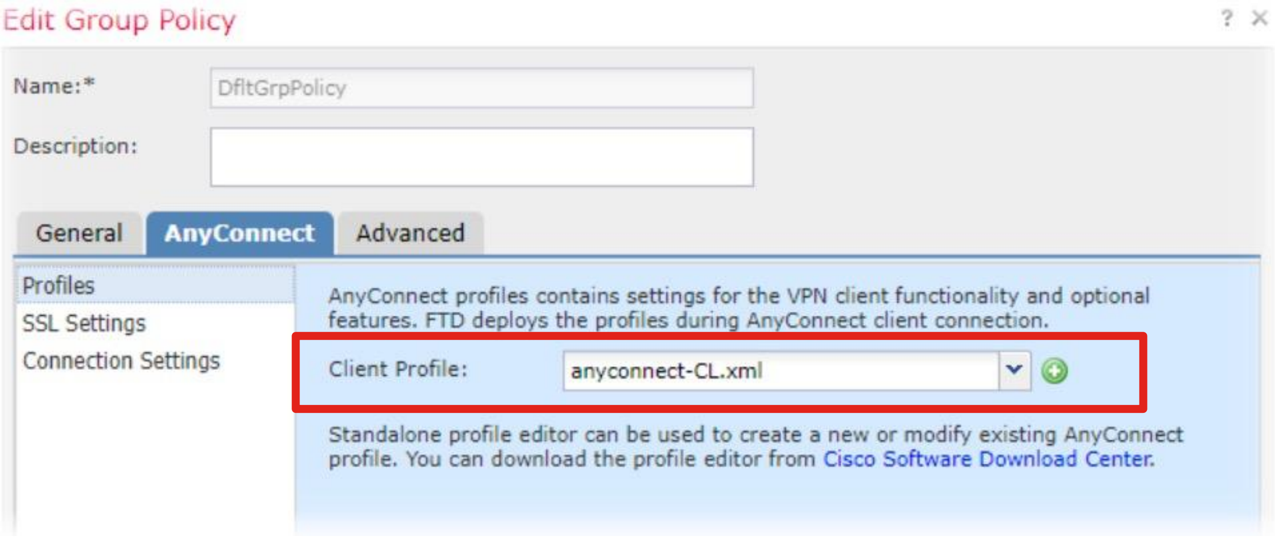
Description: AnyConnect Client profile for CL2020

Save Cancel

FMC Building Blocks

AnyConnect Client Profile Editor (cont)

Objects>Object Management>VPN>Group Policy



Edit Group Policy

Name:* DfltGrpPolicy

Description:

AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

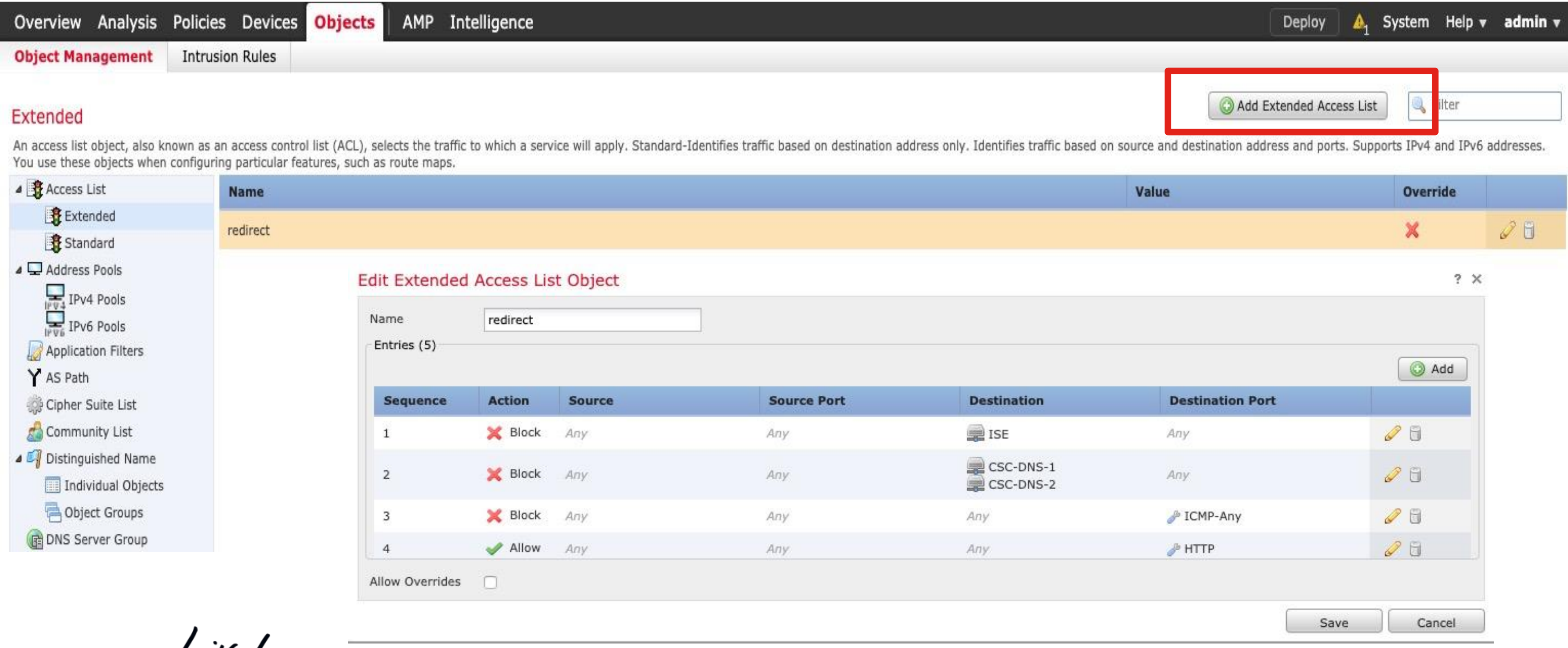
Client Profile: anyconnect-CL.xml

Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from Cisco Software Download Center.

FMC Building Blocks

Redirect ACL

Objects>Object Management>Access List>Extended



Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

Name	Value	Override
redirect		✗

Edit Extended Access List Object

Name: redirect

Entries (5)

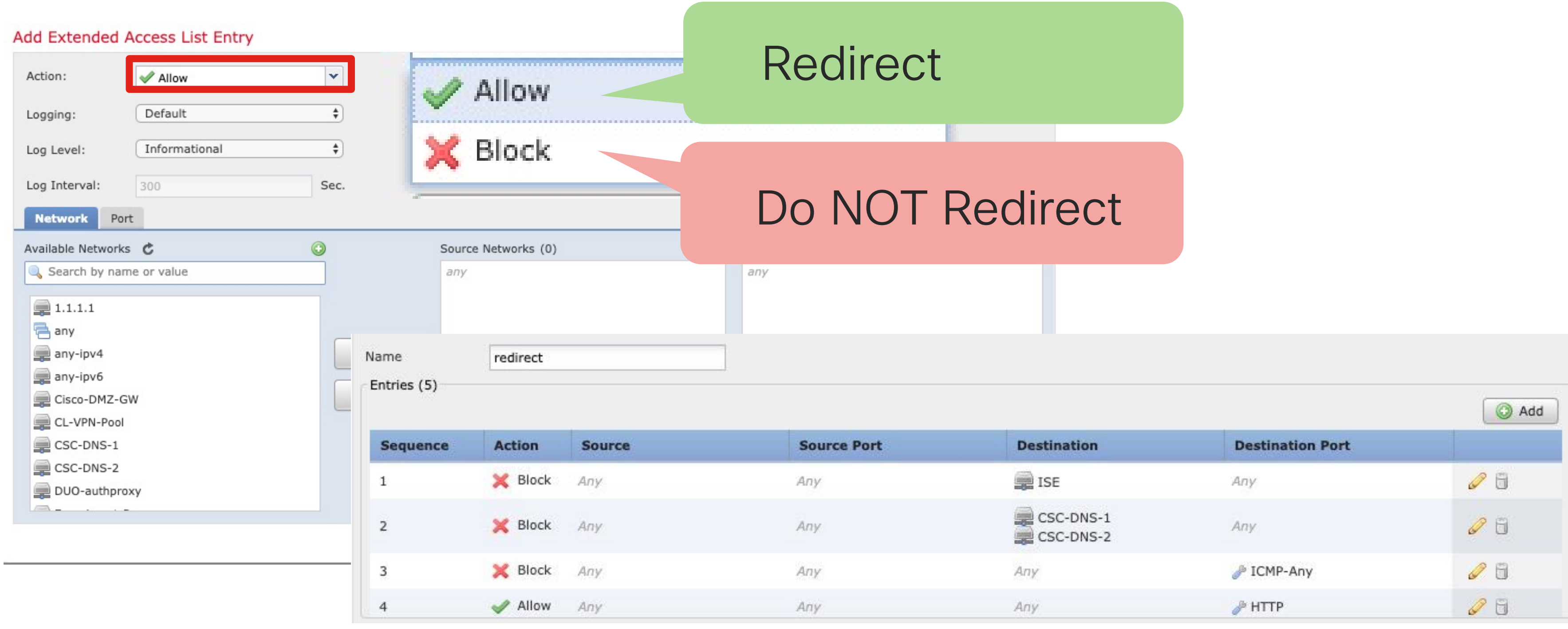
Sequence	Action	Source	Source Port	Destination	Destination Port
1	✗ Block	Any	Any	ISE	Any
2	✗ Block	Any	Any	CSC-DNS-1 CSC-DNS-2	Any
3	✗ Block	Any	Any	Any	ICMP-Any
4	✓ Allow	Any	Any	Any	HTTP

Allow Overrides □

FMC Building Blocks

Redirect ACL

Objects>Object Management>Access List>Extended



Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Allow → Redirect

Block → Do NOT Redirect

Name: redirect

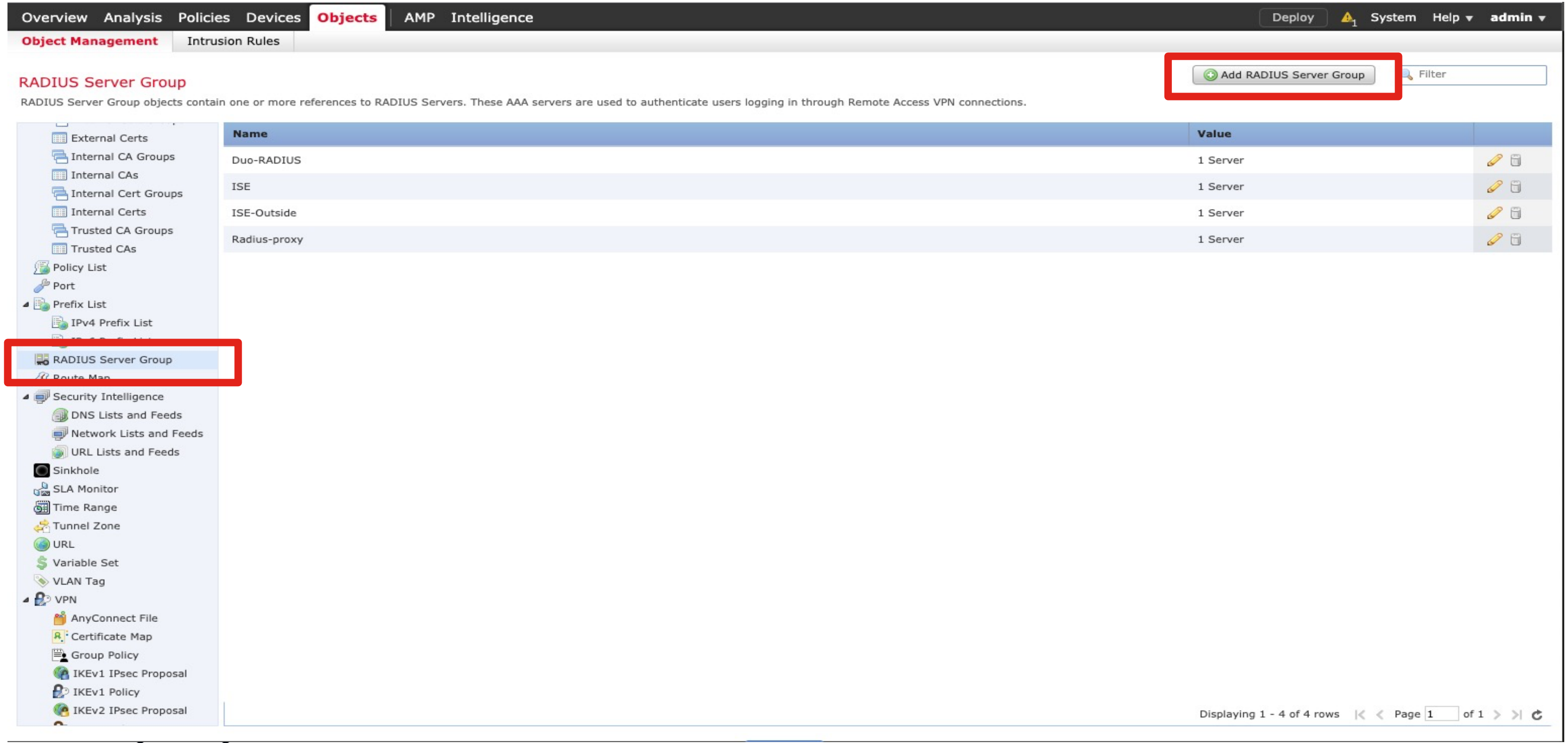
Entries (5)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	ISE	Any
2	Block	Any	Any	CSC-DNS-1 CSC-DNS-2	Any
3	Block	Any	Any	Any	ICMP-Any
4	Allow	Any	Any	Any	HTTP

FMC Building Blocks

RADIUS Servers

Objects>Object Management>RADIUS Server Group



RADIUS Server Group

RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.

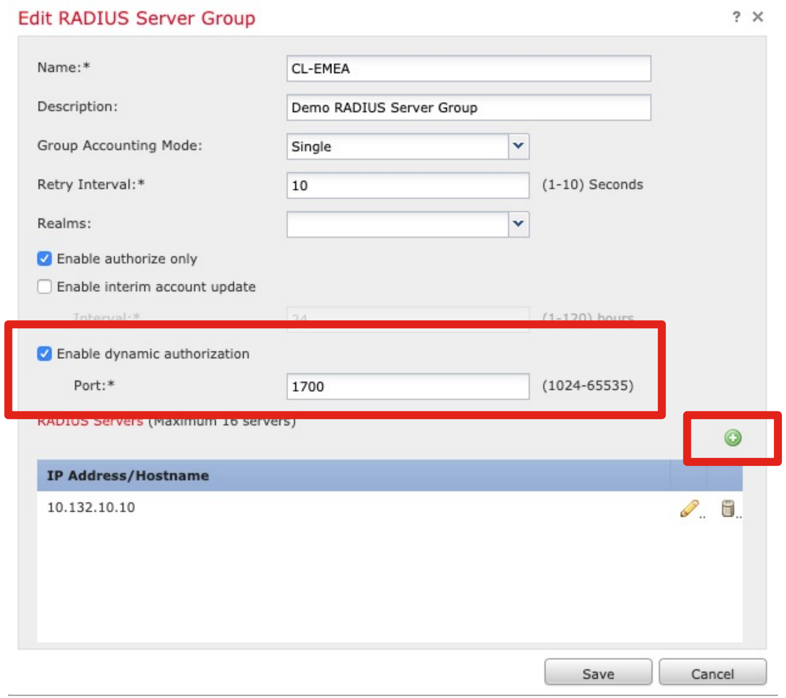
Name	Value
Duo-RADIUS	1 Server
ISE	1 Server
ISE-Outside	1 Server
Radius-proxy	1 Server

Displaying 1 - 4 of 4 rows

FMC Building Blocks

RADIUS Servers

Objects>Object Management>RADIUS Server Group



Edit RADIUS Server Group

Name:*	CL-EMEA	
Description:	Demo RADIUS Server Group	
Group Accounting Mode:	Single	
Retry Interval:*	10	(1-10) Seconds
Realms:		

☑ Enable authorize only

□ Enable interim account update

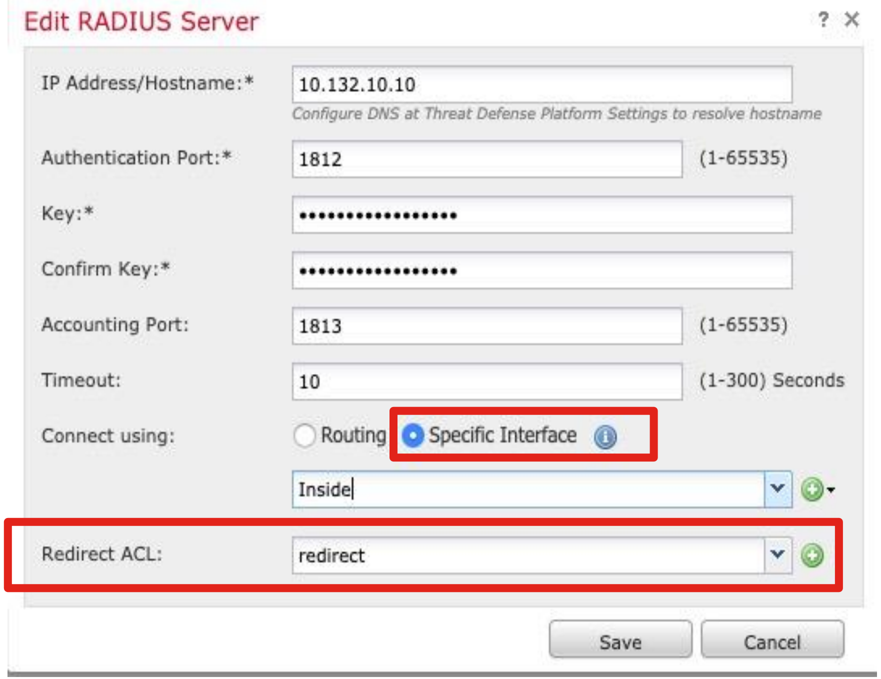
Interval:*	24	(1-120) hours

☑ Enable dynamic authorization

Port:*	1700	(1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
10.132.10.10



Edit RADIUS Server

IP Address/Hostname:*	10.132.10.10 *Configure DNS at Threat Defense Platform Settings to resolve hostname*	
Authentication Port:*	1812	(1-65535)
Key:*	••••••••••••••••	
Confirm Key:*	••••••••••••••••	
Accounting Port:	1813	(1-65535)
Timeout:	10	(1-300) Seconds
Connect using:	○ Routing ● Specific Interface Inside	
Redirect ACL:	redirect	

FMC Configuration

- AnyConnect Client
- VPN Pool
- ID Certificate
- AnyConnect Client Profile
- RADIUS Servers

- Connection Profile
- Access Control Policies

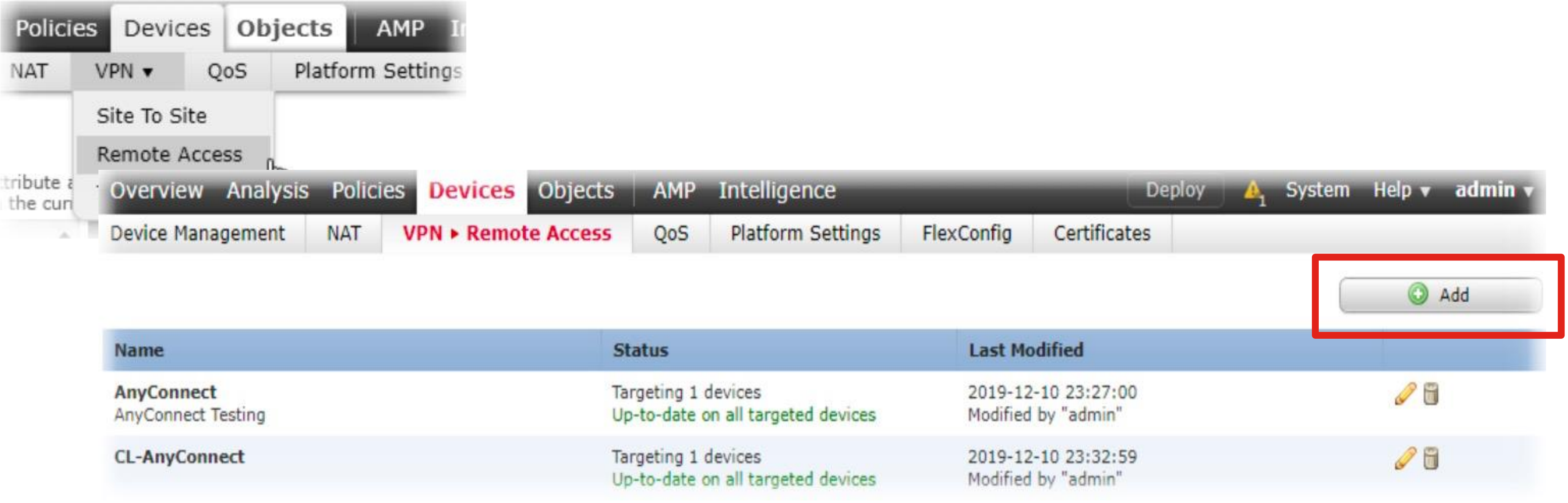
- Secondary Authentication

- Connection Profile
- Access Control Policies

FMC Configuration

Connection Profile

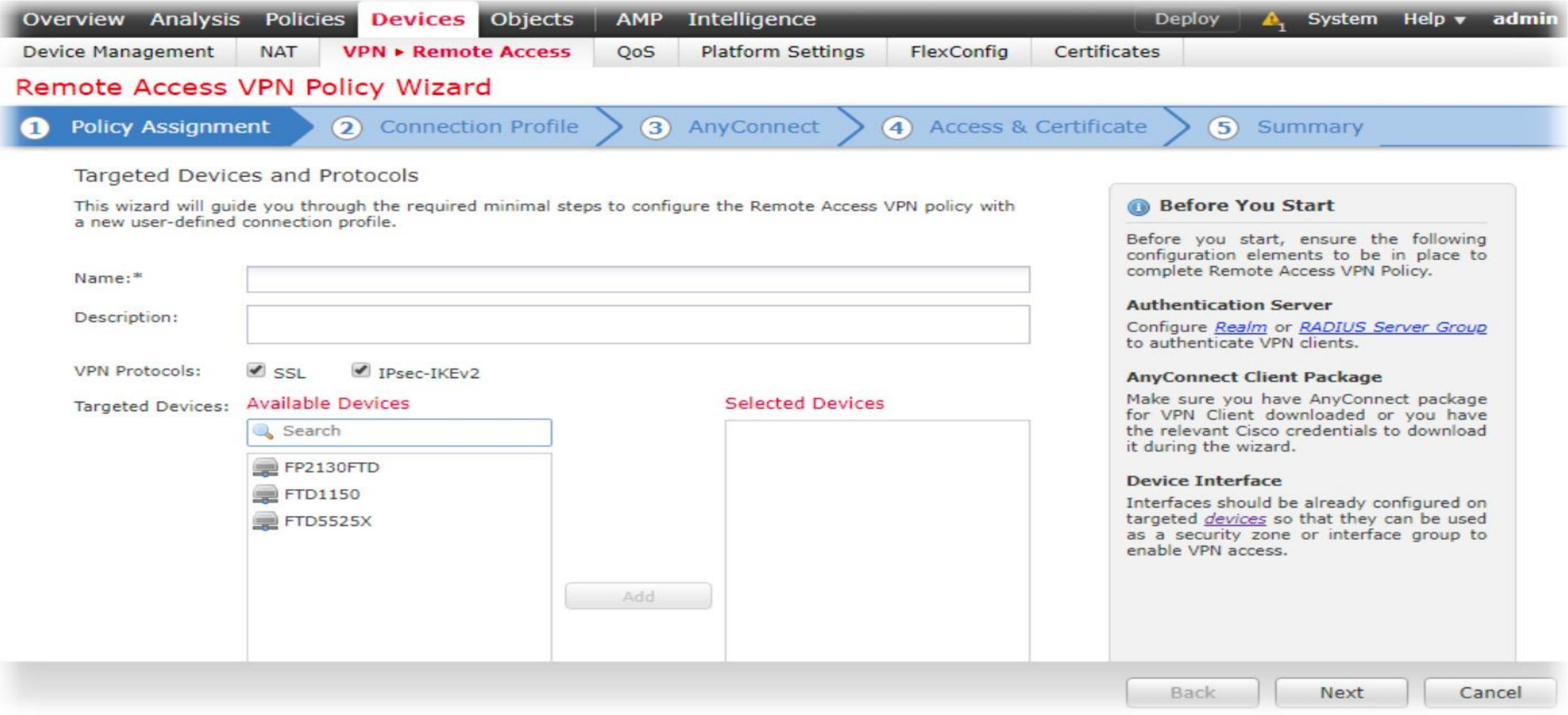
Devices>VPN>Remote Access



Name	Status	Last Modified
AnyConnect AnyConnect Testing	Targeting 1 devices Up-to-date on all targeted devices	2019-12-10 23:27:00 Modified by "admin"
CL-AnyConnect	Targeting 1 devices Up-to-date on all targeted devices	2019-12-10 23:32:59 Modified by "admin"

FMC Configuration

Remote Access VPN Policy Wizard



Remote Access VPN Policy Wizard

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

Search

- FP2130FTD
- FTD1150
- FTD5525X

Selected Devices

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

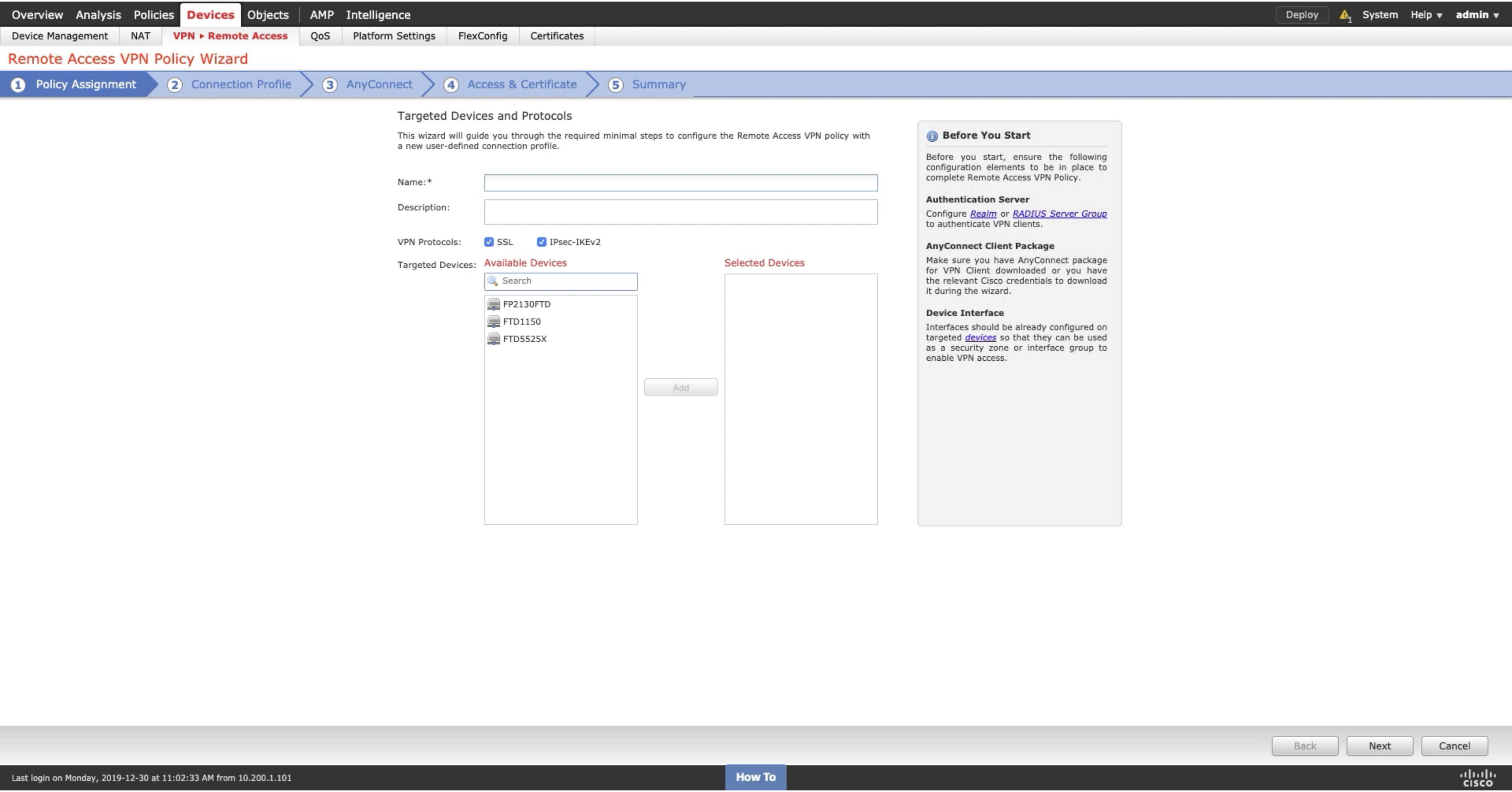
Configure Realm or RADIUS Server Group to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▸ Remote Access QoS Platform Settings FlexConfig Certificates

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:

VPN Protocols: ☑ SSL ☑ IPsec-IKEv2

Targeted Devices: Available Devices

Search

- FP2130FTD
- FTD1150
- FTD5525X

Selected Devices

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure *Realm* or *RADIUS Server Group* to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

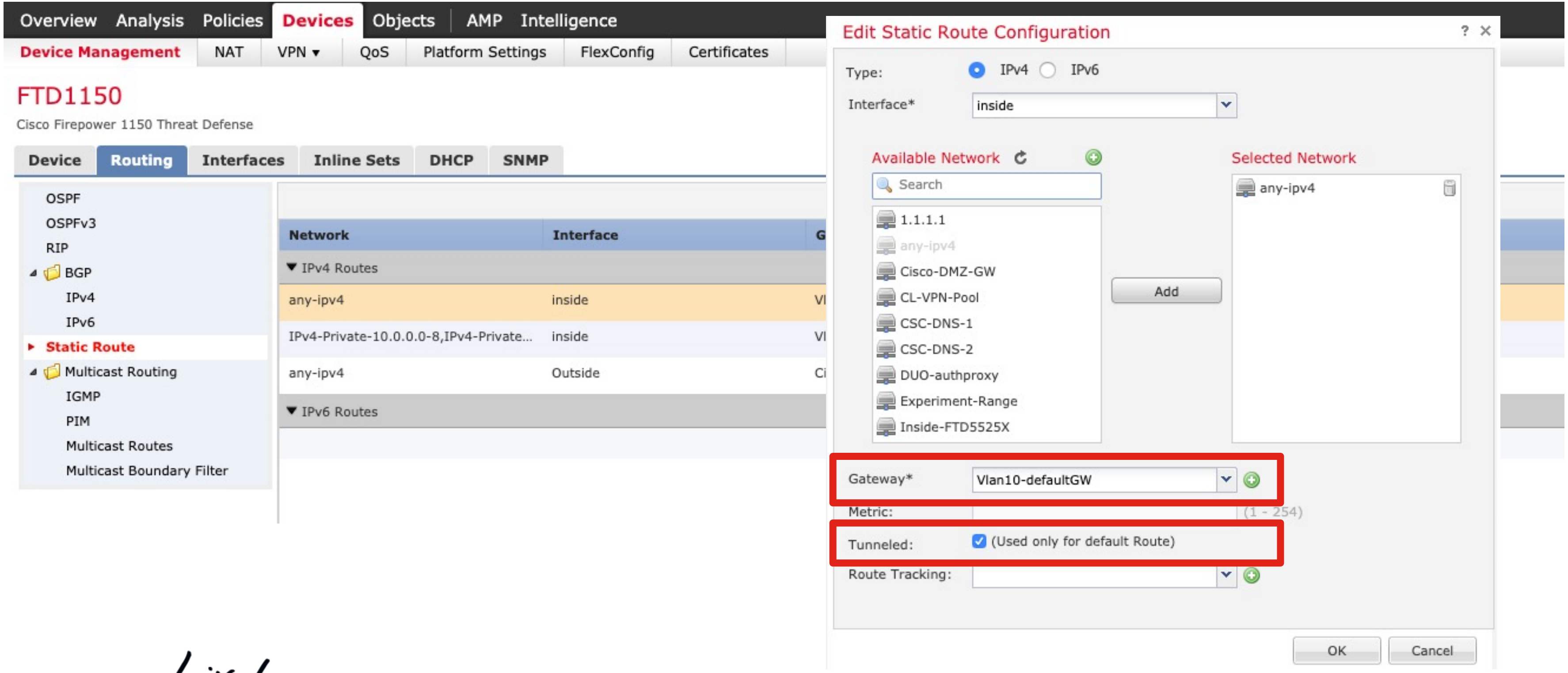
Interfaces should be already configured on targeted *devices* so that they can be used as a security zone or interface group to enable VPN access.

Last login on Monday, 2019-12-30 at 11:02:33 AM from 10.200.1.101

FMC Configuration Extras

RA Client routing

Devices>Device Management>{device}>routing



Network	Interface	G
▼ IPv4 Routes		
any-ipv4	inside	Vl
IPv4-Private-10.0.0.0-8,IPv4-Private...	inside	Vl
any-ipv4	Outside	Ci
▼ IPv6 Routes		

Type: ● IPv4 ○ IPv6

Interface*: inside

Available Network:
- 1.1.1.1
- any-ipv4
- Cisco-DMZ-GW
- CL-VPN-Pool
- CSC-DNS-1
- CSC-DNS-2
- DUO-authproxy
- Experiment-Range
- Inside-FTD5525X

Selected Network:
- any-ipv4

Gateway*: Vlan10-defaultGW

Metric: (1 - 254)

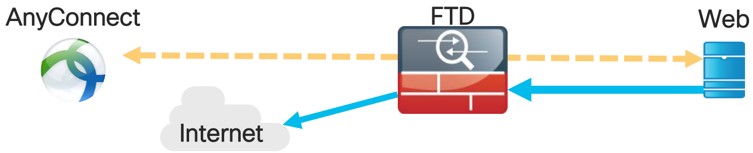
Tunneled: ☑ (Used only for default Route)

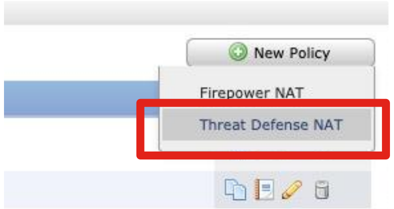
Route Tracking:

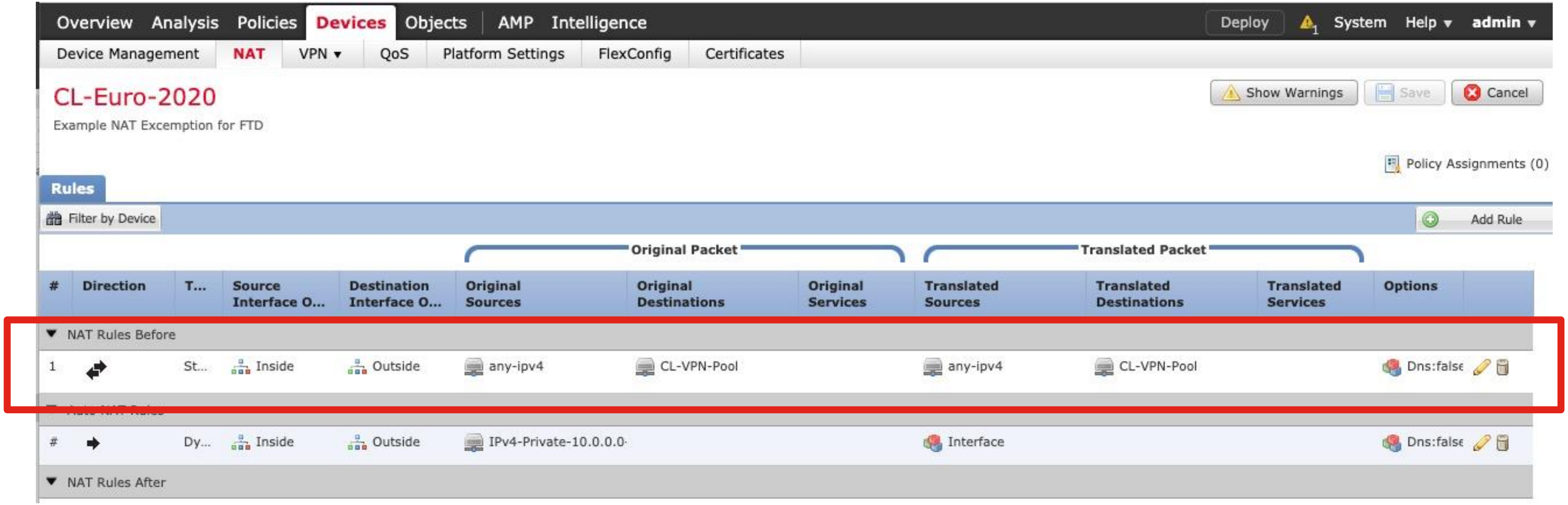
FMC Configuration Extras

RA Client NAT/PAT Exemption

Devices>NAT>






Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
Show Warnings
Save
Cancel
Policy Assignments (0)
Rules
Filter by Device
Add Rule

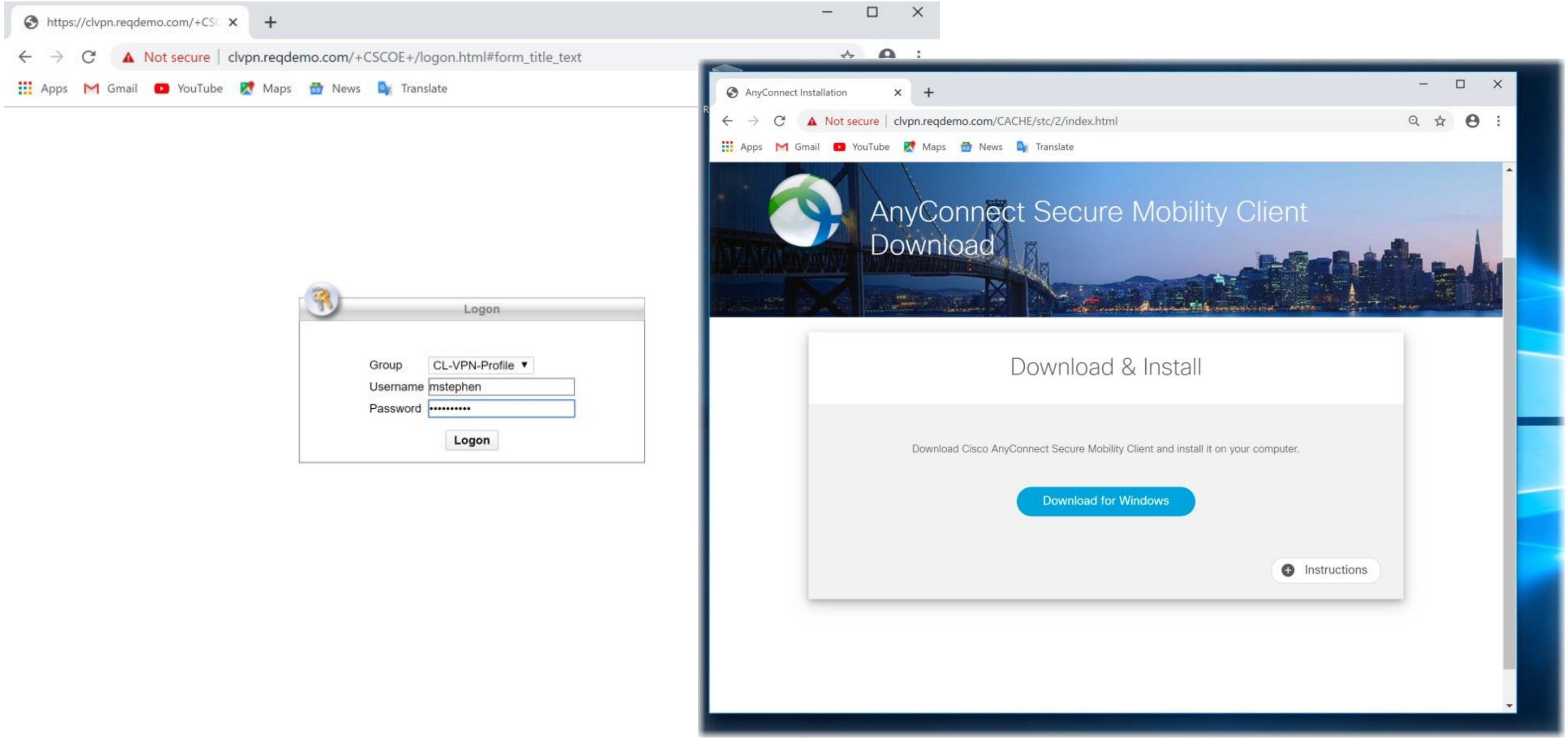
CL-Euro-2020

Example NAT Excemption for FTD

					Original Packet			Translated Packet			
#	Direction	T...	Source Interface O...	Destination Interface O...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1	⇄	St...	Inside	Outside	any-ipv4	CL-VPN-Pool		any-ipv4	CL-VPN-Pool		Dns:false
▼ Auto NAT Rules											
#	→	Dy...	Inside	Outside	IPv4-Private-10.0.0.0-			Interface			Dns:false
▼ NAT Rules After											

FMC Configuration

Remote Access VPN Client Web Installation



https://clvpn.reqdemo.com/+CSC

Not secure | clvpn.reqdemo.com/+CSCOE+/logon.html#form_title_text

Logon

Group: CL-VPN-Profile

Username: mstephen

Password: ••••••••••

AnyConnect Installation

Not secure | clvpn.reqdemo.com/CACHE/stc/2/index.html

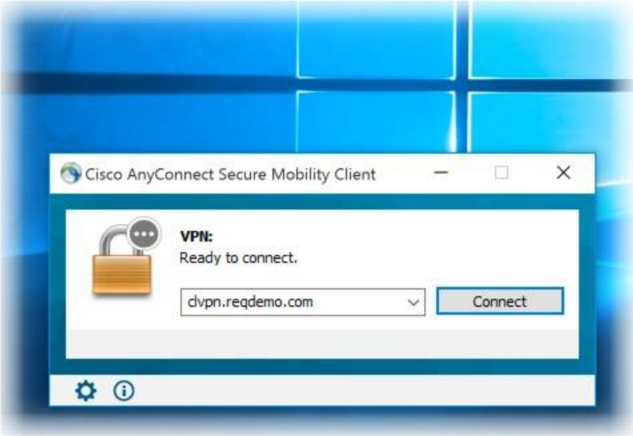
AnyConnect Secure Mobility Client Download

Download & Install

Download Cisco AnyConnect Secure Mobility Client and install it on your computer.

FMC Configuration

Remote Access VPN Client

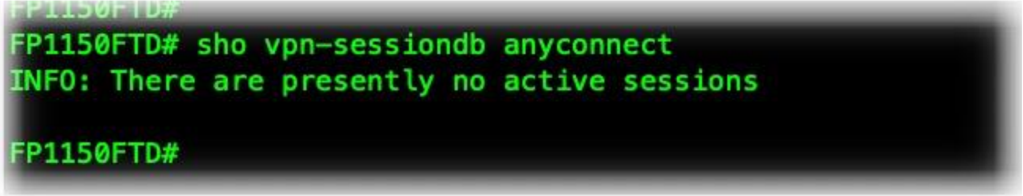


Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

clvpn.reqdemo.com

Show vpn-sessiondb anyconnect

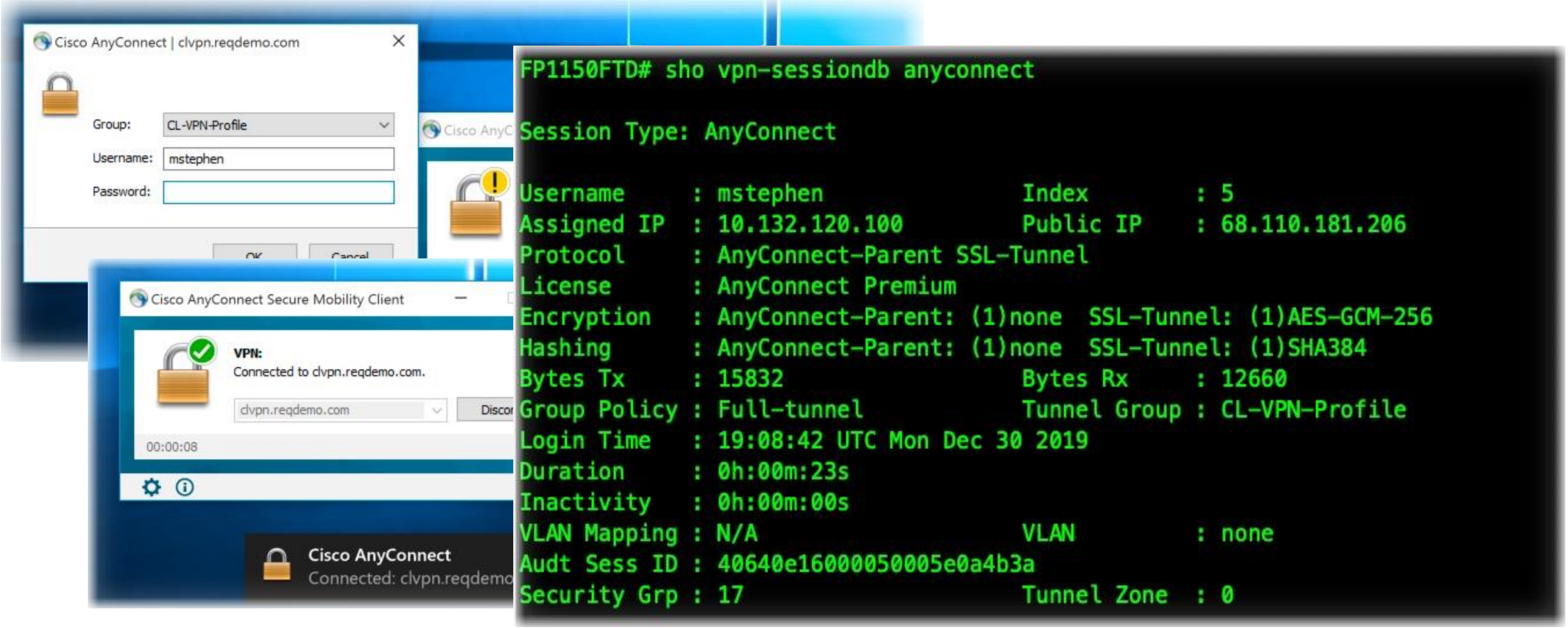


```
FP1150FTD#
FP1150FTD# sho vpn-sessiondb anyconnect
INFO: There are presently no active sessions

FP1150FTD#
```

FMC Configuration

Remote Access VPN Client

Show vpn-sessiondb anyconnect



Cisco AnyConnect | clvpn.reqdemo.com

Group: CL-VPN-Profile

Username: mstephen

Password:

Cisco AnyConnect Secure Mobility Client

VPN: Connected to clvpn.reqdemo.com.

clvpn.reqdemo.com

00:00:08

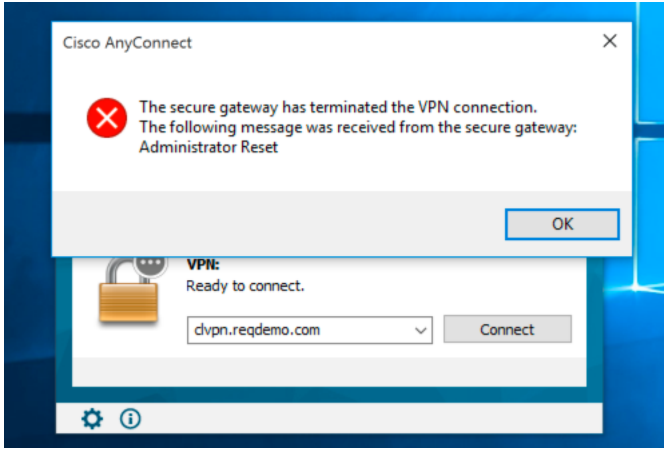
Cisco AnyConnect

Connected: clvpn.reqdemo

```
FP1150FTD# sho vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : mstephen               Index        : 5
Assigned IP  : 10.132.120.100         Public IP    : 68.110.181.206
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 15832                  Bytes Rx     : 12660
Group Policy : Full-tunnel            Tunnel Group : CL-VPN-Profile
Login Time   : 19:08:42 UTC Mon Dec 30 2019
Duration     : 0h:00m:23s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 40640e16000050005e0a4b3a
Security Grp : 17                     Tunnel Zone  : 0
```

FMC Configuration

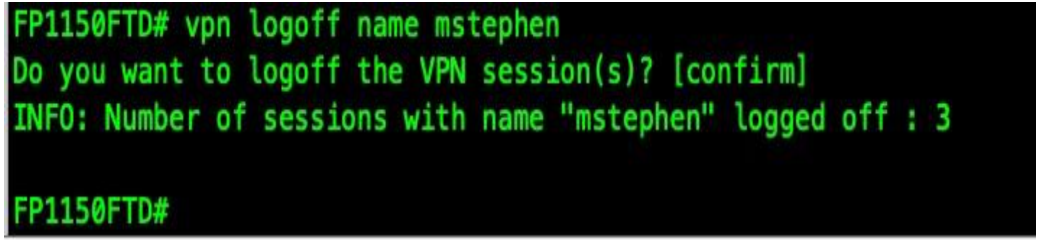
Remote Access VPN Client Control



Cisco AnyConnect

The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway:
Administrator Reset

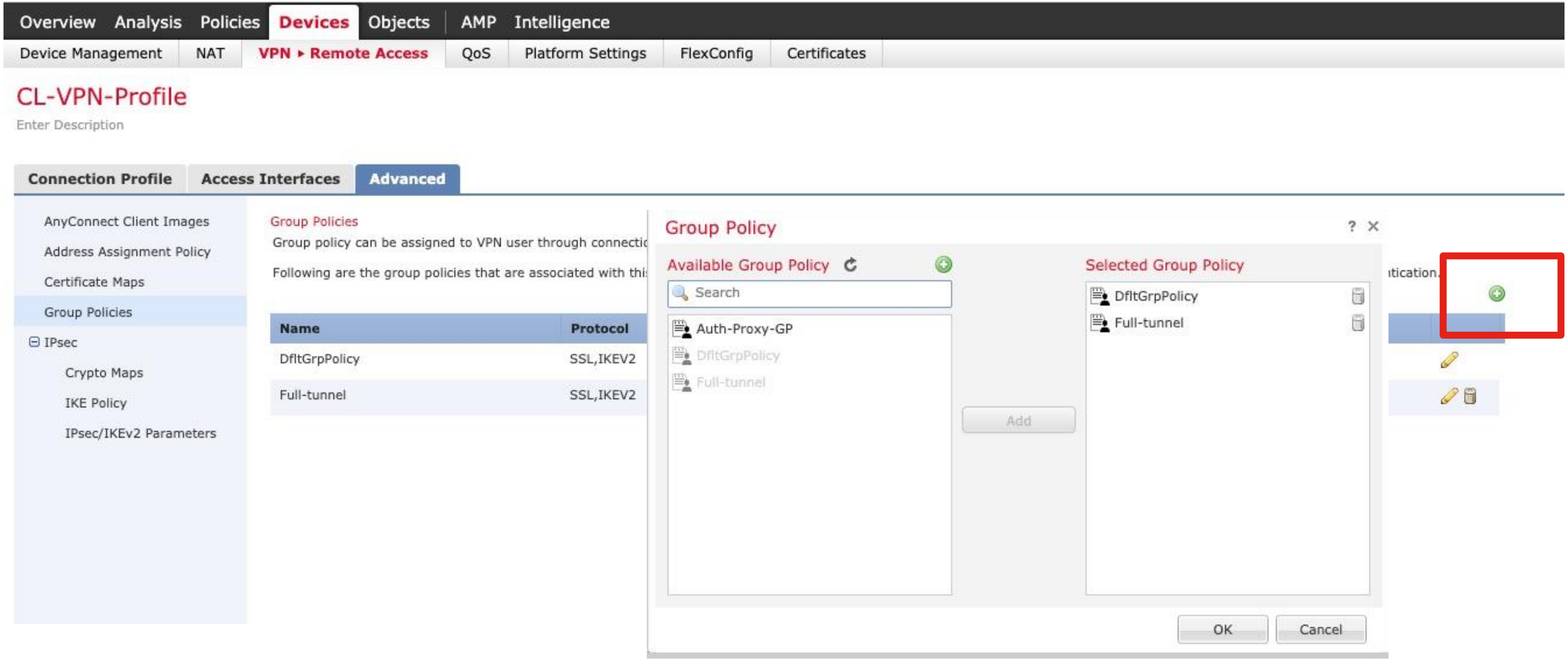
vpn logoff name mstephen



```
FP1150FTD# vpn logoff name mstephen
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "mstephen" logged off : 3

FP1150FTD#
```

FMC Configuration

Remote Access VPN Client Control



Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT **VPN ▸ Remote Access** QoS Platform Settings FlexConfig Certificates

CL-VPN-Profile

Enter Description

Connection Profile | Access Interfaces | **Advanced**

- AnyConnect Client Images
- Address Assignment Policy
- Certificate Maps
- Group Policies
- ⊟ IPsec
  - Crypto Maps
  - IKE Policy
  - IPsec/IKEv2 Parameters

Group Policies

Group policy can be assigned to VPN user through connectic

Following are the group policies that are associated with thi

Name	Protocol
DfltGrpPolicy	SSL,IKEV2
Full-tunnel	SSL,IKEV2

Group Policy

Available Group Policy

Search

- Auth-Proxy-GP
- DfltGrpPolicy
- Full-tunnel

Add

Selected Group Policy

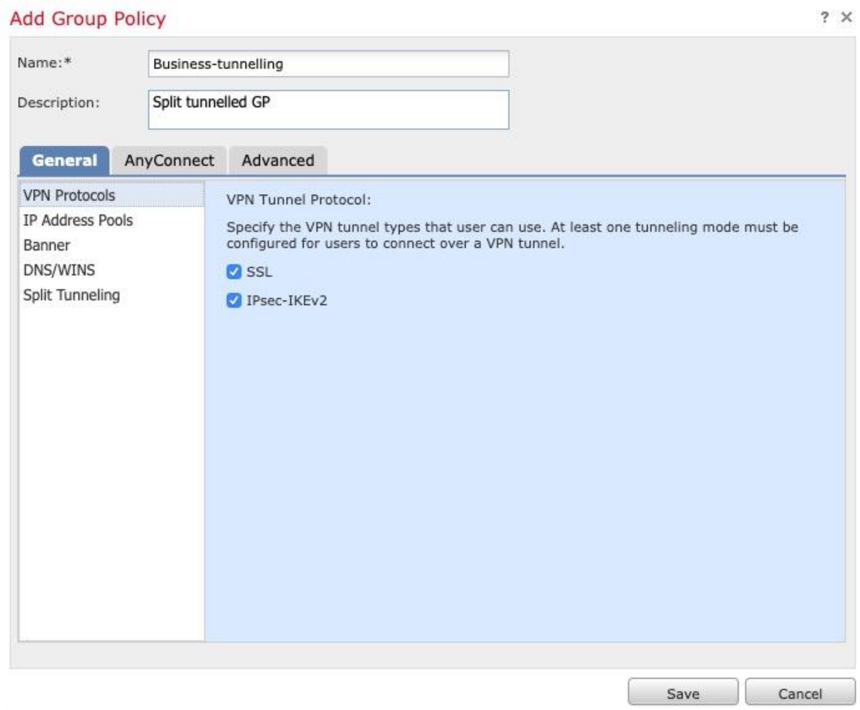
- DfltGrpPolicy
- Full-tunnel

OK Cancel

ıtication.

FMC Configuration

Remote Access VPN Client Control



Add Group Policy

Name:* Business-tunnelling

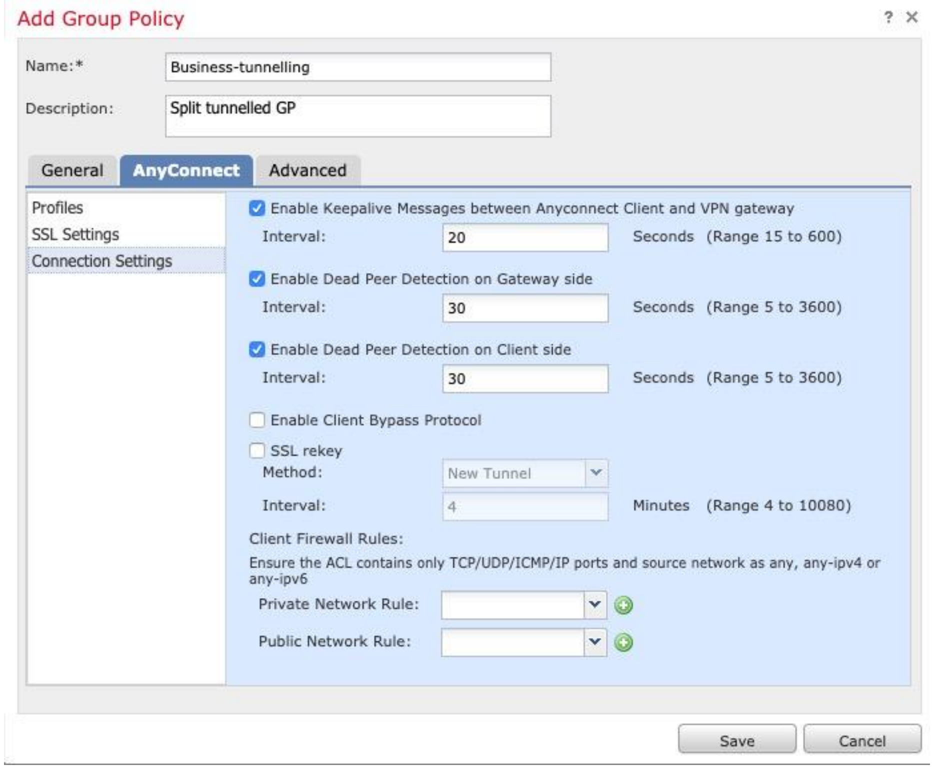
Description: Split tunnelled GP

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☑ SSL

☑ IPsec-IKEv2



Add Group Policy

Name:* Business-tunnelling

Description: Split tunnelled GP

☑ Enable Keepalive Messages between Anyconnect Client and VPN gateway

Interval: 20 Seconds (Range 15 to 600)

☑ Enable Dead Peer Detection on Gateway side

Interval: 30 Seconds (Range 5 to 3600)

☑ Enable Dead Peer Detection on Client side

Interval: 30 Seconds (Range 5 to 3600)

□ Enable Client Bypass Protocol

□ SSL rekey

Method: New Tunnel

Interval: 4 Minutes (Range 4 to 10080)

Client Firewall Rules:

Ensure the ACL contains only TCP/UDP/ICMP/IP ports and source network as any, any-ipv4 or any-ipv6

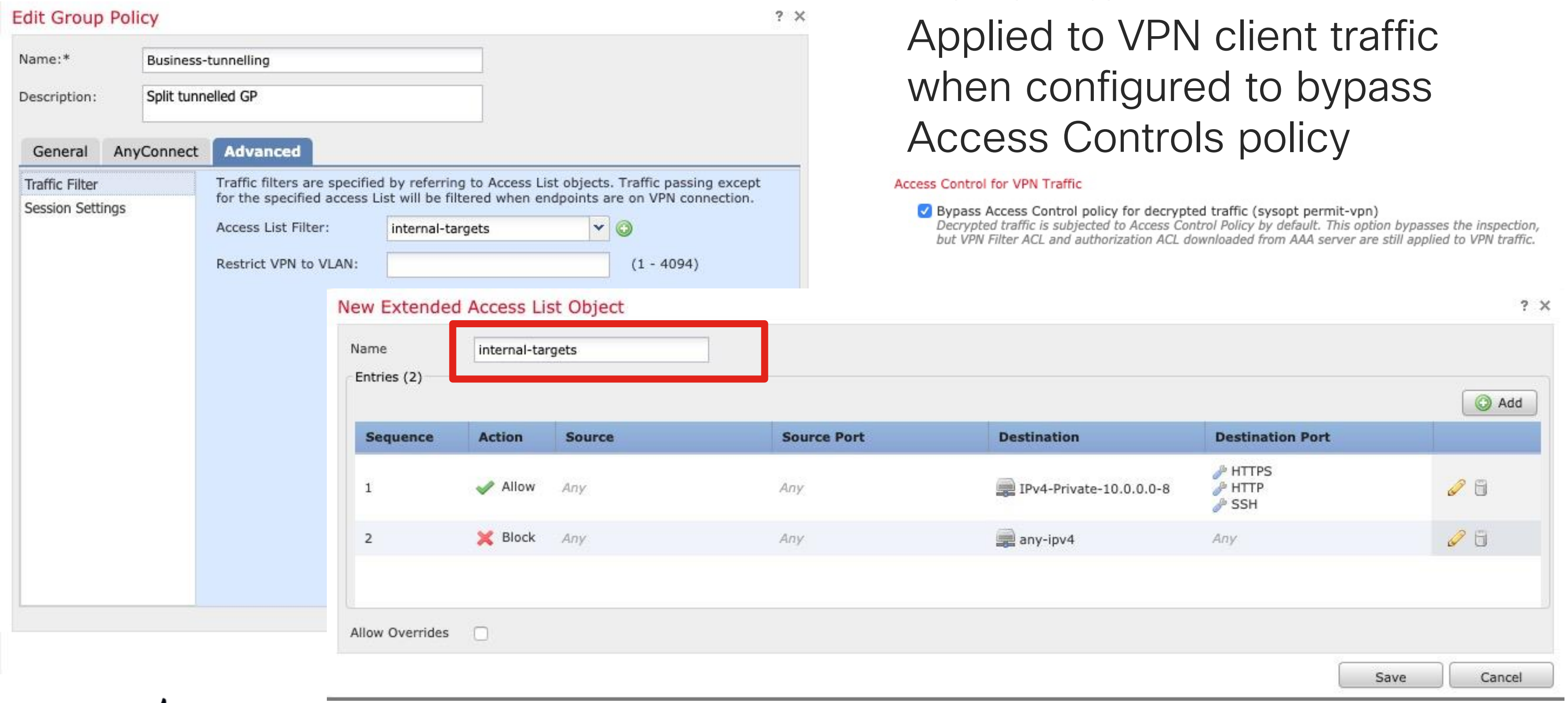
Private Network Rule:

Public Network Rule:

FMC Configuration

Remote Access VPN Client Control

Traffic Filter:
Applied to VPN client traffic when configured to bypass Access Controls policy



Edit Group Policy

Name:* Business-tunnelling

Description: Split tunnelled GP

General | AnyConnect | **Advanced**

- Traffic Filter
- Session Settings

Traffic filters are specified by referring to Access List objects. Traffic passing except for the specified access List will be filtered when endpoints are on VPN connection.

Access List Filter: internal-targets

Restrict VPN to VLAN: (1 - 4094)

Access Control for VPN Traffic

☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

New Extended Access List Object

Name: internal-targets

Entries (2)

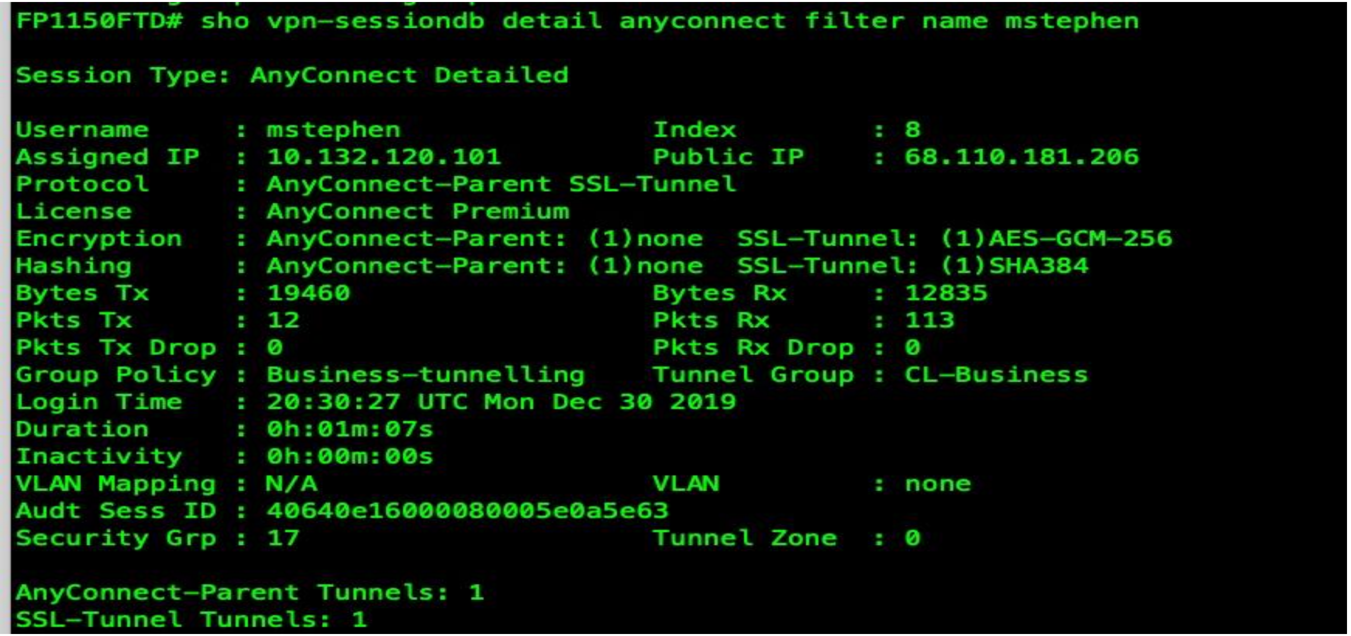
Sequence	Action	Source	Source Port	Destination	Destination Port
1	✓ Allow	Any	Any	IPv4-Private-10.0.0.0-8	HTTPS HTTP SSH
2	✗ Block	Any	Any	any-ipv4	Any

Allow Overrides □

FMC Configuration

Remote Access VPN Client Control

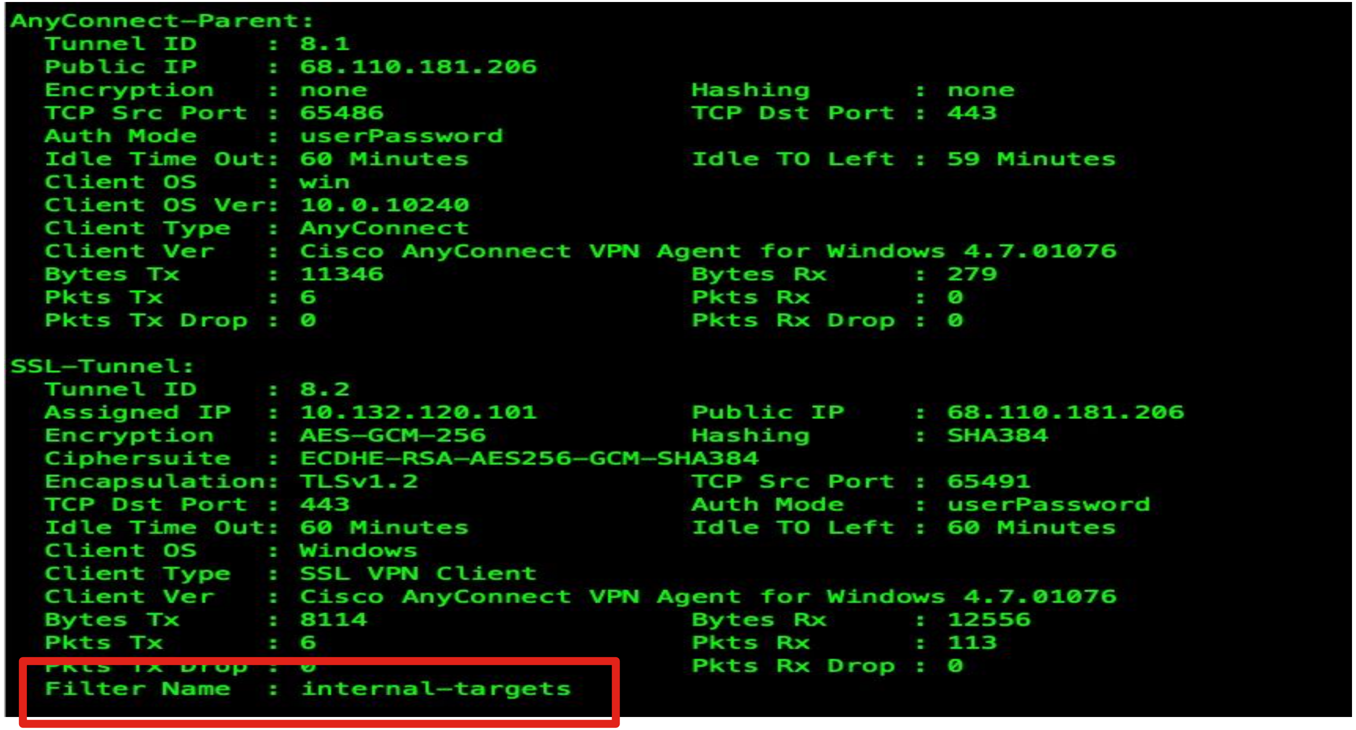
show vpn-sessiondb detail anyconnect filter name mstephen



```
FP1150FTD# sho vpn-sessiondb detail anyconnect filter name mstephen

Session Type: AnyConnect Detailed

Username     : mstephen               Index        : 8
Assigned IP  : 10.132.120.101         Public IP    : 68.110.181.206
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 19460                  Bytes Rx     : 12835
Pkts Tx      : 12                     Pkts Rx      : 113
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : Business-tunnelling    Tunnel Group : CL-Business
Login Time   : 20:30:27 UTC Mon Dec 30 2019
Duration     : 0h:01m:07s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 40640e16000080005e0a5e63
Security Grp : 17                     Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
```

FMC Configuration

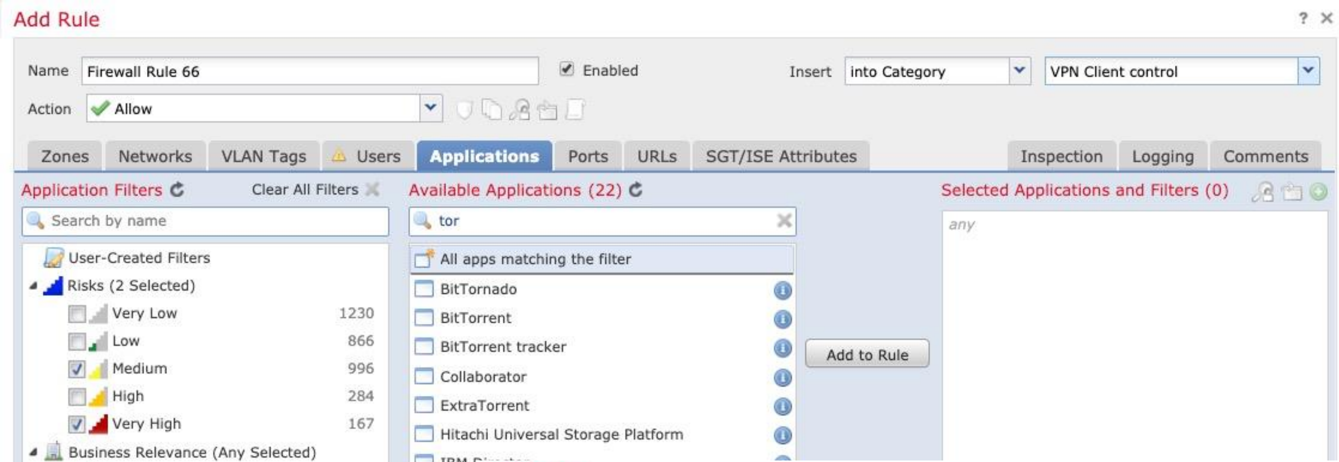
Remote Access VPN Client Control



```
AnyConnect-Parent:
  Tunnel ID    : 8.1
  Public IP    : 68.110.181.206
  Encryption   : none                   Hashing      : none
  TCP Src Port : 65486                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 60 Minutes             Idle TO Left : 59 Minutes
  Client OS    : win
  Client OS Ver: 10.0.10240
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.01076
  Bytes Tx     : 11346                  Bytes Rx     : 279
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 8.2
  Assigned IP  : 10.132.120.101         Public IP    : 68.110.181.206
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 65491
  TCP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 60 Minutes             Idle TO Left : 60 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.01076
  Bytes Tx     : 8114                   Bytes Rx     : 12556
  Pkts Tx      : 6                      Pkts Rx      : 113
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : internal-targets
```

FMC Configuration

Remote Access VPN Client Control NGFW



Add Rule

Name: Firewall Rule 66 ☑ Enabled Insert: into Category VPN Client control

Action: Allow

Application Filters Clear All Filters

Search by name

- User-Created Filters
- Risks (2 Selected)
  - □ Very Low 1230
  - □ Low 866
  - ☑ Medium 996
  - □ High 284
  - ☑ Very High 167
- Business Relevance (Any Selected)
  - □ Very Low 289
  - □ Low 160
  - □ Medium 641

Available Applications (22)

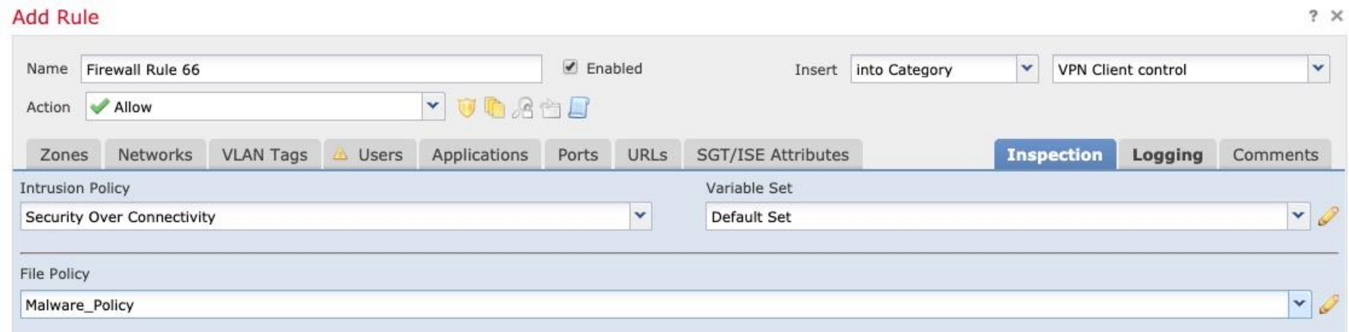
tor

- All apps matching the filter
- □ BitTornado
- □ BitTorrent
- □ BitTorrent tracker
- □ Collaborator
- □ ExtraTorrent
- □ Hitachi Universal Storage Platform
- □ IBM Director
- □ JSTO
- □ Mapl

Add to Rule

Selected Applications and Filters (0)

any



Add Rule

Name: Firewall Rule 66 ☑ Enabled Insert: into Category VPN Client control

Action: Allow

Intrusion Policy: Security Over Connectivity

Variable Set: Default Set

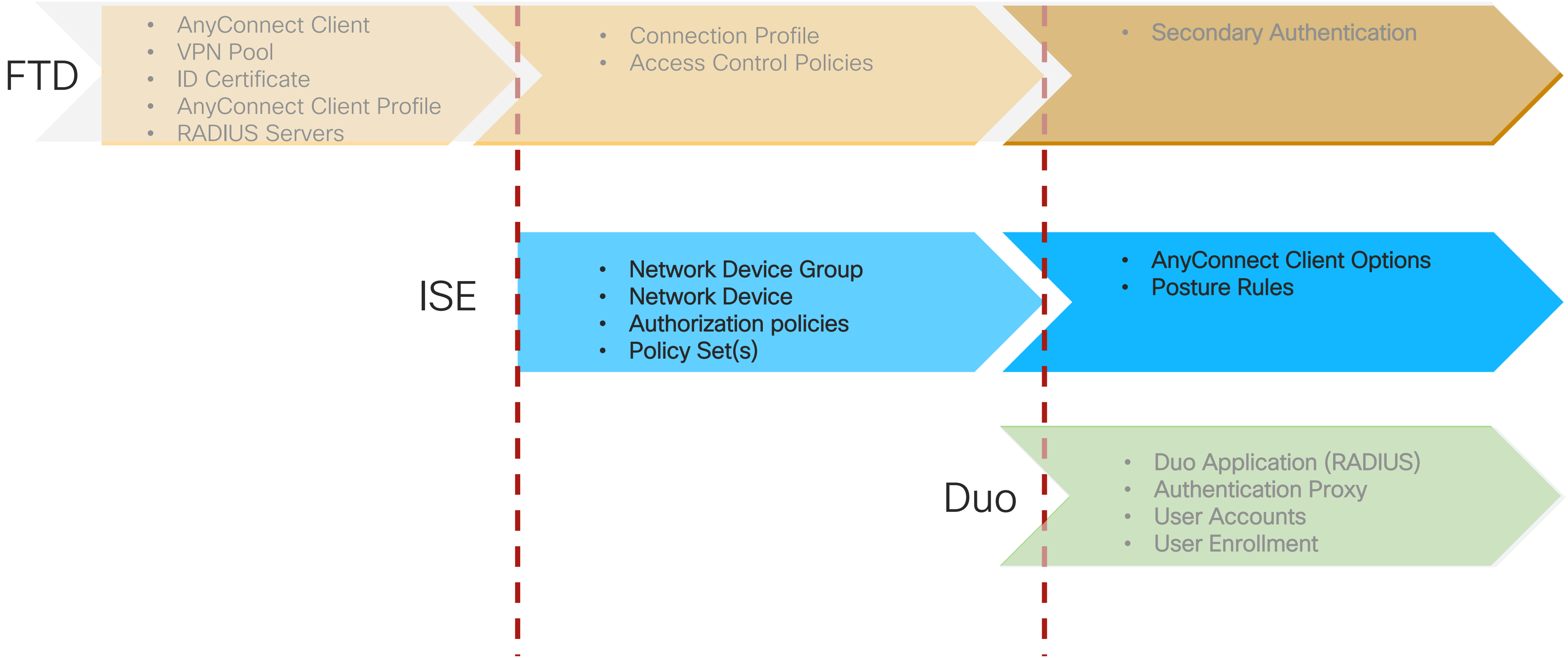
File Policy: Malware_Policy

- Zone Based
- Network
- Application
- Service/Port
- URLs

Uncheck bypass contro
Access interface tab

ISE Configuration

Roadmap to configuring



FTD

- AnyConnect Client
- VPN Pool
- ID Certificate
- AnyConnect Client Profile
- RADIUS Servers

- Connection Profile
- Access Control Policies

- Secondary Authentication

ISE

- Network Device Group
- Network Device
- Authorization policies
- Policy Set(s)

- AnyConnect Client Options
- Posture Rules

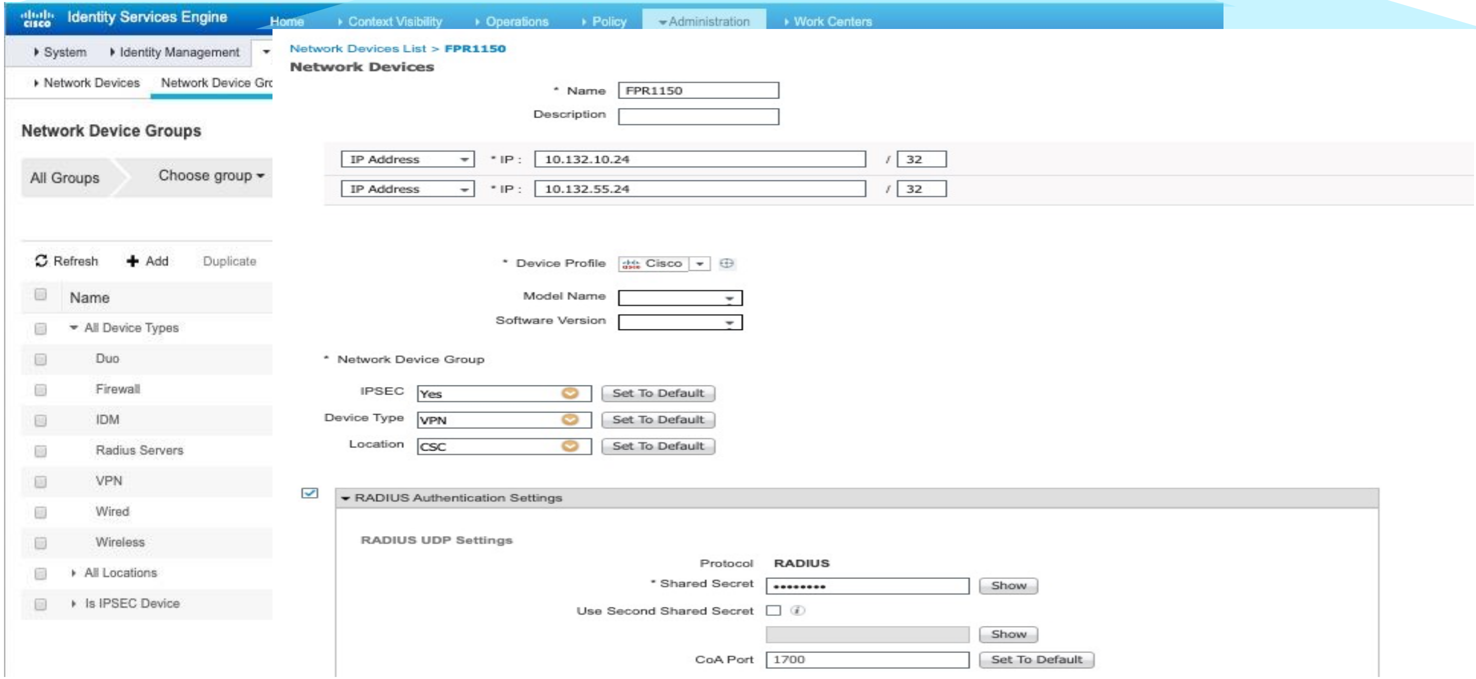
Duo

- Duo Application (RADIUS)
- Authentication Proxy
- User Accounts
- User Enrollment

ISE

- Network Device Group
- Network Device
- Authorization policies
- Policy Set(s)

- AnyConnect Client Options
- Posture Rules



Network Devices List > FPR1150

Network Devices

* Name: FPR1150

Description:

IP Address * IP : 10.132.10.24 / 32

IP Address * IP : 10.132.55.24 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

IPSEC: Yes — Set To Default

Device Type: VPN — Set To Default

Location: CSC — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: ••••••••• — Show

Use Second Shared Secret: □

Show

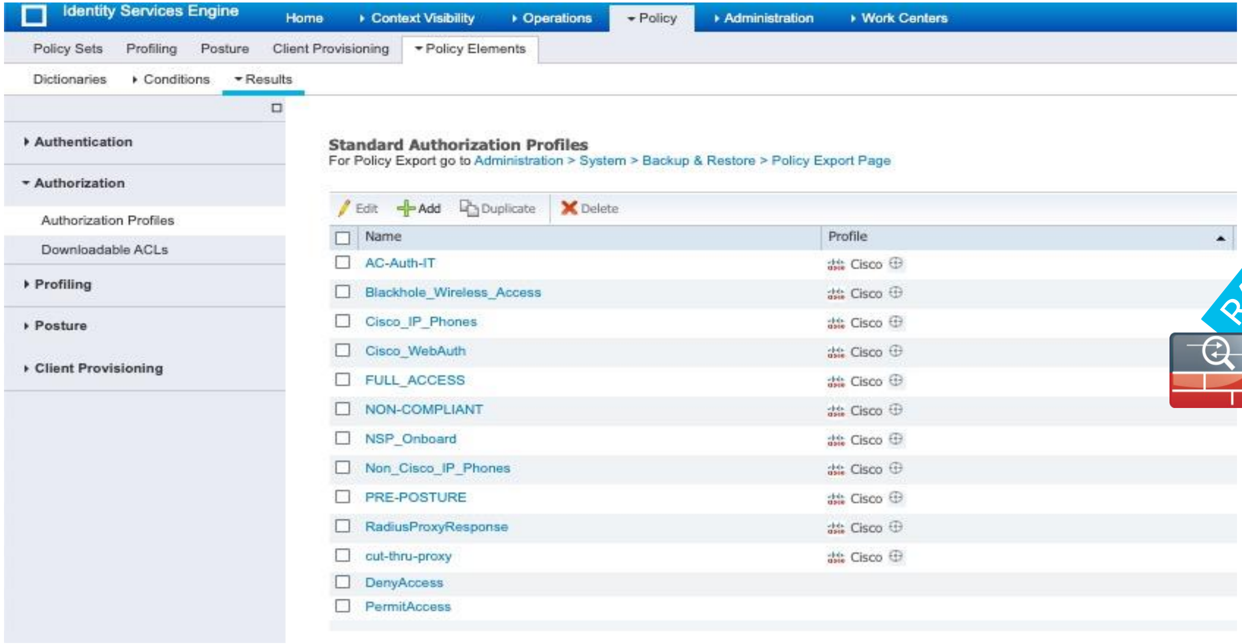
CoA Port: 1700 — Set To Default

cisco Live!

ISE

- Network Device Group
- Network Device
- Authorization policies
- Policy Set(s)

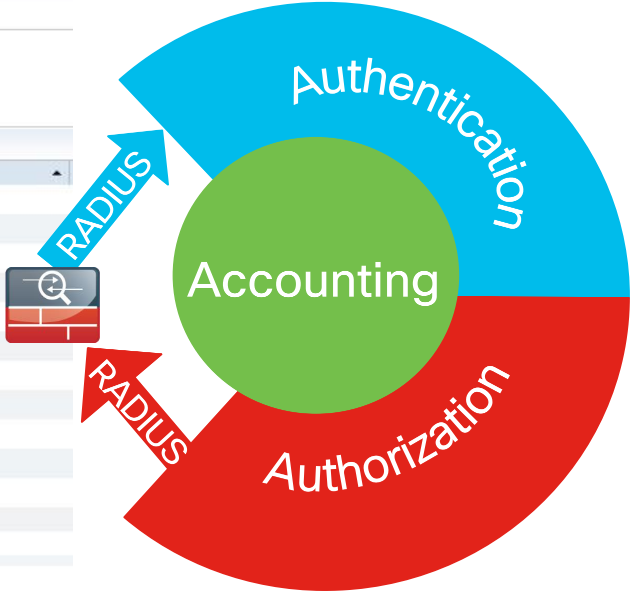
- AnyConnect Client Options
- Posture Rules



Standard Authorization Profiles

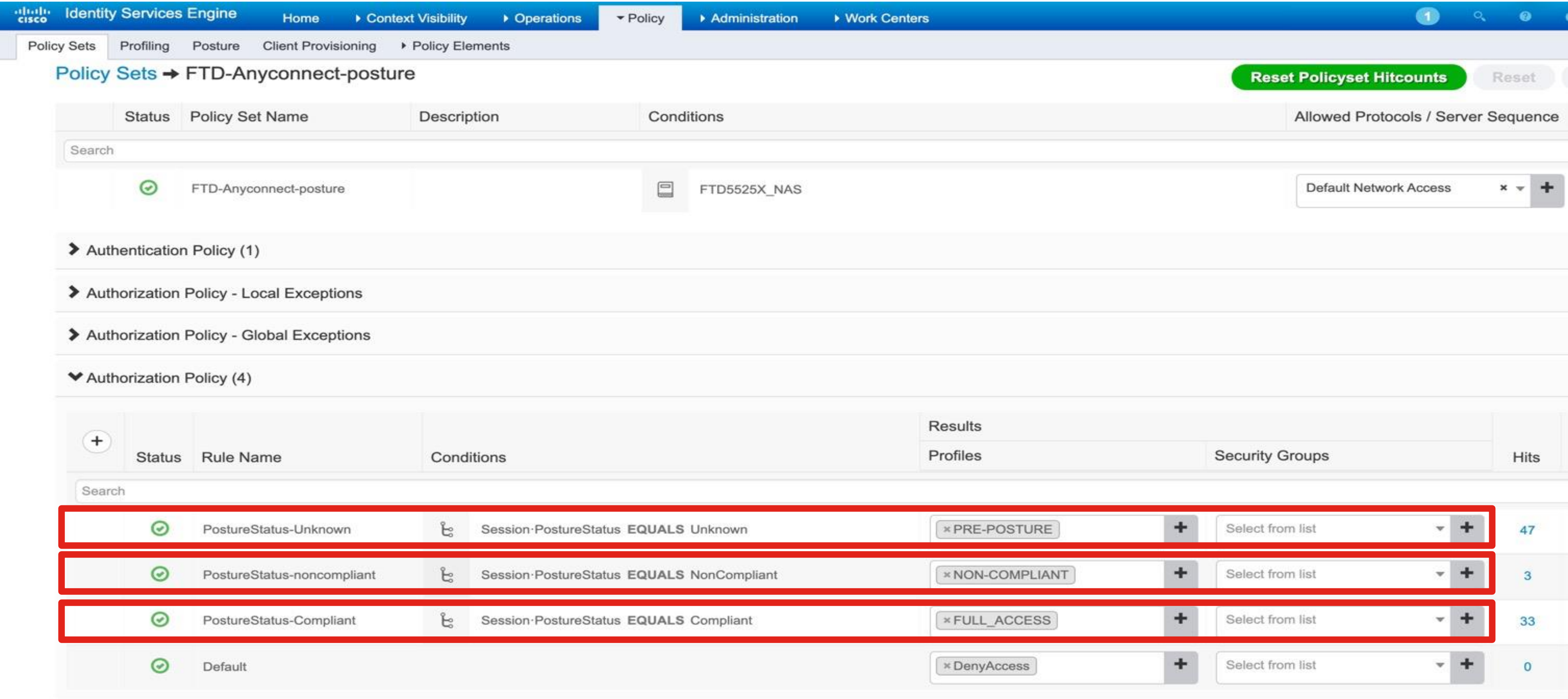
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Name	Profile
AC-Auth-IT	Cisco
Blackhole_Wireless_Access	Cisco
Cisco_IP_Phones	Cisco
Cisco_WebAuth	Cisco
FULL_ACCESS	Cisco
NON-COMPLIANT	Cisco
NSP_Onboard	Cisco
Non_Cisco_IP_Phones	Cisco
PRE-POSTURE	Cisco
RadiusProxyResponse	Cisco
cut-thru-proxy	Cisco
DenyAccess	
PermitAccess	



ISE Policy Sets

Policy>Policy Sets>{policy name}



Policy Sets → FTD-Anyconnect-posture

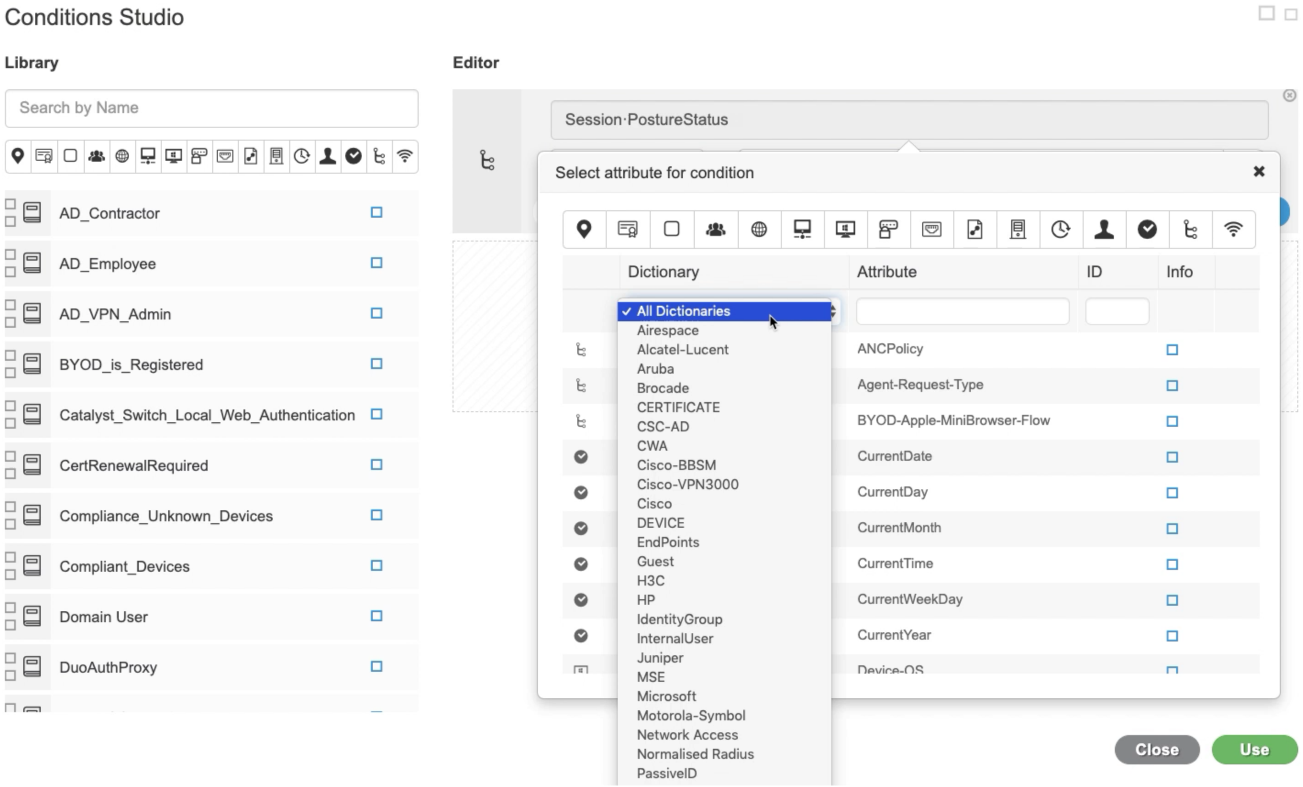
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✓	FTD-Anyconnect-posture		FTD5525X_NAS	Default Network Access

- Authentication Policy (1)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (4)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits
✓	PostureStatus-Unknown	Session·PostureStatus **EQUALS** Unknown	PRE-POSTURE	Select from list	47
✓	PostureStatus-noncompliant	Session·PostureStatus **EQUALS** NonCompliant	NON-COMPLIANT	Select from list	3
✓	PostureStatus-Compliant	Session·PostureStatus **EQUALS** Compliant	FULL_ACCESS	Select from list	33
✓	Default		DenyAccess	Select from list	0

ISE Authorization Profiles

Posture Status-Condition Studio



Conditions Studio

Library

Search by Name

- AD_Contractor
- AD_Employee
- AD_VPN_Admin
- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- CertRenewalRequired
- Compliance_Unknown_Devices
- Compliant_Devices
- Domain User
- DuoAuthProxy

Editor

Session·PostureStatus

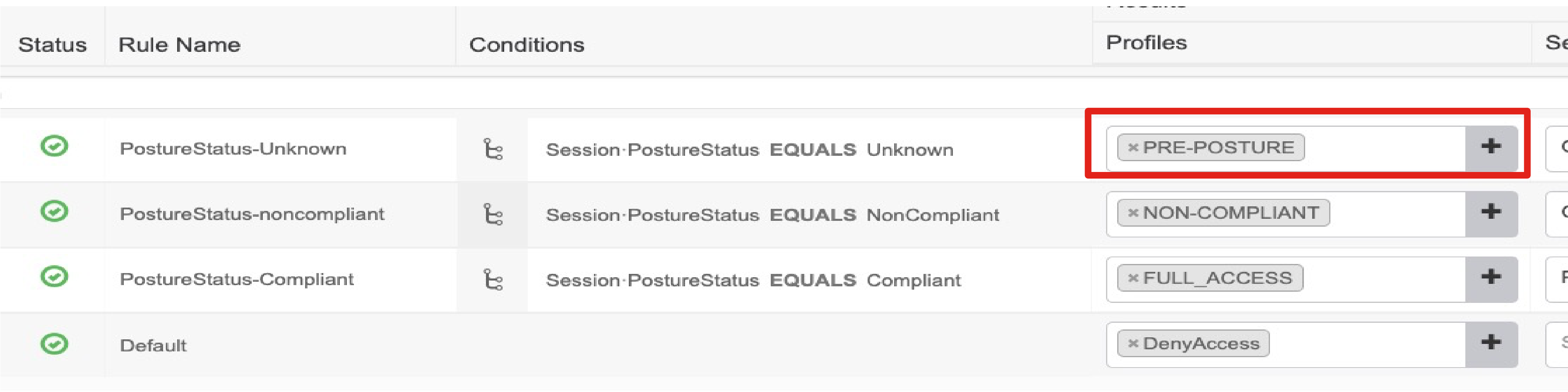
Select attribute for condition

Dictionary	Attribute	ID	Info
✓ All Dictionaries			
	ANCPolicy		□
	Agent-Request-Type		□
	BYOD-Apple-MiniBrowser-Flow		□
	CurrentDate		□
	CurrentDay		□
	CurrentMonth		□
	CurrentTime		□
	CurrentWeekDay		□
	CurrentYear		□
	Device-OS		□

- ✓ All Dictionaries
- Airespace
- Alcatel-Lucent
- Aruba
- Brocade
- CERTIFICATE
- CSC-AD
- CWA
- Cisco-BBSM
- Cisco-VPN3000
- Cisco
- DEVICE
- EndPoints
- Guest
- H3C
- HP
- IdentityGroup
- InternalUser
- Juniper
- MSE
- Microsoft
- Motorola-Symbol
- Network Access
- Normalised Radius
- PassiveID

ISE Authorization Profiles

Posture Status-Unknown

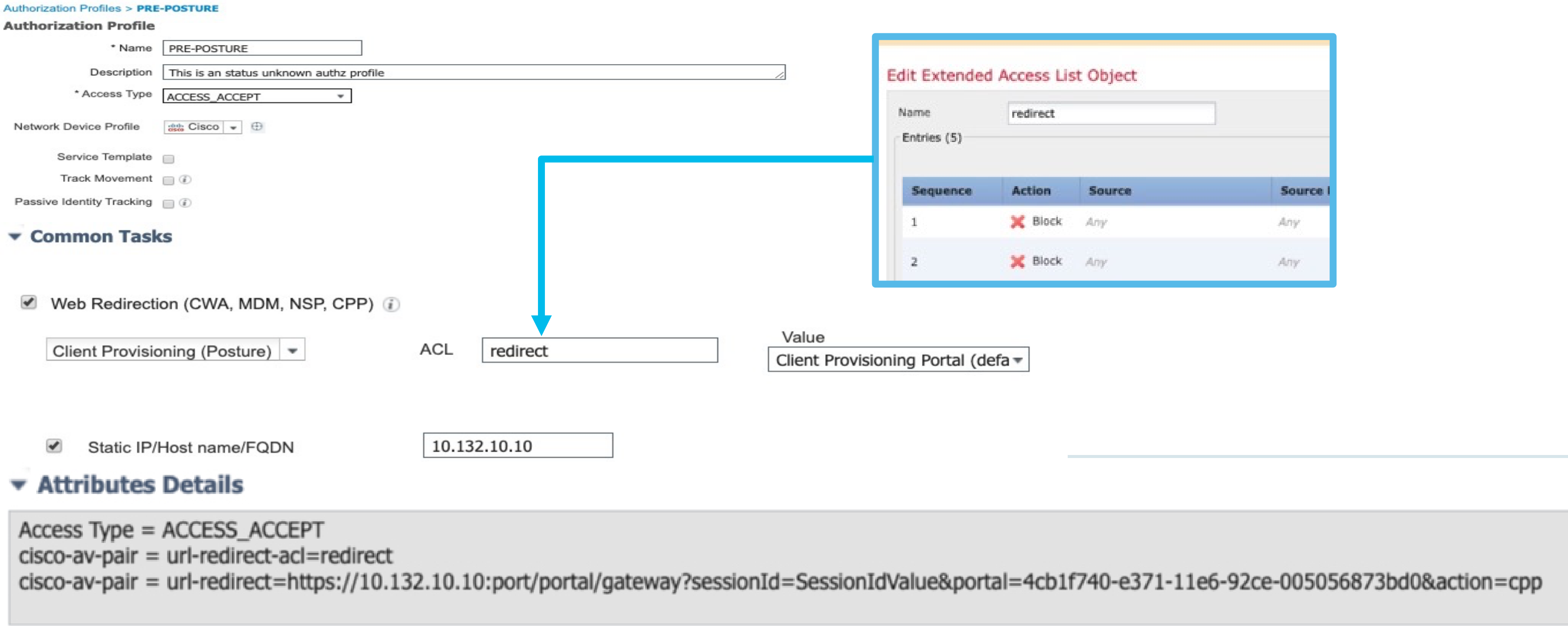


Status	Rule Name	Conditions	Profiles	Se
✓	PostureStatus-Unknown	Session·PostureStatus **EQUALS** Unknown	× PRE-POSTURE +	C
✓	PostureStatus-noncompliant	Session·PostureStatus **EQUALS** NonCompliant	× NON-COMPLIANT +	C
✓	PostureStatus-Compliant	Session·PostureStatus **EQUALS** Compliant	× FULL_ACCESS +	F
✓	Default		× DenyAccess +	S

ISE Authorization Profiles

Posture Status-Unknown

Policy>Policy Elements>Authorization>Authorization Profiles



Authorization Profiles > PRE-POSTURE

Authorization Profile

* Name	PRE-POSTURE
Description	This is an status unknown authz profile
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Passive Identity Tracking	□

Common Tasks

☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL redirect Value Client Provisioning Portal (defa

☑ Static IP/Host name/FQDN 10.132.10.10

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://10.132.10.10:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp
```

Edit Extended Access List Object

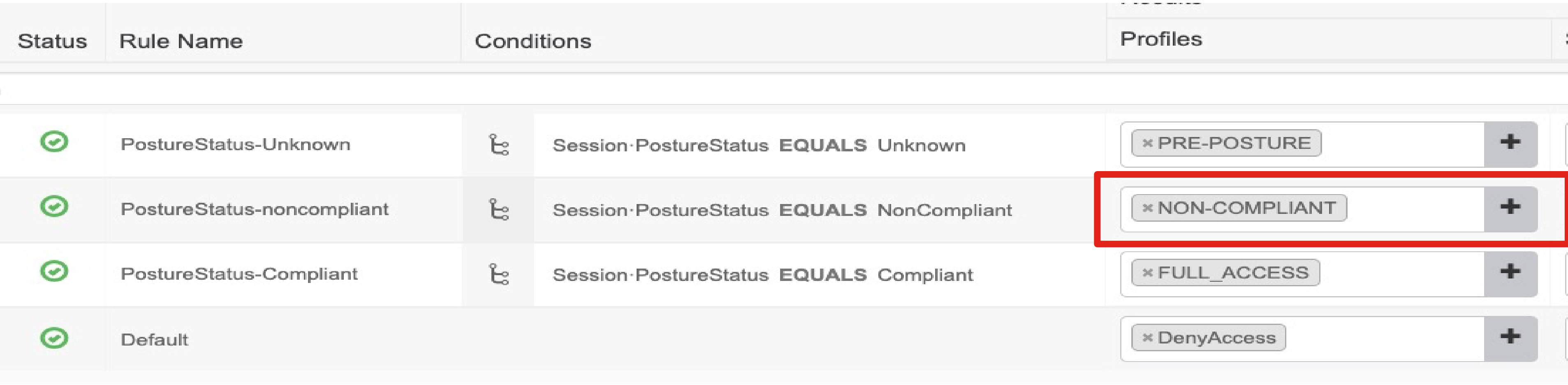
Name redirect

Entries (5)

Sequence	Action	Source	Source I
1	✗ Block	Any	Any
2	✗ Block	Any	Any

ISE Authorization Profiles

Posture Status-noncompliant

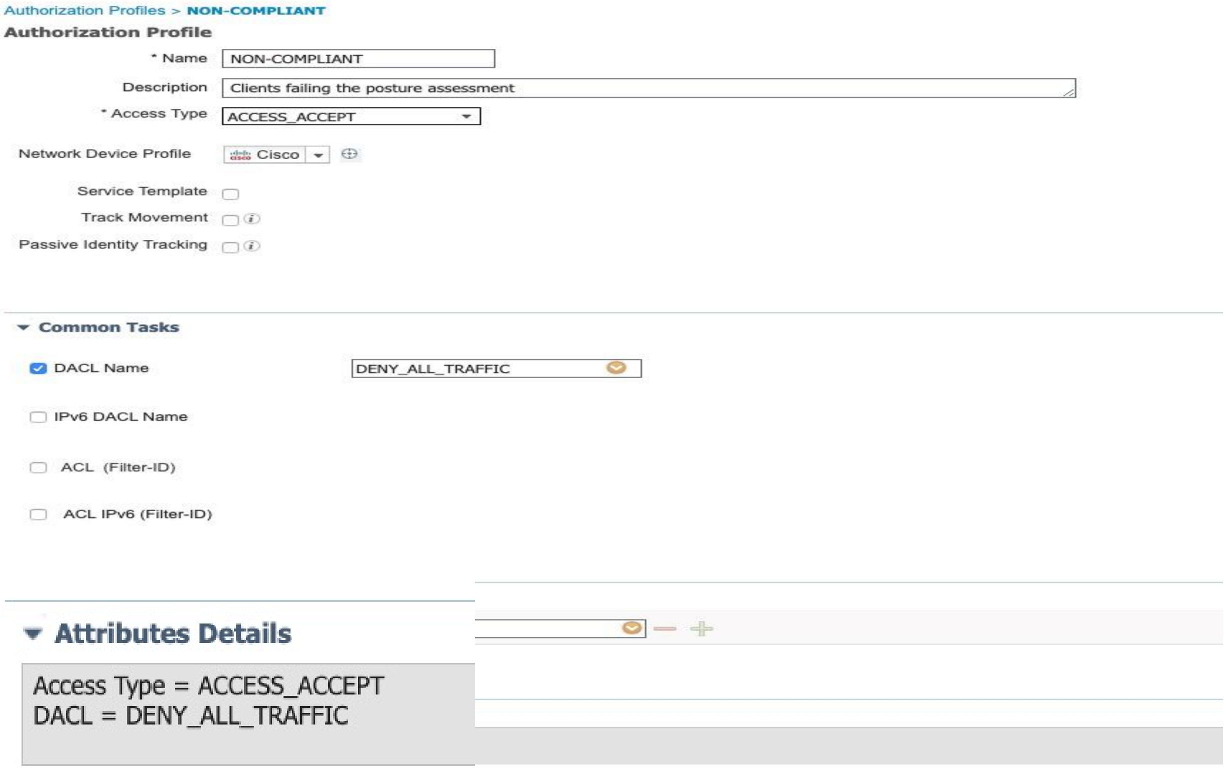


Status	Rule Name	Conditions	Profiles
✓	PostureStatus-Unknown	Session·PostureStatus **EQUALS** Unknown	× PRE-POSTURE +
✓	PostureStatus-noncompliant	Session·PostureStatus **EQUALS** NonCompliant	× NON-COMPLIANT +
✓	PostureStatus-Compliant	Session·PostureStatus **EQUALS** Compliant	× FULL_ACCESS +
✓	Default		× DenyAccess +

ISE Authorization Profiles

Posture Status-NonCompliant

Policy>Policy Elements>Authorization>Authorization Profiles



Authorization Profiles > **NON-COMPLIANT**

Authorization Profile

* Name	NON-COMPLIANT
Description	Clients failing the posture assessment
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Passive Identity Tracking	□

Common Tasks

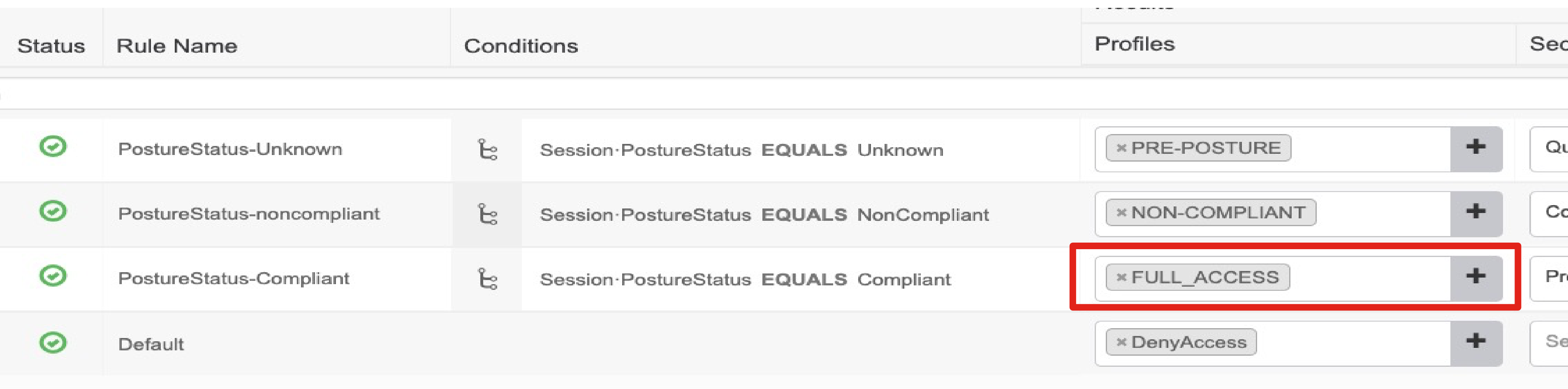
- ☑ DACL Name: DENY_ALL_TRAFFIC
- □ IPv6 DACL Name
- □ ACL (Filter-ID)
- □ ACL IPv6 (Filter-ID)

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = DENY_ALL_TRAFFIC

ISE Authorization Profiles

Posture Status-Compliant

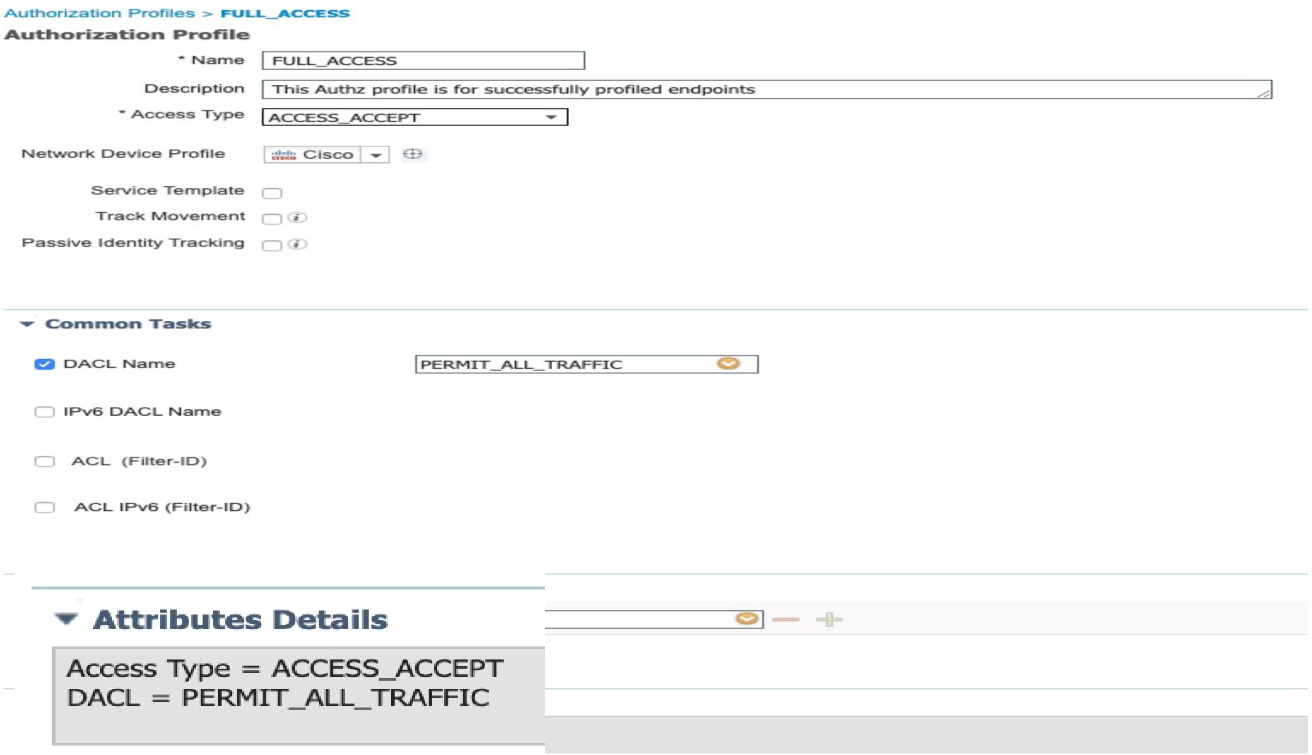


Status	Rule Name	Conditions	Profiles	Sec
✓	PostureStatus-Unknown	Session·PostureStatus **EQUALS** Unknown	× PRE-POSTURE +	Qu
✓	PostureStatus-noncompliant	Session·PostureStatus **EQUALS** NonCompliant	× NON-COMPLIANT +	Co
✓	PostureStatus-Compliant	Session·PostureStatus **EQUALS** Compliant	× FULL_ACCESS +	Pr
✓	Default		× DenyAccess +	Se

ISE Authorization Profiles

Posture Status-Compliant

Policy>Policy Elements>Authorization>Authorization Profiles



Authorization Profiles > FULL_ACCESS

Authorization Profile

* Name	FULL_ACCESS
Description	This Authz profile is for successfully profiled endpoints
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Passive Identity Tracking	□

Common Tasks

☑ DACL Name PERMIT_ALL_TRAFFIC

□ IPv6 DACL Name

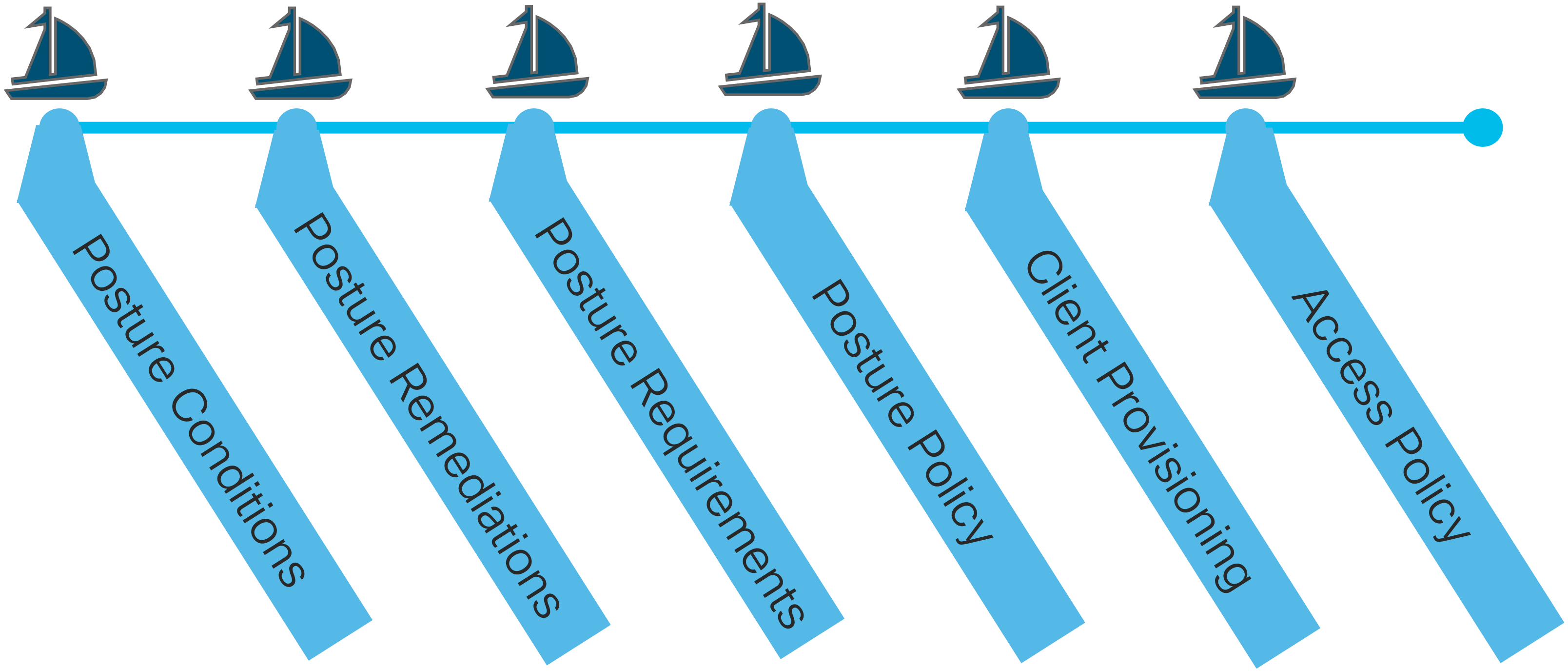
□ ACL (Filter-ID)

□ ACL IPv6 (Filter-ID)

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC

ISE Posture Configuration Steps



Posture Conditions

Posture Remediations

Posture Requirements

Posture Policy

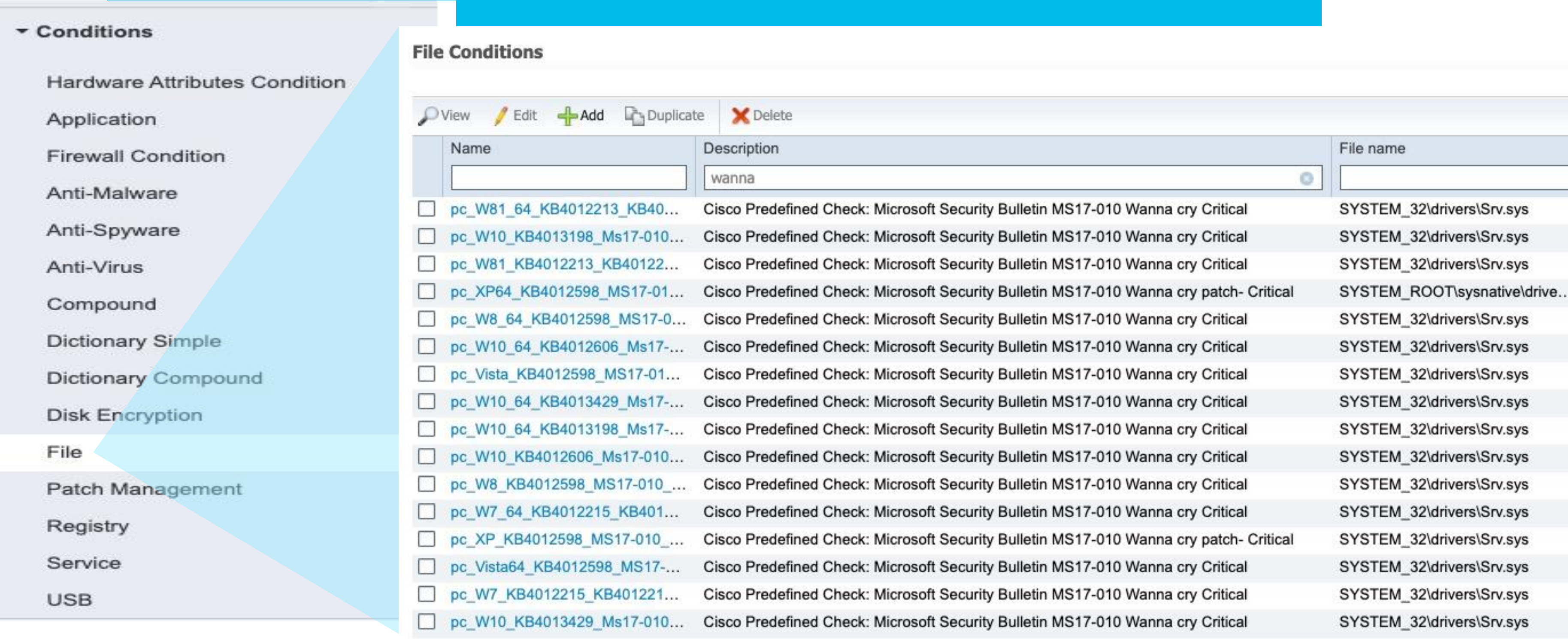
Client Provisioning

Access Policy

ISE Posture

Posture Conditions

Work Centers>Posture>Posture Elements>Conditions



- Conditions
  - Hardware Attributes Condition
  - Application
  - Firewall Condition
  - Anti-Malware
  - Anti-Spyware
  - Anti-Virus
  - Compound
  - Dictionary Simple
  - Dictionary Compound
  - Disk Encryption
  - File
  - Patch Management
  - Registry
  - Service
  - USB

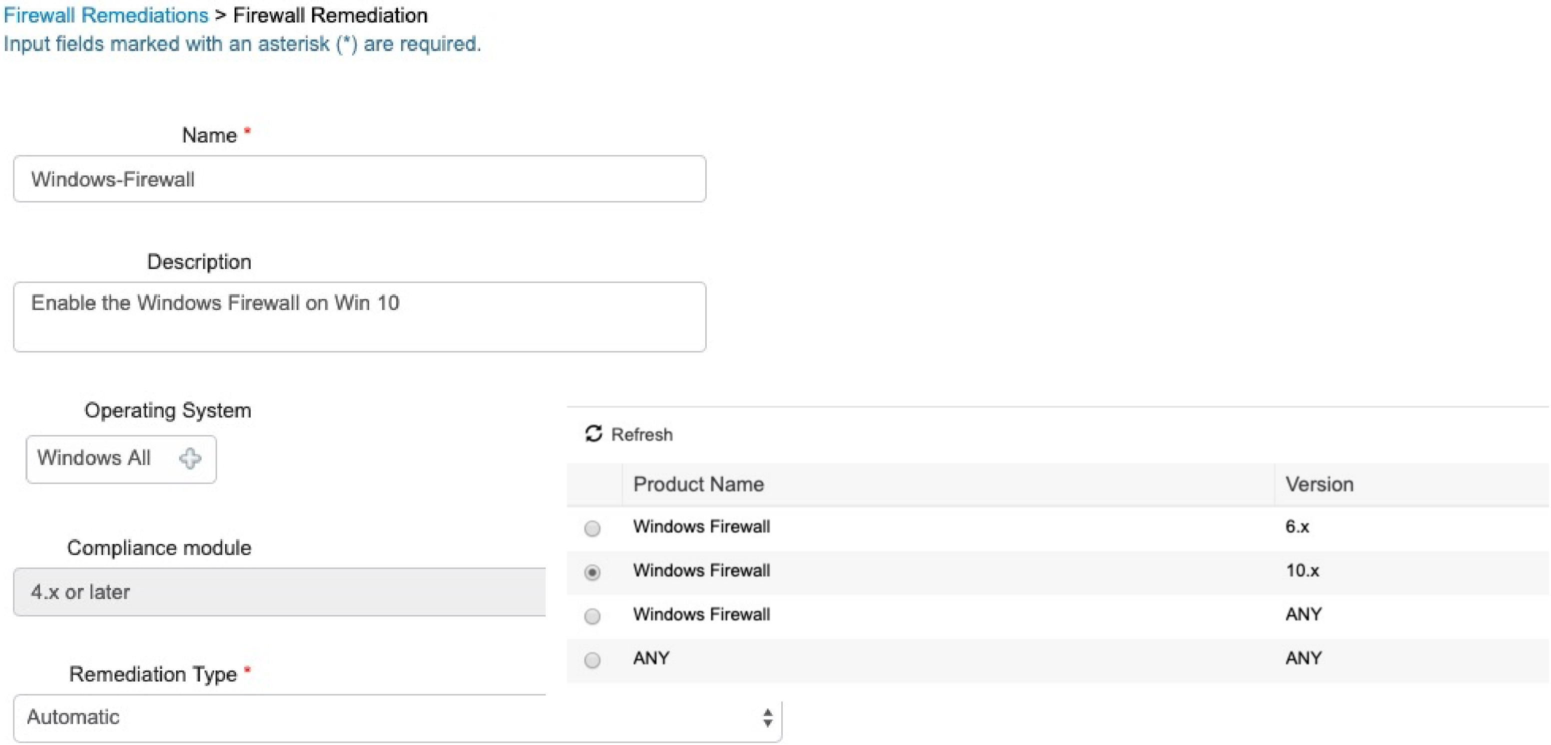
File Conditions

	Name	Description	File name
		wanna	
□	pc_W81_64_KB4012213_KB40...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W10_KB4013198_Ms17-010...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W81_KB4012213_KB40122...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_XP64_KB4012598_MS17-01...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry patch- Critical	SYSTEM_ROOT\sysnative\drive...
□	pc_W8_64_KB4012598_MS17-0...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W10_64_KB4012606_Ms17-...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_Vista_KB4012598_MS17-01...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W10_64_KB4013429_Ms17-...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W10_64_KB4013198_Ms17-...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W10_KB4012606_Ms17-010...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W8_KB4012598_MS17-010_...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W7_64_KB4012215_KB401...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_XP_KB4012598_MS17-010_...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry patch- Critical	SYSTEM_32\drivers\Srv.sys
□	pc_Vista64_KB4012598_MS17-...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W7_KB4012215_KB401221...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys
□	pc_W10_KB4013429_Ms17-010...	Cisco Predefined Check: Microsoft Security Bulletin MS17-010 Wanna cry Critical	SYSTEM_32\drivers\Srv.sys

ISE Posture

Posture Remediations

Work Centers> Posture> Posture Elements>Remediations



Firewall Remediations > Firewall Remediation

Input fields marked with an asterisk (*) are required.

Name *	Windows-Firewall
Description	Enable the Windows Firewall on Win 10
Operating System	Windows All
Compliance module	4.x or later
Remediation Type *	Automatic

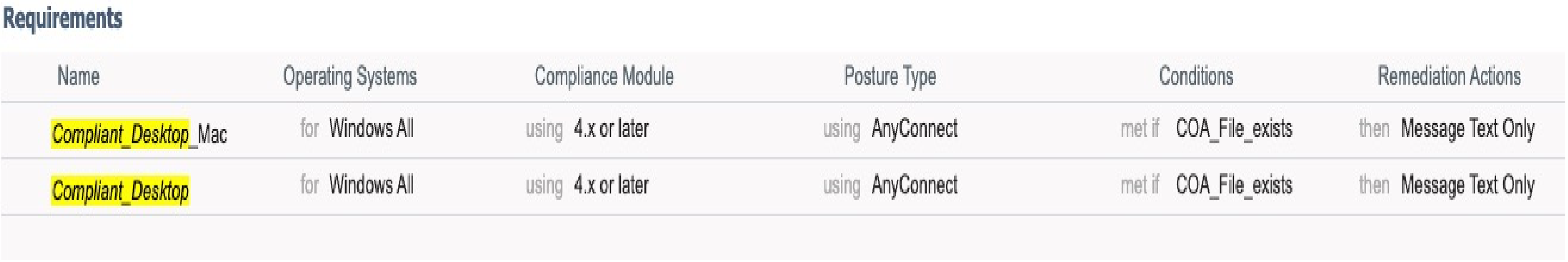
Refresh

	Product Name	Version
○	Windows Firewall	6.x
●	Windows Firewall	10.x
○	Windows Firewall	ANY
○	ANY	ANY

ISE Posture

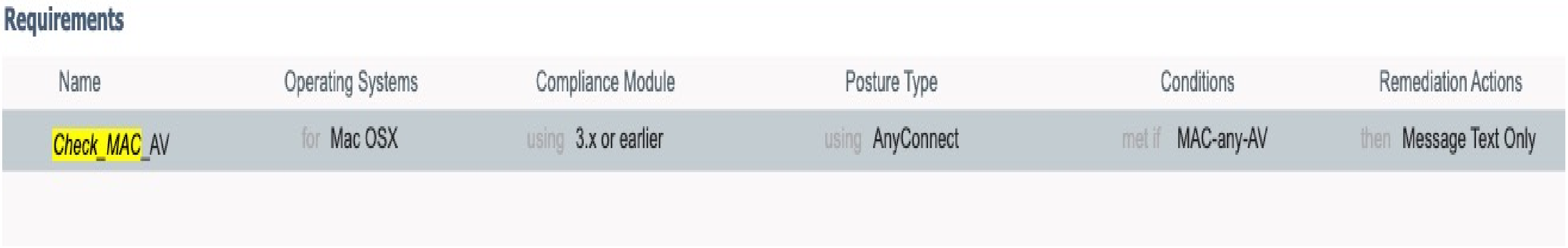
Posture Requirements

Work Centers> Posture> **Posture Elements>Requirements**



Requirements

Name	Operating Systems	Compliance Module	Posture Type	Conditions	Remediation Actions
Compliant_Desktop_Mac	for Windows All	using 4.x or later	using AnyConnect	met if COA_File_exists	then Message Text Only
Compliant_Desktop	for Windows All	using 4.x or later	using AnyConnect	met if COA_File_exists	then Message Text Only

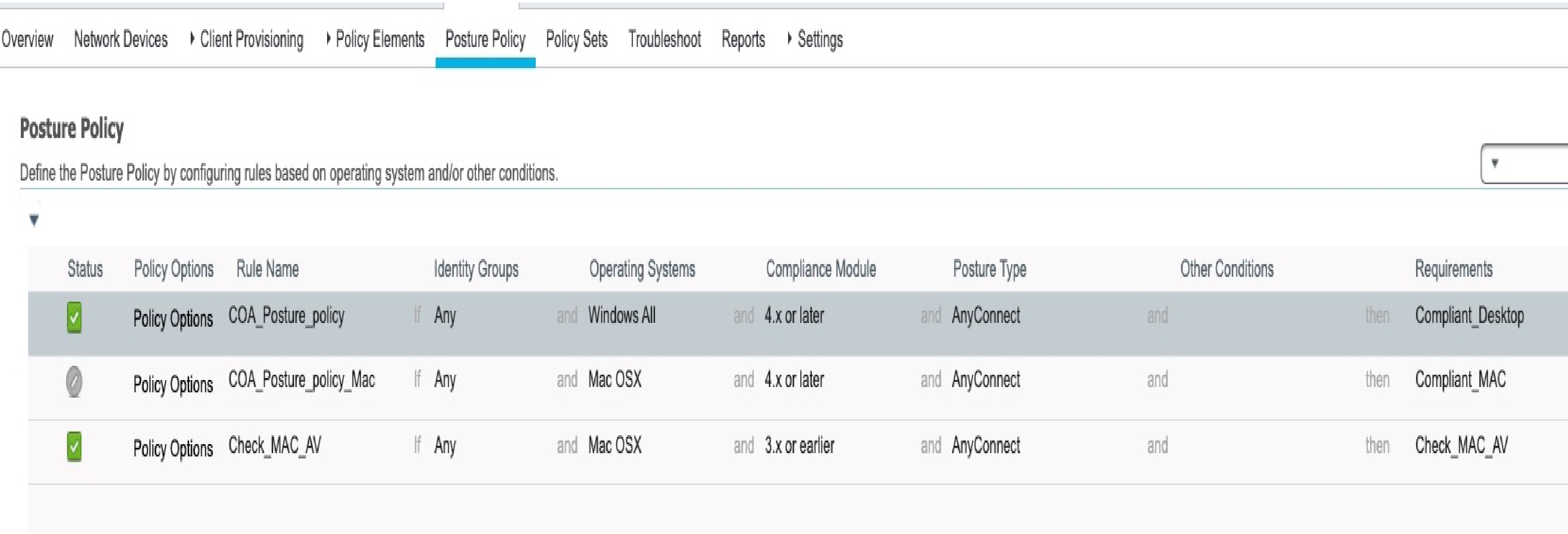


Requirements

Name	Operating Systems	Compliance Module	Posture Type	Conditions	Remediation Actions
Check_MAC_AV	for Mac OSX	using 3.x or earlier	using AnyConnect	met if MAC-any-AV	then Message Text Only

ISE Posture

Work Centers>Posture>Posture Policy



Posture Policy

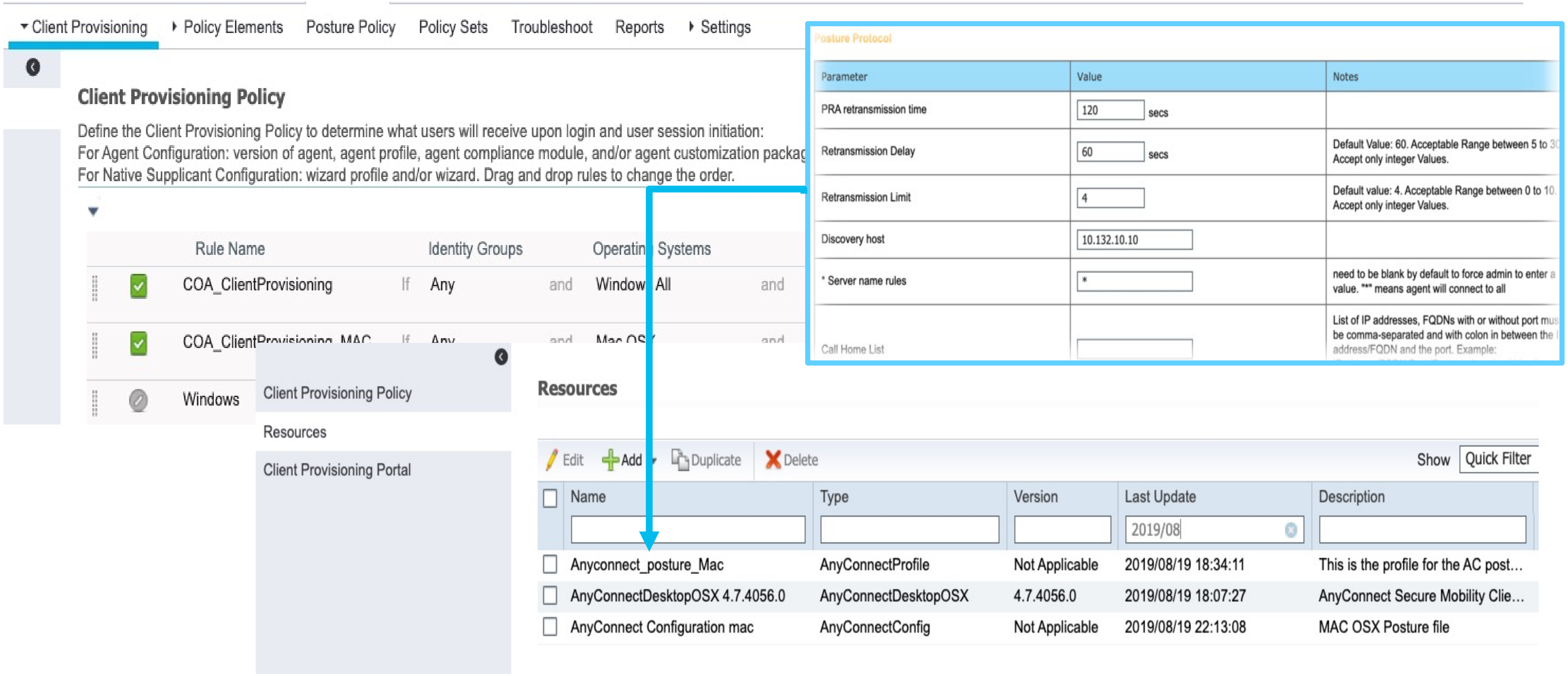
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements
✓	Policy Options	COA_Posture_policy	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and		then	Compliant_Desktop
⊘	Policy Options	COA_Posture_policy_Mac	If	Any	and	Mac OSX	and	4.x or later	and	AnyConnect	and		then	Compliant_MAC
✓	Policy Options	Check_MAC_AV	If	Any	and	Mac OSX	and	3.x or earlier	and	AnyConnect	and		then	Check_MAC_AV

ISE Posture

Client Provisioning

Work Centers>Posture>Client Provisioning



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization packag
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems	
☑	COA_ClientProvisioning	If	Any	and	Window All	and
☑	COA_ClientProvisioning_MAC	If	Any	and	Mac OSX	and
	Windows					

Posture Protocol

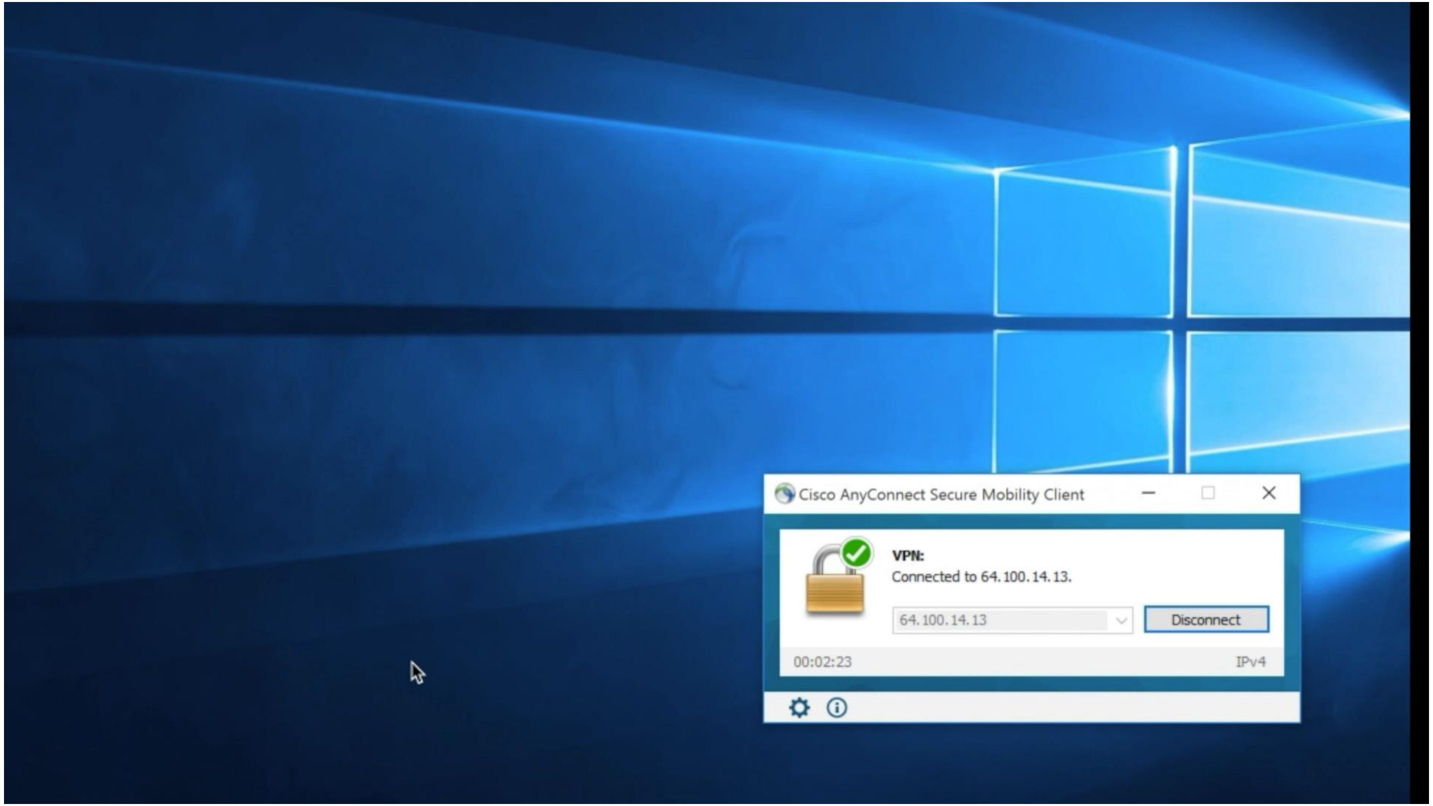
Parameter	Value	Notes
PRA retransmission time	120 secs	
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 3 Accept only integer Values.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.
Discovery host	10.132.10.10	
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List		List of IP addresses, FQDNs with or without port mus be comma-separated and with colon in between the address/FQDN and the port. Example:

Resources

☐	Name	Type	Version	Last Update	Description
				2019/08	
☐	Anyconnect_posture_Mac	AnyConnectProfile	Not Applicable	2019/08/19 18:34:11	This is the profile for the AC post...
☐	AnyConnectDesktopOSX 4.7.4056.0	AnyConnectDesktopOSX	4.7.4056.0	2019/08/19 18:07:27	AnyConnect Secure Mobility Clie...
☐	AnyConnect Configuration mac	AnyConnectConfig	Not Applicable	2019/08/19 22:13:08	MAC OSX Posture file

ISE Posture

Client Provisioning



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to 64.100.14.13.

64.100.14.13

Disconnect

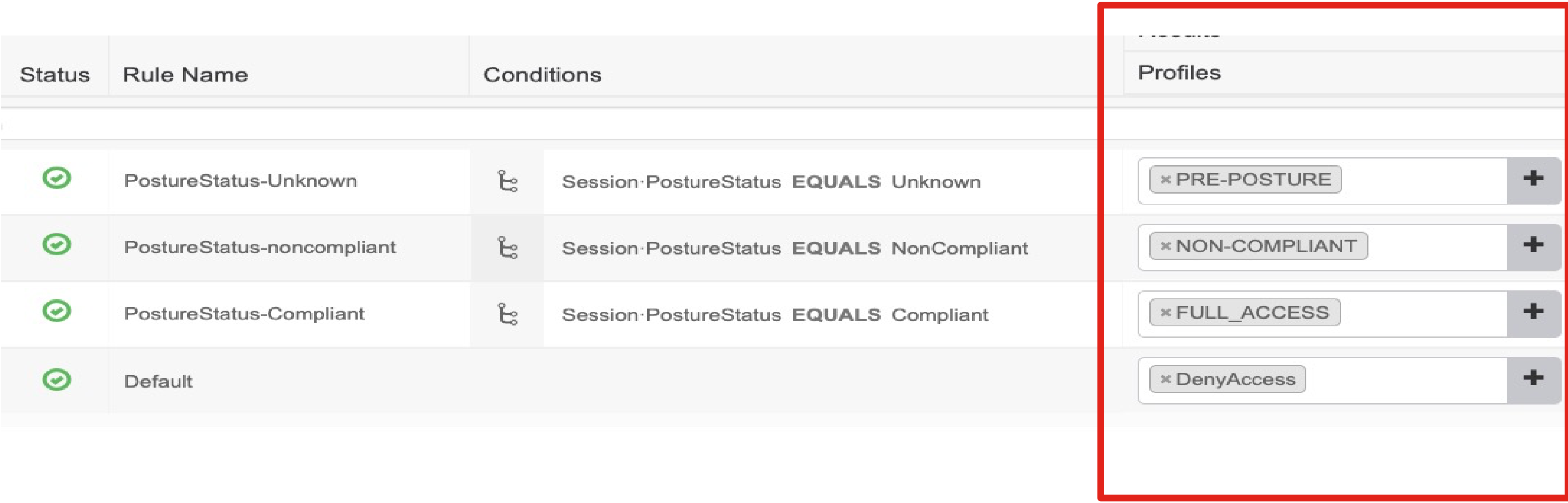
00:02:23

IPv4

ISE Posture

Access Policy

Work Centers>Posture>Policy Sets



Status	Rule Name	Conditions	Profiles
✓	PostureStatus-Unknown	Session·PostureStatus **EQUALS** Unknown	× PRE-POSTURE
✓	PostureStatus-noncompliant	Session·PostureStatus **EQUALS** NonCompliant	× NON-COMPLIANT
✓	PostureStatus-Compliant	Session·PostureStatus **EQUALS** Compliant	× FULL_ACCESS
✓	Default		× DenyAccess

ISE Posture Configuration

Detailed posture training materials – Video series from Tim Abbott

Cisco ISE Posture Configuration

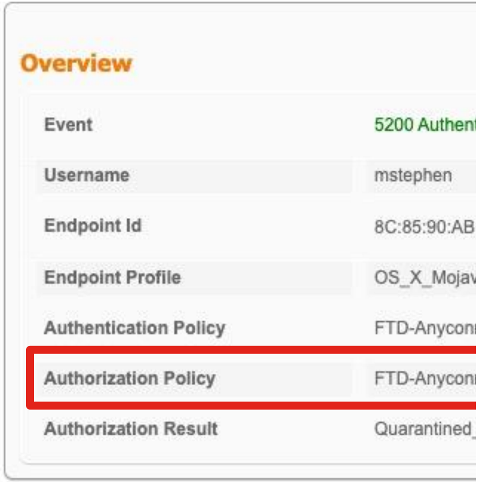
Posture Conditions

Tim Abbott
Technical Marketing Engineer
December 2019

https://youtu.be/6Kj8P8Hn7dY

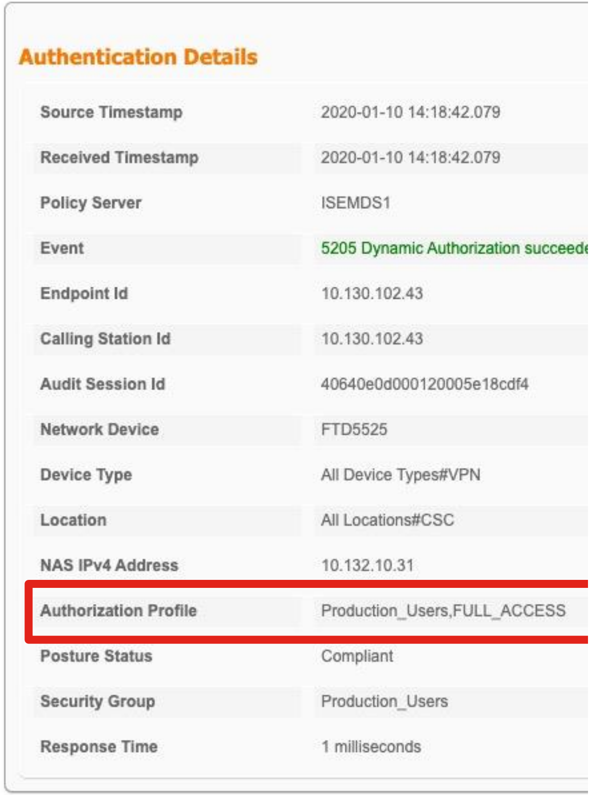
Posture Remediations:	https://youtu.be/GTHcEjJOKvc
Posture Requirements:	https://youtu.be/kmS6_SxDYMY
Posture Policy:	https://youtu.be/148VoXUCccg
Client Provisioning:	https://youtu.be/z14iNE4Luw0
Access Policy:	https://youtu.be/VEmuM865hW0

ISE Live Logs



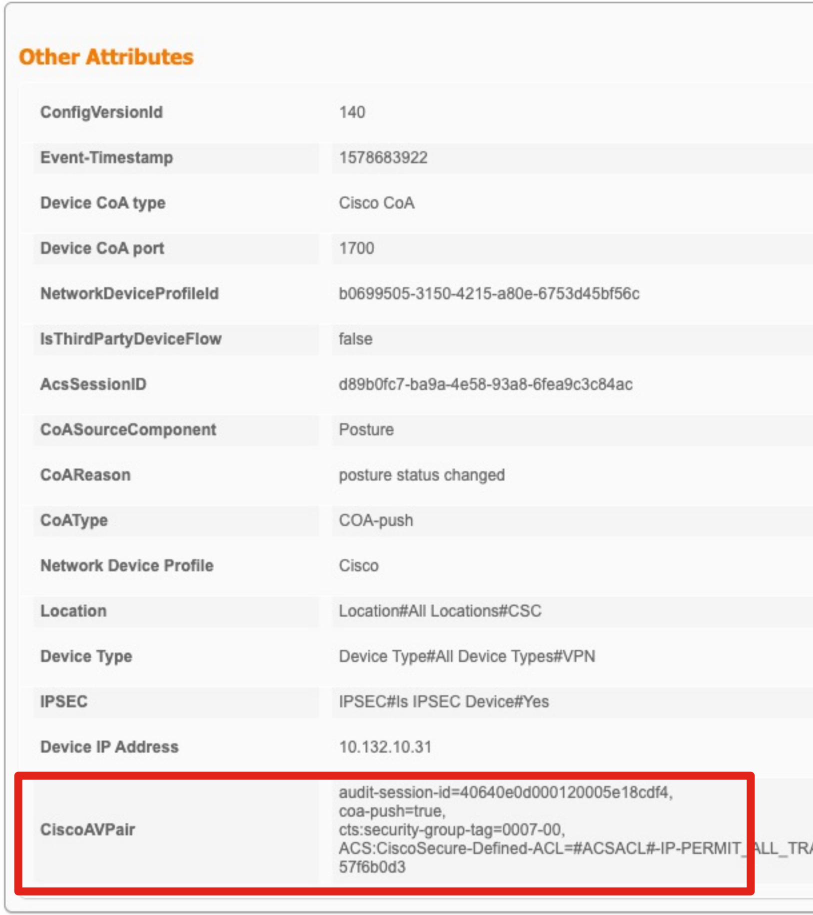
Overview

Event	5200 Authent
Username	mstephen
Endpoint Id	8C:85:90:AB
Endpoint Profile	OS_X_Mojav
Authentication Policy	FTD-Anycon
Authorization Policy	FTD-Anycon
Authorization Result	Quarantined_



Authentication Details

Source Timestamp	2020-01-10 14:18:42.079
Received Timestamp	2020-01-10 14:18:42.079
Policy Server	ISEMDS1
Event	5205 Dynamic Authorization succeede
Endpoint Id	10.130.102.43
Calling Station Id	10.130.102.43
Audit Session Id	40640e0d000120005e18cdf4
Network Device	FTD5525
Device Type	All Device Types#VPN
Location	All Locations#CSC
NAS IPv4 Address	10.132.10.31
Authorization Profile	Production_Users,FULL_ACCESS
Posture Status	Compliant
Security Group	Production_Users
Response Time	1 milliseconds

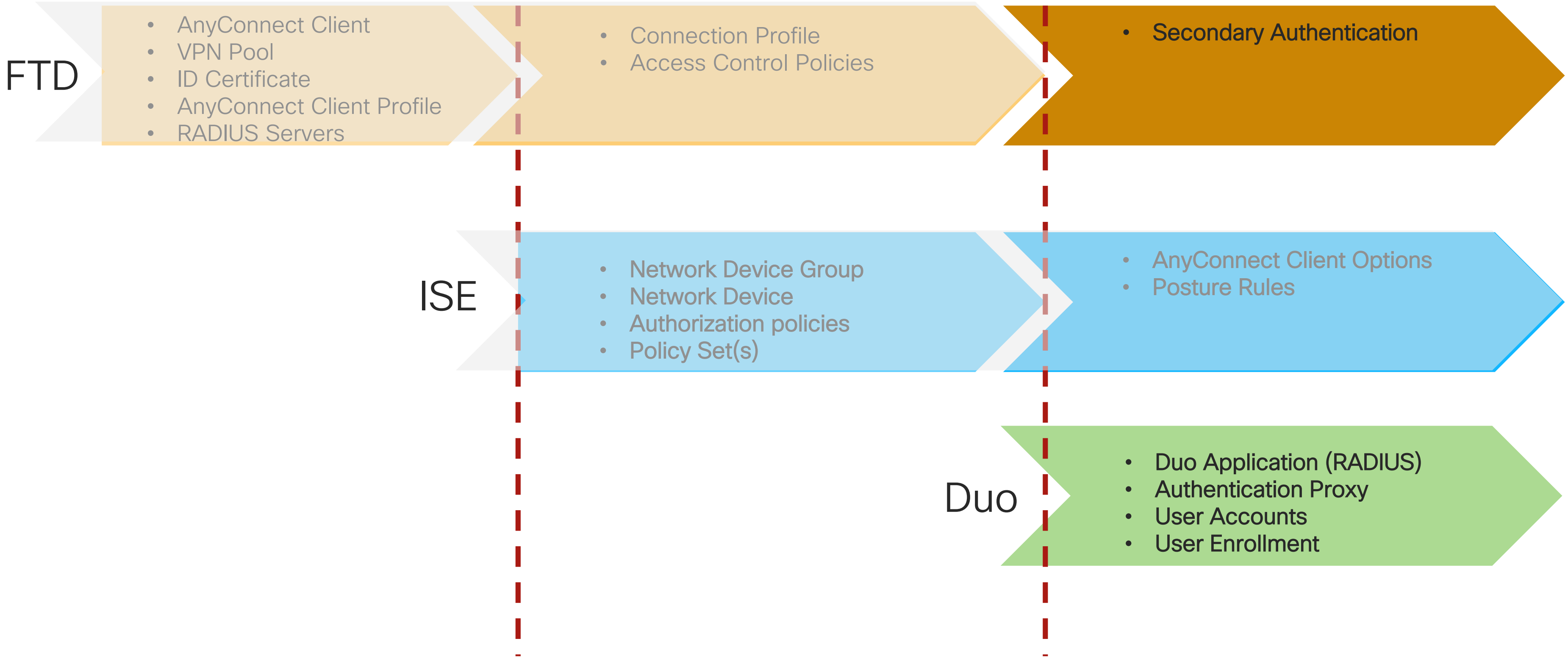


Other Attributes

ConfigVersionId	140
Event-Timestamp	1578683922
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	d89b0fc7-ba9a-4e58-93a8-6fea9c3c84ac
CoASourceComponent	Posture
CoAReason	posture status changed
CoAType	COA-push
Network Device Profile	Cisco
Location	Location#All Locations#CSC
Device Type	Device Type#All Device Types#VPN
IPSEC	IPSEC#Is IPSEC Device#Yes
Device IP Address	10.132.10.31
CiscoAVPair	audit-session-id=40640e0d000120005e18cdf4, coa-push=true, cts:security-group-tag=0007-00, ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRA 57f6b0d3

Duo Configuration

Roadmap to configuring



FTD

- AnyConnect Client
- VPN Pool
- ID Certificate
- AnyConnect Client Profile
- RADIUS Servers

- Connection Profile
- Access Control Policies

- Secondary Authentication

ISE

- Network Device Group
- Network Device
- Authorization policies
- Policy Set(s)

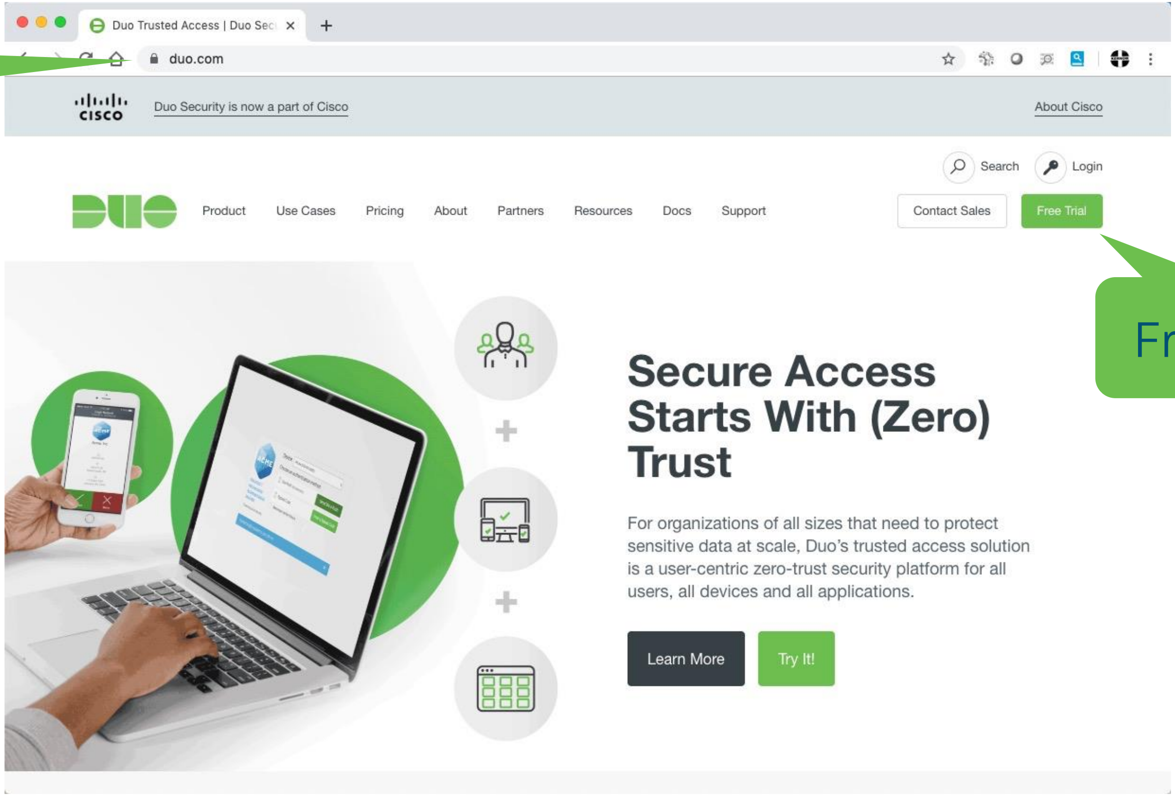
- AnyConnect Client Options
- Posture Rules

Duo

- Duo Application (RADIUS)
- Authentication Proxy
- User Accounts
- User Enrollment

Cisco Duo Multifactor Authentication (MFA)

Duo.com



Duo Trusted Access | Duo Sec

duo.com

Duo Security is now a part of Cisco

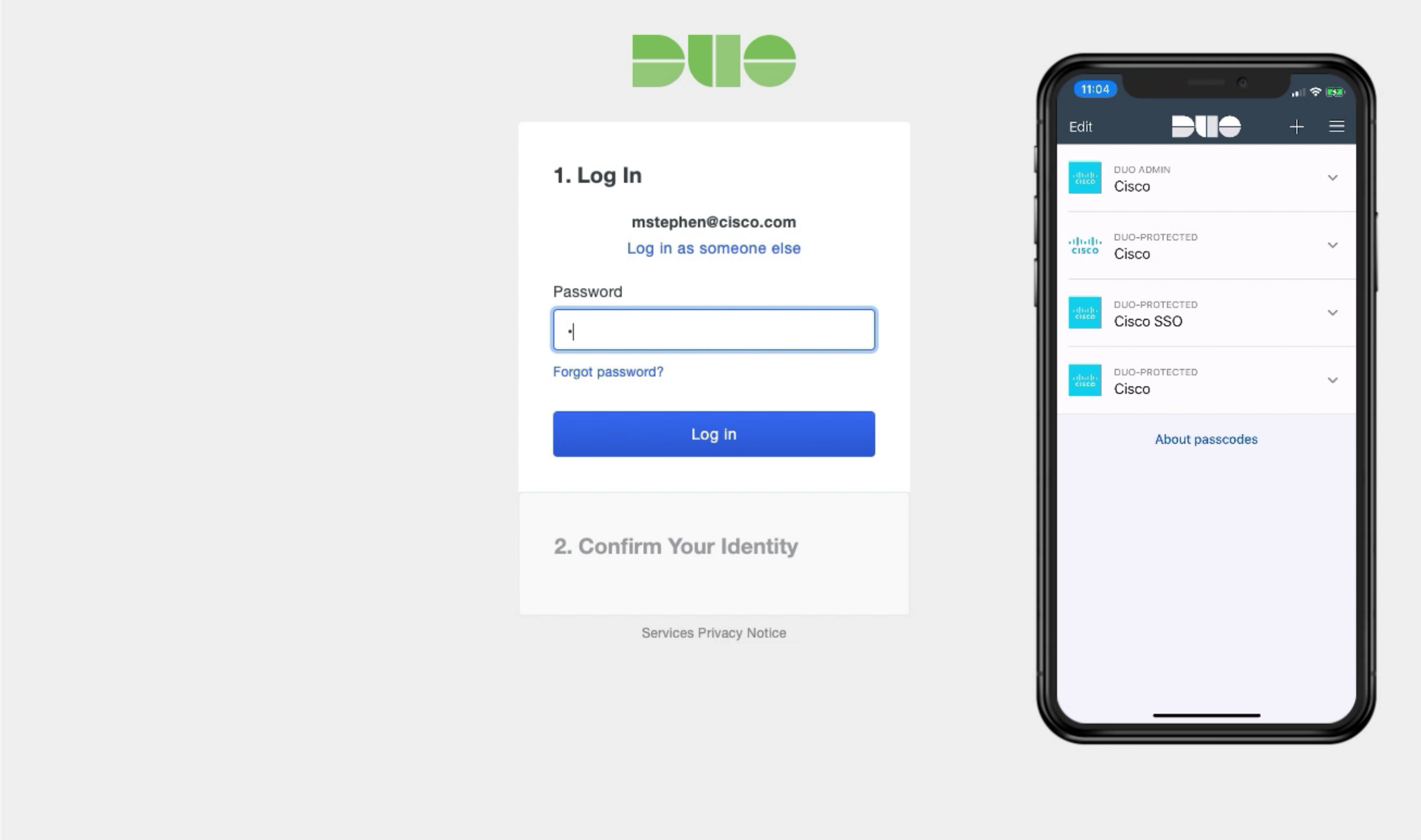
About Cisco

Secure Access Starts With (Zero) Trust

For organizations of all sizes that need to protect sensitive data at scale, Duo's trusted access solution is a user-centric zero-trust security platform for all users, all devices and all applications.

Free Trial

Duo Administration



1. Log In

mstephen@cisco.com

Log in as someone else

Password

Forgot password?

Log in

2. Confirm Your Identity

Services Privacy Notice

11:04

Edit

DUO ADMIN
Cisco

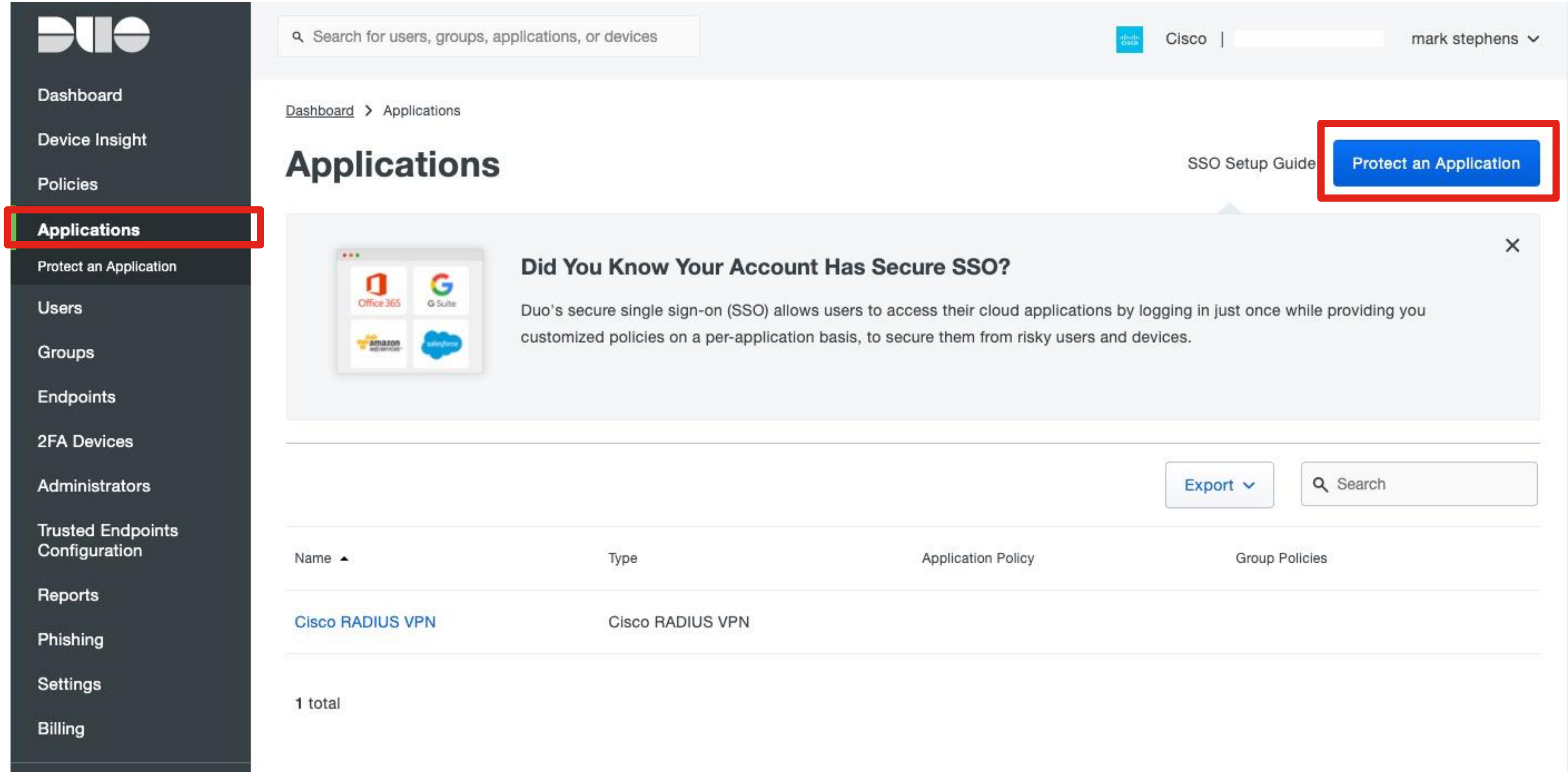
DUO-PROTECTED
Cisco

DUO-PROTECTED
Cisco SSO

DUO-PROTECTED
Cisco

About passcodes

Configuring the FTD Authentication Proxy



Applications

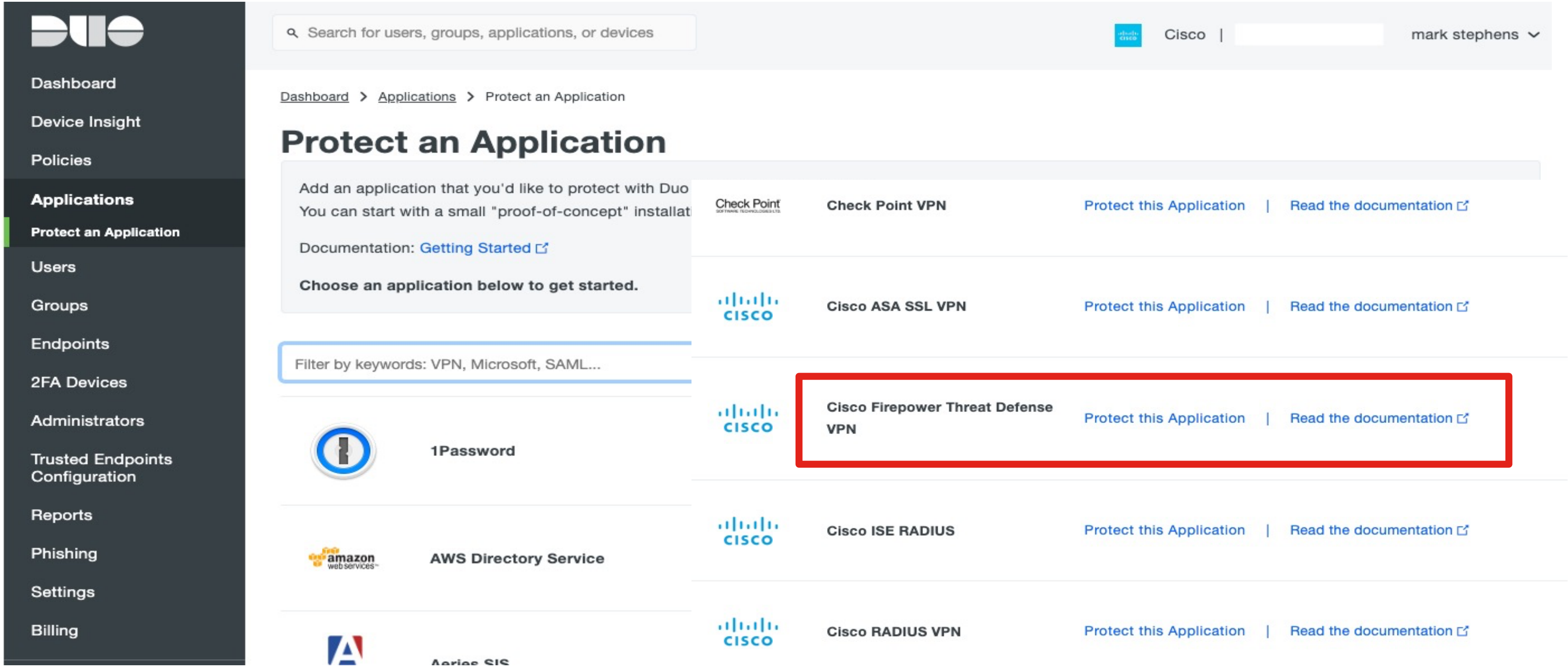
Did You Know Your Account Has Secure SSO?

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.

Name ▲	Type	Application Policy	Group Policies
Cisco RADIUS VPN	Cisco RADIUS VPN		

1 total

Duo Portal Configuration (cont)



Dashboard > Applications > Protect an Application

Protect an Application

Add an application that you'd like to protect with Duo
You can start with a small "proof-of-concept" installat

Documentation: Getting Started

Choose an application below to get started.

Filter by keywords: VPN, Microsoft, SAML...

Check Point	Check Point VPN	Protect this Application	Read the documentation
cisco	Cisco ASA SSL VPN	Protect this Application	Read the documentation
cisco	Cisco Firepower Threat Defense VPN	Protect this Application	Read the documentation
cisco	Cisco ISE RADIUS	Protect this Application	Read the documentation
cisco	Cisco RADIUS VPN	Protect this Application	Read the documentation

1Password

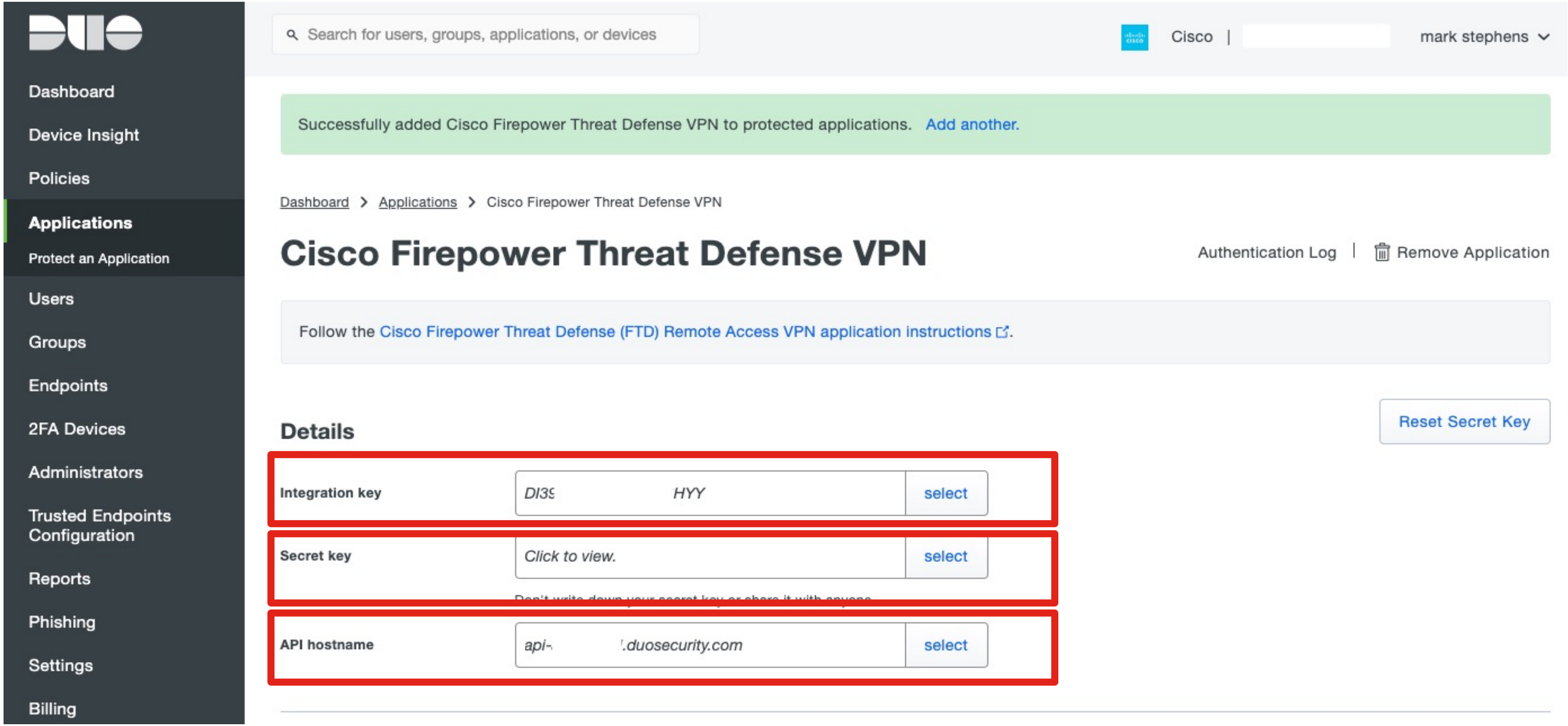
AWS Directory Service

Aeries SIS

https://duo.com/docs/cisco-firepower

cisco Live!

Duo Portal Configuration (cont)



Successfully added Cisco Firepower Threat Defense VPN to protected applications. Add another.

Dashboard > Applications > Cisco Firepower Threat Defense VPN

Cisco Firepower Threat Defense VPN

Follow the Cisco Firepower Threat Defense (FTD) Remote Access VPN application instructions.

Details

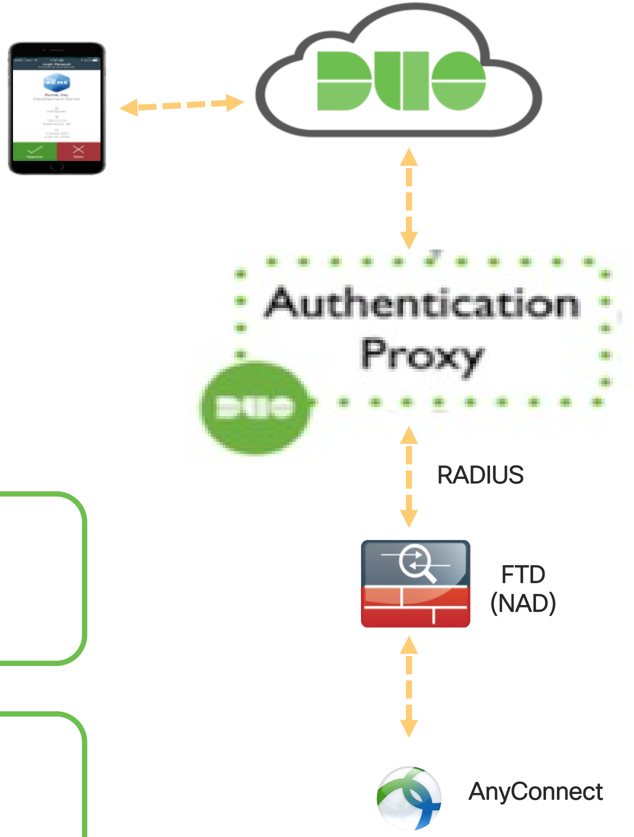
Integration key	DI3S[redacted]HYY	select
Secret key	Click to view. Don't write down your secret key or share it with anyone.	select
API hostname	api-[redacted].duosecurity.com	select

Duo Authentication Proxy

- Windows Server 2008 R2 or later (Server 2016 or 2019 recommended)
- CentOS 7 or later
- Red Hat Enterprise Linux 7 or later
- Ubuntu 16.04 or later
- Debian 7 or later.

Download the proxy from here:
https://dl.duosecurity.com/duoauthproxy-latest.exe

Detailed Training video material:
https://duo.com/docs/authproxy-overview

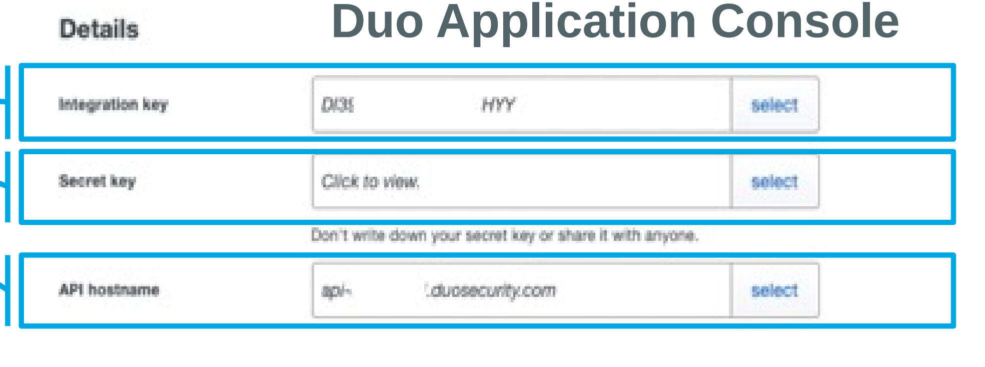


Duo Authentication Proxy

authproxy.cfg

```
[radius_server_auto]
ikey=yyyy8<from Duo Console8<yyyy
skey=-xxxxx8<from Duo Console8<xxxxx
api_host=api-xxxxxx.duosecurity.com
client=duo_only_client
radius_ip_1=<FTD2 IP address>
radius_secret_1=<secret key1>
radius_ip_2=<FTD2 IP address>
radius_secret_2=<secret key2>
port=1812

[duo_only_client]
```

Duo Application Console



Details

Integration key: DI3 HYY

Secret key: Click to view.

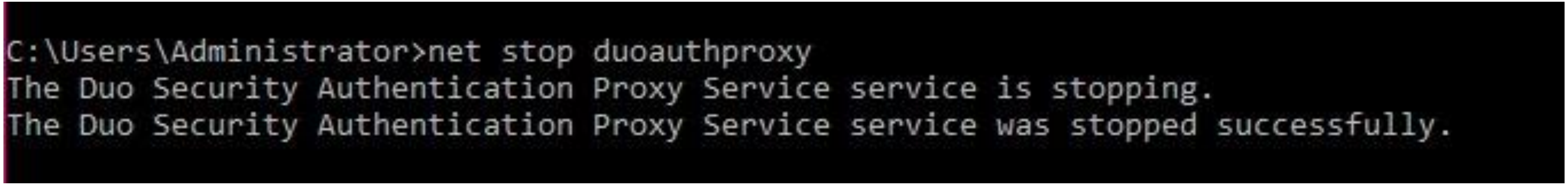
Don't write down your secret key or share it with anyone.

API hostname: api- .duosecurity.com

Windows (64-bit)	C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg
Windows (32-bit)	C:\Program Files\Duo Security Authentication Proxy\conf\authproxy.cfg
Linux	/opt/duoauthproxy/conf/authproxy.cfg

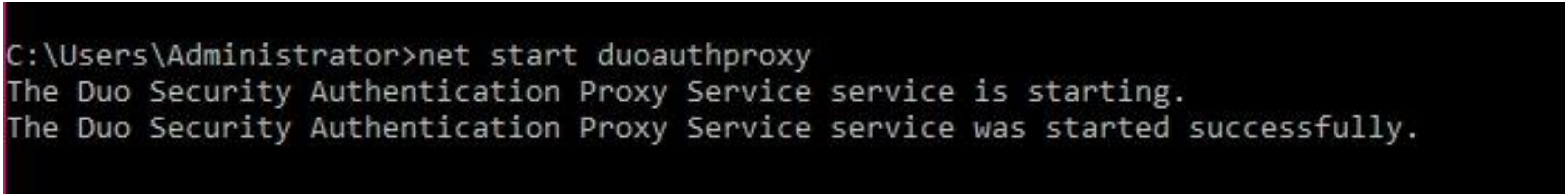
Duo Authentication Proxy

Windows: Stopping the authentication proxy Service



```
C:\Users\Administrator>net stop duoauthproxy
The Duo Security Authentication Proxy Service service is stopping.
The Duo Security Authentication Proxy Service service was stopped successfully.
```

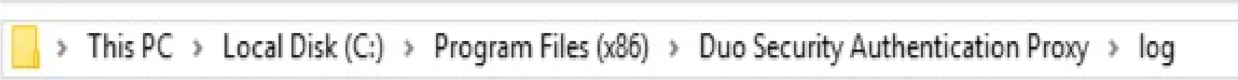
Windows: Starting the authentication proxy Service



```
C:\Users\Administrator>net start duoauthproxy
The Duo Security Authentication Proxy Service service is starting.
The Duo Security Authentication Proxy Service service was started successfully.
```

Trouble Shooting Duo Authentication Proxy

Authproxy.log


This PC › Local Disk (C:) › Program Files (x86) › Duo Security Authentication Proxy › log

```
[main]
Debug=true
```

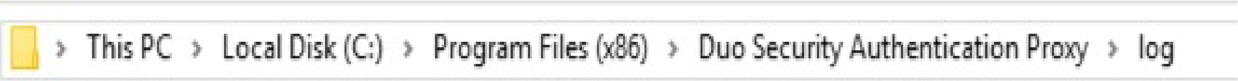
*Don’t forget to stop and restart the authentication proxy service

```
[DuoForwardServer (UDP)] dropping packet from 10.132.10.24:1145 - Unknown Client: 10.132.10.24
[DuoForwardServer (UDP)] Sending request from 10.132.10.31 to radius_server_auto
[DuoForwardServer (UDP)] Received new request id 26 from ('10.132.10.31', 16847)
[DuoForwardServer (UDP)] (('10.132.10.31', 16847), mstephen, 26): login attempt for username u'mstephen'
[DuoForwardServer (UDP)] http POST to https://api-axxxx.duosecurity.com:443/rest/v1/preauth
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPClientFactory: https://api-axxxx.duosecurity.com:443/rest/v1/preauth>
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.132.10.31', 16847), mstephen, 26): Got preauth result for: u'auth'
[HTTPPageGetter (TLSMemoryBIOProtocol),client] Valid ip check passed for: 68.110.181.206.
[HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-axxxxx.duosecurity.com:443/rest/v1/auth
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPClientFactory: https://api-axxxx.duosecurity.com:443/rest/v1/auth>
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPClientFactory: https://api-a64b806d.duosecurity.com:443/rest/v1/preauth>
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.132.10.31', 16847), mstephen, 26): Duo authentication returned 'allow': 'Success. Logging you in...'
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.132.10.31', 16847), mstephen, 26): Returning response code 2: AccessAccept
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.132.10.31', 16847), mstephen, 26): Sending response
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPClientFactory: https://api-axxxx.duosecurity.com:443/rest/v1/auth>
```

Log Decode: https://help.duo.com/s/article/2953?language=en_US

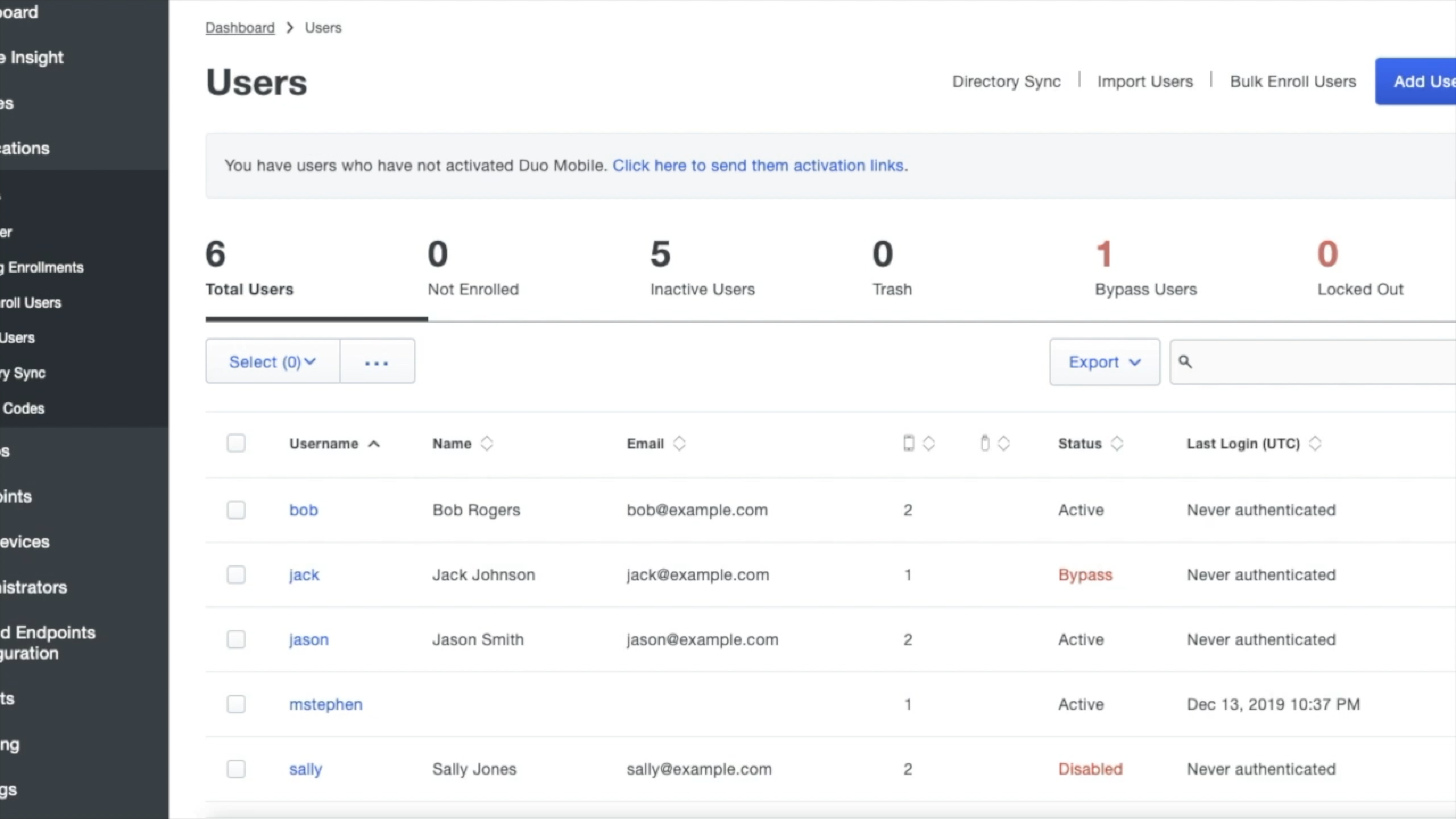
Trouble Shooting Duo Authentication Proxy

Connectivity_tool.log



This PC › Local Disk (C:) › Program Files (x86) › Duo Security Authentication Proxy › log

```
2019-12-11T03:20:47-0800 [duoauthproxy.lib.log#info] Testing section 'radius_server_auto' with configuration:
2019-12-11T03:20:47-0800 [duoauthproxy.lib.log#info] {'api_host': 'api-axxxxx.duosecurity.com',
            'client': 'duo_only_client',
            'ikey': ‘DIYxxxxxxxxxxxW77',
            'port': '1812',
            'radius_ip_1': '10.132.10.24',
            'radius_ip_2': '10.132.10.31',
            'radius_secret_1': '*****',
            'radius_secret_2': '*****',
            'skey': '*****[40]'}
[duoauthproxy.lib.log#info] There are no configuration problems
[duoauthproxy.lib.log#info] ----------------------------
[duoauthproxy.lib.log#info] Testing section 'duo_only_client' with configuration:
[duoauthproxy.lib.log#info] {}
[duoauthproxy.lib.log#info] There are no configuration problems
[duoauthproxy.lib.log#info] ----------------------------
[duoauthproxy.lib.log#info] SUMMARY
[duoauthproxy.lib.log#info] No issues detected
```



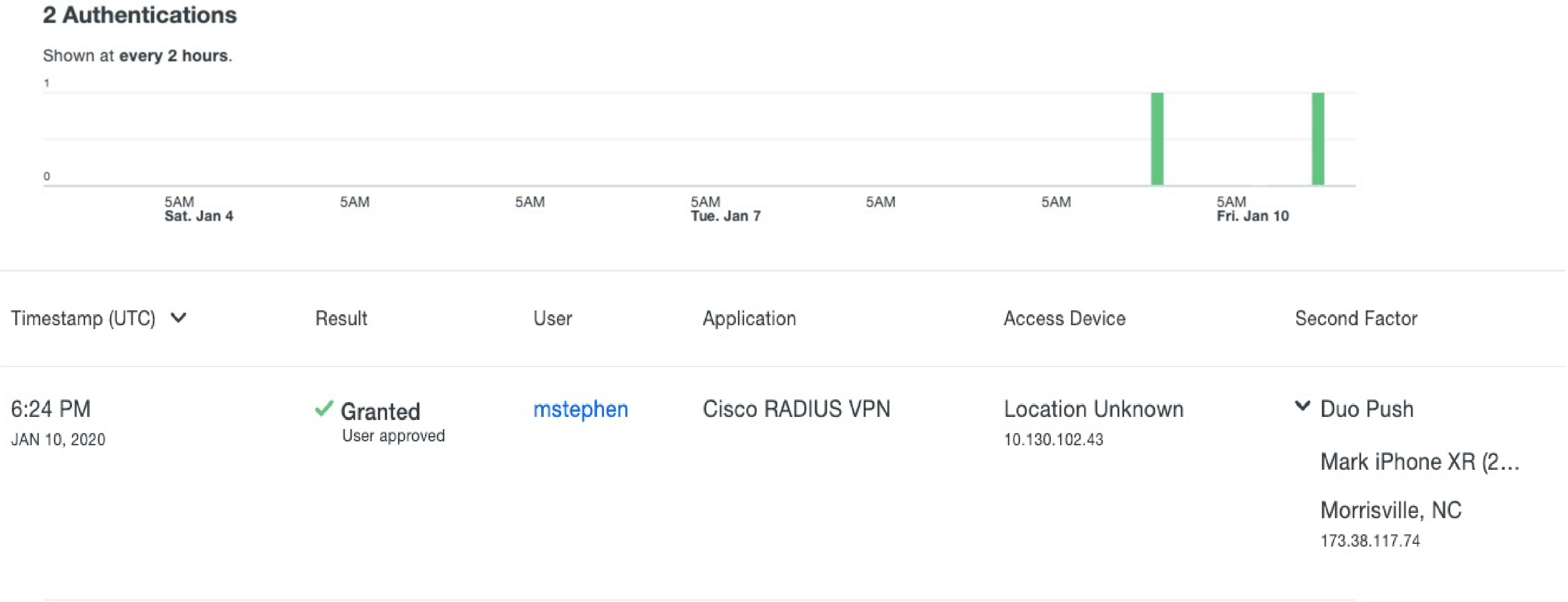
Users

You have users who have not activated Duo Mobile. Click here to send them activation links.

6	0	5	0	1	0
Total Users	Not Enrolled	Inactive Users	Trash	Bypass Users	Locked Out

□	Username	Name	Email	📱	▯	Status	Last Login (UTC)
□	bob	Bob Rogers	bob@example.com	2		Active	Never authenticated
□	jack	Jack Johnson	jack@example.com	1		Bypass	Never authenticated
□	jason	Jason Smith	jason@example.com	2		Active	Never authenticated
□	mstephen			1		Active	Dec 13, 2019 10:37 PM
□	sally	Sally Jones	sally@example.com	2		Disabled	Never authenticated

Duo Portal Authentication Log



2 Authentications

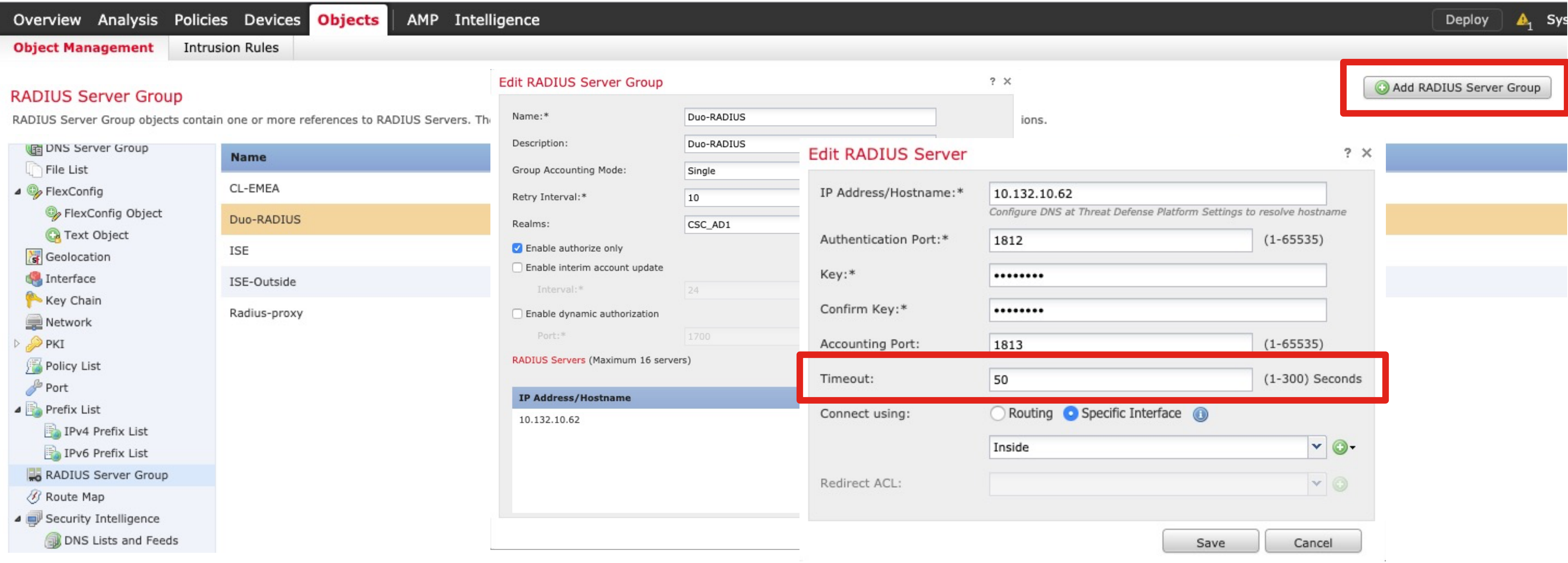
Shown at **every 2 hours**.

Timestamp (UTC) ⌄	Result	User	Application	Access Device	Second Factor
6:24 PM JAN 10, 2020	✓ Granted User approved	mstephen	Cisco RADIUS VPN	Location Unknown 10.130.102.43	⌄ Duo Push Mark iPhone XR (2... Morrisville, NC 173.38.117.74

FMC Configuration

Secondary Authentication

Objects>Object Management>RADIUS Server Group



RADIUS Server Group

RADIUS Server Group objects contain one or more references to RADIUS Servers. Th… ions.

Name
CL-EMEA
Duo-RADIUS
ISE
ISE-Outside
Radius-proxy

Edit RADIUS Server Group

Name:* Duo-RADIUS

Description: Duo-RADIUS

Group Accounting Mode: Single

Retry Interval:* 10

Realms: CSC_AD1

☑ Enable authorize only

□ Enable interim account update

Interval:* 24

□ Enable dynamic authorization

Port:* 1700

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
10.132.10.62

Edit RADIUS Server

IP Address/Hostname:* 10.132.10.62

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* 1812 (1-65535)

Key:* •••••••••

Confirm Key:* •••••••••

Accounting Port: 1813 (1-65535)

Timeout: 50 (1-300) Seconds

Connect using: ○ Routing ● Specific Interface

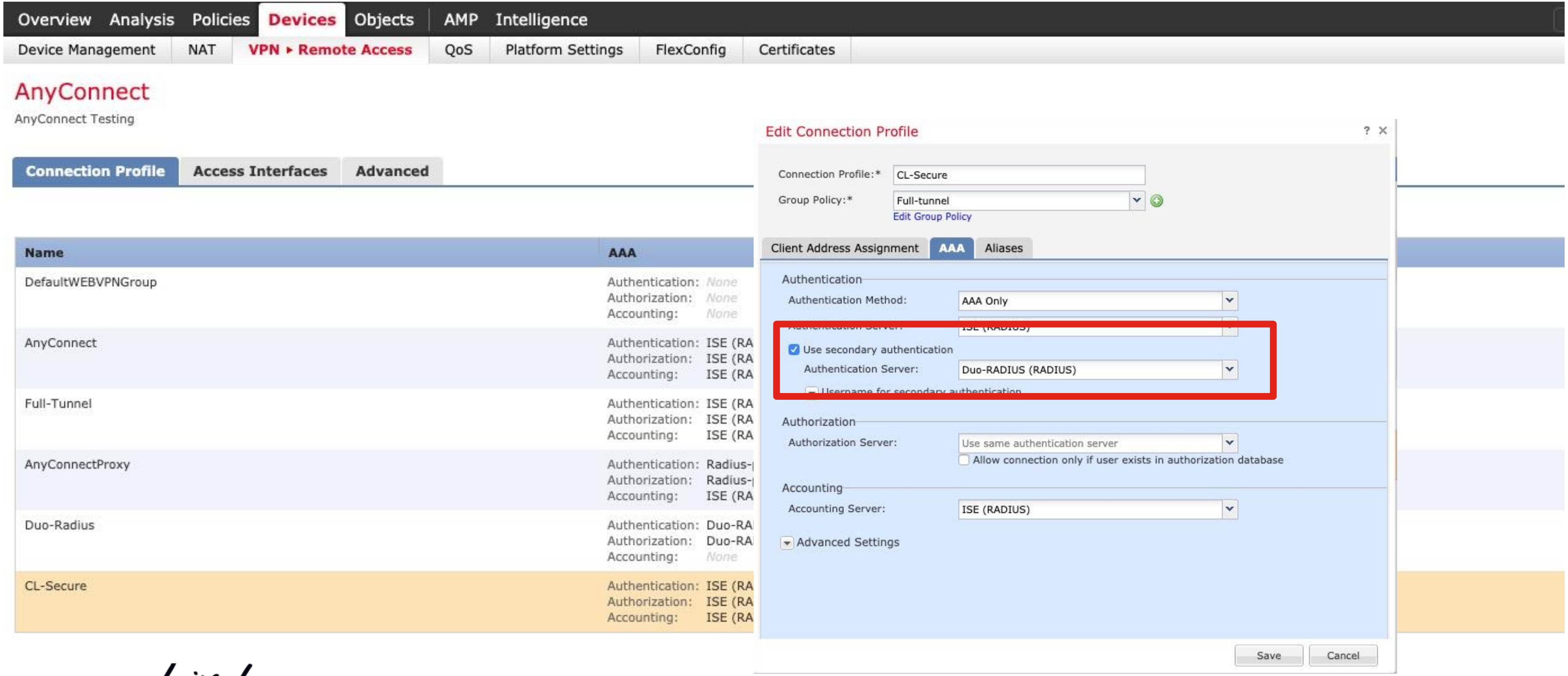
Inside

Redirect ACL:

FMC Configuration

Secondary Authentication

Devices>VPN>Remote Access



AnyConnect

AnyConnect Testing

Name	AAA
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None
AnyConnect	Authentication: ISE (RA Authorization: ISE (RA Accounting: ISE (RA
Full-Tunnel	Authentication: ISE (RA Authorization: ISE (RA Accounting: ISE (RA
AnyConnectProxy	Authentication: Radius- Authorization: Radius- Accounting: ISE (RA
Duo-Radius	Authentication: Duo-RA Authorization: Duo-RA Accounting: None
CL-Secure	Authentication: ISE (RA Authorization: ISE (RA Accounting: ISE (RA

Edit Connection Profile

Connection Profile:* CL-Secure

Group Policy:* Full-tunnel

Authentication

Authentication Method: AAA Only

Authentication Server: ISE (RADIUS)

☑ Use secondary authentication

Authentication Server: Duo-RADIUS (RADIUS)

□ Username for secondary authentication

Authorization

Authorization Server: Use same authentication server

□ Allow connection only if user exists in authorization database

Accounting

Accounting Server: ISE (RADIUS)

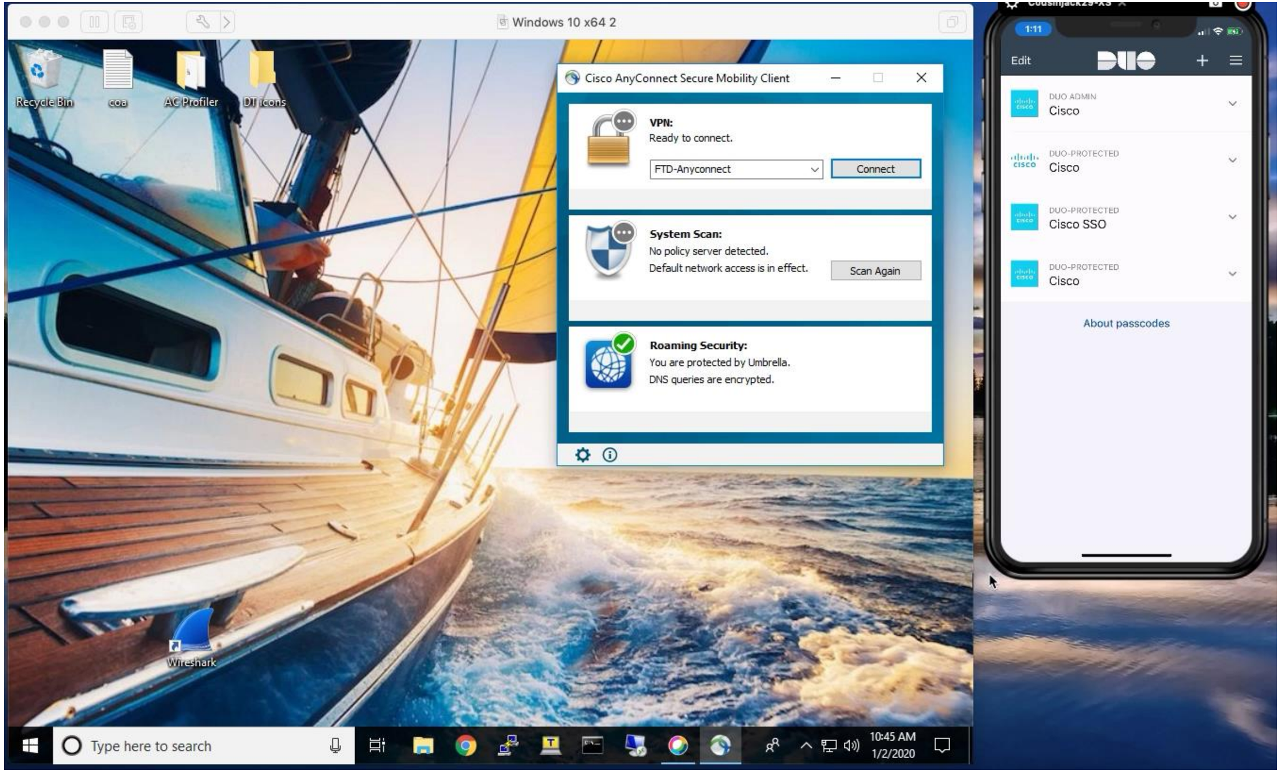
A smooth sea never made a skilled sailor

Franklin D. Roosevelt

The end user's view

The End User’s view

Remote Access VPN with posture and MFA



VPN:
Ready to connect.

FTD-Anyconnect | Connect

System Scan:
No policy server detected.
Default network access is in effect.

Scan Again

Roaming Security:
You are protected by Umbrella.
DNS queries are encrypted.

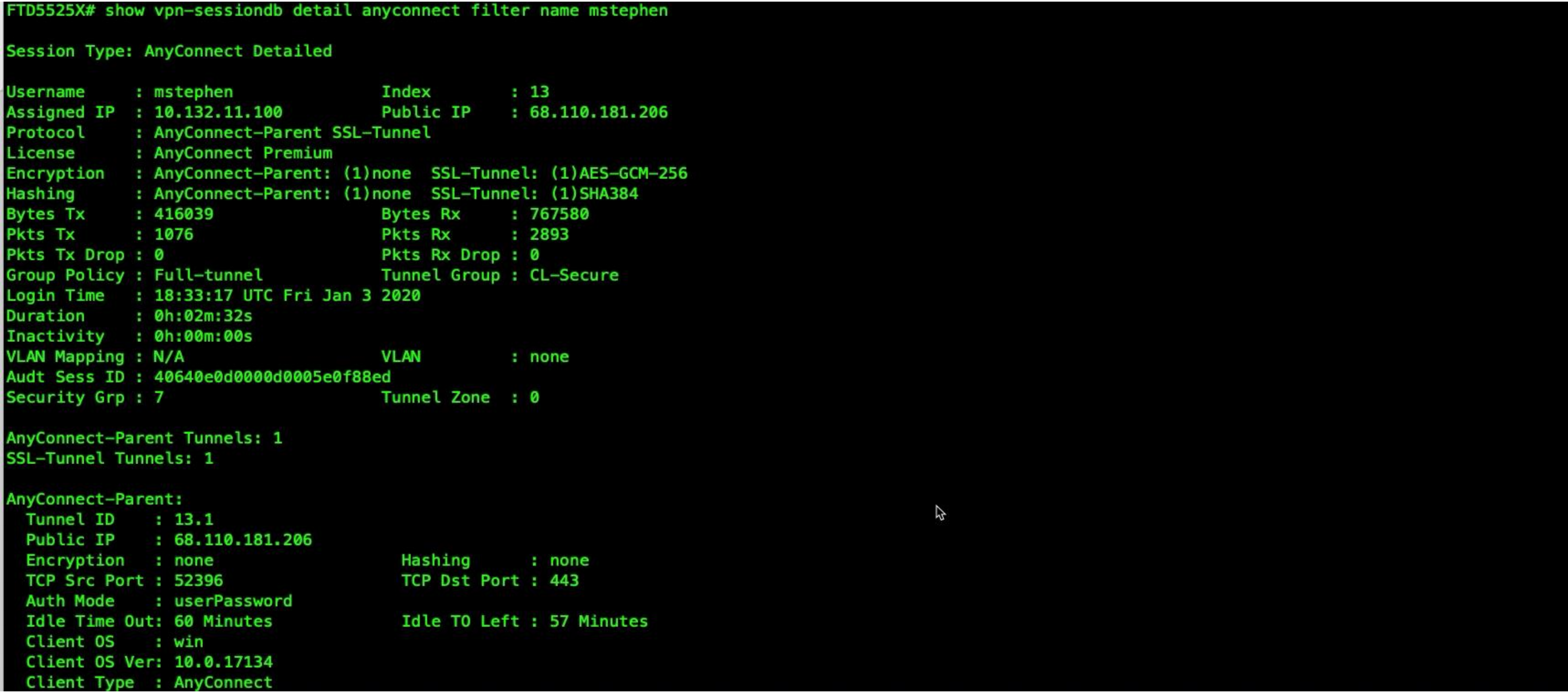
DUO ADMIN
Cisco

DUO-PROTECTED
Cisco

DUO-PROTECTED
Cisco SSO

DUO-PROTECTED
Cisco

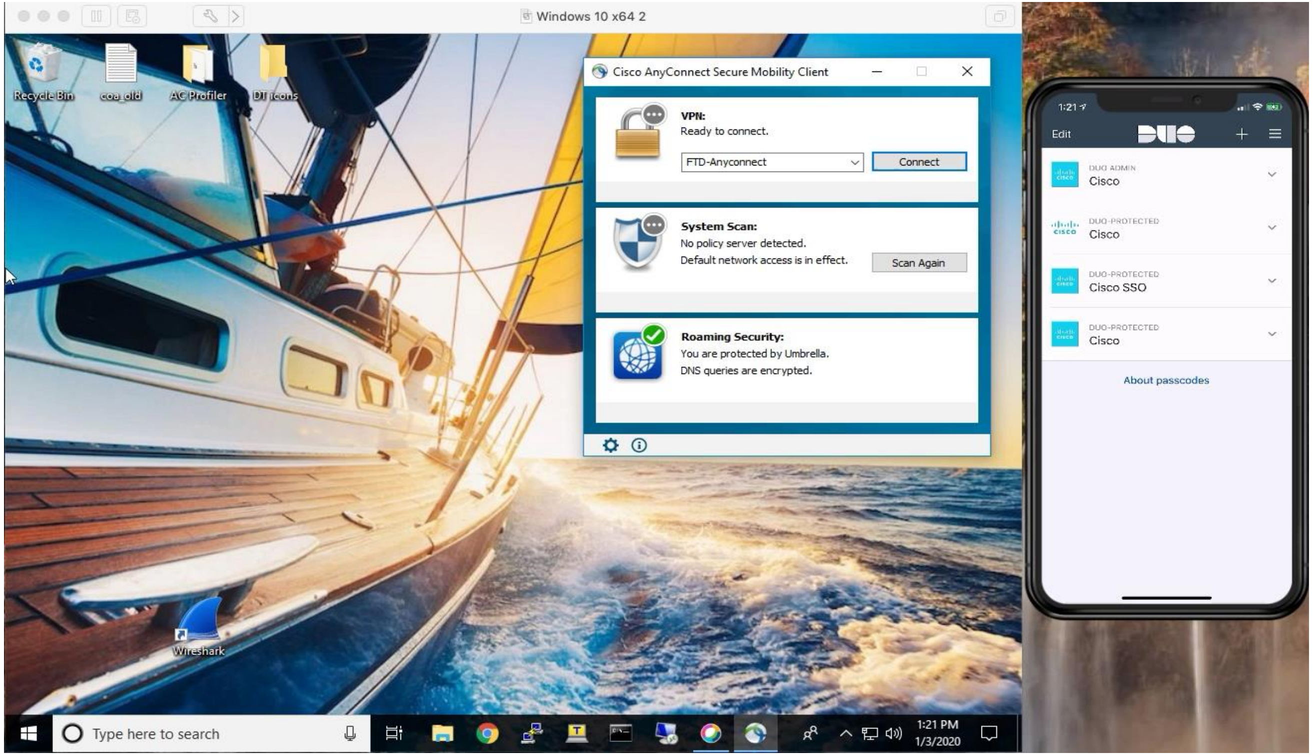
A Compliant Endpoint



```
FTD5525X# show vpn-sessiondb detail anyconnect filter name mstephen

Session Type: AnyConnect Detailed

Username     : mstephen               Index        : 13
Assigned IP  : 10.132.11.100          Public IP    : 68.110.181.206
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 416039                 Bytes Rx     : 767580
Pkts Tx      : 1076                   Pkts Rx      : 2893
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : Full-tunnel            Tunnel Group : CL-Secure
Login Time   : 18:33:17 UTC Fri Jan 3 2020
Duration     : 0h:02m:32s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 40640e0d0000d0005e0f88ed
Security Grp : 7                      Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 13.1
  Public IP    : 68.110.181.206
  Encryption   : none                   Hashing      : none
  TCP Src Port : 52396                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 60 Minutes             Idle TO Left : 57 Minutes
  Client OS    : win
  Client OS Ver: 10.0.17134
  Client Type  : AnyConnect
```

The End User’s view

Remote Access VPN with failed posture and MFA



Windows 10 x64 2

Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

FTD-Anyconnect

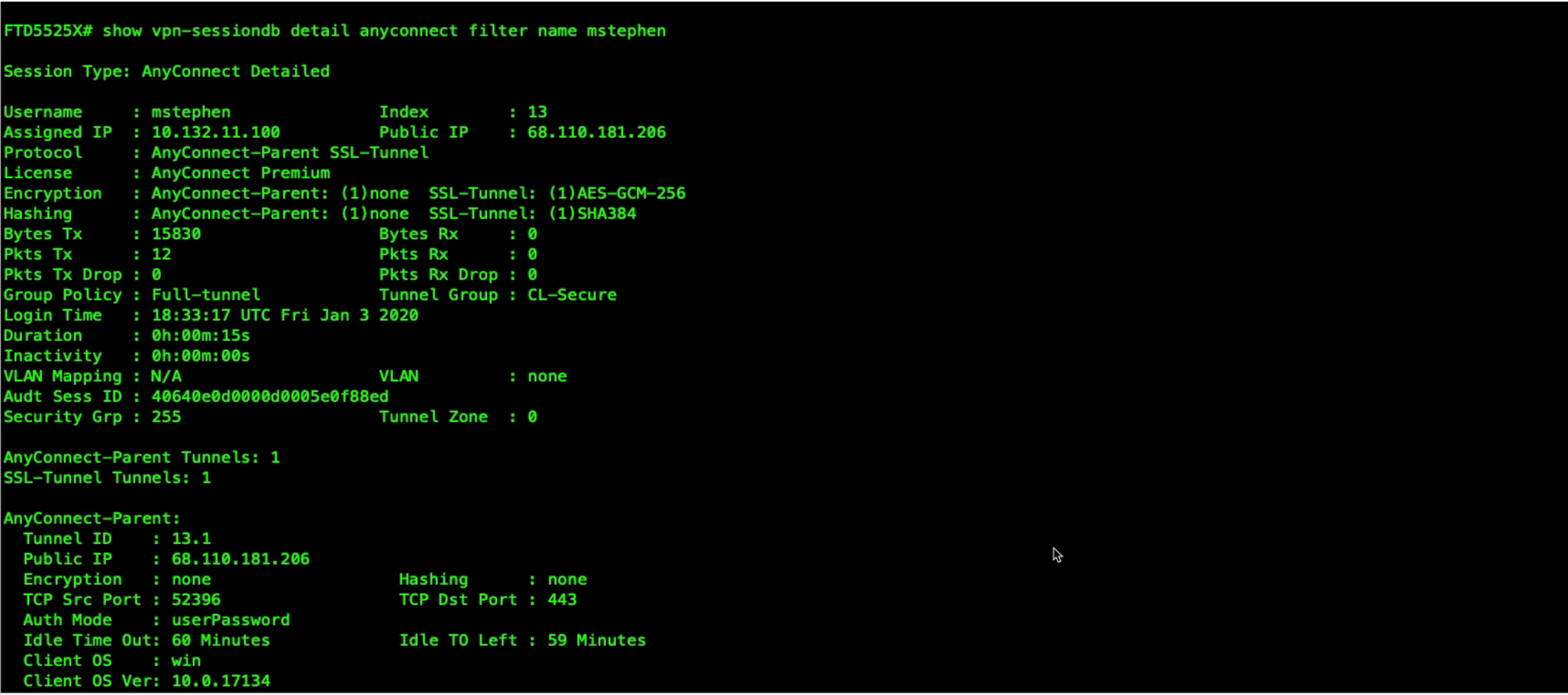
Connect

System Scan:
No policy server detected.
Default network access is in effect.

Scan Again

Roaming Security:
You are protected by Umbrella.
DNS queries are encrypted.

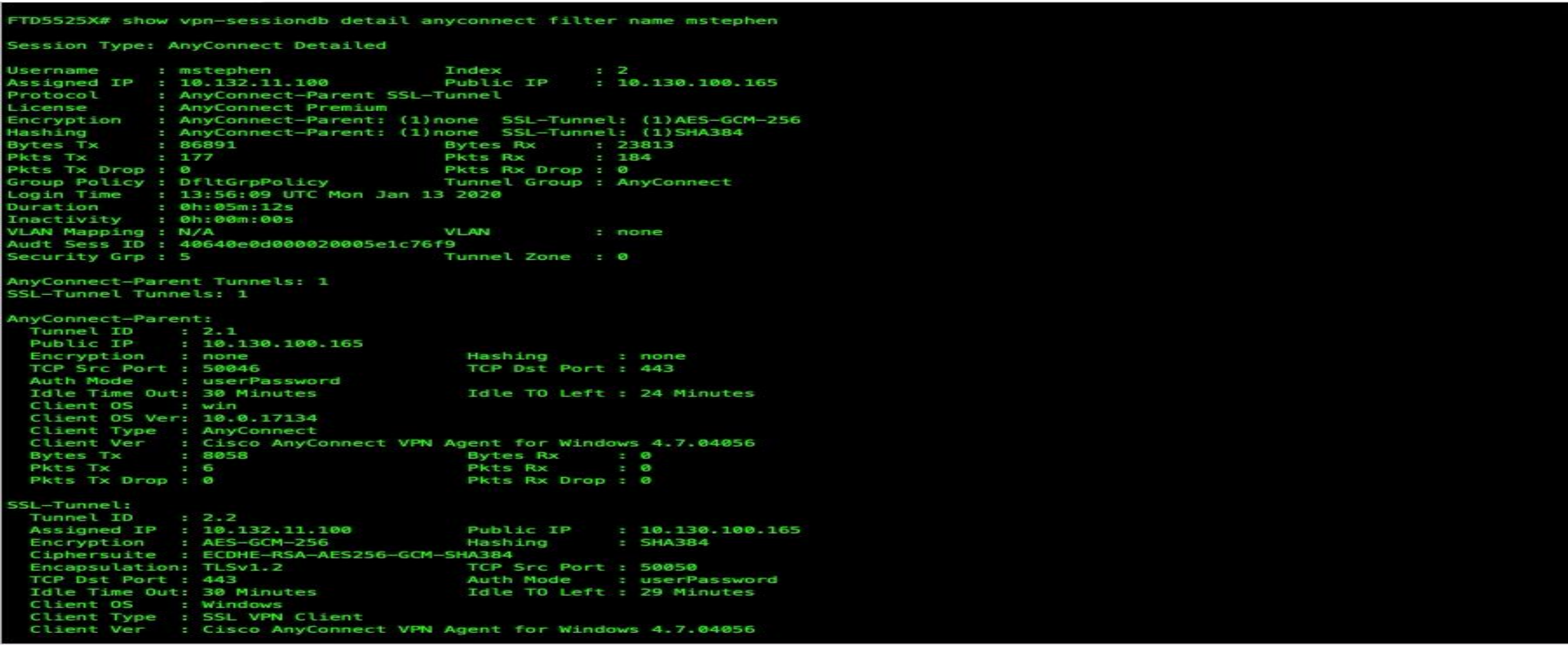
A Non-compliant Endpoint – “preposture”



```
FTD5525X# show vpn-sessiondb detail anyconnect filter name mstephen

Session Type: AnyConnect Detailed

Username     : mstephen               Index        : 13
Assigned IP  : 10.132.11.100          Public IP    : 68.110.181.206
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 15830                  Bytes Rx     : 0
Pkts Tx      : 12                     Pkts Rx      : 0
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : Full-tunnel            Tunnel Group : CL-Secure
Login Time   : 18:33:17 UTC Fri Jan 3 2020
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 40640e0d0000d0005e0f88ed
Security Grp : 255                    Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 13.1
  Public IP    : 68.110.181.206
  Encryption   : none                   Hashing      : none
  TCP Src Port : 52396                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 60 Minutes             Idle TO Left : 59 Minutes
  Client OS    : win
  Client OS Ver: 10.0.17134
```

A Non-compliant Endpoint

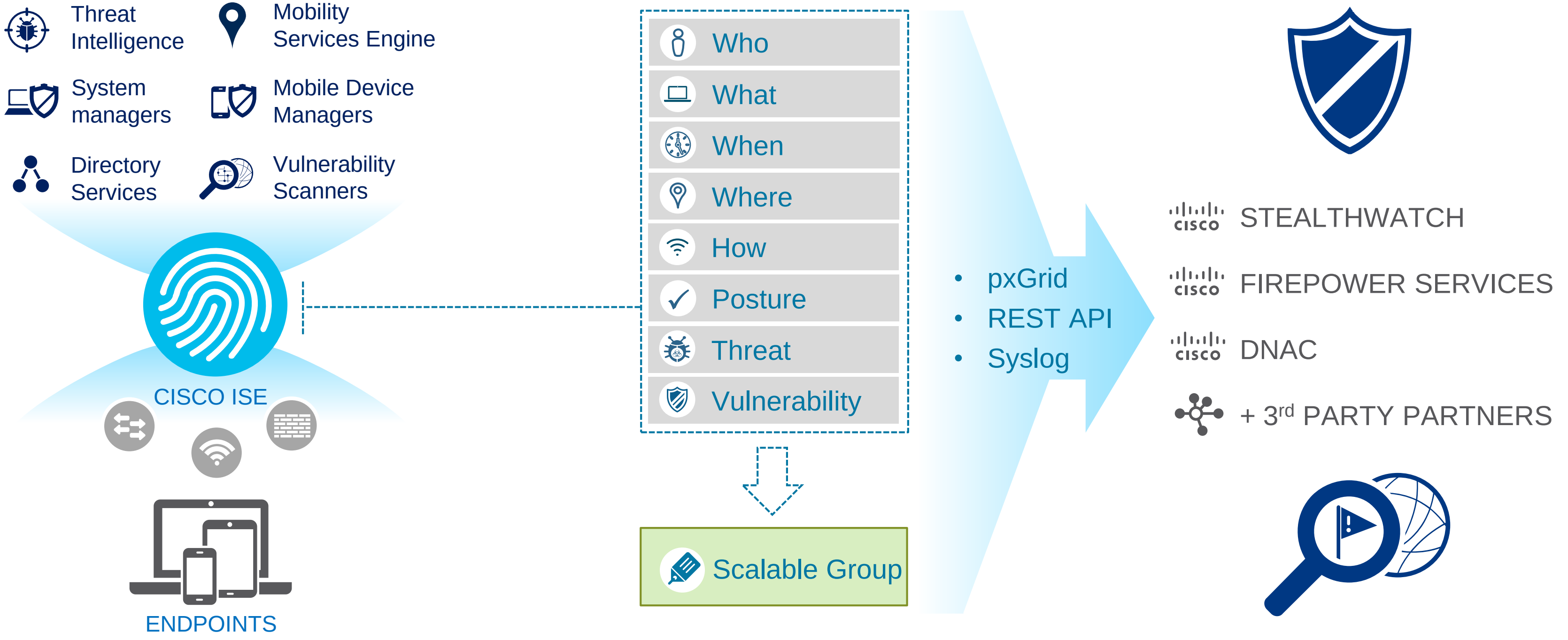
Remote Access VPN with failed posture and MFA



```
FTD5525X# show vpn-sessiondb detail anyconnect filter name mstephen

Session Type: AnyConnect Detailed

Username     : mstephen               Index        : 2
Assigned IP  : 10.132.11.100          Public IP    : 10.130.100.165
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 86891                  Bytes Rx     : 23813
Pkts Tx      : 177                    Pkts Rx      : 184
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : AnyConnect
Login Time   : 13:56:09 UTC Mon Jan 13 2020
Duration     : 0h:05m:12s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 40640e0d000020005e1c76f9
Security Grp : 5                      Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 10.130.100.165
  Encryption   : none                   Hashing      : none
  TCP Src Port : 50046                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 24 Minutes
  Client OS    : win
  Client OS Ver: 10.0.17134
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.04056
  Bytes Tx     : 8058                   Bytes Rx     : 0
  Pkts Tx      : 6                      Pkts Rx      : 0
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 2.2
  Assigned IP  : 10.132.11.100          Public IP    : 10.130.100.165
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-RSA-AES256-GCM-SHA384
  Encapsulation: TLSv1.2                TCP Src Port : 50050
  TCP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.7.04056
```

TrustSec Integration

ISE Group Based Policies (TrustSec)



Threat Intelligence

Mobility Services Engine

System managers

Mobile Device Managers

Directory Services

Vulnerability Scanners

CISCO ISE

ENDPOINTS

- Who
- What
- When
- Where
- How
- Posture
- Threat
- Vulnerability

Scalable Group

- pxGrid
- REST API
- Syslog

STEALTHWATCH

FIREPOWER SERVICES

DNAC

+ 3rd PARTY PARTNERS

Visibility and Access Control

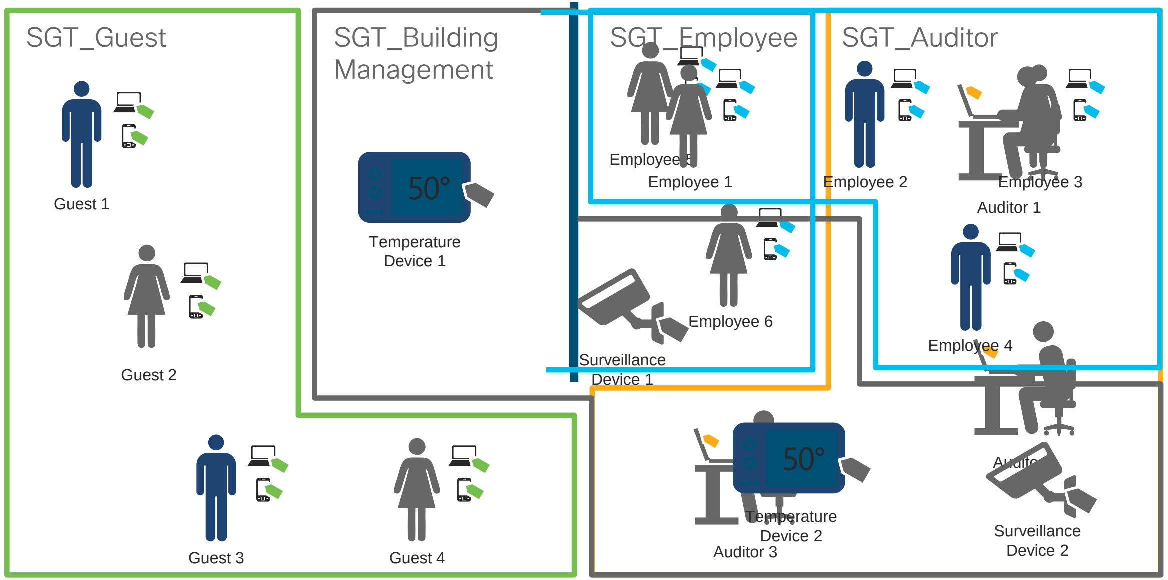
ISE builds context and applies access control restrictions to users and devices

Context Reuse

by eco-system partners for analysis & control

Dynamic Group Management

- Create new security groups and add new endpoints quickly and easily



Classify endpoints

Save time and resources with dynamic classification of endpoints as they come onto the network

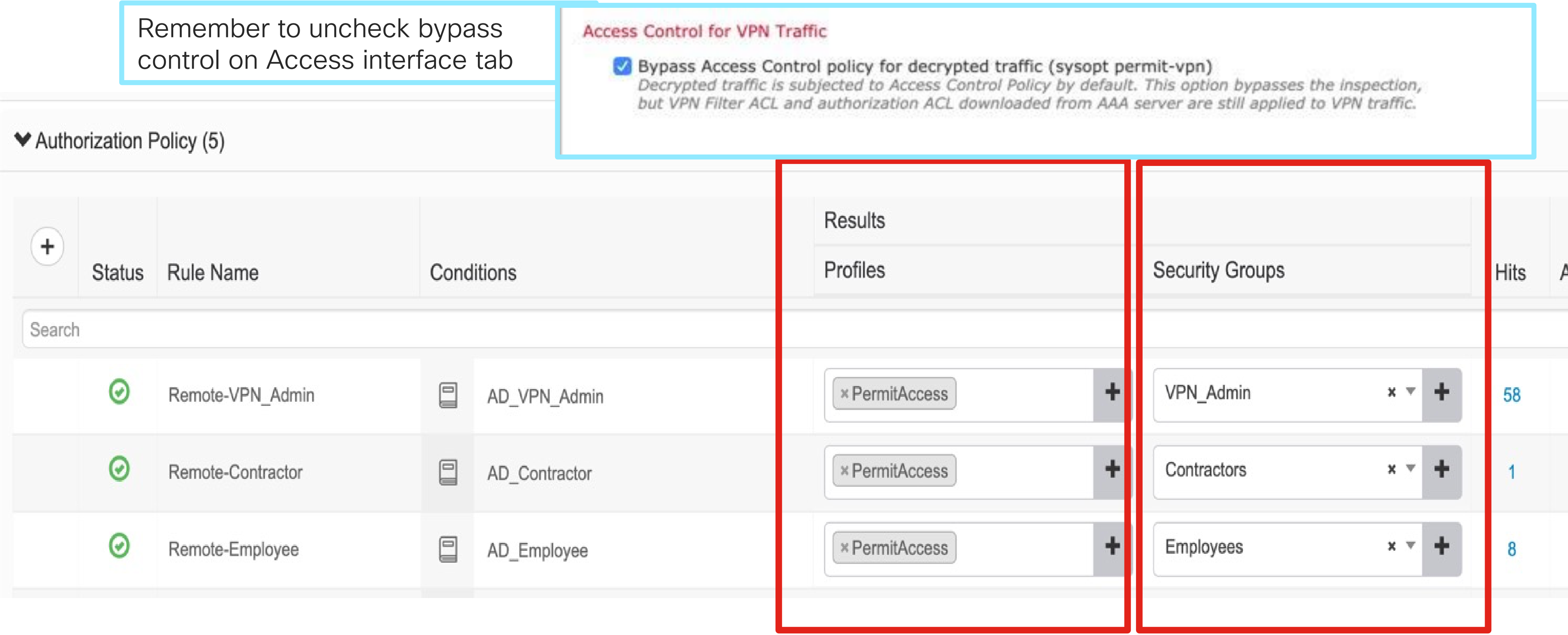
Maintain dynamically

Automatically apply consistent policies even as resources are moved or additional users/sites are added

ISE SGT Classification

Access Policy

Work Centers>Posture>Policy Sets



Remember to uncheck bypass control on Access interface tab

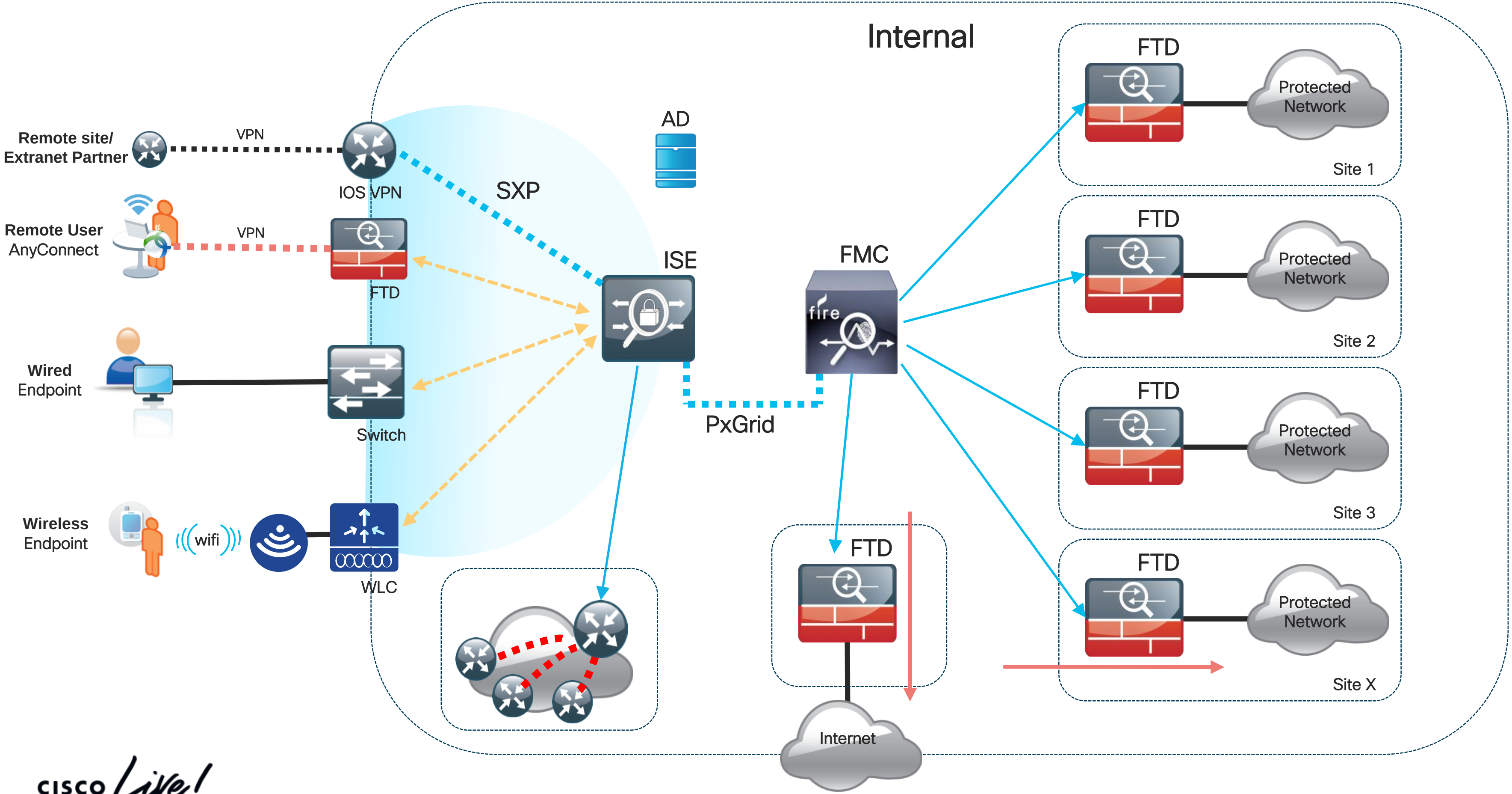
Access Control for VPN Traffic

☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

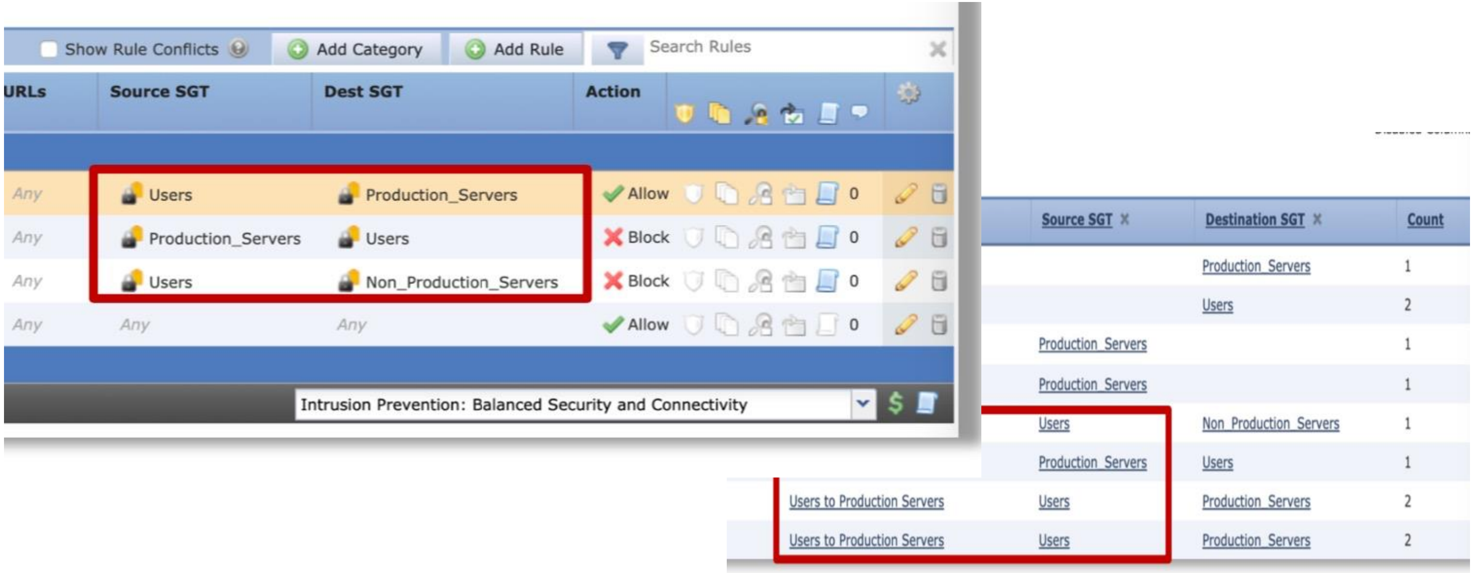
Authorization Policy (5)

+	Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits
	✓	Remote-VPN_Admin	AD_VPN_Admin	× PermitAccess	VPN_Admin	58
	✓	Remote-Contractor	AD_Contractor	× PermitAccess	Contractors	1
	✓	Remote-Employee	AD_Employee	× PermitAccess	Employees	8

TrustSec SGT Identity Controls



TrustSec SGT New features in Firepower 6.5



URLs	Source SGT	Dest SGT	Action	
Any	Users	Production_Servers	✓ Allow	0
Any	Production_Servers	Users	✗ Block	0
Any	Users	Non_Production_Servers	✗ Block	0
Any	Any	Any	✓ Allow	0

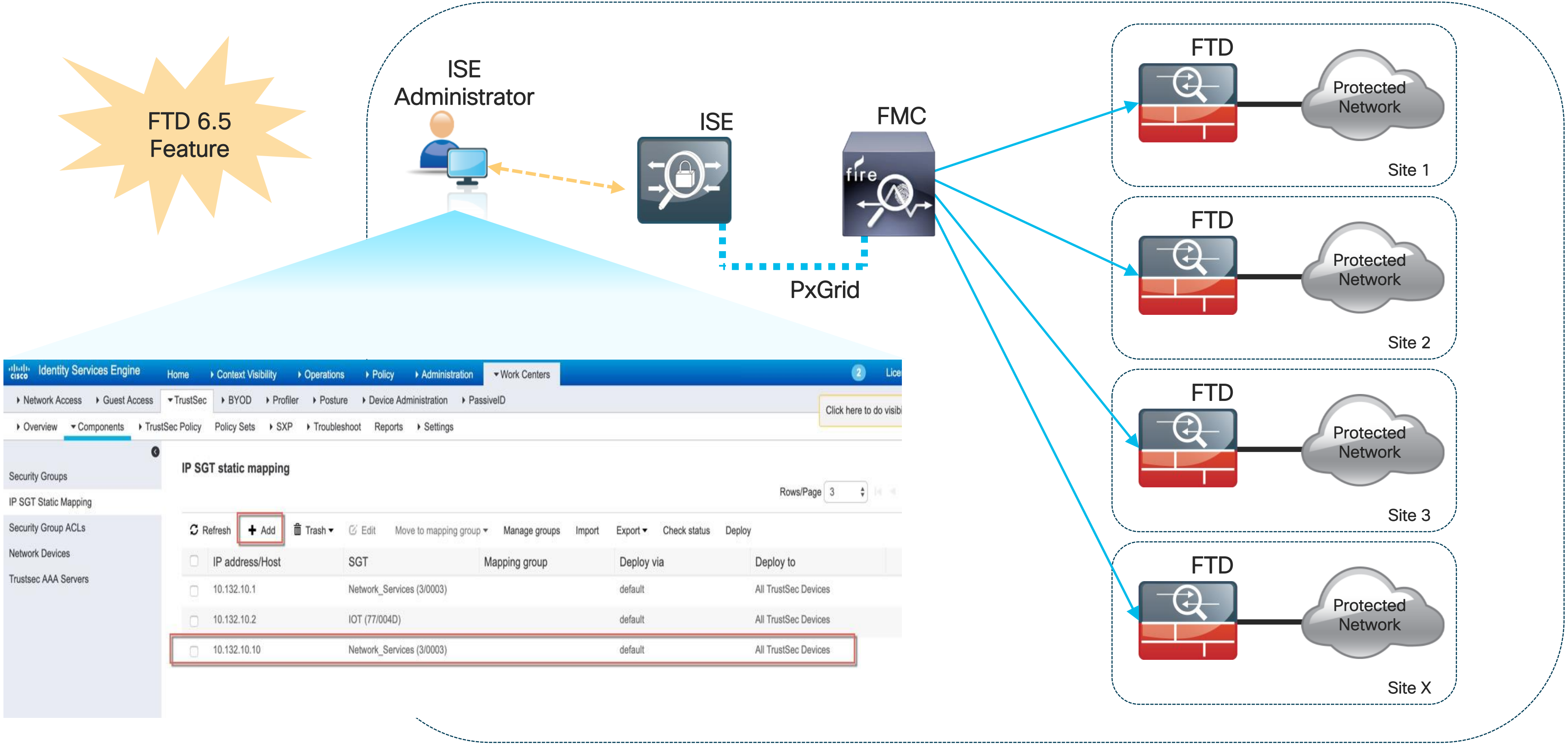
Intrusion Prevention: Balanced Security and Connectivity

	Source SGT	Destination SGT	Count
		Production_Servers	1
		Users	2
	Production_Servers		1
	Production_Servers		1
	Users	Non_Production_Servers	1
	Production_Servers	Users	1
Users to Production Servers	Users	Production_Servers	2
Users to Production Servers	Users	Production_Servers	2

- **Destination SGT Access Policy Control**
- **SXP Mapped clients – full support for all learned IP:SGT Mappings**

Static IP:SGT Binding Controls

FTD 6.5 Feature

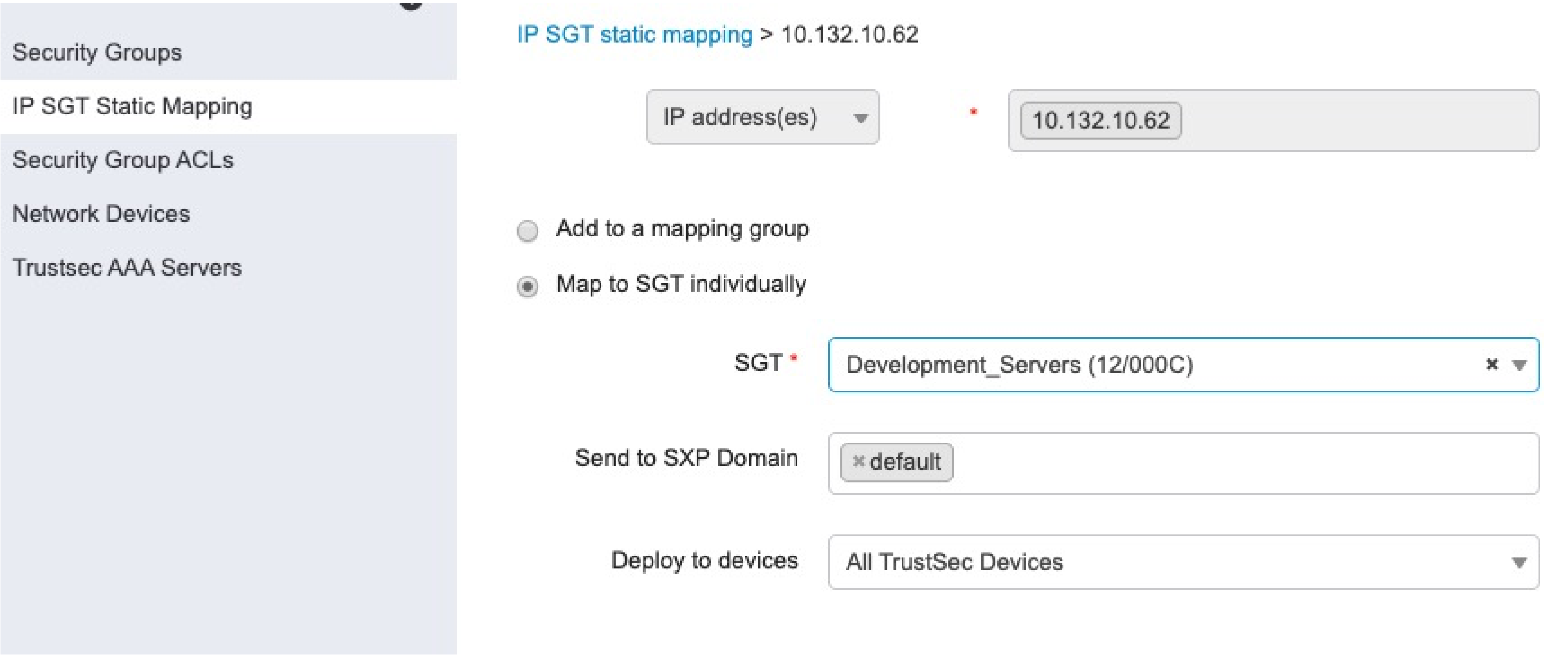


IP SGT static mapping

IP address/Host	SGT	Mapping group	Deploy via	Deploy to
10.132.10.1	Network_Services (3/0003)		default	All TrustSec Devices
10.132.10.2	IOT (77/004D)		default	All TrustSec Devices
10.132.10.10	Network_Services (3/0003)		default	All TrustSec Devices

ISE - TrustSec Rules Creation

Work Centers>Trustsec>Components>IP SGT Static Mapping



IP SGT static mapping > 10.132.10.62

IP address(es) * 10.132.10.62

○ Add to a mapping group

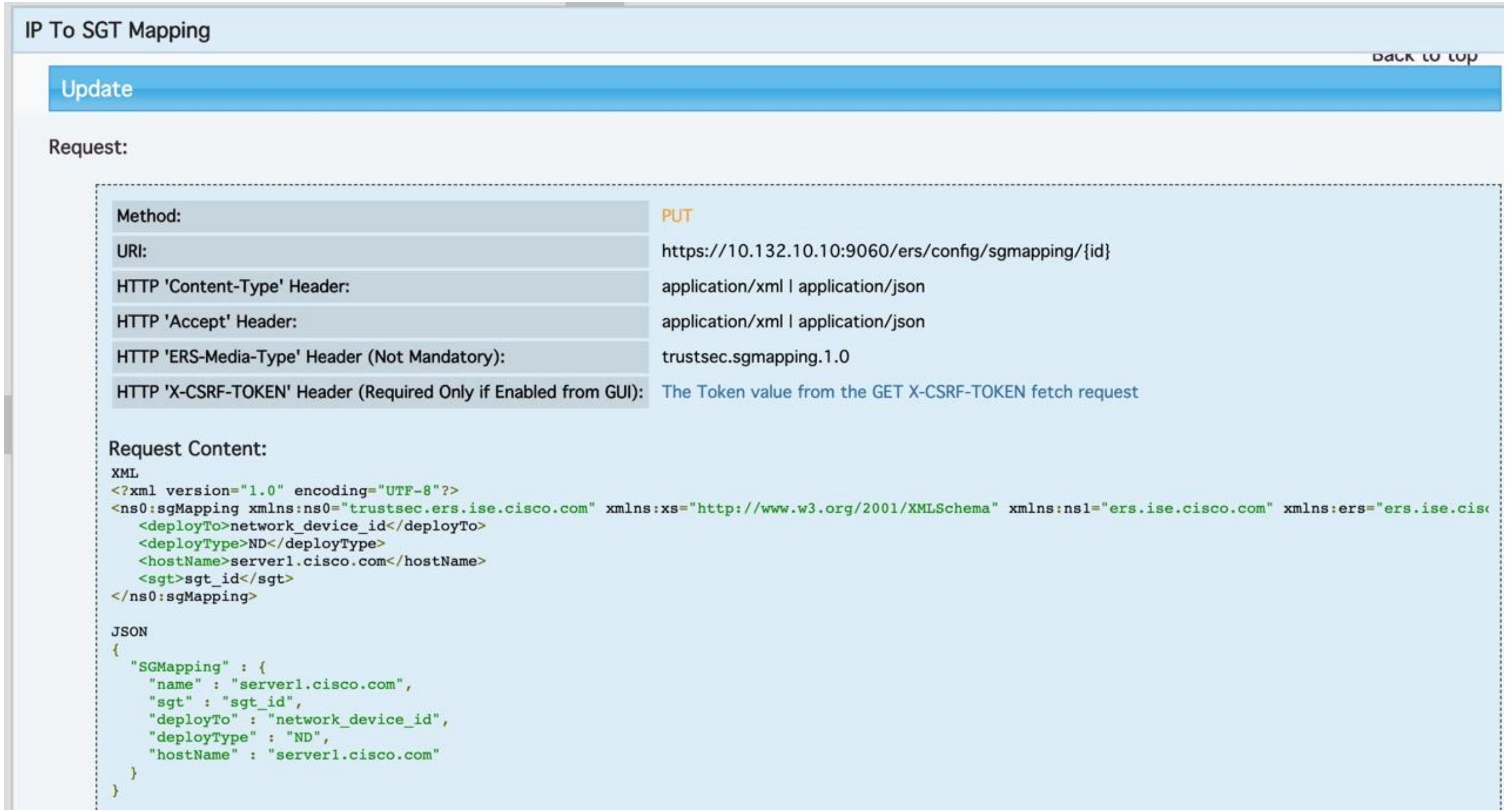
● Map to SGT individually

SGT * Development_Servers (12/000C)

Send to SXP Domain: default

Deploy to devices: All TrustSec Devices

Static IP:SGT Binding Controls via API



IP To SGT Mapping

Back to top

Update

Request:

Method:	PUT
URI:	https://10.132.10.10:9060/ers/config/sgmapping/{id}
HTTP 'Content-Type' Header:	application/xml | application/json
HTTP 'Accept' Header:	application/xml | application/json
HTTP 'ERS-Media-Type' Header (Not Mandatory):	trustsec.sgmapping.1.0
HTTP 'X-CSRF-TOKEN' Header (Required Only if Enabled from GUI):	The Token value from the GET X-CSRF-TOKEN fetch request

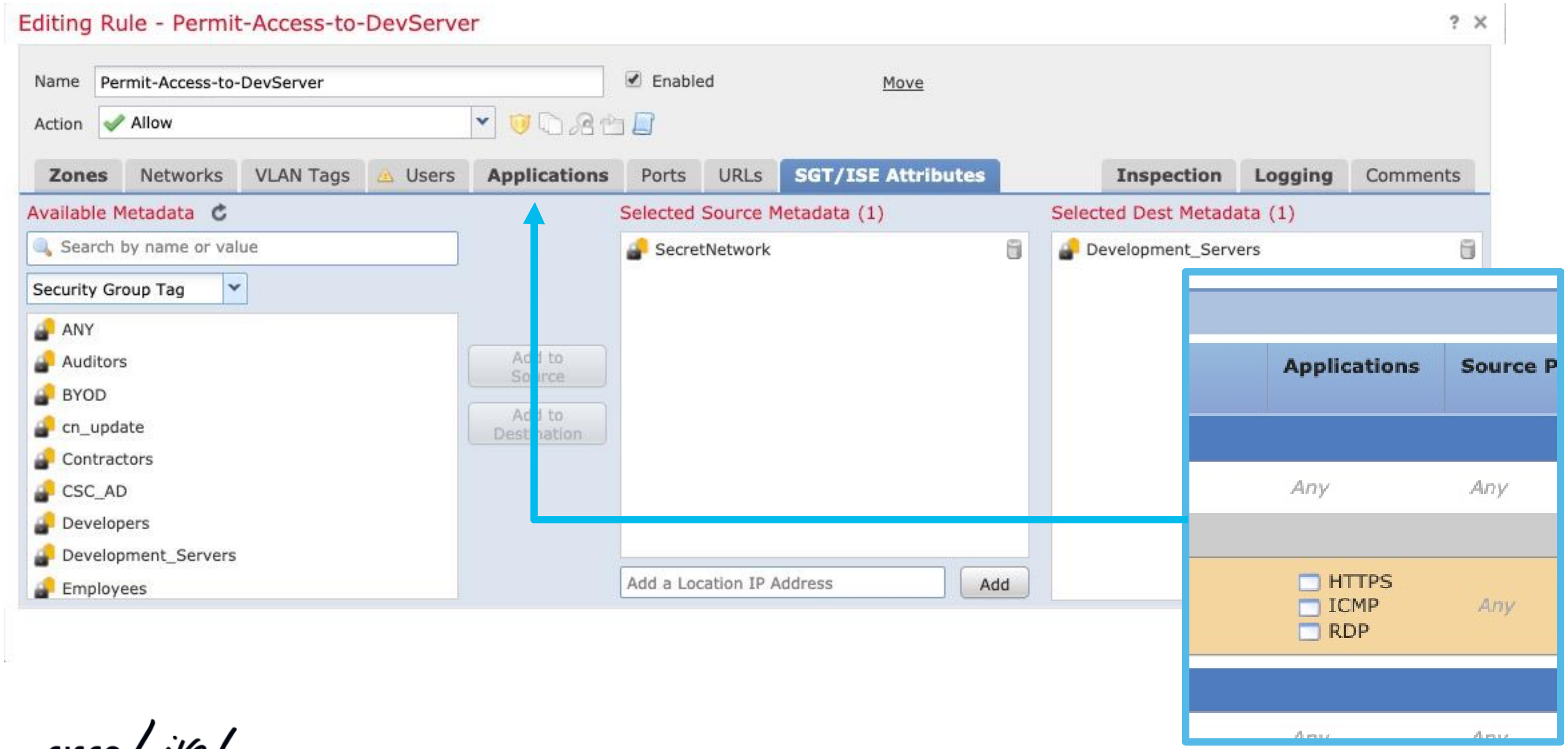
Request Content:

```
XML
<?xml version="1.0" encoding="UTF-8"?>
<ns0:sgMapping xmlns:ns0="trustsec.ers.ise.cisco.com" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisc
   <deployTo>network_device_id</deployTo>
   <deployType>ND</deployType>
   <hostName>server1.cisco.com</hostName>
   <sgt>sgt_id</sgt>
</ns0:sgMapping>

JSON
{
  "SGMapping" : {
    "name" : "server1.cisco.com",
    "sgt" : "sgt_id",
    "deployTo" : "network_device_id",
    "deployType" : "ND",
    "hostName" : "server1.cisco.com"
  }
}
```

https://<PAN>:9060/ers/sdk#Update

FMC - TrustSec Rules Creation

Policies>Access Control> Access Control >[policy]



Editing Rule - Permit-Access-to-DevServer

Name: Permit-Access-to-DevServer

☑ Enabled

Move

Action: ✓ Allow

Available Metadata

Search by name or value

Security Group Tag

- ANY
- Auditors
- BYOD
- cn_update
- Contractors
- CSC_AD
- Developers
- Development_Servers
- Employees

Selected Source Metadata (1)

- SecretNetwork

Add a Location IP Address

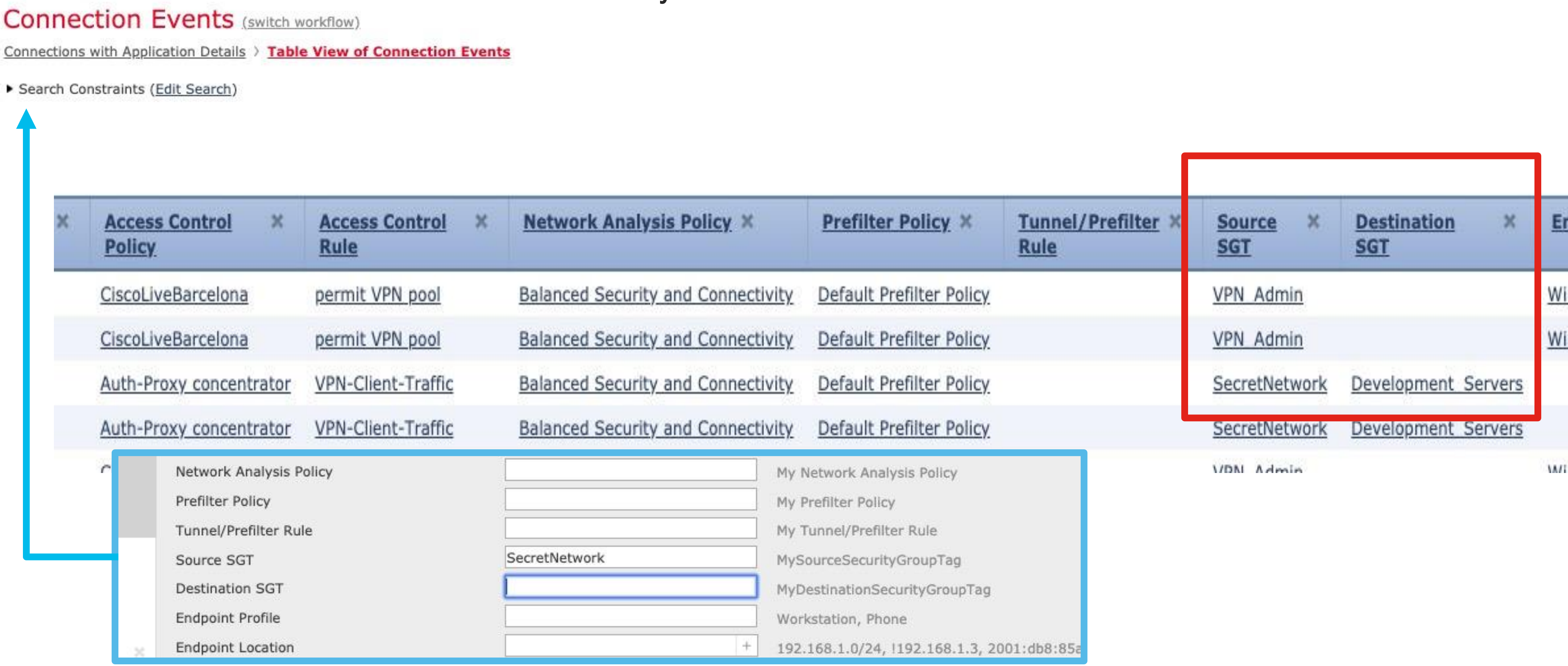
Selected Dest Metadata (1)

- Development_Servers

Applications	Source P
Any	*Any*
□ HTTPS □ ICMP □ RDP	*Any*
Any	*Any*

ISE and FMC - TrustSec Rules Creation

Analysis>Connections>Events>Table view for connection events



Connection Events (switch workflow)

Connections with Application Details › **Table View of Connection Events**

▸ Search Constraints (Edit Search)

Access Control Policy	Access Control Rule	Network Analysis Policy	Prefilter Policy	Tunnel/Prefilter Rule	Source SGT	Destination SGT	En
CiscoLiveBarcelona	permit VPN pool	Balanced Security and Connectivity	Default Prefilter Policy		VPN_Admin		Wi
CiscoLiveBarcelona	permit VPN pool	Balanced Security and Connectivity	Default Prefilter Policy		VPN_Admin		Wi
Auth-Proxy concentrator	VPN-Client-Traffic	Balanced Security and Connectivity	Default Prefilter Policy		SecretNetwork	Development_Servers	
Auth-Proxy concentrator	VPN-Client-Traffic	Balanced Security and Connectivity	Default Prefilter Policy		SecretNetwork	Development_Servers	
					VPN_Admin		Wi

Network Analysis Policy		My Network Analysis Policy
Prefilter Policy		My Prefilter Policy
Tunnel/Prefilter Rule		My Tunnel/Prefilter Rule
Source SGT	SecretNetwork	MySourceSecurityGroupTag
Destination SGT		MyDestinationSecurityGroupTag
Endpoint Profile		Workstation, Phone
Endpoint Location		192.168.1.0/24, !192.168.1.3, 2001:db8:85a

TrustSec Trouble Shooting

FMC SXP SGT:IP Binding table

```
admin@FMC:~$ sudo -i
Password: <enter_password>
root@FMC:~# cd /var/sf/user_enforcement/
root@FMC:/var/sf/user_enforcement# uip_reader -f sxp_log_entries.0 -l -p -t
```

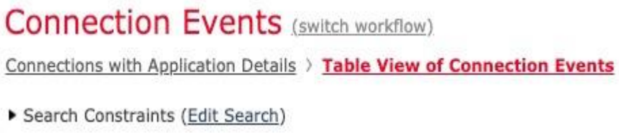
```
------------------------------------
 Entry no: 1
operation_type: SXP_BINDING_ADD
sxp_binding {
 ipPrefix: "10.10.55.1/32"
 tag: "2050"
 source: "10.132.10.10"
 peerSeq: "10.132.10.10"
 hop_timestamp: 1573153009
}
```

```
------------------------------------
 Entry no: 2
operation_type: SXP_BINDING_ADD
sxp_binding {
 ipPrefix: "10.101.128.101/32"
 tag: "1066"
 source: "10.132.10.10"
 peerSeq: "10.132.10.10"
 hop_timestamp: 1573153009
}
```

Report Creation

FMC and TrustSec SGTs

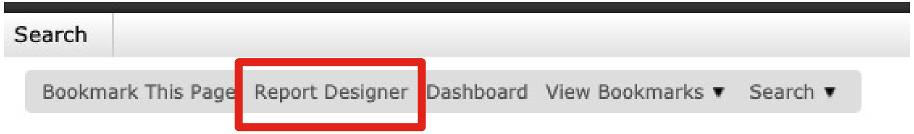
Analysis>Connections>Events>Table view for connection events



Connection Events (switch workflow)

Connections with Application Details › **Table View of Connection Events**

▸ Search Constraints (Edit Search)



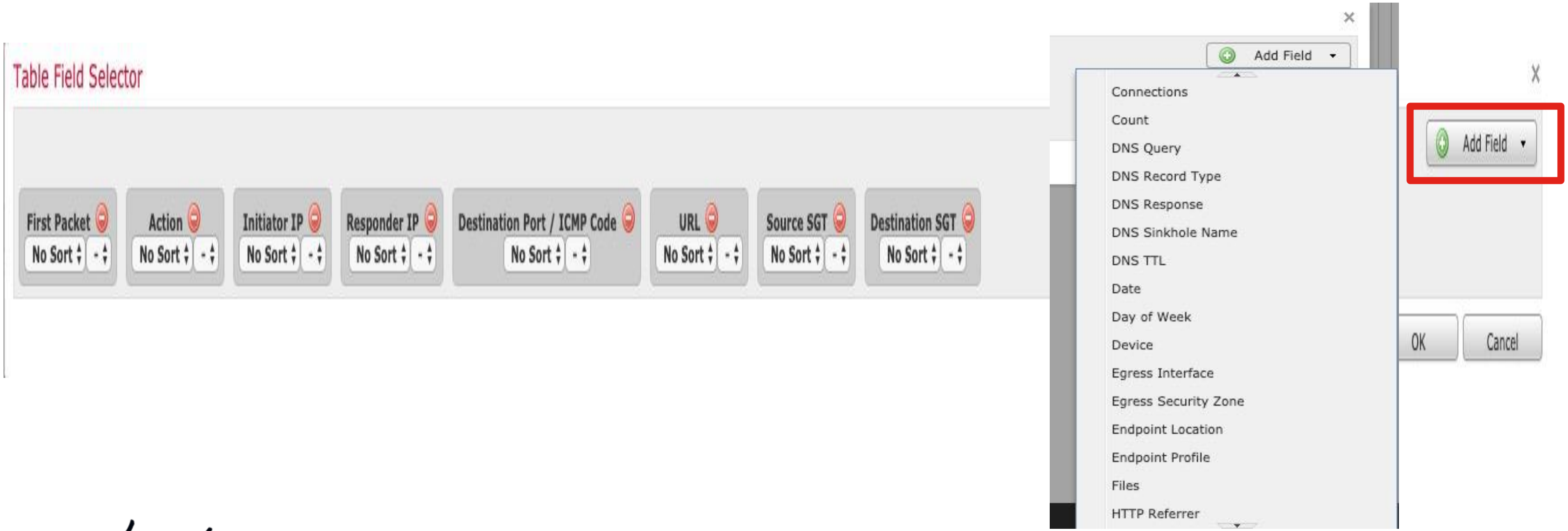
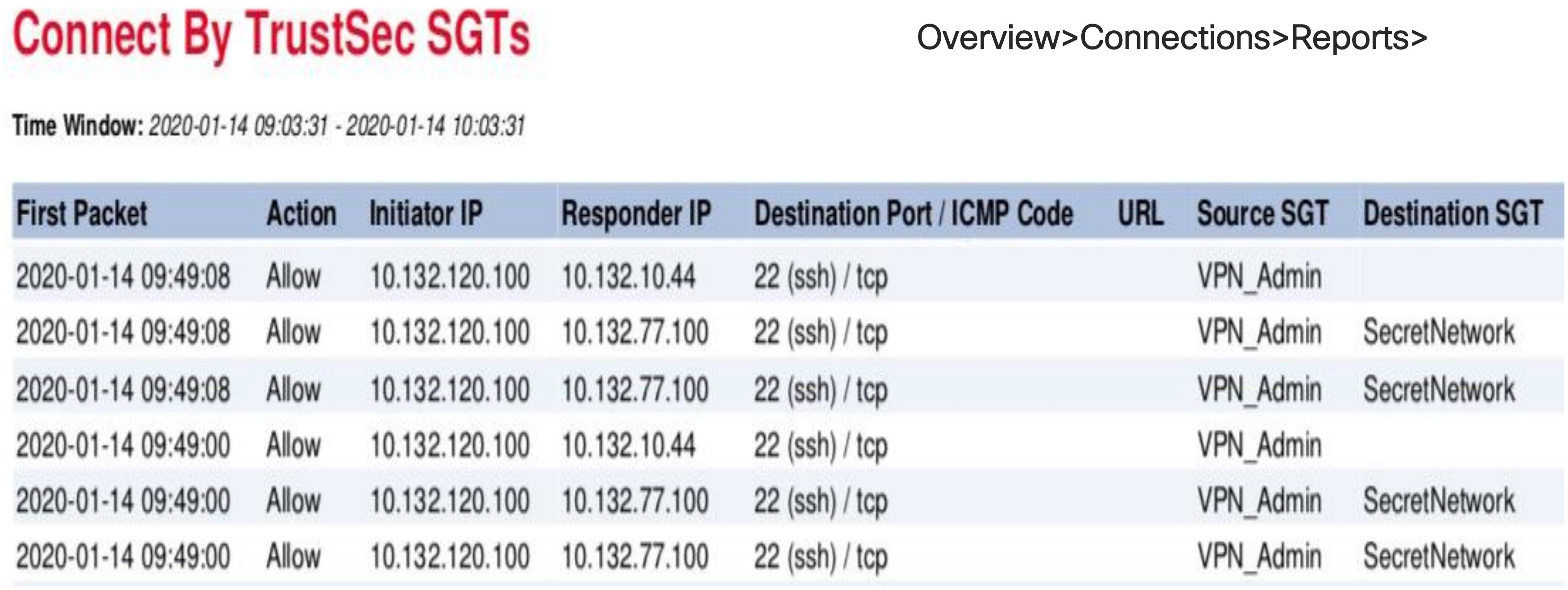


Table Field Selector

First Packet	Action	Initiator IP	Responder IP	Destination Port / ICMP Code	URL	Source SGT	Destination SGT
No Sort	No Sort	No Sort	No Sort	No Sort	No Sort	No Sort	No Sort

Reports on FMC

Overview>Connections>Reports>



Connect By TrustSec SGTs

Time Window: *2020-01-14 09:03:31 - 2020-01-14 10:03:31*

First Packet	Action	Initiator IP	Responder IP	Destination Port / ICMP Code	URL	Source SGT	Destination SGT
2020-01-14 09:49:08	Allow	10.132.120.100	10.132.10.44	22 (ssh) / tcp		VPN_Admin	
2020-01-14 09:49:08	Allow	10.132.120.100	10.132.77.100	22 (ssh) / tcp		VPN_Admin	SecretNetwork
2020-01-14 09:49:08	Allow	10.132.120.100	10.132.77.100	22 (ssh) / tcp		VPN_Admin	SecretNetwork
2020-01-14 09:49:00	Allow	10.132.120.100	10.132.10.44	22 (ssh) / tcp		VPN_Admin	
2020-01-14 09:49:00	Allow	10.132.120.100	10.132.77.100	22 (ssh) / tcp		VPN_Admin	SecretNetwork
2020-01-14 09:49:00	Allow	10.132.120.100	10.132.77.100	22 (ssh) / tcp		VPN_Admin	SecretNetwork

Conclusion

Wrap up

FTD/AnyConnect deployment is production ready, but…

- Not feature parity with ASA AnyConnect support, validate features used in production if migrating.
- Decide on management platform FMC verses FDM/CDO.
- DTLS 1.2 is an upcoming feature.
- Dynamic Access Policy or Posture control must be via ISE integration.
- No clientless SSL VPN so consider Duo Network Gateway
- MFA and SGT supported.

Almost everything will work again if you unplug it for a few minutes...including you

Work life balance, Anonymous.

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

cisco

You make **possible**