# **Implement Hardening Measures for Secure Client AnyConnect VPN**

## **Contents**

Introduction
Prerequisites
Requirements
Components Used
Background Information
Concepts
Secure Client Hardening Practices on Cisco Secure Firewall:
Identify Attacks using Logging and Syslog IDs
Attack Verification
FMC Configuration Examples
Disable AAA Authentication in the DefaultWEBVPNGroup and DefaultRAGroup Connection Profiles
Disable Hostscan / Secure Firewall Posture on the DefaultWEBVPNGroup and DefaultRAGroup (optional)
Remove Group-aliases and Enable Group-URLs
Certificate Mapping
IPsec-IKEv2
ASA Configuration Examples
Disable AAA Authentication in the DefaultWEBVPNGroup and DefaultRAGroup Connection Profiles
Disable Hostscan / Secure Firewall Posture on the DefaultWEBVPNGroup and DefaultRAGroup (optional)
Remove Group-aliases and Enable Group-URLs
Certificate Mapping
IPsec-IKEv2
Conclusion
Related Information

## Introduction

This document describes how to improve the security of your Remote Access VPN implementation.

## Prerequisites

### **Requirements**

Cisco recommends you to have knowledge of these topics:

- Cisco Secure Client AnyConnect VPN.
- ASA/FTD remote access configuration.

### **Components Used**

The best practices guide is based on these hardware and software versions:

- Cisco ASA 9.x
- Firepower Threat Defense 7.x / FMC 7.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



**Caution**: This document does not contain steps for Firepower Device Manager (FDM). The FDM only supports changing the authentication method on the DefaultWEBVPNGroup. Please use control-plane ACLs, or a custom port in the Remote Access VPN 'Global Settings' section within the FDM UI. Please reach out to Cisco Technical Assistance Center (TAC) for further assistance if needed.

### **Background Information**

The purpose of this document is to ensure the Cisco Secure Client AnyConnect VPN configuration is adhering to security best practices in a modern world where cybersecurity attacks are common.

Brute force attacks usually involve repeated attempts to gain access to a resource by using username and password combinations. Attackers try to use their internet browser, the Secure Client User Interface, or other tools to enter multiple usernames and passwords hoping they match a legitimate combination in a AAA database. When using AAA for authentication we expect the end user to enter their username and password since this is necessary to establish the connection. At the same time, we are not verifying who the user is until they enter their credentials. By nature, this allows attackers to take advantage of these scenarios:

- 1. Exposed fully qualified domain names for the Cisco Secure Firewall (especially when using a group-aliases in the connection profile):
  - If the attacker discovers the FQDN of your VPN firewall, they then have the option to select the tunnel-group using the group-alias in which they want to start the brute-force attack.
- 2. Default Connection Profile configured with AAA or Local Database:
  - If the attacker finds the FQDN of the VPN firewall, they can attempt to brute-force attack the AAA server or local database. This occurs because the connection to the FQDN lands on the Default Connection Profile, even if no group-aliases are specified.
- 3. Resource exhaustion on the firewall or on AAA servers:
  - Attackers can overwhelm AAA servers or firewall resources by sending large amounts of authentication requests and creating a Denial of Service (DoS) condition.

### Concepts

Group-Aliases:

• An alternate name by which the firewall can refer to a connection profile. After initiating a connection to the firewall, these names appear in a drop-down menu in the Secure Client UI for users to select. The removal of group-aliases removes the drop-down functionality in the Secure Client UI.

#### Group-URLs:

• A URL that can be tied to a connection profile so that incoming connections are direcly mapped to a desired connection profile. There is no drop-down functionality, as users can enter the full URL in the Secure Client UI, or the URL can be integrated with a 'Display Name' in the XML profile to hide the URL from the user.

The difference here is when group-aliases are implemented, a user initiates a connection to vpn\_gateway.example.com and is presented with aliases to select that drive them to a connection profile. With group-URLs, a user initiates a connection to vpn\_gateway.example.com/example\_group and that drives them directly to the connection profile without the need or option for a drop-down menu.

## **Secure Client Hardening Practices on Cisco Secure Firewall:**

These methods rely on mapping legitimate users to proper tunnel-groups/connection profiles while potentially malicious users are sent to a trap tunnel-group that we configure to not allow username and password combinations. Though not all combinations must be implemented, disabling group-aliases and changing the authentication method of the DefaultWEBVPNGroup and DefaultRAGroup are required for the recommendations to work effectively.

- Remove group aliases and only use group-url in the Connection Profile configuration, this allows you to have a specific FQDN that is not going to be easy for an attacker to discover and select since only the clients with the proper FQDN are able to initiate the connection. For example vpn\_gateway.example.com/example\_group is harder for an attacker to discover than vpn\_gateway.example.com.
- Disable AAA authentication in the DefaultWEBVPNGroup and DefaultRAGroup and configure certificate authentication, this avoids a possible brute-force against the local database or AAA server. The attacker in this scenario would be presented with immediate errors upon attempting to connect. There is no username or password field since the authentication is based on certificates, thus stopping brute force attempts. Another option is to create a AAA server with no supporting configuration to create a sinkhole for malicious requests.
- Utilize certificate-mapping for the connection profile. This allows incoming connections to be mapped to specific connection profiles based on attributes received from certificates on the client device. Users who have the proper certificates are mapped correctly, while attackers who fail the mapping criteria are sent to the DefaultWEBVPNGroup.
- The usage of IKEv2-IPSec instead of SSL causes tunnel-groups rely to on a specific user-group mapping in the XML profile. Without this XML on the end user machine, users are automatically sent to the default tunnel-group.



**Note**: For a more information regarding the group-alias functionality, see <u>ASA VPN Configuration</u> <u>Guide</u> and observe 'Table 1. Connection Profile Attributes for SSL VPN'.

## **Identify Attacks using Logging and Syslog IDs**

Brute-force attacks represent the predominant method of compromising Remote Access VPNs, exploiting weak passwords to gain unauthorized entry. It is crucial to know how to recognize signs of an attack by leveraging the use of logging and evaluating syslogs. Common syslogs IDs that can indicate an attack if encountered with abnormal volume are:

%ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

#### %ASA-6-113005

<#root>

#### %ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = \*\*\*\*\* : user IP =

%ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN

The username is always hidden until the **no logging hide username** command is configured on ASA.



**Note**: Note: This provides insight if valid users are generated or known by offending IPs however, please be cautious as usernames are visible in the logs.

#### **Cisco ASA Logging:**

Logging chapter of the Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide

#### **Cisco FTD Logging:**

Configure Logging on FTD via FMC

<u>Configure Syslog</u> section in the Platform Settings chapter of the Cisco Secure Firewall Management Center Device Configuration Guide

Configure and Verify Syslog in Firepower Device Manager

<u>Configuring System Logging Settings</u> section in the System Settings chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager

#### **Attack Verification**

To verify, log in to the ASA or FTD Command Line Interface (CLI), run the show aaa-server command and investigate for an unusual number of attempted and rejected authentication requests to any of the configured AAA servers:

<#root>

ciscoasa#

show aaa-server

```
Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time Oms
Number of authentication requests 8473575 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - - >>>> Unusual increments
```

<#root>

ciscoasa#

show aaa-server

Server Protocol: ldap Server Hostname: ldap-server.example.com Server Address: 10.10.10.10 Server port: 636 Server status: ACTIVE, Last transaction at unknown Number of pending requests 0 Average round trip time Oms Number of authentication requests 2228536 - - - - - >>>> Unusual increments Number of authorization requests 0 Number of accounting requests 0 Number of retransmissions 0 Number of accepts 1312 Number of rejects 2225363 - - - - - >>>> Unusual increments Number of challenges 0 Number of malformed responses 0 Number of bad authenticators 0 Number of timeouts 1 Number of unrecognized responses 0

### **FMC Configuration Examples**

Disable AAA Authentication in the DefaultWEBVPNGroup and DefaultRAGroup Connection Profiles

Navigate to **Devices > Remote Access**.

Fi ov	irewall Manage verview / Dashboards	ement Center s / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration		
Summ Provides a su Network	nary Dashbo ummary of activity on the c Threats	ard ( <u>switch dashboard)</u> appliance Intrusion Events	Status	Geolocation	QoS	Device M NAT QoS Platform FlexConf Certificat	lanagement Settings ig es	VPN Site To Site Remote Access Dynamic Access Troubleshooting	Policy	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture
► Top Z	ero Trust Applicatio	ns			- ×					Upgrade Threat Defense Upgrade Chassis Upgrade

Displays navigating the FMC GUI to get to the Remote Access VPN Policy configuration.

Edit the existing Remote Access VPN Policy and create a connection profile named 'DefaultRAGroup'

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ و	• 0	admin ~	that SECURE
												Add
Namo				Status			Last Modified					
RAVPN				Targeting 1 Up-to-date	devices on all targeted		2024-03-07 10:58:20 Modified by "admin"			q	/ i	

Displays how to edit the Remote Access VPN Policy within the FMC UI..

Edit the connection profiles named 'DefaultWEBVPNGroup' and 'DefaultRAGroup'

Firewall Management Center Devices / VPN / Edit Connection Profile Overview	Analysis Policies	Devices Objects	s Integration	Deploy Q	⊘ 🌣 🎯 🛛 admin ∽ 🔤 secure
RAVPN					Save
Enter Description Connection Profile Access Interfaces Advanced				Local Realm: LOCAL-REALM	Policy Assignments (1) Dynamic Access Policy: None
Name	АЛА			Group Policy	
DefaultWEBVPMGroup		LOCAL None None		DiltGrpPolicy	

Displays how to edit the DefaultWEBVPNGroup within the FMC UI.

Navigate to the **AAA** tab and select the **Authentication Method** dropdown. Select '**Client Certificate Only**' and select **Save**.

Edit Connection Profile		0
Connection Profile:*	DefaultWEBVPNGroup	
Group Policy:*	DfltGrpPolicy +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method:	Client Certificate Only -	
	Enable multiple certificate authentication	
Map username from clier	nt certificate	
Authorization		
Authorization Server:	<b></b>	
	Allow connection only if user exists in authorization database	
Accounting		
Accounting Server:	<b></b>	
	Cancel	8

Changing the authentication method to client certificate only for the DefaultWEBVPNGroup within the FMC UI.

Edit the DefaultRAGroup and Navigate to the **AAA** tab and select the **Authentication Method** dropdown. Select 'Client Certificate Only' and select Save.

Edit Connection Profile		
Connection Profile:*	DefaultRAGroup	
Group Policy:*	DfltGrpPolicy +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method:	Client Certificate Only -	
	Enable multiple certificate authentication	
Map username from clie	nt certificate	
Authorization		
Authorization Server:	▼	
	Allow connection only if user exists in authorization database	
Accounting		
Accounting Server:	▼	
	Cancel	/e

Changing the authentication method to client certificate only for the DefaultRAGroup within the FMC UI.



**Note**: The authentication method can also be a sinkhole AAA server. If this method is used, the AAA server configuration is fake, and does not actually process any requests. A VPN pool must also be defined in the 'Client Address Assignment' tab to save the changes.

# Disable Hostscan / Secure Firewall Posture on the DefaultWEBVPNGroup and DefaultRAGroup (optional)

This is only necessary if you have Hostscan / Secure Firewall Posture in your environment. This step prevents attackers from increasing the resource utilization on the firewall caused by the endpoint scanning process. In the FMC, this is achieved by creating a FlexConfig object with the command **without-csd** to disable the endpoint scanning functionality.

Navigate to Objects > Object Management > FlexConfig Object > Add FlexConfig Object.

Cipiects / Object Management	tt Center Overview Analysis Policies Devices Objects Integration	Deptoy Q 🧬 🌣 🚱 admin 🗸	disch SECURE									
<ul> <li>AAA Server</li> <li>Access List</li> <li>Address Pools</li> <li>Application Filters</li> </ul>	FlexConfig Object FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in RevConfig polices.	Add FlexConfig Object										
AS Path	Name Description											
BFD Template	Anyconnect_route_filtering		<b>6/</b> ₹									
Community List	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNS										
DHCP IPv6 Pool	Default_Inspection_Protocol_Disable	Disable Default Inspection.	¶a Q ≣									
> Distinguished Name DNS Server Group	Default_Inspection_Protocol_Enable	Enable Default Inspection.	¶aq ≣									
> External Attributes	DHCPv6_Prefx_Delegation_Configure	Configure one outside (PD client) and one inside interface (recip	¶a ⊂ ≣									
File List	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside i	¶aq. ]]									
<ul> <li>FlexConfig</li> <li>FlexConfig Object</li> </ul>	DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and	¶a q ≣									
Text Object	DNS_UnConfigure	Remove the DNS configurations.	¶aq									
Geolocation	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-su	¶_q =									
Key Chain	ace Eggp_Interface_Configure Configure for eigrp. 1. Configures aut											
Network	Eigrp_UnConfigure	Clears eigrp configuration for an AS	¶aq ≣									

Navigating the FMC UI to create a FlexConfig object.

Name the FlexConfig object, set the deployment to **Everytime** with the type **Append**. Then, enter the syntax exactly as shown and save the object.

Edit FlexConfig Object							0
Name: Without-CSD Description: Copy-pasting any rich text might in	troduce line break	s while generating C	LI. Please	e verify the	e CLI before deploy	/ment.	
Insert 🔻 🔣 Deployment	:: Everytime		•	Type:	Append	•	
without-csd tunnel-group DefaultRAGroup weby without-csd	pn-attributes						
▼ Variables			Drop	orthe		7	
Name	Dimension	Default Value	(Тур	e:Name)	Override	Description	
		No records to	display				
						Cancel	Save

Creating a FlexConfig object with 'without-csd'

Navigate to **Devices** > **FlexConfig** and then click the **Pencil** to edit the FlexConfig Policy.

þ	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	<b>°</b>	0	admin $\vee$	disco SECURE
														New Policy
	TexConfig Policy					Status		Last Modified						
	Flex-Test					Targeting 1 Out-of-date	devices e on 1 targeted devices	2024-04-10 21:54:19 Modified by "admin"						9 🖊 î

Editing the FlexConfig policy within the FMC.

Locate the object you created from the **User Defined** section. Then, select the arrow to add it to the **Selected Append FlexConfigs**. Lastly, select **Save** to save the FlexConfig policy.

Firewall Management Center Devices / Records Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q, 🥔 🏟 admin 🗸 👘 secure	
FlexConfig Enter Description							Nou have sensived changes Migratic Scrifton Preview Config Save Cancel Policy Assignments (1)	
Available FlexConfig C FlexConfig Object	Selec	ted Prepend F	lexConfigs		Description			
V User Defined ?) Anyconnect, route_thering 								
V System Defined								
Default_Inspection_Protocol_Disable	V Selected Append FlexConfigs							
12 Default_Inspection_Protocol_Enable	# N:	ime			Description			
DHCPv6_Prefx_Delegation_Configure	1 W	thout-CSD					٩	

Attach the FlexConfig object to the FlexConfig Policy.

Select **Policy Assignments** and choose the FTD you want to apply this FlexConfig policy to, then select **OK**. Select **Save** again if this is a new FlexConfig assignment and deploy the changes. Once deployed, verify

Firewall Management Center Devices / Response Policy Editor	Overview	Analysis	Policies Devic	ces Objects	Integrat	ion			Deploy Q	• • •	admin ~state	ECURE
FlexConfig Enter Description											Config Sinve C	Cancel
Available FlexConfig C FlexConfig Object	1 Selected	Prepend Fle	xConfigs	President								
×	a Name	Targete	d Devices	Description								
V User Defined												
2 Anyconnect_route_filtering		Targete	ed Devices									
.9 hostscan_data_limit												
"2 Keepout		Select d	evices to which you	want to apply this	policy.	Selected Devices						
12 No_Keepout		Available	e Devices	- 1		FTD1	=					
"? Remove_hostscan_datalimit			terr by manie or vare	Adi								
Www.eucedo												
V System Defined												
<sup>2</sup> Default_DNS_Configure		A l										
.7 Default_Inspection_Protocol_Disable	- Name	- 1 - E										
2 Default_Inspection_Protocol_Enable												
2 DHCPv6_Prefix_Delegation_Configure												Q.≣
.7 DHCPv6_Prefix_Delegation_UnConfigure								Cancel				
"? DNS_Configure												

Assign the FlexConfig Policy to a FirePOWER device.

Enter the FTD CLI and issue the command **show run tunnel-group** for the DefaultWEBVPNGroup and DefaultRAGroup. Verify that **without-csd** is now present in the configuration.

<#root>

FTD72#

show run tunnel-group DefaultRAGroup

tunnel-group DefaultRAGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultRAGroup webvpn-attributes
authentication certificate

without-csd

FTD72#

show run tunnel-group DefaultWEBVPNGroup

tunnel-group DefaultWEBVPNGroup general-attributes address-pool TEST-POOL tunnel-group DefaultWEBVPNGroup webvpn-attributes authentication certificate

without-csd

### **Remove Group-aliases and Enable Group-URLs**

Navigate to a connection profile and select the 'Aliases' tab. Delete the group-alias, and click the **plus** icon to add a URL alias.

Edit Connection Profile		0									
Connection Profile:* LDAP-TG											
Group Policy:* DfltGrpPolicy Edit Group Policy	<ul> <li>+</li> </ul>										
Alias Names: Incoming users can choose an alias name upon first login. Aliase this device can be turned on or off for display.	es from all connections con	figured on +									
Name	Status										
LDAP	Enabled	1									
URL Alias: Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.											
URL	Status										
	Cancel	Save									

Deleting the group-alias option for a tunnel-group within the FMC UI.

Configure an object name for the URL alias, and fill out the FQDN and/or IP address of the firewall for the URL, followed by the name you want to associate the connection profile with. In this example, we chose 'aaaldap'. The more obscure, the more secure, as it is less likely for attackers to guess the full URL even if they have obtained your FQDN. Once finished, select **Save**.



Creating a URL-Alias object within the FMC UI.

Select the URL Alias from the dropdown, check the Enabled box and select OK.



Ensure the URL-Alias is enabled within the FMC UI.

Ensure the group-alias is deleted and check that your URL Alias is now enabled then select **Save**.

Edit Connection Profile	e			0
Connection Profile:*	LDAP-TG			
Group Policy:*	DfltGrpPolic	хy	•]+	
	Edit Group Policy			
Client Address Assignmen	t AAA	Aliases		
Alias Names:				
Incoming users can choose a this device can be turned on	an alias name or off for disp	upon first login. Iav.	Aliases from all connection	ons configured on

Name	Status	
URL Alias:		
Configure the list of URL alias which your endpoints can	select on web access. If u	sers choose the
following URLs, system will automatically log them in via	this connection profile.	
		a 1977
URL	Status	
LDAP-ALIAS (https://ftd	Enabled	/1
		Seve Seve

Enabling the URL-Alias option for a tunnel-group within the FMC UI.

If desired, URL Aliases can also be pushed as part of the XML. This is achieved by editing the XML using the VPN Profile Editor or the ASA Profile Editor. To accomplish this, navigate to the Server List tab and ensure the User Group field matches the URL Alias of the connection profile when using SSL. For IKEv2, ensure the User Group field matches the exact name of the connection profile.

Server List Entry
Primary Server     Connection Information       Display Name (required)     FTD1-SSL       Primary Protocol     SSL       FQDN or IP A     User Group       Add Method During IKE Negotistion     EAP-AnyConnect        Group URL     IKE Identity (IOS gateway only)
Badup Servers Hist Address Add Move Up Move D Delete
OK Cancel

Editing the XML profile to have a URL-Alias for SSL connections.

### **Certificate Mapping**

Navigate to the **Advanced** tab within the Remote Access VPN Policy. Choose a general setting option based upon preference. Once selected, select **Add Mapping**.

RAVPN		You have unsaved changes Save Cancel
Connection Profile Access Inter	aces Advanced	Policy Assignments (1) Local Realm: None Dynamic Access Policy: None
Secure Client Images Secure Client Customization GUI Text and Messages Icons and Images Scripts Binaries Custom Installer Transforms	General Settings for Connection Profile Mapping         The divice processes the policies in the order listed below until it finds a match         Use group URL if group URL and Certificate Map match different Connection Profiles         Use group URL if group URL and Certificate to a Connection Profile         Certificate to Connection Profile Mapping         Cient request is checked against each Certificate Map associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, defailed         Please provide at least one Certificate Mapping	at connection profile will be chosen.
Localized Installer Transforms	Certificate Map Connection Profile	
Address Assignment Policy	No Records Found	
Group Policies LDAP Attribute Mapping Load Balancing V IPsec Crypto Maps IKE Policy	Default Connection Profiles	
IPsec/IKEv2 Parameters	Designer Contractions Profile will be applied when news of the Certificate May's role is matched.	

Navigating to the Advanced tab within the FMC UI to create a certificate map object within the FMC UI.

Name the certificate map object and select **Add Rule**. In this rule, define the properties of the certificate you would like to identify to map the user to a certain connection profile. Once finished, select **OK** and then select **Save**.

Add	I Certificate Map					8
Maµ C Maµ Cor	p Name*: Certificate-Map-CN pping Rule nfigure the certificate ma	atching rule			Add Rule	
#	Field	Component	Operator	Value		
1	Subject -	CN (Common Nam -	Equals -	customval	le	
	OK Cancel					
				Cance	l Sav	е

Create a certificate map and add criteria for the map within the FMC UI.

From the dropdown, select the certificate map object, and the connection profile you want the certificate map to be associated with. Then select **OK**.

Add Connection Profile to Certificate Map
Choose a Certificate Map and associate Connection Profiles to selected Certficate Map.
Certificate Map Name*:
Certificate-Map-CN - +
Connection Profile*:
LDAP-TG 🔻
Cancel

Tie the certificate map object to the desired tunnel-group within the FMC UI.

Ensure the Default Connection Profile is configured as DefaultWEBVPNGroup so if a user fails the mapping they are sent to the DefaultWEBVPNGroup. Once finished, select **Save** and deploy the changes.

RAVPN		You P	ave unsaved changes Save Cancel
Enter Description			
			Policy Assignments (1)
0		Local Realm: None	Dynamic Access Policy: None
Connection Profile Access Inter	aces Advanced		
Secure Client Images	General Settings for Connection Profile Mapping		
Secure Client Customization	The device processes the policies in the order listed below until it finds a match		
GUI Text and Messages	Use group URL if group URL and Certificate Map match different Connection Profiles		
Icons and Images	Use the configured rules to match a certificate to a Connection Profile		
Scripts	Certificate to Connection Profile Mapping Client request is checked against each Certificate Map associated Connection Profile will be used when piles are mat	ched. If none of the Certificate Man is matched, default connection profile will be chosen	
Binaries	Create response to conclusion against court contracter map, associated contractors trains the be used titled takes are man	nned, a norad of any destandance reap to measured, destant dosmocratis provide real of despare.	Add Manning
Custom Installer Transforms			Abd Mapping
Localized Installer Transforms	Certificate Map	Connection Profile	
Address Assignment Policy	Certificate-Map-CN	LDAP-TG	1
Certificate Maps			
Group Policies			
LDAP Attribute Mapping			
Load Balancing			
<ul> <li>IPsec</li> </ul>			
Crypto Maps			
IKE Policy	Default Connection Drottler		
IPsec/IKEv2 Parameters	This Connection Profile will be applied when none of the Certificate Map's rule is matched.		DefaultWEBVPNGroup *

Change the default connection profile for certificate mapping to the DefaultWEBVPNGroup within the FMC UI.

### IPsec-IKEv2

Select the desired IPsec-IKEv2 connection profile, and navigate to Edit Group Policy.

Edit Connection Profil	e	
Connection Profile:*	IKEV2	
Group Policy:*	IKEV2-IPSEC	
Client Address Assignmen	nt AAA Aliases	

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools:

Name	IP Address Range	
AnyConnect_Pool	10.50.50.1-10.50.50.6	/1
DHCP Servers:		+
Name	DHCP Server IP Address	
	Cancel	Save

Edit a group-policy within the FMC UI.

In the General tab, navigate to the VPN Protocols section and ensure the IPsec-IKEv2 box is checked.

Edit Group Policy	
Name:* IKEV2-IPSEC	
Description: General Secure	Client Advanced
VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling	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

Enable IPsec-IKEv2 within a group-policy in the FMC UI.

In the VPN Profile Editor, or ASA Profile Editor, navigate to the Server List tab. The User Group name MUST be an exact match to the connection profile name on the firewall. In this example, IKEV2 was the connection profile / User Group name. The primary protocol is configured as IPsec. The 'Display Name' in is displayed to the user in the Secure Client UI when establish a connection to this connection profile.

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certific	ate Pinning
Primary Server Display Name (required) FTD1-IPSEC FQDN or IP A Group URL Ftd1	Connection Information Primary Protocol IPsec ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only)
Backup Servers Host Address	Add Move Up
	Move D Delete
ОК	Cancel

Edit the XML profile so that the primary protocol is IPsec, and the User Group matches the connection profile name.



**Caution**: An SSL connection is required to push XML profiles to the client from the firewall. When only using IKEV2-IPsec, the XML profiles must be pushed to the clients via an out-of-band method.

Once the XML profile is pushed to the client, Secure Client uses the **User Group** from the XML profile to connect to the IKEV2-IPsec connection profile.

🕲 Cisco Secu	re Client	_		×
	AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC	~	Connect	
Cisco Se	ecure Client   FTD1-IPSEC		×	altalta cisco
Us Pa	ername: nroche ssword:			
	ОК	Canc	el	

Secure Client UI view of the IPsec-IKEv2 RAVPN connection attempt.

## **ASA Configuration Examples**

# Disable AAA Authentication in the DefaultWEBVPNGroup and DefaultRAGroup Connection Profiles

Enter the webvpn-attributes section for tunnel-group DefaultWEBVPNGroup and specify the authentication as certificate based. Repeat this process for the DefaultRAGroup. Users who land on these default connection profiles are forced to present a certificate for authentication and are not presented with the opportunity to enter username and password credentials.

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# authentication certificate ASA# configure terminal

ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes ASA(config-tunnel-webvpn)# authentication certificate

# **Disable Hostscan / Secure Firewall Posture on the DefaultWEBVPNGroup and DefaultRAGroup (optional)**

This is only necessary if you have Hostscan / Secure Firewall Posture in your environment. This step prevents attackers from increasing the resource utilization on the firewall caused by the endpoint scanning process. Enter the webvpn-attributes section for the DefaultWEBVPNGroup and DefaultRAGroup and connection profiles and implement **without-csd** to disable the endpoint scanning functionality.

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

ASA# configure terminal ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

#### **Remove Group-aliases and Enable Group-URLs**

Enter the tunnel-group(s) users are connecting to. If there is an existing group-alias, remove it. In this example it is removed. Once that is complete, create a group-url using the FQDN or IP address of the RAVPN terminating interface. The name on the end of the group-url needs to be obscure. Avoid common values such as VPN, AAA, RADIUS, LDAP as these make it easier for attackers to guess the full URL if they obtain the FQDN. Instead use internally significant names that help you identify the tunnel-group.

ASA# configure terminal ASA(config)# tunnel-group NAME webvpn-attributes ASA(config-tunnel-webvpn)# no group-alias NAME ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable

#### **Certificate Mapping**

From global configuration mode, create a certificate map and assign it a name and a sequence number. Then define a rule that users must match to utilize the mapping. In this example, users would have to match the criteria of a common name value that equals "customvalue". Next, enter the webvpn configuration and apply the certificate map to the desired tunnel-group. Once completed, enter the DefaultWEBVPNGroup and make this tunnel-group the default for users who fail the certificate mapping. If users fail the mapping, they are directed to the DefaultWEBVPNGroup. While the DefaultWEBVPNGroup is configured with certificate authentication, users do not have the option to pass username or password credentials.

ASA(config)# crypto ca certificate map NAME 1 ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

ASA(config)# webvpn ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# tunnel-group-map default-group

#### IPsec-IKEv2

this connection profile.

From global configuration mode, you can edit an existing group-policy or create a new one and enter the attributes for that group-policy. Once you are in the attributes section, enable IKEv2 as the only vpn tunnel protocol. Ensure that this group-policy is tied to a tunnel-group that is going to be utilized for IPsec-IKEV2 remote access VPN connections. Similar to the FMC steps, you must edit the XML profile via the VPN Profile Editor or the ASA Profile Editor and change the User Group field to match the name of the tunnel-group on the ASA, and change the protocol to IPsec.

ASA# configure terminal ASA(config)# group-policy GP-NAME internal ASA(config)# group-policy GP-NAME attributes ASA(config-group-policy)# vpn-tunnel-protocol ikev2 ASA(config)# tunnel-group TG-NAME general-attributes

ASA(config-tunnel-general)# default-group-policy GP-NAME

In the VPN Profile Editor, or ASA Profile Editor, navigate to the Server List tab. The User Group name MUST be an exact match to the connection profile name on the firewall. The primary protocol is configured as IPsec. The display name is shown to the user in the Secure Client UI when establishing a connection to

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certific	ate Pinning
Primary Server Display Name (required) ASA-IPsec FQDN or IP A User Group FQDN TG-NAME Group URL FQDN/TG-NAME	Connection Information Primary Protocol IPsec  ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect  IKE Identity (IOS gateway only)
Backup Servers Host Address	Add Move Up Move D Delete
ОК	Cancel

Edit the XML profile so that the primary protocol name is IPsec and the User Group name matches the tunnel-group name of the ASA for IPsec-IKEv2 RAVPN connections.



**Caution**: An SSL connection is required to push XML profiles to the client from the firewall. When only using IKEV2-IPsec, the XML profiles must be pushed to the clients via an out-of-band method.

# Conclusion

In summation, the purpose of the hardening practices in this document is to map legitimate users to custom connection profiles while attackers are forced to the DefaultWEBVPNGroup and the DefaultRAGroup. In an optimized configuration, the two default connection profiles do not have any legitmate custom AAA server configuration. Additionally, the removal of group-aliases prevents attackers from easily identifying custom connection profiles by removing the drop-down visibility upon navigating to the FQDN or public IP address of the firewall.

# **Related Information**

Cisco Technical Support and Downloads

Password Spray Attacks

Unauthorized Access Vulnerability September 2023

ASA Configuration Guides

FMC / FDM Configuration Guides