Whitepaper -Configuring IPsec IKEv2 Remote Access VPN with Cisco Secure Firewall

Marvin Rhoads

11-2-2021

Abstract / Introduction	1
Problem Statement	1
Background	2
Solution	4
Configuration	4
Important Notes Regarding Client Services:	5
IPsec and ISAKMP Settings:	9
Troubleshooting note:	10
Verification	12
Conclusion	14
References	14

Revision 1.1

- Updated

# Abstract / Introduction

There has been recent guidance<sup>1</sup> from the United States National Security Agency (NSA) recommending that organizations adopt Internet Protocol security with Internet Key Exchange version 2 (IPsec IKEv2) for Remote Access Virtual Private Networks (RA VPNs) due to numerous instances of attackers leveraging vulnerabilities in Secure Sockets Layer / Transport Layer Security (SSL/TLS) implementations.

In this paper we will demonstrate how to implement these recommendations via configuration of a solution that uses the capabilities of Cisco's current security product portfolio.

Function	Product	Version
Firewall	Cisco Secure Firewall Threat Defense Virtual	7.0.1
	(FTDv)	
Management	Cisco Secure Firewall Management Center	7.0.1
	(FMC)	
Endpoint software	Cisco AnyConnect Secure Mobility Client	4.10.03104

We will use the following Cisco products:

We will demonstrate the integration steps to configure these products to work together to deliver an end-to-end security solution that restricts an RA VPN to using IPsec IKEv2 as opposed to the more commonly used SSL/TLS method.

## Problem Statement

Most Cisco-based remote access VPNs in the installed base are currently using SSL/TLS. While the Cisco AnyConnect Secure Mobility Client has always supported both SSL/TLS and IPsec IKEv2 as transport protocols, most implementations use SSL/TLS due to its ease of configuration and the fact that it is the default selection.

There are several configuration guides published covering how to configure AnyConnect using IPsec IKEv2. For example :

https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asasoftware/213246-asa-ikev2-ra-vpn-with-windows-7-or-andro.html

https://community.cisco.com/t5/security-documents/asa-anyconnect-ikev2-configurationexample/ta-p/3117462

<sup>&</sup>lt;sup>1</sup> NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs

However, they are written for the Cisco ASA use case and there isn't (as of the time of this paper's publication) current guidance for doing the same with Cisco Secure Firewall (FTD).

A whitepaper such as this one will give organizations a prescriptive guide to adopting the NSA and CISA guidance while running the most recent products and versions from Cisco's security portfolio.

**Note:** Within the context of IPsec IKEv2, there is an option to secure access even more stringently by using exclusively "Suite B<sup>2</sup>" next generation encryption.

While Suite B is recommended for highest security when using IPsec IKEv2, it does require AnyConnect Apex licensing<sup>3</sup>. It also introduces several other requirements, notably the use of AES-256-GCM symmetric encryption, Elliptic Curve Digital Signature Algorithm (ECDSA) for the certificates used and Elliptic Curve Diffie-Hellman (ECDH) key agreement.

Also, if we forgo use of Suite B, we can use AnyConnect Plus or VPN only licensing levels. Thus, we are covering only the non-Suite B configuration steps in this paper. In either case, we should follow the minimum guidance for IPsec IKEv2 VPNs from NSA<sup>4</sup>.

## Background

## Firewall – Cisco Secure Firewall

Commonly referred to as Firepower Threat Defense (FTD) but recently rebranded as Cisco Secure Firewall, FTD is Cisco's Next-Generation Firewall (NGFW). It is a unified image combining the classic Cisco ASA stateful firewall with the Firepower Next-Generation Intrusion Prevention System (NGIPS) technology based on the underlying Snort IPS engine that was part of Cisco's acquisition of Sourcefire in 2014.

### Cisco Secure Firewall product page

FTD appliances can be deployed on a broad variety of hardware platforms as well as VMs on either onpremises hypervisors (VMware ESXi and KVM) as well as in AWS and Azure public clouds. They can also be deployed in high availability pairs or in scalable clusters.

For purposes of this paper, we are using a single FTD virtual appliance (FTDv) deployed as VM on a VMware ESXi server.

FTD also has varying license levels including the base Threat license, URL Filtering and Malware, as well as tiered performance licenses (the latter as of release 7.0). The solution described in this paper works with the base license. FTD does require remote access VPN (RA VPN) licensing for the AnyConnect client functionality.

<sup>&</sup>lt;sup>2</sup> Suite B Cryptography

<sup>&</sup>lt;sup>3</sup> AnyConnect Ordering Guide

<sup>&</sup>lt;sup>4</sup> Configuring IPsec Virtual Private Networks (NSA)

### Management - Cisco Secure Firewall Management Center (FMC)

Note this is commonly known as its former product name - Firepower Management Center or FMC.

Firewall Management Center product page

FTD devices can be managed fundamentally via two different methods:

- 1. A traditional method using Cisco's Firewall Management Center (FMC) product or
- 2. A newer modern architecture method using REST API and a combination of on-box Firepower Device Manager (FDM) and the cloud-based Cisco Defense Orchestrator (CDO) Software as a Service (SaaS) offering.

We will be using the first method.

### Endpoint Software – Cisco AnyConnect Secure Mobility Client

AnyConnect is Cisco's unified client for VPN and other secure client features (such as Posture, Umbrella Roaming Security, Network Visibility etc.). In this paper we are only using the VPN functionality to demonstrate our solution.

### AnyConnect Secure Mobility Client product page

AnyConnect is licensed per user in various feature packages – Plus, Apex and VPN-Only. Licenses are allocated from a customer's Smart Licensing portal (<u>https://software.cisco.com</u>) via the managing FMC to the managed FTD device to provide the feature to end users. The solution described here works with all the AnyConnect license types.

## Solution

## Configuration

For purposes of this discussion, we will cover only the parts specific to the features being leveraged for this integration. We will not cover basic product setup as there are numerous other references: Cisco-published product documentation, <u>Cisco Security Community documents</u> and third party training and web-based resources.

First, we follow this guide for basic setup of a remote access (RA) VPN on Firepower:

Remote Access VPNs for Firepower Threat Defense

In our case, we have an existing remote access VPN configured with the Access interface in the Outsidezone set to support the incoming connections:

$\leftarrow \rightarrow C$	) 🔓 https://fmc.ccielab.mmeteng.com/ddd/#RaVpnEditIntfProfile;uuid=000C2956-9998-0ed3-0000-004294969381;type=RA.VPNH.VPN 🏠									$\boxtimes$ =				
Firepower Manage Devices / VPN / Edit Interfe	ement Center ace Profile	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence		Deploy	Q 🧬	\$	🛛 adm	i-marvin 🔻
RA_VPN														Cancel
Policy Assignments (1)     ^       Connection Profile     Access Interfaces     Advanced														
Interfaces of the targeted device w	Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections +													
Name	Interface Trust	point	DTI	.S		SSL			IPsec-IKEv2					
Outside-Zone			•			٥			•			/	Ŵ	
Access Settings														
SSL Settings														
Web Access Port Number:*	443													
DTLS Port Number:*	443													
SSL Global Identity Certificate:	FTDv-2-self-signed	•	]+											
Note: Ensure the port used in VPN configuration is not used in other services														

To change the transport protocol for the RA VPN, we edit the access interface and select "Enable IPsec-IKEv2" in lieu of the default "Enable SSL" (SSL/TLS with DTLS is the actual detail vs. what is shown in the GUI) as follows:

Edit Acces	Edit Access Interface					
Access Interface: Protocol:	Outside-home					
<ul> <li>Enable IP</li> <li>Enable SS</li> </ul>	sec-IKEv2 SL					
🗹 Enabl	e Datagram Transport Layer Security					
Confi	gure interface specific identity certificate					
The 'SSL G configured	ilobal identity certificate' will be used if no interface identity certificate is					
	Cancel	Ж				

Click OK, save the change and then deploy.

## Important Notes Regarding Client Services

Even though we disabled SSL in this section, that applies only to the transport of the RA VPN user traffic. There is still an aspect of the system that is using SSL/TLS for what is known as Client Services.

Client services provide several features, most notably the ability to download any profile changes and AnyConnect software updates from the FTD device to the clients. Other less commonly used features include Hostscan (for posture checking with AnyConnect Apex licensing), SCEP enrollment and Cisco Secure Desktop (CSD - deprecated but still found in some deployments).

Many customers may elect to retain the client services settings to avail themselves of these features. However, it should be noted that doing so will result in the continued exposure of SSL/TLS (with any associated vulnerabilities) on the interface presenting the RA VPN service.

#### Below we can see three successive iterations of the listening ports on the target FTD device.

#### First, with SSL/DTLS enabled for the VPN:

> show asp table socket							
Protocol	Socket	State	Local Address	Foreign Address			
SSL	00008bd8	LISTEN	192.168.0.204:443	0.0.0.0:*			
DTLS	00016958	LISTEN	192.168.0.204:443	0.0.0.0:*			

#### Second, with SSL Disabled in favor of IPsec:

> show asp	table soci	ket		
Protocol	Socket	State	Local Address	Foreign Address
SSL	00008bd8	LISTEN	192.168.0.204:443	0.0.0.0:*

...and third, with Client Services disabled. Note that **only when we disable Client services is SSL/TLS truly disabled from the Outside interface**.

> show asp	table socł	ket			
Protocol	Socket	State	Local Address	Foreign	Address

To completely disable Client services, we must reference the Advanced section of the VPN Connection profile and deselect the default "Enable Client Services":

<image/> And the design of the desi	< -> 0 C	🔄 🔿 🕐 🕐 🖉 Strate S								
Celled  Celled C	Firepower Manage Devoes / VPN / Edit Advan	ement Center Overview Analysis Policies Devices Objects AMP Intelligence	• ):			Deploy Q 💞 🧔 admin 🕶				
	CCIELab					Cancel				
Added media in the second media in the seco										
Automa to the set of the						Policy.Assionments.(1)				
Calculation       A construction       A constr						Local Realm: None Dynamic Access Policy: None				
Advance under normality of a second s	Connection Profile Access into	enaces Advanced								
Addama (and many one of the set o	AnyConnect Client Images	Crypto Maps								
Center danse     Inter construction of the state of the s	Address Assignment Policy	Crypto Maps are auto generated for the interfaces on which IPsec-IKEv2 protocol is enabled. Entrusion are the list of the interface around on which IPsec-IKEv2 protocol is enabled.	to this VDN conferenties in "Access Interfac	e tak						
Que Que Que Control     Intellection     Editory (Control     Intellection)       Control     Control     Intellection)     Intellection)       Control     Control     Intellection)     Intellection)       Control     Intellection)     Intellection)     Intellection)       Control     Intellection) <td>Certificate Maps</td> <td></td> <td></td> <td></td> <td></td> <td></td>	Certificate Maps									
Cab Jacobi     Pages Jacobi     Faller Cab Jacobi	Group Policies	Interface Group	Edit Crypto Map	0	Rid					
Cardia chara     Pare     Pare Mare     Pare Allow     Pare Allow </td <td>LDAP Attribute Mapping</td> <td>Outside-home</td> <td>can orypto map</td> <td></td> <td>True .</td> <td>1</td>	LDAP Attribute Mapping	Outside-home	can orypto map		True .	1				
Amode       Calcele-Amode         Original Data       Calcele-Amode         B Datay       Proceeding         Proceeding       Calcele-Amode         India       India         India <t< td=""><td>Load Balancing</td><td></td><td>Interface Group:</td><td></td><td></td><td></td></t<>	Load Balancing		Interface Group:							
All Allaw     Max / Pressant       B Allawy     Max / Pressant       Build Charler Structure     Image: Charler Structure       Distails Charler Structure     I	V Psec		Outside-home							
At any Public 2 Processors	Crypto Maps		IKEVZ IPsec Proposals: NSA	/						
	INCEPCIECY									
C India Gara Social  C India Gara  C India	iPancik.cvz Paramears									
			Z Enable Reverse Route Injection							
Part:       Note:       Note: <t< td=""><td></td><td></td><td>Enable Client Services</td><td></td><td></td><td></td></t<>			Enable Client Services							
Note: Ensure the port seed in VMR configuration is not land in other services C incluse thread Sensory C incluse Thread S			Port:							
Carlos Protections Description			Note: Feaure the port used in VPN cor	fouration is not used in other services						
Modula Oragi IA Ukreme Danatori 20000 Respects (Respects (Respects (Respects (Respects (Respect (Re			Enable Perfect Forward Secrecy							
14 Lifenie Duration*; 2880 Securita (Junga 129-347420347) Lifenie Stare 400000 Rayen (J2-2147420347) i # 1594-2 Sectings			Modulus Group:							
Lifetines Duradio 1 2000			14							
2000         Service Target 7(2+14/25347)           Liftere Target         400000           400000         Assen Silvary 10*214/25357)           k ESH-0 Servicy			Lifetime Duration*:							
Lifetine Size 400000 Kayon Sizep (1/21/4836/) × ESH/0 Settops			28800	Seconds (Renge 120-2147483647)						
ESPed Settings			Lifetime Size:							
+ ESH/J Settings			4608000	KDARE (kendle (0,514)463041)						
			+ ESPv3 Settings							
Career OK				Cancel OK						

Again, click OK, save the change and then deploy.

When Client Services is disabled, any new clients will need to have a preconfigured profile instructing them to connect using IPsec as opposed to the default SSL/TLS method. (Even with Client services, we should use such a profile which can then be downloaded automatically vs. manually.)

One can push such a profile to computers outside of the client services feature by using tooling such as Microsoft Windows Active Directory Group Policy Objects (AD GPOs) or any of the many available enterprise endpoint management solutions (Microsoft SCCM, Dell KACE, Intel Landesk, JAMF etc.). If no remote management system is available, then we have the option of manually installing the profiles with the caveat that such an approach does not scale well for an enterprise use case.

To create such a profile, we use the AnyConnect VPN Profile Editor and make the selection for that option:

AnyConnect Profile Ed	ditor - V	'PN					_						
File Help													
VPN		Server List											
Preferences (Part	2)	Profile: Untitled											
Backup Servers													
Certificate Pinning	ng	Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins					
Certificate Enrollm	ent												
Server List	Server	erver List Entry ×											
	Server	Load Balancing Serv	ers SCEP Mobile	Certificate Pinning									
	Pr	imary Server			Connection In	formation							
				1									
		Display Name (required	I) CCIELab - IPsec	1	Primary Proto	IPsec	$\sim$						
	1	FQDN or IP Address		User Group	🗸 ASA gat	eway							
		vpn.ccielab.mrneteng	com /		Auth Me	thod During IKE Nego	EAP-AnyC	onnect 🗸					
		Group LIPI			IKE Iden	itity (IOS gateway or	ly)						
		vpn.ccielab.mrneteng.com											
		Bac	up Servers										
			Host Address			Ad	dd						
						Mov	e Up						
						Move	Down						
						Del	ete						
								>					
				OK	Cancel	]							

The resultant file is saved as an xml file and must be placed in the appropriate directory for the client AnyConnect installation to use during initial connection. For Windows, the default location is C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile. Please refer to the <u>AnyConnect</u>

<u>Secure Mobility Client Administrator Guide</u> for more details and information on other operating systems.

Note that the AnyConnect client software User Interface will need to be restarted if we manually place the profile in the folder for it to parse the available profiles and present them as options on the dropdown list for the user to select when initiating a connection.

## IPsec and ISAKMP Settings

It is also worth noting that we can select from among the available IPsec IKEv2 proposals in the Advanced > IPsec > Crypto Map section:

← → 0	🕽 🔒 🐲 https://http://https//https://https://https://https://https://https//https://https//https//https://https//ht	pe+RA, VPNH, VPN			☆ ♡ =
Firepower Manage Device / VDN / Edit Adve	ement Center Overview Analysis Policies Devices Objects AMP Intelligeno				Deploy Q 🤣 😋 🕲 admin •
CCIELab					Cancel
					Pulicy Association (1)
Connection Profile Access Int	erfaces Advanced			Local Realm: None	Dynamic Access Policy: None
AnyConnect Client Images	Crypto Maps				
Address Assignment Policy	Crypto Maps are auto generated for the interfaces on which IPsec-IKEv2 protocol is enabled.	to this 1990 configuration in 18 course interflow			
Certificate Maps	Transmission of the second second group of which a second		s. 905.		
Group Policies	Interface Group	Edit Covoto Map		 Retz	
LDAP Attribute Mapping	Outside-home	con orpportude	•	true	1
Load Balancing		Interface Group:			
Counter Marea		VEv2 IPres Protocale			
RF Policy		NSA	1		
IPsec/IKEv2 Parameters					
		Enable Reverse Route Injection			
		Enable Client Services			
		Port			
		Note: Ensure the port used in VPN cor	figuration is not used in other services		
		Enable Perfect Forward Secrecy			
		Modulus Group:			
		16			
		28800	Seconds (Renze 120-2147483647)		
		Lifetime Size:			
		4608000	Ritytes (Range 10-2147483647)		
		<ul> <li>FRDv3 Sollings</li> </ul>			
			Connell OK		

We have created such a proposal from the FMC Objects > VPN > IKEv2 IPsec Proposal menu named "NSA" with the ESP hash value of SHA-512 and ESP encryption type of AES-256.

Firepower Manage Objects / Object Manager	ment Center Overview Analysis Policies Devices Objects AMP Intelligence		De
> AAA Server > Access List	IKEv2 IPsec Proposal Plec security association regolitation with ISAKIMP, the peers agree to use a particular proposal to protect a particular de	ia flow. In XEV2 Pase Proposal datest, you can select multiple encryption and Nash Agorithms are allowed. During XEV2 regulations, the pares or	Add IKEv2 IPsec Proposal
Application Filters			
AS Path	Name		
Cipher Suite List	AES-GCM		Q, 🗑
Community List     Distinguished Name	AES-SHA		Q, 🗑
DNS Server Group	DES_SHA-1		Q, 🗑
> External Attributes	NSA		/1
> File List			
Geolocation			
Interface			
Key Chain Network		Edit IKEv2 IPsec Proposal	
> ркі		hand	
Policy List		Name:"	
Port		Description:	
> Prefix List			
Route Map			
> Security Intelligence		Available Algorithms Selected Algorithms	
Sinkhole		ESP Hash AES-GCM-256 Add AES-256	
Time Page		ESP Encryption AES-256	
Time Zone		AES-GCM-192	
Tunnel Zone		AES-192	
URL		AES	
Variable Set		3055	
VLAN Tag		DES	
✓ VPN		AFS-CMAC-256 Y	
AnyConnect File			
Custom Attribute		Cancel Save	
Group Policy			
IKEv1 IPsec Proposal			
IKEv1 Policy			
IKEv2 IPsec Proposal			
IKEv2 Policy			

We also select an Internet Key Exchange (IKE) policy, in this case using the following parameters consistent with NSA guidance:

← → ♂ (	A #2 https://imc.ccielab.mmeteng.com/ddd/	# https://fmc.cirkia.mmterg.com/ddd/Hullpoldidu/unortuuid-000C2916-680D-0x03-0002940699233ypa+8A.VP84.VPM						
Firepower Manage Devices / VPN / Edt Adva	ement Center Overview Analysis	Policies Devices Objects AMP Intelligence			De	rploy 🔍 🞸 🔅 🔞 adr	min *	
CCIELab						Save	ancel	
Connection Profile Access Int	erfaces Advanced				Local Realm: None	Policy Assignment Dynamic Access Policy: M	ts.(1) None	
AnyConnect Client Images Address Assignment Policy Certificate Maps	IKE Policy This list specifies all of the IKEv2 policy objects a	pplicable for this VPN policy when AnyConnect endpoints connect via IPsec-IK	iv2 protocol.				+	
Group Policies	Name	Integrity	Encryption	PRF Hash	DH Group			
Load Balancing	NSA	SHA512	AES-256	SHA512	16		í –	
✓ IPsec Crypto Maps IKE Policy IPsec/IKEv2 Parameters								

### Troubleshooting note

It may be useful to change the default VPN Logging Settings from "Errors" (level 3) to "Informational" (level 6) or even "Debugging" (level 7) when setting this up for the first time.

We do that via the Platform Settings for the FTD device. We can then refer to Devices > Troubleshooting in FMC to see more verbose VPN troubleshooting logs:

$\leftarrow \   \rightarrow \   G$	🛇 🔒 🖻 https://fmc.ccielab.mmeteng.com/ddd/#PFSettings;uuid=000C291E-6B8D-0ed3-0000-004294969536;type=PG.PLATFORM.NgfwPFSettings					
Firepower Manage CISCO Devices / Platform Settin	gement Center Overview Analysis Policies Devices Objects AMP Intelligence					
FTD-platform						
Enter Description						
ARP Inspection	Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog Servers					
Banner	Basic Logging Settings					
DNS	Enable Logging					
External Authentication	Enable Logging on the failover standby unit     Send syslogs in EMBLEM format     Send debug messages as syslogs Memory Size of the Internal Buffer     4096					
Fragment Settings						
HTTP Access						
ICMP Access						
SSH Access						
SMTP Server	(4096-52428800 Bytes)					
SNMP						
SSL	VPN Logging Settings					
Syslog	Enable Logging to FMC					
Timeouts	Logging Level					
Time Synchronization	informational v					

Click OK, save the change and then deploy.

We can then look under Devices > Troubleshooting to observe the log messages:

<form>     Weight Production with Production Wit</form>	€ → C 0 &	## https://fmc	ccielab anneteng conviewents/index.ogi		位				
Bit         Bit <td>Firepower Managemer</td> <td>nt Center</td> <td>Overview Analysis Policies Devices Objects AMP Intelligence</td> <td></td> <td>Deploy Q 🧬</td> <td>🗘 🙆 admin •</td>	Firepower Managemer	nt Center	Overview Analysis Policies Devices Objects AMP Intelligence		Deploy Q 🧬	🗘 🙆 admin •			
Base Control         Biolog           0 control         0 contro         0 contro         0 contro				Bookmark This Page   Report	ting   Dashboard   View Bo	okmarks   Search			
Not a set of the set		2021-16-08 074000 - 2021-10-08 07.4109							
Application	No Search Constraints (Edit Search)					Static			
	The second s								
P         P	Table view of very troubleshooting								
Non-100 (201-200)         None                Reginary               Reginary <t< td=""><td>Time X</td><td>Severity ×</td><td>Message X</td><td>Message Class X</td><td>Username ×</td><td>Device ×</td></t<>	Time X	Severity ×	Message X	Message Class X	Username ×	Device ×			
• 000-000 000000000000000000000	* 2021-10-08 07:40:28	Notice	Local:192.168.0.204:500 Remote:192.168.0.205:59394 Username:Unknown IKEv2 Received a IKE_INIT_SA request	IKE and IPsec	Unknown IKEv2	FTDv-1			
01-10-000000000	· 2021-10-08 07:40:35	Info	AAA user authentication successful : server = 122.31.1.12 : user = adm-man/m	User Authentication	adm-man/in	FTDv-1			
021-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 001200               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 00120               010-030 0012               010-030 0012               010-030 0012               010-030 0012               010-030               010-030	<ul> <li>2021-10-08 07:40:35</li> </ul>	Info	AAA retrieved default group policy (GP-CCIELab) for user = adm-man/in	User Authentication	adm-marvin	FTDv-1			
001-00 0012003               001-00 0012003               001-00 0012003               001-00 001200               001-00 001200               001-00 001200               001-00 001200               001-00 001200               001-00 001200               001-00 001200               001-00 001200               001-00 001200               001-00 001200               PAGesta Augumes	<ul> <li>2021-10-08 07:40:35</li> </ul>	Info	AAA transaction status accept : user = adm-marvin	User Authentication	adm-man/in	FTDv-1			
201-1-00 (21-00)               100 - 000 (21-0)               100 - 000 (21-0)               100 - 000 (21-0)               100 - 000 (21-0)               100 - 000 (21-00)               100 - 000 (21-00)               100 - 000 (21-00)               100 - 000 (21-00)               100 - 000 (21-00)               100 - 000 (21-00)               100 - 000 (21-00)               100 - 000 (21	<ul> <li>2021-10-08 07:40:35</li> </ul>	Info	DAP; User adm-man/n, Addr 192.168.0.205; Connection AnyConnect: The following DAP records were selected for this connection: DftAccessPolicy	dap	adm-marvin	FTDv-1			
Op:1%-00 (201/201/201/201/201/201/201/201/201/201/	<ul> <li>2021-10-08 07:40:35</li> </ul>	Info	Group <gp=ccielab> User <adm=max m=""> IP &lt;192.168.0.205&gt; AnyConnect parent session started.</adm=max></gp=ccielab>	User Authentication		FTDv-1			
201-1-00 (21-20)               No.               PAchase Augment               Pachase                Pachase               Pachase               Pachase               Pachase               Pachase               Pachase               Pachase               Pachase               Pachase               Pachase               Pa	<ul> <li>2021-10-08 07:40:38</li> </ul>	Notice	IPAA: Session=0x00006000, DHCP configured, no viable servers found for tunnel-group 'CCIELab'	IP Address Assignment		FTDv-1			
Operation of the states and and the states	<ul> <li>2021-10-08 07:40:38</li> </ul>	Info	IPAA: Session=0x00006000, Citent assigned 172.31.1.200 from local pool VPN-Pool	IP Address Assignment		FTDy-1			
2011-00 021:03               Note::::::::::::::::::::::::::::::::::::	<ul> <li>2021-10-08 07:40:38</li> </ul>	Info	IPAA: Session*0x0000000, Local pool request succeeded for tunnel-group 'OCIELab'	IP Address Assignment		FTDv-1			
Control Contro Control Control Control Control Control Control Control Control	<ul> <li>2021-10+08 07:40:38</li> </ul>	Notice	IPAA: Session-0x00006000, IPv6 address: no IPv6 address available from local pools	IP Address Assignment		FTDv-1			
2011-00 021403               Note               Note	<ul> <li>2021-10-08 07:40:38</li> </ul>	Notice	IPAA: Session=0x00006000, IPv6 address: no IPv6 address returned	IP Address Assignment		FTDv-1			
2011-00 00 24-030         Notes         Loss 2015-00 00 24-030         Notes         Notes         PTD1           2011-00 00 24-030         Notes         Loss 2015-00 00 24-030         Notes         PTD1           2011-00 00 24-030         Notes         Loss 2015-00 00 24-030         Notes         Add	<ul> <li>2021-10+08 07:40:38</li> </ul>	Notice	Local: 192.168.0.204:4500 Remote: 192.168.0.205:59395 Username:adm-marvin IREv2 SA UP. Reason: New Connection Established	IKE and IPsec	adm-manin IKEv2	FTDy-1			
2021-00 02 14:031         Mod         UND 14 00.04 4605 memory laws 120 160.200 49050 (Levin 00 Montasa) Clerk 40/Montasa Clerk 40/Mont	<ul> <li>2021-10-08 07:40:38</li> </ul>	Notice	Local:192.168.0.204:4500 Remote:192.168.0.205:59395 Usemame:adm-marvin IKEv2 Group:GP-CCIELab IPv4 Address=172.31.1.200 IPv6 address=invalid=addr-2-0.0.0.0 assigned to session	IKE and IPsec		FTDv-1			
2021-10-00 224:038         this         PEC: A cubic net mice access \$4, PEP - 644EE0223 bases 123, PEP - 644EE0223 bases 123, PEP - 148, PEP - 14	<ul> <li>2021-10+08 07:40:38</li> </ul>	Info	Local: 192.168.0.204.4500 Remote: 192.168.0.205.59395 Username:adm-manvin KEv/2 Client OS: Windows Client: AnyConnect 4.10.03104	IKE and IPsec		FTDv-1			
2021-10-02 24/2031         Mode         PBC An indicat members 105 (MPIs 03207540) Users 4 mmm high been reseted.         Bit and Pase:         Bit and Pase:         Bit and Pase:         PITO-1           2021-10-02 24/2031         Mode         MAXA strategies Test 105 (MPIs 03207540) Users 4 mmm high been reseted.         Max A fast reset 105 (MPIs 03207540)         TEO-1           2021-10-02 24/2031         Mode         MAXA strategies Test 105 (MPIs 03207540) Users 4 mmm high been reseted.         Max A fast reset 105 (MPIs 03207540)         Max A fast reset 105 (MPIs 03207540) <t< td=""><td><ul> <li>2021-10-08 07:40:38</li> </ul></td><td>Info</td><td>IPSEC: An outbound remote access SA (SPI= 0x46EED323) between 192.168.0.204 and 192.168.0.205 (user= adm-marvin) has been created.</td><td>IKE and IPsec</td><td>adm-marvin</td><td>FTDv-1</td></t<>	<ul> <li>2021-10-08 07:40:38</li> </ul>	Info	IPSEC: An outbound remote access SA (SPI= 0x46EED323) between 192.168.0.204 and 192.168.0.205 (user= adm-marvin) has been created.	IKE and IPsec	adm-marvin	FTDv-1			
2021-100 (B2 2403)     Notes     UME / Season-0000000, Use-side-market, Assigned P-1723.1.320, Susceeded adding why     Use / Antentication     PTD-1       2021-100 (B2 2403)     MA     Add variable-market, Assigned P-1723.1.320, Susceeded adding why     User / Antentication     adm - market       2021-100 (B2 2403)     MA     Add variable-market, Assigned P-1723.1.320, Susceeded adding why     User / Antentication     adm - market       V     Colorism     1     Bigs/ap/g movs 1-18 of 18 ms	<ul> <li>2021-10-08 07:40:38</li> </ul>	Info	IPSEC: An inbound remote access SA (SPI= 0x39675943) between 192.168.0.204 and 192.168.0.205 (user= adm-manin) has been created.	IKE and IPsec	adm-manin	FTDv-1			
2021-00.001242038             Mode	<ul> <li>2021-10-08 07:40:38</li> </ul>	Notice	UAUTH: Session=0x00006000, User=adm=marvin, Assigned IP=172.31.1.200, Succeeded adding entry.	User Authentication		FTDv-1			
K          Page         1         d1         >         Displaying mousts 1-18 of 18 moust           Vera         Disition	<ul> <li>2021-10-08 07:40:38</li> </ul>	Info	AAA user accounting successful : server = 172.31.1.12 : user = adm-marvin	User Authentication	adm-manin	FTDv-1			
Vee Donte	K ≤ Page 1 of 1 > H Displaying rows 1-18 of 18 rows								
Vew Deste									
	Delete								

## Verification

Once we have successfully connected, we will see the indicator in the AnyConnect User interface:



With the Advanced Window (Gear icon) VPN Statistics Transport Information indicating we are using IKEv2/IPsec:



We can further confirm with a packet capture during session establishment. As is shown below, we see the ISAKMP (<u>Internet Security Association and Key Management Protocol</u>) exchange to setup and authenticate the session:

Wi-Fi (host 192.168.0.204)							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
No.	Time	Source	Destination	Protocol	Length Info		
	1 0.000000	IntelCor_d0:b0:a6	Broadcast	ARP	42 Who has 192.168.0.204? Tell 192.168.0.205		
	2 0.002860	VMware_b9:32:f6	IntelCor_d0:b0:a6	ARP	60 192.168.0.204 is at 00:0c:29:b9:32:f6		
	3 0.002914	192.168.0.205	192.168.0.204	ISAKMP	740 IKE_SA_INIT MID=00 Initiator Request		
	4 0.005295	192.168.0.204	192.168.0.205	ISAKMP	514 IKE_SA_INIT MID=00 Responder Response		
<b>F</b>	5 0.043965	192.168.0.205	192.168.0.204	ISAKMP	622 IKE_AUTH MID=01 Initiator Request (Message fragment 1)		
	6 0.044129	192.168.0.205	192.168.0.204	ISAKMP	515 IKE_AUTH MID=01 Initiator Request (Reassembled + Message fragment 2 - last)		
	7 0.059699	192.168.0.204	192.168.0.205	ISAKMP	594 IKE_AUTH MID=01 Responder Response (Message fragment 1)		
	8 0.059699	192.168.0.204	192.168.0.205	ISAKMP	594 IKE_AUTH MID=01 Responder Response (Message fragment 2)		
	9 0.070246	192.168.0.204	192.168.0.205	ISAKMP	344 IKE_AUTH MID=01 Responder Response (Reassembled + Message fragment 3 - last)		
	10 1.509004	192.168.0.205	192.168.0.204	ISAKMP	622 IKE_AUTH MID=02 Initiator Request (Message fragment 1)		
	11 1.509260	192.168.0.205	192.168.0.204	ISAKMP	605 IKE_AUTH MID=02 Initiator Request (Reassembled + Message fragment 2 - last)		
	12 1.511646	192.168.0.204	192.168.0.205	ISAKMP	594 IKE_AUTH MID=02 Responder Response (Message fragment 1)		
	13 1.511646	192.168.0.204	192.168.0.205	ISAKMP	244 IKE_AUTH MID=02 Responder Response (Reassembled + Message fragment 2 - last)		

...followed by subsequent traffic from the client being all carried via ESP (<u>Encapsulating Security</u> <u>Payload</u>):

-1	WH-FI (host 192.168.0.204)						
File	e Edit View Go	Capture Analyze Stat	tistics Telephony Wireles	s Tools Help			
	🔳 🔬 💿 📕 🛅	🖹 🚺 ۹ 🗢 🖻	🕹 📃 🔳 🍳 Q	Q. 👖			
	Apply a display filter $<$	Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info		
	49 9.706382	192.168.0.204	192.168.0.205	ISAKMP	281 IKE_AUTH MID=05 Responder Response (Reassembled + Message fragment 15 - last)		
	50 12.730140	192.168.0.205	192.168.0.204	ESP	178 ESP (SPI=0x39e75943)		
	51 12.739380	192.168.0.205	192.168.0.204	ESP	242 ESP (SPI=0x39e75943)		
	52 12.739589	192.168.0.205	192.168.0.204	ESP	162 ESP (SPI=0x39e75943)		
	53 12.739743	192.168.0.205	192.168.0.204	ESP	146 ESP (SPI=0x39e75943)		
	54 12.739833	192.168.0.205	192.168.0.204	ESP	274 ESP (SPI=0x39e75943)		
	55 12.739914	192.168.0.205	192.168.0.204	ESP	1218 ESP (SPI=0x39e75943)		
	56 12.740013	192.168.0.205	192.168.0.204	ESP	1218 ESP (SPI=0x39e75943)		
	57 12.740082	192.168.0.205	192.168.0.204	ESP	258 ESP (SPI=0x39e75943)		
	58 12.740174	192.168.0.205	192.168.0.204	ESP	258 ESP (SPI=0x39e75943)		
	59 12.740244	192.168.0.205	192.168.0.204	ESP	258 ESP (SPI=0x39e75943)		
	60 12.740315	192.168.0.205	192.168.0.204	ESP	1218 ESP (SPI=0x39e75943)		
	61 12.740389	192.168.0.205	192.168.0.204	ESP	1218 ESP (SPI=0x39e75943)		
	62 12.740457	192.168.0.205	192.168.0.204	ESP	258 ESP (SPI=0x39e75943)		
	63 12.740526	192.168.0.205	192.168.0.204	ESP	210 ESP (SPI=0x39e75943)		

# Conclusion

We demonstrated the integration steps to configure Cisco's Secure Firewall, Firewall Management Center and AnyConnect Secure Mobility client products to work together to deliver a Remote Access Virtual Private Network (RA VPN) solution.

From the verification section, we can see that, by following the guidance presented in this paper, we establish a connection that exclusively uses IPsec IKEv2. At no point is SSL/TLS publicly exposed, either in the transport / data plane or control plane.

As noted, some customers may elect to continue to use the Client services option in order continue to have the features of AnyConnect and profile updates via the FTD device, especially if they don't have an alternative client management system in place.

The decision to do so is a local one; but it does make the effort of changing the transport protocol less effective as any SSL/TLS vulnerabilities will then continue to be exposed on the VPN headend.

Customers electing to do so should strongly consider implementing other compensating controls to ensure that any such vulnerabilities are mitigated via other means (version upgrades, configuration reviews etc.).

## References

NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs

AnyConnect Ordering Guide

Configuring IPsec Virtual Private Networks (NSA)

Suite B Cryptography

Cisco Secure Firewall product page

Firewall Management Center product page

AnyConnect Secure Mobility Client product page

Remote Access VPNs for Firepower Threat Defense

AnyConnect Secure Mobility Client Administrator Guide

Internet Security Association and Key Management Protocol

**Encapsulating Security Payload**