

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

Marvin Rhoads

6-6-2024

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 1.2

- Updated section re client services

Abstract / Introduction

There has been recent guidance¹ 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.

We will use the following Cisco products:

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

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-asa-software/213246-asa-ikev2-ra-vpn-with-windows-7-or-andro.html>

<https://community.cisco.com/t5/security-documents/asa-anyconnect-ikev2-configuration-example/ta-p/3117462>

¹ [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" next generation encryption.

While Suite B is recommended for highest security when using IPsec IKEv2, it does require AnyConnect Apex licensing³. 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 NSA⁴.

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 on-premises 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.

² [Suite B Cryptography](#)

³ [AnyConnect Ordering Guide](#)

⁴ [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 (<https://software.cisco.com>) 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, [Cisco Security Community documents](#) 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 Outside-zone set to support the incoming connections:

The screenshot shows the Firepower Management Center interface for configuring a Remote Access VPN named 'RA_VPN'. The 'Access Interfaces' tab is selected, displaying a table of interfaces and their supported protocols. Below the table, there are sections for 'Access Settings' and 'SSL Settings'.

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2	
Outside-Zone		+	+	-	

Access Settings

- Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:*

DTLS Port Number:*

SSL Global Identity Certificate: +

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:

The screenshot shows a configuration window titled "Edit Access Interface". The "Access Interface" is set to "Outside-home". Under the "Protocol:" section, the following options are visible:

- Enable IPsec-IKEv2
- Enable SSL
- Enable Datagram Transport Layer Security
- Configure interface specific identity certificate

A note below the options states: "The 'SSL Global identity certificate' will be used if no interface identity certificate is configured". At the bottom right of the window are "Cancel" and "OK" buttons.

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.

WHITEPAPER - CONFIGURING IPSEC IKEV2 REMOTE ACCESS VPN WITH CISCO SECURE FIREWALL

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 socket

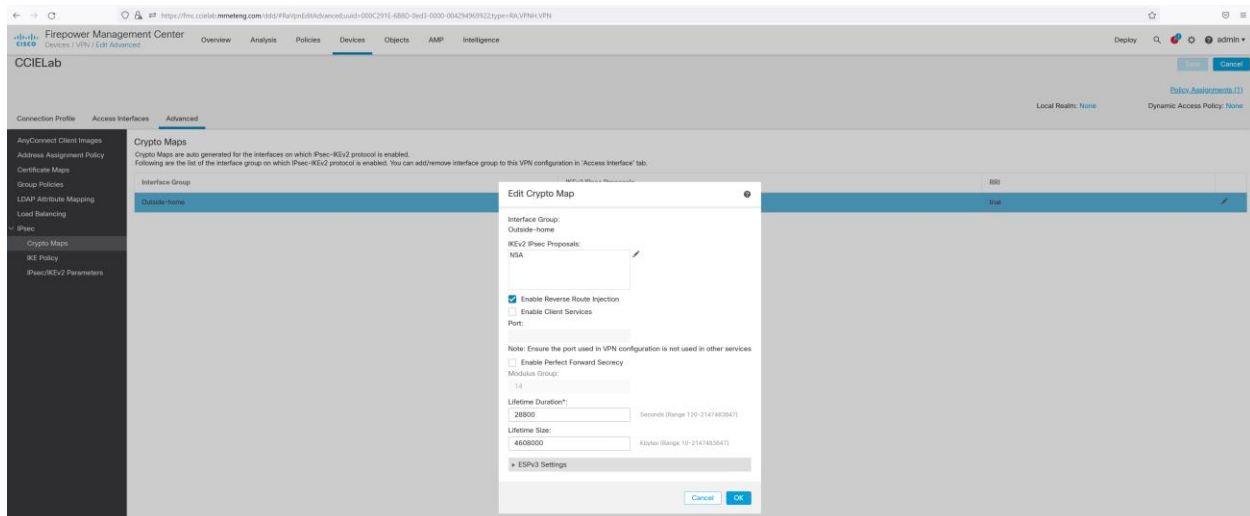
Protocol  Socket      State      Local Address      Foreign Address
SSL       00008bd8    LISTEN     192.168.0.204:443  0.0.0.0:*
```

...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 socket

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":



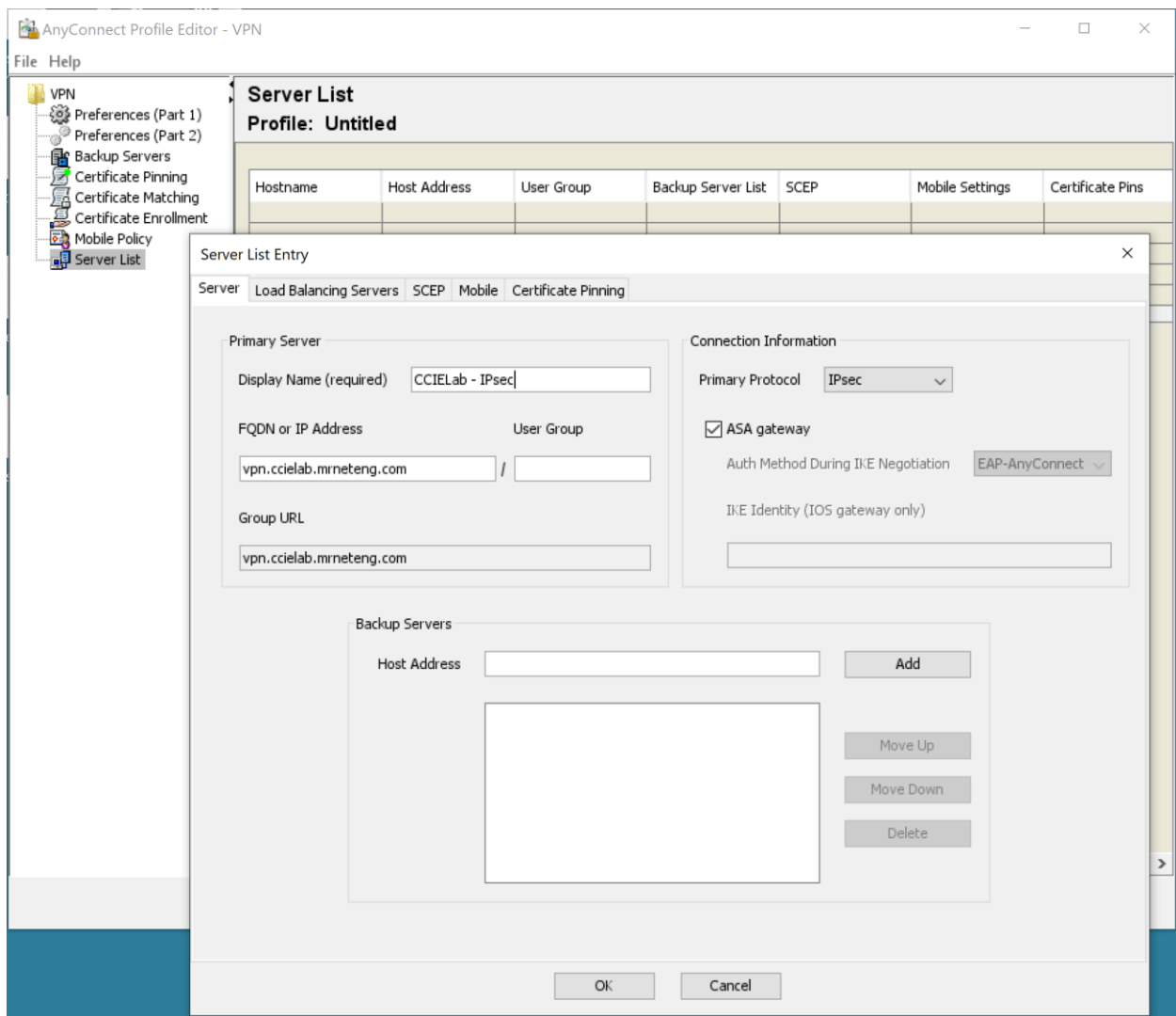
Again, click OK, save the change and then deploy.

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.)

If you wish to re-enable automatic download of the profile to update it on your clients, you must enable BOTH SSL/TLS transport and Client Services. After all clients are updated, they can be disabled once again.

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:

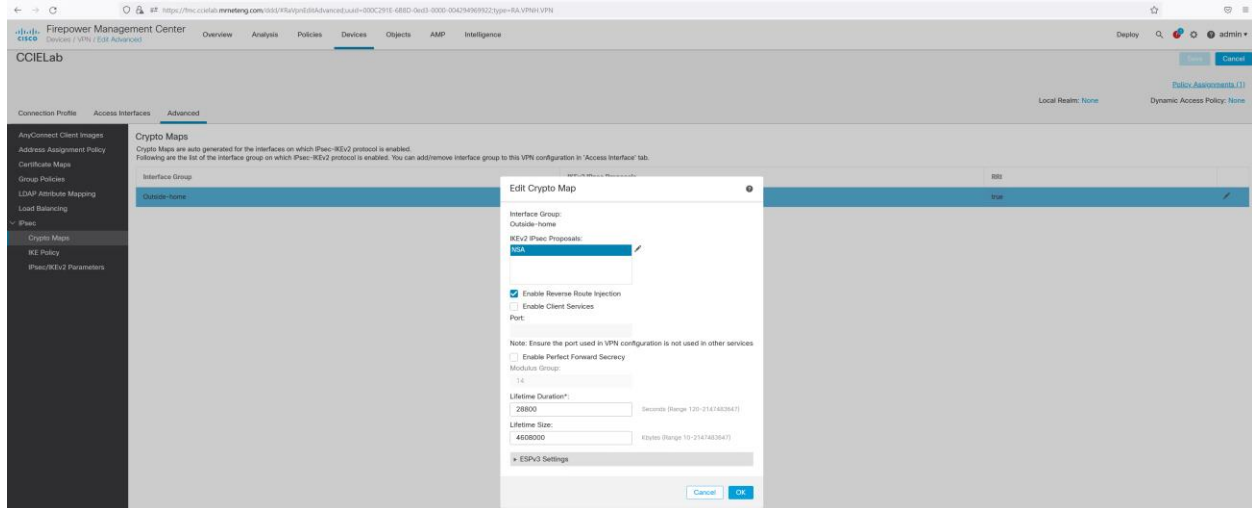


The resultant file is saved as an xml file and must be placed in the appropriate directory for the client AnyConnect installation to use during initial connection. For Windows, the default location is C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile. Please refer to the [AnyConnect Secure Mobility Client Administrator Guide](#) for more details and information on other operating systems.

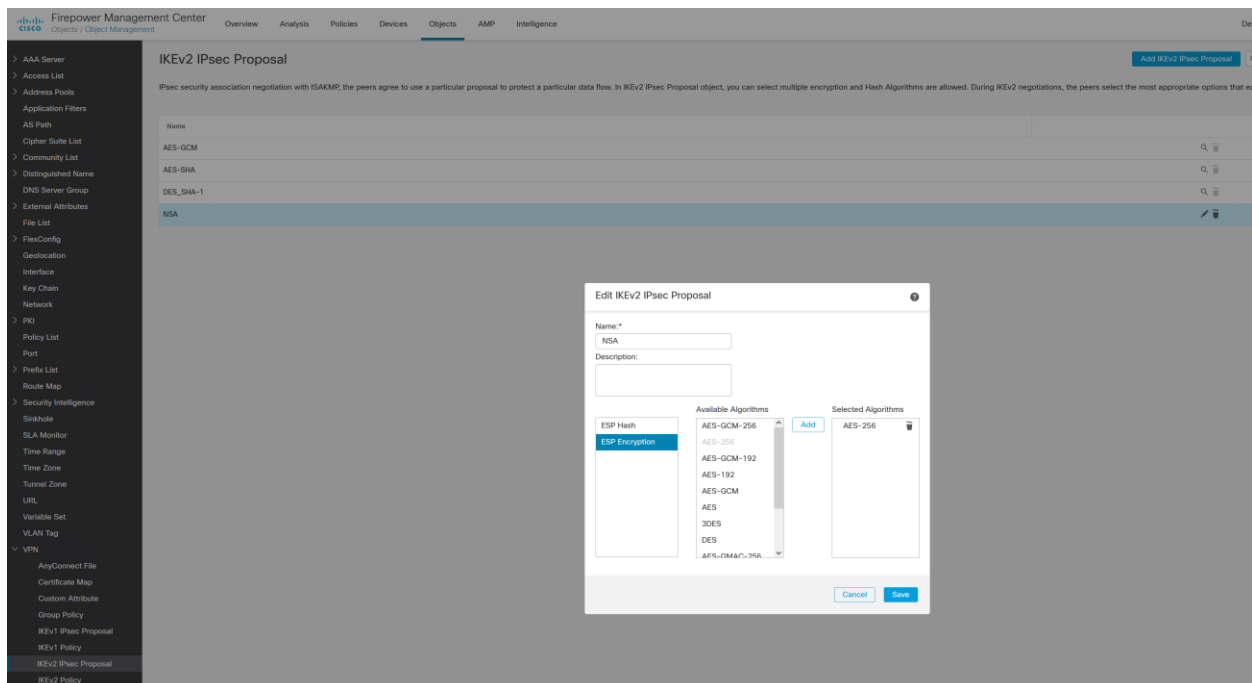
Note that the AnyConnect client software User Interface will need to be restarted if we manually place the profile in the folder for it to parse the available profiles and present them as options on the dropdown list for the user to select when initiating a connection.

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:

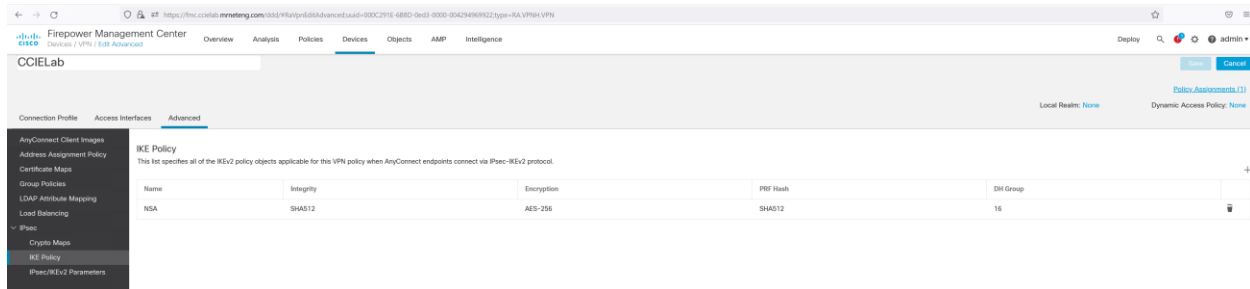


We have created such a proposal from the **FMC Objects > VPN > IKEv2 IPsec Proposal** menu named “NSA” with the ESP hash value of SHA-512 and ESP encryption type of AES-256.



WHITEPAPER - CONFIGURING IPSEC IKEV2 REMOTE ACCESS VPN WITH CISCO SECURE FIREWALL

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



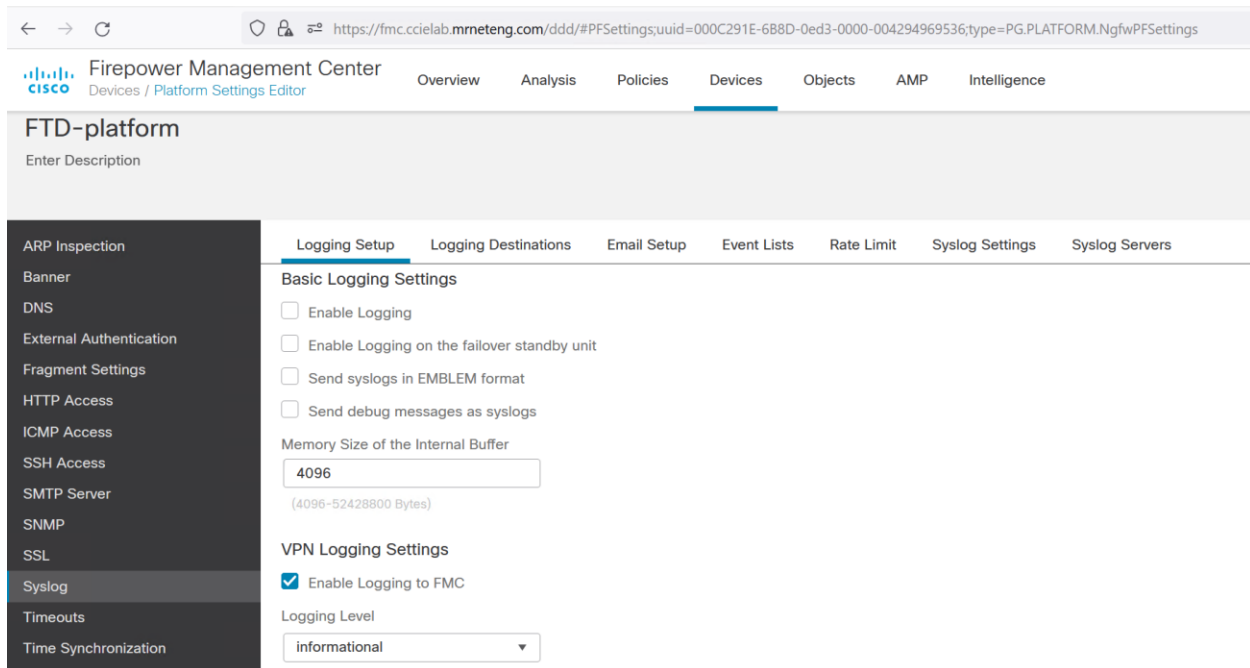
The screenshot shows the Cisco Firepower Management Center interface. The left sidebar contains a navigation menu with options like 'AnyConnect Client Images', 'Address Assignment Policy', 'Certificate Maps', 'Group Policies', 'LDAP Attribute Mapping', 'Load Balancing', 'IPsec', 'Crypto Maps', 'IKE Policy', and 'IPsec/IKEv2 Parameters'. The 'IKE Policy' option is selected. The main content area displays the 'IKE Policy' configuration page. A table lists the IKE policy objects for the VPN policy. The table has columns for Name, Integrity, Encryption, PRF Hash, and DH Group. The row shows 'NSA' with Integrity 'SHA512', Encryption 'AES-256', PRF Hash 'SHA512', and DH Group '15'.

Name	Integrity	Encryption	PRF Hash	DH Group
NSA	SHA512	AES-256	SHA512	15

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:



The screenshot shows the Cisco Firepower Management Center interface for the 'FTD-platform' configuration. The left sidebar contains a navigation menu with options like 'ARP Inspection', 'Banner', 'DNS', 'External Authentication', 'Fragment Settings', 'HTTP Access', 'ICMP Access', 'SSH Access', 'SMTP Server', 'SNMP', 'SSL', 'Syslog', 'Timeouts', and 'Time Synchronization'. The 'Syslog' option is selected. The main content area displays the 'Syslog' configuration page. The 'Logging Setup' tab is active. Under 'Basic Logging Settings', there are checkboxes for 'Enable Logging', 'Enable Logging on the failover standby unit', 'Send syslogs in EMBLEM format', and 'Send debug messages as syslogs'. The 'Memory Size of the Internal Buffer' is set to 4096. Under 'VPN Logging Settings', the checkbox for 'Enable Logging to FMC' is checked. The 'Logging Level' is set to 'informational'.

Click OK, save the change and then deploy.

WHITEPAPER - CONFIGURING IPSEC IKEV2 REMOTE ACCESS VPN WITH CISCO SECURE FIREWALL

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

The screenshot shows the Firepower Management Center interface. The breadcrumb navigation is 'Devices > Troubleshooting'. The page title is 'Table View of VPN Troubleshooting'. The table displays log messages with columns for Time, Severity, Message, Message Class, Username, and Device. The logs show a sequence of events for an IKEv2 session, including authentication, group policy retrieval, DAP records selection, IPsec SA creation, and session establishment.

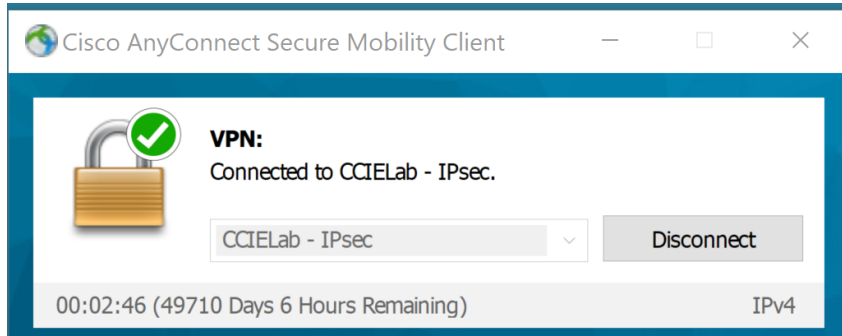
Time	Severity	Message	Message Class	Username	Device
2021-10-08 07:40:28	Notice	Local:192.168.0.204:4500 Remote:192.168.0.205:59394 Username:Unknown IKEv2 Received a IKE_INIT_SA request	IKE and IPsec	Unknown IKEv2	FTDv-1
2021-10-08 07:40:35	Info	AAA user authentication successful: server = 172.31.1.12 user = adm-marin	User Authentication	adm-marin	FTDv-1
2021-10-08 07:40:35	Info	AAA retrieved default group policy (GP-CCIElab) for user = adm-marin	User Authentication	adm-marin	FTDv-1
2021-10-08 07:40:35	Info	AAA transaction status accept: user = adm-marin	User Authentication	adm-marin	FTDv-1
2021-10-08 07:40:35	Info	DAP: User adm-marin, Addr 192.168.0.205, Connection AnyConnect: The following DAP records were selected for this connection: DftAccessPolicy	dap	adm-marin	FTDv-1
2021-10-08 07:40:35	Info	Group:GP-CCIElab-User adm-marin IP = 192.168.0.205: AnyConnect parent session started.	User Authentication	adm-marin	FTDv-1
2021-10-08 07:40:38	Notice	IPAA: Session=0x00006000: DHCP configured, no stable servers found for tunnel-group 'CCIElab'	IP Address Assignment	adm-marin	FTDv-1
2021-10-08 07:40:38	Info	IPAA: Session=0x00006000: Client assigned 172.31.1.205 from local pool VPN-Pool	IP Address Assignment	adm-marin	FTDv-1
2021-10-08 07:40:38	Info	IPAA: Session=0x00006000: Local pool request succeeded for tunnel-group 'CCIElab'	IP Address Assignment	adm-marin	FTDv-1
2021-10-08 07:40:38	Notice	IPAA: Session=0x00006000: IPv6 address: no IPv6 address available from local pools	IP Address Assignment	adm-marin	FTDv-1
2021-10-08 07:40:38	Notice	IPAA: Session=0x00006000: IPv6 address: no IPv6 address returned	IP Address Assignment	adm-marin	FTDv-1
2021-10-08 07:40:38	Notice	Local:192.168.0.204:4500 Remote:192.168.0.205:59395 Username:adm-marin IKEv2 SA UP Reason: New Connection Established	IKE and IPsec	adm-marin IKEv2	FTDv-1
2021-10-08 07:40:38	Notice	Local:192.168.0.204:4500 Remote:192.168.0.205:59395 Username:adm-marin IKEv2 Group:GP-CCIElab IPv4 Address:172.31.1.200 IPv6 address:invalid-addr-2-0.0.0 assigned to session	IKE and IPsec	adm-marin	FTDv-1
2021-10-08 07:40:38	Info	Local:192.168.0.204:4500 Remote:192.168.0.205:59395 Username:adm-marin IKEv2 Client OS: Windows Client. AnyConnect 4.10.03104	IKE and IPsec	adm-marin	FTDv-1
2021-10-08 07:40:38	Info	IPSEC: An outbound remote access SA (SPI= 0x460223) between 192.168.0.204 and 192.168.0.205 (user= adm-marin) has been created.	IKE and IPsec	adm-marin	FTDv-1
2021-10-08 07:40:38	Info	IPSEC: An inbound remote access SA (SPI= 0x3E75843) between 192.168.0.204 and 192.168.0.205 (user= adm-marin) has been created.	IKE and IPsec	adm-marin	FTDv-1
2021-10-08 07:40:38	Notice	UAUTH: Session=0x00006000: User=adm-marin. Assigned IP=172.31.1.205. Succeeded adding entry	User Authentication	adm-marin	FTDv-1
2021-10-08 07:40:38	Info	AAA user accounting successful: server = 172.31.1.12: user = adm-marin	User Authentication	adm-marin	FTDv-1

Page 1 of 1 | Displaying rows 1-18 of 18 rows

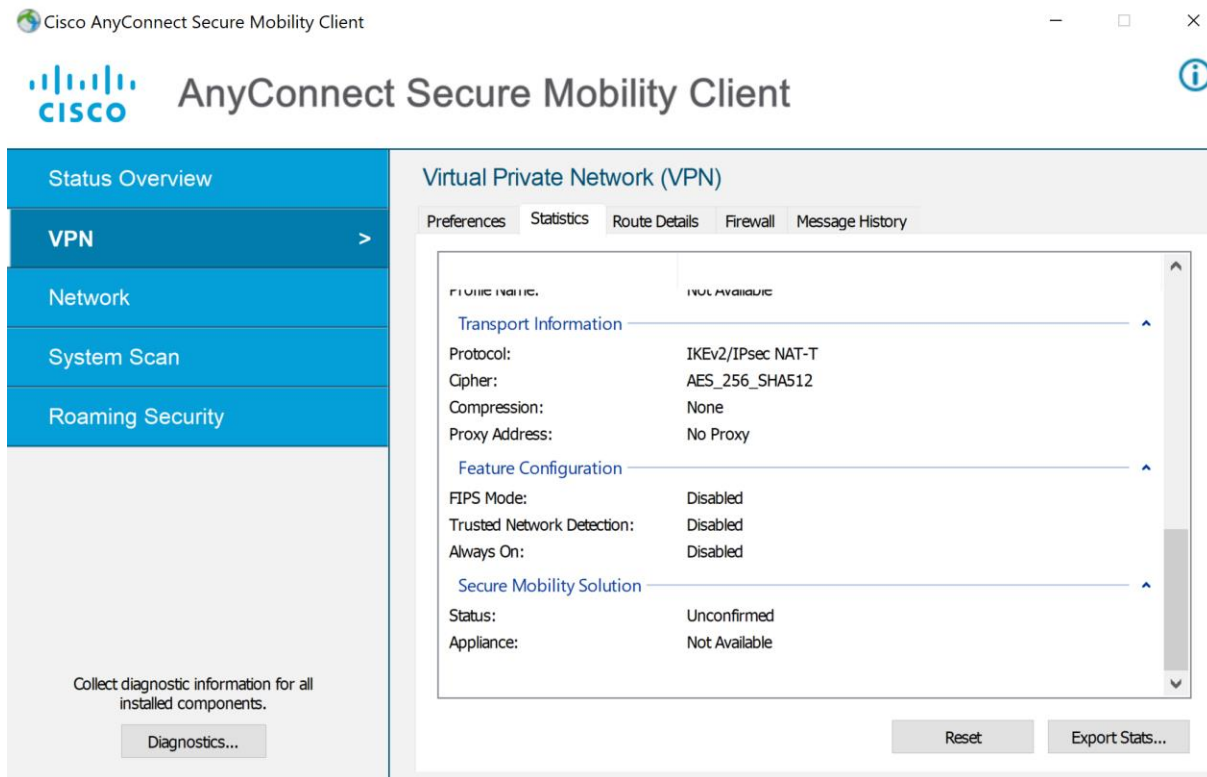
View Delete
View All Delete All

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:



WHITEPAPER - CONFIGURING IPSEC IKEV2 REMOTE ACCESS VPN WITH CISCO SECURE FIREWALL

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

Wireshark packet capture showing ISAKMP exchange. The interface is 'Wi-Fi (host 192.168.0.204)'. The display filter is 'Apply a display filter ... <Ctrl-/>'. The packet list shows:

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	Vhware_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
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 ([Encapsulating Security Payload](#)):

Wireshark packet capture showing subsequent traffic carried via ESP. The interface is 'Wi-Fi (host 192.168.0.204)'. The display filter is 'Apply a display filter ... <Ctrl-/>'. The packet list shows:

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](#)