Managing Virtual Private Network in CDO

A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet.

This section applies to Remote Access and Site-to-site VPNs on Adaptive Security Appliances (ASA) device. It also describes the SSL standards that are used to build and remote access VPN connections on ASA.

CDO supports the following types of VPN connections:

Introduction to Site-to-Site Virtual Private Network

A site-to-site VPN tunnel connects networks in different geographic locations. You can create site-to-site IPsec connections between managed devices and between managed devices and other Cisco or third-party peers that comply with all relevant standards. These peers can have any mix of inside and outside IPv4 and IPv6 addresses. Site-to-site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and Internet Key Exchange version 2 (IKEv2). After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

VPN Topology

To create a new site-to-site VPN topology you must provide a unique name, specify a topology type, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both and authentication method. Once configured, you deploy the topology to ASA.

IPsec and IKE Protocols

In CDO, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

Authentication VPN Tunnels

For authentication of VPN connections, configure a pre-shared key in the topology on each device. Pre-shared keys allow a secret key, used during the IKE authentication phase, to be shared between two peers.

VPN Encryption Domain

There are two methods to define the VPN's encryption domain: route-based or policy-based traffic selectors.

- **Policy-Based**: The encryption domain is set to allow any traffic which enters the IPSec tunnel. IPSec Local and remote traffic selectors are set to 0.0.0.0. This means that any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet. ASA supports policy-based VPN with crypto maps.
- **Route-Based**: The encryption domain is set to encrypt only specific IP ranges for both source and destination. It creates a virtual IPsec interface, and whatever traffic enters that interface is encrypted and decrypted. ASA supports route-based VPN with the use of Virtual Tunnel Interfaces (VTIs).

About Extranet Devices

You can add non-Cisco or unmanaged Cisco devices to a VPN topology as "Extranet" devices with either static or dynamic IP addresses.

- Non-Cisco Device: You can’t use CDO to create and deploy configurations to non-Cisco devices.
- Unmanaged Cisco Device: Cisco device not managed by your organization, such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.

Related Information:

- ASA Site-to-Site VPN Configuration, on page 2
- Monitor ASA Site-to-Site Virtual Private Networks

ASA Site-to-Site VPN Configuration

Cisco Defense Orchestrator (CDO) supports these aspects of site-to-site VPN functionality on Adaptive Security Appliance (ASA) devices:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Automatic or manual pre-shared keys for authentication.
- IPv4 and IPv6. All combinations of inside and outside are supported.
- IPsec IKEv2 site-to-site VPN topologies provide configuration settings to comply with Security Certifications.
- Static and dynamic interfaces.
- Support the static or dynamic IP address for the extranet device as an endpoint.

Configure Site-to-Site VPN Connections with Dynamically Addressed Peers

CDO allows you to create a site-to-site VPN connection between peers when one of the peers' VPN interface IP address is not known or when the interface obtains its address from a DHCP server. Any dynamic peer whose preshared key, IKE settings, and IPsec configurations match with another peer can establish a site-to-site VPN connection.

Consider two peers, A and B. The static peer is a device whose IP address of its VPN interface is fixed and a dynamic peer is a device whose IP address of the VPN interface is not known or has a temporary IP address.

The following use cases describe different scenarios for establishing a secure site-to-site VPN connection with dynamically-addressed peers:

- A is a static peer, and B is a dynamic peer or conversely.
- A is a static peer, and B is a dynamic peer with a resolved IP address from the DHCP server or conversely.
- A is a dynamic peer, and B is an extranet device with a static or dynamic IP address.
- A is a dynamic peer with a resolved IP address from the DHCP server, and B is an Extranet device with a static or dynamic IP address.

Note If the IP address of the interface is changed by using a local manager like Adaptive Security Device Manager (ASDM), the **Configuration Status** of that peer in CDO shows "Conflict Detected". When you resolve this out-of-band change, the **Configuration Status** of the other peer changes to the "Not Synced" state. You must deploy the CDO configuration to the device which is in "Not Synced" state.

Typically, the dynamic peer must be the one that initiates the connection as the other peer would not know the IP address of the dynamic peer. When the remote peer attempts to establish the connection, the other peer validates the connection using the preshared key, IKE settings, and IPsec configurations.

Because the VPN connection is established only after the remote peer initiates the connection, any outbound traffic that matches access control rules that allow traffic in the VPN tunnel will be dropped until that connection is established. This ensures that data does not leave your network without the appropriate encryption and VPN protection.

Note A site-to-site VPN connection cannot be configured in the following scenario:

If a device has more than one dynamic peer connection.

- Consider three devices A, B, and C.
- Configure site-to-site VPN connection between A (static peer) and B (dynamic peer).
- Configure site-to-site VPN connection between A and C (dynamic peer) by creating an Extranet device. Assign the static VPN interface IP address of A to the Extranet device and establish a connection with C.

ASA Site-to-Site VPN Guidelines and Limitations

- CDO does not support a crypto-acl to design the interesting traffic for S2S VPN. It only supports protected networks.
- Whenever IKE ports 500/4500 are in use or when there are some PAT translations that are active, the site-to-site VPN cannot be configured on the same ports as it fails to start the service on those ports.
- Transport mode is not supported only tunnel mode. IPsec tunnel mode encrypts the entire original IP datagram which becomes the payload in a new IP packet. Use tunnel mode when the firewall is protecting

traffic to and from hosts positioned behind a firewall. Tunnel mode is the normal way regular IPsec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.

- For this release, only PTP topology is supported, containing one or more VPN tunnels. Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.

Guidelines for Virtual Tunnel Interfaces

- VTIs are only configurable in IPsec mode. To terminate GRE tunnels on an ASA is unsupported.
- You can use dynamic or static routes for traffic using the tunnel interface.
- The MTU for VTIs is automatically set, according to the underlying physical interface. However, if you change the physical interface MTU after the VTI is enabled, you must disable and reenable the VTI to use the new MTU setting.
- If Network Address Translation has to be applied, the IKE and ESP packets will be encapsulated in the UDP header.
- IKE and IPsec security associations will be re-keyed continuously regardless of data traffic in the tunnel. This ensures that VTI tunnels are always up.
- Tunnel group name must match what the peer will send as its IKEv1 or IKEv2 identity.
- For IKEv1 in LAN-to-LAN tunnel groups, you can use names which are not IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.
- VTI and crypto map configurations can co-exist on the same physical interface, provided the peer address configured in the crypto map and the tunnel destination for the VTI are different.
- By default, all traffic through VTI is encrypted.
- By default, the security level for VTI interfaces is 0.
- Access list can be applied on a VTI interface to control traffic through VTI.
- Only BGP is supported over VTI.
- If ASA is terminating IOS IKEv2 VTI clients, disable the config-exchange request on IOS, because ASA cannot retrieve the mode-CFG attributes for this L2L session initiated by an IOS VTI client.
- IPv6 is not supported.

Related Information:

- Create an ASA Site-to-Site VPN Tunnel, on page 7
- Encryption and Hash Algorithms Used in VPN
- Exempt Remote Access VPN Traffic from NAT, on page 58

Encryption and Hash Algorithms Used in VPN

Because a VPN tunnel typically traverses a public network, most likely the Internet, you need to encrypt the connection to protect the traffic. You define the encryption and other security techniques to apply using IKE policies and IPsec proposals.

If your device license allows you to apply strong encryption, there is a wide range of encryption and hash algorithms, and Diffie-Hellman groups, from which to choose. However, as a general rule, the stronger the encryption that you apply to the tunnel, the worse the system performance. Find a balance between security and performance that provides sufficient protection without compromising efficiency.

We cannot provide specific guidance on which options to choose. If you operate within a larger corporation or other organization, there might already be defined standards that you need to meet. If not, take the time to research the options.

The following topics explain the available options:

Deciding Which Encryption Algorithm to Use

When determining which encryption algorithms to use for the IKE policy or IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN.

For IKEv2, you can configure multiple encryption algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

For IPsec proposals, the algorithm is used by the Encapsulating Security Protocol (ESP), which provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP.

If your device license qualifies for strong encryption, you can choose from the following encryption algorithms. If you are not qualified for strong encryption, you can select DES only.

- AES-GCM - (IKEv2 only.) Advanced Encryption Standard in Galois/Counter Mode is a block cipher mode of operation providing confidentiality and data-origin authentication and provides greater security than AES. AES-GCM offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance. GCM is a mode of AES that is required to support NSA Suite B. NSA Suite B is a set of cryptographic algorithms that devices must support to meet federal standards for cryptographic strength.
- AES-GMAC - (IKEv2 IPsec proposals only.) Advanced Encryption Standard Galois Message Authentication Code is a block cipher mode of operation providing only data-origin authentication. It is a variant of AES-GCM that allows data authentication without encrypting the data. AES-GMAC offers three different key strengths: 128-, 192-, and 256-bit keys.
- AES - Advanced Encryption Standard is a symmetric cipher algorithm that provides greater security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance.
- DES - Data Encryption Standard, which encrypts using 56-bit keys, is a symmetric secret-key block algorithm. If your license account does not meet the requirements for export controls, this is your only option. It is faster than 3DES and uses fewer system resources, but it is also less secure. If you do not need strong data confidentiality, and if system resources or speed is a concern, choose DES.
- 3DES - Triple DES, which encrypts three times using 56-bit keys, is more secure than DES because it processes each block of data three times with a different key. However, it uses more system resources and is slower than DES.
- NULL - A null encryption algorithm provides authentication without encryption. This is typically used for testing purposes only.

Deciding Which Hash Algorithms to Use

In IKE policies, the hash algorithm creates a message digest, which is used to ensure message integrity. In IKEv2, the hash algorithm is separated into two options, one for the integrity algorithm, and one for the pseudo-random function (PRF).

In IPsec proposals, the hash algorithm is used by the Encapsulating Security Protocol (ESP) for authentication. In IKEv2 IPsec Proposals, this is called the integrity hash. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP-, and there is also an -HMAC suffix (which stands for "hash method authentication code").

For IKEv2, you can configure multiple hash algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

You can choose from the following hash algorithms:

- SHA (Secure Hash Algorithm) - Standard SHA (SHA-1) produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. However, it is also more resource-intensive than MD5. For implementations that require the highest level of security, use the SHA hash algorithm.
- The following SHA-2 options, which are even more secure, are available for IKEv2 configurations. Choose one of these if you want to implement the NSA Suite B cryptography specification.
  - SHA-256 - Specifies the Secure Hash Algorithm SHA-2 with the 256-bit digest.
  - SHA-384 - Specifies the Secure Hash Algorithm SHA-2 with the 384-bit digest.
  - SHA-512 - Specifies the Secure Hash Algorithm SHA-2 with the 512-bit digest.
- MD5 (Message Digest 5) - Produces a 128-bit digest. MD5 uses less processing time for overall faster performance than SHA, but it is considered to be weaker than SHA.
- Null or None (NULL, ESP-NONE) - (IPsec Proposals only.) A null Hash Algorithm; this is typically used for testing purposes only. However, you should choose the null integrity algorithm if you select one of the AES-GCM/GMAC options as the encryption algorithm. Even if you choose a non-null option, the integrity hash is ignored for these encryption standards.

Deciding Which Diffie-Hellman Modulus Group to Use

You can use the following Diffie-Hellman key derivation algorithms to generate IPsec security association (SA) keys. Each group has different size modules. A larger modulus provides higher security but requires more processing time. You must have a matching modulus group on both peers.

If you select AES encryption, to support the large key sizes required by AES, you should use Diffie-Hellman (DH) Group 5 or higher. IKEv1 policies do not support all of the groups listed below.

To implement the NSA Suite B cryptography specification, use IKEv2 and select one of the elliptic curve Diffie-Hellman (ECDH) options: 19, 20, or 21. Elliptic curve options and groups that use 2048-bit modulus are less exposed to attacks such as Logjam.

For IKEv2, you can configure multiple groups. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

- 2 - Diffie-Hellman Group 2: 1024-bit modular exponential (MODP) group. This option is no longer considered good protection.
- 5 - Diffie-Hellman Group 5: 1536-bit MODP group. Formerly considered good protection for 128-bit keys, this option is no longer considered good protection.

- 14 - Diffie-Hellman Group 14: 2048-bit modular exponential (MODP) group. Considered good protection for 192-bit keys.
- 19 - Diffie-Hellman Group 19: National Institute of Standards and Technology (NIST) 256-bit elliptic curve modulo a prime (ECP) group.
- 20 - Diffie-Hellman Group 20: NIST 384-bit ECP group.
- 21 - Diffie-Hellman Group 21: NIST 521-bit ECP group.
- 24 - Diffie-Hellman Group 24: 2048-bit MODP group with 256-bit prime order subgroup. This option is no longer recommended.

Deciding Which Authentication Method to Use

You can use the following methods to authenticate the peers in a site-to-site VPN connection..

Preshared Keys

Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase. For IKEv1, you must configure the same preshared key on each peer. For IKEv2, you can configure unique keys on each peer.

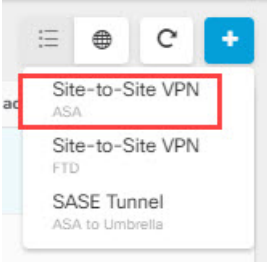
Preshared keys do not scale well compared to certificates. If you need to configure a large number of site-to-site VPN connections, use the certificate method instead of the preshared key method.

Create an ASA Site-to-Site VPN Tunnel

Use the following procedure to create a site-to-site VPN tunnel between two ASAs or an ASA with an Extranet device:

Step 1 In the navigation pane, choose **VPN** > **ASA/FDM Site-to-Site VPN**.

Step 2 Click the blue plus on the top right corner and click **Site-to-Site VPN** with ASA label.



Step 3 In the **Configuration Name** field, enter a name for the site-to-site VPN configuration you create.

Step 4 Select one of the options to create a new **Policy Based** or **Route Based** site-to-site VPN.

Step 5 In the **Peer Devices** section, do the following:

a) **Peer 1**: Select an ASA device and then click **Select**.

b) **Peer 2**: Select the other ASA device and then click **Select**.

Extranet: If you want to choose an extranet device in Peer 2, click the Extranet slider to enable it.

Select **Static**, and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for the static interface or **DHCP Assigned** for the dynamic interface.

c) Choose the **VPN Access Interface** for the endpoint devices.

d) (Applicable to Route Based VPN) Choose the **LAN Interfaces** that controls the LAN subnet. You can select multiple interfaces.

The networks attached to the selected LAN interfaces will be added to the routing policy access list. The traffic matching the routing policy access list will be encrypted/decrypted by the VPN tunnel.

e) Click **Add Network** to add the **Protected Networks** for the participating devices. A protected network defines the networks that are protected by this VPN endpoint.

f) (Optional and applicable to Policy Based) Select **NAT Exempt** to exempt the VPN traffic from NAT policies on the local VPN access interface. It must be configured manually for individual peers. If you do not want NAT rules to apply to the local network, select the interface that hosts the local network. This option works only if the local network resides behind a single routed interface (not a bridge group member). If the local network is behind more than one routed interface or one or more bridge group members, you must manually create the NAT exempt rules. For information on manually creating the required rules, see Exempt ASA Site-to-Site VPN Traffic from NAT.

g) Click **Next**.

Step 6 (Applicable to Route Based) In the **Tunnel Details**, the **VTI Address** fields are automatically filled once the peer devices are configured in the previous step. If necessary, you can manually enter an IP address that will be used as the new VTI.

Step 7 In the **IKE Settings** section, choose the IKE versions to use during Internet Key Exchange (IKE) negotiations and specify the privacy configurations: For more information on the IKE policies, see About Global IKE Policies.

Based on the configuration made by the user, CDO suggests the IKE settings. You can either continue with the recommended IKE configuration settings or define a new one.

Note IKE policies are global to a device and apply to all VPN tunnels associated with it. Therefore, adding or deleting policies affect all VPN tunnels in which this device is participating.

a) Select either or both IKE versions as appropriate.

By default, **IKEV Version 2** is enabled.

Note Enabling both IKE versions is not allowed for route-based VPN.

b) Click **Add IKEv2 Policy** and select the IKEv2 policies

Note Click **Create New IKEv2 Policy** to create new IKEv2 policies. For more information about creating new IKEv2 policies, see Managing IKEv2 Policies. To delete an existing IKEv2 Policy, hover-over the selected policy and click the x icon.

c) Enter the **Pre-Shared Key** for the participating devices. Preshared keys are secret key strings configured on each peer in the connection. IKE uses these keys during the authentication phase.

(IKEv2) **Peer 1 Pre-shared Key**, **Peer 2 Pre-shared Key**: For IKEv2, you can configure unique keys on each peer. Enter the **Pre-shared Key**. You can click the show button and enter the appropriate pre-shared for the peer. The key can be 1-127, alphanumeric characters. The following table describes the purpose of the pre-shared key for both peers.

	Local Pre-shared Key	**Remote Peer Pre-shared Key**
Peer 1	Peer 1 Pre-shared Key	Peer 2 Pre-shared Key
Peer 2	Peer 2 Pre-shared Key	Peer 1 Pre-shared Key

d) Click **IKE Version 1** to enable it.

e) Click **Add IKEv1 Policy** and select the IKEv1 policies. Click **Create New IKEv1 Policy** to create new IKEv1 policies. For more information about creating new IKEv1 policies, see theManaging IKEv1 Policies. To delete an existing IKEv1 Policy, hover-over the selected policy and click the x icon.

f) (IKEv1) **Pre-shared Key**: For IKEv1, you must configure the same preshared key on each peer. The key can be 1-127, alphanumeric characters. In this scenario, Peer 1 and Peer 2 use the same pre-shared key to encrypt and decrypt data.

g) Click **Next**.

Step 8 In the **IPSec Settings** section, based on the configuration made by the user, CDO suggests the IKEv2 proposals. You can either continue with the recommended IKE configuration settings or define a new one. For more information on the IPSec settings, see the Configuring IPsec Proposals.

a) Click **+ IKEv2 Proposals** to select the IPSec configuration. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step. To delete an existing IKEv2 Proposal, hover-over the selected proposal and click the x icon.

Note Click **Create New IKEv2 Proposals** to create new IKEv2 proposals. For more information about creating new IKEv2 policies, see the About IPsec Proposals.

b) Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Encryption and Hash Algorithms Used in VPN, on page 4

c) Click **Next**.

Step 9 In the **Finish** section, read the configuration and continue further only if you're satisfied with your configuration, click **Submit**.

You are directed to the VPN Tunnels page that shows the newly configured site-to-site VPN tunnel. The changes are staged and must be deployed manually. A routing policy is created to route the VTI traffic automatically between the devices over the VTI tunnel. To see this policy, select the device from the **Inventory** page and choose **Configuration** > **Diff**.

See the Deploy Configuration Changes section to deploy site-to-site VPN configuration on the devices associated with the new tunnel.

Delete a CDO Site-To-Site VPN Tunnel

Step 1 On the navigation bar, choose **VPN**> **ASA/FDM Site-to-Site VPN**.

Step 2 Select the desired site-to-site VPN tunnel that you want to delete.

Step 3 In the **Actions** pane, click **Delete**.

The selected site-to-site VPN tunnel is deleted.

Exempt Site-to-Site VPN Traffic from NAT

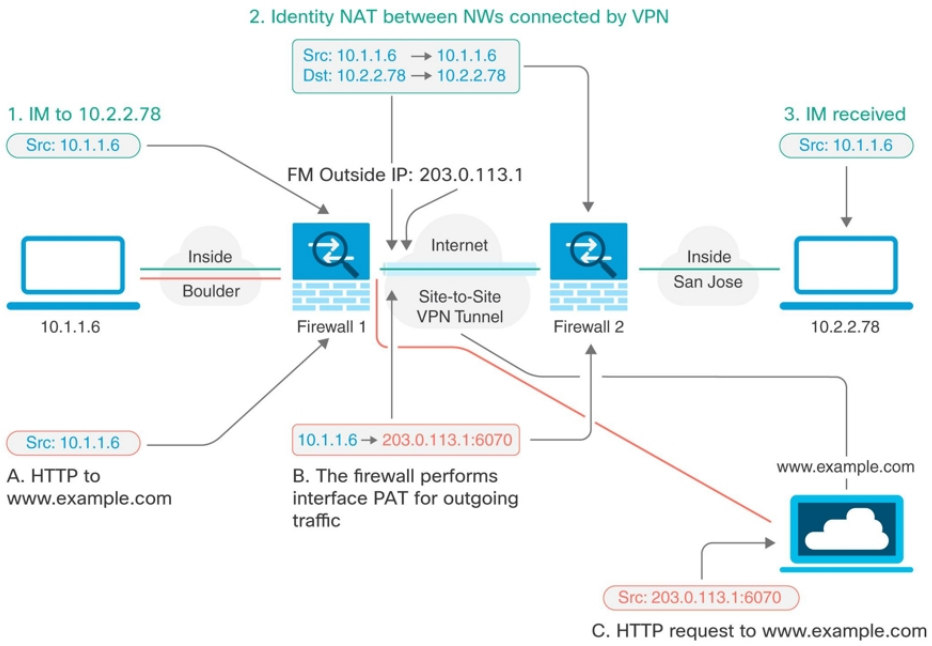
When you have a site-to-site VPN connection defined on an interface, and you also have NAT rules for that interface, you can optionally exempt the traffic on the VPN from the NAT rules. You might want to do this if the remote end of the VPN connection can handle your internal addresses.

When you create the VPN connection, you can select the **NAT Exempt** option to create the rules automatically. However, this works only if your local protected network is connected through a single routed interface (not a bridge group member). If instead, the local networks in the connection reside behind two or more routed interfaces or one or more bridge group members, you need to configure the NAT exempt rules manually.

To exempt VPN traffic from NAT rules, you create an identity manual NAT rule for the local traffic when the destination is the remote network. Then, apply NAT to the traffic when the destination is anything else (for example, the Internet). If you have more than one interface for the local network, create rules for each interface. Also, consider the following suggestions:

- If there is more than one local network in the connection, create a network object group to hold the objects that define the networks.
- If you are including both IPv4 and IPv6 networks in the VPN, create separate identity NAT rules for each.

Consider the following example, which shows a site-to-site tunnel connecting the Boulder and San Jose offices. For traffic that you want to go to the Internet (for example from 10.1.1.6 in Boulder to www.example.com), you need a public IP address provided by NAT to access the Internet. The below example uses interface Port Address Translation (PAT) rules. However, for traffic that you want to go over the VPN tunnel (for example from 10.1.1.6 in Boulder to 10.2.2.78 in San Jose), you do not want to perform NAT; you need to exempt that traffic by creating an identity NAT rule. Identity NAT translates an address to the same address.



The following example explains the configuration for Firewall1 (Boulder). The example assumes that the inside interface is a bridge group, so you need to write the rules for each member interface. The process is the same if you have a single or multiple routed inside interfaces.

Note This example assumes IPv4 only. If the VPN also includes IPv6 networks, create parallel rules for IPv6. Note that you cannot implement IPv6 interface PAT, so you need to create a host object with a unique IPv6 address to use for PAT.

Step 1 Create objects to define the various networks.

a. In the CDO navigation bar at the left, click **Objects** > **FDM Objects**.

b. Click the blue plus button + to create an object.

c. Click **ASA** > **Network**.

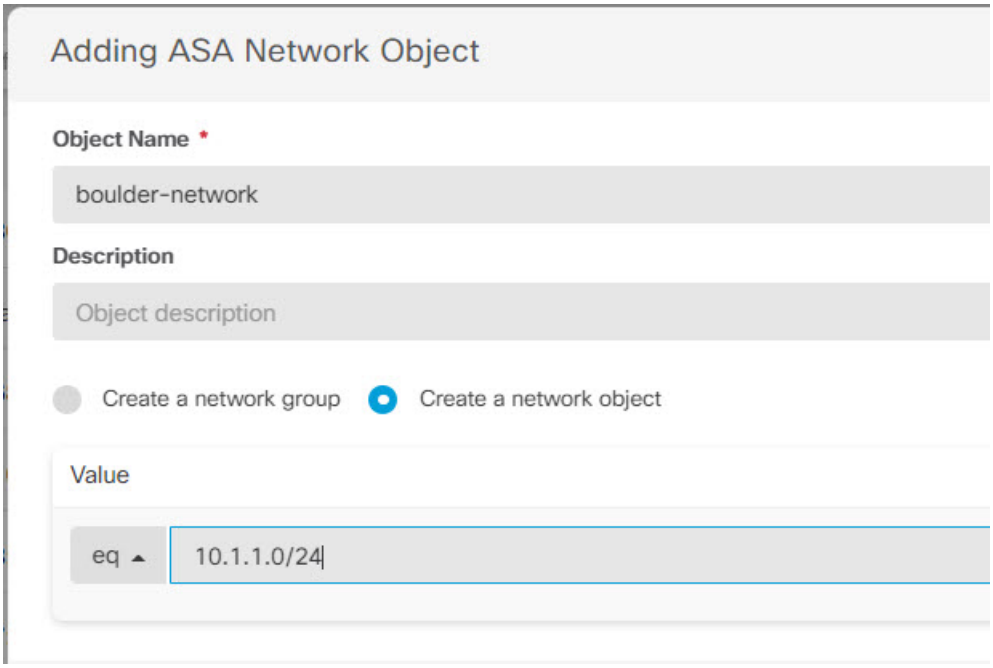
d. Identify the Boulder inside network.

e. Enter an object name (for example, boulder-network).

f. Select **Create a network object**.

g. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.
- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.



h. Click **Add**.

i. Click the blue plus button + to create an object.

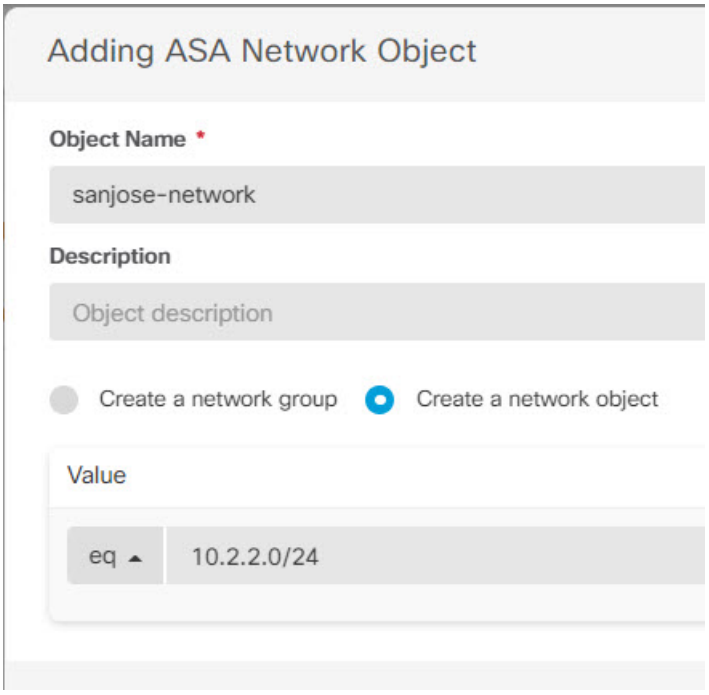
j. Define the inside San Jose network.

k. Enter the object name (for example, san-jose).

l. Select **Create a network object**.

m. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.
- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.



n. Click **Add**.

Step 2 Configure manual identity NAT for the Boulder network when going over the VPN to San Jose on Firewall1 (Boulder).

a. In the CDO navigation bar, click **Inventory**.

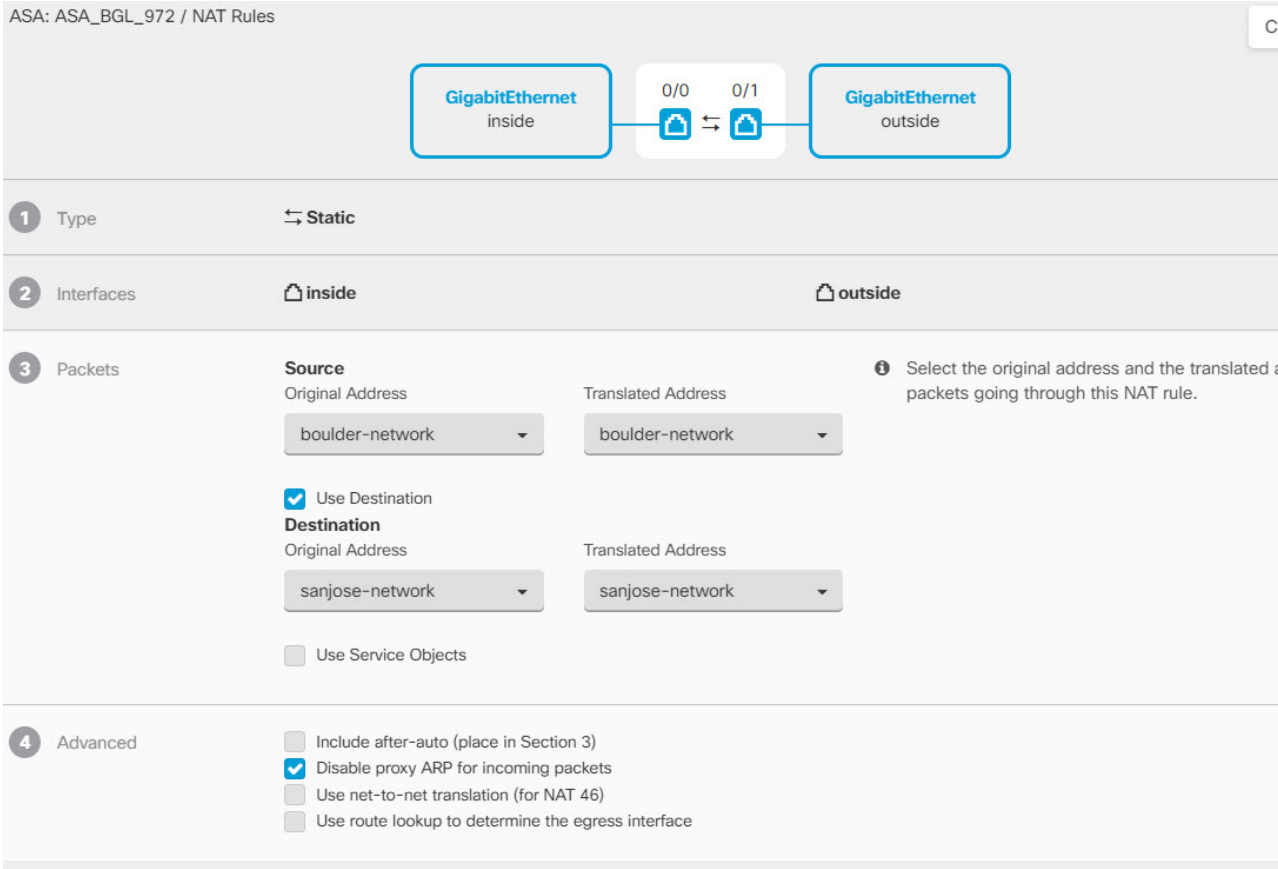
b. Use the filter to find the device for which you want to create the NAT rule.

c. In the Management area of the details panel, click **NAT** NAT.

d. Click + > **Twice NAT**.

- In section 1, select **Static.** Click **Continue**.
- In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.
- In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'boulder-network'.
- Select **Use Destination**.

- Select **Destination Original Address** = 'sanjose-network' and **Source Translated Address** = 'sanjose-network'. **Note**: Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank. This rule configures identity NAT for both source and destination.



- Select **Disable proxy ARP for incoming packets**.
- Click **Save**.
- Repeat the process to create equivalent rules for each of the other inside interfaces.

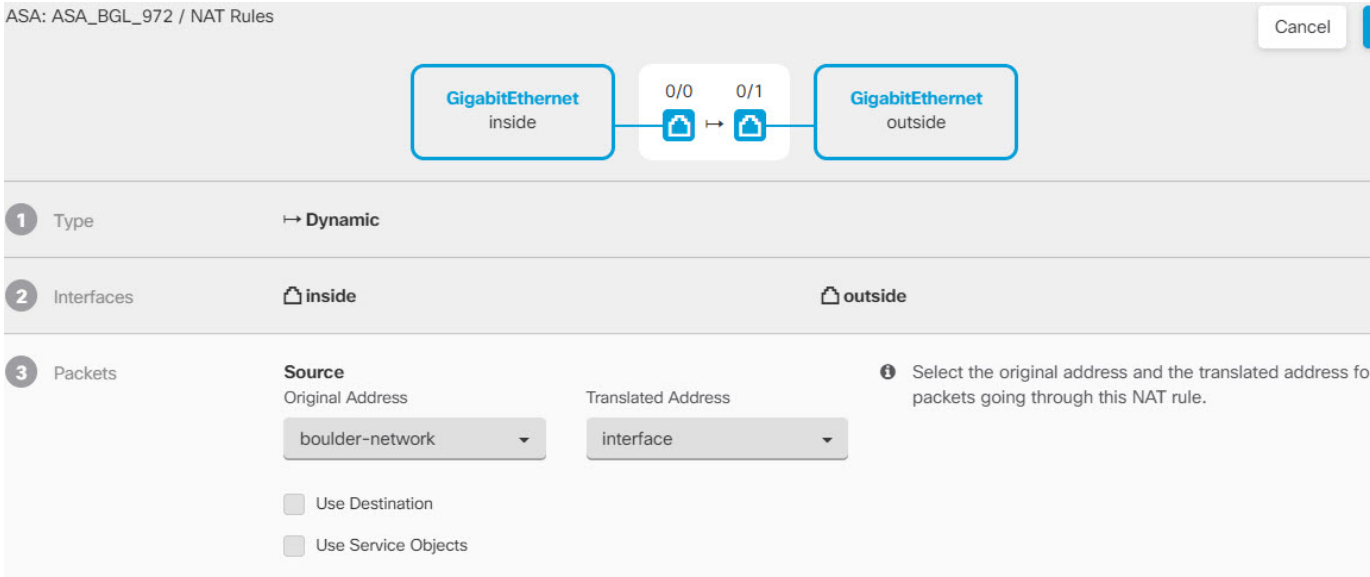
Step 3 Configure manual dynamic interface PAT when going to the Internet for the inside Boulder network on Firewall1 (Boulder). **Note**: There might already be dynamic interface PAT rules for the inside interfaces, covering any IPv4 traffic, as these are created by default during initial configuration. However, the configuration is shown here for completeness. Before completing these steps, check whether a rule already exists that covers the inside interface and network, and skip this step if it does.

a. Click + > **Twice NAT**.

b. In section 1, select **Dynamic.** Click **Continue**.

c. In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.

d. In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'interface'.



e. Click **Save**.

f. Repeat the process to create equivalent rules for each of the other inside interfaces.

Step 4 Deploy configuration changes to CDO. For more information, see Deploy Configuration Changes Made Using the CDO GUI.

Step 5 If you are also managing Firewall2 (San Jose), you can configure similar rules for that device.

- The manual identity NAT rule would be for 'sanjose-network' when the destination is boulder-network. Create new interface objects for the Firewall2 inside and outside networks.
- The manual dynamic interface PAT rule would be for 'sanjose-network' when the destination is "any."

About Global IKE Policies

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

IKE policy objects define the IKE proposals for these negotiations. The objects that you enable are the ones used when the peers negotiate a VPN connection: you cannot specify different IKE policies per connection. The relative priority of each object determines which of these policies are tried first, with the lower number being a higher priority. The connection is not established if the negotiation fails to find a policy that both peers can support.

To define the global IKE policy, you select which objects to enable for each IKE version. If the pre-defined objects do not satisfy your requirements, create new policies to enforce your security policy.

The following procedure explains how to configure the global policy through the Objects page. You can also enable, disable, and create policies when editing a VPN connection by clicking Edit for the IKE Policy settings.

The following topics explain how to configure IKE policies for each version:

- Managing IKEv1 Policies
- Managing IKEv2 Policies

Managing IKEv1 Policies

About IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv1 Policy, on page 15

Create an IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv1 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Policy** link shown in the object list.

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button + and select **FDM** > **IKEv1 Policy** to create a new IKEv1 policy.
- In the object page, select the IKEv1 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv1 properties.

- **Priority** - The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **Encryption** - The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group** - The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Lifetime** - The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).
- **Authentication** - The method of authentication to use between the two peers. For more information, see Deciding Which Authentication Method to Use.
  - **Preshared Key** - Use the preshared key that is defined on each device. These keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If the peer is not configured with the same preshared key, the IKE SA cannot be established.
  - **Certificate** - Use the device identity certificates for the peers to identify each other. You must obtain these certificates by enrolling each peer in a Certificate Authority. You must also upload the trusted CA root and intermediate CA certificates used to sign the identity certificates in each peer. The peers can be enrolled in the same or a different CA. You cannot use self-signed certificates for either peer.
- **Hash** - The hash algorithm for creating a message digest, which is used to ensure message integrity. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.

Step 5 Click **Add**.

Managing IKEv2 Policies

About IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv2 Policy, on page 17

Create an IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv2 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv2 Policy** link shown in the object list.

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv2 Policy** to create a new IKEv2 policy.
- In the object page, select the IKEv2 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv2 properties.

- **Priority** - The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **State** - Whether the IKE policy is enabled or disabled. Click the toggle to change the state. Only enabled policies are used during IKE negotiations.
- **Encryption** - The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. Select all algorithms that you want to allow, although you cannot include both mixed-mode (AES-GCM) and normal mode options in the same policy. (Normal mode requires that you select an integrity hash, whereas mixed-mode prohibits a separate integrity hash selection.) The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group** - The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest group until a match is agreed upon. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Integrity Hash** - The integrity portion of the hash algorithm for creating a message digest, which is used to ensure message integrity. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. The integrity hash is not used with the AES-GCM encryption options. For an explanation of the options, see Deciding Which Hash Algorithms to Use.
- **Pseudo-Random Function (PRF) Hash** - The pseudo-random function (PRF) portion of the hash algorithm, which is used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption.

In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use.

- **Lifetime** - The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

Step 5 Click **Add**.

About IPsec Proposals

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms called a transform set. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers.

There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec proposal, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create and select multiple IKEv1 IPsec Proposal objects.
- When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

The following topics explain how to configure IPsec proposals for each IKE version:

- Managing an IKEv1 IPsec Proposal Object
- Managing an IKEv2 IPsec Proposal Object

Managing an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are

separate objects for IKEv1 and IKEv2. Currently, Cisco Defense Orchestrator (CDO) supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

Related Topics

Create an IKEv1 IPsec Proposal Object, on page 19

Create an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Cisco Defense Orchestrator (CDO) supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

There are several pre-defined IKEv1 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv1 IPsec Proposals objects while editing the IKEv1 IPsec settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Proposal** link shown in the object list.

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button + and select **FDM** > **IKEv1 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Select the Mode in which the IKEv1 IPsec Proposal object operates.

- **Tunnel mode** encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- **Transport mode** encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination

of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

Step 5 Select the **ESP Encryption** (Encapsulating Security Protocol encryption) algorithm for this proposal. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.

Step 6 Select the **ESP Hash** or integrity algorithm to use for authentication. For an explanation of the options, see Deciding Which Hash Algorithms to Use.

Step 7 Click **Add**.

Managing an IKEv2 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.

When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

Related Topics

Create or Edit an IKEv2 IPsec Proposal Object, on page 20

Create or Edit an IKEv2 IPsec Proposal Object

There are several pre-defined IKEv2 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv2 IPsec Proposals objects while editing the IKEv2 IPsec settings in a VPN connection by clicking the Create New IPsec Proposal link shown in the object list.

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv2 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Configure the IKE2 IPsec proposal objects:

- **Encryption** - The Encapsulating Security Protocol (ESP) encryption algorithm for this proposal. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Integrity Hash** - The hash or integrity algorithm to use for authentication. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use.

Step 5 Click **Add**.

Monitor ASA Site-to-Site Virtual Private Networks

CDO allows you to monitor already existing site-to-site VPN configurations on onboarded ASA devices. It doesn't allow you to modify or delete the site-to-site configuration.

Check Site-to-Site VPN Tunnel Connectivity

Use the **Check Connectivity** button to trigger a real-time connectivity check against the tunnel to identify whether the tunnel is currently Search and Filter Site-to-Site VPN Tunnels. Unless you click the on-demand connectivity check button, a check across all tunnels, available across all onboarded devices, occurs once an hour.

Note

- CDO runs this connectivity check command on the ASA to determine if a tunnel is active or idle:

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- Model ASA device(s) tunnels will always show as **Idle**.

To check tunnel connectivity from the VPN page:

Step 1 From the main navigation bar, click VPN > ASA/FDM Site-to-Site VPN.

Step 2 Search and Filter Site-to-Site VPN Tunnels the list of tunnels for your site-to-site VPN tunnel and select it.

Step 3 In the Actions pane at the right, click **Check Connectivity**.

Identify VPN Issues

CDO can identify VPN issues on ASA. (This feature is not yet available for AWS VPC site-to-site VPN tunnels.) This article describes:

- Find VPN Tunnels with Missing Peers
- Find VPN Peers with Encryption Key Issues
- Find Incomplete or Misconfigured Access Lists Defined for a Tunnel
- Find Issues in Tunnel Configuration

  Resolve Tunnel Configuration Issues, on page 23

Find VPN Tunnels with Missing Peers

The "Missing IP Peer" condition is more likely to occur on ASA devices than FDM-managed devices.

Step 1 In the CDO navigation pane, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 Check **Detected Issues**.

Step 5 Select each device reporting an issue and look in the Peers pane at the right. One peer name will be listed. CDO reports the other peer name as, "[Missing peer IP.]"

Find VPN Peers with Encryption Key Issues

Use this approach to locate VPN Peers with encryption key issues such as:

- IKEv1 or IKEv2 keys are invalid, missing, or mismatched
- Obsolete or low encryption tunnels

Step 1 In the CDO navigation bar, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 Select each device reporting an issue and look in the Peers pane at the right. The peer information will show you both peers.

Step 5 Click on **View Peers** for one of the devices.

Step 6 Double-click the device reporting the issue in the Diagram View.

Step 7 Click **Key Exchange** in the Tunnel Details panel at the bottom. You will be able to view both devices and diagnose the key issue from that point.

Find Incomplete or Misconfigured Access Lists Defined for a Tunnel

The "incomplete or misconfigured access-list" condition could only occur on ASA devices.

Step 1 In the CDO navigation bar, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 Select each device reporting an issue and look in the Peers pane at the right. The peer information shows you both peers.

Step 5 Click on **View Peers** for one of the devices.

Step 6 Double-click the device reporting the issue in the Diagram View.

Step 7 Click **Tunnel Details** in the Tunnel Details panel at the bottom. You will see the message, "Network Policy: Incomplete"

Find Issues in Tunnel Configuration

The tunnel configuration error can occur in the following scenarios:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".

- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

Step 1 In the CDO navigation bar, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 In the **Tunnel Issues**, click **Detected Issues** to view the VPN configuration reporting errors. You can view the configuration reporting issues .

Step 5 Select the VPN configuration reporting issues.

Step 6 In the **Peers** pane on the right, the icon appears for the peer having the issue. Hover over the icon to see the issue and resolution.

Next Step: Resolve Tunnel Configuration Issues.

Resolve Tunnel Configuration Issues

This procedure attempts to resolve these tunnel configuration issues:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn’t match the other VPN tunnel, the "IKE value Mismatch" message appears.

See Find Issues in Tunnel Configuration for more information.

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the device associated with the VPN configuration reporting an issue.

Step 4 Accept the device changes.

Step 5 In the CDO navigation pane, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 6 Select the VPN configuration reporting this issue.

Step 7 In the **Actions** pane, click the **Edit** icon.

Step 8 Click **Next** in each step until you click the **Finish** button in step 4.

Step 9 Preview and Deploy Configuration Changes for All Devices.

Search and Filter Site-to-Site VPN Tunnels

Use the filter sidebar in combination with the search field to focus your search of VPN tunnels presented in the VPN tunnel diagram.

Step 1 From the main navigation bar, navigate **VPN** > **ASA/FDM Site-to-Site VPN**.

Step 2 Click the filter icon to open the filter pane.

Step 3 Use these filters to refine your search:

- **Filter by Device**-Click **Filter by Device**, select the device type tab, and check the devices you want to find by filtering.
- **Tunnel Issues-**Whether or not we have detected either side of the tunnel has issues. Some examples of a device having issues may be but not limited to is: missing associated interface or peer IP address or access list, IKEv1 proposal mismatches, etc. (Detecting tunnel issues is not yet available for AWS VPC VPN tunnels.)
- **Devices/Services**-Filter by type of device.
- **Status**–Tunnel status can be active or idle.
  - **Active**-There is an open session where network packets are traversing the VPN tunnel or a successful session was established and hasn't been timed-out yet. Active can assist to indicate that tunnel is active and relevant.
  - **Idle**-CDO was unable to discover an open session for this tunnel, the tunnel may either be not in use or there is an issue with this tunnel.
- **Onboarded** - Devices could be managed by CDO or not managed (unmanaged) by CDO.
  - **Managed** – Filter by devices that CDO manages.
  - **Unmanaged** – Filter by devices that CDO does not manage.
- **Device Types** - Whether or not either side of the tunnel is a live (connected device) or model device.

Step 4 You can also search the filtered results by device name or IP address by entering that information in the search bar. The search is case-insensitive.

Onboard an Unmanaged Site-to-Site VPN Peer

CDO will discover a site-to-site VPN tunnel when one of the peers is onboarded. If the second peer is not managed by CDO, you can filter the list of VPN tunnels to find the unmanaged device and onboard it:

Step 1 In the main navigation bar, select **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the filter panel by clicking .

Step 4 Check **Unmanaged**.

Step 5 Select a tunnel from the table from the results.

Step 6 In the **Peers** pane on the right, click **Onboard Device** and follow the instructions on the screen.

Related Information:

- Onboard Devices and Services
- Onboard ASA Device to CDO

View IKE Object Details of Site-To-Site VPN Tunnels

You can view the details of the IKE objects configured on the peers/devices of the selected tunnel. These details appear in a tree structure in a hierarchy based on the priority of the IKE policy object.

Note Extranet devices don't show the IKE Objects details.

Step 1 In the CDO navigation bar on the left, click **VPN > ASA/FDM Site-to-Site VPN**.

Step 2 In the **VPN Tunnels** page, click the name of the VPN tunnel that connects the peers.

Step 3 Under **Relationships** on the right, expand the object that you want to see its details.

View Last Successful Site-to-Site VPN Tunnel Establishment Date

Step 1 View Site-to-Site VPN Tunnel Information.

Step 2 Click the **Tunnel Details** pane.

Step 3 View the **Last Seen Active** field.

View Site-to-Site VPN Tunnel Information

The site-to-site VPN table view is a complete listing of all site-to-site VPN tunnels available across all devices onboarded to CDO. A tunnel only exists once in this list. Clicking on a tunnel listed in the table provides an option in the right side bar to navigate directly to a tunnel's peers for further investigation.

In cases where CDO does not manage both sides of a tunnel, you can click Onboard an Unmanaged Site-to-Site VPN Peer to open the main onboarding page an onboard the unmanaged peer. In cases where CDO manages both side of a tunnel, the Peer 2 column contains the name of the managed device. However, in the case of an AWS VPC, the Peer 2 column contains the IP address of the VPN gateway.

To view site-to-site VPN connections in the table view:

Step 1 From the main navigation bar, click **VPN > ASA/FDM Site-to-Site VPN.**

Step 2 Click the **Table view** button.

Step 3 Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

Site-to-Site VPN Global View

Step 1 From the main navigation bar, click **VPN > ASA/FDM Site-to-Site VPN.**

Step 2 Click the **Global view** button.

Step 3 Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

Step 4 Select one of the peers represented in the Global View.

Step 5 Click **View Details**.

Step 6 Click the other end of the VPN tunnel and CDO displays Tunnel Details, NAT Information, and Key Exchange information for that connection:

- **Tunnel Details**-Displays the name and connectivity information about the tunnel. Clicking the Refresh icon updates the connectivity information for the tunnels.
- **Tunnel Details specific to AWS connections**-Tunnel details for AWS site-to-site connections are slightly different than for other connections. For each connection from the AWS VPC to your VPN gateway, AWS creates two VPN tunnels. This is for high availability.
  - The name of the tunnel represents the name of the VPC your VPN gateway is connected to. The IP address named in the tunnel is the IP address that your VPN gateway knows as the VPC.
  - If the CDO Connectivity status shows "active," the AWS tunnel state is "Up." If the CDO Connectivity state is "inactive," the AWS tunnel state is "Down."
- **NAT Information**-Displays the type of NAT rule being used, original and translated packet information, and provides links to the NAT table to view the NAT rule for that tunnel. (Not yet available for AWS VPC site-to-site VPN.)
- **Key Exchange**-Displays the cryptographic keys in use by the tunnel and key-exchange issues. (Not yet available for AWS VPC site-to-site VPN.)

Site-to-Site VPN Tunnels Pane

The Tunnels pane displays a list of all the tunnels associated with a particular VPN gateway. For site-to-site VPN connections between your VPN gateway and an AWS VPC, the tunnels pane shows all the tunnels from your VPN gateway to the VPC. Since each site-to-site VPN connection between your VPN gateway and an AWS VPC has two tunnels, you will see double the number of tunnels you normally would for other devices.

VPN Gateway Details

Displays the number of peers connected to the VPN gateway and the IP address of the VPN gateway. This is only visible in the VPN Tunnels page.

View Peer

After you select a site-to-site VPN peer pair, the peers pane lists the two devices in the pair and allows you to click **View Peer** for one of the devices. By clicking **View Peer**, you see any other site-to-site peer that device is associated with. This is visible in the Table view and in the Global view.

Introduction to Remote Access Virtual Private Network

Remote Access irtual Private Network (RA VPN) capability enables users to connect to your network from a location outside the physical office premises. This means that they can use a computer or a supported iOS/Android device that is connected to the internet and access your network resources securely. This feature

is particularly useful for mobile workers who need to connect from their home network or a public Wi-Fi network while ensuring that their data remains safe and protected.

Related Information:

- Configure Remote Access Virtual Private Network for ASA, on page 27

Configure Remote Access Virtual Private Network for ASA

The ASA creates a remote access virtual private network (VPN) by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. It can create single-user-to-LAN connections and LAN-to-LAN connections.

The secure connection is called a tunnel, and the ASA uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The ASA functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination.

CDO provides an intuitive user interface for configuring a new remote access Virtual Private Network. It also allows you to quickly and easily configure remote access VPN connection for multiple Adaptive Security Appliance (ASA) devices onboarded in CDO.

CDO allows you to configure the remote access VPN configuration on ASA devices from scratch. It also allows you to manage the remote access VPN settings that have already been configured using another ASA management tool, such as the Adaptive Security Defense Manager (ASDM) or Cisco Security Manager (CSM). When you onboard an ASA device that already has remote access VPN settings, CDO automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. This default configuration can contain all the connection profile objects that are defined on the device. If you want to understand the RAVPN attributes that are read into CDO, see the Manage and Deploy Pre-existing ASA Remote Access VPN Configuration section. Otherwise, you can start performing steps described in the "End-to-End Remote Access VPN Configuration Process for ASA" section.

Related Information:

- End-to-End Remote Access VPN Configuration Process for ASA
  - Configure Identity Sources for ASA
    - Create an ASA Active Directory Realm Object
    - Create an ASA RADIUS Server Object or Group
  - Create ASA Remote Access VPN Group Policies, on page 34
  - Create ASA Remote Access VPN Configuration, on page 40
  - Configure ASA Remote Access VPN Connection Profile, on page 44
- Manage and Deploy Pre-existing ASA Remote Access VPN Configuration
- Create IP Address Pool
- Exempt Remote Access VPN Traffic from NAT, on page 58
- Verify ASA Remote Access VPN Configuration

- View ASA Remote Access VPN Configuration Details

End-to-End Remote Access VPN Configuration Process for ASA

This section provides the end-to-end procedure for configuring remote access VPN on an ASA device onboarded to CDO.

To enable remote access VPN for your clients, you need to configure several separate items. The following procedure provides the end-to-end process.

Step 1 Configure the identity source used for authenticating remote users. See Configure Identity Sources for ASA for more information.

You can use the following sources to authenticate users attempting to connect to your network using remote access VPN. Additionally, you can use client certificates for authentication, either alone or in conjunction with an identity source.

- Active Directory identity realm: As a primary authentication source. The user accounts are defined in your Active Directory (AD) server. See Configuring AD Identity Realms. See Create an ASA Active Directory Realm Object.
- RADIUS server group: As a primary or secondary authentication source, and for authorization and accounting. See Create an ASA RADIUS Server Object or Group.
- Local Identity Source (the local user database): As a primary or fallback source. You can define users directly on the device and not use an external server. If you use the local database as a fallback source, ensure that you define the same usernames/passwords as the ones described in the external server. **Note**: You can create user accounts directly on the ASA device only from the Adaptive Security Device Manager (ASDM). See the "Configure Local User Groups" section in the Objects for Access Control" chapter of the Cisco ASA Series Firewall ASDM Configuration Guide, X.Y.

Step 2 (optional) Create ASA Remote Access VPN Group Policies, on page 34. The group policy defines user-related attributes. You can configure group policies to provide differential access to resources based on group membership. Alternatively, use the default policy for all connections.

Step 3 Create ASA Remote Access VPN Configuration, on page 40.

Step 4 Configure ASA Remote Access VPN Connection Profile, on page 44.

Step 5 (optional) Exempt Remote Access VPN Traffic from NAT, on page 58.

Step 6 Review and deploy configuration changes to the devices.

Important If you change the Remote Access VPN configuration by using a local manager like Adaptive Security Device Manager (ASDM), the **Configuration Status** of that device in CDO shows "Conflict Detected". See Out-of-Band Changes on an ASA Device. You can Resolve Configuration Conflicts on this ASA.

What to do next

Next Steps

Once the remote access VPN configuration is downloaded to the ASA devices, the users can connect to your network from a remote location using a computer or other supported iOS or Android device connected to the Internet. You can monitor live AnyConnect remote access VPN sessions from all onboarded ASA remote access VPN head-ends in your tenant. See Monitor Remote Access Virtual Private Network Sessions.

Configure Identity Sources for ASA

Identity sources, such as Microsoft Active Directory (AD) realms and RADIUS Servers, are AAA servers and databases that define user accounts for the people in your organization. You can use this information in a variety of ways, such as providing the user identity associated with an IP address or authenticating remote access VPN connections or access to CDO.

Click **Objects** > **ASA Objects**, then click ( )>**Identity Source** to create your sources. You would then use these objects when you configure the services that require an identity source. You can apply appropriate filters to search existing sources and manage them.

Determining the Directory Base DN

When you configure directory properties, you need to specify the common base distinguished name (DN) for users and groups. The base is defined in your directory server and differs from network to network. You must enter the correct bases for identity policies to work. If the base is wrong, the system cannot determine user or group names, and thus identity-based policies will be inoperable.

Note To get the correct bases, consult the administrator who is responsible for the directory servers.

For an active directory, you can determine the correct bases by logging into the Active Directory server as a domain administrator, and using the **dsquery** command at a command prompt as follows to determine the bases:

User search base

Enter the **dsquery user** command with known username (partial or complete) to determine the base distinguished name. For example, the following command uses the partial name "John*" to return information for all users that start with "John."

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

The base DN would be "DC=csc-lab,DC=example,DC=com."

Group search base

Enter the **dsquery group** command with a known group name to determine the base distinguished name. For example, the following command uses the group name Employees to return the distinguished name:

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

The group base DN would be "DC=csc-lab,DC=example,DC=com."

You can also use the ADSI Edit program to browse the Active Directory structure (**Start** > **Run** > **adsiedit.msc**). In ADSI Edit, right-click any object, such as an organizational unit (OU), group, or user, and choose **Properties** to view the distinguished name. You can then copy the string of DC values as the base.

To verify that you have the correct base:

Step 1 Click the Test Connection button in the directory properties to verify connectivity. Resolve any problems, and save the directory properties.

Step 2 Commit changes to the device.

Step 3 Create an access rule, select the **Users** tab, and try to add known user and group names from the directory. You should see auto-complete suggestions as you type for matching users and groups in the realm that contains the directory. If these suggestions appear in a drop-down list, then the system was able to query the directory successfully. If you see no suggestions, and you are certain the string you typed should appear in a user or group name, you need to correct the corresponding search base.

What to do next

See Create an ASA Active Directory Realm Object for more information.

RADIUS Servers and Groups

You can use RADIUS servers to authenticate and authorize administration users. When you configure a feature to use RADIUS servers, you select a RADIUS group instead of individual servers. A RADIUS group is a collection of RADIUS servers that are copies of each other. If a group has more than one server, they form a chain of backup servers to provide redundancy in case one server becomes unavailable. But even if you have only one server, you must create a one-member group to configure RADIUS support for a feature.

You can use this source for the following purposes:

- Remote Access VPN, as an identity source for authentication, and for authorization and accounting. You can use AD in conjunction with a RADIUS server.
- Identity policy, as a passive identity source to collect user identity from remote access VPN logins.

See Create an ASA RADIUS Server Object or Group for more information.

Create an ASA Active Directory Realm Object

When you create or edit an identity source object such as an AD realm object, CDO sends the configuration request to the ASA devices through the SDC. The ASA then communicates with the configured AD realm.

Use the following procedure to create an object:

Step 1 In the CDO navigation bar on the left, click **Objects** > **ASA Objects**.

Step 2 Click **Create Object** ( )**RA VPN Objects (ASA & FDM)** > **Identity Source**.

Step 3 Enter an **Object Name** for the object.

Step 4 Select the **Device Type** as **ASA**.

Step 5 In the first part of the wizard, select **Active Directory Realm** as the **Identity Source Type**. Click **Continue**.

Step 6 Configure the basic realm properties.

- **Directory Username, Directory Password** - The distinguished username and password for a user with appropriate rights to the user information you want to retrieve. For Active Directory, the user does not need elevated privileges. You can specify any user in the domain. The username must be fully qualified; for example, Administrator@example.com (not simply Administrator).

Note The system generates ldap-login-dn and ldap-login-password from this information. For example, Administrator@example.com is translated as cn=administrator,cn=users,dc=example,dc=com. Note that cn=users is always part of this translation, so you must configure the user you specify here under the common name "users" folder.

- **Base Distinguished Name** - The directory tree for searching or querying user and group information, that is, the common parent for users and groups. For example, cn=users,dc=example,dc=com.

Step 7 Configure the directory server properties.

- **Hostname/IP Address**—The hostname or IP address of the directory server. If you use an encrypted connection to the server, you must enter the fully-qualified domain name, not the IP address.
- **Port**—The port number used for communications with the server. The default is 389. Use port 636 if you select LDAPS as the encryption method.
- **Encryption**—To use an encrypted connection for downloading user and group information, select **LDAPS** to use SSL to secure communications between the ASA and the LDAP server. It requires LDAP over SSL. Use port 636.

  The default is **None**, which means that user and group information is downloaded in clear text.

Step 8 (Optional) Use the **Test** button to validate the configuration.

Step 9 (Optional) Click **Add another configuration** to add multiple Active Directory (AD) servers to the AD realm. The AD servers need to be duplicates of each other and support the same AD domain. Therefore, the basic realm properties such as **Directory name**, **Directory Password**, and **Base Distinguished Name** must be the same across all AD servers associated with that AD realm.

Step 10 Click **Add**.

Edit an ASA Active Directory Realm Object

Note that you cannot change the Identity Source Type when editing an Identity source object. You must create a new object with the correct type.

Step 1 In the CDO navigation bar on the left, click **Objects** > **ASA Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon in the **Actions** pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created in the procedures above. Expand the configuration bar listed below to edit or test the hostname/IP address or encryption information.

Step 6 Click **Save**.

Step 7 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 8 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create an ASA RADIUS Server Object or Group

When you create or edit an identity source object such as a RADIUS server object or a group of RADIUS server objects, CDO sends the configuration request to ASA devices through the SDC.

Create an ASA RADIUS Server Object

RADIUS servers provide AAA (authentication, authorization, and accounting) services.

Use the following procedure to create an object:

Step 1 In the CDO navigation bar on the left, click **Objects** > **ASA Objects**.

Step 2 Click **Create Object** ( )> **RA VPN Objects (ASA & FDM)** > **Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 Select the **Device Type** as **ASA**.

Step 5 Select **RADIUS Server** as the **Identity Source Type**. Click **Continue**.

Step 6 Edit the Identity Source configuration with the following properties:

- **Server Name or IP Address** - The fully-qualified host name (FQDN) or IP address of the server.
- **Authentication Port** (Optional) - The port on which RADIUS authentication and authorization are performed. The default is 1812.
- **Timeout** - The length of time, 1-300 seconds, that the system waits for a response from the server before sending the request to the next server. The default is 10 seconds.
- Enter the **Server Secret Key**(Optional) - The shared secret that is used to encrypt data between the ASA device and the RADIUS server. The key is a case-sensitive, alphanumeric string of up to 64 characters, with no spaces. The key must start with an alphanumeric character or an underscore, and it can contain the special characters: $ & - _ . + @. The string must match the one configured on the RADIUS server. If you do not configure a secret key, the connection is not encrypted.

Step 7 Click **Add**.

Step 8 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create an ASA RADIUS Server Group

A RADIUS server group contains one or more RADIUS server objects. The servers within a group must be copies of each other. These servers form a chain of backup servers, so that if the first server is unavailable, the system can try the next server in the list.

Use the following procedure to create an object group:

Step 1 In the CDO navigation bar on the left, click **Objects** > **ASA Objects**.

Step 2 Click **Create Object** ( ) **RA VPN Objects (ASA & FDM) Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 Select the **Device Type** as **ASA**.

Step 5 Select **RADIUS Server Group** as the Identity Source Type. Click **Continue**.

Step 6 Edit the Identity Source configuration with the following properties:

- **Dead Time** - Failed servers are reactivated only after all servers have failed. The dead time is how long to wait after the last server fails before reactivating all servers.
- **Maximum Failed Attempts** - The number of failed requests (that is, requests that do not get a response) sent to a RADIUS server in the group before trying the next server. When the maximum number of failed attempts is exceeded, the system marks the server as Failed. For a given feature, if you configured a fallback method using the local database, and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for the duration of the dead time so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately.
- **Dynamic Authorization/Port** (Optional) - If you enable RADIUS dynamic authorization or change of authorization (CoA) services for this RADIUS server group, the group will be registered for CoA notification and listen on the specified port for CoA policy updates from Cisco Identity Services Engine (ISE). Enable dynamic authorization only if you are using this server group in a remote access VPN in conjunction with ISE.

Step 7 Select an AD realm that supported the RADIUS server from the drop-down menu. If you have not already created an AD realm, click **Create** from inside the drop-down menu.

Step 8 Click the **RADIUS SERVER Add** button to add existing RADIUS server objects. Optionally, you can create a new RADIUS server object from this window is necessary.

Note Add these objects in priority, as the first server in the list is used until it is unresponsive. ASA then defaults to the next server in the list.

Step 9 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Edit an ASA Radius Server Object or Group

Use the following procedure to edit a Radius server object or Radius server group:

Step 1 In the CDO navigation bar on the left, click **Objects** > **ASA Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon in the **Actions** pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created them in the procedures above. To edit or test the hostname/IP address or encryption information, expand the configuration bar.

Step 6 Click **Save**.

Step 7 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 8 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Create ASA Remote Access VPN Group Policies

A group policy is a set of user-oriented attribute/value pairs for remote access VPN connections. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

The system includes a default group policy named "DfltGrpPolicy". You can create additional group policies to provide the services you require.

Note You cannot add inconsistent group policy objects to remote access VPN configuration. Resolve all inconsistencies before adding the group policy to the remote access VPN Configuration.

Step 1 In the CDO navigation bar on the left, click **Objects > ASA Objects**.

Step 2 Click the blue plus button.

Step 3 Click **RA VPN Objects (ASA & FDM)** > **RA VPN Group Policy**.

Step 4 Enter a name for the group policy. The name can be up to 64 characters and spaces are allowed.

Step 5 In the **Device Type** drop-down, select **ASA**.

Step 6 Do any of the following:

- Click the required tabs and configure the attributes on the page:
  - ASA Remote Access VPN Group Policy Attributes
  - AnyConnect Client Profiles, on page 35
  - Session Setting Attributes, on page 36
  - Address Assignment Attributes, on page 36
  - Split Tunneling Attributes, on page 37
  - AnyConnect Attributes, on page 38
  - Traffic Filters Attributes, on page 39
  - Windows Browser Proxy Attributes, on page 40

Step 7 Click **Save** to create the group policy.

ASA Remote Access VPN Group Policy Attributes

The section describes the attributes associated with the ASA remote access VPN group policy.

General Attributes

The general attributes of a group policy define the name of the group and some other basic settings.

- **DNS Server**: Enter the IP address(s) of DNS servers for domain name resolution when connected to the VPN. You can separate the addresses using a comma.
- **Banner**: The banner text, or welcome message, to present to users at login. The default is no banner. The length can be up to 496 characters. The AnyConnect client supports partial HTML. To ensure that the banner displays properly to remote users, use the <BR> tag to indicate line breaks.
- **Default Domain**: The default domain name for users in the remote access VPN. For example, example.com. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.

AnyConnect Client Profiles

This feature is supported on FTD running software version 6.7 or later versions.

Cisco AnyConnect VPN client offers enhanced security through various built-in modules. These modules provide services such as web security, network visibility into endpoint flows, and off-network roaming protection. Each client module includes a client profile that includes a group of custom configurations as per your requirement.

You can select the AnyConnect VPN profile object and AnyConnect modules to be downloaded to clients when the VPN user downloads the VPN AnyConnect client software.

1. Choose or create an AnyConnect VPN profile object. See Upload RA VPN AnyConnect Client Profile, on page 60. Except for DART and Start Before Login modules, the AnyConnect VPN profile object must be selected.
2. Click **Add Any Connect Client Module**.

   The following AnyConnect modules are optional and you can configure these modules to be downloaded with VPN AnyConnect client software:

   - **AMP Enabler** — Deploys advanced malware protection (AMP) for endpoints.
   - **DART** — Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
   - **Feedback** — Provides information about the features and modules customers have enabled and used.
   - **ISE Posture** — Uses the OPSWAT library to perform posture checks to assess an endpoint's compliance.
   - **Network Access Manager** — Provides 802.1X (Layer 2) and device authentication to access both wired and wireless networks.
   - **Network Visibility** — Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics.
   - **Start Before Login** — Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.
   - **Umbrella Roaming Security** — Provides DNS-layer security when no VPN is active.
   - **Web Security** — Analyzes the elements of a web page, allows acceptable content, and blocks malicious or unacceptable content based on a defined security policy.
3. In the **Client Module** list, select an **AnyConnect module**.

4. In the **Profile** list, choose or create a profile object containing an AnyConnect Client Profile.
5. Select **Enable Module Download** to enable endpoints to download the client module along with the profile. If not selected, the endpoints can download only the client profile.

Session Setting Attributes

The session settings of a group policy control how long users can connect through the VPN and how many separate connections they can establish.

- **Maximum Connection Time**: The maximum length of time, in minutes, that users can stay connected to the VPN without logging out and reconnecting, from 1- 4473924 or blank. The default is unlimited (blank), but the idle timeout still applies.
- **Connection Time Alert Interval**: If you specify a maximum connection time, the alert interval defines the amount of time before the maximum time is reached to display a warning to the user about the upcoming automatic disconnect. The user can choose to end the connection and reconnect to restart the timer. The default is 1 minute. You can specify 1 to 30 minutes.
- **Idle Time**: The length of time, in minutes, that the VPN connection can be idle before it is automatically closed, from 1-35791394. If there is no communication activity on the connection for this consecutive number of minutes, the system stops the connection. The default is 30 minutes.
- **Idle Time Alert Interval**: The amount of time before the idle time is reached to display a warning to the user about the upcoming automatic disconnect due to an idle session. Any activity resets the timer. The default is 1 minute. You can specify 1 to 30 minutes.
- **Simultaneous Login Per User**: The maximum number of simultaneous connections allowed for a user. The default is 3. You can specify 1 to 2147483647 connections. Allowing many simultaneous connections might compromise security and affect performance.

Address Assignment Attributes

The address assignment attributes of a group policy define the IP address pool for the group. The pool defined here overrides the pool defined in any connection profile that uses this group. Leave these settings blank if you want to use the pool defined in the connection profile.

- **IPv4 Address Pool, IPv6 Address Pool**: These options define the address pools for the remote endpoints. Clients are assigned an address from these pools based on the IP version they use to make the VPN connection. Select the IP address pool that defines a subnet for each IP type you want to support. Leave the list empty if you do not want to support that IP version. For example, you could define an IPv4 pool as 10.100.10.0/24. The address pool cannot be on the same subnet as the IP address for the outside interface. To create a new Create IP Address Pool. You can specify a list of up to six address pools to use for local address allocation. The order in which you specify the pools is significant. The system allocates addresses from these pools in the order in which the pools appear. **Note**: You can configure both IPv4 and IPv6 address pools for the same group policy. If both versions of IP addresses are configured in the same group policy, clients configured for IPv4 will get an IPv4 address, clients configured for IPv6 will get an IPv6 address, and clients configured for both IPv4 and IPv6 addresses will get both an IPv4 and an IPv6 address.
- **DHCP Scope**: If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same pool identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group. If you do not define a network scope, the

DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address. To specify a scope, enter the network object that contains the network number host address. For example, to tell the DHCP server to use addresses from the 192.168.5.0/24 subnet pool, enter a network object that specifies 192.168.5.0 as a host address. You can use DHCP for IPv4 addressing only.

Split Tunneling Attributes

The split tunneling attributes of a group policy define how the system should handle traffic meant for the internal network vs. externally-directed traffic. Split tunneling directs some network traffic through the VPN tunnel (encrypted) and the remaining network traffic outside the VPN tunnel (unencrypted or in clear text).

Typically, in remote access VPN, you might want the VPN users to access the Internet through your device. However, you can allow your VPN users to access an outside network while they are connected to an remote access VPN. This technique is called split tunneling or hair pinning. The split tunnel allows VPN connectivity to a remote network across a secure tunnel, and it also allows connectivity to a network outside the VPN tunnel. Split tunneling reduces the network load on the FTD devices and increases the bandwidth on the outside interface.

Before you begin

For creating a split tunnel policy for IPv4 networks and another for IPv6 networks, the access-list you specify is used for both protocols. So, the access-list should contain access control entries (ACEs) for both IPv4 and IPv6 traffic.

When an ASA device is onboarded to CDO, it reads the extended ACLs associated with the device. See Group Policy for more information. If you want to create new ACLs, see ASA Policies (Extended access-list) to create them.

Note Ensure that you specify the network intended for split tunneling as the source network in the ACL you are creating.

- **IPv4 Split Tunneling**, **IPv6 Split Tunneling**: You can specify different options based on whether the traffic uses IPv4 or IPv6 addresses, but the options for each are the same. If you want to enable split tunneling, specify one of the options that require you to select network objects.
  - **Allow all traffic over tunnel**: Do no split tunneling. Once the user makes an remote access VPN connection, all the user's traffic goes through the protected tunnel. This is the default. It is also considered the most secure option.
  - **Allow specified traffic over the tunnel**: Select the extended access list that defines the source network. Any traffic from these sources goes through the protected tunnel. The client routes traffic from any other source to connections outside the tunnel (such as a local Wi-Fi or network connection).
  - **Exclude networks specified below**: Select the network objects that define the source network. The client routes any traffic from these sources to connections outside the tunnel. Traffic from any other source goes through the tunnel.
  - **Network List**: Select the extended ACL network that can have both IPv4 and IPv6 networks.
- **Split DNS**: You can configure the system to send some DNS requests through the secure connection while allowing the client to send other DNS requests to the DNS servers configured on the client. You can configure the following DNS behavior:

- **Send DNS Request as per split tunnel policy**: With this option, DNS requests are handled the same way as the split tunnel options are defined. If you enable split tunneling, DNS requests are sent based on the destination addresses. If you do not enable split tunneling, all DNS requests go over the protected connection.
- **Always send DNS requests over tunnel**: Select this option if you enable split tunneling, but you want all DNS requests sent through the protected connection to the DNS servers defined for the group.
- **Send only specified domains over tunnel**: Select this option if you want your protected DNS servers to resolve addresses for certain domains only. Then, specify those domains, separating domain names with commas. For example, example.com, example1.com. Use this option if you want your internal DNS servers to resolve names for internal domains, while external DNS servers handle all other Internet traffic.

AnyConnect Attributes

The AnyConnect attributes of a group policy define some SSL and connection settings used by the AnyConnect client for a remote access VPN connection.

- **SSL Settings**
  - **Enable Datagram Transport Layer Security (DTLS)**: Whether to allow the AnyConnect client to use two simultaneous tunnels: an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL tunnel only.
  - **DTLS Compression**: Whether to compress Datagram Transport Layer Security (DTLS) connections for this group using LZS. DTLS Compression is disabled by default.
  - **SSL Compression**: Whether to enable data compression, and if so, the method of data compression to use, **Deflate**, or **LZS**. SSL Compression is **Disabled** by default. Data compression speeds up transmission rates but also increases the memory requirement and CPU usage for each user session. Therefore, SSL compression decreases the overall throughput of the device.
  - **SSL Rekey Method**, **SSL Rekey Interval**: The client can rekey the VPN connection, renegotiating the crypto keys and initialization vectors, to increase the security of the connection. Disable rekeying by selecting **None**. To enable rekey, select **New Tunnel** to create a new tunnel each time. (The **Existing Tunnel** option results in the same action as **New Tunnel**.) If you enable rekeying, also set the rekey interval, which is 4 minutes by default. You can set the interval to 4-10080 minutes (1 week).
- **Connection Settings**
  - **Ignore the DF (Don't Fragment) bit**: Whether to ignore the Don't Fragment (DF) bit in packets that need fragmentation. Select this option to allow the forced fragmentation of packets that have the DF bit set, so that these packets can pass through the tunnel.
  - **Client Bypass Protocol**: Allows you to configure how the secure gateway manages IPv4 traffic (when it is expecting only IPv6 traffic), or how it manages IPv6 traffic (when it is expecting only IPv4 traffic).

    When the AnyConnect client makes a VPN connection to the headend, the headend assigns it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the headend assigns the AnyConnect connection

only an IPv4 address or only an IPv6 address, you can configure the Client Bypass Protocol to drop network traffic for which the headend did not assign an IP address (default, disabled, not checked), or allow that traffic to bypass the headend and be sent from the client unencrypted or "in the clear" (enabled, checked).

For example, assume that the secure gateway assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual-stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

- **MTU**: The maximum transmission unit (MTU) size for SSL VPN connections established by the Cisco AnyConnect VPN Client. The default is 1406 bytes. The range is 576 to 1462 bytes.
  - **Keepalive Messages Between AnyConnect and VPN Gateway**: Whether to exchange keepalive messages between peers to demonstrate that they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals. The default interval is 20 seconds, and the valid range is 15 to 600 seconds.
  - **DPD on Gateway Side Interval**, **DPD on Client Side Interval**: Enable Dead Peer Detection (DPD) to ensure that the VPN gateway or VPN client quickly detects when the peer is no longer responding. You can separately enable gateway or client DPD. The default interval is 30 seconds for sending DPD messages. The interval can be 5-3600 seconds.

Traffic Filters Attributes

The traffic filter attributes of a group policy define restrictions you want to place on users assigned to the group. You can use these attributes instead of creating access control policy rules to restrict remote access VPN users to specific resources, based on host or subnet address and protocol, or VLAN. By default, remote access VPN users are not restricted by the group policy from accessing any destination on your protected network.

- **Access List Filter**: Restrict access using an extended access control list (ACL). Select the Smart CLI Extended ACL object. The extended ACL lets you filter based on source address, a destination address, and protocol (such as IP or TCP). ACLs are evaluated on a top-down, first-match basis, so ensure that you place specific rules before more general rules. There is an implicit "deny any" at the end of the ACL, so if you intend to deny access to a few subnets while allowing all other access, ensure that you include a "permit any" rule at the end of the ACL. Because you cannot create network objects while editing an extended ACL Smart CLI object, you should create the ACL before editing the group policy. Otherwise, you might need to simply create the object, then go back later to create the network objects and then all the access control entries that you need. To create the ACL, log in to FDM, go to **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**, create an object, and select **Extended Access List** as the object type.
- **Restrict VPN to VLAN**: Also called "VLAN mapping," this attribute specifies the egress VLAN interface for sessions to which this group policy applies. The system forwards all traffic from this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using an ACL to filter traffic on a session. Ensure that you specify a VLAN number that is defined on a subinterface on the device. Values range from 1 to 4094.

Windows Browser Proxy Attributes

The Windows browser proxy attributes of a group policy determine how, and whether, a proxy defined on the user's browser operates.

You can select one of the following values for **Browser Proxy During VPN Session**:

- **No change in endpoint settings**: Allow the user to configure (or not configure) a browser proxy for HTTP and use the proxy if it is configured.
- **Disable browser proxy**: Do not use the proxy defined for the browser, if any. No browser connections will go through the proxy.
- **Auto detect settings**: Enable the use of automatic proxy server detection in the browser for the client device.
- **Use custom settings**: Define a proxy that should be used by all client devices for HTTP traffic. Configure the following settings:
  - **Proxy Server IP or Hostname**, **Port**: The IP address, or hostname, of the proxy server, and the port used for proxy connections by the proxy server. The host and port combined cannot exceed 100 characters.
  - **Browser Proxy Exemption List**: Connections to the hosts/ports in the exemption list do not go through the proxy. Add all the host/port values for destinations that should not use the proxy. For example, www.example.com port 80. Click **Add proxy exemption** to add items to the list. Click the trash can icon to delete items. The entire proxy exception list, combining all addresses and ports, cannot be longer than 255 characters.

Create ASA Remote Access VPN Configuration

CDO allows you to add one or more Adaptive Security Appliance (ASA) devices to the remote access VPN configuration wizard and configure the VPN interfaces, access control, and NAT exemption settings associated with the devices. Therefore, each remote access VPN configuration can have connection profiles and group policies shared across multiple ASA devices that are associated with the remote access VPN configuration. Further, you can enhance the configuration by creating connection profiles and group policies.

You can either onboard an ASA device that has already been configured with remote access VPN settings or a new device without remote access VPN settings. See Onboard ASA Device to CDO. When you onboard an ASA device that already has remote access VPN settings, CDO automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. Also, this default configuration can contain all the connection profile objects that are defined on the device. See Manage and Deploy Pre-existing ASA Remote Access VPN Configuration for more information. CDO allows you to delete the default configuration.

Important

- You are not allowed to add ASA and FTD in the same Remote Access VPN Configuration.
- An ASA device cannot have more than one remote access VPN Configuration.

Before you begin

Before adding the ASA device to the remote access VPN configuration, the following prerequisites must be met on the ASA device:

- License requirements.

  Device must be enabled for export-controlled functionality.

  To view the license summary of your ASA device, execute the show license summary command in the ASA command-line interface. To use the CDO ASA CLI interface, see Using ASA CLI in CDO interface.

  - Example of export-controlled functionality enabled in the license summary :

```
Registration: Status: REGISTERED Smart Account: Cisco SVS temp-request access
licensing@cisco.com Export-Controlled Functionality: ALLOWED

Last Renewal Attempt: None

Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
```

  The 'Export-Controlled Functionality' property must be in the 'Allowed' state for creating or editing the VPN configuration.

  If this property is in the 'Not Allowed' state, CDO displays an error message ('remote access VPN cannot be configured for devices which are not export compliant.') when you are creating or modifying the VPN configuration and doesn't allow remote access VPN configuration on the device.

- Device Identity Certificates.

  Certificates are required to authenticate connections between the clients and the ASA device. Before starting the VPN configuration, ensure that the identity certificate is already present on the ASA device.

  To determine whether or not the certificate is present on the device, execute the **show crypto CA Certificates** command in the ASA command-line interface. To use the CDO ASA CLI interface, see Using ASA CLI in CDO interface.

  If the identity certificate is not present or you want to enroll in a new certificate, install them on ASA using CDO. See ASA Certificate Management.

  The usage of digital certificates in remote access VPN context is explained in Remote Access VPN Certificate-Based Authentication, on page 57.

- Outside interfaces.

  The outside interfaces must be configured already on the ASA device. **You need to use either ASDM or ASA CLI to configure interfaces**. To know configure interfaces using ASDM, see the "Interfaces" book of the Cisco ASA Series General Operations CLI Configuration Guide, X.Y.

- Download the AnyConnect packages and upload them to a remote server. Later, use the remote access VPN wizard or ASA File Management wizard to upload the AnyConnect software packages from the server to ASAs. See Manage AnyConnect Software Packages on ASA Devices for instructions.

- There are no configuration deployments pending.

- If you are using the local database for authentication Add user accounts to the local database using ASDM or ASA CLI.

  To add user accounts using ASDM, see the "Add a User Account to the Local Database" section in the "AAA Servers and the Local Database" book of the Cisco ASA Series VPN CLI Configuration Guide, X.Y.

  To add user accounts using ASA CLI, execute **username[***username***] password [***password***] privilege [***priv_level]* command.

- ASA changes are synchronized to CDO.

1. In the CDO navigation bar at the left, click **Inventory** and search for one or more ASA devices to be synchronized.
2. Select one or more devices and then click **Check for changes**. CDO communicates with one or more FTD devices to synchronize the changes.

- Remote access VPN configuration group policy objects are consistent.
  - Ensure that all inconsistent group policy objects are resolved as they cannot be added to the remote access VPN configuration. Either address the issue or remove inconsistent group policy objects from the **Objects** page. For more information see, Resolve Duplicate Object Issues and Resolve Inconsistent Object Issues.

Step 1 Onboard ASA Device to CDO.

Step 2 In the CDO navigation bar at the left, click **VPN** > **ASA/FDM Remote Access VPN Configuration**.

Step 3 Click the blue plus button to create a new remote access VPN configuration.

Step 4 Enter a name for the Remote Access VPN configuration.

Step 5 Click the blue plus button to add ASA devices to the configuration.

You can add the device details and configure network traffic-related permissions that are associated with the device.

a. Provide the following device details:

- **Device**: Select an ASA device that you want to add and click **Select**. **Important**: You are not allowed to add ASA and FTD in the same Remote Access VPN Configuration.
- **Certificate of Device Identity**: Select the internal certificate used for establishing the identity of the device. This establishes the device identity for AnyConnect clients when they make a connection to the device. Clients must accept this certificate to complete a secure VPN connection.
- **Outside Interface**: Select the interface to which users connect when making the remote access VPN connection. Although this is normally the outside (internet-facing) interface, choose whichever interface is between the device and the end-users you are supporting with this connection profile.

  Attention You cannot create or modify remote access VPN configuration for devices that are not export compliant. You must license the ASA device with export-controlled functionality enabled and try again.

b. Click **Continue** to configure the traffic permissions.

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

  Note that if you select this option, the system configures the sysopt connection permit-vpn command, which is a global setting. This will also impact the behavior of site-to-site VPN connections.

  If you do not select this option, it might be possible for external users to spoof IP addresses in your remote access VPN address pool, and thus gain access to your network. This can happen because you will need to create access

control rules that allow your address pool to have access to internal resources. If you use access control rules, consider using user specifications to control access, rather than source IP address alone.

The downside of selecting this option is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic. This also means that no connection events will be generated for the traffic, and thus statistical dashboards will not reflect VPN connections.

- **NAT Exempt**: NAT exemption exempts addresses from translation and allows both translated and remote hosts to initiate connections with your protected hosts. Configure NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. See Exempt Remote Access VPN Traffic from NAT, on page 58.

c. Click **OK**.

The **AnyConnect Packages Detected** shows the AnyConnect packages that are already available on the device.

There are two options to upload AnyConnect package to ASA from remote access VPN wizard:

- (Option 1): Select a package from CDO's repository. The ASA must have access to the internet.
- (Option 2): Specify the ftp/http/https/scp/smb/tftp URL location where the AnyConnect package is preloaded.

See Manage AnyConnect Software Packages on ASA Devices for instructions.

Note Note: If you want to replace an existing package, see Manage AnyConnect Software Packages on ASA Devices.

Step 6 Click **OK**.

The ASA VPN configuration is created.

Modify ASA Remote Access VPN Configuration

You can modify the name and the device details of an existing remote access VPN configuration.

Step 1 Select the configuration to be modified and under **Actions**, click **Edit**.

- Modify the name if required.
- Click the blue plus button to add a new device
- Click to perform the following on the ASA device.
  - Click **Edit** to modify the existing remote access VPN configuration.
  - Click **Remove** to remove the ASA device from the remote access VPN configuration. All connection profiles and remote access VPN settings associated with that device except the group policies are deleted. You can remove the group policies explicitly from the objects page.

    Note You cannot remove the ASA if that is the only device using the configuration. Alternatively, you can remove the remote access VPN configuration.

Step 2 Deploy Configuration Changes.

What to do next

You can also search for remote access VPN configuration by typing the name of the configuration or device.
Related Information:

- Configure ASA Remote Access VPN Connection Profile, on page 44.

Configure ASA Remote Access VPN Connection Profile

A Remote Access VPN connection profile defines the characteristics that allow external users to create a VPN connection to the system using the AnyConnect client. Each profile defines the AAA servers and certificates used for authenticating users, the address pools for assigning users IP addresses, and the group policies that define various user-oriented attributes.

You can create multiple profiles within the remote access VPN configuration if you need to provide variable services to different user groups, or if you have various authentication sources. For example, if your organization merges with a different organization that uses different authentication servers, you can create a profile for the new group that uses those authentication servers.

A remote access VPN connection profile allows your users to connect to your inside networks when they are on external networks, such as their home network. Create separate profiles to accommodate different authentication methods.

Before you begin

Create ASA Remote Access VPN Configuration, on page 40.

Step 1 On the CDO navigation pane, click **VPN** > **ASA/FDM Remote Access VPN Configuration**. You can click a VPN configuration to view the summary information on how many connection profiles and group policies are currently configured.

Note To know the group policies assigned to the device, in **Actions**, click **Group Policies**. Group Policies assigned to connection profiles are automatically added to the list and cannot be removed.

If the group policy you need does not yet exist, click + and select from the list. You can create additional group policies to provide the services you require. See Create ASA Remote Access VPN Group Policies, on page 34.

Step 2 Click the connection profile and under **Actions** in the sidebar at the right, click **Add Connection Profile**.

Step 3 Configure the basic connection attributes.

- **Connection Profile Name**: The name for this connection, up to 50 characters without spaces. For example, MainOffice.

  Note The name you enter here is what users will see in the connection list in the AnyConnect client. Choose a name that will make sense to your users.

- **Group Alias, Group URL**: Aliases contain alternate names or URLs for a specific connection profile. VPN users can choose an alias name in the AnyConnect client in the list of connections when they connect to the ASA device. The connection profile name is automatically added as a group alias. You can also configure the list of group

URLs, which your endpoints can select while initiating the Remote Access VPN connection. If users connect using the group URL, the system will automatically use the connection profile that matches the URL. This URL would be used by clients who do not yet have the AnyConnect client installed. Add as many group aliases and URLs as required. These aliases and URLs must be unique across all connection profiles defined on the device. Group URLs must start with **https://**.

- For example, you might have the alias Contractor and the group URLhttps://ravpn.example.com/contractor. Once the AnyConnect client is installed, the user would simply select the group alias in the AnyConnect VPN drop-down list of connections.

Step 4 Configure the primary and optionally, secondary identity sources. These options determine how remote users authenticate to the device to enable the remote access VPN connection. The simplest approach is to use AAA only and then select an AD realm or use the LocalIdentitySource. You can use the following approaches for **Authentication Type**:

- **AAA Only**: Authenticate and authorize users based on username and password. For details, see Configure AAA for a Connection Profile , on page 45.
- **Client Certificate Only**: Authenticate users based on client device identity certificate. For details, see Configure Certificate Authentication for a Connection Profile.
- **AAA and ClientCertificate**: Use both username/password and client device identity certificate.

Step 5 Configure the address pool for clients. The address pool defines the IP addresses that the system can assign to remote clients when they establish a VPN connection. For more information, see Configure Client Address Pool Assignment.

Step 6 Click **Continue**.

Step 7 Select the **Group Policy** to use for this profile from the list and click **Select**.

The group policy sets terms for user connections after the tunnel is established. The system includes a default group policy named 'DfltGrpPolicy'. You can create additional group policies to provide the services you require. See Create ASA Remote Access VPN Group Policies, on page 34.

Step 8 Click **Continue**.

Step 9 Review the summary. First, verify that the summary is correct. You can see what end-users need to do to initially install the AnyConnect software and test that they can complete a VPN connection. Click to copy the instructions to the clipboard, and then distribute them to your users.

Step 10 Click **Done**.

Step 11 Perform step 5 of End-to-End Remote Access VPN Configuration Process for ASA.

Configure AAA for a Connection Profile

Authentication, Authorization, and Accounting (AAA) servers use username and password to determine if a user is allowed access to the remote access VPN. If you use RADIUS servers, you can distinguish authorization levels among authenticated users, to provide differential access to protected resources. You can also use RADIUS accounting services to keep track of usage.

When configuring AAA, you must configure a primary identity source. Secondary and fallback sources are optional. Use a secondary source if you want to implement dual authentication, for example, using RSA tokens or DUO.

Primary Identity Source Options

- **Primary Identity Source for User Authentication**: Authentication provides a way to identify a user, typically by having the user enter a valid username and valid password before access is granted. The primary identity source used for authenticating remote users. End-users must be defined in this source or the optional fallback source to complete a VPN connection. Select one of the following:
  - An Active Directory (AD) identity realm.
  - A RADIUS server group.
  - LocalIdentitySource (the local user database): You can define users directly on the device and not use an external server.

    You can click Configure Identity Sources for ASA to create new identity sources.
- **Fallback Local Identity Source**: If the primary source is an external server, you can select the LocalIdentitySource as a fallback in case the primary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the external server.
- **Strip options**: A realm is an administrative domain. Enabling the following options allows the authentication to be based on the username alone. You can enable any combination of these options. However, you must select both check boxes if your server cannot parse delimiters.
  - **Strip Identity Source Server from Username**: Whether to remove the identity source name from the username before passing the username on to the AAA server. For example, if you select this option and the user enters domain\username as the username, the domain is stripped off from the username and sent to the AAA server for authentication. By default, this option is unchecked.
  - **Strip Group from Username**: Whether to remove the group name from the username before passing the username on to the AAA server. This option applies to names given in the username@domain format; the option strips the domain and @ sign. By default, this option is unchecked.

Secondary Identity Source

- **Secondary Identity Source for User Authorization**: The optional second identity source. If the user successfully authenticates with the primary source, the user is prompted to authenticate with the secondary source. You can select an AD realm, RADIUS server group, or the local identity source.
- **Advanced options**: Click the **Advanced** link and configure the following options:
  - **Fallback Local Identity Source for Secondary**: If the secondary source is an external server, you can select the LocalIdentitySource as a fallback in case the secondary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the secondary external server.
  - **Use Primary Username for Secondary Login**: By default, when using a secondary identity source, the system will prompt for both username and password for the secondary source. If you select this option, the system prompts for the secondary password only and uses the same username for the secondary source that was authenticated against the primary identity source. Select this option if you configure the same usernames in both the primary and secondary identity sources.
    - **Username for Session Server**: After successful authentication, the username is shown in events and statistical dashboards, is used for determining matches for a user- or group-based SSL decryption and access control rules and is used for accounting. Because you are using two

authentication sources, you need to tell the system whether to use the Primary or Secondary username as the user identity. By default, the primary name is used.

- **Password Type**: How to obtain the password for the secondary server. The default is **Prompt**, which means the user is asked to enter the password. Select **Primary Identity Source Password** to automatically use the password entered when the user authenticated to the primary server. Select **Common Password** to use the same password for every user, then enter that password in the **Common Password** field.

- **Authorization Server**: The RADIUS server group that has been configured to authorize remote access, VPN users. After authentication is complete, authorization controls the services and commands available to each authenticated user. Authorization works by assembling a set of attributes that describe what the user is authorized to perform, their actual capabilities, and restrictions. Were you not to use authorization, authentication alone would provide the same access to all authenticated users.

  Note that if the system obtains authorization attributes from the RADIUS server that overlap those defined in the group policy, the RADIUS attributes override the group policy attributes.

  You can click Create an ASA RADIUS Server Object or Group to create new server groups.

- **Accounting Server**: (Optional.) The RADIUS server group to use to account for the remote access VPN session. Accounting tracks the services users are accessing as well as the number of network resources they are consuming. The ASA device reports user activity to the RADIUS server. Accounting information includes when sessions start and stop, usernames, the number of bytes that pass through the device for each session, the service used, and the duration of each session. You can then analyze the data for network management, client billing, or auditing. You can use accounting alone or together with authentication and authorization.

  You can click Create an ASA RADIUS Server Object or Group to create new server groups.

Configure Certificate Authentication for a Connection Profile

Note This section is not applicable for **Authentication Type** as **AAA Only**.

You can use certificates installed on the client device to authenticate remote access VPN connections.

When using client certificates, you can still configure a secondary identity source, fallback source, and authorization and accounting servers. These are AAA options; for details, see Configure ASA Remote Access VPN Connection Profile, on page 44.

The following are the certificate-specific attributes. You can configure these attributes separately for primary and secondary identity sources. Configuring a secondary source is optional.

- **Username from Certificate**: Select one of the following:
  - **Map Specific Field**: Use the certificate elements in the order of **Primary Field** and **Secondary Field**. The defaults are CN (Common Name) and OU (Organizational Unit). Select the options that work for your organization. The fields are combined to provide the username, and this is the name used in events, dashboards, and for matching purposes in SSL decryption and access control rules.
  - **Use entire DN (distinguished name) as username**: The system automatically derives the username from the DN fields.

- **Advanced options** (not applicable for **Authentication Type** as **Client Certificate Only**): Click the **Advanced** link and configure the following options:
  - **Prefill username from certificate on user login window**: Whether to fill in the username field with the retrieved username when prompting the user to authenticate.
  - **Hide username in login window**: If you select the **Prefill** option, you can hide the username, which means the user cannot edit the username in the password prompt.

Configure Client Address Pool Assignment

There must be a way for the system to provide an IP address to endpoints that connect to the remote access VPN. The AAA server can provide these addresses, a DHCP server, an IP address pool configured in the group policy, or an IP address pool configured in the connection profile. The system tries these resources in that order and stops when it obtains an available address, which it then assigns to the client. Thus, you can configure multiple options to create a failsafe in case of an unusual number of concurrent connections.

Use one or more of the following methods to configure the address pool for a connection profile.

- **IPv4 Address Pool** and **IPv4 Address Pool**: First, create up to six network objects that specify subnets. You can configure separate pools for IPv4 and IPv6. Then, select these objects in the **IPv4 Address Pool** and **IPv6 Address Pool** options, either in the group policy or in the connection profile. You do not need to configure both IPv4 and IPv6, configure the addressing scheme you want to support. You also do not need to configure the pool in both the group policy and the connection profile. The group policy overrides the connection profile settings, so if you configure the pools in the group policy, leave the options empty in the connection profile. Note that the pools are used in the order in which you list them. To create new IPv4 or IPV6 address pools, see Create IP Address Pool.
- **DHCP Servers**: First, configure a DHCP server with one or more IPv4 address ranges for the remote access VPN (you cannot configure IPv6 pools using DHCP). Then, create a host network object with the IP address of the DHCP server. You can then select this object in the **DHCP Servers** attribute of the connection profile. You can configure more than one DHCP server. If the DHCP server has multiple address pools, you can use the **DHCP Scope** attribute in the Create ASA Remote Access VPN Group Policies that you attach to the connection profile to select which pool to use. Create a host network object with the network address of the pool. For example, if the DHCP pool contains 192.168.15.0/24 and 192.168.16.0/24, setting the DHCP scope to 192.168.16.0 will ensure that an address from the 192.168.16.0/24 subnet will be selected.

Related Information:

End-to-End Remote Access VPN Configuration Process for ASA

Manage AnyConnect Software Packages on ASA Devices

You can perform one of the following steps to upload an AnyConnect package using the remote access VPN wizard:

- Upload the package from the CDO repository.
- Upload the package from the server using HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

Upload an AnyConnect Package from CDO Repository

The remote access VPN Configuration wizard presents AnyConnect packages per operating system from the CDO repository, which you can select and upload to device. Make sure that the device has access to the internet and proper DNS configuration.

Note If the desired package is unavailable in the presented list or the device has no access to the internet, you can upload the package using the server where the AnyConnect packages are preloaded.

Step 1 Click on the field that corresponds to an operating system and select an AnyConnect package.

Step 2 Click to upload the package. If the checksum doesn't match, the AnyConnect package upload fails. You can see the device's workflow tab for more details about the failure.

Upload an AnyConnect Package to ASA from Server

Download the AnyConnect client software packages to your computer and upload them to a remote server accessible from ASAs. Later, use the RA VPN wizard or ASA File Management wizard to upload the AnyConnect software packages from that server to ASAs. DNS must be configured correctly on the device for URLs that use a domain name.

The ASA RA VPN wizard supports uploading packages using HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

The syntax of supported protocols for uploading the file:

Protocol	Syntax	Example
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	ftp://[illegible]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/ filename]	scp://root:cisco123@10.10.16.6/root/events_send.py

Before you begin

Make sure that you download the "AnyConnect Headend Deployment Package" for your desired operating systems. Always download the latest AnyConnect version to ensure that you have the latest features, bug fixes, and security patches. Regularly update the packages on the device.

Important If you choose to upload the package using the ASA File Management wizard, do not modify the package's name after downloading them.

Note You can upload one AnyConnect package per Operating System (OS): Windows, Mac, and Linux. You cannot upload multiple versions for a given OS type.

Step 1 Download the AnyConnect packages from https://software.cisco.com/download/home/283000185.

- Make sure you accept the EULA and have K9 (encrypted image) privileges.
- Select the "AnyConnect Headend Deployment Package" package for your operating system. The package name will be similar to "anyconnect-win-4.7.04056-webdeploy-k9.pkg." There are separate headend packages for Windows, macOS, and Linux.

Step 2 Upload the AnyConnect packages to a remote server. Ensure that there is a network route from the ASA device and the server.

The ASA RA VPN wizard supports uploading packages HTTP, HTTPS, TFTP, FTP, SMB, or SCP protocols.

Important If you are uploading the AnyConnect package to an HTTPS server, ensure that the following steps are performed:

- Upload the trusted CA certificate of that server on the ASA device.
- Install the trusted CA certificate on the HTTPS server.

Step 3 The remote server's URL must be a direct link without prompting for authentication. If the URL is pre-authenticated, you can download the file by specifying the RA VPN wizard's URL.

Step 4 If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

Upload new AnyConnect Packages to ASA

You can either use the remote access VPN wizard or ASA File Management wizard to upload the AnyConnect software packages to ASAs.

Use the following procedure to upload new AnyConnect packages to an ASA device from an HTTP or HTTPS server:

Step 1 In the **AnyConnect Package Detected**, you can upload separate packages for Windows, Mac, and Linux endpoints.

Step 2 In the corresponding platform field, specify the server's paths where the AnyConnect packages compatible for Windows, Mac, and Linux are pre-uploaded. Examples of server paths:
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

Step 3 Click to upload the package. CDO validates if the path is reachable and the specified filename is a valid package. When the validation is successful, the names of the AnyConnect packages appear. As you add more ASA devices to the remote access VPN configuration, you can upload the AnyConnect packages to them.

Step 4 Click **OK**. The AnyConnect packages are added to the remote access VPN configuration.

Step 5 Continue to Create ASA Remote Access VPN Configuration from step 5 onwards.

What to do next

To complete a VPN connection, your users must install the AnyConnect client software on their workstation. For more information, see Install the AnyConnect Client Software on ASA .

Upload AnyConnect Packages using File Management Wizard

Use the File Management wizard to upload AnyConnect packages to a single or multiple ASA devices from an HTTP, HTTPS, TFTP, FTP, SMB, or SCP server. When you want to push AnyConnect packages to multiple ASA devices simultaneously, the bulk upload comes in handy. For more information, see ASA File Management.

Important If you choose to upload the package using the ASA File Management wizard, do not modify the package's name after downloading them.

Once the upload is complete, open the ASA RA VPN Configuration wizard and notice that the packages are auto-detected. If you upload multiple packages for an OS version, the wizard lists them in a drop-down allowing you to select one among them. Then, you can create the RA VPN configuration and deploy them to the devices.

Replace an AnyConnect Package

If the AnyConnect packages are already present on the devices, you can see them in the remote access VPN wizard. You can see all the available AnyConnect packages for an operating system in a drop-down list. You can select an existing package from the list and replace it with a new one but can't add a new package to the list.

Note If you want to replace an existing package with a new one, ensure that the new AnyConnect package is uploaded already to a server on the network that the ASA can reach.

Step 1 In the CDO navigation bar at the left, click **VPN** > **ASA/FDM Remote Access VPN**.

Step 2 Select the remote access VPN configuration to be modified, and under **Actions**, click **Edit**.

Step 3 In **AnyConnect Packages Detected**, click icon appearing beside the existing AnyConnect package. If there are multiple versions of AnyConnect package for an operating system, select the package you want to replace from the list and click **Edit**. The existing package disappears from the corresponding field.

Step 4 Specify the server's path where the new AnyConnect package is preloaded and click to upload the package.

Step 5 Click **OK**. The new AnyConnect package is added to the remote access VPN configuration.

Step 6 Continue to Create ASA Remote Access VPN Configuration, on page 40 from step 6 onwards.

Delete an AnyConnect Package

Step 1 In the CDO navigation bar at the left, click **VPN** > **ASA/FDM Remote Access VPN**.

Step 2 Select the remote access VPN configuration to be modified, and under **Actions**, click **Edit**.

Step 3 In **AnyConnect Packages Detected**, click icon appearing beside the AnyConnect package that you want to delete. If there are multiple versions of AnyConnect package for an operating system, select the package you want to delete from the list. The existing package disappears from the corresponding field.

Note Click **Cancel** to stop the delete operation and retain the existing package,

Step 4 Click **OK**. The device's **Configuration Status** is in 'Not Synced' state.

Note If you want to undo the delete action at this stage, go to **Inventory** page and click **Discard Changes** to retain the existing AnyConnect package.

Step 5 Review and deploy configuration changes to the devices.

Manage and Deploy Pre-existing ASA Remote Access VPN Configuration

When you onboard an ASDM managed ASA device that already has remote access VPN settings, it discovers and displays the existing remote access VPN configurations. CDO automatically creates a "Default remote access VPN Configuration" and associates the ASA device with this configuration. There are some remote access VPN configurations that aren't read or supported in the CDO but can be configured in the CDO command-line interface.

Note This section doesn't cover every supported or unsupported configuration in CDO. Instead, it only describes the most commonly used ones.

To see the remote access VPN configurations from an onboarded ASA, perform the following steps:

Step 1 On the CDO interface, navigate to **VPN** > **ASA/FDM Remote Access VPN Configuration**.

Step 2 Click the remote access VPN configuration corresponding to the onboarded ASA device. CDO automatically creates a "**Default_RA_VPN_Configuration**" and associates the ASA device with this configuration. You can delete the default configuration. The ASA remote access VPN configurations that are read in CDO are classified as follows:

- Device settings
- Connection profiles
- Group policies

Device Settings

The RA VPN configurations associated with the onboarded ASA device appear in **Default_RA_VPN_Configuration**. You need to click on this configuration to see the name of the ASA device (in the **Devices** pane on the right) associated with that configuration. You can also see the AnyConnect packages present in the ASA devices by clicking the edit button.

Connection Profile

CDO supports and reads the connection profiles defined in "AnyConnect Client VPN Access" of the ASA device. It does not support the "Clientless SSL VPN Access" configuration.

To see the connection profile attributes, perform the following:

Step 1 Expand **Default_RA_VPN_Configuration**.

Step 2 Click one of the connection profiles that you want and click **Edit**.

All the basic and advanced ASA RA VPN attributes can be seen in the **Connection Profile name and details** of the CDO RA VPN configuration page.

Note You can delete the default configuration (Select the default RA VPN configuration and in the **Actions** pane on the right, click **Remove**).

Primary Identity Source

- CDO reads the **Connection Aliases** and **Group URLs** attributes as **Group Alias** and **Group URL**.

Note
- The connection profiles configured with SAML, Multiple certificates and AAA, and Multiple certificates aren't read.
- The authentication server group with the interface and server group is not supported.

- CDO supports the AnyConnect connection profiles configured with "AAA", "AAA and certificate", and "Certificate only" authentication methods in **Primary Identity Source**.
- The **AAA Server Group** is read in CDO as **Primary Identity Source for User Authentication** in**Primary Identity Source** (You can see this attribute by selecting **AAA** or **AAA and Client Certificate** as the **Authentication Type**).
  - If the **AAA Server Group** has been configured something other than LOCAL, CDO reads and displays this attribute in the **Fallback Local Identity Source** field under **Primary Identity Source**. (You can see this attribute by selecting **AAA** as the authentication type).

    To learn more about the server group attributes read in CDO, see AAA Server Groups.

Secondary Identity Source

The **Secondary Identity Source** displays the secondary authentication attributes of the ASA device. To see these attributes, select **AAA** or **AAA and Client Certificate** as the authentication type, and click **View Secondary Identity Source**.

- The **Secondary Identity Source for User Authentication** displays the secondary authentication **Server Group** attribute.
  - If the **Server Group** has been configured something other than LOCAL, CDO reads and displays this attribute in the **Fallback Local Identity Source for Secondary**field under **Secondary Identity Source**.
- CDO doesn't support the **Attribute Server** and **Interface-Specific Authorization Server Groups** attributes.

To learn more about the server group attributes read in CDO, see AAA Server Groups.

Authorization Server

- The **Authorization Server** displays the authorization **Server Group** attribute.
- CDO doesn't support the authorization server group with interface and server group.

To learn more about the RADIUS server group attributes read in CDO, see RADIUS Server Group.

Accounting Server

The **Accounting Server** displays the accounting **Server Group** attribute. To learn more about the server group attributes read in CDO, see RADIUS Server Group.

Client Address Pool Assignment

CDO reads the **Client Address Assignment attributes** (**DHCP Servers**, **Client Address Pools**, and **Client IPv6 Address Pools**) as objects. (You can see these attributes in **Client Address Pool Assignment**). The DHCP server details are read as literals.

Note CDO doesn't support the IP address pools assigned on specific interfaces. However, these attributes can be seen in the ASA command-line interface (CLI).

AAA Server Groups

CDO represents an LDAP Server Group and its associated LDAP Servers as an **Active Directory Realm** object. For Active Directory (AD), a realm is equivalent to an Active Directory domain. Note that CDO does read the AD password for AD realm objects that are already present.

Step 1 In the CDO navigation bar on the left, click **Objects > ASA Objects**.

Step 2 Apply the **Active Directory Realms**filter to see this object.

Step 3 Select the Active Directory Realm object that you want and click **Edit** to see its details.

What to do next

You can see that the AD realm contains the associated AD server and its configuration. If there are multiple Active Directory (AD) servers for the AD realm, the AD servers need to be duplicates of each other and support the same AD domain. Therefore, the basic realm properties such as **Directory name**, **Directory Password**, and **Base Distinguished Name** must be the same across all AD servers associated with that AD realm. CDO displays a warning message in the Active Directory Realm object if these properties aren't the same. You have to correct these properties to make them consistent across the AD servers. If you continue without addressing this warning, CDO uses one of the AD server properties and applies it to other servers in that realm object.

RADIUS Server Group

The AAA RADIUS Server Group attributes of the ASA device are read in CDO as RADIUS Server Group objects.

Step 1 In the CDO navigation bar on the left, click **Objects** > **ASA Objects**.

Step 2 Apply the **RADIUS Server Group** filter to see this object.

Step 3 Select the object that you want and then click **Edit** to see its details.

- The **Enable dynamic authorization** in ASA is read in CDO as **Dynamic Authorization (for RA VPN only)**.
- The **Depletion** option in **Reactivation Mode** is read in CDO, and therefore the **Dead Time** value associated with depletion time is read in CDO. However, the **Timed** attribute is not read in CDO.
- CDO doesn't support **Accounting Mode**, **Timed**, **Enable interim accounting update**, **Enable interim accounting update**, and **Use authorization only mode**.

RADIUS Server

When CDO reads the Radius Servers from ASA, it creates a Radius server object specifies the name as "Name of the Radius server group_server name or IP address".

Step 1 In the CDO navigation bar on the left, click **Objects** > **ASA Objects**.

Step 2 Apply the **RADIUS Server** filter to see this object.

Step 3 Select the object that you want and then click **Edit** to see its details.

Group Policy

In the **Group Policy** section, click the drop-down to view the group policies associated with the device.

Attention CDO reads the group policies configured with tunneling protocol as **SSL VPN Client**.

CDO reads most of the group policy attributes configured in ASA. The information is displayed across the tabs in the RA VPN Group policy wizard. To see the details of group policies read from the ASA device, you need to perform the following:

Step 1 In the CDO navigation bar on the left, click **Objects > FTD Network Objects**.

Step 2 Filter for **RA VPN Group Policy**.

Step 3 Select the group policy associated with that device and click **Edit**.

What to do next

Note CDO doesn't support the Standard Access Control Lists (ACL) defined in the split tunneling in the ASA device. It supports the Extended Access Control Lists (ACL) and reads them as ACLs in the ASA policies. For more information, see ASA Remote Access VPN Group Policy Attributes. To see the policies, on the navigation bar, you can click **Policies** > **ASA Access Policies**.

To select the extended ACLs, perform the following:

- Click the **Split Tunneling** tab.
- Based on whether the traffic in ASA uses IPv4 or IPv6 addresses, select "Allow specified traffic over tunnel" or "Exclude networks specified below" from the corresponding drop-down list. Select the extended ACLs that are imported from ASA.

Create IP Address Pool

You can configure IPv4 and IPv6 IP address pools for ASAs to assign them to clients connecting remotely to your network using a VPN connection. The order in which you specify the pools is important. If you configure more than one address pool for a connection profile or group policy, the ASA uses them in the order in which you added them to the ASA.

To define the IPv4 address pool, provide the IP address range. An example of an IPv4 address pool is 10.10.147.100 - 10.10.147.177.

To define the IPv6 address pool, provide a starting IP address range, the address prefix, and the number of addresses configurable in the pool. An example of an IPv6 address pool is 2001:DB8:1::1.

If you assign addresses from a non-local subnet, we suggest that you add pools that fall on subnet boundaries to make adding routes for these networks easier.

Perform the following to create an IP address pool:

Step 1 In the CDO navigation bar on the left, click **Objects > ASA Objects**.

Step 2 Click the blue plus button + and select **ASA** > **Address Pool**.

Step 3 In the **Create IP Address Pool** dialog box enter this information:

- **Object Name**: Enter the name of the address pool. It can be up to 64 characters
- **IPv4 address pool**: Select this radio button to configure IPv4 address pools.
  - **IPv4 Address Range**: Enter the first IP address and last IP address available in each configured pool. For example, 10.10.147.100 - 10.10.147.177.

- **Mask**: Identifies the subnet on which this IP address pool resides.

- **IPv6 address pool**: Select this radio button to configure IPv6 address pools.
  - **IPv6 Address**: Enter the first IP address available in the configured pool and prefix length in bits in <address>/<prefix> format. For example, 2001:DB8:1::1/3.
  - **Number of Addresses**: Identifies the number of IPv6 addresses, starting at the IP Address, that are in the pool.

Step 4 Click **Save**.

Remote Access VPN Certificate-Based Authentication

The remote access VPN uses digital certificates for authenticating secure gateways and AnyConnect clients (endpoints) in the following scenarios:

Important CDO handles the installation of digital certificates on the VPN headends (ASA). It does not handle the installation of certificates on the AnyConnect client device. The administrator of your organization must handle it.

- Identify and authenticate the VPN headend device (ASA):

  VPN headends require an identity certificate to identify and authenticate themselves when the AnyConnect client requests a VPN connection. Using CDO, you must install the identity certificate on the device. See Installing an Identity Certificate Using PKCS12 or Certificate And Key. It is not mandatory to install the issuer's CA certificate on the AnyConnect client.

  While creating the Remote Access VPN configuration from CDO, assign the enrolled identity certificate to the outside interface of the device and download the configuration to the device. The identity certificate becomes fully operational on the outside interface of the device.

  When the AnyConnect client attempts to connect to VPN, the device authenticates itself by presenting its identity certificate to the AnyConnect client. The AnyConnect client verifies this identity certificate with its trusted CA certificate and trusts the certificate and thereby the device. If the CA certificate isn't installed on the AnyConnect client, the user must manually trust the device when prompted.

- Identify and authenticate the AnyConnect client:

  Note This applies when you use "Client Certificate Only" or "AAA and Client Certificate" as the authentication method in the connection profile of remote access VPN configuration. It does not apply for "AAA Only".

  Once the device is trusted, the AnyConnect client needs to authenticate itself to complete the VPN connection. You must install an identity certificate on the AnyConnect client and using CDO, install a trusted CA certificate on the device. These certificates must be issued from the same certificate authority. See Installing Trusted CA Certificate in ASA.

  The AnyConnect client presents its identity certificate and the device verifies this certificate with its trusted CA certificate and establishes the VPN connection.

Exempt Remote Access VPN Traffic from NAT

Configure NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. If you do not exempt VPN traffic from NAT, ensure that the existing NAT rules for the outside and inside interfaces do not apply to the remote access VPN pool of addresses. NAT exempt rules are manual static identity NAT rules for a given source/destination interface and network combination, but they are not reflected in the NAT policy, they are hidden. If you enable NAT Exempt, you must also configure the following.

- **Inside Interfaces**: Select the interfaces for the internal networks remote users will be accessing. NAT rules are created for these interfaces.
- **Inside Networks**: Select the network objects that represent internal networks remote users will be accessing. The networks list must contain the same IP types as the address pools you are supporting.

Before you begin

Create ASA network objects that match the configuration of the local IP address pools used in the connection profile and group policy of that device. These network objects must be assigned as the destination address and translated address when configuring the NAT rule. See Create an ASA Network Object.

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Use the **Inventory** filter and search field to find the ASA device for which you want to create the NAT rule.

Step 3 In the **Management** area of the details panel, click **NAT** NAT.

Step 4 Click + > **Twice NAT**.

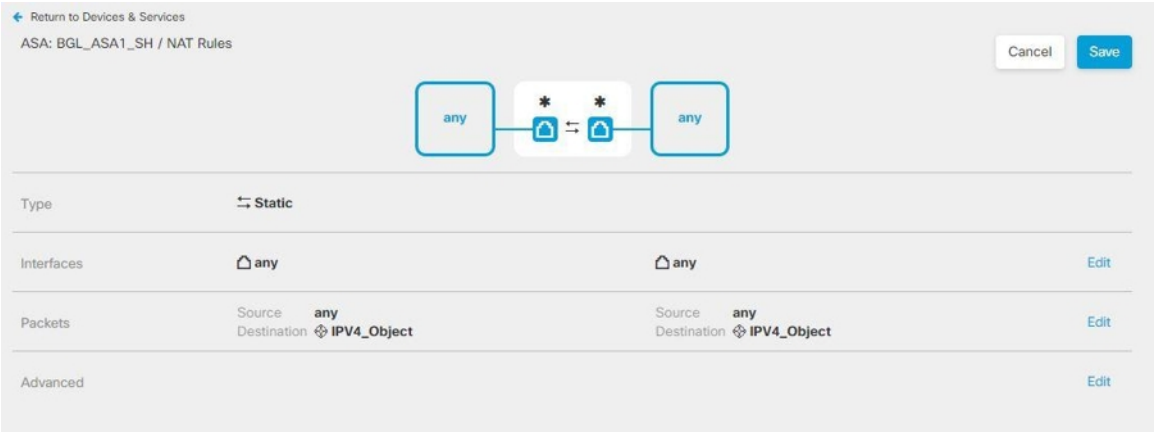
a. In section 1, select **Static.** Click **Continue**.

b. In section 2, select **Source Interface** = 'any' and **Destination Interface** = 'any'.Click **Continue**.

c. In section 3, select **Source Original Address** = 'any' and **Source Translated Address** = 'any'.

d. Select **Use Destination**.

1. **Destination Original Address** and **Source Translated Address**: Click **Choose** in the drop-down and select the network objects that match the configuration of the local IP address pools. In the below example, 'IPV4_Object' is the network object with the same configuration as the IPv4 address pool object used in the connection profile and group policy settings of the ASA (BGL_ASA1_SH) device.



2. Select **Disable proxy ARP for incoming packets**.
3. Click **Save**.
4. Repeat the process (from step 4) to create equivalent rules for each of the other network objects equivalent to IP address pools.

Step 5 Review and deploy configuration changes to the devices.

Install the AnyConnect Client Software on ASA

To complete a VPN connection, your users must install the AnyConnect client software. You can use your existing software distribution methods to install the software directly. Or, you can have users install the AnyConnect client directly from the ASA device.

Note Users must have Administrator rights on their workstations to install the software.

If you decide to have users initially install the software from the ASA device, inform users to perform the following steps:

Note Android and iOS users should download AnyConnect from the appropriate App Store.

Step 1 Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. You identify this interface when you configure the remote access VPN. The system prompts the user to log in.

Step 2 Log into the site. Users are authenticated using the directory server configured for the remote access VPN. Log in must be successful to continue. If the login is successful, the system determines if the user already has the required version of the AnyConnect client. If the AnyConnect client is absent from the user's computer or is down-level, the system automatically starts installing the AnyConnect software. When the installation is finished, AnyConnect completes the remote access VPN connection.

Modify ASA Remote Access VPN Configuration

When ASA devices are onboarded to CDO, it discovers and displays the pre-existing remote access VPN configurations from onboarded ASA devices. For more information, see Manage and Deploy Pre-existing ASA Remote Access VPN Configuration.

You can modify these configurations and download the new configuration to the device.

Step 1 In the CDO navigation bar at the left, click **VPN** > **Remote Access VPN Configuration**.

Step 2 If you want to add or remove group policies to the VPN configuration, click the VPN configuration associated with the onboarded ASA device. In the Actions pane on the left, click **Group Policies**.

a) Click the blue + icon and configure the selections and click **Select**.
b) Click Save. You can also Create ASA Remote Access VPN Group Policies.

Step 3 Click the VPN configuration, and in the **Actions** pane on the left, click **Edit**.

The wizard lists the ASA device associated with the configuration.

a) You can modify the following details in the same fashion as it was created:

- Change the name of the remote access VPN configuration.
- Click the three dots appearing in the row that shows the device details and click **Edit**.

For more information, see Create ASA Remote Access VPN Configuration, on page 40

Step 4 Click **OK**.

Step 5 Preview and Deploy Configuration Changes for All Devices

Modify ASA Connection Profile

Step 1 In the CDO navigation bar at the left, click **VPN** > **Remote Access VPN Configuratio**n.

Step 2 Expand the VPN configuration associated with the onboarded ASA device, and select a connection profile.

Step 3 In the **Actions** pane on the left, click **Edit**.

Step 4 Edit the values in the same fashion as it was created and click **Done**.

For more information, see Configure ASA Remote Access VPN Connection Profile, on page 44

Step 5 Preview and Deploy Configuration Changes for All Devices

Upload RA VPN AnyConnect Client Profile

The Remote Access VPN AnyConnect Client Profile is a group of configuration parameters stored in a file. There are different AnyConnect client profiles containing configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, AMP Enabler, ISE posture, Network Visibility, Customer Feedback Experience profiles, Umbrella roaming security, and Web Security.

CDO allows uploading of these profiles as objects which can be used in the group policy later.

- **AnyConnect VPN Profile** — AnyConnect client profiles are downloaded to clients along with the VPN AnyConnect client software. These profiles define many client-related options, such as auto-connect on startup and auto-reconnect, and whether the end-user can change the option from the AnyConnect client preferences and advanced settings. CDO supports the XML file format.
- **AMP Enabler Service Profile** — The profile is used for the AnyConnect AMP Enabler. The AMP Enabler and this profile are pushed to the endpoints from FDM-managed device when a remote access VPN user connects to the VPN. CDO supports XML and ASP file formats.
- **Feedback Profile** — You can add a Customer Experience Feedback profile and select this type to receive information about the features and modules customers have enabled and used. CDO supports the FSP file format.

- **ISE Posture Profile** — Choose this option if you add a profile file for the AnyConnect ISE Posture module. CDO supports XML and ISP file formats.
- **Network Access Manager Service Profile** — Configure and add the NAM profile file using the Network Access Manager profile editor. CDO supports XML and NSP file formats.
- **Network Visibility Service Profile** — Profile file for AnyConnect Network Visibility module. You can create the profile using the NVM profile editor. CDO supports XML and NVMSP file formats.
- **Umbrella Roaming Security Profile** — You must select this file type if you deploy the Umbrella Roaming Security module. CDO supports XML and JSON file formats.
- **Web Security Service Profile** — Select this file type when you add a profile file for the Web security module. CDO supports XML, WSO, and WSP file formats.

Before you begin

Use the suitable GUI-based AnyConnect profile editors to create the profiles you need. You can download the profile editors from Cisco Software Download Center in the AnyConnect Secure Mobility Client category and install the AnyConnect "Profile Editor - Windows / Standalone installer (MSI)." The profile editor installer contains stand-alone versions of the profile editors. The installation file is for Windows only and has the file name anyconnect-profileeditor-win-<version>-k9.msi, where <version> is the AnyConnect version. For example, anyconnect-profileeditor-win-4.3.04027-k9.msi. You must also install Java JRE 1.6 (or higher) before installing the profile editor.

Except for the Umbrella Roaming Security profile editor, this package contains all the profile editors required for creating the modules. For detailed information, see the *AnyConnect Profile Editor* chapter in the appropriate release of the Cisco AnyConnect Secure Mobility Client Administrator Guide for details. Download the Umbrella Roaming Security profile separately from the Umbrella dashboard. For detailed information, see the "Download the AnyConnect Roaming Security Profile from the Umbrella Dashboard" section of the "Umbrella Roaming Security" chapter in the Cisco Umbrella User Guide.

Step 1 In the CDO navigation bar at the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button.

Step 3 Click **RA VPN Objects (ASA & FDM)** > **AnyConnect Client Profile**.

Step 4 In the **Object Name** field, enter a name for the AnyConnect client profile.

Step 5 Click **Browse** and select the file you created using the Profile Editor.

Step 6 Click **Open** to upload the profile.

Step 7 Click **Add** to add the object.

Related information:

- Associate the client modules with the AnyConnect VPN profile in the RA VPN group policies window. See Create ASA Remote Access VPN Group Policies .

Note The client module association is supported by all ASA versions and FDM running software version 6.7 or later.

Verify ASA Remote Access VPN Configuration

After you configure the remote access VPN and deploy the configuration to the device, verify that you can make remote connections.

Step 1 From an external network, establish a VPN connection using the AnyConnect client. Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. If necessary, install the client software and complete the connection. See Install the AnyConnect Client Software on ASA . If you configured group URLs, also try those URLs.

Step 2 In the **Inventory** page, select the device (FTD or ASA) you want to verify and click **Command Line Interface** under **Device Actions**.

Step 3 Use the **show vpn-sessiondb** command to view summary information about current VPN sessions.

Step 4 The statistics should show your active AnyConnect Client session, and information on cumulative sessions, the peak concurrent number of sessions, and inactive sessions. Following is sample output from the command.

```
> show vpn-sessiondb
--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
                              Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------


   Total Active and Inactive    :      1             Total Cumulative :     50
   Device Total VPN Capacity    :  10000
   Device Load                  :     0%
   ---------------------------------------------------------------------------

   ---------------------------------------------------------------------------
   Tunnels Summary
   ---------------------------------------------------------------------------
                                Active : Cumulative : Peak Concurrent
                              ----------------------------------------------
   Clientless                 :      0 :          1 :               1
   AnyConnect-Parent          :      1 :         49 :               3
   SSL-Tunnel                 :      1 :         46 :               3
   DTLS-Tunnel                :      1 :         46 :               3
   ---------------------------------------------------------------------------
   Totals                     :      3 :        142
   ---------------------------------------------------------------------------

   ---------------------------------------------------------------------------
   IPv6 Usage Summary
   ---------------------------------------------------------------------------
                                Active : Cumulative : Peak Concurrent
                              ----------------------------------------------
   AnyConnect SSL/TLS/DTLS    :        :            :
     Tunneled IPv6            :      1 :         20 :           2
   ---------------------------------------------------------------------------
```

Step 5 Use the **show vpn-sessiondb anyconnect** command to view detailed information about current AnyConnect VPN sessions. Detailed information includes encryption used, bytes transmitted and received, and other statistics. If you use your VPN connection, you should see the bytes transmitted/received numbers change as you re-issue this command.

Step 6 Use the **show vpn-sessiondb anyconnect** command to view detailed information about current AnyConnect VPN sessions. Detailed information includes encryption used, bytes transmitted and received, and other statistics. If you use your VPN

connection, you should see the bytes transmitted/received numbers change as you re-issue this command.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

View ASA Remote Access VPN Configuration Details

Step 1 In the CDO navigation bar at the left, click **VPN** > **ASA/FDM Remote Access VPN Configuration**.

Step 2 Click on a VPN configuration object present. The group shows summary information on how many connection profiles and group policies are currently configured.

- Expand the remote access VPN configuration to view all connection profiles associated with them.
  - Click the add + button to add a new connection profile.
  - Click the view button () to open a summary of the connection profile and connection instructions. Under **Actions**, you can click **Edit** to modify the changes.
- You can click one of the following options under **Actions** to perform additional tasks:
  - Click **Group Policies** to assign/add group policies.
  - Click a configuration object or connection profile that you no longer need and click **Remove** to delete.

Monitor Remote Access Virtual Private Network Sessions

Remote access Virtual Private Network provides secure connections for remote users, such as mobile users or telecommuters. Monitoring these connections provides important indicators of connection and user session performance at a glance. Cisco Defense Orchestrator (CDO) remote access VPN monitoring capabilities enable you to determine quickly whether remote access VPN problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users. You can also disconnect remote access VPN sessions as needed.

The Remote Access Virtual Private Monitoring page provides the following information:

- A list of active and historical sessions for up to a year.

- Shows intuitive graphical visuals to provide at-a-glance views from all active VPN headends managed by CDO.
- The live session screen shows the most used operating system and VPN connection profile in the CDO tenant. It also shows the average session duration and data uploaded and downloaded.
- Filtering capabilities to narrow your search based on criteria such as device type, device names, session length, and the amount of data transmitted and received.

Related Information:

- Monitor Live AnyConnect Remote Access VPN Sessions, on page 64
- Monitor Historical AnyConnect Remote Access VPN Sessions, on page 66
- Search and Filter Remote Access VPN Sessions
- Customize the Remote Access VPN Monitoring View
- Export Remote Access VPN Sessions to a CSV File
- Disconnect all Active RA VPN Sessions of a User

Monitor Live AnyConnect Remote Access VPN Sessions

You can monitor real-time data from active AnyConnect remote access VPN sessions on the devices. This data is automatically refreshed every 10 minutes. If you want to retrieve the latest list of sessions at any point, you click the reload icon appearing on the right corner of the screen.

Before you begin

- Onboard the remote access VPN head-ends to CDO.
- Ensure that the connectivity status of the devices you want to monitor live data is "Online" on the **Inventory** page.

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Alternatively, you can click **View Active Remote Access VPN Sessions**on the CDO home page or navigate to **VPN** > **Remote Access VPN** and click the icon on the top-right corner of the screen.

Step 2 Click **RA VPN**.

Step 3 Click **Live**.

You can Search and Filter Remote Access VPN Sessions to narrow down your search based on criteria such as device type, session length, and upload and download data range.

Note The **Data TX** and **Data RX** information are not available for FTD.

View Live Remote Access VPN Data

The live data is presented both in the dashboard and tabular form.

Dashboard View

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard.

The dashboard provides at-a-glance views from all active VPN headends managed by CDO.

- **Breakdown (All Devices)**: Shows a total number of live sessions. It also shows a pie chart that is divided into four arc lengths. It illustrates the percentage of VPN sessions of the top three devices with the highest number of sessions. The remaining arc length represents the aggregate of other devices.
- Shows most used operating system and connection profile in the CDO tenant.
- Shows average session duration and data uploaded and downloaded.
- **Active Sessions by Country**: Shows an interactive heat map of the location of the users connected to your RA VPN headends.
  - Countries from which users have connected are shown in progressively darker shades of blue, depending on the relative proportion of the sessions established from that country — the darker the blue color means more sessions are established from that country.
  - The legend at the bottom of the map provides a scale that indicates the correlation between the number of sessions in a country and the shade of blue used to color the country.
  - Hover the mouse pointer on the map to see the country's name and the total number of active user sessions established from that country.
  - Hover the mouse pointer on the table to see the country's location and the total number of active user sessions on the map.

Tabular View

Click the **Show Tabular View** icon on the top right corner of the screen to view the data in tabular format.

The tabular form provides a complete list of VPN users connected presently.

- The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

Important CDO applies a standard filter to the live data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the custom filters are not supported in the visual dashboard view. Click **Clear** to remove all filters you have applied. You cannot remove the standard filter.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Monitor Historical AnyConnect Remote Access VPN Sessions

You can monitor the historical data from AnyConnect Remote Access VPN sessions recorded over the last three months.

Before you begin

- Onboard the RA VPN head-ends to CDO.

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Alternatively, you can click **View Active Remote Access VPN Sessions** on the CDO home page or navigate to **VPN** > **Remote Access VPN** and click the icon in the top-right corner.

Step 2 Click **RA VPN**.

Step 3 Click **Historical**.

CDO displays the historical data from the Remote Access VPN sessions recorded over the last three months.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range.

The **Data TX** and **Data RX** information are not available for FTD.

View Historical Remote Access VPN Data

The historical data is presented both in the dashboard and tabular form.

Dashboard View

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard. You will see the dashboard view along with the tabular view.

The dashboard provides at-a-glance views from all active VPN headends managed by CDO. It provides a bar graph showing the VPN sessions recorded for all devices in the last 24 hours, 7 days, and 30 days. You can select the duration from the drop-down. You can hover over on individual bars to see the date and the total number of sessions on that day.

Tabular View

You have to click the **Show Tabular View** icon appearing at the top right corner of the screen to see only the tabular view. The tabular form provides a complete list of VPN users connected over the last three months.

The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

Important CDO applies a standard filter to the historical data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the dashboard is not supported for custom filters. Clearing the newly applied filters relaunches the dashboard (On the screen, click **Clear** to remove manually applied filters). You cannot remove the standard filter.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as session date and time range, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Search and Filter Remote Access VPN Sessions

Search

Use the search bar functionality to find remote access VPN sessions. Start typing device name, IP address, or serial number in the search bar, and remote access VPN sessions that fit the search criteria will be displayed. Search is not case-sensitive.

Filter

Use the filter sidebar to find remote access VPN sessions based on criteria such as session time range, session length, and upload and download data range. The filter functionality is available to both live and historical views.

- **Filter by Devices**: Select one or all devices from the **All Types** tab to view sessions from selected devices. The window also categorizes the devices based on their type and displays them under the corresponding tabs.
- **Sessions Time Range** (Applicable only for historical data): View historical sessions from a specified date and time range. Note that you can view data recorded over the last three months.
- **Sessions Length**: View sessions based on a specified session's duration length. Set the time unit (hours, minutes, or seconds) and specify the minimum and maximum duration length by moving the slider. You can also specify the length in the provided fields.
- **Upload (TX)**: View sessions based on a specified amount of data uploaded or transferred to the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.
- **Download (RX)**: View sessions based on a specified amount of data downloaded or received from the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.

Customize the Remote Access VPN Monitoring View

You can modify the remote access VPN monitoring view in both live and historical modes to only include column headers that apply to the view you want. Click the column filter icon located to the right of the columns and select or deselect the columns you want.

CDO remembers your selection the next time you sign in to CDO.

Export Remote Access VPN Sessions to a CSV File

You can export the remote access VPN sessions of one or more devices to a comma-separated value (.csv) file. You can open the .csv file in a spreadsheet application such as Microsoft Excel to sort and filter the items on your list. This information helps you to analyze the remote access VPN sessions. Every time you export the sessions, CDO creates a new .csv file, where the file created has a date and time in its name.

CDO can export a maximum of 100,000 active sessions to the CSV file. If the total number of sessions from all devices exceeds the maximum limit, you can use the **View By Device** filter and generate reports for individual devices.

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Step 2 In the **View By Devices** area, select one of the following:

- **All Devices** to export active sessions from all devices listed below it.
- Click on a device that you want to export sessions of that device.

Step 3 Click the icon on the top right corner. CDO exports the rules you see on the screen to a .csv file.

Step 4 Open the .csv file in a spreadsheet application to sort and filter the results.

Disconnect Remote Access VPN Sessions of an ASA User

You can terminate all active remote access VPN sessions of all users on the ASA device. You can perform this task in both live and historical modes.

CDO provides a VPN Sessions Manager user role to allow users to view and terminate VPN sessions. See User Roles for more information.

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Step 2 In the **View By Devices** area, click on the ASA device that you want to end all active sessions on that device.

Step 3 Click **Terminate All Sessions** appearing in the top-right corner.

Step 4 Click **Yes, Terminate All Sessions** to confirm your selection.

Disconnect all Active RA VPN Sessions of a User

CDO terminates all of the user's active RA VPN sessions on that ASA device when you disconnect a user. You can perform this task in both live and historical modes.

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Step 2 Search for a user whose sessions you want to disconnect. You can type the search criteria into the **Search** bar.

Step 3 Click on an active session, and in the **Actions** pane on the right, click the **Terminate all RA VPN sessions for this user** link.