Remote Access VPNs for Firepower Threat Defense

- Firepower Threat Defense Remote Access VPN Overview, on page 1
- License Requirements for Remote Access VPN, on page 7
- Requirements and Prerequisites for Remote Access VPN, on page 7
- Guidelines and Limitations for Remote Access VPNs, on page 8
- Configuring a New Remote Access VPN Connection, on page 10
- Setting Target Devices for a Remote Access VPN Policy, on page 17
- Additional Remote Access VPN Configurations, on page 17
- Customizing Remote Access VPN AAA Settings, on page 43
- Remote Access VPN Examples, on page 59

Firepower Threat Defense Remote Access VPN Overview

Firepower Threat Defense provides secure gateway capabilities that support remote access SSL and IPsec-IKEv2 VPNs. The full tunnel client, AnyConnect Secure Mobility Client, provides secure SSL and IPsec-IKEv2 connections to the security gateway for remote users. AnyConnect is the only client supported on endpoint devices for remote VPN connectivity to Firepower Threat Defense devices. The client gives remote users the benefits of an SSL or IPsec-IKEv2 VPN client without the need for network administrators to install and configure clients on remote computers. The AnyConnect mobile client for Windows, Mac, and Linux is deployed from the secure gateway upon connectivity. The AnyConnect apps for Apple iOS and Android devices are installed from the platform app store.

Use the Remote Access VPN Policy wizard in the Firepower Management Center to quickly and easily set up SSL and IPsec-IKEv2 remote access VPNs with basic capabilities. Then, enhance the policy configuration if desired and deploy it to your Firepower Threat Defense secure gateway devices.

You can configure the following settings using the remote access VPN policy:

- Two-Factor Authentication, on page 54
- Secondary Authentication, on page 57
- Configure LDAP or Active Directory for Authorization, on page 47
- Manage Password Changes over VPN Sessions, on page 46
- Send Accounting Records to the RADIUS Server, on page 48

- Override the Selection of Group Policy or Other Attributes by the Authorization Server , on page 50
  - Deny VPN Access to a User Group, on page 50
  - Restrict Connection Profile Selection for a User Group, on page 51

You can use the following examples to allocate limited bandwidth to VPN users and to use VPN identify for user-id based access control rules:

- How to Limit AnyConnect Bandwidth Per User, on page 59
- How to Use VPN Identity for User-id Based Access Control Rules, on page 61

Remote Access VPN Features

The following section describes the features of Firepower Threat Defense remote access VPN:

- SSL and IPsec-IKEv2 remote access using the Cisco AnyConnect Secure Mobility Client.
- Firepower Management Center supports all combinations such as IPv6 over an IPv4 tunnel.
- Configuration support on both FMC and FDM. Device-specific overrides.
- Support for both Firepower Management Center and Firepower Threat Defense HA environments.
- Support for multiple interfaces and multiple AAA servers.
- Rapid Threat Containment support using RADIUS CoA or RADIUS dynamic authorization.
- VPN load balancing.

AAA

- Server authentication using self-signed or CA-signed identity certificates.
- AAA username and password-based remote authentication using RADIUS server or LDAP or AD.
- RADIUS group and user authorization attributes, and RADIUS accounting.
- Double authentication support using an additional AAA server for secondary authentication.
- NGFW Access Control integration using VPN Identity.

VPN Tunneling

- Address assignment
- Split tunneling
- Split DNS
- Client Firewall ACLs
- Session Timeouts for maximum connect and idle time

Monitoring

- New VPN Dashboard Widget showing VPN users by various characteristics such as duration and client application.
- Remote access VPN events including authentication information such as username and OS platform.
- Tunnel statistics available using the Firepower Threat Defense Unified CLI.

AnyConnect Components

AnyConnect Secure Mobility Client Deployment

Your remote access VPN Policy can include the AnyConnect Client Image and an AnyConnect Client Profile for distribution to connecting endpoints. Or, the client software can be distributed using other methods. See the *Deploy AnyConnect* chapter in the appropriate version of the Cisco AnyConnect Secure Mobility Client Administrator Guide.

Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL or IPsec-IKEv2 VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, remote users must enter the URL in the form https://*address*. After the user enters the URL, the browser connects to that interface and displays the login screen.

After a user logs in, if the secure gateway identifies the user as requiring the VPN client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure connection, and either remains or uninstalls itself (depending on the security appliance configuration) when the connection stops. In the case of a previously installed client, after login, the Firepower Threat Defense security gateway examines the client version and upgrades it as necessary.

AnyConnect Secure Mobility Client Operation

When the client negotiates a connection with the security appliance, the client connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). 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.

When an IPsec-IKEv2 VPN client initiates a connection to the secure gateway, negotiation consists of authenticating the device through Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth). The group profile is pushed to the VPN client and an IPsec security association (SA) is created to complete the VPN.

AnyConnect Client Profile and Editor

An AnyConnect client profile is a group of configuration parameters, stored in an XML file that the VPN client uses to configure its operation and appearance. These parameters (XML tags) include the names and addresses of host computers and settings to enable more client features.

You can configure a profile using the AnyConnect Profile Editor. This editor is a convenient GUI-based configuration tool that is available as part of the AnyConnect software package. It is an independent program that you run outside of the Firepower Management Center.

Remote Access VPN Authentication

Remote Access VPN Server Authentication

Firepower Threat Defense secure gateways always use certificates to identify and authenticate themselves to the VPN client endpoint.

While setting up the remote access VPN configuration using the wizard, you can enroll the selected certificate on the targeted Firepower Threat Defense device. In the wizard, under **Access & Certificate** phase, select "Enroll the selected certificate object on the target devices" option. The certificate enrollment gets automatically initiated on the specified devices. As you complete the Remote Access VPN configuration, you can view the status of the enrolled certificate under the device certificate homepage. The status provides a clear standing as to whether the certificate enrollment was successful or not. Your Remote Access VPN configuration is now fully completed and ready for deployment.

Obtaining a certificate for the secure gateway, also known as PKI enrollment, is explained in Firepower Threat Defense Certificate-Based Authentication. This chapter contains a full description of configuring, enrolling, and maintaining gateway certificates.

Remote Access VPN Client AAA

For both SSL and IPsec-IKEv2, remote user authentication is done using usernames and passwords only, certificates only, or both.

Note If you are using client certificates in your deployment, they must be added to your client's platform independent of the Firepower Threat Defense or Firepower Management Center. Facilities such as SCEP or CA Services are not provided to populate your clients with certificates.

AAA servers enable managed devices acting as secure gateways to determine who a user is (authentication), what the user is permitted to do (authorization), and what the user did (accounting). Some examples of the AAA servers are RADIUS, LDAP/AD, TACACS+, and Kerberos. For Remote Access VPN on Firepower Threat Defense devices, AD, LDAP, and RADIUS AAA servers are supported for authentication.

Only RADIUS servers can be configured and used for authorization and accounting servers.

Refer to the section Understanding Policy Enforcement of Permissions and Attributes to understand more about remote access VPN authorization.

Before you add or edit the Remote Access VPN policy, you must configure the Realm and RADIUS server groups you want to specify. For more information, see Create a Realm and RADIUS Server Groups.

Without DNS configured, the device cannot resolve AAA server names, named URLs, and CA Servers with FQDN or Hostnames, it can only resolve IP addresses.

The login information provided by a remote user is validated by an LDAP or AD realm or a RADIUS server group. These entities are integrated with the Firepower Threat Defense secure gateway.

Note If users authenticate with RA VPN using Active Directory as the authentication source, users must log in using their username; the format `domain\username` or `username@domain` fails. (Active Directory refers to this username as the *logon name* or sometimes as `sAMAccountName`.) For more information, see User Naming Attributes on MSDN.

If you use RADIUS to authenticate, users can log in with any of the preceding formats.

Once authenticated via a VPN connection, the remote user takes on a *VPN Identity*. This VPN Identity is used by *identity policies* on the Firepower Threat Defense secure gateway to recognize and filter network traffic belonging to that remote user.

Identity policies are associated with access control policies, which determine who has access to network resources. It is in this way that the remote user blocked or allowed to access your network resources.

For more information, see the About Identity Policies and Access Control Policies sections.

Related Topics

Configure AAA Settings for Remote Access VPN, on page 20

Understanding Policy Enforcement of Permissions and Attributes

The Firepower Threat Defense device supports applying user authorization attributes (also called user entitlements or permissions) to VPN connections from an external authentication server and/or authorization AAA server (RADIUS) or from a group policy on the Firepower Threat Defense device. If the Firepower Threat Defense device receives attributes from the external AAA server that conflicts with those configured on the group policy, then attributes from the AAA server always take the precedence.

The Firepower Threat Defense device applies attributes in the following order:

1. **User attributes on the external AAA server**—The server returns these attributes after successful user authentication and/or authorization.
2. **Group policy configured on the Firepower Threat Defense device**—If a RADIUS server returns the value of the RADIUS Class attribute IETF-Class-25 (OU= group-policy) for the user, the Firepower Threat Defense device places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.
3. **Group policy assigned by the Connection Profile (also known as Tunnel Group)**—The Connection Profile has the preliminary settings for the connection, and includes a default group policy applied to the user before authentication.

Note The Firepower Threat Defense device does not support inheriting system default attributes from the default group policy, *DfltGrpPolicy*. The attributes on the group policy assigned to the connection profile are used for the user session, if they are not overridden by user attributes or the group policy from the AAA server as indicated above.

Related Topics

Configure AAA Settings for Remote Access VPN, on page 20

Understanding AAA Server Connectivity

LDAP, AD, and RADIUS AAA servers must be reachable from the Firepower Threat Defense device for your intended purposes: user-identity handling only, VPN authentication only, or both activities. AAA servers are used in remote access VPN for the following activities:

- **User-identity handling**— the servers must be reachable over the Management interface.

  On the Firepower Threat Defense device, the Management interface has a separate routing process and configuration from the regular interfaces used by VPN.

- **VPN authentication**—the servers must be reachable over one of the regular interfaces: the Diagnostic interface or a data interface.

  For regular interfaces, two routing tables are used. A management-only routing table for the Diagnostic interface as well as any other interfaces configured for management-only, and a data routing table used for data interfaces. When a route-lookup is done, the management-only routing table is checked first, and then the data routing table. The first match is chosen to reach the AAA server.

Note If you place a AAA server on a data interface, be sure the management-only routing policies do not match traffic destined for a data interface. For example, if you have a default route through the Diagnostic interface, then traffic will never fall back to the data routing table. Use the **show route management-only** and **show route** commands to verify routing determination.

For both activities on the same AAA servers, in addition to making the servers reachable over the Management interface for user-identity handling, do one of the following to provide VPN authentication access to the same AAA servers:

- Enable and configure the Diagnostic interface with an IP address on the same subnet as the Management interface, and then configure a route to the AAA server through this interface. The Diagnostic interface access will be used for VPN activity, the Management interface access for identity handling.

Note When configured this way, you cannot also have a data interface on the same subnet as the Diagnostic and Management interfaces. If you want the Management interface and a data interface on the same network, for example when using the device itself as a gateway, you will not be able to use this solution because the Diagnostic interface must remain disabled.

- Configure a route through a data interface to the AAA server. The data interface access will be used for VPN activity, the Management interface access for user-identity handling.

For more information about various interfaces, see Regular Firewall Interfaces for Firepower Threat Defense.

After deployment, use the following CLI commands to monitor and troubleshoot AAA server connectivity from the Firepower Threat Defense device:

- **show aaa-server** to display AAA server statistics.
- **show route management-only** to view the management-only routing table entries.

- **show network** and **show network-static-routes** ro view the Management interface default route and static routes.
- **show route** to view data traffic routing table entries.
- **ping system** and **traceroute system** to verify the path to the AAA server through the Management interface.
- **ping interface** *ifname* and **traceroute** *destination* to verify the path to the AAA server through the Diagnostic and data interfaces.
- **test aaa-server authentication** and **test aaa-server authorization** to test authentication and authorization on the AAA server.
- **clear aaa-server statistics** *groupname* or **clear aaa-server statistics protocol** *protocol* to clear AAA server statistics by group or protocol.
- **aaa-server** *groupname* **active host** *hostname* to activate a failed AAA server, or **aaa-server** *groupname* **fail host** *hostname* to fail a AAA server.
- **debug ldap level**, **debug aaa authentication**, **debug aaa authorization**, and **debug aaa accounting**.

License Requirements for Remote Access VPN

FTD License

FTD remote access VPN requires Strong Encryption and one of the following licenses for AnyConnect:

- AnyConnect Plus
- AnyConnect Apex
- AnyConnect VPN Only

Requirements and Prerequisites for Remote Access VPN

Model Support

FTD

Supported Domains

Any

User Roles

Admin

Guidelines and Limitations for Remote Access VPNs

Remote Access VPN Policy Configuration

- You can add a new remote access VPN policy only by using the wizard. You must proceed through the entire wizard to create a new policy; the policy will not be saved if you cancel before completing the wizard.
- Two users must **not** edit a remote access VPN policy at the same time; however, the web interface does not prevent simultaneous editing. If this occurs, the last saved configuration persists.
- Moving a Firepower Threat Defense device from one domain to another domain is not possible if a remote access VPN policy is assigned to that device.
- Firepower 9300 and 4100 series in cluster mode do not support remote access VPN configuration.
- Remote access VPN connectivity could fail if there is an FTD NAT rule is misconfigured.
- Whenever IKE ports 500/4500 or SSL port 443 is in use or when there are some PAT translations that are active, the AnyConnect IPSec-IKEv2 or SSL remote access VPN cannot be configured on the same port as it fails to start the service on those ports. These ports must not be used on the Firepower Threat Defense device before configuring Remote Access VPN.
- While configuring remote access VPNs using the wizard, you can create in-line certificate enrollment objects, but you cannot use them to install the identity certificate. Certificate enrollment objects are used for generating the identity certificate on the Firepower Threat Defense device being configured as the remote access VPN gateway. Install the identity certificate on the device before deploying the remote access VPN policy to the device. For more information about how to install the identity certificate based on the certificate enrollment object, see The Object Manager.
- After you change the remote access VPN policy configurations, re-deploy the changes to the Firepower Threat Defense devices. The time it takes to deploy configuration changes depends on multiple factors such as complexity of the policies and rules, type and volume of configurations you send to the device, and memory and device model. Before deploying remote access VPN policy changes, review the Best Practices for Deploying Configuration Changes.
- The ECMP zone interfaces cannot be used in Remote Access VPN (for both IPsec and SSL). Deployment of RA VPN configuration fails if all the RA VPN interfaces that belong to security zones or interface groups also belong to one or more ECMP zones. However, if some of the RA VPN interfaces belonging to the security zones or interface groups also belongs to one or more ECMP zones, deployment of the RA VPN configuration succeeds excluding those interfaces.

Concurrent VPN Sessions Capacity Planning (Hardware Models)

The maximum concurrent VPN sessions are governed by platform-specific limits and have no dependency on the license. There is a maximum limit to the number of concurrent remote access VPN sessions allowed on a device based on the device model. This limit is designed so that system performance does not degrade to unacceptable levels. Use these limits for capacity planning.

Device Model	Maximum Concurrent Remote Access VPN Sessions
Firepower 2110	1500

Device Model	Maximum Concurrent Remote Access VPN Sessions
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10000

For capacity of other hardware models, contact your sales representative.

Note The Firepower Threat Defense device denies the VPN connections once the maximum session limit per platform is reached. The connection is denied with a syslog message. Refer the syslog messages %ASA-4-113029 and %ASA-4-113038 in the syslog messaging guide. For more information, see http://www.cisco.com/c/en/us/td/docs/security/asa/syslog-guide/syslogs.html

Controlling Cipher Usage for VPN

To prevent use of ciphers greater than DES, pre-deployment checks are available at the following locations in the Firepower Management Center:

Devices > **Platform Settings** > **SSL Settings**

Devices > **VPN** > **Remote Access** > **Advanced** > **IPsec**

For more information about SSL settings and IPsec, see Configure SSL Settings and Configure Remote Access VPN IPsec/IKEv2 Parameters, on page 42.

Authentication, Authorization, and Accounting

- Firepower Threat Defense device supports authentication of remote access VPN users using system-integrated authentication servers only; a local user database is not supported.
- The LDAP or AD authorization and accounting are not supported for remote access VPN. Only RADIUS server groups can be configured as authorization or accounting servers in the remote access VPN policy.
- Configure DNS on each device in the topology in to use remote access VPN. Without DNS, the device cannot resolve AAA server names, named URLs, and CA Servers with FQDN or Hostnames; it can only resolve IP addresses.

  You can configure DNS using the Platform Settings. For more information, see Configure DNS and DNS Server Group Objects.

Client Certificates

- If you are using client certificates in your deployment, they must be added to your client's platform independent of the Firepower Threat Defense or Firepower Management Center. Facilities such as SCEP or CA Services are not provided to populate your clients with certificates.

Unsupported Features of AnyConnect

The only supported VPN client is the Cisco AnyConnect Secure Mobility Client. No other clients or native VPNs are supported. Clientless VPN is not supported for VPN connectivity; it is only used to deploy the AnyConnect client using a web browser.

The following AnyConnect features are not supported when connecting to an Firepower Threat Defense secure gateway:

- Secure Mobility, Network Access Management, and all other AnyConnect modules and their profiles beyond the core VPN capabilities and the VPN client profile.
- Posture variants such as Hostscan and Endpoint Posture Assessment, and any Dynamic Access Policies based on the client posture.
- AnyConnect Customization and Localization support. The Firepower Threat Defense device does not configure or deploy the files necessary to configure AnyConnect for these capabilities.
- Custom Attributes for the AnyConnect Client are not supported on the Firepower Threat Defense. Hence all features that make use of Custom Attributes are not supported, such as Deferred Upgrade on desktop clients and Per-App VPN on mobile clients.
- Local authentication; VPN users cannot be configured on the Firepower Threat Defense secure gateway.

  Local CA, the secure gateway cannot act as a Certificate Authority.
- Single Sign-on using SAML 2.0.
- TACACS, Kerberos (KCD Authentication and RSA SDI).
- LDAP Authorization (LDAP Attribute Map).
- Browser Proxy.
- VPN load balancing.

Configuring a New Remote Access VPN Connection

This section provides instructions to configure a new remote access VPN policy with Firepower Threat Defense devices as VPN gateways and Cisco AnyConnect as the VPN client.

	Do This	More Info
Step 1	Review the guidelines and prerequisites.	Guidelines and Limitations for Remote Access VPNs, on page 8 Prerequisites for Configuring Remote Access VPN, on page 11
Step 2	Create a new remote access VPN policy using the wizard.	Create a New Remote Access VPN Policy, on page 12
Step 3	Update the access control policy deployed on the device.	Update the Access Control Policy on the Firepower Threat Defense Device, on page 13

	Do This	More Info
Step 4	(Optional) Configure a NAT exemption rule if NAT is configured on the device.	(Optional) Configure NAT Exemption, on page 14
Step 5	Configure DNS.	Configure DNS, on page 15
Step 6	Add an AnyConnect Client Profile.	Add an AnyConnect Client Profile XML File, on page 15
Step 7	Deploy the remote access VPN policy.	Deploy Configuration Changes
Step 8	(Optional) Verify the remote access VPN policy configuration.	Verify the Configuration, on page 16

Prerequisites for Configuring Remote Access VPN

- Deploy Firepower Threat Defense devices and configure Firepower Management Center to manage the device with required licenses with export-controlled features enabled. For more information, see VPN Licensing.
- Configure the certificate enrollment object that is used to obtain the identity certificate for each Firepower Threat Defense device that act as a remote access VPN gateway.
- Configure the RADIUS server group object and any AD or LDAP realms being used by remote access VPN policies.
- Ensure that the AAA Server is reachable from the Firepower Threat Defense device for the remote access VPN configuration to work. Configure routing (at **Devices > Device Management > Edit Device > Routing**) to ensure connectivity to the AAA servers.

  For remote access VPN double authentication, ensure that both the primary and secondary authentication servers are reachable from the Firepower Threat Defense device for the double authentication configuration to work.
- Purchase and enable one of the following Cisco AnyConnect licenses: AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only to enable the Firepower Threat Defense Remote Access VPN.
- Download the latest AnyConnect image files from Cisco Software Download Center.

  On your Firepower Management Center web interface, go to **Objects** > **Object Management** > **VPN** > **AnyConnect File** and add the new AnyConnect client image files.
- Create a security zone or interface group that contains the network interfaces that users will access for VPN connections. See Interface Objects: Interface Groups and Security Zones.
- Download the AnyConnect Profile Editor from Cisco Software Download Center to create an AnyConnect client profile. You can use the standalone profile editor to create a new or modify an existing AnyConnect profile.

Create a New Remote Access VPN Policy

You can add a new remote access VPN Policy only by using the Remote Access VPN Policy wizard. The wizard guides you to quickly and easily set up remote access VPNs with basic capabilities. Further, you can enhance the policy configuration by specifying additional attributes as desired and deploy it to your Firepower Threat Defense secure gateway devices.

Before you begin

- Ensure that you complete all the prerequisites listed in Prerequisites for Configuring Remote Access VPN, on page 11.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **(Add (** **)) Add** to create a new Remote Access VPN Policy using a wizard that walks you through a basic policy configuration.

You must proceed through the entire wizard to create a new policy; the policy is not saved if you cancel before completing the wizard.

Step 3 Select the **Target Devices** and **Protocols**.

The Firepower Threat Defense devices selected here will function as your remote access VPN gateways for the VPN client users. You can select the devices from the list or add a new device.

You can select Firepower Threat Defense devices when you create a remote access VPN policy or change them later. See Setting Target Devices for a Remote Access VPN Policy, on page 17.

You can select **SSL** or **IPSec-IKEv2**, or both the VPN protocols. Firepower Threat Defense supports both the protocols to establish secure connections over a public network through VPN tunnels.

Note Firepower Threat Defense does not support IPSec tunnels with NULL encryption. If you have selected IPSec-IKEv2, make sure that you do not choose NULL encryption for IPSec IKEv2 proposal. See Configure IKEv2 IPsec Proposal Objects.

For SSL settings, see Configure SSL Settings.

Step 4 Configure the **Connection Profile** and **Group Policy** settings.

A connection profile specifies a set of parameters that define how the remote users connect to the VPN device. The parameters include settings and attributes for authentication, address assignments to VPN clients, and group policies. Firepower Threat Defense device provides a default connection profile named *DefaultWEBVPNGroup* when you configure a remote access VPN policy.

For more information, see Configure Connection Profile Settings, on page 17.

A group policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience for VPN users. You configure attributes such as user authorization profile, IP addresses, AnyConnect settings, VLAN mapping, and user session settings and so on using the group policy. The RADIUS authorization server assigns the group policy, or it is obtained from the current connection profile.

For more information, see Configuring Group Policies, on page 37.

Step 5 Select the **AnyConnect Client Image** that the VPN users will use to connect to the remote access VPN.

The Cisco AnyConnect Secure Mobility client provides secure SSL or IPSec (IKEv2) connections to the Firepower Threat Defense device for remote users with full VPN profiling to corporate resources. After the remote access VPN policy is deployed on the Firepower Threat Defense device, VPN users can enter the IP address of the configured device interface in their browser to download and install the AnyConnect client.

Step 6 Select the **Network Interface and Identity Certificate**.

Interface objects segment your network to help you manage and classify traffic flow. A security zone object simply groups interfaces. These groups may span multiple devices; you can also configure multiple zones interface objects on a single device. There are two types of interface objects:

- Security zones—An interface can belong to only one security zone.
- Interface groups—An interface can belong to multiple interface groups (and to one security zone).

Step 7 View the **Summary** of the Remote Access VPN policy configuration.

The Summary page displays all the remote access VPN settings you have configured so far and provides links to the additional configurations that need to be performed before deploying the remote access VPN policy on the selected devices.

Click **Back** to make changes to the configuration, if required.

Step 8 Click **Finish** to complete the basic configuration for the remote access VPN policy.

When you have completed the remote access VPN policy using the wizard, it returns to the policy listing page. Set up DNS configuration, configure access control for VPN users, and enable NAT exemption (if necessary) to complete a basic RA VPN Policy configuration. Then, deploy the configuration and establish VPN connections.

Update the Access Control Policy on the Firepower Threat Defense Device

Before deploying the remote access VPN policy, you must update the access control policy on the targeted Firepower Threat Defense device with a rule that allows VPN traffic. The rule must allow all traffic coming in from the outside interface, with source as the defined VPN pool networks and destination as the corporate network.

Note If you have selected the **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** option on the Access Interface tab, you need not update the access control policy for remote access VPN.

Enable or disable the option for all your VPN connections. If you disable this option, make sure that the traffic is allowed by the access control policy or pre-filter policy.

For more information, see Configure Access Interfaces for Remote Access VPN, on page 33.

Before you begin

Complete the remote access VPN policy configuration using the Remote Access VPN Policy wizard.

Step 1 On your Firepower Management Center web interface, choose **Policies** > **Access Control**.

Step 2 Select the access control policy assigned to the target devices where the remote access VPN policy will be deployed and click **Edit**.

Step 3 Click **Add Rule** to add a new rule.

Step 4 Specify the **Name** for the rule and select **Enabled**.

Step 5 Select the **Action**, **Allow** or **Trust**.

Step 6 Select the following on the **Zones** tab:

a) Select the outside zone from Available Zones and click **Add to Source**.

b) Select the inside zone from Available Zones and click **Add to Destination**.

Step 7 Select the following on the **Networks** tab:

a) Select the inside network (inside interface and/or a corporate network) from Available networks and click **Add to Destination**.

b) Select the VPN address pool network from **Available Networks** and click **Add to Source Networks**.

Step 8 Configure other required access control rule settings and click **Add**.

Step 9 Save the rule and access control policy.

(Optional) Configure NAT Exemption

NAT exemption exempts addresses from translation and allows both translated and remote hosts to initiate connections with your protected hosts. Like identity NAT, you do not limit translation for a host on specific interfaces; you must use NAT exemption for connections through all interfaces. However, NAT exemption enables you to specify the real and destination addresses when determining the real addresses to translate (similar to policy NAT). Use static identity NAT to consider ports in the access list.

Before you begin

Check if NAT is configured on the targeted devices where remote access VPN policy is deployed. If NAT is enabled on the targeted devices, you must define a NAT policy to exempt VPN traffic.

Step 1 On your Firepower Management Center web interface, click **Devices** > **NAT**.

Step 2 Select a NAT policy to update or click **New Policy** > **Threat Defense NAT** to create a NAT policy with a NAT rule to allow connections through all interfaces.

Step 3 Click **Add Rule** to add a NAT rule.

Step 4 On the Add NAT Rule window, select the following:

a) Select the NAT Rule as **Manual NAT Rule**.

b) Select the Type as **Static**.

c) Click **Interface Objects** and select the Source and destination interface objects.

Note This interface object must be the same as the interface selected in the remote access VPN policy.

For more information, see Configure Access Interfaces for Remote Access VPN, on page 33.

a) Click **Translation** and select the source and destination networks:

- **Original Source** and **Translated Source**
- **Original Destination** and **Translated Destination**

Step 5 On the Advanced tab, select **Do not proxy ARP on Destination Interface**.

Do not proxy ARP on Destination Interface—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router.

Step 6 Click **OK**.

Configure DNS

Configure DNS on each Firepower Threat Defense device in order to use remote access VPN. Without DNS, the devices cannot resolve AAA server names, named URLs, and CA Servers with FQDN or Hostnames. It can only resolve IP addresses.

Step 1 Configure DNS server details and domain-lookup interfaces using the Platform Settings. For more information, see Configure DNS and DNS Server Group Objects.

Step 2 Configure split-tunnel in group policy to allow DNS traffic through remote access VPN tunnel if the DNS server is reachable through VNP network. For more information, see Configure Group Policy Objects.

Add an AnyConnect Client Profile XML File

An AnyConnect client profile is a group of configuration parameters stored in an XML file that the client uses to configure its operation and appearance. These parameters (XML tags) include the names and addresses of host computers and settings to enable more client features.

You can create an AnyConnect client profile using the AnyConnect Profile Editor. This editor is a GUI-based configuration tool that is available as part of the AnyConnect software package. It is an independent program that you run outside of the Firepower Management Center. For more information about AnyConnect Profile Editor, see *Cisco AnyConnect Secure Mobility Client Administrator Guide*.

Before you begin

A Firepower Threat Defense remote access VPN policy requires an AnyConnect client profile to be assigned to the VPN clients. The client profile is attached to a group policy.

Download the AnyConnect Profile Editor from Cisco Software Download Center.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access VPN policy and click **Edit**.
The connection profiles configured for the remote access VPN policy are listed.

Step 3 Select a connection profile on which you want to update the AnyConnect client profile and click **Edit**.

Step 4 Click **Add** to add a group policy or click **Edit Group Policy** > **General** > **AnyConnect**.

Step 5 Select a Client Profile from the list or click the **Add** icon to add a new one:

a) Specify the AnyConnect profile **Name**.
b) Click **Browse** and select an AnyConnect profile XML file.

Note For two-factor authentication, make sure that the timeout is updated to 60 seconds or more in the AnyConnect client profile XML file.

c) Click **Save**.

(Optional) Configure Split Tunneling

Split tunnel allows VPN connectivity to a remote network across a secure tunnel, and it also allows connectivity to a network outside VPN tunnel. You can configure split tunnel if you want to allow your VPN users to access an outside network while they are connected to a remote access VPN. To configure a split-tunnel list, you must create a Standard Access List or Extended Access List.

For more information, see Configuring Group Policies, on page 37.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.
Step 2 Select a Remote Access policy and click **Edit**.
Step 3 Select a connection profile and click **Edit**.
Step 4 Click **Add** to add a group policy, or click **Edit Group Policy** > **General** > **Split Tunneling**.
Step 5 From the **IPv4 Split Tunneling** or **IPv6 Split Tunneling** list, select **Exclude networks specified below**; and then select the networks to be excluded from VPN traffic.
If the split tunneling option is left as is, all traffic from the endpoint goes over the VPN connection.
Step 6 Click **Standard Access List** or **Extended Access List**, and select an access list from the drop-down or add a new one.
Step 7 If you chose to add a new standard or extended access list, do the following:
a) Specify the **Name** for the new access list and click **Add**.
b) Select **Allow** from the Action drop-down.
c) Select the network traffic to be allowed over the VPN tunnel and click **Add**.
Step 8 Click **Save**.

Related Topics
Access List

Verify the Configuration

Step 1 Open a web browser on a machine on the outside network.
Step 2 Enter the URL of an FTD device configured as a remote access VPN gateway.
Step 3 Enter the username and password when prompted, and click **Logon**.

Note If AnyConnect is installed on the system, you will be connected to the VPN automatically.

If AnyConnect is not installed, you will be prompted to download the AnyConnect client.

Step 4 Download AnyConnect if it is not installed already and connect to the VPN.
The AnyConnect client installs itself. On successful authentication, you will be connected to the Firepower Threat Defense remote access VPN gateway. The applicable identity or QoS policy is enforced according to your remote access VPN policy configuration.

Setting Target Devices for a Remote Access VPN Policy

You can add targeted devices while you create a new remote access VPN policy, or change them later.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** ( ) next to the remote access VPN policy that you want to edit.

Step 3 Click **Policy Assignment**.

Step 4 Do any of the following:

- To assign a device, high-availability pair, or device group to the policy, select it in the **Available Devices** list and click **Add**. You can also drag and drop the available devices to select.
- To remove a device assignment, click **Delete** ( ) next to a device, high-availability pair, or device group in the **Selected Devices** list.

Step 5 Click **OK**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Additional Remote Access VPN Configurations

Configure Connection Profile Settings

Remote Access VPN policy contains the connection profiles targeted for specific devices. These policies pertain to creating the tunnel itself, such as, how AAA is accomplished, and how addresses are assigned (DHCP or Address Pools) to VPN clients. They also include user attributes, which are identified in group policies configured on the Firepower Threat Defense device or obtained from a AAA server. A device also provides a default connection profile named *DefaultWEBVPNGroup*. The connection profile that is configured using the wizard appears in the list.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Select a **Connection Profile** and click **Edit**.
The edit connection profile page is displayed.

Step 4 (Optional) Add multiple connection profiles.
Configure Multiple Connection Profiles, on page 18

Step 5 Configure IP Addresses for VPN Clients.
Configure IP Addresses for VPN Clients, on page 19

Step 6 (Optional) Update AAA Settings for remote access VPNs.
Configure AAA Settings for Remote Access VPN, on page 20

Step 7 (Optional) Create or update Aliases.
Create or Update Aliases for a Connection Profile, on page 32

Step 8 Save the connection profile.

Configure Multiple Connection Profiles

If you decide to grant different rights to different groups of VPN users, then you can configure specific connection profiles or group policies for each of the user groups. For example, you might allow a finance group to access one part of a private network, a customer support group to access another part, and an MIS group to access other parts. In addition, you might allow specific users within MIS to access systems that other MIS users cannot access. Connection profiles and group policies provide the flexibility to do so securely.

You can configure only one connection profile when you create a VPN policy using the Remote Access Policy wizard. You can add more connection profiles later. A device also provides a default connection profile named *DefaultWEBVPNGroup*.

Before you begin

Ensure that you have configured remote access VPN using the Remote Access Policy wizard with a connection profile.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.
Existing remote access policies are listed.

Step 2 Select a remote access VPN policy and click **Edit**.

Step 3 Click **Add** and specify the following in the Add Connection Profile window:

a) **Connection Profile**—Provide a name that the remote users will use for VPN connections. The connection profile contains a set of parameters that define how the remote users connect to the VPN device.

b) **Client Address Assignment**— Assign IP Address for the remote clients from the local IP Address pools, DHCP servers, and AAA servers.

c) **AAA**— Configure the AAA servers to enable managed devices acting as secure VPN gateways to determine who a user is (authentication), what the user is permitted to do (authorization), and what the user did (accounting).

d) **Aliases**—Provide an alternate name or URL for the connection profile. Remote Access VPN administrators can enable or disable the Alias names and Alias URLs. VPN users can choose an Alias name when they connect to the Firepower Threat Defense device remote access VPN using the AnyConnect VPN client.

Step 4 Click **Save**.

Related Topics

Configure Connection Profile Settings, on page 17

Configure IP Addresses for VPN Clients

Client address assignment provides a means of assigning IP addresses for the remote access VPN users.

You can configure to assign IP Address for remote VPN clients from the local IP Address pools, DHCP Servers, and AAA servers. The AAA servers are assigned first, followed by others. Configure the **Client Address Assignment** policy in the **Advanced** tab to define the assignment criteria. The IP pool(s) defined in this connection profile will only be used if no IP pools are defined in group policy associated with the connection profile, or the system default group policy **DfltGrpPolicy**.

IPv4 Address Pools—SSL VPN clients receive new IP addresses when they connect to the Firepower Threat Defense device. Address Pools define a range of addresses that remote clients can receive. Select an existing IP address pool. You can add a maximum of six pools for IPv4 and IPv6 addresses each.

Note You can use the IP address from the existing IP pools in Firepower Management Center or create a new pool using the **Add** option. Also, you can create an IP pool in Firepower Management Center using the **Objects > Object Management > Address Pools** path. For more information, see Address Pools.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.
Existing remote access policies are listed.

Step 2 Select a remote access VPN policy click **Edit**.

Step 3 Select the connection profile that you want to update and click **Edit** > **Client Address Assignment**.

Step 4 Select the following for **Address Pools**:

a) Click **Add** to add IP addresses, and select **IPv4** or **IPv6** to add the corresponding address pool. Select the IP address pool from Available Pools and click **Add**.

Note If you share your remote access VPN policy among multiple Firepower Threat Defense devices, bear in mind that all devices share the same address pool unless you use device-level object overrides to replace the global definition with a unique address pool for each device. Unique address pools are required to avoid overlapping addresses in cases where the devices are not using NAT.

b) Select the **Add** icon in the **Address Pools** window to add a new IPv4 or IPv6 address pool. When you choose the IPv4 pool, provide a starting and ending IP address. When you choose to include a new IPv6 address pool, enter `Number of Addresses` in the range 1-16384. Select the **Allow Overrides** option to avoid conflicts with IP address when objects are shared across many devices. For more information, see Address Pools.

c) Click **OK**.

Step 5 Select the following for **DHCP Servers**:

Note The DHCP server address can be configured only with IPv4 address.

a) Specify the name and DHCP (Dynamic Host Configuration Protocol) server address as network objects. Click **Add** to choose the server from the object list. Click **Delete** to delete a DHCP server.

b) Click **Add** in the **New Objects** page to add a new network object. Enter the new object name, description, network, and select the **Allow Overrides** option as applicable. For more information, see Creating Network Objects and Allowing Object Overrides.

c) Click **OK**.

Step 6 Click **Save**.

Related Topics

Configure Connection Profile Settings, on page 17

Configure AAA Settings for Remote Access VPN

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Select a connection profile to update AAA settings, click **Edit** > **AAA**.

Step 4 Select the following for **Authentication**:

- **Authentication Method**: Determines how a user is identified before being allowed access to the network and network services. It controls access by requiring valid user credentials, which are typically a username and password. It may also include the certificate from the client.

  When you select the **Authentication Method** as:

  - **AAA Only**: If you select the **Authentication Server** as **RADIUS**, by default, the Authorization Server has the same value. Select the **Accounting Server** from the drop-down list. Whenever you select **AD** and **LDAP** from the Authentication Server drop-down list, you must manually select the **Authorization Server** and **Accounting Server** respectively.

  - **Client Certificate Only**: Each user is authenticated with a client certificate. The client certificate must be configured on VPN client endpoints. By default, the user name is derived from the client certificate fields CN and OU. If the user name is specified in other fields in the client certificate, use 'Primary' and 'Secondary' field to map appropriate fields.

    If you select the **Map specific field** option, which includes the username from the client certificate, the **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN as username** option, the system automatically retrieves the user identity. A distinguished name (DN) is a unique identification, made up of individual fields that can be used as the identifier when matching users to a connection profile. DN rules are used for enhanced certificate authentication.

    The primary and secondary fields pertaining to the **Map specific field** option contain these common values:

    - C (Country)
    - CN (Common Name)
    - DNQ (DN Qualifier)
    - EA (Email Address)
    - GENQ (Generational Qualifier)
    - GN (Given Name)
    - I (Initial)
    - L (Locality)
    - N (Name)
    - O (Organisation)
    - OU (Organisational Unit)
    - SER (Serial Number)

- SN (Surname)
- SP (State Province)
- T (Title)
- UID (User ID)
- UPN (User Principal Name)

- **Client Certificate & AAA**: Each user is authenticated with both a client certificate and AAA server. Select the required certificate and AAA configurations for authentication.

  Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

- **Authentication Server**: Authentication is the way a user is identified before being allowed access to the network and network services. Authentication requires valid user credentials, a certificate, or both. You can use authentication alone, or with authorization and accounting.

  Select (or add and select) an authentication server:

  - **Realm**: Configure an LDAP or AD realm. See Create a Realm.
  - **RADIUS Server Group**: Add a RADIUS server group object with RADIUS servers. See RADIUS Server Groups.

- Select an LDAP or AD realm, or a RADIUS server group that has been previously configured to authenticate Remote Access VPN users.

- **Use secondary authentication**: Secondary authentication is configured in addition to primary authentication to provide additional security for VPN sessions. Secondary authentication is applicable only to **AAA only** and **Client Certificate & AAA** authentication methods.

  Secondary authentication is an optional feature that requires a VPN user to enter two sets of username and password on the AnyConnect login screen. You can also configure to pre-fill the secondary username from the authentication server or client certificate. Remote access VPN authentication is granted only if both primary and secondary authentications are successful. VPN authentication is denied if any one of the authentication servers is not reachable or one authentication fails.

  You must configure a secondary authentication server group (AAA server) for the second username and password before configuring secondary authentication. For example, you can set the primary authentication server to an LDAP or Active Directory realm and the secondary authentication to a RADIUS server.

  Note By default, secondary authentication is not required.

  Authentication Server: Secondary authentication server to provide secondary username and password for VPN users.

  Select the following under **Username for secondary authentication**:

  - **Prompt**: Prompts the users to enter the username and password while logging on to VPN gateway.
  - **Use primary authentication username**: The username is taken from the primary authentication server for both primary and secondary authentication; you must enter two passwords.
  - **Map username from client certificate**: Prefills the secondary username from the client certificate.

- If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN (Distinguished Name) as username** option, the system automatically retrieves the user identity.

  See **Authentication Method** descriptions for more information about primary and secondary field mapping.

- **Prefill username from certificate on user login window**: Prefills the secondary username from the client certificate when the user connects via AnyConnect VPN client.
  - **Hide username in login window**: The secondary username is pre-filled from the client certificate, but hidden to the user so that the user does not modify the pre-filled username.

- **Use secondary username for VPN session**: The secondary username is used for reporting user activity during a VPN session.

Step 5 Select the following for **Authorization**:

- **Authorization Server**: 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. When you do not use authorization, authentication alone provides the same access to all authenticated users. Authorization requires authentication. Only RADIUS servers are supported for Authorization services.

  To know more about how remote access VPN authorization works, see Understanding Policy Enforcement of Permissions and Attributes, on page 5.

  Enter or select a RADIUS server group object that has been pre-configured to authorize Remote Access VPN users.

  When a RADIUS Server is configured for user authorization in the connection profile, the Remote Access VPN system administrator can configure multiple authorization attributes for users or user-groups. The authorization attributes that are configured on the RADIUS server can be specific for a user or a user-group. Once users are authenticated, these specific authorization attributes are pushed to the Firepower Threat Defense device.

  Note The AAA server attributes obtained from the authorization server override the attribute values that may have been previously configured on the group policy or the connection profile.

- Check **Allow connection only if user exists in authorization database** if desired.

  When enabled, the system checks the username of the client must exist in the authorization database to allow a successful connection. If the username does not exist in the authorization database, then the connection is denied.

Step 6 Select the following for **Accounting**:

- **Accounting Server**: Accounting is used to track the services that users are accessing and the amount of network resources they are consuming. When AAA accounting is activated, the network access server 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 services used, and the duration of each session. This data can then be analyzed for network management, client billing, or auditing. You can use accounting alone or together with authentication and authorization.

  Specify the RADIUS Server Group object that will be used to account for the Remote Access VPN session.

Step 7 Select the following **Advanced Settings**:

- **Strip Realm from username**: Select to remove the realm from the username before passing the username on to the AAA server. For example, if you select this option and provide *domain\username*, the domain is stripped off from the username and sent to AAA server for authentication. By default this option is unchecked.
- **Strip Group from username**: Select to remove the group name from the username before passing the username on to the AAA server. By default this option is unchecked.

  Note A realm is an administrative domain. Enabling these 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.

- **Password Management**: Enable managing the password for the Remote Access VPN users. Select to notify ahead of the password expiry or on the day the password expires.

Step 8 Click **Save**.

Related Topics

Understanding Policy Enforcement of Permissions and Attributes, on page 5
Manage a Realm

RADIUS Server Attributes for Firepower Threat Defense

The Firepower Threat Defense device supports applying user authorization attributes (also called user entitlements or permissions) to VPN connections from the external RADIUS server that are configured for authentication and/or authorization in the remote access VPN policy.

Note Firepower Threat Defense devices support attributes with vendor ID 3076.

The following user authorization attributes are sent to the Firepower Threat Defense device from the RADIUS server.

- RADIUS attributes 146 and 150 are sent from Firepower Threat Defense devices to the RADIUS server for authentication and authorization requests.
- All three (146, 150, and 151) attributes are sent from Firepower Threat Defense devices to the RADIUS server for accounting start, interim-update, and stop requests.

Table 1: RADIUS Attributes Sent from Firepower Threat Defense to RADIUS Server

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Connection Profile Name or Tunnel Group Name	146	String	Single	1-253 characters
Client Type	150	Integer	Single	2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2)
Session Type	151	Integer	Single	1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPsec VPN (IKEv2)

Table 2: Supported RADIUS Authorization Attributes

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Access-Hours	Y	1	String	Single	Name of the time range, for example, Business-h
Access-List-Inbound	Y	86	String	Single	Both of the Access-List attributes take the name ACL that is configured on the FTD device. Crea ACLs using the Smart CLI Extended Access Lis type (select **Device** > **Advanced Configuration** > **CLI** > **Objects**). These ACLs control traffic flow in the inbound (entering the FTD device) or outbound (traffic lea FTD device) direction.
Access-List-Outbound	Y	87	String	Single	
Address-Pools	Y	217	String	Single	The name of a network object defined on the FTI that identifies a subnet, which will be used as the pool for clients connecting to the RA VPN. Defi network object on the **Objects** page.
Allow-Network-Extension-Mode	Y	64	Boolean	Single	0 = Disabled 1 = Enabled
Authenticated-User-Idle-Timeout	Y	50	Integer	Single	1-35791394 minutes
Authorization-DN-Field	Y	67	String	Single	Possible values: UID, OU, O, CN, L, SP, C, EA, GN, SN, I, GENQ, DNQ, SER, use-entire-name
Authorization-Required		66	Integer	Single	0 = No 1 = Yes
Authorization-Type	Y	65	Integer	Single	0 = None 1 = RADIUS 2 = LDAP
Banner1	Y	15	String	Single	Banner string to display for Cisco VPN remote a sessions: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, and Clientless SSL
Banner2	Y	36	String	Single	Banner string to display for Cisco VPN remote a sessions: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2, and Clientless SSL. The string is concatenated to the Banner1 string , if con
Cisco-IP-Phone-Bypass	Y	51	Integer	Single	0 = Disabled 1 = Enabled
Cisco-LEAP-Bypass	Y	75	Integer	Single	0 = Disabled 1 = Enabled
Client Type	Y	150	Integer	Single	1 = Cisco VPN Client (IKEv1) 2 = AnyConnect SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 AnyConnect Client IPsec VPN (IKEv2)
Client-Type-Version-Limiting	Y	77	String	Single	IPsec VPN version number string
DHCP-Network-Scope	Y	61	String	Single	IP Address

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Extended-Authentication-On-Rekey	Y	122	Integer	Single	0 = Disabled 1 = Enabled
Framed-Interface-Id	Y	96	String	Single	Assigned IPv6 interface ID. Combines with Framed-IPv6-Prefix to create a complete ass address. For example: Framed-Interface-ID= combined with Framed-IPv6-Prefix=2001:0db the assigned IP address 2001:0db8::1:1:1:1.
Framed-IPv6-Prefix	Y	97	String	Single	Assigned IPv6 prefix and length. Combines Framed-Interface-Id to create a complete ass address. For example: prefix 2001:0db8::/64 with Framed-Interface-Id=1:1:1:1 gives the 2001:0db8::1:1:1:1. You can use this attribut an IP address without using Framed-Interfac assigning the full IPv6 address with prefix le for example, Framed-IPv6-Prefix=2001:0db
Group-Policy	Y	25	String	Single	Sets the group policy for the remote access V You can use one of the following formats: • *group policy name* • OU=*group policy name* • OU=*group policy name*;
IE-Proxy-Bypass-Local		83	Integer	Single	0 = None 1 = Local
IE-Proxy-Exception-List		82	String	Single	New line (\n) separated list of DNS domains
IE-Proxy-PAC-URL	Y	133	String	Single	PAC address string
IE-Proxy-Server		80	String	Single	IP address
IE-Proxy-Server-Policy		81	Integer	Single	1 = No Modify 2 = No Proxy 3 = Auto detec Concentrator Setting
IKE-KeepAlive-Confidence-Interval	Y	68	Integer	Single	10-300 seconds
IKE-Keepalive-Retry-Interval	Y	84	Integer	Single	2-10 seconds
IKE-Keep-Alives	Y	41	Boolean	Single	0 = Disabled 1 = Enabled
Intercept-DHCP-Configure-Msg	Y	62	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Allow-Passwd-Store	Y	16	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Authentication		13	Integer	Single	0 = None 1 = RADIUS 2 = LDAP (authoriza = NT Domain 4 = SDI 5 = Internal 6 = RAD Expiry 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	Boolean	Single	0 = Disabled 1 = Enabled

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
IPsec-Backup-Server-List	Y	60	String	Single	Server Addresses (space delimited)
IPsec-Backup-Servers	Y	59	String	Single	1 = Use Client-Configured list 2 = Disable and cle list 3 = Use Backup Server list
IPsec-Client-Firewall-Filter-Name		57	String	Single	Specifies the name of the filter to be pushed to t as firewall policy
IPsec-Client-Firewall-Filter-Optional	Y	58	Integer	Single	0 = Required 1 = Optional
IPsec-Default-Domain	Y	28	String	Single	Specifies the single default domain name to sen client (1-255 characters).
IPsec-IKE-Peer-ID-Check	Y	40	Integer	Single	1 = Required 2 = If supported by peer certificate not check
IPsec-IP-Compression	Y	39	Integer	Single	0 = Disabled 1 = Enabled
IPsec-Mode-Config	Y	31	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Over-UDP	Y	34	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Over-UDP-Port	Y	35	Integer	Single	4001- 49151. The default is 10000.
IPsec-Required-Client-Firewall-Capability	Y	56	Integer	Single	0 = None 1 = Policy defined by remote FW Are-You-There (AYT) 2 = Policy pushed CPP 4 = from server
IPsec-Sec-Association		12	String	Single	Name of the security association
IPsec-Split-DNS-Names	Y	29	String	Single	Specifies the list of secondary domain names to the client (1-255 characters).
IPsec-Split-Tunneling-Policy	Y	55	Integer	Single	0 = No split tunneling 1 = Split tunneling 2 = Loc permitted
IPsec-Split-Tunnel-List	Y	27	String	Single	Specifies the name of the network or ACL that d the split tunnel inclusion list.
IPsec-Tunnel-Type	Y	30	Integer	Single	1 = LAN-to-LAN 2 = Remote access
IPsec-User-Group-Lock		33	Boolean	Single	0 = Disabled 1 = Enabled
IPv6-Address-Pools	Y	218	String	Single	Name of IP local pool-IPv6
IPv6-VPN-Filter	Y	219	String	Single	ACL value
L2TP-Encryption		21	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bits 4 = 8 = Stateless-Req 15= 40/128-Encr/Stateless-Re
L2TP-MPPC-Compression		38	Integer	Single	0 = Disabled 1 = Enabled

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Member-Of	Y	145	String	Single	Comma-delimited string, for example: `Engineering, Sales` An administrative attribute that can be used i access policies. It does not set a group policy
MS-Client-Subnet-Mask	Y	63	Boolean	Single	An IP address
NAC-Default-ACL		92	String		ACL
NAC-Enable		89	Integer	Single	0 = No 1 = Yes
NAC-Revalidation-Timer		91	Integer	Single	300-86400 seconds
NAC-Settings	Y	141	String	Single	Name of the NAC policy
NAC-Status-Query-Timer		90	Integer	Single	30-1800 seconds
Perfect-Forward-Secrecy-Enable	Y	88	Boolean	Single	0 = No 1 = Yes
PPTP-Encryption		20	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bits 8 = Stateless-Required 15= 40/128-Encr/Stat
PPTP-MPPC-Compression		37	Integer	Single	0 = Disabled 1 = Enabled
Primary-DNS	Y	5	String	Single	An IP address
Primary-WINS	Y	7	String	Single	An IP address
Privilege-Level	Y	220	Integer	Single	An integer between 0 and 15.
Required-Client- Firewall-Vendor-Code	Y	45	Integer	Single	1 = Cisco Systems (with Cisco Integrated Cl Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cis (with Cisco Intrusion Prevention Security Ag
Required-Client-Firewall-Description	Y	47	String	Single	String
Required-Client-Firewall-Product-Code	Y	46	Integer	Single	Cisco Systems Products: 1 = Cisco Intrusion Prevention Security Age Integrated Client (CIC) Zone Labs Products: 1 = Zone Alarm 2 = Zon 3 = Zone Labs Integrity NetworkICE Product: 1 = BlackIce Defende Sygate Products: 1 = Personal Firewall 2 = P Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	Integer	Single	0 = Disabled 1 = Enabled
Require-HW-Client-Auth	Y	48	Boolean	Single	0 = Disabled 1 = Enabled

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Secondary-DNS	Y	6	String	Single	An IP address
Secondary-WINS	Y	8	String	Single	An IP address
SEP-Card-Assignment		9	Integer	Single	Not used
Session Subtype	Y	152	Integer	Single	0 = None 1 = Clientless 2 = Client 3 = Client Or Session Subtype applies only when the Session (151) attribute has the following values: 1, 2, 3,
Session Type	Y	151	Integer	Single	0 = None 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN (IKEv2) 3 = Cli SSL VPN 4 = Clientless Email Proxy 5 = Cisco Client (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv LAN-LAN 8 = VPN Load Balancing
Simultaneous-Logins	Y	2	Integer	Single	0-2147483647
Smart-Tunnel	Y	136	String	Single	Name of a Smart Tunnel
Smart-Tunnel-Auto	Y	138	Integer	Single	0 = Disabled 1 = Enabled 2 = AutoStart
Smart-Tunnel-Auto-Signon-Enable	Y	139	String	Single	Name of a Smart Tunnel Auto Signon list appen the domain name
Strip-Realm	Y	135	Boolean	Single	0 = Disabled 1 = Enabled
SVC-Ask	Y	131	String	Single	0 = Disabled 1 = Enabled 3 = Enable default ser Enable default clientless (2 and 4 not used)
SVC-Ask-Timeout	Y	132	Integer	Single	5-120 seconds
SVC-DPD-Interval-Client	Y	108	Integer	Single	0 = Off 5-3600 seconds
SVC-DPD-Interval-Gateway	Y	109	Integer	Single	0 = Off) 5-3600 seconds
SVC-DTLS	Y	123	Integer	Single	0 = False 1 = True
SVC-Keepalive	Y	107	Integer	Single	0 = Off 15-600 seconds
SVC-Modules	Y	127	String	Single	String (name of a module)
SVC-MTU	Y	125	Integer	Single	MTU value 256-1406 in bytes
SVC-Profiles	Y	128	String	Single	String (name of a profile)
SVC-Rekey-Time	Y	110	Integer	Single	0 = Disabled 1-10080 minutes
Tunnel Group Name	Y	146	String	Single	1-253 characters
Tunnel-Group-Lock	Y	85	String	Single	Name of the tunnel group or “none”

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Tunneling-Protocols	Y	11	Integer	Single	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) mutually exclusive. 0 - 11, 16 - 27, 32 - 43, 4 legal values.
Use-Client-Address		17	Boolean	Single	0 = Disabled 1 = Enabled
VLAN	Y	140	Integer	Single	0-4094
WebVPN-Access-List	Y	73	String	Single	Access-List name
WebVPN ACL	Y	73	String	Single	Name of a WebVPN ACL on the device
WebVPN-ActiveX-Relay	Y	137	Integer	Single	0 = Disabled Otherwise = Enabled
WebVPN-Apply-ACL	Y	102	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Auto-HTTP-Signon	Y	124	String	Single	Reserved
WebVPN-Citrix-Metaframe-Enable	Y	101	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Content-Filter-Parameters	Y	69	Integer	Single	1 = Java ActiveX 2 = Java Script 4 = Image 8 in images
WebVPN-Customization	Y	113	String	Single	Name of the customization
WebVPN-Default-Homepage	Y	76	String	Single	A URL such as http://example-example.com
WebVPN-Deny-Message	Y	116	String	Single	Valid string (up to 500 characters)
WebVPN-Download_Max-Size	Y	157	Integer	Single	0x7fffffff
WebVPN-File-Access-Enable	Y	94	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-File-Server-Browsing-Enable	Y	96	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-File-Server-Entry-Enable	Y	95	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	String	Single	Comma-separated DNS/IP with an optional v (for example *.cisco.com, 192.168.1.*, wwwin
WebVPN-Hidden-Shares	Y	126	Integer	Single	0 = None 1 = Visible
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	Boolean	Single	Enabled if clientless home page is to be rende Smart Tunnel.
WebVPN-HTML-Filter	Y	69	Bitmap	Single	1 = Java ActiveX 2 = Scripts 4 = Image 8 =
WebVPN-HTTP-Compression	Y	120	Integer	Single	0 = Off 1 = Deflate Compression
WebVPN-HTTP-Proxy-IP-Address	Y	74	String	Single	Comma-separated DNS/IP:port, with http= c prefix (for example http=10.10.10.10:80, https=11.11.11.11:443)

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
WebVPN-Idle-Timeout-Alert-Interval	Y	148	Integer	Single	0-30. 0 = Disabled.
WebVPN-Keepalive-Ignore	Y	121	Integer	Single	0-900
WebVPN-Macro-Substitution	Y	223	String	Single	Unbounded.
WebVPN-Macro-Substitution	Y	224	String	Single	Unbounded.
WebVPN-Port-Forwarding-Enable	Y	97	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-List	Y	72	String	Single	Port forwarding list name
WebVPN-Port-Forwarding-Name	Y	79	String	Single	String name (example, “Corporate-Apps”). This text replaces the default string, “Application A on the clientless portal home page.
WebVPN-Post-Max-Size	Y	159	Integer	Single	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	Integer	Single	0-30. 0 = Disabled.
WebVPN Smart-Card-Removal-Disconnect	Y	225	Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-Smart-Tunnel	Y	136	String	Single	Name of a Smart Tunnel
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	String	Single	Name of a Smart Tunnel auto sign-on list appen the domain name
WebVPN-Smart-Tunnel-Auto-Start	Y	138	Integer	Single	0 = Disabled 1 = Enabled 2 = Auto Start
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	String	Single	One of “e networkname,” “i networkname,” or “a networkname is the name of a Smart Tunnel netw e indicates the tunnel excluded, i indicates the tu specified, and a indicates all tunnels.
WebVPN-SSL-VPN-Client-Enable	Y	103	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Keep- Installation	Y	105	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Required	Y	104	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSO-Server-Name	Y	114	String	Single	Valid string
WebVPN-Storage-Key	Y	162	String	Single	
WebVPN-Storage-Objects	Y	161	String	Single	
WebVPN-SVC-Keepalive-Frequency	Y	107	Integer	Single	15-600 seconds, 0=Off

Attribute Name	FTD	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
WebVPN-SVC-Client-DPD-Frequency	Y	108	Integer	Single	5-3600 seconds, 0=Off
WebVPN-SVC-DTLS-Enable	Y	123	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SVC-DTLS-MTU	Y	125	Integer	Single	MTU value is from 256-1406 bytes.
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	Integer	Single	5-3600 seconds, 0=Off
WebVPN-SVC-Rekey-Time	Y	110	Integer	Single	4-10080 minutes, 0=Off
WebVPN-SVC-Rekey-Method	Y	111	Integer	Single	0 (Off), 1 (SSL), 2 (New Tunnel)
WebVPN-SVC-Compression	Y	112	Integer	Single	0 (Off), 1 (Deflate Compression)
WebVPN-UNIX-Group-ID (GID)	Y	222	Integer	Single	Valid UNIX group IDs
WebVPN-UNIX-User-ID (UIDs)	Y	221	Integer	Single	Valid UNIX user IDs
WebVPN-Upload-Max-Size	Y	158	Integer	Single	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-URL-List	Y	71	String	Single	URL list name
WebVPN-User-Storage	Y	160	String	Single	
WebVPN-VDI	Y	163	String	Single	List of settings

Table 3: RADIUS Attributes Sent to Firepower Threat Defense

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Address-Pools	217	String	Single	The name of a network object defined on the FTD device that identifies a subnet, which will be used as the address pool for clients connecting to the RA VPN. Define the network object on the **Objects** page.
Banner1	15	String	Single	The banner to display when the user logs in.
Banner2	36	String	Single	The second part of the banner to display when the user logs in. Banner2 is appended to Banner1.
Downloadable ACLs	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Supported via Cisco-AV-Pair configuration.

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Filter ACLs	86, 87	String	Single	Filter ACLs are referred to by ACL name in the RADIUS server. It requires the ACL configuration to be already present on the Firepower Threat Defense device, so that it can be used during RADIUS authorization. 86=Access-List-Inbound 87=Access-List-Outbound
Group-Policy	25	String	Single	The group policy to use in the connection. You must create the group policy on the RA VPN **Group Policy** page. You can use one of the following formats: • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	Integer	Single	The number of separate simultaneous connections the user is allowed to establish, 0 - 2147483647.
VLAN	140	Integer	Single	The VLAN on which to confine the user's connection, 0 - 4094. You must also configure this VLAN on a subinterface on the FTD device.

Create or Update Aliases for a Connection Profile

Aliases contain alternate names or URLs for a specific connection profile. Remote Access VPN administrators can enable or disable the Alias names and Alias URLs. VPN users can choose an Alias name when they connect to the Firepower Threat Defense device. Aliases names for all connections configured on this device can be turned on or off for display. You can also configure the list of Alias URLs, which your endpoints can select while initiating the Remote Access VPN connection. If users connect using the Alias URL, system will automatically log them using the connection profile that matches the Alias URL.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Select a **Connection Profile** and click **Edit**.

Step 4 Click **Aliases**.

Step 5 To add an Alias name, do the following:

a) Click **Add** under Alias Names.
b) Specify the **Alias Name**.
c) Select the **Enabled** check box in each window to enable the aliases.
d) Click **OK**.

Step 6 To add an Alias URL, do the following:

a) Click **Add** under Alias URLs.
b) Select the **Alias URL** from the list or create a new URL object. For more information see Creating URL Objects.
c) Select the **Enabled** check box in each window to enable the aliases.
d) Click **OK**.

- Click **Edit** to edit the Alias name or the Alias URL.
- To delete an Alias name or the Alias URL, click **Delete** in that row.

Step 7 Click **Save**.

Related Topics

Configure Connection Profile Settings, on page 17

Configure Access Interfaces for Remote Access VPN

The **Access Interface** table lists the interface groups and security zones that contain the device interfaces. These are configured for remote access SSL or IPsec IKEv2 VPN connections. The table displays the name of each interface group or security-zone, the interface trustpoints used by the interface, and whether Datagram Transport Layer Security (DTLS) is enabled.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Click **Access Interface**.

Step 4 To add an access interface, select **Add** and specify values for the following in the **Add Access Interface** window:

a) **Access Interface**—Select the interface group or security zone to which the interface belongs.

The interface group or security zone must be a Routed type. Other interface types are not supported for Remote Access VPN connectivity.

b) Associate the **Protocol** object with the access interface by selecting the following options:

- **Enable IPSet-IKEv2**—Select this option to enable **IKEv2** settings.
- **Enable SSL**—Select this option to enable **SSL** settings.
  - Select **Enable Datagram Transport Layer Security**.

    When selected, it enables Datagram Transport Layer Security (DTLS) on the interface and allows an AnyConnect VPN client to establish an SSL VPN connection using two simultaneous tunnels—an SSL tunnel and a DTLS tunnel.

    Enabling DTLS avoids the latency and bandwidth problems associated with certain SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

    To configure SSL settings for the AnyConnect VPN client, see Group Policy AnyConnect Options.
  - Select the **Configure Interface Specific Identity Certificate** check box and select **Interface Identity Certificate** from the drop-down list.

    If you do not select the Interface Identity Certificate, the **Trustpoint** will be used by default.

    If you do not select the Interface Identity Certificate or Trustpoint, the **SSL Global Identity Certificate** will be used by default.

c) Click **OK** to save the changes.

Step 5 Select the following under **Access Settings**:

- **Allow Users to select connection profile while logging in**—If you have multiple connection profiles, selecting this option allows the user to select the correct connection profile during login. You must select this option for **IPsec-IKEv2** VPNs.

Step 6 Use the following options to configure **SSL Settings**:

- **Web Access Port Number**—The port to use for VPN sessions. The default port is 443.
- **DTLS Port Number**—The UDP port to use for DTLS connections. The default port is 443.
- **SSL Global Identity Certificate**— The selected **SSL Global Identity Certificate** will be used for all the associated interfaces if the **Interface Specific Identity Certificate** is not provided.

Step 7 For **IPsec-IKEv2 Settings**, select the **IKEv2 Identity Certificate** from the list or add an identity certificate.

Step 8 Under the **Access Control for VPN Traffic** section, select the following option if you want to bypass access control policy:

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

  Note If you select this option, you need not update the access control policy for remote access VPN as specified in Update the Access Control Policy on the Firepower Threat Defense Device, on page 13.

Step 9 Click **Save** to save the access interface changes.

Related Topics

Interface Objects: Interface Groups and Security Zones

Configuring Remote Access VPN Advanced Options

Cisco AnyConnect Secure Mobility Client Image

Cisco AnyConnect Secure Mobility Client Image

The Cisco AnyConnect Secure Mobility client provides secure SSL or IPsec (IKEv2) connections to the Firepower Threat Defense device for remote users with full VPN profiling to corporate resources. Without a previously-installed client, remote users can enter the IP address of an interface configured to accept clientless VPN connections in their browser to download and install the AnyConnect client. The Firepower Threat Defense device downloads the client that matches the operating system of the remote computer. After downloading, the client installs and establishes a secure connection. In case of a previously installed client, when the user authenticates, the Firepower Threat Defense device, examines the version of the client, and upgrades the client if necessary.

The Remote Access VPN administrator associates any new or additional AnyConnect client images to the VPN policy. The administrator can unassociate the unsupported or end of life client packages that are no longer required.

The Firepower Management Center determines the type of operating system by using the file package name. If the user renamed the file without indicating the operating system information, the valid operating system type must be selected from the list box.

Download the AnyConnect client image file by visiting Cisco Software Download Center.

Related Topics

Adding a Cisco AnyConnect Mobility Client Image to the Firepower Management Center, on page 35

Adding a Cisco AnyConnect Mobility Client Image to the Firepower Management Center

You can upload the Cisco AnyConnect Mobility client image to the Firepower Management Center by using the **AnyConnect File** object. For more information, see Firepower Threat Defense File Objects. For more information about the client image, see Cisco AnyConnect Secure Mobility Client Image, on page 34.

Click **Show re-order** link to view a specific client image.

Note To delete an already installed Cisco AnyConnect client image, click **Delete** in that row.

Step 1 On the Firepower Management Center web interface, choose **Devices > VPN > Remote Access**, choose and edit a listed RA VPN policy, then choose the **Advanced** tab.

Step 2 Click **Add** in the **Available AnyConnect Images** portion of the **AnyConnect Images** dialog.

Step 3 Enter the **Name**, **File Name**, and **Description** for the available AnyConnect Image.

Step 4 Click **Browse** to navigate to the location for selecting the client image to be uploaded.

Step 5 Click **Save** to upload the image in the Firepower Management Center.

Once you upload the client image to the Firepower Management Center, the operating system displays platform information for the image that you uploaded to the Firepower Management Center.

Related Topics

Cisco AnyConnect Secure Mobility Client Image, on page 34

Update AnyConnect Images for Remote Access VPN Clients

When new AnyConnect client updates are available in Cisco Software Download Center, you can download the packages manually and add them to the remote access VPN policy so that the new AnyConnect packages are upgraded on the VPN client systems according to their operating systems.

Before you begin

Instructions in this section help you update new AnyConnect client images to remote access VPN clients connecting to Firepower Threat Defense VPN gateway. Ensure that the following configurations are complete before updating your AnyConnect images:

- Download the latest AnyConnect image files from Cisco Software Download Center.
- On your Firepower Management Center web interface, go to **Objects** > **Object Management** > **VPN** > **AnyConnect File** and add the new AnyConnect client image files.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access policy in the list and click **Edit**.

Step 3 Click **Advanced** > **AnyConnect Client Image**> **Add**.

Step 4 Select a client image file from **Available AnyConnect Images** and click **Add**.

If the required AnyConnect client image is not listed, click **Add** to browse and upload an image.

Step 5 Save the remote access VPN policy.
After the remote access VPN policy changes are deployed, the new AnyConnect client images are updated on the Firepower Threat Defense device that is configured as the remote access VPN gateway. When a new VPN user connects to the VPN gateway, the user will get the new AnyConnect client image to download depending on the operating system of the client system. For existing VPN users, the AnyConnect client image will be updated in their next VPN session.

Related Topics

Remote Access VPN Connection Profile Options

Remote Access VPN Address Assignment Policy

The Firepower Threat Defense device can use an IPv4 or IPv6 policy for assigning IP addresses to Remote Access VPN clients. If you configure more than one address assignment method, the Firepower Threat Defense device tries each of the options until it finds an IP address.

IPv4 or IPv6 Policy

You can use the IPv4 or IPv6 policy to address an IP address to Remote Access VPN clients. Firstly, you must try with the IPv4 policy and later followed by IPv6 policy.

- **Use Authorization Server**—Retrieves address from an external authorization server on a per-user basis. If you are using an authorization server that has IP address configured, we recommend using this method. Address assignment is supported by RADIUS-based authorization server only. It is not supported for AD/LDAP. This method is available for both IPv4 and IPv6 assignment policies.
- **Use DHCP**—Obtains IP addresses from a DHCP server configured in a connection profile. You can also define the range of IP addresses that the DHCP server can use by configuring DHCP network scope in the group policy. If you use DHCP, configure the server in the **Objects > Object Management > Network** pane. This method is available for IPv4 assignment policies.

  For more information about DHCP network scope configuration, see Group Policy General Options.
- **Use an internal address pool**—Internally configured address pools are the easiest method of address pool assignment to configure. If you use this method, create the IP address pools in the **Objects > Object Management >Address Pools** pane and select the same in the connection profile. This method is available for both IPv4 and IPv6 assignment policies.
- **Reuse an IP address so many minutes after it is released**—Delays the reuse of an IP address after its return to the address pool. Adding a delay helps to prevent problems firewalls can experience when an IP address is reassigned quickly. By default, the delay is set to zero, meaning the Firepower Threat Defense device does not impose a delay in reusing the IP address. If you want to extend the delay, enter the number of minutes in the range 0 - 480 to delay the IP address reassignment. This configurable element is available for IPv4 assignment policies.

Related Topics

Configure Connection Profile Settings, on page 17
Remote Access VPN Authentication, on page 4

Configure Certificate Maps

Certificate maps let you define rules matching a user certificate to a connection profile based on the contents of the certificate fields. Certificate maps are used for certificate authentication on secure gateways.

The rules or the certificate maps are defined in Firepower Threat Defense Certificate Map Objects.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Click **Advanced** > **Certificate Maps**.

Step 4 Select the following options under the **General Settings for Certificate Group Matching** pane:

Selections are priority-based, if a match is not found for the first selection matching continues down the list of options. When the rules are satisfied, the mapping is done. If the rules are not satisfied, the default connection profile (listed at the bottom) is used for this connection. Select any, or all, of the following options to establish authentication and to determine which connection profile (tunnel group) that should be mapped to the client.

- **Use Group URL if Group URL and Certificate Map match different Connection profiles**
- **Use the configured rules to match a certificate to a Connection Profile**—Enable this to use the rules defined here in the Connection Profile Maps.

Note Configuring a certificate mapping implies certificate-based authentication. The remote user will be prompted for a client certificate regardless of the configured Authentication Method.

Step 5 Under the **Certificate to Connection Profile Mapping** section, click **Add Mapping** to create certificate to connection profile mapping for this policy.

a) Choose or create a **Certificate Map** object.
b) Select the **Connection Profile** that should be used if the rules in the certificate map object are satisfied.
c) Click **OK** to create the mapping.

Step 6 Click **Save**.

Configuring Group Policies

A group policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. For example, in the group policy object, you configure general attributes such as addresses, protocols, and connection settings.

The group policy applied to a user is determined when the VPN tunnel is being established. The RADIUS authorization server assigns the group policy, or it is obtained from the current connection profile.

Note There is no group policy attribute inheritance on the Firepower Threat Defense. A group policy object is used, in its entirety, for a user. The group policy object identified by the AAA server upon login is used, or, if that is not specified, the default group policy configured for the VPN connection is used. The provided default group policy can be set to your default values, but will only be used if it is assigned to a connection profile and no other group policy has been identified for the user.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Click **Advanced** > **Group Policies**.

Step 4 Select one or more group policies to associate with this remote access VPN policy. These are above and beyond the default group policy assigned during the remote access VPN policy creation. Click **Add**.

Use the **Refresh** and **Search** utilities to locate the group policy. Add a new group policy object if necessary.

Step 5 Select group policies from the available group policy and click **Add** to select them.

Step 6 Click **OK** to complete the group policy selection.

Related Topics

Configure Group Policy Objects

Configuring IPsec Settings for Remote Access VPNs

The IPsec settings are applicable only if you selected IPsec as the VPN protocol while configuring your remote access VPN policy. If not, you can enable IKEv2 using the Edit Access Interface dialog box. See Configure Access Interfaces for Remote Access VPN, on page 33 for more information.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click **Advanced**.

The list of IPsec settings appears in a navigation pane on the left of the screen.

Step 4 Use the navigation pane to edit the following IPsec options:

a) **Crypto Maps**—The Crypto Maps page lists the interface groups on which IKEv2 protocol is enabled. Crypto Maps are auto generated for the interfaces on which IKEv2 protocol is enabled. To edit a Crypto Map, see Configure Remote Access VPN Crypto Maps, on page 39. You can add or remove interface groups to the selected VPN policy in **Access Interface**. See Configure Access Interfaces for Remote Access VPN, on page 33 for more information.

b) **IKE Policy**—The IKE Policy page lists all the IKE policy objects applicable for the selected VPN policy when AnyConnect endpoints connect using the IPsec protocol. See IKE Policies in Remote Access VPNs, on page 40 for more information. To add a new IKE policy, see Configure IKEv2 Policy Objects. Firepower Threat Defense supports only AnyConnect IKEv2 clients. Third-party standard IKEv2 clients are not supported.

c) **IPsec/IKEv2 Parameters**—The IPsec/IKEv2 Parameters page enables you to modify the IKEv2 session settings, IKEv2 Security Association settings, IPsec settings, and NAT Transparency settings. See Configure Remote Access VPN IPsec/IKEv2 Parameters, on page 42 for more information.

Step 5 Click **Save**.

Configure Remote Access VPN Crypto Maps

Crypto maps are automatically generated for the interfaces on which IPsec-IKEv2 protocol has been enabled. You can add or remove interface groups to the selected VPN policy in **Access Interface**. See Configure Access Interfaces for Remote Access VPN, on page 33 for more information.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click the **Advanced** > **Crypto Maps**, and select a row in the table and click **Edit** to edit the Crypto map options.

Step 4 Select **IKEv2 IPsec Proposals** and select the transform sets to specify which authentication and encryption algorithms will be used to secure the traffic in the tunnel.

Step 5 Select **Enable Reverse Route Injection** to enable static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint.

Step 6 Select **Enable Client Services** and specify the port number.

The Client Services Server provides HTTPS (SSL) access to allow the AnyConnect Downloader to receive software upgrades, profiles, localization and customization files, CSD, SCEP, and other file downloads required by the AnyConnect client. If you select this option, specify the client services port number. If you do not enable the Client Services Server, users will not be able to download any of these files that the AnyConnect client might need.

Note You can use the same port that you use for SSL VPN running on the same device. Even if you have an SSL VPN configured, you must select this option to enable file downloads over SSL for IPsec-IKEv2 clients.

Step 7 Select **Enable Perfect Forward Secrecy** and select the **Modulus group**.

Use Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices. If you select this option, also select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key in the **Modulus Group** list.

Modulus group is 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 the modulus group that you want to allow in the remote access VPN configuration:

- 1—Diffie-Hellman Group 1 (768-bit modulus).
- 2—Diffie-Hellman Group 2 (1024-bit modulus).
- 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher).
- 14—Diffie-Hellman Group 14 (2048-bit modulus, considered good protection for 128-bit keys).
- 19—Diffie-Hellman Group 19 (256-bit elliptical curve field size).
- 20—Diffie-Hellman Group 20 (384-bit elliptical curve field size).
- 21—Diffie-Hellman Group 21 (521-bit elliptical curve field size).

- 24—Diffie-Hellman Group 24 (2048-bit modulus and 256-bit prime order subgroup).

Step 8 Specify the **Lifetime Duration (seconds)**.

The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. Generally, 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.

You can specify a value from 120 to 2147483647 seconds. The default is 28800 seconds.

Step 9 Specify the **Lifetime Size (kbytes)**.

The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires.

You can specify a value from 10 to 2147483647 kbytes. The default is 4,608,000 kilobytes. No specification allows infinite data.

Step 10 Select the following **ESPv3 Settings**:

- **Validate incoming ICMP error messages**—Choose whether to validate ICMP error messages received through an IPsec tunnel and destined for an interior host on the private network.
- **Enable 'Do Not Fragment' Policy**—Define how the IPsec subsystem handles large packets that have the do-not-fragment (DF) bit set in the IP header, and select one of the following from the **Policy** list:
  - Copy—Maintains the DF bit.
  - Clear—Ignores the DF bit.
  - Set—Sets and uses the DF bit.
- Select Enable Traffic Flow Confidentiality (TFC) Packets— Enable dummy TFC packets that mask the traffic profile which traverses the tunnel. Use the **Burst**, **Payload Size**, and **Timeout** parameters to generate random length packets at random intervals across the specified SA.

  Note Enabling traffic flow confidentiality (TFC) packets prevents the VPN tunnel from being idle. Thus the VPN idle timeout configured in the group policy does not work as expected when you enable the TFC packets.

  - Burst—Specify a value from 1 to 16 bytes.
  - Payload Size—Specify a value from 64 to 1024 bytes.
  - Timeout—Specify a value from 10 to 60 seconds.

Step 11 Click **OK**.

Related Topics

Interface Objects: Interface Groups and Security Zones

IKE Policies in Remote Access VPNs

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.

Note Firepower Threat Defense supports only IKEv2 for remote access VPNs.

Unlike IKEv1, in an IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy. Since peers choose during the Phase 1 negotiation, this makes it possible to create a single IKE proposal, but consider multiple, different proposals to give higher priority to your most desired options. For IKEv2, the policy object does not specify authentication, other policies must define the authentication requirements.

An IKE policy is required when you configure a remote access IPsec VPN.

Configuring Remote Access VPN IKE Policies

The IKE Policy table specifies all the IKE policy objects applicable for the selected VPN configuration when AnyConnect endpoints connect using the IPsec protocol. For more information, see IKE Policies in Remote Access VPNs, on page 40.

Note Firepower Threat Defense supports only IKEv2 for remote access VPNs.

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click **Advanced** > **IKE Policy**.

Step 4 Click **Add** to select from the available IKEv2 policies, or add a new IKEv2 policy and specify the following:

- **Name**—Name of the IKEv2 policy.
- **Description**—Optional description of the IKEv2 policy
- **Priority**—The priority value determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA).
- **Lifetime**— Lifetime of the security association (SA), in seconds
- **Integrity**—The Integrity Algorithms portion of the Hash Algorithm used in the IKEv2 policy.
- **Encryption**—The Encryption Algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations.
- **PRF Hash**—The pseudorandom function (PRF) portion of the Hash Algorithm used in the IKE policy. In IKEv2, you can specify different algorithms for these elements.
- **DH Group**—The Diffie-Hellman group used for encryption.

Step 5 Click **Save**.

Related Topics

Remote Access VPN Access Interface Options

Configure Remote Access VPN IPsec/IKEv2 Parameters

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click **Advanced** > **IPsec**> **IPsec/IKEv2 Parameters**.

Step 4 Select the following for **IKEv2 Session Settings**:

- **Identity Sent to Peers**—Choose the identity that the peers will use to identify themselves during IKE negotiations:
  - **Auto**—Determines the IKE negotiation by connection type: IP address for preshared key, or Cert DN for certificate authentication (not supported).
  - **IP address**—Uses the IP addresses of the hosts exchanging ISAKMP identity information.
  - **Hostname**—Uses the fully qualified domain name (FQDN) of the hosts exchanging ISAKMP identity information. This name comprises the hostname and the domain name.
- **Enable Notification on Tunnel Disconnect**—Allows an administrator to enable or disable the sending of an IKE notification to the peer when an inbound packet that is received on an SA does not match the traffic selectors for that SA. Sending this notification is disabled by default.
- **Do not allow device reboot until all sessions are terminated**—Check to enable waiting for all active sessions to voluntarily terminate before the system reboots. This is disabled by default.

Step 5 Select the following for **IKEv2 Security Association (SA) Settings**:

- **Cookie Challenge**—Whether to send cookie challenges to peer devices in response to SA initiated packets, which can help thwart denial of service (DoS) attacks. The default is to use cookie challenges when 50% of the available SAs are in negotiation. Select one of these options:
  - **Custom**—Specify **Threshold to Challenge Incoming Cookies**, the percentage of the total allowed SAs that are in-negotiation. This triggers cookie challenges for any future SA negotiations. The range is zero to 100%. The default is 50%.
  - Always— Select to send cookie challenges to peer devices always.
  - Never— Select to never send cookie challenges to peer devices.
-
- **Number of SAs Allowed in Negotiation**—Limits the maximum number of SAs that can be in negotiation at any time. If used with Cookie Challenge, configure the cookie challenge threshold lower than this limit for an effective cross-check. The default is 100 %.
- **Maximum number of SAs Allowed**—Limits the number of allowed IKEv2 connections.

Step 6 Select the following for **IPsec Settings**:

- **Enable Fragmentation Before Encryption**—This option lets traffic travel across NAT devices that do not support IP fragmentation. It does not impede the operation of NAT devices that do support IP fragmentation.
- **Path Maximum Transmission Unit Aging**—Check to enable PMTU (Path Maximum Transmission Unit) Aging, the interval to Reset PMTU of an SA (Security Association).
- **Value Reset Interval**—Enter the number of minutes at which the PMTU value of an SA (Security Association) is reset to its original value. Valid range is 10 to 30 minutes, default is unlimited.

Step 7 Select the following for **NAT Settings**:

- **Keepalive Messages Traversal**—Select whether to enable NAT keepalive message traversal. NAT traversal keepalive is used for the transmission of keepalive messages when there is a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow. If you select this option, configure the interval, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active. The value can be from 10 to 3600 seconds. The default is 20 seconds.
- **Interval**—Sets the NAT keepalive interval, from 10 to 3600 seconds. The default is 20 seconds.

Step 8 Click **Save**.

Customizing Remote Access VPN AAA Settings

This section provides information about customizing your AAA preferences for remote access VPNs. For more information, see Configure AAA Settings for Remote Access VPN, on page 20.

Authenticate VPN Users via Client Certificates

You can configure remote access VPN authentication using client certificate when you create a new remote access VPN policy using the wizard or by editing the policy later.

Before you begin

Configure the certificate enrollment object that is used to obtain the identity certificate for each Firepower Threat Defense device that acts as a VPN gateway.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**; or click **Add** to create a new remote access VPN policy.

Step 3 For a new remote access VPN policy, configure the authentication while selecting connection profile settings. For an existing configuration, select the connection profile that includes the client profile, and click **Edit**.

Step 4 Click **AAA** > **Authentication Method** > **Client Certificate Only**.

With this authentication method, the user is authenticated using a client certificate. You must configure the client certificate on VPN client endpoints. By default, the user name is derived from client certificate fields CN and OU respectively. If the user name is specified in other fields in the client certificate, use 'Primary' and 'Secondary' field to map appropriate fields.

If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display the following default values, respectively: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN as username** option, the system automatically retrieves the user identity. A distinguished name (DN) is a unique identification, made up of individual fields, that can be used as the identifier when matching users to a connection profile. DN rules are used for enhanced certificate authentication.

- Primary and Secondary fields pertaining to the **Map specific field** option contains these common values:
  - C (Country)
  - CN (Common Name)
  - DNQ (DN Qualifier
  - EA (Email Address)
  - GENQ (Generational Qualifier)
  - GN (Given Name)
  - I (Initial)
  - L (Locality)
  - N (Name)
  - O (Organisation)
  - OU (Organisational Unit)
  - SER (Serial Number)
  - SN (Surname)
  - SP (State Province)
  - T (Title)
  - UID (User ID)
  - UPN (User Principal Name)
- Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

For more information, see Configure AAA Settings for Remote Access VPN, on page 20.

Related Topics

Configure Connection Profile Settings, on page 17
Adding Certificate Enrollment Objects

Configure Remote Access VPN Login via Client Certificate and AAA Server

When remote access VPN authentication is configured to use both client certificate and authentication server, VPN client authentication is done using both the client certificate validation and AAA server.

Before you begin

- Configure the certificate enrollment object that is used to obtain the identity certificate for each Firepower Threat Defense device that acts as a VPN gateway.
- Configure the RADIUS server group object and any AD or LDAP realms being used by this remote access VPN policy.
- Ensure that the AAA Server is reachable from the Firepower Threat Defense device for the remote access VPN configuration to work.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a existing remote access policy and click **Edit**; or click **Add** to create a new remote access VPN policy.

Step 3 For a new remote access VPN policy, configure the authentication while selecting connection profile settings. For an existing configuration, select the connection profile that includes the client profile, and click **Edit**.

Step 4 Click **AAA** > **Authentication Method**, **Client Certificate & AAA**.

- When you select the **Authentication Method** as:

Client Certificate & AAA—Both types of authentication are done.

- **AAA**—If you select the **Authentication Server** as **RADIUS**, by default, the Authorization Server has the same value. Select the **Accounting Server** from the drop-down list. Whenever you select **AD** and **LDAP** from the Authentication Server drop-down list, you must manually select the **Authorization Server** and **Accounting Server** respectively.
- **Client Certificate**—User is authenticated using client certificate. Client certificate must be configured on VPN client endpoints. By default, user name is derived from client certificate fields CN & OU respectively. In case, user name is specified in other fields in the client certificate, use 'Primary' and 'Secondary' field to map appropriate fields.

  If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN as username** option, the system automatically retrieves the user identity. A distinguished name (DN) is a unique identification, made up of individual fields, that can be used as the identifier when matching users to a connection profile. DN rules are used for enhanced certificate authentication.

  Primary and Secondary fields pertaining to the **Map specific field** option contains these common values:

  - C (Country)
  - CN (Common Name)
  - DNQ (DN Qualifier
  - EA (Email Address)
  - GENQ (Generational Qualifier)
  - GN (Given Name)
  - I (Initial)
  - L (Locality)
  - N (Name)

- O (Organisation)
- OU (Organisational Unit)
- SER (Serial Number)
- SN (Surname)
- SP (State Province)
- T (Title)
- UID (User ID)
- UPN (User Principal Name)

- Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

For more information, see Configure AAA Settings for Remote Access VPN, on page 20.

Related Topics

Configure Connection Profile Settings, on page 17
Adding Certificate Enrollment Objects

Manage Password Changes over VPN Sessions

Password management allows a remote access VPN administrator to configure the notification settings for the remote access VPN users on their password expiry. Password management is available in AAA settings with authentication methods AAA Only and Client Certificate & AAA. For more information, see Configure AAA Settings for Remote Access VPN, on page 20.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**.

Step 3 Select the connection profile that includes AAA settings and click **Edit**.

Step 4 Select **AAA** > **Advanced Settings** > **Password Management**.

Step 5 Select **Enable Password Management** and select one of the following:

- Notify User - Notify user ahead of password expiry; specify the number of days in the box.
- Notify user on the day of password expiration - Notify user on the day their passwords expire.

Step 6 Click **Save**.

Related Topics

Configure Connection Profile Settings, on page 17

Configure LDAP or Active Directory for Authorization

When you want to configure remote access VPN with LDAP or Active Directory (AD) server for authorization, you must configure an attribute map using a FlexConfig object as the attribute map is not supported directly on Firepower Management Center web interface.

Before you begin

Ensure that you have created a Realm object for LDAP or AD.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Create a remote access VPN policy with LDAP or AD realm object as the authentication server. Or edit an existing remote access VPN configuration and select LDAP or AD realm as the authentication server.

Step 3 Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

Step 4 Create a FlexConfig policy and create and assign the following two FlexConfig objects in the append section:

See Configure the FlexConfig Policy.

a) Create the FlexConfig Object for LDAP Attribute Map with **Deployment type**: Once and **Type**: Append.

Enter the following in the object body:

```
lda attribute-map <LDAP_Map_for_VPN_Access>
          map-name  memberOf Group-Policy
          map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
LabAdminAccessGroupPolicy
          map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com VPNAccessGroupPolicy
```

b) Create a FlexConfig Object associating the LDAP attribute map to the LDAP AAA-server, with **Deployment type**: Everytime and **Type**: Append.

Note This mapping is required to reinstate the LDAP-attribute-map association because it is negated by Firepower Management Center.

Enter the following in the object body area:

```
aaa-server <LDAP/AD_Realm_name> host <AD Server IP>
          ldap-attribute-map <LDAP_Map_for_VPN_Access>
          exit
```

Use the same *aaa-server* same as the LDAP realm name used in the AAA server settings of the connection profile that you have added to the remote access VPN policy configuration.

For more information, see Configure FlexConfig Text Objects.

a) Click **Save**.

Make sure the order of the FlexConfig objects in the FlexConfig Policy is the LDAP Attribute Map FlexConfig object followed by the AAA-server object.

This will configure the LDAP attribute map and associate it with the LDAP server configuration on the Firepower Threat Defense device.

Related Topics

Configure FlexConfig Objects

Send Accounting Records to the RADIUS Server

Accounting records in remote access VPN help the VPN administrator track the services that users access and the amount of network resources they consume. Accounting information includes when users 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. This data can then be analyzed for network management, client billing, or auditing.

You can use accounting alone or together with authentication and authorization. When you activate AAA accounting, the network access server reports user activity to the configured accounting server. You can configure a RADIUS server as the accounting server so that all the user activity information is sent from Firepower Management Center to the RADIUS server.

Note You can use the same RADIUS server or separate RADIUS servers for authentication, authorization, and accounting in remote access VPN AAA settings.

Before you begin

Configure a RADIUS group object with RADIUS servers to which authentication requests or accounting records will be sent. See RADIUS Server Group Options.

Ensure that the RADIUS servers are reachable from the Firepower Threat Defense device. Configure routing on your Firepower Management Center at **Devices** > **Device Management** > **Edit Device** > **Routing** to ensure connectivity to the RADIUS server.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**, or create a new remote access VPN policy.

Step 3 Select the connection profile that includes AAA settings and click **Edit** > **AAA**.

Step 4 Select a RADIUS server as the **Accounting Server**.

Step 5 Click **Save**.

Related Topics

Configure Connection Profile Settings, on page 17
Configure AAA Settings for Remote Access VPN, on page 20

Delegating Group Policy Selection to Authorization Server

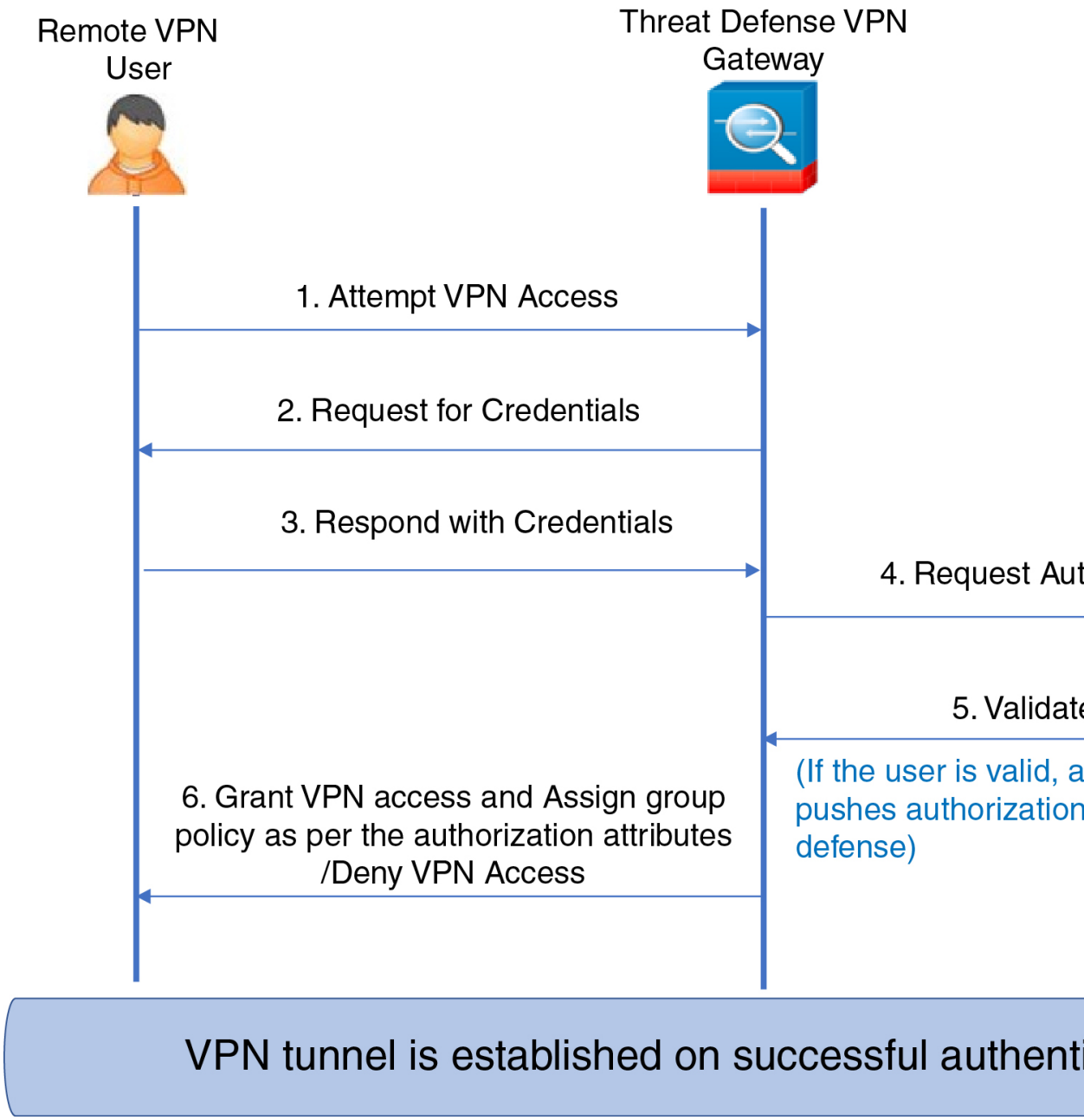
The group policy applied to a user is determined when the VPN tunnel is being established. You can select a group policy for a connection profile while creating a remote access VPN policy using the wizard or update the connection policy for connection profiles later. However, you can configure the AAA (RADIUS) server to assign the group policy or it is obtained from the current connection profile. If the Firepower Threat Defense device receives attributes from the external AAA server that conflicts with those configured on the connection profile, then attributes from the AAA server always take the precedence.

You can configure ISE or the RADIUS Server to set the Authorization Profile for a user or user-group by sending IETF RADIUS Attribute 25 and map to the corresponding group policy name. You can configure specific group policy to a user or user group to push a Downloadable ACL, set a banner, Restrict VLAN, and

configure the advanced option of applying an SGT to the session. These attributes are applied to all users that are part of that group when the VPN connection is established.

For more information, see the Configure Standard Authorization Policies section of Cisco Identity Services Engine Administrator Guide and RADIUS Server Attributes for Firepower Threat Defense, on page 23.

Figure 1: Remote Access VPN Group Policy Selection by AAA Server



Related Topics

Configure Group Policy Objects
Configure Connection Profile Settings, on page 17

Override the Selection of Group Policy or Other Attributes by the Authorization Server

When a remote access VPN user connects to the VPN, the group policy and other attributes configured in the connection profile are assigned to the user. However, the remote access VPN system administrator can delegate the selection of group policy and other attributes to the authorization server by configuring ISE or the RADIUS Server to set the Authorization Profile for a user or user-group. Once users are authenticated, these specific authorization attributes are pushed to the Firepower Threat Defense device.

Before you begin

Ensure that you configure a remote access VPN policy with RADIUS as the authentication server.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**.

Step 3 Select RADIUS or ISE as the authorization server if not configured already.

Step 4 Select **Advanced** > **Group Policies** and add the required group policy. For detailed information about a group policy object, see Configure Group Policy Objects.

You can map only one group policy to a connection profile; but you can create multiple group policies in a remote access VPN policy. These group policies can be referenced in ISE or the RADIUS server and configured to override the group policy configured in the connection profile by assigning the authorization attributes in the authorization server.

Step 5 Deploy the configuration on the target Firepower Threat Defense device.

Step 6 On the authorization server, create an Authorization Profile with RADIUS attributes for IP address and downloadable ACLs.

When the group policy is configured in the authorization server selected for remote access VPN, the group policy overrides the group policy configured in the connection profile for the remote access VPN user after the user is authenticated.

Related Topics

Configure Group Policy Objects

Deny VPN Access to a User Group

When you do not want an authenticated user or user group to be able to use VPN, you can configure a group policy to deny VPN access. You can configure a group policy in a remote access VPN policy and reference it in the ISE or RADIUS server configuration for authorization.

Before you begin

Ensure that you have configured remote access VPN using the Remote Access Policy wizard and configured authentication settings for the remote access VPN policy.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**.

Step 3 Select **Advanced** > **Group Policies**.

Step 4 Select a group policy and click **Edit** or add a new group policy.

Step 5 Select **Advanced** > **Session Settings** and set **Simultaneous Login Per User** to 0 (zero).

This stops the user or user group from connecting to the VPN even once.

Step 6 Click **Save** to save the group policy and then save the remote access VPN configuration.

Step 7 Configure ISE or the RADIUS server to set the Authorization Profile for that user/user-group to send IETF RADIUS Attribute 25 and map to the corresponding group policy name.

Step 8 Configure the ISE or RADIUS server as the authorization server in the remote access VPN policy.

Step 9 Save and deploy the remote access VPN policy.

Related Topics

Configure Connection Profile Settings, on page 17

Restrict Connection Profile Selection for a User Group

When you want to enforce a single connection profile on a user or user group, you can choose to disable the connection profile so that the group alias or URLs are not available for the users to select when they connect using the AnyConnect VPN client.

For example, if your organization wants to use specific configurations for different VPN user groups such as mobile users, corporate-issued laptop users, or personal laptop users, you can configure connection a profile specific to each of these user groups and apply the appropriate connection profile when the user connects to the VPN.

The AnyConnect client, by default, shows a list of the connection profiles (by connection profile name, alias, or alias URL) configured in Firepower Management Center and deployed on Firepower Threat Defense. If custom connection profiles are not configured, AnyConnect shows the *DefaultWEBVPNGroup* connection profile. Use the following procedure to enforce a single connection profile for a user group.

Before you begin

- On your Firepower Management Center web interface, configure remote access VPN using the remote access VPN policy wizard with Authentication Method as 'Client Certificate Only' or 'Client Certificate + AAA'. Choose the username fields from the certificate.
- Configure ISE or RADIUS server for authorization and associate the group policy with the authorization server.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**.

Step 3 Select **Access Interfaces** and disable **Allow users to select connection profile while logging in**.

Step 4 Click **Advanced** > **Certificate Maps**.

Step 5 Select **Use the configured rules to match a certificate to a Connection Profile**.

Step 6 Select the **Certificate Map Name** or click the **Add** icon to add a certificate rule.

Step 7 Select the **Connection Profile**, and click **Ok**.
With this configuration, when a user connects from the AnyConnect client, the user will have the mapped connection profile and will be authenticated to use the VPN.

Related Topics

Configure Group Policy Objects

Configure Connection Profile Settings, on page 17

Update the AnyConnect Client Profile for Remote Access VPN Clients

AnyConnect Client Profile is an XML file that contains an administrator-defined end user requirements and authentication policies to be deployed on a VPN client system as part of AnyConnect. It makes the preconfigured network profiles available to end users.

You can use the GUI-based AnyConnect Profile Editor, an independent configuration tool, to create an AnyConnect Client Profile. The standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from Cisco Software Download Center.

See the AnyConnect Profile Editor chapter in the appropriate release of the Cisco AnyConnect Secure Mobility Client Administrator Guide for details.

Before you begin

- Ensure that you have configured remote access VPN using the Remote Access Policy wizard and deployed the configuration on Firepower Threat Defense device. See Create a New Remote Access VPN Policy, on page 12.
- On your Firepower Management Center web interface, go to **Objects** > **Object Management** > **VPN** > **AnyConnect File** and add the new AnyConnect client image.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access VPN policy and click **Edit**.

Step 3 Select the connection profile that includes the client profile to be edited, and click **Edit**.

Step 4 Click **Edit Group Policy** > **AnyConnect** > **Profiles**.

Step 5 Select the client profile XML file from the list or click **Add** to add a new client profile.

Step 6 Save the group policy, connection profile, and then the remote access VPN policy.

Step 7 Deploy the changes.
Changes to the client profile will be updated on the VPN clients when they connect to the remote access VPN gateway.

Related Topics

Configure Group Policy Objects

RADIUS Dynamic Authorization

Firepower Threat Defense has the capability to use RADIUS servers for user authorization of VPN remote access and firewall cut-through-proxy sessions using dynamic access control lists (ACLs) or ACL names per user. To implement dynamic ACLs for dynamic authorization or RADIUS Change of Authorization (RADIUS CoA), you must configure the RADIUS server to support them. When the user tries to authenticate, the RADIUS server sends a downloadable ACL or ACL name to the Firepower Threat Defense. Access to a given service is either permitted or denied by the ACL. Firepower Threat Defense deletes the ACL when the authentication session expires.

Related Topics

RADIUS Server Groups
Interface Objects: Interface Groups and Security Zones

Configuring RADIUS Dynamic Authorization, on page 53
RADIUS Server Attributes for Firepower Threat Defense, on page 23

Configuring RADIUS Dynamic Authorization

Before you begin:

- Only one interface can be configured in the security zone or interface group if it is referred in a RADIUS Server.
- A dynamic authorization enabled RADIUS server requires Firepower Threat Defense 6.3 or later for the dynamic authorization to work.
- Interface selection in RADIUS server is not supported on Firepower Threat Defense 6.2.3 or earlier versions. The interface option will be ignored during deployment.
- FTD posture VPN does not support group policy change through dynamic authorization or RADIUS change of authorization (CoA).

Table 4: Procedure

	Do This	More Info
Step 1	Log on to your Firepower Management Center web interface.	
Step 2	Configure a RADIUS server object with dynamic authorization.	RADIUS Server Group Options
Step 3	Configure a route to ISE server through an interface enabled for change of authorization (CoA) to establish connectivity from Firepower Threat Defense to RADIUS server through routing or a specific interface.	RADIUS Server Group Options Configure ISE/ISE-PIC for User Control
Step 4	Configure a remote access VPN policy and select the RADIUS server group object that you have created with dynamic authorization.	Create a New Remote Access VPN Policy, on page 12
Step 5	Configure the DNS server details and domain-lookup interfaces using the Platform Settings.	Configure DNS, on page 15 DNS Server Group Objects
Step 6	Configure a split-tunnel in group policy to allow DNS traffic through Remote Access VPN tunnel if the DNS server is reachable through VNP network.	Configure Group Policy Objects
Step 7	Deploy the configuration changes.	Deploy Configuration Changes

Two-Factor Authentication

You can configure two-factor authentication for the remote access VPN. With two-factor authentication, the user must supply a username and static password, plus an additional item such as an RSA token or a passcode. Two-factor authentication differs from using a second authentication source in that two-factor is configured on a single authentication source, with the relationship to the RSA server tied to the primary authentication source.

Firepower Threat Defense supports RSA tokens and Duo Push authentication requests to Duo Mobile for the second factor in conjunction with any RADIUS or AD server as the first factor in the two-factor authentication process.

Configuring RSA Two-Factor Authentication

About this task:

You can configure the RADIUS or AD server as the authentication agent in the RSA server, and use the server in Firepower Management Center as the primary authentication source in the remote access VPN.

When using this approach, the user must authenticate using a username that is configured in the RADIUS or AD server, and concatenate the password with the one-time temporary RSA token, separating the password and token with a comma: *password*,*token*.

In this configuration, it is typical to use a separate RADIUS server (such as one supplied in Cisco ISE) to provide authorization services. You would configure the second RADIUS server as the authorization and, optionally, accounting server.

Before you begin:

Ensure that the following configurations are complete before configuring RADIUS two-factor authentication on Firepower Threat Defense:

On the RSA Server

- Configure RADIUS or Active Directory server as an authentication agent.
- Generate and download the configuration (*sdconf.rec*) file.
- Create a token profile, assign the token to the user, and distribute the token to the user. Download and install the token on the remote access VPN client system.

For more information, see RSA SecureID Suite documentation.

On the ISE Server

- Import the configuration (*sdconf.rec*) file generated on the RSA server.
- Add the RSA server as the external identity source and specify the shared secret.

Table 5: Procedure

	Do This	More Info
Step 1	Log on to your Firepower Management Center web interface.	

	Do This	More Info
Step 2	Create a RADIUS server group.	RADIUS Server Group Options
Step 3	Create a RADIUS Server object within the new RADIUS server group, with RADIUS or AD server as the host and with a timeout of 60 seconds or more.	RADIUS Server Options **Note** The RADIUS or AD server must be the same server that is configured as the authentication agent in RSA server. For two-factor authentication, make sure that the timeout is updated to 60 seconds or more in the AnyConnect client profile XML file as well.
Step 4	Configure a new remote access VPN policy using the wizard or edit an existing remote access VPN policy.	Create a New Remote Access VPN Policy, on page 12
Step 5	Select RADIUS as the authentication server and then select the newly-created RADIUS server group as the authentication server.	Configure AAA Settings for Remote Access VPN, on page 20
Step 7	Deploy the configuration changes.	Deploy Configuration Changes

Configuring Duo Two-Factor Authentication

About this task:

You can configure the Duo RADIUS server as the primary authentication source. This approach uses the Duo RADIUS Authentication Proxy. (You cannot use a direct connection with the Duo Cloud Service over LDAPS.)

For the detailed steps to configure Duo, see https://duo.com/docs/cisco-firepower.

You would then configure Duo to forward authentication requests directed to the proxy server to use another RADIUS server, or an AD server, as the first authentication factor, and the Duo Cloud Service as the second factor.

When using this approach, the user must authenticate using a username that is configured on both the Duo Cloud or web server, and the associated RADIUS server. The user must enter the password configured in the RADIUS server, followed by one of the following Duo codes:

- **Duo-passcode**. For example, *my-password*,123456.
- **push**. For example, *my-password*,**push**. Use push to tell Duo to send a push authentication to the Duo Mobile app, which the user must have already installed and registered.
- **sms**. For example, *my-password*,**sms**. Use **sms** to tell Duo to send an SMS message with a new batch of passcodes to the user's mobile device. The user's authentication attempt will fail when using **sms**. The user must then re-authenticate and enter the new passcode as the secondary factor.
- **phone**. For example, *my-password*,**phone**. Use **phone** to authenticate using phone callback.

For more information on login options with examples, see https://guide.duo.com/anyconnect.

Before you begin:

Before configuring two-factor authentication with Duo Authentication Proxy on Firepower Threat Defense, ensure that you complete the following configurations:

- Configure a working primary authentication (RADIUS or AD) for your remote access VPN users before you begin to deploy Duo.
- Install Duo proxy service on a Windows or Linux machine within your network to integrate Duo with Firepower Threat Defense remote access VPN. This Duo proxy server also acts as a RADIUS server.

  Download and install the most recent Duo authentication proxy from the following location:

  - **Windows**: https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**: https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - Verify the checksum at https://duo.com/docs/checksums#duo-authentication-proxy.

- Configure Duo authentication file `authproxy.cfg`. Follow instructions on the https://duo.com/docs/cisco-firepower#configure-the-proxy page to configure the authentication configuration settings.

  The `authproxy.cfg` configuration file must contain the details for RADIUS or ISE server, Firepower Threat Defense device, Duo proxy server details, Integration Key, Secret key, and API host details.
- Ensure that you have the right API host information in the `authproxy.cfg` file.
- Configure other required settings such as secondary authentication factor in the newly installed Duo proxy server at **Duo Security Server** > **Duo Admin Panel** > **Applications** > **CISCO RADIUS VPN**.

Table 6: Procedure

	Do This	More Info
Step 1	Log on to your Firepower Management Center web interface.	
Step 2	Create a RADIUS server group.	RADIUS Server Group Options
Step 3	Create a RADIUS Server object within the new RADIUS server group with Duo proxy server as the host with a timeout of 60 seconds or more.	RADIUS Server Options **Note** For two-factor authentication, make sure that the timeout is updated to 60 seconds or more in the AnyConnect client profile XML file as well.
Step 4	Configure a new remote access VPN policy using the wizard or edit an existing remote access VPN policy.	Create a New Remote Access VPN Policy, on page 12

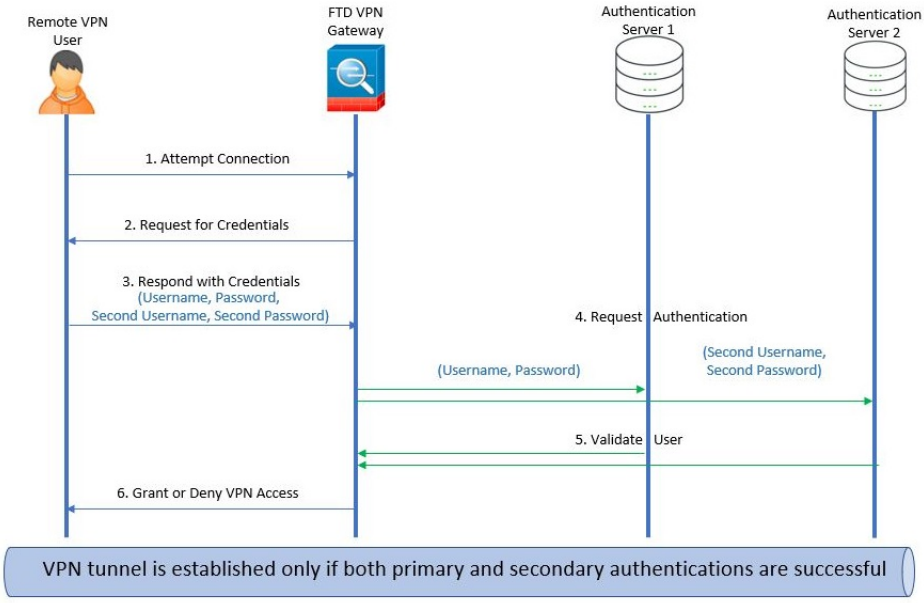
	Do This	More Info
Step 5	Select RADIUS as the authentication server and then select the RADIUS server group created with the Duo proxy server as the authentication server.	Configure AAA Settings for Remote Access VPN, on page 20
Step 7	Deploy the configuration changes.	Deploy Configuration Changes

Secondary Authentication

Secondary authentication or double authentication in Firepower Threat Defense adds an additional layer of security to remote access VPN connections by using two different authentication servers. With secondary authentication enabled, an AnyConnect VPN user must provide two sets of credentials to login to the VPN gateway.

Firepower Threat Defense remote access VPN supports secondary authentication in AAA Only and Client Certificate & AAA authentication methods.

Figure 2: Remote Access VPN Secondary or Double Authentication



Related Topics

Configure Remote Access VPN Secondary Authentication, on page 57

Configure Remote Access VPN Secondary Authentication

When remote access VPN authentication is configured to use both client certificate and authentication sever, VPN client authentication is done using both the client certificate validation and AAA server.

Before you begin

- Configure two authentication (AAA) servers— the primary and secondary authentication servers, and required identity certificates. The authentication servers can be RADIUS server, and AD or LDAP realms.
- Ensure that the AAA servers are reachable from the Firepower Threat Defense device for the remote access VPN configuration to work. Configure routing (at **Devices > Device Management > Edit Device > Routing**) to ensure connectivity to the AAA servers.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**; or click **Add** to create a new remote access VPN policy.

Step 3 For a new remote access VPN policy, configure the authentication while selecting connection profile settings. For an existing configuration, select the connection profile that includes the client profile, and click **Edit**.

Step 4 Click **AAA** > **Authentication Method**, **AAA** or **Client Certificate & AAA**.

- When you select the **Authentication Method** as:

  Client Certificate & AAA—Authentication is done using both client certificate and AAA server.

  - **AAA**—If you select the **Authentication Server** as **RADIUS**, by default, the Authorization Server has the same value. Select the **Accounting Server** from the drop-down list. Whenever you select **AD** and **LDAP** from the Authentication Server drop-down list, you must manually select the **Authorization Server** and **Accounting Server** respectively.
  - Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

- **Use secondary authentication** — Secondary authentication is configured in addition to primary authentication to provide additional security for VPN sessions. Secondary authentication is applicable only to **AAA only** and **Client Certificate & AAA** authentication methods.

  Secondary authentication is an optional feature that requires a VPN user to enter two sets of username and password on the AnyConnect login screen. You can also configure to pre-fill the secondary username from the authentication server or client certificate. Remote access VPN authentication is granted only if both primary and secondary authentications are successful. VPN authentication is denied if any one of the authentication servers is not reachable or one authentication fails.

  You must configure a secondary authentication server group (AAA server) for the second username and password before configuring secondary authentication. For example, you can set the primary authentication server to an LDAP or Active Directory realm and the secondary authentication to a RADIUS server.

  Note By default, secondary authentication is not required.

  Authentication Server— Secondary authentication server to provide secondary username and password for VPN users.

  Select the following under **Username for secondary authentication**:

  - **Prompt**: Prompts the users to enter the username and password while logging on to VPN gateway.
  - **Use primary authentication username**: The username is taken from the primary authentication server for both primary and secondary authentication; you must enter two passwords.
  - **Map username from client certificate**: Prefills the secondary username from the client certificate.

- If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN (Distinguished Name) as username** option, the system automatically retrieves the user identity.

  See **Authentication Method** descriptions for more information about primary and secondary field mapping.

- **Prefill username from certificate on user login window**: Prefills the secondary username from the client certificate when the user connects via AnyConnect VPN client.
  - **Hide username in login window**: The secondary username is pre-filled from the client certificate, but hidden to the user so that the user does not modify the pre-filled username.

- **Use secondary username for VPN session**: The secondary username is used for reporting user activity during a VPN session.

For more information, see Configure AAA Settings for Remote Access VPN, on page 20.

Related Topics

Configure Connection Profile Settings, on page 17

Remote Access VPN Examples

How to Limit AnyConnect Bandwidth Per User

This section provides instructions to limit the maximum bandwidth consumed by VPN users when the users connect using the Cisco AnyConnect VPN client to Firepower Threat Defense remote access VPN gateway. You can limit the maximum bandwidth by using a Quality of service (QoS) policy in Firepower Threat Defense, to ensure that a single user or group or users do not take over the entire resource. This configuration lets you give priority to critical traffic, prevent bandwidth hogging, and manage network. If a When traffic exceeds the maximum rate, the Firepower Threat Defense drops the excess traffic.

	Do This	More Info
Step 1	Create and set up a realm.	Create and Set up an Active Directory Realm, on page 60.
Step 2	Create a QoS policy and QoS rule for the user or group available in the newly created realm.	Create a QoS Policy and Rule, on page 60
Step 3	Configure a remote access VPN policy and select the newly-created realm for user authentication.	Create or Update a Remote Access VPN Policy, on page 61
Step 4	Deploy the remote access VPN policy.	Deploy Configuration Changes

Create and Set up an Active Directory Realm

This section provides instructions to create a realm and specify the VPN users and user groups whose activity you want to monitor.

Step 1 On your Firepower Management Center web interface, choose **System** > **Integration** > **Realms**.

Step 2 Click **New realm**, specify the realm details, and click **OK**.

Step 3 Enter the required details on the following tabs and then click **Save**:

- **Directory**—You can specify more than one directory for a realm, in which case each domain controller is queried in the order listed on the realm's **Directory** page to match user and group credentials for user control.

  See Configure a Realm Directory.

- **Realm Configuration**—You can update the realm settings entered while creating the realm.
- **User Download**—You can include or exclude users and groups from being downloaded to Firepower Management Center.

Step 4 Slide **State** to the right to enable a realm to be able to use it for user control. See Manage a Realm.

Step 5 Click download to download users and user groups to Firepower Management Center. See Download Users and Groups.

Step 6 Click **Save**.

Related Topics

Create a Realm

Create a QoS Policy and Rule

QoS policies deployed to managed devices govern rate limiting. You can create a QoS policy by selecting a realm to limit the VPN bandwidth a user or user group can consume. Each QoS policy can target multiple devices; each device can have one deployed QoS policy at a time.

Step 1 On your Firepower Management Center web interface, choose **Devices** > **QoS** > **New Policy**.

Step 2 Enter a **Name** and, optionally, a **Description**.

Step 3 Choose the **Available Devices** where you want to deploy the QoS policy, then click **Add to Policy**, or drag and drop to the **Selected Devices**.

Note Select the same device where you want to deploy the remote access VPN policy. You must assign devices before you deploy the policy.

Step 4 On QoS policy **Rules**, click **Add Rule**.

Step 5 Enter a **Name**.

Step 6 Configure rule components:

- **Enabled**—Specify whether the rule is Enabled.
- **Apply QoS On**—Choose the interfaces you want to rate limit, either Interfaces in Destination Interface Objects or Interfaces in Source Interface Objects. Your choice must correspond with a populated interface constraint (not any).

- **Traffic Limit Per Interface**—Enter a Download Limit and an Upload Limit in Mbits/sec. The default value of Unlimited prevents matching traffic from being rate limited in that direction.
- **Users**—Click the **Users** tab, and select the newly-created realm and users to limit the VPN traffic. Click other tabs corresponding to the conditions you want to add. You must configure a source or destination interface condition, corresponding to your choice for Apply QoS On.
- **Comments**—Click the Comments tab, add a comment, and click **OK**.

Step 7 Save the rule.

In the policy editor, set the rule position. Click and drag or use the right-click menu to cut and paste. Rules are numbered starting at 1. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles that traffic. Proper rule order reduces the resources required to process network traffic and prevents rule preemption.

Step 8 Click **Save** to save the policy.

Related Topics

Creating a QoS Policy
Rate Limiting with QoS Policies

Create or Update a Remote Access VPN Policy

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Create new remote access VPN policy using the wizard and select the newly created realm as the **Authentication Server**. For the existing remote access VPN policy, edit the policy and performing the following:

a) Select the connection profile that you want to assign for your VPN users and click **Edit**.
b) Choose **AAA** > **Authentication Method** > **AAA or Certificate & AAA**.

Note User identity is not supported with SAML single sign-on (SS) authentication. Choose the appropriate Authentication Method when you want to use user identity (Realm) for authentication.

c) Select the required realm as the **Authentication Server**.
d) Update other connection profile options as required and click **Save**.

Step 3 Complete the required configurations for remote access VPN policy and click **Save**.

Related Topics

Configuring a New Remote Access VPN Connection, on page 10
Configure Connection Profile Settings, on page 17

How to Use VPN Identity for User-id Based Access Control Rules

	Do This	More Info
Step 1	Create and set up a realm.	Create and Set up an Active Directory Realm, on page 60.

	Do This	More Info
Step 2	Create an identity policy and add an identity rule.	Create an Identity Policy and an Identity Rule, on page 62.
Step 3	Associate the identity policy with an access control policy.	Associate an Identity Policy with an Access Control Policy, on page 63
Step 4	Configure a remote access VPN policy and select the newly-created realm for user authentication.	Create or Update a Remote Access VPN Policy, on page 61
Step 5	Deploy the remote access VPN policy.	Deploy Configuration Changes

Create and Set up an Active Directory Realm

This section provides instructions to create a realm and specify the VPN users and user groups whose activity you want to monitor.

Step 1 On your Firepower Management Center web interface, choose **System** > **Integration** > **Realms**.

Step 2 Click **New realm**, specify the realm details, and click **OK**.

Step 3 Enter the required details on the following tabs and then click **Save**:

- **Directory**—You can specify more than one directory for a realm, in which case each domain controller is queried in the order listed on the realm's **Directory** page to match user and group credentials for user control.

  See Configure a Realm Directory.

- **Realm Configuration**—You can update the realm settings entered while creating the realm.
- **User Download**—You can include or exclude users and groups from being downloaded to Firepower Management Center.

Step 4 Slide **State** to the right to enable a realm to be able to use it for user control. See Manage a Realm.

Step 5 Click download to download users and user groups to Firepower Management Center. See Download Users and Groups.

Step 6 Click **Save**.

Related Topics

Create a Realm

Create an Identity Policy and an Identity Rule

Identity policies contain identity rules to perform user authentication based on the realm and authentication method associated with the traffic. Identity rules associate sets of traffic with a realm and an authentication method: passive authentication, active authentication, or no authentication. You must fully configure the realms and authentication methods you plan to use before you can invoke them in your identity rules.

Step 1 On your Firepower Management Center web interface, choose **Policies** > **Access Control** > **Identity** and lick **New Policy**.

Step 2 Enter a **Name** and **Description**, and then click **Save**.

Step 3 To add a rule to the policy, click **Add Rule**, and enter a **Name**.

Step 4 Specify whether the rule is **Enabled**.

Step 5 To add the rule to an existing category, indicate where you want to **Insert** the rule. To add a new category, click **Add Category**.

Step 6 Choose a rule **Action** from the list and select the interface configured in remote access VPN as the source interface.

Step 7 Click **Realms & Settings**, choose the new realm created for the identity rule from the **Realms** list. Make sure that you select the same realm selected for user authentication in remote access VPN policy.

Step 8 Configure your preferred settings for the users in the selected realm and select other required rule options.

Step 9 Click **Add** to save the rule and then save the identity policy.

Related Topics

Create and Manage Identity Policies

Associate an Identity Policy with an Access Control Policy

You must associate an identity policy with an access control policy that is deployed on the Firepower Threat Defense device where the remote access VPN policy will be deployed.

Step 1 On your Firepower Management Center web interface, choose **Policies** > **Access Control** > **Access Control**.

Step 2 Select the required access control policy and click **Edit**.

Step 3 In the access control policy editor, click **Advanced**.

Step 4 Click **Edit** ( ) in the **Identity Policy Settings** area.

If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 5 Choose an identity policy from the drop-down list.

You can click edit in edit the identity policy.

Step 6 Click **OK**.

Step 7 Click **Save** to save the access control policy.

Related Topics

Create and Manage Identity Policies

Create or Update a Remote Access VPN Policy

Step 1 On your Firepower Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Create new remote access VPN policy using the wizard and select the newly created realm as the **Authentication Server**. For the existing remote access VPN policy, edit the policy and performing the following:

a) Select the connection profile that you want to assign for your VPN users and click **Edit**.

b) Choose **AAA** > **Authentication Method** > **AAA or Certificate & AAA**.

Note User identity is not supported with SAML single sign-on (SS) authentication. Choose the appropriate Authentication Method when you want to use user identity (Realm) for authentication.

c) Select the required realm as the **Authentication Server**.

d) Update other connection profile options as required and click **Save**.

Step 3 Complete the required configurations for remote access VPN policy and click **Save**.

Related Topics

Configuring a New Remote Access VPN Connection, on page 10
Configure Connection Profile Settings, on page 17