

Connection Profiles, Group Policies, and Users

This chapter describes how to configure VPN connection profiles (formerly called “tunnel groups”), group policies, and users. This chapter includes the following sections.

- Overview of Connection Profiles, Group Policies, and Users, on page 1
- Connection Profiles, on page 2
- Configure Connection Profiles, on page 6
- Group Policies, on page 32
- Use of a Zone Labs Integrity Server, on page 71
- Configure User Attributes, on page 78
- Best Practices for Configuring and Adjusting VPN Filter ACL, on page 86

Overview of Connection Profiles, Group Policies, and Users

Groups and users are core concepts in managing the security of virtual private networks (VPNs) and in configuring the ASA. They specify attributes that determine user access to and use of the VPN. A *group* is a collection of users treated as a single entity. *Users* get their attributes from *group policies*. *A connection profile* identifies the group policy for a specific connection. If you do not assign a particular group policy to a user, the default group policy for the connection applies.

In summary, you first configure connection profiles to set the values for the connection. Then you configure group policies. These set values for users in the aggregate. Then you configure users, which can inherit values from groups and configure certain values on an individual user basis. This chapter describes how and why to configure these entities.

Note You configure connection profiles using **tunnel-group** commands. In this chapter, the terms “connection profile” and “tunnel group” are often used interchangeably.

Connection profiles and group policies simplify system management. To streamline the configuration task, the ASA provides a default LAN-to-LAN connection profile (DefaultL2Lgroup), a default remote access connection profile for IKEv2 VPN (DefaultRAgroup), a default connection profile for Clientless SSL and AnyConnect Client SSL connections (DefaultWEBVPNgroup), and a default group policy (DfltGrpPolicy). The default connection profiles and group policy provide settings are likely to be common for many users. As you add users, you can specify that they “inherit” parameters from a group policy. Thus you can quickly configure VPN access for large numbers of users.

If you decide to grant identical rights to all VPN users, then you do not need to configure specific connection profiles or group policies, but VPNs seldom work that way. 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.



Note The ASA also includes the concept of object groups, which are a superset of network lists. Object groups let you define VPN access to ports as well as networks. Object groups relate to ACLs rather than to group policies and connection profiles. For more information about using object groups, see Chapter 20, "Objects" in the general operations configuration guide.

The security appliance can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. Dynamic Access Policy (DAP) record
2. Username
3. Group policy
4. Group policy for the connection profile
5. Default group policy

Therefore, DAP values for an attribute have a higher priority than those configured for a user, group policy, or connection profile.

When you enable or disable an attribute for a DAP record, the ASA applies that value and enforces it. For example, when you disable HTTP proxy in dap webvpn configuration mode, the ASA looks no further for a value. When you instead use the no value for the http-proxy command, the attribute is not present in the DAP record, so the security appliance moves down to the AAA attribute in the username, and if necessary, to the group policy and finds a value to apply. The ASA clientless SSL VPN configuration supports only one **http-proxy** and one **https-proxy** command each. We recommend that you use ASDM to configure DAP.

Connection Profiles

A connection profile consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. Connection profiles include a small number of attributes that pertain to creating the tunnel itself. Connection profiles include a pointer to a group policy that defines user-oriented attributes.

The ASA provides the following default connection profiles: DefaultL2Lgroup for LAN-to-LAN connections, DefaultRAgroup for IPSEC remote access connections, and DefaultWEBVPNGroup for SSL VPN (browser-based and AnyConnect Client based) connections. You can modify these default connection profiles, but you cannot delete them. You can also create one or more connection profiles specific to your environment. Connection profiles are local to the ASA and are not configurable on external servers.

Note Some profiles (such as IKEv1 in phase 1) may be unable to determine whether an endpoint is remote access or LAN-to-LAN. If it cannot determine the tunnel group, it defaults to

```
tunnel-group-map default-group <tunnel-group-name>
```

(default is *DefaultRAGroup*).

General Connection Profile Connection Parameters

General parameters are common to all VPN connections. The general parameters include the following:

- Connection profile name—You specify a connection-profile name when you add or edit a connection profile. The following considerations apply:
  - For clients that use preshared keys to authenticate, the connection profile name is the same as the group name that a client passes to the ASA.
  - Clients that use certificates to authenticate pass this name as part of the certificate, and the ASA extracts the name from the certificate.
- Connection type—Connection types include IKEv1 remote-access, IPsec LAN-to-LAN, and AnyConnect (SSL/IKEv2). A connection profile can have only one connection type.
- Authentication, Authorization, and Accounting servers—These parameters identify the server groups or lists that the ASA uses for the following purposes:
  - Authenticating users
  - Obtaining information about services users are authorized to access
  - Storing accounting records

A server group can consist of one or more servers.

- Default group policy for the connection—A group policy is a set of user-oriented attributes. The default group policy is the group policy whose attributes the ASA uses as defaults when authenticating or authorizing a tunnel user.
- Client address assignment method—This method includes values for one or more DHCP servers or address pools that the ASA assigns to clients.
- Password management—This parameter lets you warn a user that the current password is due to expire in a specified number of days (the default is 14 days), then offer the user the opportunity to change the password.
- Strip group and strip realm—These parameters direct the way the ASA processes the usernames it receives. They apply only to usernames received in the form user@realm.

  A realm is an administrative domain appended to a username with the @ delimiter (user@abc). If you strip the realm, the ASA uses the username and the group (if present) for authentication. If you strip the group, the ASA uses the username and the realm (if present) for authentication.

  Enter the strip-realm command to remove the realm qualifier, and enter the strip-group command to remove the group qualilfier from the username during authentication. If you remove both qualifiers,

authentication is based on the *username* alone. Otherwise, authentication is based on the full *username@realm* or *username*<delimiter> *group* string. You must specify strip-realm if your server is unable to parse delimiters.

In addition, for L2TP/IPsec clients only, when you specify the strip-group command the ASA selects the connection profile (tunnel group) for user connections by obtaining the group name from the username presented by the VPN client.

- Authorization required—This parameter lets you require authorization before a user can connect, or turn off that requirement.
- Authorization DN attributes—This parameter specifies which Distinguished Name attributes to use when performing authorization.

IPsec Tunnel-Group Connection Parameters

IPsec parameters include the following:

- A client authentication method: preshared keys, certificates, or both.
  - For IKE connections based on preshared keys, this is the alphanumeric key itself (up to 128 characters long), associated with the connection policy.
  - Peer-ID validation requirement—This parameter specifies whether to require validating the identity of the peer using the peer's certificate.
  - If you specify certificates or both for the authentication method, the end user must provide a valid certificate in order to authenticate.
- An extended hybrid authentication method: XAUTH and hybrid XAUTH.

  You use **isakmp ikev1-user-authentication** command to implement hybrid XAUTH authentication when you need to use digital certificates for ASA authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID.
- ISAKMP (IKE) keepalive settings. This feature lets the ASA monitor the continued presence of a remote peer and report its own presence to that peer. If the peer becomes unresponsive, the ASA removes the connection. Enabling IKE keepalives prevents hung connections when the IKE peer loses connectivity.

  There are various forms of IKE keepalives. For this feature to work, both the ASA and its remote peer must support a common form. This feature works with the following peers:
  - Cisco AnyConnect VPN Client
  - Cisco IOS software
  - Cisco Secure PIX Firewall

    Non-Cisco VPN clients do not support IKE keepalives.

    If you are configuring a group of mixed peers, and some of those peers support IKE keepalives and others do not, enable IKE keepalives for the entire group. The feature does not affect the peers that do not support it.

If you disable IKE keepalives, connections with unresponsive peers remain active until they time out, so we recommend that you keep your idle timeout short. To change your idle timeout, see Configure Group Policies, on page 35.

Note To reduce connectivity costs, disable IKE keepalives if this group includes any clients connecting via ISDN lines. ISDN connections normally disconnect if idle, but the IKE keepalive mechanism prevents connections from idling and therefore from disconnecting.

If you do disable IKE keepalives, the client disconnects only when either its IKE or IPsec keys expire. Failed traffic does not disconnect the tunnel with the Peer Timeout Profile values as it does when IKE keepalives are enabled.

If you have a LAN-to-LAN configuration using IKE main mode, make sure that the two peers have the same IKE keepalive configuration. Both peers must have IKE keepalives enabled or both peers must have it disabled.

- If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the issuing certificates (including the root certificate and any subordinate CA certificates).
- You can notify users who are using outdated versions of Windows client software that they need to update their client, and you can provide a mechanism for them to get the updated client version. You can configure and change the client-update, either for all connection profiles or for particular connection profiles.
- If you configure authentication using digital certificates, you can specify the name of the trustpoint that identifies the certificate to send to the IKE peer.

Connection Profile Connection Parameters for SSL VPN Sessions

The table below provides a list of connection profile attributes that are specific to SSL VPN (AnyConnect Client and clientless) connections. In addition to these attributes, you configure general connection profile attributes common to all VPN connections.

Note In earlier releases, “connection profiles” were known as “tunnel groups.” You configure a connection profile with tunnel-group commands. This chapter often uses these terms interchangeably.

Table 1: Connection Profile Attributes for SSL VPN

	Function
authentication	Sets the authentication method, AAA or certificate.
customization	Identifies the name of a previously defined customization to apply. Customizations determine the appearance of the windows that the user sees upon login. You configure the customization parameters as part of configuring clientless SSL VPN.

	Function
nbns-server	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
group-alias	Specifies one or more alternate names by which the server can refer to a connection profile. At login, the user selects the group name from a drop-down menu.
group-url	Identifies one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login. A Load Balancing deployment that uses Group URLs for AnyConnect Client connectivity, requires each ASA node in the cluster to configure a Group URL for the virtual cluster address, as well as a Group URL for the node's Load Balancing public address.
dns-group	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a connection profile.
hic-fail-group-policy	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to "Use Failure Group-Policy" or "Use Success Group-Policy, if criteria match."
override-svc-download	Overrides downloading the group-policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
radius-reject-message	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.

Configure Connection Profiles

This section describes the contents and configuration of connection profiles in both single-context mode or multiple-context mode.



Note Multiple-context mode applies only to IKEv2 and IKEv1 site to site and does not apply to AnyConnect Client, Clientless SSL VPN, legacy Cisco VPN client, the Apple native VPN client, the Microsoft native VPN client, or cTCP for IKEv1 IPsec.

You can modify the default connection profiles, and you can configure a new connection profile as any of the three tunnel-group types. If you do not explicitly configure an attribute in a connection profile, that attribute gets its value from the default connection profile. The default connection-profile type is remote access. The subsequent parameters depend upon your choice of tunnel type. To see the current configured and default configuration of all your connection profiles, including the default connection profile, enter the **show running-config all tunnel-group** command.

Maximum Connection Profiles

The maximum number of connection profiles (tunnel groups) that an ASA can support is a function of the maximum number of concurrent VPN sessions for the platform + 5. Attempting to add an additional tunnel group beyond the limit results in the following message: “ERROR: The limit of 30 configured tunnel groups has been reached.”

Default IPsec Remote Access Connection Profile Configuration

The contents of the default remote-access connection profile are as follows:

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
```

```
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

IPsec Tunnel-Group General Attributes

The general attributes are common across more than one tunnel-group type. IPsec remote access and clientless SSL VPN tunnels share most of the same general attributes. IPsec LAN-to-LAN tunnels use a subset. Refer to the *Cisco Secure FIrewall ASA Series Command Reference* for complete descriptions of all commands. This section describes, in order, how to configure remote-access and LAN-to-LAN connection profiles.

Configure Remote-Access Connection Profiles

Use a remote-access connection profile when setting up a connection between the following remote clients and a central-site ASA:

- Secure Client (connecting with SSL or IPsec/IKEv2)
- Clientless SSL VPN (browser-based connecting with SSL)
- Cisco ASA 5500 Easy VPN hardware client (connecting with IPsec/IKEv1)

We also provide a default group policy named DfltGrpPolicy.

To configure a remote-access connection profile, first configure the tunnel-group general attributes, then the remote-access attributes. See the following sections:

- Specify a Name and Type for the Remote Access Connection Profile, on page 9.
- Configure Remote-Access Connection Profile General Attributes, on page 9.
- Configure Double Authentication, on page 13
- Configure Remote-Access Connection Profile IPsec IKEv1 Attributes, on page 15.
- Configure IPsec Remote-Access Connection Profile PPP Attributes, on page 17

Specify a Name and Type for the Remote Access Connection Profile

Procedure

Create the connection profile, specifying its name and type, by entering the **tunnel-group** command.

For a remote-access tunnel, the type is **remote-access**.

tunnel-group *tunnel_group_name* **type remote-access**

Example:

For example, to create a remote-access connection profile named TunnelGroup1, enter the following command:

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

Configure Remote-Access Connection Profile General Attributes

To configure or change the connection profile general attributes, specify the parameters in the following steps:

Procedure

Step 1 To configure the general attributes, enter the **tunnel-group general-attributes** task in either single or multiple context mode, which enters tunnel-group general-attributes configuration mode. The prompt changes to indicate the change in mode.

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

Step 2 Specify the name of the authentication-server group, if any, to use. If you want to use the LOCAL database for authentication if the specified server group fails, append the keyword **LOCAL**:

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

The name of the authentication server group can be up to 16 characters long.

You can optionally configure interface-specific authentication by including the name of an interface after the group name. The interface name, which specifies where the tunnel terminates, must be enclosed in parentheses. The following command configures interface-specific authentication for the interface named test using the server named servergroup1 for authentication:

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

Step 3 Specify the name of the authorization-server group, if any, to use. When you configure this value, users must exist in the authorization database to connect:

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

The name of the authorization server group can be up to 16 characters long. For example, the following command specifies the use of the authorization-server group FinGroup:

```
hostname(config-tunnel-general)# authorization-server-groupFinGroup
hostname(config-tunnel-general)#
```

Step 4 Specify the name of the accounting-server group, if any, to use:

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

The name of the accounting server group can be up to 16 characters long. For example, the following command specifies the use of the accounting-server group named comptroller:

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

Step 5 Specify the name of the default group policy:

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

The name of the group policy can be up to 64 characters long. The following example sets DfltGrpPolicy as the name of the default group policy:

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

Step 6 Specify the names or IP addresses of the DHCP server (up to 10 servers), and the names of the DHCP address pools (up to 6 pools). The defaults are no DHCP server and no address pool. The dhcp-server command will allow you to configure the ASA to send additional options to the specified DHCP servers when it is trying to get IP addresses for VPN clients. See the dhcp-server command in the Cisco Secure Firewall ASA Series Command Reference guide for more information.

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

Note
If you specify an interface name, you must enclosed it within parentheses.

You configure address pools with the **ip local pool** command in global configuration mode.

Step 7 Specify the name of the NAC authentication server group, if you are using Network Admission Control, to identify the group of authentication servers to be used for Network Admission Control posture validation. Configure at least one Access Control Server to support NAC. Use the **aaa-server** command to name the ACS group. Then use the **nac-authentication-server-group** command, using the same name for the server group.

The following example identifies acs-group1 as the authentication server group to be used for NAC posture validation:

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

The following example inherits the authentication server group from the default remote access group:

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

Note
NAC requires a Cisco Trust Agent on the remote host.

Step 8 Specify whether to strip the group or the realm from the username before passing it on to the AAA server. The default is not to strip either the group name or the realm:

```
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
hostname(config-tunnel-general)#
```

A realm is an administrative domain. If you strip the realm, the ASA uses the username and the group (if present) authentication. If you strip the group, the ASA uses the username and the realm (if present) for authentication. Enter the **strip-realm** command to remove the realm qualifier, and use the strip-group command to remove the group qualilfier from the username during authentication. If you remove both qualifiers, authentication is based on the *username* alone. Otherwise, authentication is based on the full *username@realm* or *username*<delimiter> *group* string. You must specify **strip-realm** if your server is unable to parse delimiters.

Step 9 Optionally, if your server is a RADIUS, RADIUS with NT, or LDAP server, you can enable password management.

Note
If you are using an LDAP directory server for authentication, password management is supported with the Sun Microsystems JAVA System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory.

Sun—The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.

Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.

This feature, which is disabled by default, warns a user when the current password is about to expire. The default is to begin warning the user 14 days before expiration:

```
hostname(config-tunnel-general)# password-management
```

```
hostname(config-tunnel-general)#
```

If the server is an LDAP server, you can specify the number of days (0 through 180) before expiration to begin warning the user about the pending expiration:

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

Note
The **password-management** command, entered in tunnel-group general-attributes configuration mode replaces the deprecated **radius-with-expiry** command that was formerly entered in tunnel-group ipsec-attributes mode.

When you configure the **password-management** command, the ASA notifies the remote user at login that the user's current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.

Note that this does not change the number of days before the password expires, but rather, the number of days ahead of expiration that the ASA starts warning the user that the password is about to expire.

If you do specify the **password-expire-in-days** keyword, you must also specify the number of days.

Specifying this command with the number of days set to 0 disables this command. The ASA does not notify the user of the pending expiration, but the user can change the password after it expires.

See Configure Microsoft Active Directory Settings for Password Management, on page 28 for more information.

The ASA Version 7.1 and later generally supports password management for the AnyConnect VPN Client, the Cisco IPsec VPN Client, the SSL VPN full-tunneling client, and Clientless connections when authenticating with LDAP or with any RADIUS connection that supports MS-CHAPv2. Password management is *not* supported for any of these connection types for Kerberos/AD (Windows password) or NT 4.0 Domain.

Some RADIUS servers that support MS-CHAP do not currently support MS-CHAPv2. The **password-management** command requires MS-CHAPv2, so please check with your vendor.

Note
The RADIUS server (for example, Cisco ACS) could proxy the authentication request to another authentication server. However, from the ASA perspective, it is talking only to a RADIUS server.

For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the ASA implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers. Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

Step 10

Step 11 Specify the attribute or attributes to use in deriving a name for an authorization query from a certificate. This attribute specifies what part of the subject DN field to use as the username for authorization:

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

For example, the following command specifies the use of the CN attribute as the username for authorization:

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

The authorization-dn-attributes are **C** (Country), **CN** (Common Name), **DNQ** (DN qualifier), **EA** (E-mail Address), **GENQ** (Generational qualifier), **GN** (Given Name), **I** (Initials), **L** (Locality), **N** (Name), **O** (Organization), **OU** (Organizational Unit), **SER** (Serial Number), **SN** (Surname), **SP** (State/Province), **T** (Title), **UID** (User ID), and **UPN** (User Principal Name).

Step 12 Specify whether to require a successful authorization before allowing a user to connect. The default is not to require authorization.

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

Configure Double Authentication

Double authentication is an optional feature that requires a user to enter an additional authentication credential, such as a second username and password, on the login screen. Specify the following commands to configure double authentication.

Procedure

Step 1 Specify the secondary authentication server group. This command specifies the AAA server group to use as the secondary AAA server.

Note
This command applies only to AnyConnect VPN connections.

The secondary server group cannot specify an SDI server group. By default, no secondary authentication is required.

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

If you use the none keyword, no secondary authentication is required. The *groupname* value specifies the AAA server group name. Local specifies the use of the internal server database, and when used with the groupname value, LOCAL specifies fallback.

For example, to set the primary authentication server group to sdi_group and the secondary authentication server group to ldap_server, enter the following commands:

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

Note
If you use the **use-primary-name** keyword, then the login dialog requests only one username. In addition, if the usernames are extracted from a digital certificate, only the primary username is used for authentication.

Step 2 If obtaining the secondary username from a certificate, enter **secondary-username-from-certificate**:

```
hostname(config-tunnel-general)# secondary-username-from-certificate C | CN | ... | use-script
```

The values for the DN fields to extract from the certificate for use as a secondary username are the same as for the primary **username-from-certificate** command. Alternatively, you can specify the use-script keyword, which directs the ASA to use a script file generated by ASDM.

For example, to specify the Common Name as the primary username field and Organizational Unit as the secondary username field, enter the following commands:

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# username-from-certificate cn
hostname(config-tunnel-general)# secondary-username-from-certificate ou
```

Step 3 Use the **secondary-pre-fill-username** command in tunnel-group webvpn-attributes mode to enable extracting a secondary username from a client certificate for use in authentication. Use the keywords to specify whether this command applies to a clientless connection or an SSL VPN client (AnyConnect) connection and whether you want to hide the extracted username from the end user. This feature is disabled by default. Clientless and SSL-client options can both exist at the same time, but you must configure them in separate commands.

```
hostname(config-tunnel-general)# secondary-pre-fill-username-from-certificate
{clientless | client} [hide]
```

For example, to specify the use of pre-fill-username for both the primary and secondary authentication for a connection, enter the following commands:

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# pre-fill-username client
hostname(config-tunnel-general)# secondary-pre-fill-username client
```

Step 4 Specify which authentication server to use to obtain the authorization attributes to apply to the connection. The primary authentication server is the default selection. This command is meaningful only for double authentication.

```
hostname(config-tunnel-general)# authentication-attr-from-server {primary | secondary}
```

For example, to specify the use of the secondary authentication server, enter the following commands:

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authentication-attr-from-server secondary
```

Step 5 Specify which authentication username, primary or secondary, to associate with the session. The default value is primary. With double authentication enabled, it is possible that two distinct usernames are authenticated for the session. The administrator must designate one of the authenticated usernames as the session username. The session username is the username provided for accounting, session database, syslogs, and debug output.

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

For example, to specify that the authentication username associated with the session must come from the secondary authentication server, enter the following commands:

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

Configure Remote-Access Connection Profile IPsec IKEv1 Attributes

To configure the IPsec IKEv1 attributes for a remote-access connection profile, perform the following steps. The following description assumes that you have already created the remote-access connection profile. Remote-access connection profiles have more attributes than LAN-to-LAN connection profiles.

Procedure

Step 1 To specify the IPsec attributes of an remote-access tunnel-group, enter tunnel-group ipsec-attributes mode by entering the following command in either single or multiple context mode. The prompt changes to indicate the mode change.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

This command enters tunnel-group ipsec-attributes configuration mode, in which you configure the remote-access tunnel-group IPsec attributes in either single or multiple context mode.

For example, the following command designates that the tunnel-group ipsec-attributes mode commands that follow pertain to the connection profile named TG1. Notice that the prompt changes to indicate that you are now in tunnel-group ipsec-attributes mode:

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Step 2 Specify the preshared key to support IKEv1 connections based on preshared keys. For example, the following command specifies the preshared key xyzx to support IKEv1 connections for an IPsec IKEv1 remote access connection profile:

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

Step 3 Specify whether to validate the identity of the peer using the peer's certificate:

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

The possible *option* values are **req** (required), **cert (**if supported by certificate), and **nocheck (**do not check). The default is **req**.

For example, the following command specifies that peer-id validation is required:

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

Step 4 Specify whether to enable sending of a certificate chain. The following command includes the root certificate and any subordinate CA certificates in the transmission:

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

This attribute applies to all IPsec tunnel-group types.

Step 5 Specify the name of a trustpoint that identifies the certificate to be sent to the IKE peer:

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

The following command specifies mytrustpoint as the name of the certificate to be sent to the IKE peer:

```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

Step 6 Specify the ISAKMP keepalive threshold and the number of retries allowed:

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

The **threshold** parameter specifies the number of seconds (10 through 3600) that the peer is allowed to idle before beginning keepalive monitoring. The **retry** parameter is the interval (2 through 10 seconds) between retries after a keepalive response has not been received. IKE keepalives are enabled by default. To disable ISAKMP keepalives, enter **isakmp keepalive disable**.

For example, the following command sets the IKE keepalive threshold value to 15 seconds and sets the retry interval to 10 seconds:

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

The default value for the **threshold** parameter is 300 for remote-access and 10 for LAN-to-LAN, and the default value for the retry parameter is 2.

To specify that the central site (secure gateway) should never initiate ISAKMP monitoring, enter the following command:

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

Step 7 Specify the ISAKMP hybrid authentication method, XAUTH or hybrid XAUTH.

You use **isakmp ikev1-user-authentication** command to implement hybrid XAUTH authentication when you need to use digital certificates for ASA authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID. Hybrid XAUTH breaks phase 1 of IKE down into the following two steps, together called hybrid authentication:

a) The ASA authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
b) An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.

Note
Before the authentication type can be set to hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

You can use the **isakmp ikev1-user-authentication** command with the optional interface parameter to specify a particular interface. When you omit the interface parameter, the command applies to all the interfaces and serves as a back-up when the per-interface command is not specified. When there are two **isakmp ikev1-user-authentication** commands specified for a connection profile, and one uses the **interface** parameter and one does not, the one specifying the interface takes precedence for that particular interface.

For example, the following commands enable hybrid XAUTH on the inside interface for a connection profile called example-group:

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

Configure IPsec Remote-Access Connection Profile PPP Attributes

To configure the Point-to-Point Protocol attributes for a remote-access connection profile, perform the following steps. PPP attributes apply *only* to IPsec remote-access connection profiles. The following description assumes that you have already created the IPsec remote-access connection profile.

Procedure

Step 1 Enter tunnel-group ppp-attributes configuration mode, in which you configure the remote-access tunnel-group PPP attributes, by entering the following command. The prompt changes to indicate the mode change:

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

For example, the following command designates that the tunnel-group ppp-attributes mode commands that follow pertain to the connection profile named TG1. Notice that the prompt changes to indicate that you are now in tunnel-group ppp-attributes mode:

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

Step 2 Specify whether to enable authentication using specific protocols for the PPP connection. The protocol value can be any of the following:

- pap—Enables the use of Password Authentication Protocol for the PPP connection.
- chap—Enables the use of Challenge Handshake Authentication Protocol for the PPP connection.
- ms-chap-v1 or ms-chap-v2—Enables the use of Microsoft Challenge Handshake Authentication Protocol, version 1 or version 2 for the PPP connection.
- eap—Enables the use of Extensible Authentication protocol for the PPP connection.

CHAP and MSCHAPv1 are enabled by default.

The syntax of this command is:

```
hostname(config-tunnel-ppp)# authentication protocol
hostname(config-tunnel-ppp)#
```

To disable authentication for a specific protocol, use the **no** form of the command:

```
hostname(config-tunnel-ppp)# no authentication protocol
hostname(config-tunnel-ppp)#
```

For example, the following command enables the use of the PAP protocol for a PPP connection:

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

The following command enables the use of the MS-CHAP, version 2 protocol for a PPP connection:

```
hostname(config-tunnel-ppp)# authentication ms-chap-v2
hostname(config-tunnel-ppp)#
```

The following command enables the use of the EAP-PROXY protocol for a PPP connection:

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

The following command disables the use of the MS-CHAP, version 1 protocol for a PPP connection:

```
hostname(config-tunnel-ppp)# no authentication ms-chap-v1
hostname(config-tunnel-ppp)#
```

Configure LAN-to-LAN Connection Profiles

An IPsec LAN-to-LAN VPN connection profile applies only to LAN-to-LAN IPsec client connections. While many of the parameters that you configure are the same as for IPsec remote-access connection profiles, LAN-to-LAN tunnels have fewer parameters. The following sections show you how to configure a LAN-to-LAN connection profile:

- Specify a Name and Type for a LAN-to-LAN Connection Profile, on page 19
- Configure LAN-to-LAN Connection Profile General Attributes, on page 19
- Configure LAN-to-LAN IPsec IKEv1 Attributes, on page 20

Default LAN-to-LAN Connection Profile Configuration

The contents of the default LAN-to-LAN connection profile are as follows:

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

LAN-to-LAN connection profiles have fewer parameters than remote-access connection profiles, and most of these are the same for both groups. For your convenience in configuring the connection, they are listed separately here. Any parameters that you do not explicitly configure inherit their values from the default connection profile.

Specify a Name and Type for a LAN-to-LAN Connection Profile

To specify a name and a type for a connection profile, enter the **tunnel-group** command, as follows:

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

For a LAN-to-LAN tunnel, the type is **ipsec-l2l**.; for example, to create the LAN-to-LAN connection profile named docs, enter the following command:

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

Configure LAN-to-LAN Connection Profile General Attributes

To configure the connection profile general attributes, perform the following steps:

Procedure

Step 1 Enter tunnel-group general-attributes mode by specifying the general-attributes keyword in either single or multiple context mode:

tunnel-group *tunnel-group-name* **general-attributes**

Example:

For the connection profile named docs, enter the following command:

```
hostname(config)# tunnel-group docs general-attributes
hostname(config-tunnel-general)#
```

The prompt changes to indicate that you are now in config-general mode, in which you configure the tunnel-group general attributes.

Step 2 Specify the name of the default group policy:

default-group-policy *policyname*

Example:

The following command specifies that the name of the default group policy is MyPolicy:

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

Configure LAN-to-LAN IPsec IKEv1 Attributes

To configure the IPsec IKEv1 attributes, perform the following steps:

Procedure

Step 1 To configure the tunnel-group IPsec IKEv1 attributes, enter tunnel-group ipsec-attributes configuration mode by entering the tunnel-group command with the IPsec-attributes keyword in either single or multiple context mode.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

For example, the following command enters config-ipsec mode so that you can configure the parameters for the connection profile named TG1:

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

The prompt changes to indicate that you are now in tunnel-group ipsec-attributes configuration mode.

Step 2 Specify the preshared key to support IKEv1 connections based on preshared keys.

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

For example, the following command specifies the preshared key XYZX to support IKEv1 connections for an LAN-to-LAN connection profile:

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

Step 3 Specify whether to validate the identity of the peer using the peer's certificate:

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

The available options are **req** (required), **cert (**if supported by certificate), and **nocheck (**do not check). The default is **req**. For example, the following command sets the peer-id-validate option to **nocheck**:

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

Step 4 Specify whether to enable sending of a certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission:

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

You can apply this attribute to all tunnel-group types.

Step 5 Specify the name of a trustpoint that identifies the certificate to be sent to the IKE peer:

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

For example, the following command sets the trustpoint name to mytrustpoint:

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

You can apply this attribute to all tunnel-group types.

Step 6 Specify the ISAKMP (IKE) keepalive threshold and the number of retries allowed. The **threshold** parameter specifies the number of seconds (10 through 3600) that the peer is allowed to idle before beginning keepalive monitoring. The **retry** parameter is the interval (2 through 10 seconds) between retries after a keepalive response has not been received. IKE keepalives are enabled by default. To disable IKE keepalives, enter the **no** form of the **isakmp** command:

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

For example, the following command sets the ISAKMP keepalive threshold to 15 seconds and sets the retry interval to 10 seconds:

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

The default value for the **threshold** parameter for LAN-to-LAN is 10, and the default value for the retry parameter is 2.

To specify that the central site (secure gateway) should never initiate ISAKMP monitoring, enter the following command:

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

Step 7 Specify the ISAKMP hybrid authentication method, XAUTH or hybrid XAUTH.

You use **isakmp ikev1-user-authentication** command to implement hybrid XAUTH authentication when you need to use digital certificates for ASA authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID. Hybrid XAUTH breaks phase 1 of IKE down into the following two steps, together called hybrid authentication:

a) The ASA authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
b) An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.

Note
Before the authentication type can be set to hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

For example, the following commands enable hybrid XAUTH for a connection profile called example-group:

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
hostname(config-tunnel-ipsec)#
```

About Tunnel Groups for Standards-based IKEv2 Clients

A tunnel group is a set of records that contain tunnel connection policies. You configure a tunnel group to identify AAA servers, specify connection parameters, and define a default group policy. The ASA stores tunnel groups internally.

The default tunnel group for IPsec remote access is the DefaultRAGroup. You may modify the default tunnel group, but not delete it.

IKEv2 allows asymmetric authentication methods to be configured (that is, preshared key authentication for the originator but certificate authentication or EAP authentication for the responder) using separate local and remote authentication CLIs. Therefore, with IKEv2 you have asymmetric authentication, in which one side authenticates with one credential and the other side uses another credential (either a preshared key, certificate, or EAP).

The DefaultRAGroup should be configured for EAP authentication because these client connections cannot be mapped to a specific tunnel group unless certificate authentication is used with certificate DN matching.

Standards-based IKEv2 Attribute Support

The ASA supports the following IKEv2 attributes:

- INTERNAL_IP4_ADDRESS/INTERNAL_IP6_ADDRESS—IPv4 or IPv6 address



Note Dual stack (assignment of both an IPv4 and IPv6 address) is not supported for IKEv2. If both an IPv4 and an IPv6 address are requested and both addresses may be assigned, only an IPv4 address is assigned.

- INTERNAL_IP4_NETMASK—IPv4 address network mask
- INTERNAL_IP4_DNS/INTERNAL_IP6_DNS—Primary/Secondary DNS address
- INTERNAL_IP4_NBNS—Primary/Secondary WINS address
- INTERNAL_IP4_SUBNET/INTERNAL_IP6_SUBNET—Split-tunneling lists
- APPLICATION_VERSION—Ignored. No response is sent to avoid communicating any version information about the ASA for security reasons. However, the client configuration payload request may include this attribute, and the string appears on the ASA in the **vpn-sessiondb** command output and in the syslog.

DAP Support

To allow DAP policy configuration per connection type, a new Client Type, IPsec-IKEv2-Generic-RA, can be used to apply specific policy for this connection type.

Tunnel Group Selection for Remote Access Clients

The following table provides a list of remote access clients and their available tunnel group options:

Remote Access Client	Tunnel Group List	Group URL	Certificate DN Matching	Default Group (DefaultRAGroup)	Other
AnyConnect VPN Client	Yes	Yes	Yes	Yes	N/A

Windows L2TP/IPsec (Main Mode IKEv1)	No	No	• Yes (when using local machine certificates) • No (when using PSK)	Yes	N/A
Standards-based IKEv2	No	No	• Yes (when using local machine certificates) • No (when using EAP authentication)	Yes **Note** You must use the DefaultRAGroup tunnel group.	N/A

Authentication Support for Standards-based IKEv2 Clients

The following table provides a list of standards-based IKEv2 clients and their supported authentication methods:



Note Authentication method limitations are based on lack of support on the client, not on the ASA. All EAP method authentication is proxied by the ASA between the client and EAP server. EAP method support is based on client and EAP server support for the EAP method.

Client Type/ Authentication Method	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	Certificate Only	PSK
StrongSwan on Linux	N/A	• ISE—Yes • ACS—Yes • FreeRadius—Yes • AD via FreeRadius—Yes	• ISE—Yes • ACS—Yes • FreeRadius—Yes • AD via FreeRadius—Yes	Yes	Yes
StrongSwan on Android	N/A	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	No	Yes	N/A
Windows 7/8/8.1	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	N/A	Yes	NA

Client Type/ Authentication Method	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	Certificate Only	PSK
Windows Phone	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	N/A	N/A	N/A
Samsung Knox	N/A	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	Yes	N/A
iOS 8	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	N/A	Yes	Yes
Android Native Client	N/A	• ISE—Yes • ACS —Yes • FreeRadius—Yes • AD via FreeRadius—Yes	N/A	Yes	Yes

Add Multiple Certificate Authentication

The Aggregate Authentication protocol has been extended to define the protocol exchange for multiple-certificate authentication and utilize this for both session types. After the client makes an SSL connection and enters into aggregate authentication, another SSL connection is made, and the ASA sees that the client requires certificate authentication and requests the client certificate.

The ASA configures the required authentication for an AnyConnect Client connection of a remote-access type tunnel group. A tunnel-group mapping is performed with the existing methods such as certificate rule mapping, group-url, and so on, but then the required authentication methods are negotiated with the client.

Example

tunnel-group <name> webvpn-attributes

authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml] | saml [certificate | multiple-certificate]}

The authentication options are AAA only, certificate only, multiple-certificate only, AAA and certificate, AAA and multiple-certificate, SAML, SAML and certificate, or Multiple certificates and SAML.

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa         Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml   Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa  Use username and password for authentication
saml  Use SAML for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>ASA(config-tunnel-webvpn)# authentication aaa?

ASA(config-tunnel-webvpn)# authentication saml?
tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

Configure the query-identity Option for Retrieval of EAP Identity

The Microsoft Windows 7 IKEv2 client sends an IP address as the Internet Key Exchange (IKE) identity that prevents the Cisco ASA server from using it efficiently for tunnel-group lookup. The ASA must be configured with the **query-identity** option for EAP authentication to allow the ASA to retrieve a valid EAP identity from the client.

For certificate-based authentication, the ASA server and Microsoft Windows 7 client certificates must have an Extended Key Usage (EKU) field as follows:

- For the client certificate, EKU field = client authentication certificate.
- For the server certificate, EKU field = server authentication certificate.

You can obtain the certificates from the Microsoft Certificate Server or other CA server.

For EAP authentication, the Microsoft Windows 7 IKEv2 client expects an EAP identity request before any other EAP requests. Make sure that you configure the **query-identity** keyword in the tunnel group profile on the IKEv2 ASA server to send an EAP identity request to the client.

Note DHCP intercept is supported for IKEv2 to allow Windows to do split-tunneling. This feature only works with IPv4 split-tunneling attributes.

Procedure

Step 1 To set the connection type to IPsec remote access, enter the **tunnel-group** command. The syntax is **tunnel-group** *name* **type** *type,* where name is the name you assign to the tunnel group, and type is the type of tunnel:

In the following example, the IKEv2 preshared key is configured as 44kkaol59636jnfx:

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

Note
You must configure the **ikev2 remote-authentication pre-shared-key** command or **ikev2 remote-authentication certificate** command to complete the authentication.

Step 2 To specify Extensible Authentication Protocol (EAP) as the method that supports user authentication with standards-based, third-party IKEv2 remote access clients, use the **ikev2 remote-authentication eap** [**query-identity**] command.

Note
Before you can enable EAP for remote authentication, you must configure local authentication using a certificate and configure a valid trustpoint using the **ikev2 local-authentication** {**certificate** *trustpoint*} command. Otherwise, the EAP authentication request is rejected.

You may configure multiple options that allow the client to use any of the configured options, but not all, for remote authentication.

For IKEv2 connections, the tunnel group mapping must know which authentication methods to allow for remote authentication (PSK, certificate, and EAP) and local authentication (PSK and certificate), and which trust point to use for local authentication. Currently, mapping is performed using the IKE ID, which is taken from the peer or peer certificate field value (using the certificate map). If both options fail, then the in-coming connection is mapped to the default remote access tunnel group, DefaultRAGroup. A certificate map is an applicable option only when the remote peer is authenticated via a certificate. This map allows mapping to different tunnel groups. For certificate authentication only, the tunnel group lookup is performed using rules or using the default setting. For EAP and PSK authentication, the tunnel group lookup is performed using the IKE ID on the client (it matches the tunnel group name) or using the default setting.

For EAP authentication, you must use the DefaultRAGroup tunnel group unless the client allows the IKE ID and username to be configured independently.

The following example shows an EAP request for authentication being denied:

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Step 3 Save your changes.

```
hostname(config)# write memory
```

```
hostname(config)#
```

To verify that the tunnel is up and running, use the **show vpn-sessiondb summary** or **show crypto ipsec sa** command.

Configure Microsoft Active Directory Settings for Password Management

If you are using an LDAP directory server for authentication, password management is supported with the Sun Microsystems JAVA System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory.

- Sun—The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.
- Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.

To use password management with Microsoft Active Directory, you must set certain Active Directory parameters as well as configuring password management on the ASA. This section describes the Active Directory settings associated with various password management actions. These descriptions assume that you have also enabled password management on the ASA and configured the corresponding password management attributes. The specific steps in this section refer to Active Directory terminology under Windows 2000. This section assumes that you are using an LDAP directory server for authentication.

Use Active Directory to Force the User to Change Password at Next Logon

To force a user to change the user password at the next logon, specify the **password-management** command in tunnel-group general-attributes configuration mode on the ASA and perform the following steps under Active Directory:

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

Step 2 Right-click to choose **Username** > **Properties** > **Account**.

Step 3 Check the **User must change password at next logon** check box.

The next time this user logs on, the ASA displays the following prompt: “New password required. Password change required. You must enter a new password with a minimum length *n* to continue.” You can set the minimum required password length, *n*, as part of the Active Directory configuration at Start > Programs > Administrative Tools > Domain Security Policy > Windows Settings > Security Settings > Account Policies > Password Policy. Select **Minimum password length**.

Use Active Directory to Specify Maximum Password Age

To enhance security, you can specify that passwords expire after a certain number of days. To specify a maximum password age for a user password, specify the **password-management** command in tunnel-group general-attributes configuration mode on the ASA and perform the following steps under Active Directory:



Note The **radius-with-expiry** command, formerly configured as part of tunnel-group remote-access configuration to perform the password age function, is deprecated. The **password-management** command, entered in tunnel-group general-attributes mode, replaces it.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Domain Security Policy** > **Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy**.

Step 2 Double-click Maximum password age.

Step 3 Check the **Define this policy setting** check box and specify the maximum password age, in days, that you want to allow.

Use Active Directory to Enforce Minimum Password Length

To enforce a minimum length for passwords, specify the **password-management** command in tunnel-group general-attributes configuration mode on the ASA and perform the following steps under Active Directory:

Procedure

Step 1 Chose **Start** > **Programs** > **Administrative Tools** > **Domain Security Policy**.

Step 2 Chose **Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy**.

Step 3 Double-click **Minimum Password Length**.

Step 4 Check the **Define this policy setting** check box and specify the minimum number of characters that the password must contain.

Use Active Directory to Enforce Password Complexity

To enforce complex passwords—for example, to require that a password contain upper- and lowercase letters, numbers, and special characters—enter the **password-management** command in tunnel-group general-attributes configuration mode on the ASA and perform the following steps under Active Directory:

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Domain Security Policy. Select Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy**.

Step 2 Double-click Password must meet complexity requirements to open the Security Policy Setting dialog box.

Step 3 Check the Define this policy setting check box and select **Enable**.

Enforcing password complexity takes effect only when the user changes passwords; for example, when you have configured Enforce password change at next login or Password expires in *n* days. At login, the user receives a prompt to enter a new password, and the system will accept only a complex password.

Configure the Connection Profile for RADIUS/SDI Message Support for the AnyConnect Client

This section describes procedures to ensure that the AnyConnect VPN client using RSA SecureID Software tokens can properly respond to user prompts delivered to the client through a RADIUS server proxying to an SDI server(s).

Note If you have configured the double-authentication feature, SDI authentication is supported only on the primary authentication server.

When a remote user connects to the ASA with the AnyConnect VPN client and attempts to authenticate using an RSA SecurID token, the ASA communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

During authentication, the RADIUS server presents access challenge messages to the ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA is communicating directly with an SDI server than when communicating through the RADIUS proxy. Therefore, in order to appear as a native SDI server to the AnyConnect Client, the ASA must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. The AnyConnect Client may fail to respond and authentication may fail.

Configure the Security Appliance to Support RADIUS/SDI Messages, on page 30 describes how to configure the ASA to ensure successful authentication between the client and the SDI server.

Configure the Security Appliance to Support RADIUS/SDI Messages

To configure the ASA to interpret SDI-specific RADIUS reply messages and prompt the AnyConnect Client user for the appropriate action, perform the following steps:

Procedure

Step 1 Configure a connection profile (tunnel group) to forward RADIUS reply messages in a manner that simulates direct communication with an SDI server using the **proxy-auth sdi** command from tunnel-group webvpn configuration mode. Users authenticating to the SDI server must connect over this connection profile.

Example:

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

Step 2 Configure the RADIUS reply message text on the ASA to match (in whole or in part) the message text sent by the RADIUS server with the **proxy-auth_map sdi** command from tunnel-group webvpn configuration mode.

The default message text used by the ASA is the default message text used by Cisco Secure Access Control Server (ACS). If you are using Cisco Secure ACS, and it is using the default message text, you do not need to configure the message text on the ASA. Otherwise, use the **proxy-auth_map sdi** command to ensure the message text matches.

The table below shows the message code, the default RADIUS reply message text, and the function of each message. Because the security appliance searches for strings in the order that they appear in the table, you must ensure that the string you use for the message text is not a subset of another string.

For example, “new PIN” is a subset of the default message text for both new-pin-sup and next-ccode-and-reauth. If you configure new-pin-sup as “new PIN,” when the security appliance receives “new PIN with the next card code” from the RADIUS server, it will match the text to the new-pin-sup code instead of the next-ccode-and-reauth code.

SDI Op-codes, Default Message Text, and Message Function

Message Code	Default RADIUS Reply Message Text	Function
next-code	Enter Next PASSCODE	Indicates the user must enter the NEXT tokencode without the PIN.
new-pin-sup	Please remember your new PIN	Indicates the new system PIN has been supplied and displays that PIN for the user.
new-pin-meth	Do you want to enter your own pin	Requests from the user which new PIN method to use to create a new PIN.
new-pin-req	Enter your new Alpha-Numerical PIN	Indicates a user-generated PIN and requests that the user enter the PIN.
new-pin-reenter	Reenter PIN:	Used internally by the ASA for user-supplied PIN confirmation. The client confirms the PIN without prompting the user.
new-pin-sys-ok	New PIN Accepted	Indicates the user-supplied PIN was accepted.

Message Code	Default RADIUS Reply Message Text	Function
next-ccode-and-reauth	new PIN with the next card code	Follows a PIN operation and indicates the user must wait for the next tokencode and to enter both the new PIN and next tokencode to authenticate.
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	Used internally by the ASA to indicate the user is ready for the system-generated PIN.

The following example enters aaa-server-host mode and changes the text for the RADIUS reply message new-pin-sup:

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your new PIN"
```

Group Policies

This section describes group policies and how to configure them.

A group policy is a set of user-oriented attribute/value pairs for IPsec connections that are stored either internally (locally) on the device or externally on a RADIUS server. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

Enter the **group-policy** commands in global configuration mode to assign a group policy to users or to modify a group policy for specific users.

The ASA includes a default group policy. In addition to the default group policy, which you can modify but not delete, you can create one or more group policies specific to your environment.

You can configure internal and external group policies. Internal groups are configured on the ASA's internal database. External groups are configured on an external authentication server, such as RADIUS. Group policies include the following attributes:

- Identity
- Server definitions
- Client firewall settings
- Tunneling protocols
- IPsec settings
- Hardware client settings
- Filters
- Client configuration settings

- Connection settings

Modify the Default Group Policy

The ASA supplies a default group policy. You can modify this default group policy, but you cannot delete it. A default group policy, named DfltGrpPolicy, always exists on the ASA, but this default group policy does not take effect unless you configure the ASA to use it. When you configure other group policies, any attribute that you do not explicitly specify inherits its value from the default group policy.



Note AnyConnect Client profiles, including any or all AnyConnect Client Profile Types (such as Network Access Manager, Umbrella, and so on), that are configured on (and then assigned to) the DfltGrpPolicy, are not inherited by other group policies, unless the other group policies explicitly are configured to inherit from the DfltGrpPolicy. In other words, AnyConnect Client profiles that are associated with the DfltGrpPolicy are not inherited when specific AnyConnect Client profiles are configured on a group policy.

To view the default group policy, enter the following command:

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

To configure the default group policy, enter the following command:

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```



Note The default group policy is always internal. Despite the fact that the command syntax is hostname(config)# group-policy DfltGrpPolicy {internal | external}, you cannot change its type to external.

To change any of the attributes of the default group policy, use the **group-policy attributes** command to enter attributes mode, then specify the commands to change whatever attributes that you want to modify:

```
hostname(config)# group-policy DfltGrpPolicy attributes
```



Note The attributes mode applies only to internal group policies.

The default group policy, DfltGrpPolicy, that the ASA provides is as follows:

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server value 10.10.10.1.1
```

```
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client

password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain value cisco.com
split-dns none
split-tunnel-all-dns disable
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
client-bypass-protocol disable
gateway-fqdn none
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
msie-proxy lockdown enable
vlan none
nac-settings none
address-pools none
ipv6-address-pools none
smartcard-removal-disconnect enable
scep-forwarding-url none
client-firewall none
client-access-rule none
webvpn
 url-list none
 filter none
 homepage none
 html-content-filter none

 http-proxy disable

 anyconnect ssl dtls enable
 anyconnect mtu 1406
 anyconnect firewall-rule client-interface private none
 anyconnect firewall-rule client-interface public none
 anyconnect keep-installer installed
 anyconnect ssl keepalive 20
 anyconnect ssl rekey time none
 anyconnect ssl rekey method none
 anyconnect dpd-interval client 30
```

```
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression lzs
  anyconnect modules none
  anyconnect profiles none
  anyconnect ask none
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none

  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information

  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable

  always-on-vpn profile-setting
```

You can modify the default group policy, and you can also create one or more group policies specific to your environment.

Configure Group Policies

A group policy can apply to any kind of tunnel. In each case, if you do not explicitly define a parameter, the group takes the value from the default group policy.

You can perform these configuration tasks in both single context mode or multiple-context mode:

Note Multiple-context mode applies only to IKEv2 and IKEv1 site to site and does not apply to AnyConnect, Clientless SSL VPN, the Apple native VPN client, the Microsoft native VPN client, or cTCP for IKEv1 IPsec.

Configure an External Group Policy

External group policies take their attribute values from the external server that you specify. For an external group policy, you must identify the AAA server group that the ASA can query for attributes and specify the password to use when retrieving attributes from the external AAA server group. If you are using an external authentication server, and if your external group-policy attributes exist in the same RADIUS server as the users that you plan to authenticate, you have to make sure that there is no name duplication between them.

Note External group names on the ASA refer to user names on the RADIUS server. In other words, if you configure external group X on the ASA, the RADIUS server sees the query as an authentication request for user X. So external groups are really just user accounts on the RADIUS server that have special meaning to the ASA. If your external group attributes exist in the same RADIUS server as the users that you plan to authenticate, there must be no name duplication between them.

The ASA supports user authorization on an external LDAP or RADIUS server. Before you configure the ASA to use an external server, you must configure the server with the correct ASA authorization attributes and, from a subset of these attributes, assign specific permissions to individual users. Follow the instructions in Configure an External AAA Server for VPN to configure your external server.

Procedure

To configure an external group policy, perform the following step and specify a name and type for the group policy, along with the server-group name and a password:

```
hostname(config)# group-policy group_policy_name type server-group server_group_name password
 server_password
hostname(config)#
```

Note
For an external group policy, RADIUS is the only supported AAA server type.

For example, the following command creates an external group policy named ExtGroup that gets its attributes from an external RADIUS server named ExtRAD and specifies that the password to use when retrieving the attributes is newpassword:

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

Note
You can configure several vendor-specific attributes (VSAs), as described in Configure an External AAA Server for VPN. If a RADIUS server is configured to return the Class attribute (#25), the ASA uses that attribute to authenticate the Group Name. On the RADIUS server, the attribute must be formatted as: OU=*groupname*; where *groupname* is identical to the Group Name configured on the ASA—for example, OU=Finance.

Create an Internal Group Policy

To configure an internal group policy, enter configuration mode, use the group-policy command, specify a name, and the **internal** type for the group policy:

```
hostname(config)# group-policy group_policy_name internal
hostname(config)#
```

For example, the following command creates the internal group policy named GroupPolicy1:

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

Note You cannot change the name of a group policy after you create it.

You can configure the attributes of an internal group policy by copying the values of a preexisting group policy by appending the keyword **from** and specifying the name of the existing policy:

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
```

For example, the following command creates the internal group policy named GroupPolicy2 by copying the attributes of GroupPolicy1:

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```

Configure General Internal Group Policy Attributes

Group Policy Name

The group policy name was chosen when the internal group policy was created. You cannot change the name of a group policy once it has been created. See Create an Internal Group Policy, on page 36 for more information.

Configure the Group Policy Banner Message

Specify the banner, or welcome message, if any, that you want to display. The default is no banner. The message that you specify is displayed on remote clients when they connect. To specify a banner, enter the **banner** command in group-policy configuration mode. The banner text can be up to 500 characters long.

Note Ensure that you use normal line breaks in the banner dialog and not “\n”.

The overall banner length, which is displayed during post-login on the VPN remote client, has increased from 510 to 4000 characters in ASA version 9.5.1.

Note A carriage-return and line-feed included in the banner counts as two characters.

To delete a banner, enter the **no** form of this command. Be aware that using the **no** version of the command deletes all banners for the group policy.

A group policy can inherit this value from another group policy. To prevent inheriting a value, enter the **none** keyword instead of specifying a value for the banner string, as follows:

```
hostname(config-group-policy)# banner {value banner_string | none}
```

The following example shows how to create a banner for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

Specify Address Pools for Remote Access Connections

When remote access clients connect to the ASA, the ASA can assign the client an IPv4 or IPv6 address based on the group-policy specified for the connection.

You can specify a list of up to six local address pools to use for local address allocation. The order in which you specify the pools is significant. The ASA allocates addresses from these pools in the order in which the pools appear in this command.

Assign an IPv4 Address Pool to an Internal Group Policy

Before you begin

Create the IPv4 address pool.

Procedure

Step 1 Enter group policy configuration mode.

group-policy *value* **attributes**

Example:

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Step 2 Assign the address pool named ipv4-pool1, ipv4-pool2, and ipv4pool3 to the FirstGroup group policy. You are allowed to specify up to 6 address pools for group-policy.

address-pools value *pool-name1 pool-name2 pool-name6*

Example:

```
asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
asa4(config-group-policy)#
```

Step 3 (Optional) Use the **no address-pools value pool-name** command to remove the address-pools from the group policy configuration and return the address pool setting to inherit the address pool information from other sources such as the DefltGroupPolicy.

no address-pools value *pool-name1 pool-name2 pool-name6*

Example:

```
hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
hostname(config-group-policy)#
```

Step 4 (Optional) The **address-pools none** command disables this attribute from being inherited from other sources of policy, such as the DefltGrpPolicy.

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

Step 5 (Optional) The **no address pools none** command removes the **address-pools none** command from the group policy, restoring the default value, which is to allow inheritance.

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

Assign an IPv6 Address Pool to an Internal Group Policy

Before you begin

Create the IPv6 address pool. See IP Addresses for VPNs.

Procedure

Step 1 Enter group policy configuration mode.

group-policy *value* **attributes**

Example:

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Step 2 Assign the address pool named ipv6-pool to the FirstGroup group policy. You can assign up to six ipv6 address pools to a group policy.

Example:

This example shows ipv6-pool1, ipv6-pool2, and ipv6-pool3 being assigned to the FirstGroup group policy.

```
hostname(config-group-policy)# ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

Step 3 (Optional) Use the **no ipv6-address-pools value pool-name** command to remove the address-pools from the group policy configuration and return the address pool setting to inherit the address pool information from other sources such as the DfltGroupPolicy.

no ipv6-address-pools value pool-name1 pool-name2 pool-name6

Example:

```
hostname(config-group-policy)# no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

Step 4 (Optional) Use the **ipv6-address-pools none** command to disable this attribute from being inherited from other sources of policy, such as the DfltGrpPolicy.

```
hostname(config-group-policy)# ipv6-address-pools none
hostname(config-group-policy)#
```

Step 5 (Optional) Use the **no ipv6-address pools none** command to remove the **ipv6-address-pools none** command from the group policy, restoring the default value, which is to allow inheritance.

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

Specify the Tunneling Protocol for the Group Policy

Specify the VPN tunnel type for this group policy by entering the **vpn-tunnel-protocol**{ ikev1 | ikev2 | l2tp-ipsec | ssl-client} command from group-policy configuration mode.

The default value is to inherit the attributes of the Default Group Policy. To remove the attribute from the running configuration, enter the **no** form of this command.

The parameter values for this command include:

- ikev1—Negotiates an IPsec IKEv1 tunnel between two peers (the Cisco VPN Client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
- ikev2—Negotiates an IPsec IKEv2 tunnel between two peers (the AnyConnect Client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
- **l2tp-ipsec**—Negotiates an IPsec tunnel for an L2TP connection.
- ssl-client—Negotiates an SSL tunnel using TLS or DTLS with the AnyConnect Client.

Enter this command to configure one or more tunneling modes. You must configure at least one tunneling mode for users to connect over a VPN tunnel.

The following example shows how to configure the IPsec IKEv1 tunneling mode for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

Specify a VLAN for Remote Access or Apply a Unified Access Control Rule to the Group Policy

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol. You can specify an IPv4 or IPv6 unified access control list for your group policy or allow it to inherit the ACLs specified in the Default Group Policy.

Choose one of the following options to specify an egress VLAN (also called "VLAN mapping") for remote access or specify an ACL to filter the traffic:

Note When doing VLAN mapping with IPv6, the outside (destination) address must be unique for each of the VLANs so that decrypted traffic is routed to inside networks. You cannot have the same destination network with different VLANs and route metrics.

- Enter the following command in group-policy configuration mode to specify the egress VLAN for remote access VPN sessions assigned to this group policy or to a group policy that inherits this group policy:

  [**no**] **vlan** {*vlan_id* |**none**}

  no vlan removes the *vlan_id* from the group policy. The group policy inherits the vlan value from the default group policy.

  none removes the *vlan_id* from the group policy and disables VLAN mapping for this group policy. The group policy does not inherit the vlan value from the default group policy.

  vlan_id is the number of the VLAN, in decimal format, to assign to remote access VPN sessions that use this group policy. The VLAN must be configured on this ASA per the instructions in the "Configuring VLAN Subinterfaces and 802.1Q Trunking" in the general operations configuration guide.

Note For clientless VPN connections, the egress VLAN feature works for only HTTP protocol.

- Specify the name of the access control rule (ACL) to apply to VPN session, using the **vpn-filter** command in group policy mode. You can specify an IPv4 or IPv6 ACL using the vpn-filter command.

Note You can also configure this attribute in username mode, in which case the value configured under username supersedes the group-policy value.

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

You configure ACLs to permit or deny various types of traffic for this group policy. You then enter the **vpn-filter** command to apply those ACLs.

To remove the ACL, including a null value created by entering the **vpn-filter none** command, enter the **no** form of this command. The **no** option allows inheritance of a value from another group policy.

A group policy can inherit this value from another group policy. To prevent inheriting a value, enter the **none** keyword instead of specifying an ACL name. The **none** keyword indicates that there is no ACL and sets a null value, thereby disallowing an ACL.

The following example shows how to set a filter that invokes an ACL named acl_vpn for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

A **vpn-filter** command is applied to post-decrypted traffic after it exits a tunnel and pre-encrypted traffic before it enters a tunnel. An ACL that is used for a vpn-filter should not also be used for an interface access-group. When a **vpn-filter** command is applied to a group policy that governs Remote Access VPN client connections, the ACL should be configured with the client assigned IP addresses in the **src_ip** position of the ACL and the local network in the **dest_ip** position of the ACL.

When a **vpn-filter** command is applied to a group-policy that governs a LAN to LAN VPN connection, the ACL should be configured with the remote network in the **src_ip** position of the ACL and the local network in the **dest_ip** position of the ACL.

Caution should be used when constructing the ACLs for use with the vpn-filter feature. The ACLs are constructed with the post-decrypted traffic in mind. However, ACLs are also applied to the traffic in the opposite direction. For this pre-encrypted traffic that is destined for the tunnel, the ACLs are constructed with the **src_ip** and **dest_ip** positions swapped.

Also note that the VPN filter applies to initial connections only. It does not apply to secondary connections, such as a SIP media connection, that are opened due to the action of application inspection.

In the following example, the vpn-filter is used with a Remote Access VPN client. This example assumes that the client assigned IP address is 10.10.10.1/24 and the local network is 192.168.1.0/24.

The following ACE allows the Remote Access VPN client to telnet to the local network:

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

The following ACE allows the local network to telnet to the Remote Access client:

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
 23 192.168.1.0 255.255.255.0
```



Note The ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23** allows the local network to initiate a connection to the Remote Access client on any TCP port if it uses a source port of 23. The ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0** allows the Remote Access client to initiate a connection to the local network on any TCP port if it uses a source port of 23.

In the next example, the vpn-filter is used with a LAN to LAN VPN connection. This example assumes that the remote network is 10.0.0.0/24 and the local network is 192.168.1.0/24. The following ACE allows remote network to telnet to the local network:

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

The following ACE allows the local network to telnet to the remote network:

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23
 192.168.1.0 255.255.255.0
```



Note The ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23** allows the local network to initiate a connection to the remote network on any TCP port if it uses a source port of 23. The ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0** allows the remote network to initiate a connection to the local network on any TCP port if it uses a source port of 23.

Specify VPN Access Hours for a Group Policy

Before you begin

Create a time range. See the "Configuring Time Ranges" in the general operations configuration guide.

Procedure

Step 1 Enter group policy configuration mode.

group-policy *value* **attributes**

Example:

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Step 2 You can set the VPN access hours by associating a configured time-range policy with a group policy using the **vpn-access-hours** command in group-policy configuration mode. This command assigns a VPN access time range named business-hours to the group policy named FirstGroup.

A group policy can inherit a time-range value from a default or specified group policy. To prevent this inheritance, enter the **none** keyword instead of the name of a time-range in this command. This keyword sets VPN access hours to a null value, which allows no time-range policy.

vpn-access-hours value {*time-range-name* | **none**}

Example:

```
hostname(config-group-policy)# vpn-access-hours value business-hours
hostname(config-group-policy)#
```

Specify Simultaneous VPN Logins for a Group Policy

You can set a limit on the number of simultaneous sessions a given user can maintain for a group policy. The default is 3 simultaneous sessions.

Stale AnyConnect Client, IPsec Client, or Clientless sessions (sessions that are terminated abnormally) might remain in the session database, even though a "new" session has been established with the same username.

If the allowed number of simultaneous sessions is 1, and the same user logs in again after an abnormal termination, then the stale session is removed from the database, and the new session is established. If, however, the existing session is still an active connection and the same user logs in again, perhaps from another PC, the first session is logged off and removed from the database, and the new session is established.

If the number of allowed simultaneous sessions is greater than 1, then, when the user has reached that maximum number and tries to log in again, the session with the longest idle time is logged off. If all current sessions have been idle an equally long time, then the oldest session is logged off. This action frees up a session and allows the new login.

Once the maximum session limit is reached, it takes some time for the system to delete the oldest session. Thus, a user might not be able to immediately log on and might have to retry the new connection before it completes successfully. This should not be a problem if users log off their sessions as expected. You can optionally remove the delay by configuring the system to not wait for the deletion to complete and immediately allow the new user connection.

Procedure

	Command or Action	Purpose

Step 1	Specify the number of simultaneous logins allowed for any user, using the **vpn-simultaneous-logins** *integer* command in group-policy configuration mode.	**vpn-simultaneous-logins** *integer*
		The default value is 3. The range is an integer from 0 through 2147483647. A group policy can inherit this value from another group policy. Enter 0 to disable login and prevent user access. The following example shows how to allow a maximum of 4 simultaneous logins for the group policy named FirstGroup:
		`hostname(config)# group-policy FirstGroup attributes`
		`hostname(config-group-policy)# vpn-simultaneous-logins 4`
		Note
		• While the maximum limit for the number of simultaneous logins is very large, allowing several simultaneous logins could compromise security and affect performance.

	Command or Action	Purpose
		• When you connect to different tunnel groups with different group policies, **vpn-simultaneous-logins** deletes user sessions even if the existing sessions use a different group policy.

Step 2	(Optional.) When the simultaneous login limit is reached, configure the system to establish new sessions without waiting for the oldest session to be deleted.	**vpn-simultaneous-login-delete-no-delay**
		This option is disabled by default.
		`hostname(config)# group-policy FirstGroup attributes`
		`hostname(config-group-policy)# vpn-simultaneous-login-delete-no-delay`

Restrict Access to a Specific Connection Profile

Specify whether to restrict remote users to access only through the connection profile, using the **group-lock** command in group-policy configuration mode.

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

The *tunnel-grp-name* variable specifies the name of an existing connection profile that the ASA requires for the user to connect. Group-lock restricts users by checking if the group configured in the VPN client is the same as the connection profile to which the user is assigned. If it is not, the ASA prevents the user from connecting. If you do not configure group-lock, the ASA authenticates users without regard to the assigned group. Group locking is disabled by default.

To remove the **group-lock** attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value from another group policy.

To disable group-lock, enter the **group-lock** command with the **none** keyword. The none keyword sets group-lock to a null value, thereby allowing no group-lock restriction. It also prevents inheriting a group-lock value from a default or specified group policy

Specify the Maximum VPN Connection Time in a Group Policy

Procedure

Step 1 (Optional) Configure a maximum amount of time for VPN connections, using the **vpn-session-timeout** {*minutes* command in group-policy configuration mode or in username configuration mode.

The minimum time is 1 minute, and the maximum time is 35791394 minutes. There is no default value. At the end of this period of time, the ASA terminates the connection.

The following example shows how to set a VPN session timeout of 180 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

The following example shows how to set a VPN session timeout of 180 minutes for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

Other actions using the [**no**] **vpn-session-timeout** {*minutes* | **none**} command:

- To remove the attribute from this policy and allow inheritance, enter the **no vpn-session-timeout** form of this command.
- To allow an unlimited timeout period, and thus prevent inheriting a timeout value, enter **vpn-session-timeout none**.

Step 2 Configure the time at which a session timeout alert message is displayed to the user using the **vpn-session-timeout alert-interval** {*minutes* | } command.

This alert message tells users how many minutes left until their VPN session is automatically disconnected. The following example shows how to specify that users will be notified 20 minutes before their VPN session is disconnected. You can specify a range of 1-30 minutes.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

Other actions using the [**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} command:

- Use the no form of the command to indicate that the VPN session timeout alert-interval attribute will be inherited from the Default Group Policy:

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- The **vpn-session-timeout alert-interval none** indicates that users will not receive an alert.

Specify a VPN Session Idle Timeout for a Group Policy

Procedure

Step 1 (Optional) To configure a VPN idle timeout period use the **vpn-idle-timeout** *minutes* command in group-policy configuration mode or in username configuration mode.

If there is no communication activity on the connection in this period, the ASA terminates the connection. The minimum time is 1 minute, the maximum time is 35791394 minutes, and the default is 30 minutes.

The following example shows how to set a VPN idle timeout of 15 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

Other actions using the [**no**] **vpn-idle-timeout** {*minutes* | **none**} command:

- Enter **vpn-idle-timeout none** to disable VPN idle timeout and pevent inheriting a timeout value.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout none
hostname(config-group-policy)#
```

  This results in AnyConnect Client (both SSL and IPsec/IKEv2) and Clientless VPN using the global webvpn **default-idle-timeout** *seconds* value. This command is entered in webvpn-config mode, for example: `hostnamee(config-webvpn)# default-idle-timeout 300`. The default is 1800 seconds (30 min), the range is 60-86400 seconds.

  For all webvon connections , the **default-idle-timeout** value is enforced only if **vpn-idle-timeout none** is set in the group policy/username attribute. A non-zero idle timeout value is required by ASA for all AnyConnect Client connections.

  For Site-to-Site (IKEv1, IKEv2) and IKEv1 remote-access VPNs, we recommend you Disable timeout and allow for an unlimited idle period.

- To disable the idle timeout for this group policy or user policy, enter **no vpn-idle-timeout**. The value will be inherited.
- If you do not set **vpn-idle-timeout** at all, in anyway, the value is inherited, which defaults to 30 minutes.

Note
vpn-idle-timeout controls only the maximum time for a parent session. Child sessions (SSL/DTLS) are aggressively terminated much sooner by a hardcoded 5-minute TCP inactivity timeout or on failing the 3×Dead Peer Detection (DPD) check. For more details, see the note in Configure Dead Peer Detection. For further details on DPD, keepalives, and timeout attributes, see Answer AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer.

Step 2 (Optional) You can optionally configure the time at which an idle timeout alert message is displayed to the user using the **vpn-idle-timeout alert-interval** {*minutes*} command.

This alert message tells users how many minutes they have left until their VPN session is disconnected due to inactivity. The default alert interval is one minute.

The following example shows how to set a VPN idle timeout alert interval of 3 minutes for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

Other actions using the [**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} command:

- The **none** parameter indicates that users will not receive an alert.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- To remove the alert interval for this group or user policy enter **no vpn-idle-timeout alert-interval**. The value will be inherited.

- If you do not set this parameter at all, the default alert interval is one minute.

Configure WINS and DNS Servers for a Group Policy

You can specify primary and secondary WINS servers and DNS servers. The default value in each case is none. To specify these servers, perform the following steps:

Procedure

Step 1 Specify the primary and secondary WINS servers:

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

The first IP address specified is that of the primary WINS server. The second (optional) IP address is that of the secondary WINS server. Specifying the **none** keyword instead of an IP address sets WINS servers to a null value, which allows no WINS servers and prevents inheriting a value from a default or specified group policy.

Every time that you enter the **wins-server** command, you overwrite the existing setting. For example, if you configure WINS server x.x.x.x and then configure WINS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole WINS server. The same is true for multiple servers. To add a WINS server rather than overwrite previously configured servers, include the IP addresses of all WINS servers when you enter this command.

The following example shows how to configure WINS servers with the IP addresses 10.10.10.15 and 10.10.10.30 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

Step 2 Specify the primary and secondary DNS servers:

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

The first IP address specified is that of the primary DNS server. The second (optional) IP address is that of the secondary DNS server. Specifying the **none** keyword instead of an IP address sets DNS servers to a null value, which allows no DNS servers and prevents inheriting a value from a default or specified group policy. You can specify up to four DNS server addresses: up to two IPv4 addresses and two IPv6 addresses.

Every time that you enter the **dns-server** command, you overwrite the existing setting. For example, if you configure DNS server x.x.x.x and then configure DNS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole DNS server. The same is true for multiple servers. To add a DNS server rather than overwrite previously configured servers, include the IP addresses of all DNS servers when you enter this command.

The following example shows how to configure DNS servers with the IP addresses 10.10.10.15, 10.10.10.30, 2001:DB8::1, and 2001:DB8::2 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30
2001:DB8::1 2001:DB8::2
hostname(config-group-policy)#
```

Step 3 If there is no default domain name specified in the **DefaultDNS DNS** server group, you must specify a default domain. Use the domain name and top level domain for example, **example.com.**

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

Step 4 (Optional.) Configure the DHCP network scope:

dhcp-network-scope {*ip_address* | **none**}

If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same subnet identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group.

If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

To specify a scope, enter a routeable address on the same subnet as the desired pool, but not within the pool. The DHCP server determines which subnet this IP address belongs to and assigns an IP address from that pool.

We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the DHCP scope. Do not use the network number. You can use DHCP for IPv4 addressing only. If the address you choose is not an interface address, you might need to create a static route for the scope address.

Specifying **none** prevents DHCP address assignment, for example, from a default or inherited group policy.

Example:

The following example enters attribute configuration mode for FirstGroup and sets the DHCP scope to 10.100.10.1.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

Set the Split-Tunneling Policy

Set the rules for tunneling traffic by specifying the split-tunneling policy for IPv4 traffic:

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

Set the rules for tunneling traffic by specifying the split-tunneling policy for IPv6 traffic:

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

The policies options are:

- **tunnelspecified**— Tunnels all traffic to or from the networks specified in the Network List through the tunnel. Data to all other addresses travels in the clear and is routed by the remote user's Internet service provider.

  For versions of ASA 9.1.4 and higher, when you specify an include list, you can also specify an exclude list for a subnet inside the include range. Addresses in the excluded subnet will not be tunneled, and the rest of the include list will be. The networks in the exclusion list will not be sent over the tunnel. The exclusion list is specified using deny entries, and the inclusion list is specified using permit entries.

- **excludespecified**—Does not tunnel traffic to or from the networks specified in the Network List. Traffic from or to all other addresses is tunneled. . The VPN client profile that is active on the client must have Local LAN Access enabled. This option works with AnyConnect Clients only.

Note Networks in the exclusion list that are not a subset of the include list are ignored by the client.

- **tunnelall —**Specifies that all traffic goes through the tunnel. This policy disables split tunneling. Remote users have access to the corporate network, but they do not have access to local networks. This is the default option.

Note Split tunneling is a traffic management feature, not a security feature. For optimum security, we recommend that you do not enable split tunneling.

Example

The following examples shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup for IPv4 and IPv6:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

Specify a Network List for Split-Tunneling

In split tunneling, network lists determine what network traffic travels across the tunnel. AnyConnect Client makes split tunneling decisions on the basis of a network list, which is an ACL.

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
```

```
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

- **value** access-list name — identifies an ACL that enumerates the networks to tunnel or not tunnel. The ACL can be a unified ACL with ACEs that specify both IPv4 and IPv6 addresses.
- **none** — indicates that there is no network list for split tunneling; the ASA tunnels all traffic. Specifying the **none** keyword sets a split tunneling network list with a null value, thereby disallowing split tunneling. It also prevents inheriting a default split tunneling network list from a default or specified group policy.

To delete a network list, enter the **no** form of this command. To delete all split tunneling network lists, enter the **no split-tunnel-network-list** command without arguments. This command deletes all configured network lists, including a null list if you created one by entering the **none** keyword.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, enter the **split-tunnel-network-list none** command.

Example

The following example shows how to create a network list named FirstList, and add it to the group policy named FirstGroup. FistList is an exclusion list and an inclusion list that is a subnet of the exclusion list:

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

The following example shows how to create a network list named v6, and add the v6 split tunnel policy to the group policy named GroupPolicy_ipv6-ikev2. v6 is an exclusion list and an inclusion list that is a subnet of the exclusion list:

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value v6
```

Verify the Split Tunnel Configuration

Run the **show runn group-policy attributes** command to verify your configuration. This example shows that the administrator has set both an IPv4 and IPv6 network policy and used the network list (unified ACL), **FirstList** for both policies.

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
 split-tunnel-policy tunnelspecified
 ipv6-split-tunnel-policy tunnelspecified
 split-tunnel-network-list value FirstList
```

Configure Domain Attributes for Split Tunneling

You can specify a default domain name or a list of domains to be resolved through the split tunnel, which we refer to as split DNS.

AnyConnect 3.1 supports true split DNS functionality for Windows and Mac OS X platforms. If the group policy on the security appliance enables split-include tunneling, and if it specifies the DNS names to be tunneled, AnyConnect tunnels any DNS queries that match those names to the private DNS server. True split DNS allows tunnel access to only DNS requests that match the domains pushed to the client by the ASA. These requests are not sent in the clear. On the other hand, if the DNS requests do not match the domains pushed down by the ASA, AnyConnect lets the DNS resolver on the client operating system submit the host name in the clear for DNS resolution.



Note Split DNS supports standard and update queries (including A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR, and CNAME). PTR queries matching any of the tunneled networks are allowed through the tunnel.

For Mac OS X, AnyConnect can use true split-DNS for a certain IP protocol only if one of the following conditions is met:

- Split-DNS is configured for one IP protocol (such as IPv4), and Client Bypass Protocol is configured for the other IP protocol (such as IPv6) in the group policy (with no address pool configured for the latter IP protocol).
- Split-DNS is configured for both IP protocols.

Define a Default Domain Name

The ASA passes the default domain name to the AnyConnect Client. The client appends the domain name to DNS queries that omit the domain field. This domain name applies only to tunneled packets.When there are no default domain names, users inherit the default domain name in the default group policy.

To specify the default domain name for users of the group policy, enter the **default-domain** command in group-policy configuration mode. To delete a domain name, enter the **no** form of this command.

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

The **value** domain-name parameter identifies the default domain name for the group. To specify that there is no default domain name, enter the **none** keyword. This command sets a default domain name with a null value, which disallows a default domain name and prevents inheriting a default domain name from a default or specified group policy.

To delete all default domain names, enter the **no default-domain** command without arguments. This command deletes all configured default domain names, including a null list if you created one by entering the **default-domain** command with the **none** keyword. The **no** form allows inheriting a domain name.

The following example shows how to set a default domain name of FirstDomain for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

Define a List of Domains for Split Tunneling

Enter a list of domains to be resolved through the split tunnel, in addition to the default domain. Enter the **split-dns** command in group-policy configuration mode. To delete a list, enter the **no** form of this command.

When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, enter the **split-dns** command with the **none** keyword.

To delete all split tunneling domain lists, enter the **no split-dns** command without arguments. This deletes all configured split tunneling domain lists, including a null list created by issuing the **split-dns** command with the **none** keyword.

The parameter **value** domain-name provides a domain name that the ASA resolves through the split tunnel. The **none** keyword indicates that there is no split DNS list. It also sets a split DNS list with a null value, thereby disallowing a split DNS list, and prevents inheriting a split DNS list from a default or specified group policy. The syntax of the command is as follows:

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2... domain-nameN]
 | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

Enter a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 492 characters. You can use only alphanumeric characters, hyphens (-), and periods (.). If the default domain name is to be resolved through the tunnel, you must explicitly include that name in this list.

The following example shows how to configure the domains Domain1, Domain2, Domain3, and Domain4 to be resolved through split tunneling for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```



Note When configuring split DNS, ensure the private DNS servers specified do not overlap with the DNS servers configured for the client platform. If they do, name resolution does not function properly and queries may be dropped.

Configure DHCP Intercept for Windows XP and Split Tunneling

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. To avoid this problem, the ASA limits the number of routes it sends to 27 to 40 routes, with the number of routes dependent on the classes of the routes.

DHCP Intercept lets Microsoft Windows XP clients use split-tunneling with the ASA. The ASA replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to Windows XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous.

The **intercept-dhcp** command enables or disables DHCP intercept.

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
```

```
hostname(config-group-policy)#
```

The *netmask* variable provides the subnet mask for the tunnel IP address. The **no** form of this command removes the DHCP intercept from the configuration:

[**no**] **intercept-dhcp**

The following example shows how to set DHCP Intercepts for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

Configure Browser Proxy Settings for use with Remote Access Clients

Follow these steps to configure the proxy server parameters for a client.

Procedure

Step 1 Configure a browser proxy server and port for a client device by entering the **msie-proxy server** command in group-policy configuration mode:

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

The default value is **none**, which is not specifying any proxy server settings on the browser of the client device. To remove the attribute from the configuration, use the **no** form of the command.

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

The following example shows how to configure the IP address 192.168.10.1 as a browser proxy server, using port 880, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

Step 2 Configure the browser proxy actions ("methods") for a client device by entering the **msie-proxy method** command in group-policy configuration mode.

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

The default value is **no-modify**. To remove the attribute from the configuration, use the **no** form of the command.

```
hostname(config-group-policy)# no msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

The available methods are as follows:

- **auto-detect**—Enables the use of automatic proxy server detection in the browser for the client device.
- **no-modify**—Leaves the HTTP browser proxy server setting in the browser unchanged for this client device.
- **no-proxy—**Disables the HTTP proxy setting in the browser for the client device.
- **use-server—**Sets the HTTP proxy server setting in the browser to use the value configured in the **msie-proxy server** command.

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

The following example shows how to configure auto-detect as the browser proxy setting for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

The following example configures the browser proxy setting for the group policy named FirstGroup to use the server QAserver, port 1001 as the server for the client device:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

Step 3 Configure browser proxy exception list settings for a local bypass on the client device by entering the **msie-proxy except-list** command in group-policy configuration mode. These addresses are not accessed by a proxy server. This list corresponds to the Exceptions box in the Proxy Settings dialog box.

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

To remove the attribute from the configuration, use the **no** form of the command:

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value** server:port—Specifies the IP address or name of an MSIE server and port that is applied for this client device. The port number is optional.

- **none**—Indicates that there is no IP address/hostname or port and prevents inheriting an exception list.

By default, msie-proxy except-list is disabled.

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

The following example shows how to set a browser proxy exception list, consisting of the server at IP address 192.168.20.1, using port 880, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

Step 4 Enable or disable browser proxy local-bypass settings for a client device by entering the **msie-proxy local-bypass** command in group-policy configuration mode.

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

To remove the attribute from the configuration, use the **no** form of the command.

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

By default, msie-proxy local-bypass is disabled.

The following example shows how to enable browser proxy local-bypass for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

Configure Security Attributes for IPsec (IKEv1) Clients

To specify the security settings for a group, perform these steps.

Procedure

Step 1 Specify whether to let users store their login passwords on the client system, using the **password-storage** command with the **enable** keyword in group-policy configuration mode. To disable password storage, use the **password-storage** command with the **disable** keyword.

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

For security reasons, password storage is disabled by default. Enable password storage only on systems that you know to be in secure sites.

To remove the password-storage attribute from the running configuration, enter the **no** form of this command:

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

Specifying the **no** form enables inheritance of a value for password-storage from another group policy.

This command does not apply to interactive hardware client authentication or individual user authentication for hardware clients.

The following example shows how to enable password storage for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

Step 2 Specify whether to enable IP compression, which is disabled by default.

Note
IP compression is not supported for IPsec IKEv2 connections.

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

To enable LZS IP compression, enter the **ip-comp** command with the **enable** keyword in group-policy configuration mode. To disable IP compression, enter the **ip-comp** command with the **disable** keyword.

To remove the **ip-comp** attribute from the running configuration, enter the **no** form of this command. This enables inheritance of a value from another group policy.

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

Enabling data compression might speed up data transmission rates for remote dial-in users connecting with modems.

Tip
Data compression increases the memory requirement and CPU usage for each user session and consequently decreases the overall throughput of the ASA. For this reason, we recommend that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users, and enable compression only for them.

Step 3 Specify whether to require that users reauthenticate on IKE re-key by using the **re-xauth** command with the **enable** keyword in group-policy configuration mode.

Note
IKE re-key is not supported for IKEv2 connections.

If you enable reauthentication on IKE re-key, the ASA prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE re-key occurs. Reauthentication provides additional security.

If the configured re-key interval is very short, users might find the repeated authorization requests inconvenient. To avoid repeated authorization requests, disable reauthentication. To check the configured re-key interval, in monitoring mode, enter the **show crypto ipsec sa** command to view the security association lifetime in seconds and lifetime in kilobytes of data. To disable user reauthentication on IKE re-key, enter the **disable** keyword. Reauthentication on IKE re-key is disabled by default.

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

To enable inheritance of a value for reauthentication on IKE re-key from another group policy, remove the re-xauth attribute from the running configuration by entering the **no** form of this command:

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

Note
Reauthentication fails if there is no user at the other end of the connection.

Step 4 Specify whether to enable perfect forward secrecy. In IPsec negotiations, perfect forward secrecy ensures that each new cryptographic key is unrelated to any previous key. A group policy can inherit a value for perfect forward secrecy from another group policy. Perfect forward secrecy is disabled by default. To enable perfect forward secrecy, use the **pfs** command with the **enable** keyword in group-policy configuration mode.

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

To disable perfect forward secrecy, enter the **pfs** command with the **disable** keyword.

To remove the perfect forward secrecy attribute from the running configuration and prevent inheriting a value, enter the **no** form of this command.

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

Configure IPsec-UDP Attributes for IKEv1 Clients

IPsec over UDP, sometimes called IPsec through NAT, lets a hardware client connect via UDP to a ASA that is running NAT. It is disabled by default. IPsec over UDP is proprietary; it applies only to remote-access connections, and it requires mode configuration. The ASA exchanges configuration parameters with the client while negotiating SAs. Using IPsec over UDP may slightly degrade system performance.

To enable IPsec over UDP, configure the **ipsec-udp** command with the **enable** keyword in group-policy configuration mode, as follows:

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

To use IPsec over UDP, you must also configure the **ipsec-udp-port** command, as described in this section.

To disable IPsec over UDP, enter the **disable** keyword. To remove the IPsec over UDP attribute from the running configuration, enter the **no** form of this command. This enables inheritance of a value for IPsec over UDP from another group policy.

The following example shows how to set IPsec over UDP for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

If you enabled IPsec over UDP, you must also configure the **ipsec-udp-port** command in group-policy configuration mode. This command sets a UDP port number for IPsec over UDP. In IPsec negotiations, the ASA listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic. The port numbers can range from 4001 through 49151. The default port value is 10000.

To disable the UDP port, enter the **no** form of this command. This enables inheritance of a value for the IPsec over UDP port from another group policy.

```
hostname(config-group-policy)# ipsec-udp-port port
```

The following example shows how to set an IPsec UDP port to port 4025 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

Configure Attributes for VPN Hardware Clients

Procedure

Step 1 (Optional) Configure Network Extension Mode with the following command:

[**no**] **nem** [**enable** | **disable**]

Network extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. PAT does not apply. Therefore, devices behind the Easy VPN Server have direct access to devices on the private network behind the Easy VPN Remote over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.

Example:

The following example shows how to set NEM for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

To disable NEM, enter the **disable** keyword. To remove the NEM attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value from another group policy.

Step 2 (Optional) Configure Secure Unit Authentication with the following command:

[**no**] **secure-unit-authentication** [**enable** | **disable**]

Secure unit authentication provides additional security by requiring VPN hardware clients to authenticate with a username and password each time that the client initiates a tunnel. With this feature enabled, the hardware client does not a use the saved username and password if configured. Secure unit authentication is disabled by default.

Secure unit authentication requires that you have an authentication server group configured for the connection profile the hardware client(s) uses. If you require secure unit authentication on the primary ASA, be sure to configure it on any backup servers as well.

Note
With this feature enabled, to bring up a VPN tunnel, a user must be present to enter the username and password.

Example:

The following example shows how to enable secure unit authentication for the group policy named FirstGroup:

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

To disable secure unit authentication, enter the **disable** keyword. To remove the secure unit authentication attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value for secure unit authentication from another group policy.

Step 3 (Optional) Configure User Authentication with the following command:

[**no**] **user-authentication** [**enable** | **disable**]

When enabled, user authentication requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel. Individual users authenticate according to the order of authentication servers that you configure. User authentication is disabled by default.

If you require user authentication on the primary ASA, be sure to configure it on any backup servers as well.

Example:

The following example shows how to enable user authentication for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

To disable user authentication, enter the **disable** keyword. To remove the user authentication attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value for user authentication from another group policy.

Step 4 Set an idle timeout for individual users that have authenticated with the following command:

[**no**] **user-authentication-idle-timeout** *minutes* | **none**]

The *minutes* parameter specifies the number of minutes in the idle timeout period. The minimum is 1 minute, the default is 30 minutes, and the maximum is 35791394 minutes.

If there is no communication activity by a user behind a hardware client in the idle timeout period, the ASA terminates the client's access. This timer terminates only the client's access through the VPN tunnel, not the VPN tunnel itself.

Example:

The following example shows how to set an idle timeout value of 45 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)#user-authentication-idle-timeout 45
```

To delete the idle timeout value, enter the **no** form of this command. This option allows inheritance of an idle timeout value from another group policy. To prevent inheriting an idle timeout value, enter the **user-authentication-idle-timeout** command with the **none** keyword. This command sets the idle timeout with a null value, which disallows an idle timeout and prevents inheriting a user authentication idle timeout value from a default or specified group policy.

Note
The idle timeout indicated in response to the **show uauth** command is always the idle timeout value of the user who authenticated the tunnel on the Cisco Easy VPN remote device.

Step 5 Configure IP Phone Bypass with the followng command:

ip-phone-bypass enable

IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. IP Phone Bypass is disabled by default. This only applies when IUA is enabled.

Note
You must also configure MAC address exemption on the client to exempt these clients from authentication.

To disable IP Phone Bypass, enter the **disable** keyword. To remove the IP phone Bypass attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value for IP Phone Bypass from another group policy.

Step 6 Configure LEAP Bypass with the following command:

leap-bypass enable

LEAP Bypass only applies when **user-authentication** is enabled. This command lets LEAP packets from Cisco wireless access point devices establish LEAP authentication and then authenticate again per user authentication. LEAP Bypass is disabled by default.

LEAP users behind a hardware client have a circular dilemma: they cannot negotiate LEAP authentication because they cannot send their credentials to the RADIUS server behind the central site device over the tunnel. The reason they cannot send their credentials over the tunnel is that they have not authenticated on the wireless network. To solve this problem, LEAP Bypass lets LEAP packets, and only LEAP packets, traverse the tunnel to authenticate the wireless connection to a RADIUS server before individual users authenticate. Then the users proceed with individual user authentication.

LEAP Bypass operates correctly under the following conditions:

- **secure-unit-authentication** must be disabled. If interactive unit authentication is enabled, a non-LEAP (wired) device must authenticate the hardware client before LEAP devices can connect using that tunnel.
- **user-authentication** is enabled. Otherwise, LEAP Bypass does not apply.

- Access points in the wireless environment must be Cisco Aironet Access Points running Cisco Discovery Protocol (CDP). The wireless NIC cards for PCs can be other brands.

Example:

The following example shows how to set LEAP Bypass for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

To disable LEAP Bypass, enter the **disable** keyword. To remove the LEAP Bypass attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value for LEAP Bypass from another group policy:

Configure Group Policy Attributes for AnyConnect Client Connections

After enabling AnyConnect Client connections as described in AnyConnect VPN Client Connections, you can enable or require AnyConnect Client features for a group policy. Follow these steps in group-policy webvpn configuration mode:

Procedure

Step 1 Enter group policy webvpn configuration mode. For example:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

Step 2 To disable the permanent installation of the AnyConnect Client on the endpoint computer, use the anyconnect keep-installer command with the **none** keyword. For example:

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

The default is that permanent installation of the client is enabled. The client remains installed on the endpoint at the end of the AnyConnect Client session.

Step 3 To enable compression of HTTP data over the AnyConnect Client SSL connection for the group policy, enter the anyconnect ssl compression command. By default, compression is set to **none** (disabled). To enable compression, use the **deflate** keyword. For example:

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

Step 4 Configure Dead Peer Detection

Step 5 You can ensure that the AnyConnect Client connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle by adjusting the frequency of keepalive messages using the **anyconnect ssl keepalive command:**

anyconnect ssl keepalive {none | *seconds***}**

Adjusting keepalives also ensures the AnyConnect Client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

The following example configures the security appliance to enable the AnyConnect Client to send keepalive messages, with a frequency of 300 seconds (5 minutes):

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

Step 6 To enable the AnyConnect Client to perform a re-key on an SSL session, use the anyconnect ssl rekey command:

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}}

By default, re-key is disabled.

Specifying the method as new-tunnel specifies that the AnyConnect Client establishes a new tunnel during SSL re-key. Specifying the method as none disables re-key. Specifying the method as ssl specifies that SSL renegotiation takes place during re-key. Instead of specifying the method, you can specify the time; that is, the number of minutes from the start of the session until the re-key takes place, from 1 through 10080 (1 week).

The following example configures the AnyConnect Client to renegotiate with SSL during re-key and configures the re-key to occur 30 minutes after the session begins:

```
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
hostname(config-group-webvpn)#
```

Step 7 The Client Protocol Bypass feature allows you to configure how the AnyConnect Client manages IPv4 traffic when ASA is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

When the AnyConnect Client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect Client connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or “in the clear.”

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

If establishing an IPsec tunnel (as opposed to an SSL connection), the ASA is not notified whether or not IPv6 is enabled on the client, so ASA always pushes down the client bypass protocol setting.

Use the client-bypass-protocol command to enable or disable the client bypass protocol feature. This is the command syntax:

client-bypass-protocol {enable | disable}

The following example enables client bypass protocol:

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

The following example disables client bypass protocol:

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

The following example removes an enabled or disabled client bypass protocol setting:

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

Step 8 If you have configured Load Balancing between your ASAs, specify the FQDN of the ASA in order to resolve the ASA IP address used for re-establishing the VPN session. This setting is critical to support client roaming between networks of different IP protocols (such as IPv4 to IPv6).

You cannot use the ASA FQDN present in the AnyConnect Client profile to derive the ASA IP address after roaming. The addresses may not match the correct device (the one the tunnel was established to) in the load balancing scenario.

If the device FQDN is not pushed to the client, the client will try to reconnect to whatever IP address the tunnel had previously established. In order to support roaming between networks of different IP protocols (from IPv4 to IPv6), AnyConnect Client must perform name resolution of the device FQDN after roaming, so that it can determine which ASA address to use for re-establishing the tunnel. The client uses the ASA FQDN present in its profile during the initial connection. During subsequent session reconnects, it always uses the device FQDN pushed by ASA (and configured by the administrator in the group policy), when available. If the FQDN is not configured, the ASA derives the device FQDN (and sends it to the client) from whatever is set under Device Setup > Device Name/Password and Domain Name.

If the device FQDN is not pushed by the ASA, the client cannot re-establish the VPN session after roaming between networks of different IP protocols.

Use the gateway-fqdn command to configure the FQDN of the ASA. This is the command syntax:

gateway-fqdn { **value** *FQDN_Name* | **none**} or **no gateway-fqdn**

The following example defines the FQDN of the ASA as ASAName.example.cisco.com

```
hostname(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy)#
```

The following example removes the FQDN of the ASA from the group policy. The group policy then inherits this value from the Default Group Policy.

```
hostname(config-group-policy)# no gateway-fqdn
hostname(config-group-policy)#
```

The following example defines the FQDN as an empty value. The global FQDN configured using hostname and domain-name commands will be used if available.

```
hostname(config-group-policy)# gateway-fqdn none
hostname(config-group-policy)#
```

Configure Backup Server Attributes

Configure backup servers if you plan on using them. IPsec backup servers let a VPN client connect to the central site when the primary ASA is unavailable.When you configure backup servers, the ASA pushes the server list to the client as the IPsec tunnel is established. Backup servers do not exist until you configure them, either on the client or on the primary ASA.

Configure backup servers either on the client or on the primary ASA. If you configure backup servers on the ASA, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.



Note If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. In addition, if you use hostnames and the DNS server is unavailable, significant delays can occur.

To configure backup servers, enter the **backup-servers** command in group-policy configuration mode:

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

To remove a backup server, enter the **no** form of this command with the backup server specified. To remove the backup-servers attribute from the running configuration and enable inheritance of a value for backup-servers from another group policy, enter the **no** form of this command without arguments.

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

The **clear-client-config** keyword specifies that the client uses no backup servers. The ASA pushes a null server list.

The **keep-client-config** keyword specifies that the ASA sends no backup server information to the client. The client uses its own backup server list, if configured. This is the default.

The *server1 server 2.... server10* parameter list is a space-delimited, priority-ordered list of servers for the VPN client to use when the primary ASA is unavailable. This list identifies servers by IP address or hostname. The list can be 500 characters long, and it can contain up to10 entries.

The following example shows how to configure backup servers with IP addresses 10.10.10.1 and 192.168.10.14, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

Configure Network Admission Control Parameters

The group-policy NAC commands in this section all have default values. Unless you have a good reason for changing them, accept the default values for these parameters.

The ASA uses Extensible Authentication Protocol (EAP) over UDP (EAPoUDP) messaging to validate the posture of remote hosts. Posture validation involves the checking of a remote host for compliancy with safety requirements before the assignment of a network access policy. An Access Control Server must be configured for Network Admission Control before you configure NAC on the security appliance.

The Access Control Server downloads the posture token, an informational text string configurable on the ACS, to the security appliance to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown. Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the security appliance.

To configure Network Admission Control settings for the default group policy or an alternative group policy, perform the following steps.

Procedure

Step 1 (Optional) Configure the status query timer period. The security appliance starts the status query timer after each successful posture validation and status query response. The expiration of this timer triggers a query for changes in the host posture, referred to as a status query. Enter the number of seconds in the range 30 through 1800. The default setting is 300.

To specify the interval between each successful posture validation in a Network Admission Control session and the next query for changes in the host posture, use the **nac-sq-period** command in group-policy configuration mode:

```
hostname(config-group-policy)# nac-sq-period seconds
hostname(config-group-policy)#
```

To inherit the value of the status query timer from the default group policy, access the alternative group policy from which to inherit it, then use the **no** form of this command:

```
hostname(config-group-policy)# no nac-sq-period [seconds]
hostname(config-group-policy
```

The following example changes the value of the status query timer to 1800 seconds:

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)#
```

The following example inherits the value of the status query timer from the default group policy:

```
hostname(config-group-policy)# no nac-sq-period
```

```
hostname(config-group-policy)#
```

Step 2 (Optional) Configure the NAC revalidation period. The security appliance starts the revalidation timer after each successful posture validation. The expiration of this timer triggers the next unconditional posture validation. The security appliance maintains posture validation during revalidation. The default group policy becomes effective if the Access Control Server is unavailable during posture validation or revalidation. Enter the interval in seconds between each successful posture validation. The range is 300 through 86400. The default setting is 36000.

To specify the interval between each successful posture validation in a Network Admission Control session, use the **nac-reval-period** command in group-policy configuration mode:

```
hostname(config-group-policy)# nac-reval-period seconds
hostname(config-group-policy)#
```

To inherit the value of the Revalidation Timer from the default group policy, access the alternative group policy from which to inherit it, then use the **no** form of this command:

```
hostname(config-group-policy)# no nac-reval-period [seconds]
hostname(config-group-policy)#
```

The following example changes the revalidation timer to 86400 seconds:

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

The following example inherits the value of the revalidation timer from the default group policy:

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)#
```

Step 3 (Optional) Configure the default ACL for NAC. The security appliance applies the security policy associated with the selected ACL if posture validation fails. Specify **none** or an extended ACL. The default setting is **none**. If the setting is **none** and posture validation fails, the security appliance applies the default group policy.

To specify the ACL to be used as the default ACL for Network Admission Control sessions that fail posture validation, use the **nac-default-acl** command in group-policy configuration mode:

```
hostname(config-group-policy)# nac-default-acl {acl-name | none}
hostname(config-group-policy)#
```

To inherit the ACL from the default group policy, access the alternative group policy from which to inherit it, then use the **no** form of this command:

```
hostname(config-group-policy)# no nac-default-acl [acl-name | none]
hostname(config-group-policy)#
```

The elements of this command are as follows:

- *acl-name*—Specifies the name of the posture validation server group, as configured on the ASA using the **aaa-server host** command. The name must match the server-tag variable specified in that command.
- **none**—Disables inheritance of the ACL from the default group policy and does not apply an ACL to NAC sessions that fail posture validation.

Because NAC is disabled by default, VPN traffic traversing the ASA is not subject to the NAC Default ACL until NAC is enabled.

The following example identifies acl-1 as the ACL to be applied when posture validation fails:

```
hostname(config-group-policy)# nac-default-acl acl-1
hostname(config-group-policy)#
```

The following example inherits the ACL from the default group policy:

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)#
```

The following example disables inheritance of the ACL from the default group policy and does not apply an ACL to NAC sessions that fail posture validation:

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

Step 4 Configure NAC exemptions for VPN. By default, the exemption list is empty.The default value of the filter attribute is **none**. Enter the **vpn-nac-exempt command** once for each operating system (and ACL) to be matched to exempt remote hosts from posture validation.

To add an entry to the list of remote computer types that are exempt from posture validation, use the **vpn-nac-exempt** command in group-policy configuration mode:

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

To disable inheritance and specify that all hosts are subject to posture validation, use the **none** keyword immediately following **vpn-nac-exempt**:

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

To remove an entry from the exemption list, use the **no** form of this command and name the operating system (and ACL) in the entry to be removed:

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}]
 [disable]
hostname(config-group-policy)#
```

To remove all entries from the exemption list associated with this group policy and inherit the list from the default group policy, use the **no** form of this command without specifying additional keywords:

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

The syntax elements for these commands are as follows:

- *acl-name*—Name of the ACL present in the ASA configuration.
- disable—Disables the entry in the exemption list without removing it from the list.
- **filter**—(Optional) Apply an ACL to filter the traffic if the computer matches the OS name.
- **none**—When entered immediately after **vpn-nac-exempt**, this keyword disables inheritance and specifies that all hosts are subject to posture validation.When entered immediately after **filter**, this keyword indicates that the entry does not specify an ACL.
- **OS—**Exempts an operating system from posture validation.
- *os name*—Operating system name. Quotation marks are required only if the name includes a space (for example, “Windows XP”).

The following example disables inheritance and specifies that all hosts will be subject to posture validation:

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

The following example removes all entries from the exemption list:

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

Step 5 Enable or disable Network Admission Control by entering the following command:

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

To inherit the NAC setting from the default group policy, access the alternative group policy from which to inherit it, then use the **no** form of this command:

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

By default, NAC is disabled. Enabling NAC requires posture validation for remote access. If the remote computer passes the validation checks, the ACS server downloads the access policy for the ASA to enforce. NAC is disabled by default.

An Access Control Server must be present on the network.

The following example enables NAC for the group policy:

```
hostname(config-group-policy)# nac enable
```

```
hostname(config-group-policy)#
```

Configure VPN Client Firewall Policies

A firewall isolates and protects a computer from the Internet by inspecting each inbound and outbound packet of data to determine whether to allow it through the firewall or to drop it. Firewalls provide extra security if remote users in a group have split tunneling configured. In this case, the firewall protects the user's computer, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN. Remote users connecting to the ASA with the VPN client can choose the appropriate firewall option.

Set personal firewall policies that the ASA pushes to the VPN client during IKE tunnel negotiation by using the **client-firewall** command in group-policy configuration mode. To delete a firewall policy, enter the **no** form of this command.

To delete all firewall policies, enter the **no client-firewall** command without arguments. This command deletes all configured firewall policies, including a null policy if you created one by entering the **client-firewall** command with the **none** keyword.

When there are no firewall policies, users inherit any that exist in the default or other group policy. To prevent users from inheriting such firewall policies, enter the **client-firewall** command with the **none** keyword.

The Add or Edit Group Policy dialog box on the Client Firewall tab lets you configure firewall settings for VPN clients for the group policy being added or modified.

Note Only VPN clients running Microsoft Windows can use these firewall features. They are currently not available to hardware clients or other (non-Windows) software clients.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN client drops the connection to the ASA. (This firewall enforcement mechanism is called Are You There (AYT), because the VPN client monitors the firewall by sending it periodic "are you there?" messages; if no reply comes, the VPN client knows the firewall is down and terminates its connection to the ASA.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called push policy or Central Protection Policy (CPP). On the ASA, you create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The ASA pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

Configure AnyConnect Client Firewall Policies

Firewall rules for the AnyConnect Client can specify IPv4 and IPv6 addresses.

Before you begin

You have created Unified Access Rules with IPv6 addresses specified.

Procedure

Step 1 Enter webvpn group policy configuration mode.

webvpn

Example:

```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```

Step 2 Specify an access control rule for the private or public network rule. The private network rule is the rule applied to the VPN virtual adapter interface on the client.

anyconnect firewall-rule client-interface {private | public} value *[RuleName]*

```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value
ClientFWRule
```

Step 3 Display the group policy attributes as well as the webvpn policy attribute for the group policy.

show runn group-policy [value]

Example:

```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
webvpn
  anyconnect firewall-rule client-interface private value ClientFWRule
```

Step 4 Remove the client firewall rule from the private network rule.

no anyconnect firewall-rule client-interface private value [*RuleName*]

Example:

```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value
hostname(config-group-webvpn)#
```

Use of a Zone Labs Integrity Server

This section introduces the Zone Labs Integrity server, also called the Check Point Integrity server, and presents an example procedure for configuring the ASA to support the Zone Labs Integrity server. The Integrity server is a central management station for configuring and enforcing security policies on remote PCs. If a remote PC does not conform to the security policy dictated by the Integrity server, it is not granted access to the private network protected by the Integrity server and ASA.

The VPN client software and the Integrity client software are co-resident on a remote PC. The following steps summarize the actions of the remote PC, ASA, and Integrity server in the establishment of a session between the PC and the enterprise private network:

1. The VPN client software (residing on the same remote PC as the Integrity client software) connects to the ASA and tells the ASA what type of firewall client it is.
2. After the ASA approves the client firewall type, the ASA passes Integrity server address information back to the Integrity client.
3. With the ASA acting as a proxy, the Integrity client establishes a restricted connection with the Integrity server. A restricted connection is only between the Integrity client and the Integrity server.
4. The Integrity server determines if the Integrity client is in compliance with the mandated security policies. If the Integrity client is in compliance with security policies, the Integrity server instructs the ASA to open the connection and provide the Integrity client with connection details.
5. On the remote PC, the VPN client passes connection details to the Integrity client and signals that policy enforcement should begin immediately and the Integrity client can enter the private network.
6. After the VPN connection is established, the Integrity server continues to monitor the state of the Integrity client using client heartbeat messages.



Note The current release of the ASA supports one Integrity server at a time, even though the user interfaces support the configuration of up to five Integrity servers. If the active Integrity server fails, configure another one on the ASA and then reestablish the VPN client session.

To configure the Integrity server, perform the following steps:

Procedure

Step 1 Configure an Integrity server using the IP address 10.0.0.5.

```
zonelabs-Integrity server-address {hostname1 | ip-address1}
```

Example:

```
hostname(config)# zonelabs-Integrity server-address 10.0.0.5
```

Step 2 Specify port 300 (the default port is 5054).

```
zonelabs-integrity port port-number
```

Example:

```
hostname(config)# zonelabs-integrity port 300
```

Step 3 Specify the inside interface for communications with the Integrity server.

```
zonelabs-integrity interface interface
```

Example:

```
hostname(config)# zonelabs-integrity interface inside
```

Step 4 Ensure that the ASA waits 12 seconds for a response from either the active or standby Integrity servers before declaring the Integrity server as failed and closing the VPN client connections.

Note
If the connection between the ASA and the Integrity server fails, the VPN client connections remain open by default so that the enterprise VPN is not disrupted by the failure of an Integrity server. However, you may want to close the VPN connections if the Zone Labs Integrity server fails.

```
zonelabs-integrity fail-timeout timeout
```

Example:

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

Step 5 Configure the ASA so that connections to VPN clients close when the connection between the ASA and the Zone Labs Integrity server fails.

```
zonelabs-integrity fail-close
```

Example:

```
hostname(config)# zonelabs-integrity fail-close
```

Step 6 Return the configured VPN client connection fail state to the default and ensure that the client connections remain open.

```
zonelabs-integrity fail-open
```

Example:

```
hostname(config)# zonelabs-integrity fail-open
```

Step 7 Specify that the Integrity server connects to port 300 (the default is port 80) on the ASA to request the server SSL certificate.

```
zonelabs-integrity ssl-certificate-port cert-port-number
```

Example:

```
hostname(config)# zonelabs-integrity ssl-certificate-port 300
```

Step 8 While the server SSL certificate is always authenticated, specify that the client SSL certificate of the Integrity server be authenticated.

```
zonelabs-integrity ssl-client-authentication {enable | disable}
```

Example:

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
```

Set the Firewall Client Type to Zone Labs

Procedure

	Command or Action	Purpose
Step 1	To set the firewall client type to the Zone Labs Integrity type, enter the following command: **Example:** `hostname(config)# client-firewall req zonelabs-integrity`	**client-firewall {opt | req} zonelabs-integrity**

What to do next

For more information, see Configure VPN Client Firewall Policies, on page 70. The command arguments that specify firewall policies are not used when the firewall type is **zonelabs-integrity**, because the Integrity server determines these policies.

Set the Client Firewall Parameters

Enter the following commands to set the appropriate client firewall parameters. You can configure only one instance of each command. For more information, see Configure VPN Client Firewall Policies, on page 70.

- Cisco Integrated Firewall

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated
acl-in ACL acl-out ACL
```

- Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

- No Firewall

```
hostname(config-group-policy)# client-firewall none
```

- Custom Firewall

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
 num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

- Zone Labs Firewalls

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

Note When the firewall type is **zonelabs-integrity**, do not include arguments. The Zone Labs Integrity Server determines the policies.

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm
 policy {AYT | CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req}
zonelabs-zonealarmorpro policy {AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in
 ACL acl-out ACL}
```

- Sygate Personal Firewalls

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal

hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro

hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

- Network Ice,Black Ice Firewall

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

Table 2: client-firewall Command Keywords and Variables

Parameter	Description
acl-in ACL	Provides the policy the client uses for inbound traffic.
acl-out ACL	Provides the policy the client uses for outbound traffic.
AYT	Specifies that the client PC firewall application controls the firewall policy. The ASA checks to make sure that the firewall is running. It asks, "Are You There?" If there is no response, the ASA tears down the tunnel.
cisco-integrated	Specifies Cisco Integrated firewall type.
cisco-security-agent	Specifies Cisco Intrusion Prevention Security Agent firewall type.
CPP	Specifies Policy Pushed as source of the VPN client firewall policy.
custom	Specifies Custom firewall type.
description string	Describes the firewall.
networkice-blackice	Specifies Network ICE Black ICE firewall type.
none	Indicates that there is no client firewall policy. Sets a firewall policy with a null value, thereby disallowing a firewall policy. Prevents inheriting a firewall policy from a default or specified group policy.
opt	Indicates an optional firewall type.
product-id	Identifies the firewall product.
req	Indicates a required firewall type.

sygate-personal	Specifies the Sygate Personal firewall type.
sygate-personal-pro	Specifies Sygate Personal Pro firewall type.
sygate-security-agent	Specifies Sygate Security Agent firewall type.
vendor-id	Identifies the firewall vendor.
zonelabs-integrity	Specifies Zone Labs Integrity Server firewall type.
zonelabs-zonealarm	Specifies Zone Labs Zone Alarm firewall type.
zonelabs-zonealarmorpro policy	Specifies Zone Labs Zone Alarm or Pro firewall type.
zonelabs-zonealarmpro policy	Specifies Zone Labs Zone Alarm Pro firewall type.

The following example shows how to set a client firewall policy that requires Cisco Intrusion Prevention Security Agent for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

Configure Client Access Rules

Configure rules that limit the remote access client types and versions that can connect via IPsec through the ASA by using the **client-access-rule** command in group-policy configuration mode. Construct rules according to these guidelines:

- If you do not define any rules, the ASA permits all connection types.
- When a client matches none of the rules, the ASA denies the connection. If you define a deny rule, you must also define at least one permit rule; otherwise, the ASA denies all connections.
- For both software and hardware clients, type and version must exactly match their appearance in the **show vpn-sessiondb remote** display.
- The ***** character is a wildcard, which you can enter multiple times in each rule. For example, **client-access rule 3 deny type * version 3.*** creates a priority 3 client access rule that denies all client types running versions 3.x software.
- You can construct a maximum of 25 rules per group policy.
- There is a limit of 255 characters for an entire set of rules.
- You can enter n/a for clients that do not send client type and/or version.

To delete a rule, enter the **no** form of this command. This command is equivalent to the following command:

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version
4.0
```

To delete all rules, enter the **no client-access-rule command** without arguments. This deletes all configured rules, including a null rule if you created one by issuing the **client-access-rule** command with the **none** keyword.

By default, there are no access rules. When there are no client access rules, users inherit any rules that exist in the default group policy.

To prevent users from inheriting client access rules, enter the **client-access-rule** command with the **none** keyword. The result of this command is that all client types and versions can connect.

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type
type version {version | none}

hostname(config-group-policy)# no client-access rule [priority {permit | deny} type
 type version version]
```

The table below explains the meaning of the keywords and parameters in these commands.

Table 3: client-access rule Command Keywords and Variables

Parameter	Description
deny	Denies connections for devices of a particular type and/or version.
none	Allows no client access rules. Sets client-access-rule to a null value, thereby allowing no restriction. Prevents inheriting a value from a default or specified group policy.
permit	Permits connections for devices of a particular type and/or version.
priority	Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the ASA ignores it.
type *type*	Identifies device types via free-form strings. The string must match exactly its appearance in the **show vpn-sessiondb remote** display, except that you can enter the * character as a wildcard.
version version	Identifies the device version via free-form strings, for example 7.0. A string must match exactly its appearance in the **show vpn-sessiondb remote** display, except that you can enter the * character as a wildcard.

The following example shows how to create client access rules for the group policy named FirstGroup. These rules permit Cisco VPN clients running software version 4.x, while denying all Windows NT clients:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client"
version 4.*
```

Note The “type” field is a free-form string that allows any value, but that value must match the fixed value that the client sends to the ASA at connect time.

Configure User Attributes

This section describes user attributes and how to configure them.

By default, users inherit all user attributes from the assigned group policy. The ASA also lets you assign individual attributes at the user level, overriding values in the group policy that applies to that user. For example, you can specify a group policy giving all users access during business hours, but give a specific user 24-hour access.

View the Username Configuration

To display the configuration for all usernames, including default values inherited from the group policy, enter the **all** keyword with the **show running-config username** command, as follows:

```
hostname# show running-config all username
hostname#
```

This displays the encrypted password and the privilege level, for all users, or, if you supply a username, for that specific user. If you omit the **all** keyword, only explicitly configured values appear in this list. The following example displays the output of this command for the user named testuser:

```
hostname# show running-config all username testuse
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

Configure Attributes for Individual Users

To configure specific users, you assign a password (or no password) and attributes to a user using the **username** command, which enters username mode. Any attributes that you do not specify are inherited from the group policy.

The internal user authentication database consists of the users entered with the **username** command. The **login** command uses this database for authentication. To add a user to the ASA database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username you want to remove. To remove all usernames, use the **clear configure username** command without appending a username.

Set a User Password and Privilege Level

Enter the **username** command to assign a password and a privilege level for a user. You can enter the **nopassword** keyword to specify that this user does not require a password. If you do specify a password, you can specify whether that password is stored in an encrypted form.

The optional **privilege** keyword lets you set a privilege level for this user. Privilege levels range from 0 (the lowest) through 15. System administrators generally have the highest privilege level. The default level is 2.

```
hostname(config)# username name {nopassword | password password [encrypted]}
[privilege priv_level]}

hostname(config)# no username [name]
```

The table below describes the meaning of the keywords and variables used in this command.

username Command Keywords and Variables

Keyword/Variable	Meaning
encrypted	Indicates that the password is encrypted.
name	Provides the name of the user.
nopassword	Indicates that this user needs no password.
password password	Indicates that this user has a password, and provides the password.
privilege priv_level	Sets a privilege level for this user. The range is from 0 to 15, with lower numbers having less ability to use commands and administer the ASA. The default privilege level is 2. The typical privilege level for a system administrator is 15.

By default, VPN users that you add with this command have no attributes or group policy association. You must explicitly configure all values.

The following example shows how to configure a user named anyuser with an encrypted password of pw_12345678 and a privilege level of 12:

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege
 12
hostname(config)#
```

Configure User Attributes

After configuring the user's password (if any) and privilege level, you set the other attributes. These can be in any order. To remove any attribute-value pair, enter the **no** form of the command.

Enter username mode by entering the **username** command with the **attributes** keyword:

```
hostname(config)# username name attributes
hostname(config-username)#
```

The prompt changes to indicate the new mode. You can now configure the attributes.

Configure VPN User Attributes

The VPN user attributes set values specific to VPN connections, as described in the following sections.

Configure Inheritance

You can let users inherit from the group policy the values of attributes that you have not configured at the username level. To specify the name of the group policy from which this user inherits attributes, enter the **vpn-group-policy** command. By default, VPN users have no group-policy association:

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

For an attribute that is available in username mode, you can override the value of an attribute in a group policy for a particular user by configuring it in username mode.

The following example shows how to configure a user named anyuser to use attributes from the group policy named FirstGroup:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

Configure Access Hours

Associate the hours that this user is allowed to access the system by specifying the name of a configured time-range policy:

To remove the attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a time-range value from another group policy. To prevent inheriting a value, enter the **vpn-access-hours none** command. The default is unrestricted access.

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

The following example shows how to associate the user named anyuser with a time-range policy called 824:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

Configure Maximum Simultaneous Logins

Specify the maximum number of simultaneous logins allowed for this user. The range is 0 through 2147483647. The default is 3 simultaneous logins. To remove the attribute from the running configuration, enter the **no** form of this command. Enter 0 to disable login and prevent user access.

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```

Note While the maximum limit for the number of simultaneous logins is very large, allowing several could compromise security and affect performance.

The following example shows how to allow a maximum of 4 simultaneous logins for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

Configure the Idle Timeout

Procedure

Step 1 (Optional) To configure a VPN idle timeout period use the **vpn-idle-timeout** *minutes* command in group-policy configuration mode or in username configuration mode.

If there is no communication activity on the connection in this period, the ASA terminates the connection. The minimum time is 1 minute, the maximum time is 35791394 minutes, and the default is 30 minutes.

The following example shows how to set a VPN idle timeout of 15 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

Other actions using the [**no**] **vpn-idle-timeout** {*minutes* | **none**} command:

- Enter **vpn-idle-timeout none** to disable VPN idle timeout and pevent inheriting a timeout value.

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  This results in AnyConnect Client (both SSL and IPsec/IKEv2) and Clientless VPN using the global webvpn **default-idle-timeout** *seconds* value. This command is entered in webvpn-config mode, for example: `hostnamee(config-webvpn)# default-idle-timeout 300`. The default is 1800 seconds (30 min), the range is 60-86400 seconds.

  For all webvon connections , the **default-idle-timeout** value is enforced only if **vpn-idle-timeout none** is set in the group policy/username attribute. A non-zero idle timeout value is required by ASA for all AnyConnect Client connections.

  For Site-to-Site (IKEv1, IKEv2) and IKEv1 remote-access VPNs, we recommend you Disable timeout and allow for an unlimited idle period.

- To disable the idle timeout for this group policy or user policy, enter **no vpn-idle-timeout**. The value will be inherited.
- If you do not set **vpn-idle-timeout** at all, in anyway, the value is inherited, which defaults to 30 minutes.

Note

vpn-idle-timeout controls only the maximum time for a parent session. Child sessions (SSL/DTLS) are aggressively terminated much sooner by a hardcoded 5-minute TCP inactivity timeout or on failing the 3×Dead Peer Detection (DPD) check. For more details, see the note in Configure Dead Peer Detection. For further details on DPD, keepalives, and timeout attributes, see Answer AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer.

Step 2 (Optional) You can optionally configure the time at which an idle timeout alert message is displayed to the user using the **vpn-idle-timeout alert-interval** {*minutes*} command.

This alert message tells users how many minutes they have left until their VPN session is disconnected due to inactivity. The default alert interval is one minute.

The following example shows how to set a VPN idle timeout alert interval of 3 minutes for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

Other actions using the [**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} command:

- The **none** parameter indicates that users will not receive an alert.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- To remove the alert interval for this group or user policy enter **no vpn-idle-timeout alert-interval**. The value will be inherited.
- If you do not set this parameter at all, the default alert interval is one minute.

Configure the Maximum Connect Time

Procedure

Step 1 (Optional) Configure a maximum amount of time for VPN connections, using the **vpn-session-timeout** {*minutes* command in group-policy configuration mode or in username configuration mode.

The minimum time is 1 minute, and the maximum time is 35791394 minutes. There is no default value. At the end of this period of time, the ASA terminates the connection.

The following example shows how to set a VPN session timeout of 180 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

The following example shows how to set a VPN session timeout of 180 minutes for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
```

```
hostname(config-username)#
```

Other actions using the [**no**] **vpn-session-timeout** {*minutes* | **none**} command:

- To remove the attribute from this policy and allow inheritance, enter the **no vpn-session-timeout** form of this command.
- To allow an unlimited timeout period, and thus prevent inheriting a timeout value, enter **vpn-session-timeout none**.

Step 2 Configure the time at which a session timeout alert message is displayed to the user using the **vpn-session-timeout alert-interval** {*minutes* | } command.

This alert message tells users how many minutes left until their VPN session is automatically disconnected. The following example shows how to specify that users will be notified 20 minutes before their VPN session is disconnected. You can specify a range of 1-30 minutes.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

Other actions using the [**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} command:

- Use the no form of the command to indicate that the VPN session timeout alert-interval attribute will be inherited from the Default Group Policy:

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- The **vpn-session-timeout alert-interval none** indicates that users will not receive an alert.

Apply an ACL Filter

Specify the name of a previously-configured, user-specific ACL to use as a filter for VPN connections. To disallow an ACL and prevent inheriting an ACL from the group policy, enter the **vpn-filter** command with the none keyword. To remove the ACL, including a null value created by issuing the **vpn-filter none** command, enter the **no** form of this command. The **no** option allows inheritance of a value from the group policy. There are no default behaviors or values for this command.

You configure ACLs to permit or deny various types of traffic for this user. Note that the VPN filter applies to initial connections only. It does not apply to secondary connections, such as a SIP media connection, that are opened due to the action of application inspection. You then use the **vpn-filter** command to apply those ACLs.

```
hostname(config-username)# vpn-filter {value ACL_name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```

Note Clientless SSL VPN does not use ACLs defined in the **vpn-filter** command.

The following example shows how to set a filter that invokes an ACL named acl_vpn for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

Specify the IPv4 Address and Netmask

Specify the IP address and netmask to assign to a particular user. To remove the IP address, enter the **no** form of this command.

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

The following example shows how to set an IP address of 10.92.166.7 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

Specify the network mask to use with the IP address specified in the previous step. If you used the **no vpn-framed-ip-address** command, do not specify a network mask. To remove the subnet mask, enter the **no** form of this command. There is no default behavior or value.

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

The following example shows how to set a subnet mask of 255.255.255. 254 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

Specify the IPv6 Address and Netmask

Specify the IPv6 address and netmask to assign to a particular user. To remove the IP address, enter the **no** form of this command.

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

The following example shows how to set an IP address and netmask of 2001::3000:1000:2000:1/64 for a user named anyuser. This address indicates a prefix value of 2001:0000:0000:0000 and an interface ID of 3000:1000:2000:1.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

Specify the Tunnel Protocol

Specify the VPN tunnel types (IPsec or clientless SSL VPN) that this user can use. The default is taken from the default group policy, the default for which is IPsec. To remove the attribute from the running configuration, enter the **no** form of this command.

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

The parameter values for this command are as follows:

- **IPsec—**Negotiates an IPsec tunnel between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
- **webvpn—**Provides clientless SSL VPN access to remote users via an HTTPS-enabled web browser, and does not require a client

Enter this command to configure one or more tunneling modes. You must configure at least one tunneling mode for users to connect over a VPN tunnel.

The following example shows how to configure clientless SSL VPN and IPsec tunneling modes for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

Restrict Remote User Access

Configure the **group-lock** attribute with the **value** keyword to restrict remote users to access only through the specified, preexisting connection profile. Group-lock restricts users by checking whether the group configured in the VPN client is the same as the connection profile to which the user is assigned. If it is not, the ASA prevents the user from connecting. If you do not configure group-lock, the ASA authenticates users without regard to the assigned group.

To remove the **group-lock** attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value from the group policy. To disable group-lock, and to prevent inheriting a group-lock value from a default or specified group policy, enter the **group-lock** command with the **none** keyword.

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

The following example shows how to set group lock for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

Enable Password Storage for Software Client Users

Specify whether to let users store their login passwords on the client system. Password storage is disabled by default. Enable password storage only on systems that you know to be in secure sites. To disable password storage, enter the **password-storage** command with the **disable** keyword. To remove the password-storage attribute from the running configuration, enter the **no** form of this command. This enables inheritance of a value for password-storage from the group policy.

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

This command has no bearing on interactive hardware client authentication or individual user authentication for hardware clients.

The following example shows how to enable password storage for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```

Best Practices for Configuring and Adjusting VPN Filter ACL

This section provides best practices to follow while updating an existing VPN filter ACL without interrupting the traffic.

Update an Existing VPN Filter ACL

Follow these steps when you want to update a vpn-filter ACL applied on the ASA device:

1. Create a new vpn-filter ACL on your system (Example: *new_acl.txt*).
2. Download the current vpn-filter ACL from the device (Example: *old_acl.txt*).
3. Create modify instructions for the ACL:

```
* Add update in-progress to ACL remark
echo ?access-list <name> line 1 ACL update in-progress? > push.txt
* Delete old rules
sed ?s/^/no /g? old.acl >> push.txt
 * Add new rules
cat new.acl >> push.txt
 * Remove update in-progress to ACL remark
echo ?no access-list <name> ACL update in-progress? >> push.txt
```

4. Upload push.txt to the device.

Replace an existing VPN Filter ACL with a new one

Follow these steps to replace a vpn-filter ACL that is applied on the ASA device:

1. Creating a new vpn-filter ACL each time you want to replace an existing one.

2. Update the group-policy with the vpn-filter ACL.
3. Delete the old vpn-filter ACL applied on the device.