

v

- validate-attribute, on page 3
- validate-kdc, on page 5
- validate-key, on page 7
- validation-policy, on page 9
- validation-usage, on page 11
- vdi, on page 13
- verify, on page 15
- verify-header, on page 19
- version, on page 21
- virtual http, on page 23
- virtual telnet, on page 25
- vlan (group-policy), on page 27
- vlan (interface), on page 29
- vpdn group, on page 32
- vpdn username, on page 35
- vpn-access-hours, on page 37
- vpn-addr-assign, on page 39
- vpn-mode, on page 41
- vpnclient connect, on page 43
- vpnclient enable, on page 44
- vpnclient ipsec-over-tcp, on page 45
- vpnclient mac-exempt, on page 47
- vpnclient management, on page 49
- vpnclient mode, on page 51
- vpnclient nem-st-autoconnect, on page 53
- vpnclient server, on page 55
- vpnclient server-certificate, on page 57
- vpnclient trustpoint, on page 59
- vpnclient username, on page 61
- vpnclient vpngroup, on page 62
- vpn-filter, on page 64
- vpn-framed-ip-address, on page 66
- vpn-framed-ipv6-address, on page 67

- vpn-group-policy, on page 68
- vpn-idle-timeout, on page 70
- vpn load-balancing, on page 72
- vpn-sessiondb, on page 75
- vpn-sessiondb logoff, on page 77
- vpn-session-timeout, on page 80
- vpnsetup, on page 82
- vpn-simultaneous-logins, on page 84
- vpn-tunnel-protocol, on page 86
- vtep-nve, on page 88
- vxlan port, on page 90

validate-attribute

To validate RADIUS attributes when using RADIUS accounting, use the **validate-attribute** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

validate-attribute [*attribute_number*]
no validate-attribute [*attribute_number*]

Syntax Description

attribute_number	The RADIUS attribute to be validated with RADIUS accounting. Values range from 1-191. Vendor Specific Attributes are not supported.

Command Default

This option is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Radius-accounting parameter configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

When this command is configured, the security appliance will also do a match on these attributes in addition to the Framed IP attribute. Multiple instances of this command are allowed.

You can find a list of RADIUS attribute types here:

http://www.iana.org/assignments/radius-types

Examples

The following example shows how to enable RADIUS accounting for the user name RADIUS attribute:

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# validate-attribute 1
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

validate-kdc

To enable the authentication of the Kerberos Key Distribution Center (KDC) using an uploaded keytab file, use the **validate-kdc** command in aaa-server group mode. To disable KDC authentication, use the **no** form of this command.

validate-kdc
no validate-kdc

Command Default

This option is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server group	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.8(4)	This command was added.

Usage Guidelines

You can configure a Kerberos AAA server group to authenticate the servers in the group using the **validate-kdc** command. To accomplish the authentication, you must also import a keytab file that you exported from the Kerberos Key Distribution Center (KDC). By validating the KDC, you can prevent an attack where the attacker spoofs the KDC so that user credentials are authenticated against the attacker's Kerberos server.

When you enable KDC validation, after obtaining the ticket-granting ticket (TGT) and validating the user, the system also requests a service ticket on behalf of the user for **host**/*ASA_hostname*. The system then validates the returned service ticket against the secret key for the KDC, which is stored in a keytab file that you generated from the KDC and then uploaded to the ASA. If KDC authentication fails, the server is considered untrusted and the user is not authenticated.

To accomplish KDC authentication, you must do the following:

1. (On the KDC.) Create a user account in the Microsoft Active Directory for the ASA (go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**). For example, if the fully-qualified domain name (FQDN) of the ASA is asahost.example.com, create a user named asahost.
2. (On the KDC.) Create a host service principal name (SPN) for the ASA using the FQDN and user account:

```
C:> setspn -A HOST/asahost.example.com asahost
```

1. (On the KDC.) Create a keytab file for the ASA (line feeds added for clarity):

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
```

```
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

1. (On the ASA.) Import the keytab (in this example, new.keytab) to the ASA using the **aaa kerberos import-keytab** command.
2. (On the ASA.) Add the **validate-kdc** command to the Kerberos AAA server group configuration. The keytab file is used only by server groups that contain this command.



Note You cannot use KDC validation in conjunction with Kerberos Constrained Delegation (KCD). The **validate-kdc** command will be ignored if the server group is used for KCD.

Examples

The following example shows how to import a keytab named new.keytab that resides on an FTP server, and enable KDC validation in a Kerberos AAA server group.

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab

ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos

ciscoasa(config-aaa-server-group)# validate-kdc
```

Related Commands

Commands	Description
aaa kerberos import-keytab	Imports a Kerberos keytab file that was exported from a Kerberos Key Distribution Center (KDC)
clear aaa kerberos keytab	Clears the imported Kerberos keytab file.
show aaa kerberos keytab	Shows information about the Kerberos keytab file.

validate-key

To specify the pre-shared key for LISP messages, use the **validate-key** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect lisp** command. To remove the key, use the **no** form of this command.

validate-key *key*
no validate-key *key*

Syntax Description

key	Specify the pre-shared key for LISP messages.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Specify the LISP pre-shared key so the ASA can read LISP message contents.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.

3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.
4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following example limits EIDs to those on the 10.10.10.0/24 network and specifies the pre-shared key:

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

validation-policy

To specify the conditions under which a trustpoint can be used to validate the certificates associated with an incoming user connection, use the **validation-policy command** in crypto ca trustpoint configuration mode. To specify that the trustpoint cannot be used for the named condition, use the **no** form of the command.

[**no**] **validation-policy** { **ssl-client | ipsec-client** } [**no-chain**] [**subordinate-only**]

Syntax Description

ipsec-client	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate IPsec connections.
no-chain	Disables the chaining of subordinate certificates that are not resident on the security device.
ssl-client	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate SSL connections.
subordinate-only	Disables validation of client certificates issued directly from the CA represented by this trustpoint.

Command Default

No default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Remote-access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPsec), or both, depending on deployment requirements, to permit access to virtually any network application or resource. The **validation-policy** command allows you to specify the protocol type permitted to access on-board CA certificates.

The **no-chain** option with this command prevents an ASA from supporting subordinate CA certificates that are not configured as trustpoints on it.

The ASA can have two trustpoints with the same CA resulting in two different identity certificates from the same CA. This option is disabled automatically if the trustpoint is authenticated to a CA that is already associated with another trustpoint that has enabled this feature. This prevents ambiguity in the choice of path-validation parameters. If the user attempts to activate this feature on a trustpoint that has been authenticated

to a CA already associated with another trustpoint that has enabled this feature, the action is not permitted. No two trustpoints can have this setting enabled and be authenticated to the same CA.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint, central, and designates it an SSL trustpoint:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# validation-policy ssl
ciscoasa(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for trustpoint, checkin1,and sets it to accept certificates that are subordinate to the specified trustpoint.

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# validation-policy subordinates-only
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
id-usage	Specifies how the enrolled identity of a trustpoint can be used
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

validation-usage

To specify the usage types for which validation with this trustpoint is allowed, use the **validation-usage** command in crypto ca trustpoint configuration mode. To not specify the usage types, use the **no** form of the command.

validation-usage { **ipsec-client** | **ssl-client** | **ssl-server** | **ssh-client** }
no validation-usage [**ipsec-client** | **ssl-client** | **ssl-server** | **ssh-client**]

Syntax Description

ipsec-client	Indicates that IPsec client connections can be validated using this trustpoint.
ssl-client	Indicates that SSL client connections can be validated using this trustpoint.
ssl-server	Indicates that SSL server certificates can be validated using this trustpoint.
ssh-client	SSH client connections can be validated using this trustpoint.

Command Default

ipsec-client, ssl-client

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added to replace the client-types command.
9.20(4)/9.24(1)	Added **ssh-client** for authentication for SSH clients.

Usage Guidelines

When there are multiple trustpoints associated with the same CA certificate, only one of the trustpoints can be configured for a specific client type. However, one of the trustpoints can be configured for one client type and the other trustpoint with another client type.

If there is a trustpoint associated with the same CA certificate that is already configured with a client type, the new trustpoint is not allowed to be configured with the same client-type setting. The **no** form of the command clears the setting so that a trustpoint cannot be used for any client validation.

Remote access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPsec), or both, depending on deployment requirements, to permit access to any network application or resource.

Related Commands

Command	Description
crypto ca trustpoint	Enters the crypto ca trustpoint configuration mode for the specified trustpoint.

vdi

To provide secure remote access for Citrix Receiver applications running on mobile devices to XenApp and XenDesktop VDI servers through the ASA, use the **vdi** command.

vdi type citrix url *url* **domain** *domain* **username** *username* **password** *password*

Syntax Description

domain *domain*	Domain for logging into the virtualization infrastructure server. This value can be a clientless macro.
password *password*	Password for logging into the virtualization infrastructure server. This value can be a clientless macro.
type	Type of VDI. For a Citrix Receiver type, this value must be *citrix* .
url *url*	Full URL of the XenApp or XenDesktop server including http or https, hostname, and port number, as well as the path to the XML service.
username *username*	Username for logging into the virtualization infrastructure server. This value can be a clientless macro.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

In a VDI model, administrators publish desktops pre-loaded with enterprise applications, and end users remotely access these desktops. These virtualized resources appear just as any other resources, such as email, so that users do not need to go through a Citrix Access Gateway to access them. Users log onto the ASA using Citrix Receiver mobile client, and the ASA connects to a pre-defined Citrix XenApp or XenDesktop Server. The administrator must configure the Citrix server's address and logon credentials under Group Policy so that when users connect to their Citrix Virtualized resource, they enter the ASA's SSL VPN IP address and credentials instead of pointing to the Citrix Server's address and credentials. When the ASA has verified the credentials, the receiver client starts to retrieve entitled applications through the ASA.

Supported Mobile Devices

- iPad—Citrix Receiver version 4.x or later
- iPhone/iTouch—Citrix Receiver version 4.x or later

- Android 2.x phone—Citrix Receiver version 2.x or later
- Android 3.x tablet—Citrix Receiver version 2.x or later
- Android 4.0 phone—Citrix Receiver version 2.x or later

Examples

If both username and group policy are configured, username settings take precedence over group policy.

```
configure terminal
 group-policy DfltGrpPolicy attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password   <password>
configure terminal
 username <username> attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password   <password>]
```

Related Commands

Command	Description
debug webvpn citrix	Provides insight into the process of launching Citrix-based applications and desktops.

verify

To verify the checksum of a file, use the **verify** command in privileged EXEC mode.

verify*path*
verify { **/md5 | sha-512** } *path* [*expected_value*]
verify /signature running

Syntax Description

/md5	Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
/sha-512	Calculates and displays the SHA-512 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
/signature running	Verifies the signature of the running ASA image.
expected_value	(Optional) The known hashed value for the specified image. The ASA displays a message verifying that the hashed values match or that there is a mismatch.

path	• **disk0:**/[*path*/]*filename* Indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* Indicates the external Flash memory card. • **flash:**/[*path*/]*filename* This option indicates the internal Flash card. **flash** is an alias for **disk0:**. • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] The **type** can be one of the following keywords: • **ap**—ASCII passive mode • **an**—ASCII normal mode • **ip**—(Default) Binary passive mode • **in**—Binary normal mode • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **verify** command. • **system:running-config** Calculates or verifies the hash for the running configuration. • **system:text** Calculates or verifies the hash for the text of the ASA process.

Command Default

The current flash device is the default file system.

Note When you specify the **/md5** or **/sha-512** option, you can use a network file, such as from FTP, HTTP or TFTP, as the source. The **verify** command without the **/md5** or **/sha-512** option only lets you verify local images in flash.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.3(2)	The **signature** keyword was added.
9.6(2)	The **system:text** option was added.

Usage Guidelines

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into flash memory; it is not displayed when the image file is copied from one disk to another.

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into flash memory or onto a server. A variety of image information is available on Cisco.com.

To display the contents of flash memory, use the **show flash** command. The flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into flash memory, use the **verify** command. Note, however, that the **verify** command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the ASA and saved in the file system without detection. If a corrupt image is transferred successfully to the ASA, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of the ASA software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all security appliance software images for comparison against local system image values. You can also specify SHA-512 (**/sha-512**).

To perform the MD5 or SHA-512 integrity check, issue the **verify** command using the **/md5** or **/sha-512** keyword. For example, issuing the **verify /md5 flash:cdisk.bin** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Examples

The following example shows the **verify** command used on an image file called cdisk.bin. Some of the text was removed for clarity:

```
ciscoasa# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
ciscoasa#
```

The following example shows the **verify** command used on a signature image in disk0:

```
ciscoasa(config)# verify lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Digital signature successfully validate
ciscoasa(config)# verify /signature lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6
Digital signature successfully validated
ciscoasa(config)# verify /signature cdisk.smp
Verifying file integrity of disk0:/cdisk.smp
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc6cc420aadfff8db42fae6088bc74959fdbc11f
Computed Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc6cc420aadfff8db42fae6088bc74959fdbc11f
CCO Hash      SHA-512:
cd5d459b6d2616e3530d9ed7c488b5a1b51269f19ad853fbf9c630997e716ded4fda61fa2afe6e293dc82f05997fd787b0ec22839c92a87a37811726e152fade
Signature Verified
ciscoasa(config)#
ciscoasa(config)# verify /signature corrupt.SSA
%ERROR: Signature algorithm not supported for file disk0:/corrupt.SSA.
ciscoasa(config)#
```

Related Commands

Command	Description
copy	Copies files.
dir	Lists the files in the system.

verify-header

To allow only known IPv6 extension headers and enforces the order of IPv6 extension headers, use the **verify-header** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect ipv6** command. To disable these parameters, use the **no** form of this command.

verify-header { **order | type** }
no verify-header { **order | type** }

Syntax Description

order	Enforces the order of IPv6 extension headers as defined in the RFC 2460 specification.
type	Allows only known IPv6 extension headers.

Command Default

Both order and type are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

These parameters are enabled by default. To disable them, enter the no keyword.

Examples

The following example disables the order and type parameters for an IPv6 inspection policy map:

```
ciscoasa(config)# policy-map type inspect ipv6 ipv6-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# no verify-header order
ciscoasa(config-pmap-p)# no verify-header type
```

Related Commands

Command	Description
inspect ipv6	Enables IPv6 inspection.
parameters	Enters parameters configuration mode for an inspection policy map.

Command	Description
policy-map type inspect ipv6	Creates an IPv6 inspection policy map.

version

To specify the version of RIP used globally by the ASA, use the **version** command in router configuration mode. To restore the defaults, use the **no** form of this command.

version { **1** | **2** }
no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Command Default

The ASA accepts Version 1 and Version 2 packets but sends only Version 1 packets.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip send version** and **rip receive version** commands on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the ASA to send and receive RIP Version 2 packets on all interfaces:

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.

Command	Description
router rip	Enables the RIP routing process and enter router configuration mode for that process.

virtual http

To configure a virtual HTTP server, use the **virtual http** command in global configuration mode. To disable the virtual server, use the **no** form of this command.

virtual http *ip_address* [**warning**]
no virtual http *ip_address* [**warning**]

Syntax Description

ip_address	Sets the IP address for the virtual HTTP server on the ASA. Make sure this address is an unused address that is routed to the ASA.
warning	(Optional) Notifies users that the HTTP connection needs to be redirected to the ASA. This keyword applies only for text-based browsers, where the redirect cannot happen automatically.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was deprecated because the inline basic HTTP authentication method used in prior releases was replaced by the redirection method; this command was no longer needed.
7.2(2)	This command was revived because you can now choose between using basic HTTP authentication (the default) or using HTTP redirection using the **aaa authentication listener** command. The redirection method does not require an extra command for cascading HTTP authentications.

Usage Guidelines

When you use HTTP authentication on the ASA (see the **aaa authentication match** or the **aaa authentication include** command), the ASA uses basic HTTP authentication by default. You can change the authentication method so that the ASA redirects HTTP connections to web pages generated by the ASA itself using the **aaa authentication listener** command with the **redirect** keyword.

However, if you continue to use basic HTTP authentication, then you might need the **virtual http** command when you have cascading HTTP authentications.

If the destination HTTP server requires authentication in addition to the ASA, then the **virtual http** command lets you authenticate separately with the ASA (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the ASA is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This command redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the ASA. The ASA prompts for the AAA server username and password. After the AAA server authenticates the user, the ASA redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.

For inbound users (from lower security to higher security), you must also include the virtual HTTP address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual HTTP IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual HTTP address. A **static** statement is not required.



Note Do not set the **timeout uauth** command duration to 0 seconds when using the **virtual http** command, because this setting prevents HTTP connections to the real web server.

Examples

The following example shows how to enable virtual HTTP along with AAA authentication:

```
ciscoasa(config)# virtual http 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list ACL-IN remark This is the HTTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list ACL-IN remark This is the virtual HTTP address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list AUTH remark This is the HTTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list AUTH remark This is the virtual HTTP address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
aaa authentication listener http	Sets the method by which the ASA authentica
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the ASA virtual server.
sysopt uauth allow-http-cache	When you enable the **virtual http** command, this command lets you use the username and password in the browser cache to reconnect to the virtual server.
virtual telnet	Provides a virtual Telnet server on the ASA to let users authenticate with the ASA before initiating other types of connections that require authentication.

virtual telnet

To configure a virtual Telnet server on the ASA, use the **virtual telnet** command in global configuration mode. You might need to authenticate users with the virtual Telnet server if you require authentication for other types of traffic for which the ASA does not supply an authentication prompt. To disable the server, use the **no** form of this command.

virtual telnet *ip_address*
no virtual telnet *ip_address*

Syntax Description

ip_address	Sets the IP address for the virtual Telnet server on the ASA. Make sure this address is an unused address that is routed to the ASA.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the ASA, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the ASA, and the ASA provides a Telnet prompt.

You must configure authentication for Telnet access to the virtual Telnet address as well as the other services you want to authenticate using the **authentication match** or **aaa authentication include** command.

When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message "Authentication Successful." Then, the user can successfully access other services that require authentication.

For inbound users (from lower security to higher security), you must also include the virtual Telnet address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual Telnet IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual Telnet address. A **static** statement is not required.

To logout from the ASA, reconnect to the virtual Telnet IP address; you are prompted to log out.

Examples

This example shows how to enable virtual Telnet along with AAA authentication for other services:

```
ciscoasa(config)# virtual telnet 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list ACL-IN remark This is the SMTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq telnet
ciscoasa(config)# access-list ACL-IN remark This is the virtual Telnet address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list AUTH remark This is the SMTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
ciscoasa(config)# access-list AUTH remark This is the virtual Telnet address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the ASA virtual server.
virtual http	When you use HTTP authentication on the ASA, and the HTTP server also requires authentication, this command allows you to authenticate separately with the ASA and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the ASA is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.

vlan (group-policy)

To assign a VLAN to a group policy, use the **vlan** command in group-policy configuration mode. To remove the VLAN from the configuration of the group policy and replace it with the VLAN setting of the default group policy, use the **no** form of this command.

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

Syntax Description

none	Disables the assignment of a VLAN to the remote access VPN sessions that match this group policy. The group policy does not inherit the vlan value from the default group policy.
vlan_id	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, using the **vlan** command in interface configuration mode.

Command Default

The default value is none.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

This command specifies the egress VLAN interface for sessions assigned to this group policy. The ASA forwards all traffic on this group to that VLAN. You can assign a VLAN to each group policy to simplify access control. Applying the VLAN interface configuration disrupts the client-to-client communication. All packets, including packets destined to a second client, are forced to the vlan interface. You must have a device downstream to route packets back to the firewall to maintain client-to-client communication.

Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with vlan mapping option. These inspection engines ignore the vlan-mapping setting which could result in packets being incorrectly routed.

Examples

The following command assigns the VLAN 1 to the group policy:

```
ciscoasa(config-group-policy)# vlan 1
ciscoasa(config-group-policy)
```

The following command removes VLAN mapping from the group policy:

```
ciscoasa(config-group-policy)# vlan none
ciscoasa(config-group-policy)
```

Related Commands

Command	Description
show vlan	Shows the VLANs configured on the ASA.
vlan (Interface configuration mode)	Assigns a VLAN ID to a subinterface.
show vpn-session_summary.db	Displays the number IPsec, Cisco AnyConnect, and NAC sessions, and the number of VLANs in use.
show vpn-sessiondb	Displays information about VPN sessions, including VLAN mapping and NAC results.

vlan (interface)

To assign a VLAN ID to a subinterface, use the **vlan** command in interface configuration mode. To remove a VLAN ID, use the **no** form of this command. Subinterfaces require a VLAN ID to pass traffic. VLAN subinterfaces let you configure multiple logical interfaces on a single physical interface. VLANs let you keep traffic separate on a given physical interface, for example, for multiple security contexts.

vlan *id* [**secondary** *vlan_range*]
no vlan [**secondary** *vlan_range*]

Syntax Description

id	Specifies an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.
secondary *vlan_range*	(Optional) Specifies one or more secondary VLANs. The *vlan_id* is an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. The secondary VLANs can be separated by spaces, commas, and dashes (for a contiguous range). When the ASA receives traffic on the secondary VLANs, it maps the traffic to the primary VLAN.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.
9.5(2)	We added the **secondary** keyword.

Usage Guidelines

You can configure a primary VLAN, as well as one or more secondary VLANs. When the ASA receives traffic on the secondary VLANs, it maps it to the primary VLAN. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the ASA changes the old ID. To remove some secondary VLANs from the list, you can use the **no** command and only list the VLANs to remove. You can only selectively remove listed VLANs; you cannot remove a single VLAN in a range, for example.

You need to enable the physical interface with the **no shutdown** command to let subinterfaces be enabled. If you enable subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Therefore, you cannot prevent traffic from passing through the physical interface by bringing down the interface. Instead, ensure that the physical interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical interface pass untagged packets, you can configure the **nameif** command as usual.

The maximum number of subinterfaces varies depending on your platform. See the CLI configuration guide for the maximum subinterfaces per platform.

Examples

The following example assigns VLAN 101 to a subinterface:

```
ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

The following example changes the VLAN to 102:

```
ciscoasa(config)# show running-config interface
gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-interface)# vlan 102
ciscoasa(config)# show running-config interface
gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

The following example maps a set of secondary VLANs to VLAN 200:

```
interface gigabitethernet 0/6.200
vlan 200 secondary 500 503 600-700
```

The following example removes secondary VLAN 503 from the list:

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
vlan 200 secondary 500 600-700
no nameif
no security-level
no ip address
```

The following example shows how VLAN mapping works with the Catalyst 6500. Consult the Catalyst 6500 configuration guide on how to connect nodes to PVLANS.

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the current configuration of the interface.

vpdn group

To create or edit a vpdn group and configure PPPoE client settings, use the **vpdn group** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

vpdn group *group_name* { **localname** *username* | **request dialout pppoe | ppp authentication** { **chap | mschap | pap** } }
no vpdn group *group_name* { **localname** *name* | **request dialout pppoe | ppp authentication** { **chap | mschap | pap** } }

Note PPPoE is not supported when failover is configured on the ASA, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

localname *username*	Links the user name to the vpdn group for authentication, and must match the name configured with the **vpdn username** command.
ppp authentication{chap | mschap | pap}}	Specifies the Point-to-Point Protocol (PPP) authentication protocol. The Windows client dial-up networking settings lets you specify what authentication protocol to use (PAP, CHAP, or MS-CHAP). Whatever you specify on the client must match the setting you use on the security appliance. Password Authentication Protocol (PAP) lets PPP peers authenticate each other. PAP passes the host name or username in clear text. Challenge Handshake Authentication Protocol (CHAP) lets PPP peers prevent unauthorized access through interaction with an access server. MS-CHAP is a Microsoft derivation of CHAP. PIX Firewall supports MS-CHAP Version 1 only (not Version 2.0). If an authentication protocol is not specified on the host, do not specify the ppp authentication option in your configuration.
request dialout pppoe	Specifies to allow dial out PPPoE requests.
vpdn group *group_name*	Specifies a name for the vpdn group

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Virtual Private Dial-up Networking (VPDN) is used to provide long distance, point-to-point connections between remote dial-in users and a private network. VDPN on the security appliance uses the Layer 2 tunneling technology PPPoE to establish dial-up networking connections from the remote user to the private network across a public network.

PPPoE is the Point-to-Point Protocol (PPP) over Ethernet. PPP is designed to work with network layer protocols such as IP, IPX, and ARA. PPP also has CHAP and PAP as built-in security mechanisms.

The **show vpdn session pppoe** command displays session information for PPPOE connections. The **clear configure vpdn group** command removes all **vpdn group** commands from the configuration and stops all the active L2TP and PPPoE tunnels. The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Because PPPoE encapsulates PPP, PPPoE relies on PPP to perform authentication and ECP and CCP functions for client sessions operating within the VPN tunnel. Additionally, PPPoE is not supported in conjunction with DHCP because PPP assigns the IP address for PPPoE.



Note Unless the VPDN group for PPPoE is configured, PPPoE cannot establish a connection.

To define a VPDN group to be used for PPPoE, use the **vpdn group** *group_name* **request dialout pppoe** command. Then use the **pppoe client vpdn group** command from interface configuration mode to associate a VPDN group with a PPPoE client on a particular interface.

If your ISP requires authentication, use the **vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} command to select the authentication protocol used by your ISP.

Use the **vpdn group** *group_name* **localname** *username* command to associate the username assigned by your ISP with the VPDN group.

Use the **vpdn username** *username* password *password* command to create a username and password pair for the PPPoE connection. The username must be a username that is already associated with the VPDN group specified for PPPoE.



Note If your ISP is using CHAP or MS-CHAP, the username may be called the remote system name and the password may be called the CHAP secret.

The PPPoE client functionality is turned off by default, so after VPDN configuration, enable PPPoE with the **ip address** *if_name* **pppoe** [**setroute**] command. The setroute option causes a default route to be created if no default route exists.

As soon as PPPoE is configured, the security appliance attempts to find a PPPoE access concentrator with which to communicate. When a PPPoE connection is terminated, either normally or abnormally, the ASA attempts to find a new access concentrator with which to communicate.

The following **ip address** commands should not be used after a PPPoE session is initiated because they will terminate the PPPoE session:

- **ip address outside pppoe**, because it attempts to initiate a new PPPoE session.
- **ip address outside dhcp**, because it disables the interface until the interface gets its DHCP configuration.
- **ip address outside** *address netmask*, because it brings up the interface as a normally initialized interface.

Examples

The following example creates a vdpn group *telecommuters* and configures the PPPoE client:

```
ciscoasa(config)# vpdn group telecommuters request dialout pppoe
ciscoasa(config)# vpdn group telecommuters localname user1
ciscoasa(config)# vpdn group telecommuters ppp authentication pap
ciscoasa(config)# vpdn username user1 password test1
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-subif)# ip address pppoe setroute
```

Related Commands

Command	Description
clear configure vpdn group	Removes all vpdn group commands from the configurations.
clear configure vpdn username	Removes all vpdn username commands from the configuration.
show vpdn group *group_name*	Displays the vpdn group configuration.
vpdn username	Creates a username and password pair for the PPPoE connection.

vpdn username

To create a username and password pair for PPPoE connections, use the **vpdn username** command in global configuration mode.

vpdn username *username* **password** *password* [**store-local**]
no vpdn username *username* **password** *password* [**store-local**]

Note PPPoE is not supported when failover is configured on the ASA, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

password	Specifies the password.
store-local	Stores the username and password in a special location of NVRAM on the security appliance. If an Auto Update Server sends a clear config command to the security appliance and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.
username	Specifies the username.

Command Default

No default behavior or values. See Usage Guidelines.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The vpdn username must be a username that is already associated with the VPDN group specified with the **vpdn group** *group_name* **localname** *username* command.

The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Examples

The following example creates the vpdn username *bob_smith* with the password *telecommuter* 9/8:

```
ciscoasa(config)# vpdn username bob_smith password telecommuter9/8
```

Related Commands

Command	Description
clear configure vpdn group	Removes all **vpdn group** commands from the configurations.
clear configure vpdn username	Removes all **vpdn username** commands from the configuration.
show vpdn group	Displays the VPDN group configuration.
vpdn group	Create a VPDN group and configures PPPoE client settings,

vpn-access-hours

To associate a group policy with a configured time-range policy, use the **vpn-access-hours** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-range value from another group policy. To prevent inheriting a value, use the **vpn-access-hours none** command.

vpn-access hours value { *time-range* } **| none**
no vpn-access hours

Syntax Description

none	Sets VPN access hours to a null value, thereby allowing no time-range policy. Prevents inheriting a value from a default or specified group policy.
time-range	Specifies the name of a configured time-range policy.

Command Default

Unrestricted.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to associate the group policy named FirstGroup with a time-range policy called 824:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-access-hours 824
```

Related Commands

Command	Description
time-range	Sets days of the week and hours of the day for access to the network, including start and end dates.

vpn-addr-assign

To specify a method for assigning IPv4 addresses to remote access clients, use the **vpn-addr-assign** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all configured VPN address assignment methods from the ASA, user the **no** version of this command. without arguments.

vpn-addr-assign { **aaa | dhcp | local** [**reuse-delay** *delay*] }
no vpn-addr-assign { **aaa | dhcp | local** [**reuse-delay** *delay*] }

Syntax Description

aaa	Assigns IPv4 addresses from an external or internal (LOCAL) AAA authentication server.
dhcp	Obtains IP addresses via DHCP.
local	Assigns IP addresses from an IP address pool configured on the ASA and associates them with a tunnel group.
reuse-delay *delay*	The delay before a released IP address can be reused. The range is 0 to 480 minutes. The default is 0 (disabled).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0.3	The reuse-delay option was added.
9.5(2)	Support for multiple context mode was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

If you choose DHCP, you should also use the **dhcp-network-scope** command to define the range of IP addresses that the DHCP server can use. You must use the dhcp-server command to indicate the IP addresses that the DHCP server uses.

If you choose local, you must also use the **ip local pool** command to define the range of IP addresses to use. You then use the **vpn-framed-ip-address** and **vpn-framed-netmask** commands to assign IP addresses and netmasks to individual users.

With the local pool, you can use the reuse-delay delay option to adjust the delay before a released IP address can be reused. Increasing the delay prevents problems firewalls may experience when an IP address is returned to the pool and reassigned quickly.

If you choose AAA, you obtain IP addresses from either a previously configured RADIUS server.

Examples

The following example shows how to configure DHCP as the address assignment method:

```
ciscoasa(config)# vpn-addr-assign dhcp
```

Related Commands

Command	Description
dhcp-network-scope	Specifies the range of IP addresses the ASA DHCP server should use to assign addresses to users of a group policy.
ip local pool	Creates a local IP address pool.
ipv6-addr-assign	Specifies a method for assigning IPv6 addresses to remote access clients.
vpn-framed-ip-address	Specifies the IP address to assign to a particular user.
vpn-framed-ip-netmask	Specifies the netmask to assign to a particular user.

vpn-mode

To configure distributed site-to-site VPN mode for a cluster, use the **vpn-mode** command in cluster group configuration mode.

vpn-mode [**centralized | distributed**] [**backup** { **flat | remote-chassis** }]
no vpn-mode [{ **centralized** | **distributed** [**backup** { **flat | remote-chassis** }] }]

Command Default

The default VPN mode is centralized. The default backup is flat.

Syntax Description

centralized	VPN sessions are centralized, running only on the cluster master unit.
distributed	VPN sessions are distributed across the members of the cluster.
backup	(Firepower 9300) Sets how backup sessions are allocated.
flat	(Firepower 9300) Backup sessions are allocated on any other member of the cluster.
remote-chassis	(Firepower 9300) Backup sessions allocated on another chassis' member.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	—	• Yes	—	• Yes

Command History

Release	Modification
9.9(1)	Command added for the Firepower 9300.
9.23(1)	Support added for the Secure Firewall 4200.
9.24(1)	For the Secure Firewall 4200, you must disable clustering to change the mode. A reload is no longer required.

Usage Guidelines

Secure Firewall 4200

Clustering must be disabled before changing the mode. After reenabling clustering, the mode is synched to data nodes.

Firepower 9300

Changing the VPN mode between centralized and distributed requires all nodes in the cluster to reload. Changing the backup mode is dynamic and will not terminate sessions.

In flat backup mode, standby sessions are established on any other cluster member. This will protect users from blade failures, however, chassis failure protection is not guaranteed.

In remote-chassis backup mode standby sessions are established on a member of another chassis in the cluster. This will protect users from both blade failures and chassis failures.

If remote-chassis is configured in a single chassis environment (intentionally configured or the result of a failure), no backups will be created until another chassis joins.

Examples

```
ciscoasa (cfg-cluster)# vpn-mode distributed
WARNING: Do you want to proceed with changing the vpn-mode, save the device configuration,
and initiate a reboot? [confirm]
```

Related Commands

Command	Description
cluster group	Configures the cluster group settings.
show cluster vpn-sessiondb distribution	View the distribution of active and backup sessions across cluster members.

vpnclient connect

To attempt to establish an Easy VPN Remote connection to the configured server or servers, use the **vpnclient connect** command in global configuration mode.

vpnclient connect

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Examples

The following example shows how to attempt to establish an Easy VPN Remote connection to a configured EasyVPN server:

```
ciscoasa
(config)#
vpnclient connect
ciscoasa
(config)#
```

vpnclient enable

To enable the Easy VPN Remote feature, use the **vpnclient enable** command in global configuration mode. To disable the Easy VPN Remote feature, use the **no** form of this command:

vpnclient enable
no vpnclient enable

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

If you enter the vpnclient enable command, the supported ASA functions as an Easy VPN Remote hardware client.

Examples

The following example shows how to enable the Easy VPN Remote feature:

```
ciscoasa
(config)#
vpnclient enable
ciscoasa
(config)#
```

The following example shows how to disable the Easy VPN Remote feature:

```
ciscoasa
(config)#
no
vpnclient enable
ciscoasa
(config)#
```

vpnclient ipsec-over-tcp

To configure the ASA running as an Easy VPN Remote hardware client to use TCP-encapsulated IPsec, use the **vpnclient ipsec-over-tcp** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient ipsec-over-tcp [**port** *tcp_port*]
no vpnclient ipsec-over-tcp

Syntax Description

port	(Optional) Specifies the use of a particular port.
tcp_port	(Required if you specify the keyword **port**.) Specifies the TCP port number to be used for a TCP-encapsulated IPsec tunnel.

Command Default

The Easy VPN Remote connection uses port 10000 if the command does not specify a port number.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

By default, the Easy VPN client and server encapsulate IPsec in User Datagram Protocol (UDP) packets. Some environments, such as those with certain firewall rules, or NAT and PAT devices, prohibit UDP. To use standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) in such environments, you must configure the client and the server to encapsulate IPsec within TCP packets to enable secure tunneling. If your environment allows UDP, however, configuring IPsec over TCP adds unnecessary overhead.

If you configure an ASA to use TCP-encapsulated IPsec, enter the following command to let it send large packets over the outside interface:

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

This command clears the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether the packet can be fragmented. This command lets the Easy VPN hardware client send packets that are larger than the MTU size.

Examples

The following example shows how to configure the Easy VPN Remote hardware client to use TCP-encapsulated IPsec, using the default port 10000, and to let it send large packets over the outside interface:

```
ciscoasa
(config)#
vpnclient ipsec-over-tcp
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa
(config)#
```

The next example shows how to configure the Easy VPN Remote hardware client to use TCP-encapsulated IPsec, using the port 10501, and to let it send large packets over the outside interface:

```
ciscoasa
(config)#
vpnclient ipsec-over-tcp port 10501
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa
(config)#
```

vpnclient mac-exempt

To exempt devices behind an Easy VPN Remote connection from individual user authentication requirements, use the **vpnclient mac-exempt** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]
no vpnclient mac-exempt

Syntax Description

mac_addr_1	MAC address, in dotted hexadecimal notation, specifying a manufacturer and serial number of a device for which to exempt individual user authentication. For more than one device, specify each MAC address, separating each with a space and the respective network mask. The first 6 characters of the MAC address identify the device manufacturer, and the last 6 characters are the serial number. The last 24 bits are the unit's serial number in hexadecimal format.
mac_mask_1	Network mask for the corresponding MAC address. Use a space to separate the network mask and any subsequent MAC address and network mask pairs.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Devices such as Cisco IP phones, wireless access points, and printers are incapable of performing authentication, and therefore do not authenticate when individual unit authentication is enabled. If individual user authentication is enabled, you can use this command to exempt such devices from authentication. The exemption of devices from individual user authentication is also called "device pass-through."

The format for specifying the MAC address and mask in this command uses three hex digits, separated by periods; for example, the MAC mask ffff.ffff.ffff matches just the specified MAC address. A MAC mask of

all zeroes matches no MAC address, and a MAC mask of ffff.ff00.0000 matches all devices made by the same manufacturer.



Note You must have Individual User Authentication and User Bypass configured on the headend device. For example, if you have the ASA as the headend, configure the following under group policy:ciscoasa(config-group-policy)# **user-authentication enable**ciscoasa(config-group-policy)# **ip-phone-bypass enable**

Examples

Cisco IP phones have the Manufacturer ID 00036b, so the following command exempts any Cisco IP phone, including Cisco IP phones, you might add in the future:

```
ciscoasa
(config)#
vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
ciscoasa
(config)#
```

The next example provides greater security but less flexibility because it exempts one specific Cisco IP phone:

```
ciscoasa
(config)#
vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
ciscoasa
(config)#
```

vpnclient management

To generate IPsec tunnels for management access to the Easy VPN Remote hardware client, use the **vpnclient management** command in global configuration mode.

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]
vpnclient management clear

To remove the attribute from the running configuration, use the **no** form of this command, which sets up IPsec tunnels exclusively for management in accordance with the **split-tunnel-policy** and **split-tunnel-network-list** commands.

no vpnclient management clear

Syntax Description

clear	Uses normal routing to provide management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client. This option does not create management tunnels. **Note** Use this option if a NAT device is operating between the client and the Internet.
ip_addr	IP address of the host or network for which to build a management tunnel from the Easy VPN hardware client. Use this argument with the **tunnel** keyword. Specify one or more IP addresses, separating each with a space and the respective network mask.
ip_mask	Network mask for the corresponding IP address. Use a space to separate the network mask and any subsequent IP address and network mask pairs.
tunnel	Automates the setup of IPsec tunnels specifically for management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

It assumes the ASA 5505 configuration contains the following commands:

- **vpnclient server** to specify the peer.
- **vpnclient mode** to specify the client mode (PAT) or network extension mode.

One of the following:

- **vpnclient vpngroup** to name the tunnel group and the IKE pre-shared key used for authentication on the Easy VPN server.
- **vpnclient trustpoint** to name the trustpoint identifying the RSA certificate to use for authentication



Note The public address of an ASA behind a NAT device is inaccessible unless you add static NAT mappings on the NAT device.



Note Regardless of your configuration, DHCP requests (including renew messages) should not flow over IPsec tunnels. Even with a vpnclient management tunnel, DHCP traffic is prohibited.

Examples

The following example shows how to generate an IPsec tunnel from the outside interface of the ASA 5505 to the host with the IP address/mask combination 192.168.10.10 255.255.255.0:

```
ciscoasa
(config)#
vpnclient management tunnel 192.168.10.0 255.255.255.0
ciscoasa
(config)#
```

The following example shows how to provide management access to the outside interface of the ASA 5505 without using IPsec:

```
ciscoasa(config)# vpnclient management clear
ciscoasa(config)#
```

vpnclient mode

To configure the Easy VPN Remote connection for either client mode or network extension mode, use the **vpnclient mode** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient mode { **client-mode | network-extension-mode** }
no vpnclient mode

Syntax Description

client-mode	Configures the Easy VPN Remote connection to use client mode (PAT).
network-extension-mode	Configures the Easy VPN Remote connection to use network extension mode (NEM).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

The Easy VPN Client supports one of two modes of operation: client mode or NEM. The mode of operation determines whether the inside hosts, relative to the Easy VPN Client, are accessible from the Enterprise network over the tunnel. Specifying a mode of operation is mandatory before making a connection because Easy VPN Client does not have a default mode.

- In client mode, the Easy VPN client performs port address translation (PAT) for all VPN traffic from its inside hosts. This mode requires no IP address management for either the inside address of the hardware client (which has a default RFC 1918 address assigned to it) or the inside hosts. Because of PAT, the inside hosts are not accessible from the enterprise network.
- In NEM, all nodes on the inside network and the inside interface are assigned addresses routable across the enterprise network. The inside hosts are accessible from the enterprise network over a tunnel. Hosts on the inside network are assigned IP addresses from an accessible subnet (statically or through DHCP). PAT is not applied to the VPN traffic when in network extension mode.



Note If the Easy VPN hardware client is using NEM and has connections to secondary servers, use the **crypto map set reverse-route** command on each headend device to configure dynamic announcements of the remote network using Reverse Route Injection (RRI).

Examples

The following example shows how to configure an Easy VPN Remote connection for client mode:

```
ciscoasa
(config)#
vpnclient mode client-mode
ciscoasa
(config)#
```

The following example shows how to configure an Easy VPN Remote connection for NEM:

```
ciscoasa
(config)#
vpnclient mode network-extension-mode
ciscoasa
(config)#
```

vpnclient nem-st-autoconnect

To configure the Easy VPN Remote connection to automatically initiate IPsec data tunnels when NEM and split tunneling are configured, use the **vpnclient nem-st-autoconnect** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient nem-st-autoconnect
no vpnclient nem-st-autoconnect

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Before entering the **vpnclient nem-st-autoconnect** command, ensure that network extension mode is enabled for the hardware client. Network extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. IPsec encapsulates all traffic from the private network behind the hardware client to networks behind the ASA. PAT does not apply. Therefore, devices behind the ASA have direct access to devices on the private network behind the hardware client over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel. After the tunnel is up, either side can initiate data exchange.



Note You must also configure the Easy VPN server to enable network extension mode. To do so, use the **nem enable** command in group-policy configuration mode.

IPsec data tunnels are automatically initiated and sustained when in network extension mode, except when split-tunneling is configured.

Examples

The following example shows how to configure an Easy VPN Remote connection to automatically connect in network extension mode with split-tunneling configured. Network extension mode is enabled for the group policy FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)
# nem enable
ciscoasa
(config)#
vpnclient nem-st-autoconnect
ciscoasa
(config)#
```

Related Commands

Command	Description
nem	Enables network extension mode for hardware clients.

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

no vpnclient sercure interface

vpnclient server

To configure the primary and secondary IPsec servers, for the Easy VPN Remote connection, use the **vpnclient server** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server *ip_primary_address* [*ip_secondary_address_1 … ipsecondary_address_10*]
no vpnclient server

Syntax Description

ip_primary_address	IP address or DNS name of the primary Easy VPN (IPsec) server. Any ASA or VPN 3000 Concentrator Series can act as an Easy VPN server.
ip_secondary_address_n	(Optional) List of the IP addresses or DNS names of up to ten backup Easy VPN servers. Use a space to separate the items in the list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

A server must be configured before a connection can be established. The **vpnclient server** command supports IPv4 addresses, the names database, or DNS names and resolves addresses in that order.

You can use either the IP address or the hostname of a server.

Examples

The following example associates the name headend-1 with the address 10.10.10.10 and uses the **vpnclient server** command to specify three servers: headend-dns.example.com (primary), headend-1 (secondary), and 192.168.10.10 (secondary):

```
ciscoasa
(config)#
names
ciscoasa(config)# 10.10.10.10 headend-1
```

```
ciscoasa(config)# vpnclient server headend-dns.example.com headend-1 192.168.10.10
ciscoasa(config)#
```

The following example shows how to configure a VPN client primary IPsec server with the IP address 10.10.10.15 and secondary servers with the IP addresses 10.10.10.30 and 192.168.10.45.

```
ciscoasa
(config)#
vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
ciscoasa
(config)#
```

vpnclient server-certificate

To configure the Easy VPN Remote connection to accept only connections to Easy VPN servers with the specific certificates specified by the certificate map, use the **vpnclient server-certificate** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server-certificate *certmap_name*
no vpnclient server-certificate

Syntax Description

certmap_name	Specifies the name of a certificate map that specifies the acceptable Easy VPN server certificate. The maximum length is 64 characters.

Command Default

Easy VPN server certificate filtering is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Use this command to enable Easy VPN server certificate filtering. You define the certificate map itself using the crypto ca certificate map and crypto ca certificate chain commands.

Examples

The following example shows how to configure an Easy VPN Remote connection to support only connections to Easy VPN servers with the certificate map name homeservers:

```
ciscoasa
(config)#
vpnclient server-certificate homeservers
ciscoasa
(config)#
```

Related Commands

Command	Description
certificate	Adds the indicated certificate.

Command	Description
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN Remote connection.

vpnclient trustpoint

To configure the RSA identity certificate to be used by the Easy VPN Remote connection, use the **vpnclient trustpoint** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient trustpoint *trustpoint_name* [**chain**]
no vpnclient trustpoint

Syntax Description

chain	Sends the entire certificate chain.
trustpoint_name	Specifies the name of a trustpoint identifying the RSA certificate to use for authentication.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Define the trustpoint using the **crypto ca trustpoint** command. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint sub mode control CA-specific configuration parameters which specify how the ASA obtains the CA certificate, how the ASA obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

Examples

The following example shows how to configure an Easy VPN Remote connection to use the specific identity certificate named central and to send the entire certificate chain:

```
ciscoasa(config)# crypto ca trustpoint
central
ciscoasa
(config)#
vpnclient trustpoint central chain
ciscoasa
```

```
(config)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters the trustpoint submode for the specified trustpoint and manages trustpoint information.

vpnclient username

To configure the VPN username and password for the Easy VPN Remote connection, use the **vpnclient username** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient username *xauth_username* **password** *xauth password*
no vpnclient username

Syntax Description

xauth_password	Specifies the password to use for XAUTH. The maximum length is 64 characters.
xauth_username	Specifies the username to use for XAUTH. The maximum length is 64 characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

The XAUTH username and password parameters are used when secure unit authentication is disabled and the server requests XAUTH credentials. If secure unit authentication is enabled, these parameters are ignored, and the ASA prompts the user for a username and password.

Examples

The following example shows how to configure the Easy VPN Remote connection to use the XAUTH username testuser and the password ppurkm1:

```
ciscoasa
(config)#
vpnclient username testuser password ppurkm1
ciscoasa
(config)#
```

vpnclient vpngroup

To configure the VPN tunnel group name and password for the Easy VPN Remote connection, use the **vpnclient vpngroup** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient vpngroup *group_name* **password** *preshared_key*
no vpnclient vpngroup

Syntax Description

group_name	Specifies the name of the VPN tunnel group configured on the Easy VPN server. The maximum length is 64 characters, and no spaces are allowed.
preshared_key	The IKE pre-shared key used for authentication by the Easy VPN server. The maximum length is 128 characters.

Command Default

If the configuration of the ASA running as an Easy VPN Remote hardware client does not specify a tunnel group, the client attempts to use an RSA certificate.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command applies only to an ASA running as an Easy VPN Remote hardware client: ASA 5505 running releases 7.2(1) through 9.2, or ASA 5506 or 5508 models running release 9.5(1) or later.

Use the pre-shared key as the password.

You must also configure a server and specify the mode before establishing a connection.

Examples

The following example shows how to configure an Easy VPN Remote connection with a VPN tunnel group with the group name TestGroup1 and the password my_key123.

```
ciscoasa
(config)#
vpnclient vpngroup TestGroup1 password my_key123
ciscoasa
(config)#
```

Related Commands

Command	Description
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN connection.

vpn-filter

To specify the name of the ACL to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the ACL, including a null value created by issuing the **vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **vpn-filter none** command.

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

vpn-filter { **value** *ACL name* **| none** }
no vpn-filter

Syntax Description

none	Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *ACL name*	Provides the name of the previously configured access list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	• Yes	—
Username configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for IPv4 and IPv6 ACLs was added. Support for multiple context mode was added.
9.1.(4)	Support for IPv4 and IPv6 ACLs was added. If the deprecated command **ipv6-vpn-filter** is mistakenly used to specify IPv6 ACLs, the connection will be terminated.

Usage Guidelines

Clientless SSL VPN does not use the ACL defined in the **vpn-filter** command.

By design, the vpn-filter feature allows for traffic to be filtered in inbound direction only. The outbound rule is automatically compiled. When creating an icmp access-list, do not specify icmp type in the access-list formatting if you want directional filters.

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.

Examples

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

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

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
ipv6-vpn-filter	Deprecated command which was used previously to specify IPv6 ACLs.

vpn-framed-ip-address

To specify the IPv4 address to assign to an individual user, use the **vpn-framed-ip-address** command in username mode. To remove the IP address, use the **no** form of this command.

vpn-framed-ip-address { *ip_address* } { *subnet_mask* }
no vpn-framed-ip-address

Syntax Description

ip_address	Provides the IP address for this user.
subnet_mask	Specifies the subnetwork mask.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to set an IP address of 10.92.166.7 for a user named anyuser:

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
vpn-framed-ip-address 10.92.166.7 255.255.255.254
```

vpn-framed-ipv6-address

Use the **vpn-framed-ipv6-address** command in username mode to assign a dedicated IPv6 address to a user. To remove the IP address, use the **no** form of this command.

vpn-framed-ip6-address *ip_address/subnet_mask*
no vpn-framed-ip6-address *ip_address/subnet_mask*

Syntax Description

ip_address	Provides the IP address for this user.
subnet_mask	Specifies the subnetwork mask.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

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.

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
vpn-framed-ipv6-address
2001::3000:1000:2000:1/64
ciscoasa(config-username)
```

Related Commands

Command	Description
vpn-framed-ip-address	Specifies an IPv4 address to assign to an individual user.

vpn-group-policy

To have a user inherit attributes from a configured group policy, use the vpn-group-policy command in username configuration mode. To remove a group policy from a user configuration, use the **no** version of this command. Using this command lets users inherit attributes that you have not configured at the username level.

vpn-group-policy { *group-policy name* }
no vpn-group-policy { *group-policy name* }

Syntax Description

group-policy name	Provides the name of the group policy.

Command Default

By default, VPN users have no group policy association.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can override the value of an attribute in a group policy for a particular user by configuring it in username mode, if that attribute is available in username mode.

Examples

The following example shows how to configure a user named anyuser to use attributes from the group policy named FirstGroup:

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)# vpn-group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Adds a group policy to the ASA database.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a group policy.

Command	Description
username	Adds a user to the ASA database.
username attributes	Enters username attributes mode, which lets you configure AVPs for specific users.

vpn-idle-timeout

To configure a user timeout period use the **vpn-idle-timeout** 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. You can optionally extend the timeout alert-interval from the default one minute.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-idle-timeout none** command.

vpn-idle-timeout { *minutes* | **none** } [**alert-interval** *minutes*]
no vpn-idle-timeout
no vpn-idle-timeout alert-interval

Syntax Description

minutes	Specifies the number of minutes in the timeout period, and the number of minutes before the time-out alert. Use an integer between 1 and 35791394.
none	AnyConnect (SSL IPsec/IKEv2): Use the global WebVPN default-idle-timeout value (seconds) from the command: ciscoasa**(config-webvpn)# default-idle-timeout** The range for this value in the WebVPN **default-idle-timeout** command is 60-86400 seconds; the default Global WebVPN Idle timeout in seconds -- default is 1800 seconds (30 min). **Note** A non-zero idle timeout value is required by ASA for all AnyConnect connections. For a WebVPN user, the **default-idle-timeout** value is enforced only if vpn-idle-timeout none is set in the group policy/username attribute. Site-to-Site (IKEv1, IKEv2) and IKEv1 remote-access: Disable timeout and allow for an unlimited idle period.

Command Default

30 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The Secure Client supports session resumption for SSL and IKEv2 connection. With this capability, end user devices can go into sleep mode, lose their WiFi, or any of the like and resume the same connection upon return.

Examples

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

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-idle-timeout 30
```

The security appliance uses the default-idle-timeout value if no idle timeout is defined for a user, if the vpn-idle-timeout value is 0, or if the value does not fall into the valid range.

Related Commands

default-idle-timeout	Specifies the global WebVPN default idle timeout.
group-policy	Creates or edits a group policy.
vpn-session-timeout	Configures the maximum amount of time allowed for VPN connections. At the end of this period of time, the ASA terminates the connection.

vpn load-balancing

To enter vpn load-balancing mode, in which you can configure VPN load balancing and related functions, use the **vpn load-balancing** command in global configuration mode.

vpn load-balancing

Note To use VPN load balancing, you must have an ASA 5510 with a Plus license or an ASA 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	Support for the ASA 5510 with a Plus license and models above 5520 was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

A load-balancing cluster can include security appliance models 5510 (with a Plus license), or ASA 5520 and above. You can also include VPN 3000 Series Concentrators in the cluster. While mixed configurations are possible, administration is generally simpler if the cluster is homogeneous.

Use the **vpn load-balancing** command to enter vpn load-balancing mode. The following commands are available in vpn load-balancing mode:

- **cluster encryption**
- **cluster ip address**
- **cluster key**

- **cluster port**
- **interface**
- **nat**
- **participate**
- **priority**
- **redirect-fqdn**

See the individual command descriptions for detailed information.

Upgrade Guidelines

During a software upgrade, the VPN load-balancing cluster does not form if members run different versions. Perform one of these actions:

1. Upgrade all members to the same version. The VPN load-balancing cluster re-forms automatically after all members run the same version.

   VPN load balancing is unavailable during the mixed-version window.

2. For a hitless upgrade, temporarily remove the cluster keys from all members. Keep the interval without cluster keys as short as possible. Upgrade all members and then reconfigure the cluster keys on all members.

   VPN load balancing remains available during the upgrade.

Note This requirement applies to ASA Version 9.22.3.26, 9.20.4.49, 9.24.1.26, 9.18.4.94, 9.23.1.47, and 9.16.4.103.

In these ASA versions, if you choose option 2, syslog 718089 is logged:

%ASA-1-718089: VPN LB cluster is running without authentication. Configure 'cluster key' to secure the cluster.

Cluster encryption and cluster keys secure authentication between VPN load-balancing members and help protect the group from denial-of-service (DoS) and spoofing attacks.

Examples

The following is an example of the **vpn load-balancing** command; note the change in the prompt:

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)#
```

The following is an example of a VPN load-balancing command sequence that includes an interface command that specifies the public interface of the cluster as “test” and the private interface of the cluster as “foo”:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
```

```
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
```

ciscoasa(config-load-balancing)# **participate**

Related Commands

Command	Description
clear configure vpn load-balancing	Removes the load-balancing runtime configuration and disables load balancing.
show running-config vpn load-balancing	Displays the current VPN load-balancing virtual cluster configuration.
show vpn load-balancing	Displays VPN load-balancing runtime statistics.

vpn-sessiondb

To specify the maximum number of VPN sessions or Secure Client VPN sessions, use the vpn-sessiondb command from global configuration mode. To remove the limit from the configuration, use the no form of the command:

vpn-sessiondb { **max-anyconnect-premium-or-essentials-limit** *number* | **max-other-vpn-limit** *number* }

Syntax Description

max-anyconnect-premium-or-essentials-limit number	Specifies the maximum number of AnyConnect sessions, from 1 to the maximum sessions allowed by the license.
max-other-vpn-limit number	Specifies the maximum number of VPN sessions other than Secure Client sessions, from 1 to the maximum sessions allowed by the license. This includes Cisco VPN client (IPsec IKEv1) and LAN-to-LAN VPN.

Command Default

By default, the ASA does not limit the number of VPN sessions lower than the licensed maximum.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The following keywords were changed: • max-anyconnect-premium-or-essentials-limit replaced max-session-limit • max-other-vpn-limit replaced max-webvpn-session-limit
9.0(1)	Support for multiple context mode was added.

Examples

The following example sets the maximum AnyConnect sessions to 200:

```
ciscoasa(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 200
```

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and WebVPN sessions.
vpn-sessiondb max-webvpn-session-limit	Sets a maximum number of WebVPN sessions.

vpn-sessiondb logoff

To log off all or selected VPN sessions, use the **vpn-sessiondb logoff** command in global configuration mode.

vpn-sessiondb logoff { **all** | **anyconnect** | **email-proxy** | **index index_number** | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol-name* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *groupname* | **vpn-lb** | **webvpn** } [**noconfirm**]

Syntax Description

all	Logs off all VPN sessions.
anyconnect	Logs of all AnyConnect VPN client sessions.
email-proxy	(Deprecated) Logs off all e-mail proxy sessions.
index *index_number*	Logs off a single session by index number. Specify the index number for the session. You can view index numbers for each session with the show vpn-sessiondb detail command.
ipaddress *IPaddr*	Logs off sessions for the IP address hat you specify.
l2l	Logs off all LAN-to-LAN sessions.
name *username*	Logs off sessions for the username that you specify.
protocol *protocol-name*	Logs off sessions for protocols that you specify. The protocols include:

	• ikev1—Sessions using the Internet Key Exchange version 1 (IKEv1) protocol. • ikev2—Sessions using the Internet Key Exchange version 2 (IKEv2) protocol. • ipsec—IPsec sessions using either IKEv1 or IKEv2. • ipseclan2lan—IPsec LAN-to-LAN sessions. • ipseclan2lanovernatt—IPsec LAN-to-LAN over NAT-T sessions. • ipsecovernatt—IPsec over NAT-T sessions. • ipsecovertcp—IPsec over TCP sessions. • ipsecoverudp—IPsec over UDP sessions. • l2tpOverIpSec—L2TP over IPsec sessions. • l2tpOverIpsecOverNatT—L2TP over IPsec over NAT-T sessions. • webvpn—Clientless SSL VPN sessions. • imap4s—IMAP4 sessions. • pop3s—POP3 sessions. • smtps—SMTP sessions. • anyconnectParent—Secure Client sessions, regardless of the protocol used for the session (terminates AnyConnect IPsec IKEv2 and SSL sessions). • ssltunnel—SSL VPN sessions, including AnyConnect sessions using SSL and clientless SSL VPN sessions. • dtlstunnel—Secure Client sessions with DTLS enabled.
ra-ikev1-ipsec	Logs off all IPsec IKEv1 remote-access sessions.
ra-ikev2-ipsec	Logs off all IPsec IKEv2 remote-access sessions.
tunnel-group *groupname*	Logs off sessions for the tunnel group (connection profile) that you specify.
webvpn	Logs off all clientless SSL VPN sessions.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The following protocol keywords were changed or added: • remote was changed to ra-ikev1-ipsec. • ike was changed to ikev1. • ikev2 was added. • anyconnectParent was added.
9.0(1)	Support for multiple context mode was added.
9.3(2)	The **ra-ikev2-ipsec** keyword was added.
9.8(1)	The **email-proxy** option was deprecated.

Examples

The following example shows how to log off all Secure Client sessions:

```
ciscoasa# vpn-sessiondb logoff anyconnect
```

The following example shows how to log off all IPsec sessions:

```
ciscoasa# vpn-sessiondb logoff protocol IPsec
```

vpn-session-timeout

To configure a maximum amount of time allowed for VPN connections, use the **vpn-session-timeout** command in group-policy configuration mode or in username configuration mode. At the end of this period of time, the ASA terminates the connection. You can optionally extend the timeout alert-interval from the default one minute.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-session-timeout none** command.

vpn-session-timeout { *minutes* | **none** } [**alert-interval** *minutes*]
no vpn-session-timeout
no vpn-session-timeout alert-interval

Syntax Description

minutes	Specifies the number of minutes in the timeout period, and the number of minutes before the time-out alert. Use an integer between 1 and 35791394.
none	Permits an unlimited session timeout period. Sets session timeout with a null value, thereby disallowing a session timeout. Prevents inheriting a value from a default or specified group policy.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	**alert-interval** applied to AnyConnect VPNs

Examples

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

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

Related Commands

group-policy	Creates or edits a group policy.
vpn-idle-timeout	Configures the user timeout period. If there is no communication activity on the connection in this period, the ASA terminates the connection.

vpnsetup

To display a list of steps for configuring VPN connections on the ASA, use the **vpnsetup** command from global configuration mode.

vpnsetup { **ipsec-remote-access | l2tp-remote-access | site-to-site | ssl-remote-access** } **steps**

Syntax Description

ipsec-remote-access	Displays steps to configure the ASA to accept IPsec connections.
l2tp-remote-access	Displays steps to configure the ASA to accept L2TP connections.
site-to-site	Displays steps to configure the ASA to accept LAN-to-LAN connections.
ssl-remote-access	Displays steps to configure the ASA to accept SSL connections.
steps	Specifies to display the steps for the connection type.

Command Default

This command has no default settings

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(3)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example shows the output of the **vpnsetup ssl-remote-access steps command:**

```
ciscoasa(config-t)# vpnsetup ssl-remote-access steps
Steps to configure a remote access SSL VPN remote access connection and AnyConnect with
examples:
1. Configure and enable interface
 interface GigabitEthernet0/0
  ip address 10.10.4.200 255.255.255.0
  nameif outside
  no shutdown
 interface GigabitEthernet0/1
  ip address 192.168.0.20 255.255.255.0
  nameif inside
  no shutdown
```

```
2. Enable WebVPN on the interface
 webvpn
  enable outside
3. Configure default route
 route outside 0.0.0.0 0.0.0.0 10.10.4.200
4. Configure AAA authentication and tunnel group
 tunnel-group DefaultWEBVPNGroup type remote-access
 tunnel-group DefaultWEBVPNGroup general-attributes
  authentication-server-group LOCAL
5. If using LOCAL database, add users to the Database
 username test password t3stP@ssw0rd
 username test attributes
  service-type remote-access
Proceed to configure AnyConnect VPN client:
6. Point the ASA to an AnyConnect image
 webvpn
  svc image anyconnect-win-2.1.0148-k9.pkg
7. enable AnyConnect
 svc enable
8. Add an address pool to assign an ip address to the AnyConnect client
 ip local pool client-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
9. Configure group policy
 group-policy DfltGrpPolicy internal
 group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol svc webvpn
ciscoasa(config-t)#
```

Related Commands

Command	Description
show running-config	Displays the running configuration of the ASA.

vpn-simultaneous-logins

To configure the number of simultaneous logins permitted for a user, use the **vpn-simultaneous-logins** command in group-policy configuration mode or username configuration mode. To remove the attribute and return to the default value, use the **no** form of this command.

vpn-simultaneous-logins *integer*
no vpn-simultaneous-logins

Syntax Description

integer	A number between 0 and 2147483647.

Command Default

The default is 3 simultaneous logins.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This option allows inheritance of a value from another group policy. Enter 0 to disable login and prevent user access.

Note While the maximum limit for the number of simultaneous logins is very large, allowing several simultaneous logins could compromise security and affect performance.

Stale AnyConnect, 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 value of vpn-simultaneous-logins 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 simultaneous logins is a value greater than 1, then, when you have reached that maximum number and try 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, using the **vpn-simultaneous-login-delete-no-delay** command.

Examples

The following example shows how to allow a maximum of 4 simultaneous logins for the group policy named FirstGroup:

```
ciscoasa(config)#  group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

To configure a VPN tunnel type (IPsec with IKEv1 or IKEv2, L2TP over IPsec, SSL, or clientless SSL), use the **vpn-tunnel-protocol** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpn-tunnel-protocol { **ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless** }
no vpn-tunnel-protocol { **ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless** }

Syntax Description

ikev1	Negotiates an IPsec tunnel with IKEv1 between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
ikev2	Negotiates an IPsec tunnel with IKEv2 between two peers (a remote access 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 VPN tunnel with an SSL VPN client.
ssl-clientless	Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client.

Command Default

The default is IPsec.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.17(1)	The ssl-clientless keyword was removed due to support removal for clientless web VPN.
8.4(1)	The ipsec keyword was replaced by the ikev1 and ikev2 keywords.
7.3(1)	The **svc** keyword was added.
7.2(1)	The **l2tp-ipsec** keyword was added.

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use 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.

Note To support fallback from IPsec to SSL, the **vpn-tunnel-protocol** command must have both the **svc** and **ipsec** arguments configured.

Examples

The following example shows how to configure WebVPN and IPsec tunneling modes for the group policy named “FirstGroup”:

```
ciscoasa
(config)#

group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 vpn-tunnel-protocol webvpn
ciscoasa
(config-group-policy)#
 vpn-tunnel-protocol IPsec
```

Related Commands

Command	Description
address pools	Specifies a list of address pools for allocating addresses to remote clients.
show running-config group-policy	Displays the configuration for all group-policies or for a specific group-policy.

vtep-nve

To associate a VXLAN VNI interface with the VTEP source interface, use the **vtep-nve** command in interface configuration mode. To remove the association, use the **no** form of this command.

vtep-nve 1
no vtep-nve 1

Syntax Description

1	Specifies the NVE instance, which is always 1.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

You can configure one VTEP source interface per ASA or per security context. You can configure one NVE instance that specifies this VTEP source interface. All VNI interfaces must be associated with this NVE instance.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and associates the VNI 1 interface with it:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

vxlan port

To set the VXLAN UDP port, use the **vxlan port** command in global configuration mode. To remove restore the default port, use the **no** form of this command.

vxlan port *udp_port*
no vxlan port *udp_port*

Syntax Description

udp_port	Sets the VXLAN UDP port. The default is 4789.

Command Default

The default port is 4789.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nve configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789. If your network uses a non-standard port, you can change it.

Examples

For example:

```
ciscoasa(config)# vxlan port 5678
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.

Command	Description
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.