

traffic-export

To control the operation of IP traffic capture mode in IP traffic export, use the **traffic-export** command in privileged EXEC mode.

traffic-export interface *type number* { **start** | **stop** | **clear** | **copy** *memory-device* }

Syntax Description		
	<i>type number</i>	Type and number of the interface over which the packets being captured travel.
	start	Initiates a packet capture sequence.
	stop	Halts a packet capture sequence.
	clear	Clears the packet capture buffer.
	copy	Copies the contents of the packet capture buffer to an external device.
	<i>memory-device</i>	External memory device to which captured packets are transmitted. Options are <i>flash:</i> , <i>tftp:</i> , or <i>usbflash0:</i> .

Command Default This command has no defaults.

Command Modes Privileged EXEC.

Command History	Release	Modification
	12.4(11)T	This command was introduced.

Usage Guidelines Use the **traffic-export** command to control the operation of IP traffic capture mode in IP traffic export. The operator uses CLI commands to start or stop capture of packets flowing across a monitored interface, to copy the captured packets to an external memory device, or to clear the internal buffer which holds the captured packets.

Examples The following example illustrates the use of the **traffic-export** command to initiate the capture of packets on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 start
%RITE-5-CAPTURE_START: Started IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to halt the packet capture sequence on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 stop
%RITE-5-CAPTURE_STOP: Stopped IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to copy the contents of the packet capture buffer to an external memory device. The example of the interactive dialog identifies the external memory device and the remote host in which it resides.

```
Router# traffic-export interface fastethernet0/0 copy tftp:
Address or name of remote host []? 172.18.207.15
Capture buffer filename []? atmcapture
Copying capture buffer to tftp://172.18.207.15/atmcapture !!
router#
```

The following example illustrates the use of the **traffic-export** command to clear the packet capture buffer that is in local memory.

```
Router# traffic-export interface fastethernet 0/0 clear
%RITE-5-CAPTURE_CLEAR: Cleared IP traffic capture buffer for interface FastEthernet0/0
router#
```

Related Commands

Command	Description
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
ip traffic-export profile	Creates an IP traffic export or IP traffic capture profile on an ingress interface.

transfer-encoding type

To permit or deny HTTP traffic according to the specified transfer-encoding of the message, use the **transfer-encoding type** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

```
transfer-encoding type {chunked | compress | deflate | gzip | identity | default} action {reset |
allow} [alarm]
```

```
no transfer-encoding type {chunked | compress | deflate | gzip | identity | default} action {reset
| allow} [alarm]
```

Syntax Description

chunked	Encoding format (specified in RFC 2616, <i>Hypertext Transfer Protocol—HTTP/1</i>) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator.
compress	Encoding format produced by the UNIX “compress” utility.
deflate	“ZLIB” format defined in RFC 1950, <i>ZLIB Compressed Data Format Specification version 3.3</i> , combined with the “deflate” compression mechanism described in RFC 1951, <i>DEFLATE Compressed Data Format Specification version 1.3</i> .
gzip	Encoding format produced by the “gzip” (GNU zip) program.
identity	Default encoding, which indicates that no encoding has been performed.
default	All of the transfer encoding types.
action	Encoding types outside of the specified type are subject to the specified action (reset or allow).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If a given type is not specified, all transfer-encoding types are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Only encoding types specified by the **transfer-encoding-type** command are allowed through the firewall.

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
  application http
    strict-http action allow alarm
    content-length maximum 1 action allow alarm
    content-type-verification match-req-rsp action allow alarm
    max-header-length request 1 response 1 action allow alarm
    max-uri-length 1 action allow alarm
    port-misuse default action allow alarm
    request-method rfc default action allow alarm
    request-method extension default action allow alarm
    transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
  ip inspect firewall in
!
!
```

transport port

To configure the transport protocol for establishing a connection with the Diameter peer, use the **transport port** command in Diameter peer configuration mode. To block all sessions that are bound to the peer from using the connection, use the **no** form of this command.

transport tcp port *port-number*

no transport tcp port *port-number*

Syntax Description

tcp	Currently, TCP is the only supported transport protocol for establishing the connection with the Diameter peer.
<i>port-number</i>	Character string identifying the peer connection port.

Command Default

TCP is the default transport protocol.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced .

Examples

The following example configures TCP as the transport protocol and port 4100 as the peer connection port:

```
Router (config-dia-peer)# transport tcp port 4100
```

Related Commands

Command	Description
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

trm register

To allow the user to manually register the platform with the Trend Router Provisioning Server (TRPS), use the **trm register** command in privileged EXEC mode.

trm register

Syntax Description This command has no arguments or keywords.

Command Default This command is not enabled.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.4(15)XZ	This command was introduced.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines Use the **trm register** command to enable manual registration of the platform with the TRPS. If you do not use this command, the system sends a registration request to the TRPS every minute after boot-up until the registration is successful.

Examples The following is sample output from the **trm register** command:

```
Router# trm register

Processing registration request.
Please run 'show ip trm subscription' status to get more info
```

trustpoint (tti-petitioner)

To specify the trustpoint that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the Secure Device Provisioning (SDP) petitioner and the SDP registrar, use the **trustpoint** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint *trustpoint-label*

no trustpoint *trustpoint-label*

Syntax Description	<i>trustpoint-label</i>	Name of trustpoint.
Defaults	If a trustpoint is not specified, a default trustpoint called “tti” is generated.	
Command Modes	tti-petitioner configuration	
Command History	Release	Modification
	12.3(8)T	This command was introduced.
Usage Guidelines	Use the trustpoint command in tti-petitioner configuration mode to associate a trustpoint with the SDP petitioner.	
Examples	<p>The following example shows how specify the trustpoint “mytrust”:</p> <pre>crypto wui tti petitioner trustpoint mytrust</pre> <p>After the SDP exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the show running-config command shows an automatically generated configuration which generates the default trustpoint “tti”:</p> <pre>crypto pki trustpoint tti enrollment url http://pkil-36a.cisco.com:80 revocation-check crl rsakeypair tti 1024 auto-enroll 70</pre>	
Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.
	crypto wui tti petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.

trustpoint signing

To specify the trustpoint and associated certificate to be used when signing all introduction data during the Secure Device Provisioning (SDP) exchange, use the **trustpoint signing** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint signing *trustpoint-label*

no trustpoint signing *trustpoint-label*

Syntax Description	<i>trustpoint-label</i>	Name of trustpoint.
--------------------	-------------------------	---------------------

Defaults	If a trustpoint is not specified, any existing device certificate is used. If none is available, a self-signed certificate is generated.
----------	--

Command Modes	tti-petitioner configuration
---------------	------------------------------

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines	Use the trustpoint signing command in tti-petitioner configuration mode to associate a specific trustpoint with the petitioner for signing its certificate.
------------------	--

Examples	The following example shows how to specify the trustpoint mytrust:
----------	--

```
crypto provisioning petitioner
trustpoint signing mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
enrollment url http://pki1-36a.cisco.com:80
revocation-check crl
rsakeypair tti 1024
auto-enroll 70
```

Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.
	crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.
	trustpoint (tti-petitioner)	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar.

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the **no** form of this command.

```
tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre ipv6 | ipip
[decapsulate-any] | ipsec ipv4 | iptalk | ipv6 | ipsec ipv6 | mpls | nos | rbscp}
```

```
no tunnel mode
```

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible Connectionless Network Protocol (CLNS) tunnel.
gre	Generic routing encapsulation (GRE) protocol. This is the default.
gre multipoint	Multipoint GRE (mGRE).
gre ipv6	GRE tunneling using IPv6 as the delivery protocol.
ipip	IP-over-IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. This tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipsec ipv4	Tunnel mode is IPSec, and the transport is IPv4.
iptalk	Apple IPTalk encapsulation.
ipv6	Static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
ipsec ipv6	Tunnel mode is IPSec, and the transport is IPv6.
mpls	Multiprotocol Label Switching (MPLS) encapsulation.
nos	KA9Q/NOS compatible IP over IP.
rbscp	Rate Based Satellite Control Protocol (RBSCP).

Command Default

The default is GRE tunneling.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The aurp , dvmrp , and ipip keywords were added.
11.2	The optional decapsulate-any keyword was added.
12.2(13)T	The gre multipoint keyword was added.

Release	Modification
12.3(7)T	The following keywords were added: <ul style="list-style-type: none"> • gre ipv6 to support GRE tunneling using IPv6 as the delivery protocol. • ipv6 to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6. • rbscp to support RBSCP.
12.3(14)T	The ipsec ipv4 keyword was added.
12.2(18)SXE	The gre multipoint keyword added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	The ipsec ipv6 keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a router connects to an mouted (multicast) router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

GRE tunneling can be done between Cisco routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address, you can ping the other end of the tunnel to check the connection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IPsec profile. Combining mGRE tunnels and IPsec encryption allows a single mGRE interface to support multiple IPsec tunnels, thereby simplifying the size and complexity of the configuration.



Note

GRE tunnel keepalives configured using the **keepalive** command under a GRE interface are supported only on point-to-point GRE tunnels.

RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPSec, over satellite links without breaking the end-to-end model.

IPSec in IPv6 Transport

IPv6 IPSec encapsulation provides site-to-site IPSec protection of IPv6 unicast and multicast traffic. This feature allows IPv6 routers to work as a security gateway, establishes IPSec tunnels between another security gateway router, and provides crypto IPSec protection for traffic from an internal network when being transmitting across the public IPv6 Internet. IPv6 IPSec is very similar to the security gateway model using IPv4 IPSec protection.

Examples

Cayman Tunneling

The following example shows how to enable Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

GRE Tunneling

The following example shows how to enable GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre
```

IPSec in IPv4 Transport

The following example shows how to configure a tunnel using IPSec encapsulation with IPv4 as the transport mechanism:

```
Router(config)# crypto ipsec profile PROF
Router(config)# set transform tset
Router(config)# interface Tunnel0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel source Loopback0
Router(config-if)# tunnel destination 172.16.1.1
Router(config-if)# tunnel protection ipsec profile PROF
```

IPSec in IPv6 Transport

The following example shows how to configure an IPv6 IPSec tunnel interface:

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64
Router(config-if)# tunnel destination 10.0.0.1
Router(config-if)# tunnel source Ethernet 0/0
Router(config-if)# tunnel mode ipsec ipv6
Router(config-if)# tunnel protection ipsec profile profile1
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ! Ensures longer packets are fragmented before they are encrypted; otherwise, the
  ! receiving router would have to do the reassembly.
  ip mtu 1416
  ! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
  ! advertise routes that are learned via the mGRE interface back out that interface.
  no ip split-horizon eigrp 1
  no ip next-hop-self eigrp 1
  delay 1000
  ! Sets IPSec peer address to Ethernet interface's public address.
  tunnel source Ethernet0
  tunnel mode gre multipoint
  ! The following line must match on all nodes that want to use this mGRE tunnel.
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
```

RBSCP Tunneling

The following example shows how to enable RBSCP tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode rbscp
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPSec profile.
tunnel source	Sets the source address of a tunnel interface.

tunnel protection

To associate a tunnel interface with an IP Security (IPSec) profile, use the **tunnel protection** command in interface configuration mode. To disassociate a tunnel with an IPSec profile, use the **no** form of this command.

tunnel protection ipsec profile *name* [shared]

no tunnel protection ipsec profile *name* [shared]

Syntax Description

ipsec profile	Enables generic routing encapsulation (GRE) tunnel encryption via IPSec.
<i>name</i>	Name of the IPSec profile. This value must match the <i>name</i> specified in the crypto ipsec profile command.
shared	(Optional) Allows the tunnel protection IPSec Security Association Database (SADB) to share the same dynamic crypto map instead of creating a unique crypto map per tunnel interface. Note Unlike the tunnel protection command, which specifies that IPSec encryption will be performed after GRE encapsulation, configuring a crypto map on a tunnel interface specifies that encryption will be performed before GRE encapsulation. Note If the shared keyword is used, the tunnel source command must specify an interface instead of an IP address. Crypto sockets are not shared if the tunnel source is not specified as an interface.

Defaults

Tunnel interfaces are not associated with IPSec profiles.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(5)T	The shared keyword was added through DDTS CSCec28392.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(5)	The shared keyword was changed so that if it is used with the tunnel protection command, the tunnel source command must specify an interface instead of an IP address.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **tunnel protection** command to specify that IPSec encryption will be performed after the GRE has been added to the tunnel packet. The **tunnel protection** command can be used with multipoint GRE (mGRE) and point-to-point GRE (p-pGRE) tunnels. With p-pGRE tunnels, the tunnel destination address will be used as the IPSec peer address. With mGRE tunnels, multiple IPSec peers are possible; the corresponding Next Hop Resolution Protocol (NHRP) mapping nonbroadcast multiaccess (NBMA) destination addresses will be used as the IPSec peer addresses.

The shared Keyword

If you want to configure two Dynamic Multipoint VPN (DMVPN) mGRE and IPSec tunnels on the same router with the same local endpoint (tunnel source) configuration, you *must* issue the **shared** keyword.

The dynamic crypto map that is created by the **tunnel protection** command is always different from a crypto map that is configured directly on the interface.

**Note**

GRE tunnel keepalives (configured with the **keepalive** command under the GRE interface) are not supported in combination with the **tunnel protection** command.

Examples

The following example shows how to associate the IPSec profile “vpnprof” with an mGRE tunnel interface. In this example, the IPSec source peer address will be the IP address from Ethernet interface 0. There is a static NHRP mapping from IP address 10.0.0.3 to IP address 172.16.2.1, so for this NHRP mapping the IPSec destination peer address will be 172.16.2.1. The IPSec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**. Other NHRP mappings (static or dynamic) will automatically create additional IPSec security associations (SAs) with the same source peer address and the destination peer address from the NHRP mapping. The IPSec proxy for these NHRP mappings will be as follows: **permit gre host ethernet0-ip-address host NHRP-mapping-NBMA-address**.

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
  ip mtu 1416
  ip nhrp authentication donttell
  ip nhrp map multicast dynamic
  ip nhrp network-id 99
  ip nhrp holdtime 300
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.
  no ip split-horizon eigrp 1
  no ip next-hop-self eigrp 1
  delay 1000
! Sets the IPSec peer address to the Ethernet interface's public address.
  tunnel source Ethernet0
  tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
```

The following example shows how to associate the IPSec profile “vpnprof” with a p-pGRE tunnel interface. In this example, the IPSec source peer address will be the IP address from Ethernet interface 0. The IPSec destination peer address will be 172.16.1.10 (per the **tunnel destination address** command). The IPSec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**.

```
interface Tunnel1
 ip address 10.0.1.1 255.255.255.252
 ! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
 ! receiving router would have to do the reassembly.
 ip mtu 1420
 tunnel source Ethernet0
 tunnel destination 172.16.1.10
 tunnel protection ipsec profile vpnprof
```

In the following example, the crypto sockets are shared between the Tunnel0 and Tunnel1 interfaces because the **tunnel protection** command on both interfaces uses the same profile and is configured with the **shared** keyword. Both tunnels specify the tunnel source to be an Ethernet0/0 interface.

```
interface Tunnel0
 ip address 10.255.253.3 255.255.255.0
 no ip redirects
 ip mtu 1436
 ip nhrp authentication h1there
 ip nhrp map 10.255.253.1 192.168.1.1
 ip nhrp map multicast 192.168.1.1
 ip nhrp network-id 253
 ip nhrp holdtime 600
 ip nhrp nhs 10.255.253.1
 ip ospf message-digest-key 1 md5 wellikey
 ip ospf network broadcast
 ip ospf cost 35
 ip ospf priority 0
 no ip mroute-cache
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 253
 tunnel protection ipsec profile dmvpn-profile shared
```

```
interface Tunnel1
 ip address 10.255.254.3 255.255.255.0
 no ip redirects
 ip mtu 1436
 ip nhrp authentication h1there
 ip nhrp map multicast 192.168.1.3
 ip nhrp map 10.255.254.1 192.168.1.3
 ip nhrp network-id 254
 ip nhrp holdtime 600
 ip nhrp nhs 10.255.254.1
 ip ospf message-digest-key 1 md5 wellikey
 ip ospf network broadcast
 ip ospf priority 0
 no ip mroute-cache
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 254
 tunnel protection ipsec profile dmvpn-profile shared
```

Related Commands	Command	Description
	crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers.
	interface	Configures an interface type and enters interface configuration mode.
	keepalive (tunnel interfaces)	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing the tunnel protocol down for a specific interface.
	permit	Sets conditions for a named IP access list.
	tunnel source	Sets the source address for a tunnel interface.

type echo protocol ipIcmpEcho



Note

Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type echo protocol ipIcmpEcho** command is replaced by the **icmp-echo** command. See the **icmp-echo** command for more information.

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **type echo protocol ipIcmpEcho** command in IP SLA monitor configuration mode.

```
type echo protocol ipIcmpEcho {destination-ip-address | destination-hostname} [source-ipaddr
{ip-address | hostname} | source-interface interface-name]
```

Syntax Description

<i>destination-ip-address</i> <i>destination-hostname</i>	Destination IP address or hostname for the operation.
source-ipaddr { <i>ip-address</i> <i>hostname</i> }	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-interface <i>interface-name</i>	(Optional) Specifies the source interface for the operation.

Defaults

No IP SLAs operation type is configured for the operation being configured.

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The following keyword and arguments were added: <ul style="list-style-type: none"> source-ipaddr {<i>ip-address</i> <i>hostname</i>}
12.3(7)XR	The source-interface keyword and <i>interface-name</i> argument were added.
12.3(11)T	The source-interface keyword and <i>interface-name</i> argument were added.
12.4(4)T	This command was replaced by the icmp-echo command.
12.2(33)SRB	This command was replaced by the icmp-echo command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was replaced by the icmp-echo command.
12.2(33)SXI	This command was replaced by the icmp-echo command.

Usage Guidelines

The default request packet data size for an ICMP echo operation is 28 bytes. Use the **request-data-size** command to modify this value. This data size is the payload portion of the ICMP packet, which makes a 64-byte IP packet.

You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation. To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla monitor** global configuration command) and then reconfigure the operation with the new operation type.

Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the IP/ICMP protocol and the destination IP address 172.16.1.175.

```
ip sla monitor 10
  type echo protocol ipIcmpEcho 172.16.1.175
!
ip sla monitor schedule 10 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

udp idle-time

To configure the idle timeout of User Datagram Protocol (UDP) sessions going through the firewall, use the **udp idle-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

udp idle-time *seconds*

no udp idle-time *seconds*

Syntax Description	<i>seconds</i>	Amount of time, in seconds, for which a UDP session will continue to be managed while there is no activity.
---------------------------	----------------	---

Command Default	None
------------------------	------

Command Modes	Parameter-map type inspect configuration
----------------------	--

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines When you are configuring an inspect type parameter map, you can enter the **udp idle-time** subcommand after you enter the **parameter-map type inspect** command.

When the software detects a valid UDP packet, the software establishes state information for a new UDP session. Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples The following example specifies that if there is no activity, the UDP session will continue to be managed for 75 seconds:

```
parameter-map type inspect eng-network-profile
  udp idle-time 75
```

Related Commands	Command	Description
	ip inspect udp idle-time	Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity).
	parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.

unmatched-action

To define the action when the user request does not match the IP address or host site configuration, use the **unmatched-action** command in URL rewrite configuration mode. To disable the action, use the **no** form of this command.

unmatched-action [**direct-access** | **redirect**]

no unmatched-action [**direct-access** | **redirect**]

Syntax Description	
direct-access	(Optional) Provides direct access to the URL and an information page stating that the user can access the URL directly.
redirect	(Optional) Provides the user with direct access to the URL, but the user does not receive the information page as with the direct-access keyword.

Command Default Direct access to the URL

Command Modes URL rewrite configuration (config-webvpn-url-rewrite)

Command History	Release	Modification
	12.4(20)T	This command was introduced.

Examples The following example shows that the user has direct access to the URL:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# unmatched-action direct-access
```

Related Commands ^R	Command	Description
	host (webvpn url rewrite)	Selects the hostname of the site to be mangled on an SSL VPN gateway.
	ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.

url (ips-auto-update)

To define a location in which to retrieve the Cisco IOS Intrusion Prevention System (IPS) signature configuration files, use the **url** command in IPS-auto-update configuration mode.

```
url url
```

Syntax Description	<i>url</i>	Location in which the router retrieves the latest signature files.
---------------------------	------------	--

Command Default The default value is defined in the signature definition XML.

Command Modes IPS-auto-update configuration

Command History	Release	Modification
	12.4(11)T	This command was introduced.

Usage Guidelines Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Examples In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# show ip ips auto-update
```

```
IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
  hours (0-23) : 0-23
  days of month (1-31) : 1-31
  days of week: (0-6) : 1-5
```

Related Commands	Command	Description
	ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

url rewrite

To mangle selective URL requests on a Secure Socket Layer virtual private network (SSL VPN) gateway and enter URL rewrite mode, use the **url rewrite** command in webvpn context configuration mode. To disable selected URL requests, use the **no** form of this command.

url rewrite

no url rewrite

Syntax Description

This command has no arguments or keywords.

Command Default

All requests are mangled.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Configuring the **url rewrite** command enters the url rewrite submode, in which selected IP addresses or hosts are defined for mangling.

Examples

The following example shows that selective URL mangling has been configured for IP address 10.1.1.0 255.255.0.0:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# ip 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
host (webvpn url rewrite)	Selects the name of the host site to be mangled on an SSL VPN gateway.
ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.
unmatched-action (webvpn url rewrite)	Defines the action when the user request does not match the IP address or host site configuration.

urlfilter

To enable Cisco IOS URL filtering, use the **urlfilter** command in policy-map-class configuration mode. To disable URL filtering, use the **no** form of this command.

urlfilter *parameter-map-name*

no urlfilter *parameter-map-name*

Syntax Description	<i>parameter-map-name</i> Name of the parameter map for the URL filter.
---------------------------	---

Command Default	None
------------------------	------

Command Modes	Policy-map-class configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	You can use this command only after entering the policy-map type inspect , class type inspect , and parameter-map type inspect commands.
-------------------------	---

Examples	The following example enables Cisco IOS firewall URL filtering:
-----------------	---

```
policy-map type inspect p1
 class type inspect c1
  urlfilter param1
```

Related Commands	Command	Description
	class type inspect	Specifies the traffic (class) on which an action is to be performed.
	policy-map type inspect	Creates Level 3 and Level 4 inspect type policy maps.

url-list

To enter webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

url-list *name*

no url-list *name*

Syntax Description

<i>name</i>	Name of the URL list. The list name can up to 64 characters in length.
-------------	--

Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of a SSL VPN website is not configured. If the command is not used to attach a URL list to a policy group, then a URL list is not attached to a group policy.

Command Modes

Webvpn context configuration
Webvpn group policy configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Entering this command places the router in SSL VPN URL list configuration mode. In this mode, the list of URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

Examples

The following example creates a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

The following example attaches a URL list to a policy group configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
Router(config-webvpn-url)# exit
```

```
Router(config-webvpn-context)# policy group ONE  
Router(config-webvpn-group)# url-list ACCESS
```

Related Commands

Command	Description
heading	Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website.
policy group	Attaches a URL list to policy group configuration.
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.
url-text	Adds an entry to a URL list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

url-text

To add an entry to a URL list, use the **url-text** command in webvpn URL list configuration mode. To remove the entry from a URL list, use the **no** form of this command.

```
url-text {name url-value url}
```

```
no url-text {name url-value url}
```

Syntax Description

<i>name</i>	Text label for the URL. The label must be inside quotation marks if it contains spaces.
url-value <i>url</i>	An HTTP URL.

Command Default

An entry is not added to a URL list.

Command Modes

Webvpn URL list configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" url-value products.mycompany.com
```

Related Commands

Command	Description
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.

usage

To specify the intended use for the certificate, use the **usage** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

```
usage method1 [method2 [method3]]
```

```
no usage method1 [method2 [method3]]
```

Syntax Description	<i>method1</i> [<i>method2</i> [<i>method3</i>]]	Intended use for the certificate; the available options are ike , ssl-client , and ssl-server . You must choose at least one method, and you may choose all three methods.
---------------------------	--	--

Defaults	ike
-----------------	------------

Command Modes	Ca-trustpoint configuration
----------------------	-----------------------------

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines	<p>Before you can issue the usage command, you must enable the crypto ca trustpoint command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.</p> <p>This command may be used as a hint to set or clear key usage or other attributes in the certificate request.</p>
-------------------------	---

Examples	The following example shows how to specify the certificate named “frog” for Internet Key Exchange (IKE):
-----------------	--

```
crypto ca trustpoint frog
  enrollment url http://frog.phoobin.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet-0
  usage ike
  auto-enroll regenerate
  password revokeme
  rsa-key frog 2048
```

Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.

user

To enter the names of users that are allowed to authenticate using the local authentication server, use the **user** command in local RADIUS server configuration mode. To remove the username and password from the local RADIUS server, use the **no** form of this command.

```
user username {password | nthash} password [group group-name | mac-auth-only]
```

```
no user username {password | nthash} password [group group-name | mac-auth-only]
```

Syntax Description

<i>username</i>	Name of the user that is allowed to authenticate using the local authentication server.
password	Indicates that the user password will be entered.
nthash	Indicates that the NT value of the password will be entered.
<i>password</i>	User password.
group <i>group-name</i>	(Optional) Name of group to which the user will be added.
mac-auth-only	(Optional) Specifies that the user is allowed to authenticate using only MAC authentication.

Defaults

If no group name is entered, the user is not assigned to a VLAN and is never required to reauthenticate.

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.2(15)JA	This command was modified to support MAC address authentication on the local authenticator.
12.3(2)JA	This command was modified to support EAP-FAST authentication on the local authenticator.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

This command is not supported on bridges.

If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string.

Examples

The following example shows that the user named “user1” has been allowed to authenticate using the local authentication server (using the password “userisok”). This user will be added to the group named “team1”.

```
Router(config-radsrv)# user user1 password userisok group team1
```

The following example shows how to add a user to the list of clients allowed to authenticate using MAC-based authentication on the local authenticator.

```
AP(config-radsrv)# user 00074218d01b password 00074218d01b group cashiers
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
vlan	Specifies a VLAN to be used by members of a user group.

user-group

To define a user group for dynamically authenticating and enforcing security policies on a per user basis, use the **user-group** command in identity policy configuration mode. To delete the user-group, use the **no** form of this command.

user-group *group-name*

no user-group *group-name*

Syntax Description

<i>group-name</i>	Name of the user-group.
-------------------	-------------------------

Command Default

None

Command Modes

Identity policy configuration (config-identity policy)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **user-group** command is used if the Tag and Template method of user-group support is used. The Tag and Template method associates IP addresses with user-groups using locally defined policies. A tag is received from the access control server (ACS), and this tag matches a template (identity policy with defined user-group) on the network access device (NAD).

To use the **user-group** command, you must first enter identity policy configuration mode by using the **identity policy** command. The identity policy defines one or more user-groups, to which source IP addresses are associated.



Note

Another method of user-group association is available. User-group support can be achieved by configuring the supplicant-group attribute on the ACS.

Examples

The following example creates the identity policy “auth_proxy_ip” and configures the user-group “auth_proxy_ug”:

```
Router(config)# identity policy auth_proxy_ip
Router(config-identity-policy)# user-group auth_proxy_ug
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
identity policy	Creates an identity policy.

user-group logging

To enable user-group syslogs, use the **user-group logging** command in global configuration mode. To disable user-group syslogs, use the **no** form of this command.

user-group logging [**group** *group-name*]

no user-group logging [**group** *group-name*]

Syntax Description

group	(Optional) Configures logging for a specific user group.
<i>group-name</i>	(Optional) Name of the user-group.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example enables syslogs for the user-group “auth_proxy_ug”:

```
Router(config)# user-group logging group auth_proxy_ug
```

Related Commands

Command	Description
user-group	Creates a user-group for dynamically authenticating and enforcing security policies on a per user basis

username

To establish a username-based authentication system, use the **username** command in global configuration mode. Use the **no** form of this command to remove an established username-based authentication.

username *name* {**nopassword** | **password** *password* | **password** *encryption-type* *encrypted-password*}

username *name* **one-time** {**password** {**0** | **7** | *password*} | **secret** {**0** | **5** | *password*}}

username *name* **password** *secret*

username *name* [**access-class** *number*]

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]

username *name* **dnis**

username *name* [**nocallback-verify**]

username *name* [**noescape**]

username *name* [**nohangup**]

one-time {**password** {**0** | **7** | *password*} | **secret** {**0** | **5** | *password*}}

username *name* [**privilege** *level*]

username *name* [**secret** {**0** | **5** | *password*}]

username *name* **user-maxlinks** *number*

username [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*

no username *name*

Syntax Description

<i>name</i>	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
nopassword	No password is required for this user to log in. This is usually most useful in combination with the autocommand keyword.
one-time	Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations.
secret	Specifies a secret for the user.

0	Specifies that an unencrypted password or secret (depending on the configuration) follows.
5	Specifies that a hidden secret follows.
7	Specifies that a hidden password follows.
password	Specifies a possibly encrypted password for this username.
<i>password</i>	Specifies the password a user enters.
<i>encryption-type</i>	Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
<i>encrypted-password</i>	Encrypted password a user enters.
password	Password to access the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
<i>secret</i>	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
access-class	(Optional) Specifies an outgoing access list that overrides the access list specified in the access-class line configuration command. It is used for the duration of the user's session.
<i>number</i>	(Optional) Access list number.
autocommand	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
<i>command</i>	(Optional) The command string. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
callback-dialstring	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
<i>telephone-number</i>	(Optional) For asynchronous callback only: telephone number to pass to the DCE device.
callback-rotary	(Optional) For asynchronous callback only: permits you to specify a rotary group number. The next available line in the rotary group is selected.
<i>rotary-group-number</i>	(Optional) For asynchronous callback only: integer between 1 and 100 that identifies the group of lines on which you want to enable a specific username for callback.
callback-line	(Optional) For asynchronous callback only: specific line on which you enable a specific username for callback.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
<i>line-number</i>	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you want to enable a specific username for callback. Numbering begins with zero.

<i>ending-line-number</i>	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as tty), then <i>line-number</i> and <i>ending-line-number</i> are absolute rather than relative line numbers.
dnis	Do not require password when obtained via DNIS.
nocallback-verify	(Optional) Authentication not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the autocommand keyword) has completed. Instead, the user gets another EXEC prompt.
privilege	(Optional) Sets the privilege level for the user.
<i>level</i>	(Optional) Number between 0 and 15 that specifies the privilege level for the user.
user-maxlinks	Limit the user's number of inbound links.
<i>number</i>	User-maxlinks limit for inbound links.
lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
<i>name</i>	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
privilege	(Optional) Sets the privilege level for the user.
<i>privilege-level</i>	(Optional) Number between 0 and 15 that specifies the privilege level for the user.
view	(Optional) For command-line interface (CLI) view only: associates a CLI view name with the local authentication, authorization, and accounting (AAA) database.
<i>view-name</i>	(Optional) For CLI view only: view name, which was specified via the parser view command, that is to be associated with the AAA local database.
password <i>password</i>	Password to access the CLI view.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	11.1	The following keywords and arguments were added: <ul style="list-style-type: none"> • username <i>name</i> [callback-dialstring <i>telephone-number</i>] • username <i>name</i> [callback-rotary <i>rotary-group-number</i>] • username <i>name</i> [callback-line [tty] <i>line-number</i> [<i>ending-line-number</i>]] • username <i>name</i> [nocallback-verify]
	12.3(7)T	The following keywords and arguments were added: <ul style="list-style-type: none"> • lawful-intercept • view • <i>view-name</i>
	12.2(33)SRB	The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SRB: <ul style="list-style-type: none"> • lawful-intercept • view • <i>view-name</i>
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SB	The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SB: <ul style="list-style-type: none"> • lawful-intercept • view • <i>view-name</i>
	12.4	The following keywords and arguments were integrated into Cisco IOS Release 12.4: <ul style="list-style-type: none"> • one-time • secret • Keywords 0, 5, 7

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for the Challenge Handshake Authentication Protocol (CHAP). Add a username entry for each remote system from which the local router requires authentication.

**Note**

To enable the local router to respond to remote CHAP challenges, one **username name** entry must be the same as the **hostname** entry that has already been assigned to the other router.

**Note**

To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).

**Note**

Per-user privilege levels override virtual terminal (VTY) privilege levels.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If there is no *secret* specified and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. CHAP debugging information is available using the **debug ppp negotiation**, **debug serial-interface**, and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example implements a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example implements an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example implements an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example enables CHAP on interface serial 0 of “server_1.” It also defines a password for a remote server named “server_r.”

```
hostname server_1
username server_r password theirsystem
interface serial 0
  encapsulation ppp
  ppp authentication chap
```

When you look at your configuration file, the passwords will be encrypted, and the display will look similar to the following:

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

In both of the following configuration examples, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco

username user 2 privilege 2 password 0 cisco
```

The following example removes the username-based authentication for user 2:

```
no username user 2
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

username (dot1x credentials)

To specify the username for an 802.1X credentials profile, use the **username** command in dot1x credentials configuration mode. To remove the username, use the **no** form of this command.

username *name*

no username

Syntax Description

<i>name</i>	Name of the credentials profile.
-------------	----------------------------------

Command Default

A username is not specified.

Command Modes

Dot1x credentials configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

Examples

The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
username router
password secret
description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
dot1x credentials basic-user
dot1x pae supplicant
```

Related Commands

Command	Description
dot1x credentials	Specifies an 802.1X credentials profile to be used.

username (ips-autoupdate)

To define a username and password in which to access signature files from the server, use the **username** command in IPS-auto-update configuration mode.

```
username name password password
```

Syntax Description

<i>name</i>	Username required to access the latest updated signature file package.
password <i>password</i>	Password required to access the latest updated signature file package.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, you can optionally issue the **username** command to specify a username and password to access signature files.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration:

```
Router# clock set ?
      hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)# ^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update
```

```
IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
  hours (0-23) : 0-23
  days of month (1-31) : 1-31
  days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

username secret

To encrypt a user password with message digest algorithm 5 (MD5) encryption, use the **username secret** command in global configuration mode.

All Platforms Except the Cisco 7600 Series Router

```
username name secret {[0] password | 5 encrypted-secret}
```

Cisco 7600 Series Router

```
username name secret {0 | 5} password
```

Syntax Description

<i>name</i>	Username.
0	(Optional) For all platforms except the Cisco 7600 series router, specifies that the clear-text password immediately following this value is MD5 encrypted. For the Cisco 7600 series router, specifies that the clear-text password immediately following this value is not encrypted.
<i>password</i>	Clear-text password.
5 encrypted-secret	MD5-encrypted text string, which will be stored as the encrypted user password.
5	For the Cisco 7600 series router, specifies that the clear-text password immediately following this value is encrypted using an MD5-type encryption method.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines**All Platforms Except the Cisco 7600 Series Router**

Use the **username secret** command to configure a username and MD5-encrypted user password. The optional **0** keyword enables MD5 encryption on a clear-text password; the **5** keyword enters an MD5 encryption string and saves it as the user MD5-encrypted secret. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear-text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using nonreversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Cisco 7600 Series Router

Use this command to enable Enhanced Password Security for the specified, unretrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols, such as CHAP, that require clear-text passwords.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an “info” username that does not require a password but connects the user to a general-purpose information service.

The **username** command provides username and/or secret authentication for login purposes only. The *name* argument can be one word only. Spaces and quotation marks are not allowed. You can use multiple **username** commands to specify options for a single user.

Examples**All Platforms Except the Cisco 7600 Series Router**

The following example shows how to configure username “abc” and enable MD5 encryption on the clear-text password “xyz”:

```
username abc secret xyz
```

The following example shows how to configure username “cde” and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Cisco 7600 Router

The following example shows how to configure username “xyz” and enter an MD5 encrypted text string that is stored as the username password:

```
username xyz secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.

user-profile location

To store user bookmarks in a directory on a device, use the **user-profile location** command in webvpn context configuration mode. To remove a directory that has been configured, use the **no** form of this command.

user-profile location device:*directory*

no user-profile location device:*directory*

Syntax Description

device:	Storage location on a device. See Table 182 for a list of acceptable storage locations.
<i>directory</i>	Name of the directory.

Command Default

The default location is flash:/webvpn/<context-name>/.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

[Table 182](#) lists accept storage locations.

Table 182 Type of Storage Location

Type of Storage Location	Description
archive	Archived file system.
Bootflash	Bootflash memory.
disk0	On Disk 0.
disk1	On Disk 1.
Flash	Flash memory.
FTP	FTP network server.
HTTP	HTTP file server.
HTTPS	HTTP secure server.
null	Null destination for copies. You can copy a remote file to null to determine its size.
NVRAM	Storage location is in NVRAM.
PRAM	Phase-change memory (PRAM)—type of nonvolatile computer memory.

Table 182 *Type of Storage Location (continued)*

Type of Storage Location	Description
RCP	Remote copy protocol network server.
SCP	Secure Copy—A means of securely transferring computer files between a local and a remote host or between two remote hosts using the Secure Shell (SSH) protocol.
slot0	On Slot 0.
slot1	On Slot 1.
system	System memory, including the running configuration.
tmsys	Temporary system in a file system.

Examples

The following example shows bookmarks are stored in flash on the directory `webvpn/sslvpn_context/`.

```
Router# webvpn context context1
Router# user-profile location flash:/webvpn/sslvpn_context/
```

Related Commands

Command	Description
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

view

To add a normal command-line interface (CLI) view to a superview, use the **view** command in view configuration mode. To remove a CLI view from a superview, use the **no** form of this command.

view *view-name*

no view *view-name*

Syntax Description	<i>view-name</i>	CLI view that is to be added to the given superview.
--------------------	------------------	--

Defaults	A superview will not contain any CLI views until this command is enabled.
----------	---

Command Modes	View configuration
---------------	--------------------

Command History	Release	Modification
	12.3(11)T	This command was introduced.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines	Before you can use this command to add normal views to a superview, ensure that the following steps have been taken:
------------------	--

- A password has been configured for the superview (via the **secret 5** command).
- The normal views that are to be added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples	The following sample output from the show running-config command shows that “view_one” and “view_two” have been added to superview “su_view1,” and “view_three” and “view_four” have been added to superview “su_view2”:
----------	---

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.

vlan (local RADIUS server group)

To specify a VLAN to be used by members of the user group, use the **vlan** command in local RADIUS server group configuration mode. To reset the parameter to the default value, use the **no** form of this command.

vlan *vlan*

no vlan *vlan*

Syntax Description

<i>vlan</i>	VLAN ID.
-------------	----------

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The access point or router moves group members into the VLAN that you specify, overriding any other VLAN assignments. You can assign only one VLAN to a user group.

Examples

The following example shows that VLAN “225” is to be used by members of the user group:

```
vlan 225
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.

Command	Description
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

<i>group-name</i>	VLAN group name.
<i>vlan-list</i>	VLAN list name. See the “Usage Guidelines” section for additional information about the <i>vlan-list</i> argument.

Defaults

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXII	This command was introduced.

Usage Guidelines

The VLAN group name may contain up to 32 characters and must begin with a letter.

The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Router(config)# vlan group ganymede vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Router(config)# no vlan group ganymede vlan-list 7
```

Related Commands

Command	Description
show vlan group	Displays the VLANs mapped to VLAN groups.

vpng aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpng aaa attribute** command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

```
vpng aaa attribute {nas-ip-address vpng-nas | nas-port {vpng-nas | physical-channel-id}}
```

```
no vpng aaa attribute {nas-ip-address vpng-nas | nas-port}
```

Syntax Description	nas-ip-address vpng-nas	Enables reporting of the VPDN NAS IP address to the AAA server.
	nas-port vpng-nas	Enables reporting of the VPDN NAS port to the AAA server.
	nas-port physical-channel-id	Enables reporting of the VPDN NAS port physical channel identifier to the AAA server.

Command Default AAA attributes are not reported to the AAA server.

Command Modes Global configuration

Command History	Release	Modification
	11.3NA	This command was introduced.
	11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.
	12.1(5)T	This command was modified to support the PPP extended NAS-Port format.
	12.2(13)T	Support was added for the physical-channel-id keyword.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d** keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

**Note**

Reporting of NAS AAA attributes related to a VPDN on a AAA server is not supported for Point-to-Point Tunneling Protocol (PPTP) sessions with multihop deployment.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpdn enable
vpdn-group 1
  accept-dialin
  protocol any
  virtual-template 1
!
  terminate-from hostname nas1
  local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
vpdn aaa attribute nas-port physical-channel-id
```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```
vpdn enable
vpdn-group L2TP-tunnel
  accept-dialin
  protocol l2tp
  virtual-template 1
!
  terminate-from hostname nas1
  local name ts1
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 172.16.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vrf (isakmp profile)

To define the virtual routing and forwarding (VRF) value to which the IP Security (IPSec) tunnel will be mapped, use the **vrf** command in Internet Security Association Key Management (ISAKMP) profile configuration mode. To disable the VRF that was defined, use the **no** form of this command.

```
vrf ivrf
```

```
no vrf ivrf
```

Syntax Description

<i>ivrf</i>	VRF to which the IPSec tunnel will be mapped.
-------------	---

Defaults

The VRF will be the same as the front door VRF (FVRF).

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to map IPSec tunnels that terminate on a global interface to a specific Virtual Private Network (VPN).

If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to a Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.

If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange [IKE] main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

Examples

The following example shows that two IPSec tunnels to VPN 1 and VPN 2 are terminated:

```
crypto isakmp profile vpn1
  vrf vpn1
  keyring vpn1
  match identity address 172.16.1.1 255.255.255.255
crypto isakmp profile vpn2
  vrf vpn2
  keyring vpn2
  match identity address 10.1.1.1 255.255.255.255
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
```

```
crypto map crypmap 1 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set vpn1
  set isakmp-profile vpn1
  match address 101
crypto map crypmap 3 ipsec-isakmp
  set peer 10.1.1.1
  set transform-set vpn2
  set isakmp-profile vpn2
  match address 102
!
!
interface Ethernet1/2
  ip address 172.26.1.1 255.255.255.0
  duplex half
  no keepalive
  no cdp enable
  crypto map crypmap
```

vrfname

To associate a Virtual Private Network (VPN) front-door routing and forwarding instance (FVRF) with a SSL VPN gateway, use the **vrfname** command in webvpn gateway configuration mode. To disassociate the FVRF from the SSL VPN gateway, use the **no** form of this command.

vrfname *name*

no vrfname *name*

Syntax Description	<i>name</i>	Name of the VRF.
---------------------------	-------------	------------------

Command Default	A VPN FVRF is not associated with a SSL VPN gateway.	
------------------------	--	--

Command Modes	Webvpn gateway (config-webvpn-gateway)	
----------------------	--	--

Command History	Release	Modification
	12.4(15)T	This command was introduced.

Usage Guidelines	Only one FVRF can be associated with each SSL VPN context configuration.	
-------------------------	--	--

Examples	The following example shows FVRF has been configured:	
-----------------	---	--

```
Router (config) ip vrf vrf_1
Router (config-vrf) end
Router (config) webvpn gateway mygateway
Router (config-webvpn-gateway) vrfname vrf_1
Router (config-webvpn-gateway) end
```

Related Commands	Command	Description
		webvpn gateway

vrf-name

To associate a Virtual Private Network (VPN) routing and forwarding instance (VRF) with a SSL VPN context, use the **vrf-name** command in webvpn context configuration mode. To remove the VRF from the WebVPN context configuration, use the **no** form of this command.

vrf-name *name*

no vrf-name

Syntax Description

<i>name</i>	Name of the VRF.
-------------	------------------

Command Default

A VPN VRF is not associated with a SSL VPN context.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The VRF is first defined in global configuration mode. Only one VRF can be associated with each SSL VPN context configuration.

Examples

The following example associates a VRF with a SSL VPN context:

```
Router (config)# ip vrf BLUE
Router (config-vrf)# rd 10.100.100.1
Router (config-vrf)# webvpn context context1
Router (config-webvpn-context)# vrf-name BLUE
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

web-agent-url

To configure the Netegrity agent URL to which Single SignOn (SSO) authentication requests will be dispatched, use the **web-agent-url** command in webvpn sso server configuration mode. To remove the Netegrity agent URL, use the **no** form of this command.

web-agent-url *url*

no web-agent-url *url*

Syntax Description

<i>url</i>	URL to which SSO authentication requests will be dispatched.
------------	--

Command Default

Authentication requests will not be dispatched to a Netegrity agent URL.

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines



Note

A web agent URL and policy server secret key are required for a SSO server configuration. If they are not configured, a warning message is displayed. (See the warning message information in the Examples section below.)

Examples

The following example shows that SSO authentication requests will be dispatched to the URL `http://www.example.com/webvpn/`:

```
webvpn context context1
  sso-server test-sso-server
    web-agent-url http://www.example.com/webvpn/
```

Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server "example"
Warning: must configure SSO policy server secret key for sso-server "example"
Warning: invalid configuration. SSO for "example" being disabled
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

webvpn



Note

Effective with Cisco IOS Release 12.4(6)T, the **webvpn** command is replaced by the **webvpn context** and **webvpn gateway** commands. See the these commands for more information.

To enter Web VPN configuration mode, use the **webvpn** command in global configuration mode. To remove all commands that were entered in Web VPN configuration mode, use the **no** form of this command.

webvpn

no webvpn

Syntax Description

This command has no arguments or keywords.

Defaults

Web VPN configuration mode is not entered.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the webvpn context and webvpn gateway commands.

Examples

The following example shows that Web VPN configuration mode has been entered:

```
Router (config)# webvpn
Router (config-webvpn)#
```

Related Commands

Command	Description
webvpn enable	Enables WebVPN in the system.

webvpn cef

To enable Secure Socket Layer virtual private network (SSL VPN) full-tunnel Cisco Express Forwarding (CEF) support, use the **webvpn cef** command in global configuration mode. To disable full-tunnel CEF support, use the **no** form of this command.

webvpn cef

no webvpn cef

Syntax Description There are no arguments or keywords.

Command Default This command is set by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.4(20)T	This command was introduced.

Usage Guidelines IP CEF must be turned on before this command can take effect.

Examples The following example shows that full-tunnel CEF is being disabled:

```
Router (config)# no webvpn cef
```

Related Commands	Command	Description
	ip cef	Enables CEF on the route processor card.

webvpn context

To enter webvpn context configuration mode to configure the Secure Sockets Layer Virtual Private Network (SSL VPN) context, use the **webvpn context** command in global configuration mode. To remove the SSL VPN configuration from the router configuration file, use the **no** form of this command.

webvpn context *name*

no webvpn context *name*

Syntax Description

<i>name</i>	Name of the SSL VPN context configuration.
-------------	--

Command Default

Webvpn context configuration mode is not entered, and a SSL VPN context is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The SSL VPN context defines the central configuration of the SSL VPN. Entering the **webvpn context** command places the router in webvpn context configuration mode.



Note

The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while a SSL VPN gateway is in an enabled state (in service).

Examples

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# inservice
```

Related Commands

Command	Description
aaa authentication (WebVPN)	Configures AAA authentication for SSL VPN sessions.
csd enable	Enables CSD support for SSL VPN sessions.
default-group-policy	Specifies a default group policy for SSL VPN sessions.
gateway (WebVPN)	Specifies the gateway for SSL VPN sessions.
inservice	Enables a SSL VPN gateway or context process.
login-message	Configures a message for a user login text box on the login page.

Command	Description
logo	Configures a custom logo to be displayed on the login and portal pages of a SSL VPN website.
max-users (WebVPN)	Limits the number of connections to a SSL VPN that will be permitted
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
policy group	Enters a webvpn group policy configuration mode to configure a group policy.
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
secondary-color	Configures the color of the secondary title bars on the login and portal pages of a SSL VPN website.
secondary-text-color	Configures the color of the text on the secondary bars of a SSL VPN website.
title	Configures the HTML title string that is shown in the browser title and on the title bar of a SSL VPN website.
title-color	Configures the color of the title bars on the login and portal pages of a SSL VPN website.
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.
vrf-name	Associates a VRF with a SSL VPN context.

webvpn create template

To create templates for multilanguage support for messages initiated by the head-end in a Secure Socket Layer Virtual Private Network (SSL VPN), configure the **webvpn create template** command in user EXEC or privileged EXEC mode.

webvpn create template {**browser-attribute** | **language** | **url-list**} *device*:

Syntax Description	Parameter	Description
	browser-attribute	Creates a template file named “battr_tpl.xml”.
	language	Creates a template file named “lang.js”.
	url-list	Creates a template file named “url_list_tpl.xml”.
	<i>device</i> :	Storage device on the system for the templates, such as flash: or disk0.

Command Default Template files are not created.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	12.4(22)T	This command was introduced.

Usage Guidelines After template files have been created, they can be copied to a PC for editing and then reimported to the storage device.

Examples The following example shows that a browser-attribute template file is to be created in flash:

```
Router# webvpn create template browser-attribute flash:
```

The following example shows that the language file is to be created in flash:

```
Router# webvpn create template language flash:
```

The following example shows that a URL list template is to be created in flash:

```
Router# webvpn create template url-list flash:
```

Related Commands	Command	Description
	browser-attribute import	Imports user-defined browser attributes into a webvpn context.
	import	Imports a user-defined URL list into a webvpn context.

Command	Description
language	Specifies the language to be used in a webvpn context.
url-list	Enters webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a SSL VPN and attaches the URL list to a policy group.

webvpn enable



Note

Effective with Cisco IOS Release 12.4(6)T, the **webvpn enable** command is replaced by the **inservice** command. See the **inservice** command for more information.

To enable WebVPN in the system, use the **webvpn enable** command in global configuration mode. To disable WebVPN in the system, use the **no** form of this command.

```
webvpn enable [gateway-addr ip-address]
```

```
no webvpn enable [gateway-addr ip-address]
```

Syntax Description

gateway-addr <i>ip-address</i>	(Optional) Enables WebVPN on only the IP address that is specified. If this keyword and argument are not configured, WebVPN is enabled globally on all IP addresses.
--	--

Defaults

WebVPN is disabled in the system.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the inservice command.

Usage Guidelines

This command initializes the required system data structures, initializes TCP sockets, and performs other startup tasks related to WebVPN.

Examples

The following example shows that WebVPN has been enabled in the system:

```
webvpn enable
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

webvpn gateway

To enter webvpn gateway configuration mode to configure a SSL VPN gateway, use the **webvpn gateway** command in global configuration mode. To remove the SSL VPN gateway from the router configuration file, use the **no** form of this command.

webvpn gateway *name*

no webvpn gateway *name*

Syntax Description

<i>name</i>	Name of the virtual gateway service.
-------------	--------------------------------------

Command Default

Webvpn gateway configuration mode is not entered, and a SSL VPN gateway is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering the **webvpn gateway** command places the router in webvpn gateway configuration mode. Configuration settings specific to the SSL VPN gateway are entered in this configuration mode.

The SSL VPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through a secure encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer.

The gateway is configured using an IP address at which SSL VPN remote-user sessions terminate. The gateway is not active until the **inservice** command has been entered in SSL VPN gateway configuration mode. Only one gateway can be configured in a SSL VPN-enabled network.

Examples

The following example creates and enables a SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ip address 10.1.1.1 port 443
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN
Router(config-webvpn-gateway)# http-redirect 80
Router(config-webvpn-gateway)# inservice
```

Related Commands

Command	Description
hostname (WebVPN)	Configures a SSL VPN hostname.
http-redirect	Configures HTTP traffic to be carried over HTTPS.
inservice	Enables a SSL VPN gateway or context process.
ip address (WebVPN)	Configures a proxy IP address on a SSL VPN gateway.

Command	Description
ssl encryption	Configures the specify the encryption algorithms that the SSL protocol will use for an SSL VPN.
ssl trustpoint	Configures the certificate trust point on a SSL VPN gateway.

webvpn install

To install a Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN Client package file to a Secure Socket Layer virtual private network (SSL VPN) gateway for distribution to end users, use the **webvpn install** command in global configuration mode. To remove a package file from the SSL VPN gateway, use the **no** form of this command.

webvpn install [*csd location-name* | *svc location-name* [**sequence** *sequence-number*]]

no webvpn install [*csd location-name* | *svc location-name* [**sequence** *sequence-number*]]

Syntax Description

csd <i>location-name</i>	(Optional) Installs the CSD client software package. The filename and path are entered.
svc <i>location-name</i>	(Optional) Installs the Cisco AnyConnect VPN Client software package. The filename and path are entered.
sequence <i>sequence-number</i>	(Optional) Allows for multiple packages to be installed to one gateway. If the sequence keyword and the <i>sequence-number</i> argument are not configured, a sequence number of 1 is applied to the package.

Command Default

Neither a CSD nor a Cisco AnyConnect VPN Client package file is installed to a WebVPN gateway.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	The sequence <i>sequence-number</i> keyword and argument were added.

Usage Guidelines

The installation packages must first be copied to a local file system, such as disk, flash or USB flash. The CSD and Cisco AnyConnect VPN Client software packages are pushed to end users as access is needed. The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or a later version must be installed before a CSD or Cisco AnyConnect VPN Client package can be installed.



Note Secure Sockets Layer Virtual Private Network (SSL VPN) Client (SVC) is the predecessor of Cisco AnyConnect VPN Client software.

If you have not entered the **sequence** keyword and the *sequence-number* argument and you want to install another package, you can remove the previous package (using the **no** form of the command) or you can provide another sequence number.

If you try to install a package with a sequence number that is being used, you will get an error message.

Examples

The following example shows how to install the Cisco AnyConnect VPN Client package to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg
```

```
SSLVPN Package SSL-VPN-Client : installed successfully
```

The following example shows how to install the CSD package to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg
```

```
SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

The following example shows how to install Cisco AnyConnect VPN Client package to an SSL VPN gateway. The file is being copied to a USB file system.

```
Router(config)# webvpn install csd usbflash0:securedesktop-ios-3.1.1.45-k9.pkg
```

```
SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

Related Commands

Command	Description
show webvpn install status	Displays the installation status of SVC or CSD client software packages.

webvpn sslvpn-vif nat

To enable Network Address Translation (NAT) on the WebVPN virtual interface, use the **webvpn sslvpn-vif nat** command in global configuration mode. To disable NAT on the WebVPN virtual interface, use the **no** form of this command.

```
webvpn sslvpn-vif nat {enable | inside | outside}
```

```
no webvpn sslvpn-vif nat {enable | inside | outside}
```

Syntax Description

enable	Enables address translation.
inside	Enables the inside interface for address translation.
outside	Enables the outside interface for address translation.

Command Default

NAT is disabled by default on the WebVPN virtual interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **show running-config** command to verify if NAT has been enabled.

Examples

The following example shows that NAT has been enabled on the WebVPN virtual interface:

```
Router(config)# webvpn sslvpn-vif nat enable
```

wins

Command	Description
show running-config	Displays the contents of the current running configuration file.

To specify the primary and secondary Windows Internet Naming Service (WINS) servers, use the **wins** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

wins *primary-server secondary-server*

no wins *primary-server secondary-server*

Syntax Description

<i>primary-server</i>	Name of the primary WINS server.
<i>secondary-server</i>	Name of the secondary WINS server.

Defaults

No default behavior or values.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **wins** command.

Examples

The following example shows how to define a primary and secondary WINS server for the group “cisco”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  wins 10.1.1.2 10.1.1.3
```

Related Commands	Command	Description
	acl	Configures split tunneling.
	crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

wlccp authentication-server client

To configure the list of servers to be used for 802.1X authentication, use the **wlccp authentication-server client** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server client {any | eap | leap | mac} *list*

no wlccp authentication-server client {any | eap | leap | mac} *list*

Syntax Description

any	Specifies client devices that use any authentication.
eap	Specifies client devices that use Extensible Authentication Protocol (EAP) authentication.
leap	Specifies client devices that use Light Extensible Authentication Protocol (LEAP) authentication.
mac	Specifies client devices that use MAC-based authentication.
<i>list</i>	List of client devices.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can specify a list of client devices that use any type of authentication, or you can specify a list of client devices that use a certain type of authentication (such as EAP, LEAP, or MAC-based authentication).

Examples

The following example shows how to configure the server list for LEAP authentication for client devices:

```
Router (config)# wlccp authentication-server client leap leap-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.

Command	Description
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp authentication-server infrastructure

To configure the list of servers to be used for 802.1X authentication for the wireless infrastructure devices, use the **wlccp authentication-server infrastructure** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server infrastructure *list*

no wlccp authentication-server infrastructure *list*

Syntax Description	<i>list</i>	List of servers to be used for 802.1X authentication for the wireless infrastructure devices, such as access points, repeaters, and wireless-aware routers.
Defaults	No default behavior or values	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(11)JA	This command was introduced on Cisco Aironet access points.
	12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.
Examples	<p>This example shows how to configure the server list for 802.1X authentication for infrastructure devices participating in Cisco Centralized Key Management:</p> <pre>Router (config)# wlccp authentication-server infrastructure wlan-list1</pre>	
Related Commands	Command	Description
	debug wlccp packet	Displays packet traffic to and from the WDS router.
	debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
	show wlccp wds	Shows information about access points and client devices on the WDS router.
	wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
	wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp wds priority interface

To configure the router or access point to provide WDS, use the **wlccp wds priority interface** command in global configuration mode. To remove the WDS configuration from the router or access point, use the **no** form of the command .

wlccp wds priority *priority* **interface** *interface*

no wlccp wds priority *priority* **interface** *interface*

Syntax Description

<i>priority</i>	Priority of this WDS candidate. The valid range is from 1 to 255. The greater the priority value, the higher the priority.
<i>interface</i>	Interface on which the router sends out WDS advertisements. Supported interface types are as follows: <ul style="list-style-type: none"> • For access points—bvi • For wireless-aware routers—bvi, svi, Fast Ethernet, and Gigabit Ethernet.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced with support for Cisco Aironet access points.
12.3(11T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The WDS candidate with the highest priority becomes the active WDS device.

Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS with priority 200:

```
Router (config)# wlccp wds priority 200 interface bvi 1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.

Command	Description
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.

xauth userid mode

To specify how the Easy VPN client handles extended authentication (Xauth) requests, use the **xauth userid mode** command in Cisco IOS Easy VPN remote configuration mode. To remove the setting, use the **no** form of this command.

```
xauth userid mode {http-intercept | interactive | local}
```

```
no xauth userid mode {http-intercept | interactive | local}
```

Syntax Description	http-intercept	HTTP connections are intercepted from the user through the inside interface and the prompt.
	interactive	To authenticate, the user must use the command-line interface (CLI) prompts on the console. Interactive is the default behavior.
	local	The saved username or password is used in the configuration.

Defaults If the command is not configured, the default behavior is interactive.

Command Modes Cisco IOS Easy VPN remote configuration (config-crypto-ezvpn)

Command History	Release	Modification
	12.3(14)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines If you want to be prompted by the console, use the **interactive** keyword. If you want to use a saved username or password, use the **local** keyword. If a local username or password is defined, the mode changes to that username or password.

Examples The following example shows that HTTP connections will be intercepted from the user and that the user can authenticate using web-based activation:

```
crypto ipsec client ezvpn tunnel22
  connect manual
  group tunnel22 key 22tunnel
  mode client
  peer 192.168.0.1
  xauth userid mode http-intercept
!
!
interface Ethernet0
  ip address 10.4.23.15 255.0.0.0
```

```

crypto ipsec client ezvpn tunnel22 inside !
interface Ethernet1
 ip address 192.168.0.13 255.255.255.128
 duplex auto
 crypto ipsec client ezvpn catch22
!
```

Related Commands

Command	Description
crypto ipsec client ezvpn	Creates a Cisco Easy VPN remote configuration.
debug crypto ipsec client ezvpn	Displays information about voice control messages that have been captured by the Voice DSP Control Message Logger.
debug ip auth-proxy ezvpn	Displays information related to proxy authentication behavior for web-based activation.
show crypto ipsec client ezvpn	Displays the Cisco Easy VPN Remote configuration.
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

zone-member security

To attach an interface to a security zone, use the **zone-member security** command in interface configuration mode. To detach the interface from a zone, use the **no** form of this command.

```
zone-member security zone_name
```

```
no zone-member security zone_name
```

Syntax Description	<i>zone_name</i>	Name of the security zone to which an interface is attached.
---------------------------	------------------	--

Command Default	None
------------------------	------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	The zone-member security command puts an interface into a security zone. When an interface is in a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped by default. To permit traffic through an interface that is a zone member, you must make that zone part of a zone-pair to which you apply a policy. If the policy permits traffic (via inspect or pass actions), traffic can flow through the interface.
-------------------------	--

Examples	The following example attaches interface e0 to the zone z1:
-----------------	---

```
interface e0
  zone-member security z1
```

Related Commands	Command	Description
	zone security	Creates a zone.

zone-pair security

To create a zone-pair, use the **zone-pair security** command in global configuration mode. To delete a zone-pair, use the **no** form of this command.

```
zone-pair security zone-pair-name {source source-zone-name | self} destination [self | destination-zone-name]
```

```
no zone-pair security zone-pair-name {source source-zone-name | self } destination [self | destination-zone-name]
```

Syntax Description

<i>zone-pair-name</i>	Name of the zone being attached to an interface.
source <i>source-zone-name</i>	Name of the router from which traffic is originating.
destination <i>destination-zone-name</i>	Name of the router from which traffic is bound.
self	System-defined zone. Indicates whether traffic will be going to or from a router.

Command Default

A zone-pair is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command creates a zone-pair, which permits a unidirectional firewall policy between a pair of security zones. After you enter this command, you can enter the submode command **service-policy type inspect**.

If you created only one zone, you can use the system-defined default zone (self) as part of a zone-pair. Such a zone-pair and its associated policy applies to traffic directed to the router or generated by the router. It does not affect traffic through the router.

You can specify the **self** keyword for the source or destination, but not for both. You can not modify or unconfigure the self zone.

Examples

The following example creates zones z1 and z2, identifies them, and creates a zone-pair where z1 is the source and z2 is the destination:

```
zone security z1
description finance department networks

zone security z2
description engineering services network
```

```
zone-pair security zp source z1 destination z2
```

```
zone-pair security
```

The following example defines zone-pair z1-z2 and attaches the service policy p1 to the zone-pair:

```
zone-pair security zp source z1 destination z2
service-policy type inspect p1
```

Related Commands

Command	Description
service-policy type inspect	Attaches a firewall policy to a zone-pair.
zone-pair	Creates a zone-pair.

zone security

To create a security zone, use the **zone security** command in global configuration mode. To delete a security zone, use the **no** form of this command.

zone security *zone-name*

no zone security *zone-name*

Syntax Description	<i>zone-name</i>	Name of the security zone. You can enter up to 256 alphanumeric characters.
---------------------------	------------------	---

Command Default	There is a system-defined “self” zone.
------------------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	We recommend that you create at least two security zones so that you can create a zone pair. If you create only one zone, you can use the default system-defined self zone. The self zone cannot be used for traffic going through a router.
-------------------------	--

To configure an interface to be a member of a security zone, use the **zone-member security** command.

Examples	The following example creates and describes zones x1 and z1:
-----------------	--

```
zone security x1
  description testzonex

zone security z1
  description testzonez
```

Related Commands	Command	Description
	description (identify zone)	Contains a description of a zone.
	zone-member security	Attaches an interface to a zone.
	zone-pair security	Creates a zone-pair.