

ca authenticate

To allow the FWSM to authenticate its certification authority (CA) by obtaining the CA's self-signed certificate, which contains the CA's public key, use the **ca authenticate** command.

```
ca authenticate ca_nickname [fingerprint]
```

Syntax Description

<i>ca_nickname</i>	Name of the certification authority (CA).
<i>fingerprint</i>	(Optional) Key consisting of alphanumeric characters that the FWSM uses to authenticate the CA's certificate.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. If you previously declared the CA and want to update its characteristics, specify the name you previously created. The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

The FWSM supports the CA servers from VeriSign, Entrust, Baltimore Technologies, and Microsoft.

The certificate lifetime and the certificate revocation list (CRL) are checked in coordinated universal time (UTC). The FWSM clock is synchronized with the switch. This clock setting determines the certificate lifetime and revocation.

The FWSM authenticates the entity certificate (the device certificate). The FWSM assumes that the certificate is issued by the same trusted point or root (the CA server). As a result, the trusted point or root should have the same root certificate (issuer certificate). The FWSM assumes that the entity exchanges the entity certificate only and cannot process a certificate chain that includes both the entity and root certificates.

To authenticate a peer's certificate(s), the FWSM must obtain the CA certificate containing the CA public key. Because the CA certificate is a self-signed certificate, you should authenticate the key manually by contacting the CA administrator. You can authenticate the public key in that certificate by including the key's fingerprint within the **ca authenticate** command. The FWSM will discard the received CA certificate and generate an error message if the fingerprint that you specified is different from the received one. You can also compare the two fingerprints without entering the key within the command.

If you are using RA mode (within the **ca configure** command), when you issue the **ca authenticate** command, the RA signing and encryption certificates and the CA certificate are returned from the CA.

The **ca authenticate** command is not saved to the FWSM configuration. However, the public keys that are embedded in the received CA (and RA) certificates are saved in the configuration as part of the RSA public key record (called the “RSA public key chain”). To save the public keys permanently to the Flash partition, use the **ca save all** command. To see the CA’s certificate, use the **show ca certificate** command.

**Note**

If the CA does not respond by a timeout period after this command is entered, the terminal control is returned so that it is not tied up. In this situation, you must reenter the command.

Examples

This example shows that a request for the CA’s certificate was sent to the CA. The fingerprint was not included in the command. The CA sends its certificate and the FWSM prompts for verification of the CA’s certificate by checking the CA certificate’s fingerprint. If both fingerprints match, then the certificate is considered valid.

```
fwsm/context_name(config)# ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
```

This example shows the error message. The fingerprint is included in the command. The two fingerprints do not match, and therefore the certificate is not valid.

```
fwsm/context_name(config)# ca authenticate myca 0123456789ABCDEF0123
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 5432
%Error in verifying the received fingerprint. Type help or '?' for a list of
available commands.
```

Related Commands

show ca

ca configure

To specify the communication parameters between the FWSM and the CA, use the **ca configure** command. To return to the default settings, use the **no** form of this command.

```
[no] ca configure ca_nickname { ca | ra } retry_period retry_count [crloptional]
```

Syntax Description

<i>ca_nickname</i>	Name of the certification authority (CA).
ca	Contacts the CA.
ra	Contacts the registration authority (RA).
<i>retry_period</i>	Number of minutes that the FWSM waits before resending a certificate request to the CA when it does not receive a response from the CA to its previous request; valid values are from 1 to 60 minutes.
<i>retry_count</i>	How many times that the FWSM will resend a certificate request when it does not receive a certificate from the CA from the previous request; valid values are from 1 to 100.
crloptional	(Optional) Allows other peers' certificates to be accepted by the FWSM even if the appropriate certificate revocation list (CRL) is not accessible to the FWSM.

Defaults

The defaults are as follows:

- The *retry_period* is 1 minute.
- The *retry_count* is 0 (there is no limit to the number of times that the FWSM should contact the CA to obtain a pending certificate).
- The default is without the **crloptional** optional keyword.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. If you previously declared the CA and want to update its characteristics, specify the name that you previously created. The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

Examples

This example shows that *myca* is the name of the CA and that the CA is contacted rather than the RA. It also indicates that the FWSM will wait 5 minutes before sending another certificate request, if it does not receive a response, and will resend a total of 15 times before dropping its request. If the CRL is not accessible, **crloptional** tells the FWSM to accept other peer's certificates.

```
fwsm/context_name(config)# ca configure myca ca 5 15 crloptional
```

Related Commands

ca authenticate

show ca

ca crl request

To allow the FWSM to obtain an updated CRL from the CA at any time, use the **ca crl request** command. To delete the CRL from the FWSM, use the **no** form of this command.

[no] **ca crl request** *ca_nickname*

Syntax Description

<i>ca_nickname</i>	Name of the certification authority (CA).
--------------------	---

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. If you previously declared the CA and want to update its characteristics, specify the name you previously created. The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

A CRL lists all the network devices certificates that have been revoked. The FWSM will not accept revoked certificates; any peer with a revoked certificate cannot exchange IPsec traffic with the FWSM.

The first time that the FWSM receives a certificate from a peer, it downloads a CRL from the CA. The FWSM then checks the CRL to make sure that the peer's certificate has not been revoked. If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.

A CRL can be reused with subsequent certificates until the CRL expires. When the CRL expires, the FWSM automatically updates it by downloading a new CRL and replaces the expired CRL with the new CRL.

If the FWSM has a CRL that has not yet expired, but you suspect that the CRL's contents are out of date, use the **ca crl request** command to request that the latest CRL is downloaded to replace the old CRL.

The **ca crl request** command is not saved with the FWSM configuration between reloads.

The **show ca crl** command allows you to know whether there is a CRL in RAM, and where and when the CRL is downloaded.

Examples

This example shows how the FWSM obtains an updated CRL from the CA with the name myca:

```
fwsm/context_name(config)# ca crl request myca
```

Related Commands

ca authenticate

show ca

ca enroll

To send an enrollment request to the CA requesting a certificate for all of the FWSM's key pairs, use the **ca enroll** command. To cancel the current enrollment request, use the **no** form of this command.

```
[no] ca enroll ca_nickname challenge_password [serial] [ipaddress]
```

Syntax Description

<i>ca_nickname</i>	Name of the certification authority (CA).
<i>challenge_password</i>	Required password that gives the CA administrator some authentication when a user calls to ask for a certificate to be revoked; the password can be up to 80 characters.
serial	(Optional) Returns the FWSM's serial number in the certificate.
ipaddress	(Optional) Returns the FWSM's IP address in the certificate.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. (If you previously declared the CA and want to update its characteristics, specify the name that you previously created.) The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

You can use the **ca enroll** command to send an enrollment request to the CA requesting a certificate for all of the FWSM's key pairs. This action is also known as "enrolling" with the CA.

The FWSM needs a signed certificate from the CA for each of its RSA key pairs. If you previously generated general-purpose keys, entering the **ca enroll** command obtains one certificate corresponding to the one general-purpose RSA key pair. If you previously generated special usage keys, entering this command obtains two certificates corresponding to each of the special-usage RSA key pairs.

If you already have a certificate for the keys, you will not be able to complete this command; instead, you are prompted to remove the existing certificate first.

The **ca enroll** command is not saved with the FWSM configuration between reloads. To verify if the enrollment process succeeded and to display the FWSM's certificate, use the **show ca certificate** command.

The required challenge password is necessary in the event that you need to revoke the FWSM's certificate(s). When you ask the CA administrator to revoke the certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

**Note**

Do not forget the password; this password is not stored in memory anywhere.

If you lose the password, the CA administrator may still be able to revoke the FWSM's certificate but will require further manual authentication of the FWSM administrator identity.

The FWSM's serial number is optional. If you provide the **serial** optional keyword, the serial number is included in the obtained certificate. The serial number is not used by IPsec or Internet Key Exchange (IKE) but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular device. Ask the CA administrator if serial numbers should be included in the certificate. If you are in doubt, specify the **serial** optional keyword.

The FWSM's IP address is optional. If you enter the **ipaddress** optional keyword, the IP address is included in the obtained certificate. Normally, you do not include the **ipaddress** optional keyword because the IP address binds the certificate to a specific entity. If you move the FWSM, you need to issue a new certificate.

**Note**

When configuring ISAKMP for certificate-based authentication, you should match the ISAKMP identity type with the certificate type. Enter the **ca enroll** command to obtain a certificate with the identity based on the host name. Enter the **isakmp identity** command to obtain a certificate based on the address instead of the host name. You can reconcile this disparity of identity types by using the **isakmp identity address** command. See the **isakmp** command for information about the **isakmp identity address** command.

Examples

This example shows how the FWSM sends an enrollment request to the CA myca.example.com:

```
fwsM/context_name(config)# ca enroll myca.example.com 1234567890 serial
```

Related Commands

ca authenticate
show ca

ca generate rsa

To generate the RSA key pairs for your FWSM, use the **ca generate rsa** command.

```
ca generate rsa {key | specialkey} key_modulus_size
```

Syntax Description

key	Generates an RSA key for the FWSM.
specialkey	Generates two special-purpose RSA key pairs instead of one general-purpose key.
<i>key_modulus_size</i>	Modulus used to generate the RSA key in a size measured in bits; valid values are 512 , 768 , 1024 , and 2048 bits.



Note

Before using this command, make sure that your Firewall Services Module host name and domain name have been configured (using the **hostname** and **domain-name** commands). If a domain name is not configured, the FWSM uses a default domain of ciscopix.com.

Defaults

The defaults are as follows:

- The RSA key modulus default (during PDM setup) is **768**.
- The default domain is ciscofws.com.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

RSA keys are generated in pairs—one public RSA key and one private RSA key

If your FWSM already has RSA keys when you use this command, you are warned and prompted to replace the existing keys with new keys.



Note

The larger the key modulus size that you specify, the longer it takes to generate an RSA. We recommend a default value of 768.

PDM uses the Secure Socket Layer (SSL) communications protocol to communicate with the firewall.

SSL uses the private key generated with the **ca generate rsa** command. For a certificate, SSL uses the key obtained from a certification authority (CA). If that does not exist, it uses the FWSM self-signed certificate that was created when the RSA key pair was generated.

The **ca generate rsa** command is not saved in the FWSM configuration. However, the keys generated by this command are saved in a persistent data file in the Flash partition, which you can save with the **ca save all** command and view with the **show ca my rsa key** command.

Examples

This example shows how one general-purpose RSA key pair is generated. The selected size of the key modulus is 1024.

```
fws(config) ca generate rsa key 1024
Key name:firewall.cisco.com
Usage:General Purpose Key
Key Data:
 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c8ed4c
 9f5e0b52 aea931df 04db2872 5c4c0afd 9bd0920b 5e30de82 63d834ac f2e1db1f
1047481a 17be5a01 851835f6 18af8e22 45304d53 12584b9c 2f48fad5 31e1be5a
bb2ddc46 2841b63b f92cb3f9 8de7cb01 d7ea4057 7bb44b4c a64a9cf0 efaacd42
e291e4ea 67efbf6c 90348b75 320d7fd3 c573037a ddb2dde8 00df782c 39020301 0001
```

Related Commands show ca

ca identity

To declare the CA that the FWSM uses, use the **ca identity** command. To remove the **ca identity** command from the configuration and delete all the certificates that are issued by the specified CA and CRLs, use the **no** form of this command.

```
[no] ca identity ca_nickname [ca_ipaddress | hostname [:ca_script_location] [ldap_ip address |
hostname]]
```

Syntax Description

<i>ca_nickname</i>	Name of the certification authority (CA).
<i>ca_ipaddress</i>	(Optional) CA's IP address.
<i>hostname</i>	(Optional) Host name.
<i>:ca_script_location</i>	(Optional) Location and script on the CA server.
<i>ldap_ipaddress</i>	(Optional) IP address of the Lightweight Directory Access Protocol (LDAP) server.

Defaults

The defaults are as follows:

- *:ca_script_location*—The location and script on the CA server is `/cgi-bin/pkiclient.exe`.
- *ldap_ipaddress*—Querying of a certificate or a CRL is done through Cisco's PKI protocol.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If the CA supports LDAP, the query functions may also use LDAP.

The FWSM supports one CA at one time.

If the CA administrator has not put the CGI script in this location, you need to provide the location and the name of the script in the **ca identity** command.

The FWSM uses a subset of the HTTP protocol to contact the CA and must identify a particular cgi-bin script to handle CA requests. The default location and script on the CA server is `/cgi-bin/pkiclient.exe`. If the CA administrator has not put the CGI script in the previously listed location, you need to include the location and the name of the script within the **ca identity** command.

By default, querying a certificate or a CRL is done through the Cisco's PKI protocol. If the CA supports the Lightweight Directory Access Protocol (LDAP), the query functions may use LDAP. You must include the IP address of the LDAP server within the **ca identity** command.

Examples

This example shows that the CA myca.example.com is declared as the FWSM's supported CA. The CA's IP address of 205.139.94.231 is provided.

```
fwsM/context_name(config)# ca identity myca.example.com 205.139.94.231
```

Related Commands

show ca

ca save all

To save the FWSM's RSA key pairs, the CA, RA, and FWSM's certificates, and the CA's CRLs in the persistent data file in the Flash partition between reloads, use the **ca save all** command. To remove the saved data from the FWSM's Flash partition, use the **no** form of this command.

[no] **ca save all**

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The **ca save** command is not saved with the FWSM configuration between reloads. To see the current status of the requested certificates and relevant information of the received certificates, use the **show ca certificate** command. Because the certificates contain no sensitive data, any user can issue this **show** command.

Examples This command shows how to save the FWSM RSA key pairs:

```
fwsM/context_name(config)# ca save all
```

Related Commands **show ca**

ca subject-name

To create the device certificate with the subject distinguished name (DN), use the **ca subject-name** command. To remove the subject names, use the **no** form of this command.

[no] ca subject-name *ca_nickname* *X.500_string*

Syntax Description

<i>ca_nickname</i>	Name of the certification authority (CA).
<i>X.500_string</i>	Character string indicating the DN sent.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Specify the *X.500_string* using the RFC 1779 format.

The **ca subject-name** *ca_nickname* *X.500_string* command is a certificate enrollment enhancement that supports X.500 directory names.

When the **ca subject-name** *ca_nickname* *X.500_string* command is configured, the FWSM enrolls the device certificate with the subject DN that is specified in the *X.500_string* using the RFC 1779 format. The supported DN attributes are listed in [Table 2-4](#).

Table 2-4 Supported DN Attributes

Attribute	Description
ou	Organizational Unit Name
o	Organization Name
st	State or Province Name
c	Country Name
ea	E-mail address (a non-RFC 1779 format attribute)

For more information on RFC 1779, refer to <http://www.ietf.org/rfc/rfc1779.txt>.

FWSM software version 2.2(1) supports X.509 (certificate support) on the VPN client. The Cisco IOS software, the VPN 3000 concentrator, and the FWSM look for the correct VPN group (mode configuration group) according to the “ou” attribute. (The “ou” attribute is part of the subject DN of the device certificate when the Easy VPN client negotiates the RSA signature.)

**Note**

If you use the *X.500_string* to communicate between a Cisco VPN 3000 head end and the FWSM, you must not configure the VPN 3000 head end to use DNS names for the backup servers. Instead, you must specify the backup servers by their IP addresses.

Examples

This example shows how to create the device certificate with the subject DN (where my_department is the VPN group):

```
fwsM/context_name(config)# ca subject-name myca ou=my_department, o=my_org, st=CA, c=US
```

Related Commands

show ca

ca verifycertdn

To verify the certificate's Distinguished Name (DN) and act as a subject name filter that is based on the *X.500_string*, use the **ca verifycertdn** command. To disable subject name filtering, use the **no** form of this command.

[no] ca verifycertdn *X.500_string*

Syntax Description

<i>X.500_string</i>	Character string that indicates the DN sent.
---------------------	--

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you enter the **ca verifycertdn** command and the subject name of the peer certificate matches the *X.500_string*, then it is filtered out and ISAKMP negotiation fails.

Examples

This example shows how to verify the certificate's DN:

```
fwsM/context_name(config)# ca verifycertdn woeruweoru
```

Related Commands

show ca

ca zeroize rsa

To delete all the RSA keys that were previously generated by the FWSM, use the **ca zeroize rsa** command.

```
ca zeroize rsa [keypair_name]
```

Syntax Description

keypair_name (Optional) Name of the key pair.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **ca zeroize rsa** command deletes all the RSA keys that were previously generated by the FWSM. If you use this command, you must also perform two additional tasks as follows:

1. Use the **no ca identity** command to manually remove the FWSM's certificates from the configuration. This step deletes all the certificates that were issued by the CA.
2. Ask the CA administrator to revoke the FWSM's certificates at the CA. Supply the challenge password that you created when you originally obtained the FWSM's certificates using the **crypto ca enroll** command.

To save the RSA key pair, enter the **ca save all** command. To delete a specific RSA key pair, specify the name of the RSA key that you want to delete using the optional keyword *keypair_name* within the **ca zeroize rsa** command.



Note

You may have more than one pair of RSA keys due to the Secure Shell (SSH). See the **ssh** command for more information.

Examples

This example shows how to delete the RSA keys:

```
fwsm/context_name(config)# ca zeroize rsa keys
```

Related Commands

show ca

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command. To disable packet capture capabilities, use the **no** form of this command.

```
capture capture_name [access-list access_list_name] [buffer buf_size] [ethernet-type type]
[interface interface_name] [packet-length bytes] [circular-buffer]
```

```
no capture capture-name [access-list access_list_name] [circular-buffer] [ interface
interface_name]
```

Syntax Description

<i>capture_name</i>	Name of the packet capture.
access-list <i>access_list_name</i>	(Optional) Selects packets based on IP or higher fields for a specific access list identification.
buffer <i>buf_size</i>	(Optional) Defines the buffer size used to store the packet in bytes.
ethernet-type <i>type</i>	(Optional) Selects an EtherType to exclude from capture.
interface <i>interface_name</i>	(Optional) Name of the interface on which to use packet capture.
packet-length <i>bytes</i>	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
circular-buffer	(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.

Defaults

The defaults are as follows:

- The **buffer size** is 512 KB.
- All theEtherTypes are accepted.
- All the IP packets are matched.
- The **packet-length** is 68 bytes.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. The FWSM can track packet information for traffic that passes through the general-purpose processor, including management traffic and inspection engines. The FWSM cannot capture traffic that goes through the network processors (such as most through traffic). We recommend contacting technical support if you want to use the packet capture feature.

When selecting an EtherType to exclude from capture, an exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner EtherType is used for matching. By default, all the EtherTypes are accepted.

Once the byte buffer is full, packet capture stops.

To enable packet capturing, attach the capture to an interface with the *interface* optional argument. Multiple interface statements attach the capture to multiple interfaces.

If you copy the buffer contents to a TFTP server in ASCII format, then you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and then read it with TCPDUMP or Ethereal.

The **ethernet-type** and **access-list** optional keywords select the packets to store in the buffer. A packet must pass both the Ethernet and access list filters before the packet is stored in the capture buffer.

The **capture** *capture_name* **circular-buffer** command allows you to enable the capture buffer to overwrite itself, starting from the beginning, when the capture buffer is full.

Enter the **no capture** command with either the **access-list** or **interface** optional keyword unless you want to clear the capture itself. Entering **no capture** without optional keywords deletes the capture. If the **access-list** optional keyword is specified, the access list is removed from the capture and the capture is preserved. If the **interface** optional keyword is specified, the capture is detached from the specified interface and the capture is preserved.

**Note**

The **capture** command is not saved to the configuration, and the **capture** command is not copied to the standby module during failover.

Use the **copy capture:** *capture_name* **tftp://server/path** [**pcap**] command to copy capture information to a remote TFTP server.

Use the **https://fwsM-ip-address/capture/capture_name** [**/pcap**] command to see the packet capture information with a web browser.

If you specify the **pcap** optional keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)

Examples

To enable packet capture, enter the following:

```
fwsM(config)# capture capttest interface inside interface outside
```

On a web browser, the capture contents for a capture named “mycapture” can be viewed at the following location:

```
https://171.69.38.95/capture/mycapture/pcap
```

To download a libpcap file (used in web browsers such as Internet Explorer or Netscape Navigator) to a local machine, enter the following:

```
https://171.69.38.95/capture/http/pcap
```

This example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
fwsM/context_name(config)# access-list http permit tcp host 10.120.56.15 eq http host  
171.71.69.234  
fwsM/context_name(config)# access-list http permit tcp host 171.71.69.234 host  
10.120.56.15 eq http  
fwsM/context_name(config)# capture http access-list http packet-length 74 interface inside
```

This example shows how to capture ARP packets:

```
fwsM/context_name(config)# capture arp ethernet-type arp interface outside
```

Related Commands

clear capture

copy capture

show capture

cd

To change the current working directory to the one specified, use the **cd** command.

cd disk: *path*

Syntax Description	disk: <i>path</i>	Changes the current working directory.
--------------------	--------------------------	--

Defaults	If you do not specify a directory, the directory is changed to the root of the disk.
----------	--

Command Modes	Security Context Mode: single context mode and multiple context mode Access Location: system command line Command Mode: privileged mode Firewall Mode: routed firewall mode and transparent firewall mode
---------------	--

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples	This example shows how to change to the config directory: fws#(config)# cd disk:/config/
----------	--

Related Commands	copy disk copy flash copy tftp dir format mkdir more pwd rename rmdir
------------------	--

changeto

To change the execution space in which commands are applied, use the **changeto** command.

changeto {**system** | **context** *name*}

Syntax Description

system	Changes the command execution space to system.
context	Changes the command execution space to context.
<i>name</i>	Execution space name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The name of the context is inserted in the command line prompt. The prompt changes only when you are working within a context. The prompt does not change when you change from single context mode to multiple context mode.

Examples

This example shows how to change to a context named “test1”:

```
fws(config)# changeto context test1
fws#/my_context(config)#
```

This example shows how to change from the context named “test1” back to the system context:

```
fws#/my_context(config)# changeto system
fws#(config)#
```

Related Commands

context

checkheaps

To configure checkheaps verification intervals, use the **checkheaps** command in global configuration mode. To set the value to the default, use the **no** form of this command. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

checkheaps {**check-interval** | **validate-checksum**} *seconds*

[**no**] **checkheaps** {**check-interval** | **validate-checksum**} [*seconds*]

Syntax Description	check-interval	validate-checksum
	Sets the buffer verification interval. The buffer verification process checks the sanity of the heap (allocated and freed memory buffers). During each invocation of the process, the FWSM checks the entire heap, validating each memory buffer. If there is a discrepancy, the FWSM issues either an “allocated buffer error” or a “free buffer error.” If there is an error, the FWSM dumps traceback information when possible and reloads.	Sets the code space checksum validation interval. When the FWSM first boots up, the FWSM calculates a hash of the entire code. Later, during the periodic check, the FWSM generates a new hash and compares it to the original. If there is a mismatch, the FWSM issues a “text checksum checkheaps error.” If there is an error, the FWSM dumps traceback information when possible and reloads.
	<i>seconds</i>	Sets the interval in seconds between 1 and 2147483.

Defaults

The default intervals are 60 seconds each.

Command Modes

Security Context Mode: single context and system mode
 Access Location: system and context command line
 Command Mode: global configuration
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.3	This command was introduced.

Examples

The following example sets the buffer allocation interval to 200 seconds and the code space checksum interval to 500 seconds:

```
fws(config)# checkheaps check-interval 200
fws(config)# checkheaps validate-checksum 500
```

Related Commands `show checkheaps`

class

To create a class to which you can assign contexts and then enter the class submode, use the **class** command. Use the **no** form of this command to remove a class.

[no] **class** *name*

Syntax Description

<i>name</i>	Class name string of up to 20 characters.
-------------	---

Defaults

The default class is a special class to which all the unassigned contexts belong.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The class parameters determine the resource limitations for each class member. The class name is limited to 20 characters. The default class cannot be removed. Enter **default** for the *name* to change the limits for the default class. To remove a class, use the **no** form of this command. After you enter the **class** command, the FWSM enters the class subconfiguration mode. In this submode, you can enter the **limit-resource (class submode)** command.

By default, all the security contexts have access to most of the FWSM resources. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, then you can configure resource management to limit the use of resources per context.

See the **limit-resource (class submode)** command for a list of resources. See also the **show resource types** command.



Note

The FWSM does not limit the bandwidth per context. The switch/router containing the FWSM can limit the bandwidth per VLAN. Refer to the Catalyst 6500 series switch or Cisco 7600 series router documentation for more information.

Default Class

All the contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to default.

If a context belongs to another class, the other class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, you create a class with a 2 percent limit for all the concurrent connections, but no other limits. All other limits are inherited from default. Conversely, if you create a class with a 2 percent limit for all the resources, the class uses no settings from default.

By default, the default class provides unlimited access to most resources for all the contexts. The following resources are limited by per context:

- Telnet—5
- SSH—5
- IPsec—5
- Bridge-table entries—65,535

All other contexts provide unlimited access.

Resource Members

To use the settings of a resource class, assign the context to the class. All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default. You can only assign a context to one resource class. The exception is that the limits that are undefined in the member class are inherited from the default class. A context could be a member of the default plus another class.

To assign a context to a class, enter the **member (context submode)** command.

Examples

This example shows how to create a class named “empire”:

```
fws(config)# class empire
fws(config-class)# limit-resource all 50%
fws(config-class)# limit-resource empire 50%
fws(config-class)# exit
```

```
fws(config)# show class
Class Name      Members    ID    Flags
default         All        1     0001
empire          0          2     0000
```

This example shows how to change the default class parameters:

```
fws(config)# class default
fws(config-class)# limit-resource all 10%
fws(config-class)# limit-resource default 50%
fws(config-class)# exit
```

Related Commands

config-url (context submode)
limit-resource (class submode)
show class
show context
show resource allocation
show resource types

clear

To remove configuration files and commands from the configuration or reset command values, use a form of the **clear** command.

clear *command*

Syntax Description

<i>command</i>	Item to remove or reset.
----------------	--------------------------

Defaults

The default setting depends on which **clear** command is used.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can use the **no** form of a command to change the configuration.

The **clear** commands can be used in modes with different security levels. The **clear** commands that can be used in less secure modes can also be used in more secure modes. However, if a **clear** command appears in a more secure mode, that command is not available in a less secure mode.

clear aaa

To enable, disable, or view TACACS+, RADIUS, or local user authentication, authorization, and accounting, use the **clear aaa** command.

clear aaa authentication | authorization | accounting

Syntax Description

authentication	Specifies AAA authentication.
authorization	Specifies AAA authorization.
accounting	Specifies AAA accounting.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove a defined server group:

```
fwsml/context_name(config)# clear aaa authentication
```

Related Commands

config-url (context submode)
limit-resource (class submode)
show class
show context
show resource allocation
show resource types

clear aaa accounting

To clear the local, TACACS+, or RADIUS user account, use the **clear aaa accounting** command.

```
clear aaa accounting {include | exclude} service interface_name source_ip source_mask
[destination_ip destination_mask] server_tag
```

include	Creates a new rule with the specified service to include.
exclude	Creates an exception to a previously stated rule by excluding the specified service from accounting.
<i>service</i>	Accounting service; valid values are any , ftp , http , telnet , or <i>protocollport</i> .
<i>interface_name</i>	Interface name from which users require authentication.
<i>source_ip</i>	IP address of the source host or network of the hosts that you want to be authenticated or authorized.
<i>source_mask</i>	Network mask of the source IP.
<i>destination_ip</i>	(Optional) IP address of the hosts that you want to access the source IP address; 0 indicates all hosts.
<i>destination_mask</i>	(Optional) Network mask of the destination IP.
<i>server_tag</i>	AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When specifying the *service*, use **any** to provide accounting for all the TCP services. To provide accounting for UDP services, use the *protocollport* argument. For *protocollport*, the TCP *protocol* appears as 6, the UDP protocol appears as 17, and so on, and the port is the TCP or UDP destination port. A port value of 0 (zero) indicates all the ports. For protocols other than TCP and UDP, the *port* is not applicable and should not be used. Enter **LOCAL** to use the local FWSM user authentication database.

Examples

This example shows how to clear the user account:

```
fwsm/context_name(config)# clear aaa accounting
```

Related Commands

aaa accounting

clear aaa authentication

To clear the local, TACACS+, or RADIUS user authentication, use the **clear aaa authentication** command.

```
clear aaa authentication { include | exclude } authen_service interface_name source_ip
source_mask [destination_ip destination_mask] server_tag
```

Syntax Description		
include		Creates a new rule with the specified service to include.
exclude		Creates an exception to a previously stated rule by excluding the specified service from accounting.
<i>authen_service</i>		Type of traffic to include or exclude from authentication based on the service optional keyword selected. See the “Usage Guidelines” section for valid values.
<i>interface_name</i>		Interface name from which users require authentication.
<i>source_ip</i>		IP address of the local host or network of the hosts that you want to be authenticated or authorized.
<i>source_mask</i>		Network mask of the local IP.
<i>destination_ip</i>		(Optional) IP address of the hosts that you want to access the local IP address; 0 indicates all hosts.
<i>destination_mask</i>		(Optional) Network mask of the destination IP.
<i>server_tag</i>		AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Enter **LOCAL** to use the local FWSM user authentication database.

Examples

This example shows how to clear AAA authentication:

```
fswm/context_name (config) # clear aaa authentication
```

Related Commands

aaa accounting

clear aaa authorization

To clear the local or TACACS+ user authentication, use the **clear aaa authorization** command.

```
clear aaa authorization {include | exclude} authen_service interface_name source_ip
source_mask [destination_ip destination_mask] server_tag
```

Syntax Description		
include		Creates a new rule with the specified service to include.
exclude		Creates an exception to a previously stated rule by excluding the specified service from accounting.
<i>authen_service</i>		Type of traffic to include or exclude from authentication based on the service optional keyword selected. See the “Usage Guidelines” section for valid values.
<i>interface_name</i>		Interface name from which users require authentication.
<i>source_ip</i>		IP address of the local host or network of the hosts that you want to be authenticated or authorized.
<i>source_mask</i>		Network mask of the local IP.
<i>destination_ip</i>		(Optional) IP address of the hosts that you want to access the local IP address; 0 indicates all hosts.
<i>destination_mask</i>		(Optional) Network mask of the destination IP.
<i>server_tag</i>		AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **aaa authorization** command is supported for use with local and TACACS+ servers but not with RADIUS servers. Enter **LOCAL** to use the local FWSM user authentication database.

Examples

This example shows how to clear AAA authorization:

```
fwsM/context_name(config)# clear aaa authorization
```

Related Commands aaa accounting
 clear aaa accounting

clear aaa-server

To remove a defined server group, use the **clear aaa-server** command.

clear aaa-server [*tag*]

Syntax Description	
<i>tag</i>	(Optional) AAA server group tag; enter LOCAL to use the local FWSM user authentication database.

Defaults This command has no default settings.

Command Modes

- Security Context Mode: single context mode and multiple context mode
- Access Location: context command line
- Command Mode: configuration mode
- Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove a defined server group:

```
fwsM/context_name(config)# clear aaa-server LOCAL
```

Related Commands aaa-server

clear access-group

To remove access groups from all the interfaces, use the **clear access-group** command.

clear access-group

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all the access groups:

```
fwsM/context_name (config) # clear access-group
```

Related Commands **access-group**
show access-group

clear access-list

To remove an access list or clear an access-list counter, use the **clear access-list** command.

```
clear access-list [id [counters]]
```

Syntax Description	
<i>id</i>	(Optional) Name or number of an access list.
counters	(Optional) Clears access-list counters.

Defaults All the access lists are cleared.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines When you enter the **clear access-list** command, all the **access-list** commands, including the **access-list deny-flow-max** command, are cleared if you do not specify an *id*. Also removed are commands that refer to an ACL, for example, the **access group** command.

Examples This example shows how to clear a specific access-list counter:

```
fwsM/context_name(config)# clear access-list 77 23 counters
```

This example shows how to clear all the access-list counters:

```
fwsM/context_name(config)# clear access-list inbound counters
```

Related Commands **access-list extended**
show access-list

clear activation-key

To clear the FWSM activation key and revert the FWSM to the default feature set, use the **clear activation-key** command.

clear activation-key

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: system command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines In multiple security context mode, the default feature set allows two contexts.

Examples This example shows how to clear an activation key:

```
fws(config)# clear activation-key
```

Related Commands activation key

clear alias

To remove all the **alias** commands from the configuration, use the **clear alias** command.

clear alias

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all the **alias** commands from the configuration:

```
fwsM/context_name(config)# clear alias
```

Related Commands `alias`

clear arp

To clear all the entries in the ARP cache table except for those you configure directly with the **arp interface_name ip mac** command, use the **clear arp** command.

clear arp [timeout | statistics]

Syntax Description

timeout	(Optional) Clears the ARP timeout.
statistics	(Optional) Clears the ARP statistics entries.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: privileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the ARP cache table entries:

```
fwsM/context_name (config) # clear arp
```

Related Commands

arp
show arp

clear arp-inspection

To clear the ARP inspection configuration, use the **clear arp-inspection** command.

clear arp-inspection

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: Transparent

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to clear the ARP inspection configuration:

```
fwsM/context_name(config)# clear arp-inspection
```

Related Commands

- arp
- arp-inspection
- show arp

clear auth-prompt

To clear the AAA challenge text for HTTP, FTP, and Telnet access, use the **clear auth-prompt** command.

clear auth-prompt

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes

- Security Context Mode: single context mode and multiple context mode
- Access Location: context command line
- Command Mode: configuration mode
- Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to clear the AAA challenge text in the authorization prompt:

```
fwsM/context_name (config) # clear auth-prompt
```

Related Commands

- auth-prompt**
- show auth-prompt**

clear banner

To remove all the banners, use the **clear banner** command.

clear banner

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to clear banners:

```
fwsM/context_name(config)# clear banner
```

Usage Guidelines **banner**
show banner

clear blocks

To remove all block information, use the **clear blocks** command.

clear blocks queue history

Syntax Description	queue	Specifies the block queue.
	history	Specifies the blocks history.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to clear banners:
 fsm/context_name (config) # **clear blocks**

Usage Guidelines show blocks

clear ca

To remove the Certificate Authority (CA) configuration, use the **clear ca** command.

clear ca

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to clear the ca configuration:

```
fwsm/context_name(config)# clear ca
```

Usage Guidelines **ca configure**
show ca

clear capture

To clear the capture buffer, use the **clear capture** *capture_name* command.

clear capture *capture_name*

Syntax Description	
	<i>capture_name</i> Name of the packet capture.

Defaults	
	This command has no default settings.

Command Modes	
	Security Context Mode: single context mode and multiple context mode
	Access Location: system and context command line
	Command Mode: privileged mode
	Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines	
	The shortened form of the clear capture (for example, cl cap or clear cap) is not supported to prevent accidental destruction of all the packet captures.

Examples	
	This example shows how to clear the capture buffer for the capture buffer “orlando”: <pre>fwsM/context_name(config)# clear capture orlando</pre>

Related Commands	
	capture show capture

clear class

To remove all the classes and restore the default class to its default settings, use the **clear class** command.

clear class

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: multiple context mode
 Access Location: system command line
 Command Mode: config mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all the classes:

```
fws(config)# clear class
```

Related Commands **class**
show class

clear configure

To clear aspects of the running configuration, use the **clear configure** command.

clear configure { **primary** | **secondary** | **all** }

Syntax Description

primary	(Optional) Sets particular commands to their default values, removes interface names from all the commands in the configuration, and returns the commands to their default settings.
secondary	(Optional) Removes particular commands from the configuration and returns the commands to their default settings.
all	(Optional) Combines the entire running configuration and returns to the default settings.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear configure all** command resets a configuration to its default values. Use this command to create a template configuration or when you want to clear all the values.

Using the **clear config all** command in context mode clears the entire running configuration for a context, but it does not clear that context's configuration URL or delete the context. In addition, the parameters that are entered in the system configuration are not deleted.



Note

If you enter the **clear configure** command in system mode, the system configuration and all context configurations are cleared.

The **clear configure primary** command resets the default values for the **interface**, **ip**, **mtu**, **nameif**, and **route** commands to their default values, removes interface names from all the commands in the configuration, and returns to the default settings.

The **clear configure secondary** command allows you to remove the **aaa-server**, **alias**, **access-list**, **apply**, **global**, **outbound**, **static**, **telnet**, and **url-server** commands from the configuration, and return to the default settings, but does not remove the **tftp-server** commands.

Use the **write erase** command to clear the startup configuration in the Flash partition.

clear configure

Examples

This example shows how to clear the configuration in RAM:

```
fwsM/context_name(config)# clear configure all
```

Related Commands

configure

show configure

write

clear conn

To remove the connections from the system, use the **clear conn** command.

clear conn

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: multiple context mode
Access Location: context command line
Command Mode: privileged mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the connections from the system:

```
fwsM/context_name# clear conn
```

Related Commands **show conn**

clear console-output

To remove the currently captured console output, use the **clear console-output** command.

clear console-output

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system command line
 Command Mode: privileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the currently configured console output:

```
fwsM/context_name# clear console-output
```

Related Commands **show console-output**

clear context

To stop all contexts (including the admin context) from running and remove the context entries from the system configuration, use the **clear context** command.

clear context

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes

- Security Context Mode: multiple context mode
- Access Location: system command line
- Command Mode: configuration mode
- Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The **clear context** command clears all contexts, their configuration, and any context subcommands (member and config-url) for all contexts. The **clear context** command does not remove the RM class definitions.

Examples This example show how to stop all the running contexts and remove the context entries from the system configuration:

```
fws(config)# clear context
```

Related Commands

- context
- show context

clear counters

To clear the protocol stack counters, use the **clear counters** command.

```
clear counters [context context-name | top N | all | summary] [protocol protocol_name
[:counter_name] | detail]
```

Syntax Description

context	(Optional) Specifies a context.
<i>context-name</i>	(Optional) Context name.
top <i>N</i>	(Optional) Displays the counter details for the specified location.
all	(Optional) Displays the filter details.
summary	(Optional) Displays a counter summary.
protocol	(Optional) Displays the counters for the specified protocol.
<i>protocol_name</i>	(Optional) Protocol by name.
: <i>counter_name</i>	(Optional) Counter by name.
detail	(Optional) Displays the counters in detail.

Defaults

clear counters summary detail

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the protocol stack counters:

```
fws(config)# clear counters
```

Related Commands

show counters

clear crashdump

To delete the crash information file from the Flash partition of the FWSM, use the **clear crashdump** command.

clear crashdump

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: system command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to delete the crash information file:

```
fwsm(config)# clear crashdump
```

Related Commands **crashdump force**
show crashdump

clear crypto dynamic-map

To remove the **crypto dynamic-map** commands from the configuration, use the **clear crypto dynamic-map** command.

```
clear [crypto] dynamic-map [dynamic-map-name] [dynamic-seq-num]
```

Syntax Description

crypto	(Optional) Specifies crypto for the dynamic map.
<i>dynamic-map-name</i>	(Optional) Name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	(Optional) Sequence number that corresponds to the dynamic crypto map entry.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **crypto** keyword is optional.

Examples

This example shows how to remove the **crypto dynamic-map** commands from the configuration:

```
fwsM/context_name(config)# clear crypto dynamic-map alarms 323
```

Related Commands

crypto dynamic-map

show crypto engine

clear crypto interface counters

To clear the crypto interface counters, use the **clear crypto interface counters** command.

clear crypto interface counters

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The **clear crypto interface counters** command clears only the packet, payload byte, queue length, and moving average counters. It does not affect any actual packets that are queued.

Examples This example shows how to clear the crypto interface counters:

```
fwsms#/context_name(config)# clear crypto interface counters
```

Related Commands **crypto map interface**
show crypto interface

clear crypto ipsec sa

To delete IPSec security associations, use the **clear crypto ipsec sa** command.

```
clear [crypto] ipsec sa [counters | entry {destination-address protocol spi} | map map-name | peer]
```

Syntax Description

crypto	(Optional) Specifies the crypto configuration.
counters	(Optional) Clears the traffic counters that are maintained for each security association.
entry	(Optional) Deletes the IPSec security association with the specified address, protocol, and SPI.
<i>destination-address</i>	(Optional) IP address of the peer or the remote peer.
<i>protocol</i>	(Optional) Security associations by protocol; valid values are ah or esp .
<i>spi</i>	(Optional) Security Parameter Index (SPI) number that is used to identify a security association; valid values are from 256 to 4294967295 (a hexadecimal value of FFFF FFFF).
map <i>map-name</i>	(Optional) Deletes any IPSec security associations for the named crypto map set.
peer	(Optional) Deletes any IPSec security associations for the specified peer.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If the security associations were established through the Internet Key Exchange (IKE), they are deleted. Future IPSec traffic requires new security associations. When IKE is used, the IPSec security associations are established only when needed.

If the security associations are manually established, the security associations are deleted.

If you enter the **clear [crypto] ipsec sa** command with no arguments, all the IPSec security associations are deleted.

If the security associations are manually established, the security associations are deleted and reinstalled. (When IKE is not used, the IPSec security associations are created as soon as the configuration is completed.)

If any of the previous commands cause a particular security association to be deleted, all the “sibling” security associations that were established during the same Internet Key Exchange (IKE) negotiation are deleted as well.

The **counters** optional keyword clears the traffic counters that are maintained for each security association; it does not clear the security association.

If you make configuration changes that affect security associations, these changes will not apply to existing security associations but to negotiations for subsequent security associations. You can use the **clear [crypto] ipsec sa** command to restart all the security associations so that they use the most current configuration settings. In the case of manually established security associations, if you make changes that affect security associations, you must use the **clear [crypto] ipsec sa** command before the changes take effect.

**Note**

If you make significant changes to an IPSec configuration, such as access list or peers, the **clear [crypto] ipsec sa** command does not activate the new configuration. In such a case, you should rebind the crypto map to the interface with the **crypto map interface** command.

If the FWSM is processing active IPSec traffic, we recommend that you clear only the portion of the security association database that is affected by the changes to avoid causing active IPSec traffic to temporarily fail.

The **clear [crypto] ipsec sa** command clears only the IPSec security associations. To clear the IKE security associations, use the **clear [crypto] isakmp sa** command.

Examples

This example shows how to clear (and reinitialize, if appropriate) all the IPSec security associations at the FWSM:

```
fwsm/context_name(config)# clear crypto ipsec sa
```

This example shows how to clear (and reinitialize, if appropriate) the inbound and outbound IPSec security associations that are established for address 10.0.0.1 using the AH protocol with the SPI of 256:

```
fwsm/context_name(config)# clear crypto ipsec sa entry 10.0.0.1 AH 256
```

Related Commands

crypto ipsec security-association lifetime

crypto map interface

show crypto map

clear crypto isakamp sa

To remove the **isakamp policy** commands for IKE SAs from the configuration, use the **clear crypto isakamp sa** command.

clear crypto isakamp sa

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the **isakamp policy** commands from the configuration:

```
fwsM/context_name(config)# clear isakamp sa
```

Related Commands

- isakmp**
- isakmp policy**
- show isakmp**
- show isakmp policy**

clear dhcpd

To clear all of the DHCP server commands, binding, and statistics information, use the **clear dhcpd** command.

clear dhcpd [binding | statistics]

Syntax Description	binding	(Optional) Clears all the client address bindings.
	statistics	(Optional) Clears statistical information, such as the address pool, number of bindings, malformed messages, sent messages, and received messages.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear dhcpd** command clears all of the **dhcpd** commands, binding, and statistics information. The **clear dhcpd statistics** command clears the **show dhcpd statistics** counters.

Examples

This example shows how to clear the **dhcpd** commands:

```
fwsM/context_name (config) # clear dhcpd statistics
```

Related Commands

dhcpd
dhcprelay
show dhcpd
show dhcprelay

clear dhcprelay

To clear the DHCP-relay configuration commands, use the **clear dhcprelay** command.

clear dhcprelay [**statistics**]

Syntax Description	statistics	(Optional) Clears the DHCP relay statistical counters.
--------------------	------------	--

Defaults	This command has no default settings.
----------	---------------------------------------

Command Modes	Security Context Mode: single context mode and multiple context mode Access Location: context command line Command Mode: configuration mode Firewall Mode: Routed
---------------	--

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines	The clear dhcprelay command clears all DHCP relay configurations. The clear dhcprelay statistics command clears the show dhcprelay statistics counters.
------------------	--

Examples	This example shows how to clear all DHCP relay configurations: <pre>fwsM/context_name(config)# clear dhcprelay statistics</pre>
----------	--

Related Commands	dhcpd dhcprelay show dhcpd show dhcprelay
------------------	--

clear dispatch stats

To clear dispatch layer statistics, use the **clear dispatch stats** command.

```
clear dispatch stats [funcid | all]
```

Syntax Description	funcid	(Optional) Specifies the dispatch layer statistics function ID.
	all	(Optional) Specifies all dispatch layer statistics.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system command line
 Command Mode: privileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all of the dispatch layer statistics:

```
fws(config)# clear dispatch stats all
```

Related Commands **show dispatch stats**
show dispatch table

clear dynamic-map

To delete a dynamic crypto map entry, use the **clear dynamic-map** command.

```
clear [crypto] dynamic-map [dynamic-map-name] [dynamic-seq-num]
```

Syntax Description

crypto	(Optional) Specifies the crypto configuration
<i>dynamic-map-name</i>	(Optional) Map name.
<i>dynamic-seq-num</i>	(Optional) Map sequence number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove a dynamic map entry:

```
fwsM/context_name(config)# clear dynamic-map
```

Related Commands

crypto dynamic-map
dynamic-map

clear established

To remove all established commands, use the **clear established** command.

clear established

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines To remove an established connection created by the **established** command, enter the **clear xlate** command.

Examples This example shows how to remove established commands:

```
fwsM/context_name (config) # clear established
```

Related Commands **established**
show established

clear failover

To remove all failover configurations, use the **clear failover** command.

clear failover

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the failover configuration:

```
fws(config)# clear failover
```

Related Commands

- failover
- failover interface ip
- failover interface-policy
- failover lan interface
- failover lan unit
- failover link
- failover polltime
- failover replication http
- failover reset
- show failover
- write standby

clear filter

To remove all **filter** commands from the configuration, use the **clear filter** command

clear filter

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all **filter** commands:

```
fwsM/context_name (config) # clear filter
```

Related Commands

- filter ftp**
- filter https**
- filter url**

clear firewall

To set the firewall mode to the default setting, use the **clear firewall** command

```
clear firewall
```

Syntax Description This command has no arguments or keywords.

Defaults The default firewall mode is routed.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to set the firewall mode to routed:

```
fwsM/context_name(config)# clear firewall
```

Related Commands **firewall**
show firewall

clear fixup

To reset the fixup configuration, use the **clear fixup** command.

clear fixup

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The **clear fixup** command does not remove the default **fixup protocol** commands.

Examples This example shows how to reset the fixup configuration:

```
fwsM/context_name (config) # clear fixup
```

Related Commands **fixup protocol**
show fixup

clear flashfs

To clear the file system part of the Flash partition in the FWSM, use the **clear flashfs** command.

clear flashfs

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system command line
 Command Mode: privileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The **clear flashfs** command clears the file system part of the Flash partition in the FWSM.
 The **clear flashfs** command does not affect the configuration that is stored in the Flash partition.

Examples This example shows how to clear the file system part of the Flash partition on the FWSM:

```
fwsM# clear flashfs
```

Related Commands

- clear flashfs**
- no flashfs**
- show flashfs**

clear floodguard

To disable flood guard, use the **clear floodguard** command.

clear floodguard

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to disable flood guard:
fwsM/context_name (config) # **clear floodguard**

Related Commands **floodguard**
show floodguard

clear fragment

To reset the fragment databases and defaults, use the **clear fragment** command.

clear fragment

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The **clear fragment** command resets the fragment databases. Specifically, all fragments awaiting reassembly are discarded. In addition, the size is reset to 200, the chain limit is reset to 24, and the timeout is reset to 5 seconds.

All fragments currently waiting for reassembly are discarded and the **size**, **chain**, and **timeout** optional keywords are reset to their default values.

The **sysopt security fragguard** and **fragguard** commands have been replaced by the **fragment** command.

Examples This example shows how to reset the fragment database and defaults:

```
fwsM/context_name(config)# clear fragment
```

Related Commands **fragment**
show fragment

clear ftp

To set the FTP mode to the default setting, use the **clear ftp** command.

clear ftp

Syntax Description This command has no arguments or keywords.

Defaults The default FTP mode is passive.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: system command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to set the FTP mode to passive:

```
fwsn(config)# clear ftp
```

Related Commands **ftp mode**
show ftp

clear gc

To remove the garbage collection process statistics, use the **clear gc** command.

```
clear gc
```

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system command line
 Command Mode: privileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the garbage collection process statistics:

```
fws# clear gc
```

Related Commands `show gc`

clear global

To remove the **global** commands from the configuration, use the **clear global** command.

clear global

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: Transparent

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the **global** commands from the configuration:

```
fwsM/context_name (config) # clear global
```

Related Commands **global**
show global

clear hostname

To clear the host name in the FWSM command line prompt, use the **clear hostname** command.

clear hostname

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to change a host name:

```
fws(config)# clear hostname
fws(config)#
```

Related Commands **hostname**
show hostname

clear http

To remove all HTTP hosts and disable the server, use the **clear http** command.

clear http

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all HTTP hosts and disable the HTTP servers:
`fwsM/context_name (config) # clear http`

Related Commands **http**
show http

clear icmp

To remove the access for ICMP traffic that terminates at an interface, use the **clear icmp** command.

clear icmp

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The **clear icmp** command clears the ICMP entries.

Examples This command shows how to remove the access for ICMP traffic:

```
fwsm/context_name(config)# clear icmp
```

Related Commands **icmp**
show http

clear interface stats

To clear the interface statistics, use the **clear interface stats** command.

clear interface [*interface*] **stats**

Syntax Description	<i>interface-id</i> (Optional) Interface identification name or number.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Security Context Mode: single context mode and multiple context mode Access Location: system and context command line Command Mode: configuration mode Firewall Mode: routed firewall mode and transparent firewall mode
----------------------	---

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines	The clear interface command clears all the interface statistics. This command does not shut down all the system interfaces. The clear interface command also clears the packet drop count of Unicast RPF for all interfaces.
-------------------------	--

Examples	This command shows how to clear the statistics for the inside interface: <pre>fwsM/context_name(config)# clear interface inside stats</pre>
-----------------	--

Related Commands	interface show interface
-------------------------	---

clear ip address

To clear all the IP addresses, use the **clear ip address** command.

clear ip address

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines After changing an **ip address** command, use the **clear xlate** command.

Examples This example shows how to clear all the interface IP addresses and stop all traffic through the FWSM module:

```
fwsm/context_name(config)# clear ip address
```

Related Commands

- clear ip verify reverse-path**
- ip address**
- ip prefix-list**
- ip verify reverse-path**
- show ip address**
- show ip verify**

clear ip ospf

To clear information about the IP OSPF, use the **clear ospf** command.

```
clear ip ospf [pid] {process | counters | neighbor [neighbor-intf] [neighbor-id]}
```

Syntax Description		
<i>pid</i>	(Optional) Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.	
process	Clears the OSPF routing process ID.	
counters	Clears the OSPF counters.	
neighbor	Clears the OSPF neighbor.	
neighbor-intf	(Optional) Clears the OSPF interface router designation.	
neighbor-id	(Optional) Clears the OSPF neighbor router ID.	

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command does not remove any part of the configuration. To remove the OSPF configuration, use the **no** form of the **router ospf** or **routing interface** command.

Examples

This example shows how to clear the OSPF IP parameters:

```
fwsM/context_name(config)# clear ip ospf
```

Related Commands

routing interface
show ip ospf

clear ip verify reverse-path

To remove the **ip verify reverse-path** commands from the configuration, use the **clear ip verify reverse-path** command.

```
clear ip verify reverse-path [interface int_name] [statistics]
```

Syntax Description

interface <i>int_name</i>	Removes the ip verify reverse-path command configuration from the configuration.
statistics	(Optional) Removes the statistical information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear ip verify** command allows you to remove the **ip verify** commands from the configuration. Unicast reverse path forwarding (RPF) is a unidirectional input function that screens inbound packets arriving on an interface. The outbound packets are not screened.

Examples

This example shows how to remove the **ip verify reverse-path** commands from the configuration:

```
fwsM/context_name(config)# clear ip verify reverse-path
```

Related Commands

clear ip address
ip address
ip prefix-list
ip verify reverse-path
show ip address
show ip verify

clear local-host

To clear the information that is displayed for the local hosts, use the **clear local-host** command.



Note

Clearing the network state of a local host stops all connections and xlates that are associated with the local hosts.

```
clear local-host [ip_address]
```

Syntax Description

ip_address (Optional) Local host IP address.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Use the *ip_address* option to limit the display to a single host.

On the FWSM, the cleared hosts are released from the license limit. You can see the number of hosts that are counted toward the license limit by entering the **show local-host** command.

Examples

This example shows how the **clear local-host** command clears the information about the local hosts:

```
fwsM/context_name(config)# clear local-host 10.1.1.15
fwsM/context_name(config)# show local-host 10.1.1.15
```

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Related Commands

[show local-host](#)

clear logging

To clear the logging buffer, turn on suppressed messages, or reset disallowed messages to the original set, use the **clear logging** command.

clear logging [rate-limit | disabled]

Syntax Description

rate-limit	Resets the disallowed messages to the original set.
disabled	Turns on all suppressed messages.

Defaults

Entering this command without options clears the logging buffer.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: privileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To clear the logging buffer, enter the **clear logging** command without any options. To turn on all suppressed messages, enter the **clear logging disabled** command. To reset disallowed messages, enter the **clear logging rate-limit** command.

Examples

This example shows how to reset the disallowed messages:

```
fwsM/context_name(config)# clear logging rate-limit
```

After the information is cleared, nothing more displays.

Related Commands

[show logging rate-limit](#)

clear mac-address-table

To remove the interface name entries from the bridge table, use the **clear mac-address-table** command.

clear mac-address-table *interface_name*

Syntax Description

<i>interface_name</i>	Specifies the interface name.
-----------------------	-------------------------------

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Transparent

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the interface name entries from the bridge table:

```
fwsM/context_name(config)# clear mac-address-table my_context
```

Related Commands

[mac-address-table aging-time](#)
[mac-address-table static](#)
[show mac-address-table](#)

clear mac-learn

To stop MAC learning, use the **clear mac-learn** command.

clear mac-learn

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: Transparent

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to stop MAC learning:

```
fws(config)# clear mac-learn
```

Related Commands [show mac-learn](#)

clear mgcp

To remove the Media Gateway Command Protocol (MGCP) configuration and reset the command queue limit to the default of 200, use the **clear mgcp** command.

clear mgcp

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes

- Security Context Mode: single context mode and multiple context mode
- Access Location: context command line
- Command Mode: configuration mode
- Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the MGCP configuration and reset the command queue:

```
fwsM/context_name (config) # clear mgcp
```

Related Commands

- [mgcp](#)
- [show mgcp](#)

clear monitor-interface

To remove the interface-monitor configuration for failover, use the **clear monitor-interface** command.

clear monitor-interface

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the interface monitor configuration:

```
fwsM/context_name(config)# clear monitor-interface
```

Related Commands [failover](#)
[monitor-interface](#)
[show monitor-interface](#)

clear mp-passwd

To remove the maintenance partition password and reset to the default password, use the **clear mp-passwd** command.

```
clear mp-passwd
```

Syntax Description This command has no arguments or keywords.

Defaults The default password is “cisco.”

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: system command line
Command Mode: privileged mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the maintenance partition password:

```
fwsm(config)# clear mp-passwd
```

Related Commands [upgrade-mp](#)

clear nat

To remove the NAT configuration, use the **clear nat** command.

clear nat

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: privileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.
	2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Usage Guidelines



Note

In transparent firewall mode, only NAT id 0 is valid.

Examples This example shows how to remove the NAT configuration:

```
fwsM/context_name(config)# clear nat
```

Related Commands

- clear nat**
- nat**
- show nat**

clear name

To clear the list of names from the FWSM configuration, use the **clear name** command.

clear name

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to clear the name list from the FWSM:

```
fwsM/context_name(config)# clear name
```

Related Commands

- clear names**
- name**
- names**
- show name**
- show names**

clear names

To disable the use of the **name** commands, use the **clear names** command.

clear names

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to disable the use of the names:

```
fwsM/context_name(config)# clear names
```

Related Commands

clear name

name

names

show name

show names

clear object-group

To remove all the **object group** commands from the configuration, use the **clear object-group** command.

```
clear object-group [{protocol | service | icmp-type | network}] [obj_grp_id]
```

Syntax Description

protocol	(Optional) Clears a protocol group.
service	(Optional) Clears a service group.
icmp-type	(Optional) Clears an ICMP group.
network	(Optional) Clears a network group.
<i>obj_grp_id</i>	(Optional) Name of a previously defined object group.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the **object-group** commands from the configuration:

```
fwsM/context_name(config)# clear object-group
```

Related Commands

[object-group](#)
[show object-group](#)

clear pager

To restore the **pager** command default settings, use the **clear pager** command.

```
clear pager
```

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: unprivileged mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to restore the **pager** command default settings:

```
fws> clear pager
```

Related Commands [pager](#)
[show pager](#)

clear password

To reset the password to “cisco,” use the **clear password** command.

```
clear {password | passwd }
```

Syntax Description		
	password	Specifies that you are clearing the password.
	passwd	Specifies that you are clearing the password

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: config mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to reset the password to “cisco”:

```
fws(config)# clear password
```

Related Commands **password/passwd**
show password/passwd

clear pdm

To remove all the FWSM Device Manager locations, disable logging, and clear the PDM buffer, use the **clear pdm** command.

```
clear pdm [location | group | logging]
```

Syntax Description

location	(Optional) Specifies the PDM location.
group	(Optional) Specifies the PDM group.
logging	(Optional) Specifies the logging messages and level.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear pdm**, **pdm group**, **pdm history**, **pdm location**, and **pdm logging** commands may appear in the configuration, but they are designed to work as internal PDM-to-FWSM commands accessible only to the PDM buffer.

Examples

This example shows how to remove all the FWSM Device Manager locations, disable logging, and clear the PDM buffer:

```
fws(config)# clear pdm
```

Related Commands

pdm
show pdm

clear privilege

To remove the configuration or display privilege levels for the commands, use the **clear privilege** command.

clear privilege

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes

- Security Context Mode: single context mode and multiple context mode
- Access Location: system command line
- Command Mode: configuration mode
- Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the configuration or display privilege levels for the commands:

```
fwsm(config)# clear privilege
```

Related Commands

- privilege**
- show privilege**

clear resource usage

To set the peak counter to the value of the current counter and clear the denied counter, use the **clear resource usage** command.

```
clear resource usage [context context_name | top n | all | summary | system] [resource {[rate]
resource_name | all} | detail]
```

Syntax Description

context	(Optional) Specifies the context.
<i>context_name</i>	(Optional) Name of the context.
top <i>n</i>	(Optional) Specifies a number of resources.
all	(Optional) Specifies all resources.
summary	(Optional) Specifies a summary of resources.
system	(Optional) Specifies the system resources.
resource	(Optional) Specifies a specific resource.
rate	(Optional) Specifies a resource rate.
<i>resource_name</i>	(Optional) Resource name.
all	(Optional) Specifies all resources.
detail	(Optional) Specifies the details.

Defaults

All configurable resources.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear resource usage** command operates on the resources specified in the command. If no resource type is specified, the command uses the default for all resources. If the resource type detail is specified, all resource types are cleared.

Examples

This example show how to remove the list of system resources that were used:

```
fws(config)# clear resource usage
```

Related Commands show resource allocation
 show resource types
 show resource usage

clear rip

To remove the Routing Information Protocol (RIP) settings, use the **clear rip** command.

clear rip

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode
 Command Mode: configuration mode
 Firewall Mode: Routed

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the RIP settings:

```
fwsn(config)# clear rip
```

Related Commands **rip**
show rip

clear route

To remove the **route** commands from the configuration that does not contain the **connect** keyword, use the **clear route** command.

```
clear route [interface_name ip_address [netmask gateway_ip]]
```

Syntax Description

<i>interface_name</i>	(Optional) Internal or external network interface name.
<i>ip_address</i>	(Optional) Internal or external network IP address.
<i>netmask</i>	(Optional) Specifies a network mask to apply to the <i>ip_address</i> .
<i>gateway_ip</i>	(Optional) Specifies the IP address of the gateway router (the next hop address for this route).

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Use **0.0.0.0** to specify a default route. You can abbreviate the 0.0.0.0 IP address as **0** and the 0.0.0.0 *netmask* as **0**.

Examples

This example shows how to remove the **route** commands from the configuration that does not contain the **connect** keyword:

```
fwsn(config)# clear route
```

Related Commands

route

show route

clear route-map

To remove the conditions for redistributing the routes from one routing protocol into another routing protocol, use the **clear route-map** command.

```
clear route-map map_tag [permit | deny] [seq_num]
```

Syntax Description

<i>map_tag</i>	Text for the route map tag. Defines a meaningful name for the route map up to 58 characters in length.
permit	(Optional) Specifies that if the match criteria are met for this route map, the route is redistributed as controlled by the set actions.
deny	(Optional) Specifies that if the match criteria are met for the route map, the route is not redistributed.
<i>seq_num</i>	(Optional) Route map sequence number; valid values are from 0 to 65535.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If the match criteria are not met, and the **permit** keyword is specified, the next route map with the same *map_tag* is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

Examples

This example shows how to remove the conditions of redistributing routes from one routing protocol into another routing protocol:

```
fwsm(config)# clear route-map 77 permit
```

Related Commands

route

route-map

show route

clear routing

To reset the interface-specific routing configuration to its defaults and remove the interface-specific routing configuration, use the **clear routing** command.

clear routing

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes

- Security Context Mode: single context mode
- Access Location: context command line
- Command Mode: privileged mode
- Firewall Mode: transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines This command does not remove any OSPF data structures that have been defined.

Examples This example shows how to reset the interface-specific routing configuration to its default settings and remove the interface-specific routing configuration:

```
fws(config)# clear routing
```

Related Commands

- route
- route-map
- show route

clear rpc-server

To clear the remote processor call (RPC) services from the FWSM, use the **clear rpc-server** command.

clear rpc-server [active]

Syntax Description	active (Optional) Identifies the RPC services that are currently active on the FWSM.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Security Context Mode: single context mode Access Location: system and context command line Command Mode: configuration mode Firewall Mode: routed firewall mode and transparent firewall mode
----------------------	---

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines	The rpc-server command displays the configured router ospf subcommands.
-------------------------	---



Note

If the highest-level IP address on the FWSM is a private address, this address is sent in hello packets and database definitions (DBDs). To prevent this action, set the **router-id ip_address** to a global address.

Examples	This example shows how to clear the RPC services from the FWSM:
-----------------	---

```
fwsm(config)# clear rpc-server active
```

Related Commands	rpc-server show rpc-server
-------------------------	---

clear same-security-traffic

To disable the same-security interface communication, use the **clear same-security-traffic** command.

clear same-security-traffic

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to disable the same-security interface communication:
fws(config)# **clear same-security-traffic**

Related Commands **same-security-traffic**
show routing

clear service

To remove the **service** commands from the configuration, use the **clear service** command.

clear service

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the **service** commands from the configuration:

```
fwsM/context_name(config)# clear service
```

Related Commands **service**
show service

clear shun

To disable all the shuns that are currently enabled and clear the shun statistics, use the **clear shun** command.

clear shun [*statistics*]

Syntax Description	<i>statistics</i> (Optional) Interface counters only.
---------------------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Security Context Mode: single context mode and multiple context mode Access Location: context command line Command Mode: privileged mode
----------------------	--

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples	This example shows how to disable all the shuns that are currently enabled and clear the shun statistics: <code>fwsM/context_name(config)# clear shun</code>
-----------------	---

Related Commands	show shun shun
-------------------------	---------------------------------

clear snmp-server

To disable the Simple Network Management Protocol (SNMP) server, use the **clear snmp-server** command.

clear snmp-server

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to disable the SNMP server:

```
fwsM/context_name(config)# clear snmp-server
```

Related Commands **show snmp-server**
snmp-server

clear ssh

To remove all the **ssh** commands from the configuration, use the **clear ssh** command.

```
clear ssh
```

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all the **ssh** commands from the configuration:

```
fwsM/context_name (config) # clear ssh
```

Related Commands **show ssh**
ssh

clear static

To remove all the **static** commands from the configuration, use the **clear static** command.

clear static

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.
	2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Examples This example shows how to remove all the **static** commands from the configuration:

```
fwsM/context_name(config)# clear static
```

Related Commands show ssh
 static

clear sysopt

To remove all the **sysopt** commands from the configuration, use the **clear sysopt** command.

clear sysopt

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all the **sysopt** commands from the configuration:

```
fwsM/context_name (config) # clear sysopt
```

Related Commands **show sysopt**
sysopt

clear tacacs-server

To remove all the **tacacs-server** commands from the configuration, use the **clear tacacs-server** command.

clear tacacs-server

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove all the **tacacs-server** commands from the configuration:

```
fwsM/context_name(config)# clear tacacs-server
```

Related Commands **aaa server**
telnet

clear telnet

To remove the Telnet connection and the idle timeout from the configuration, use the **clear telnet** command.

```
clear telnet [ip_address [netmask] [interface_name]]
```

Syntax Description

<i>ip_address</i>	(Optional) IP address of a host or network that can access the FWSM Telnet console.
<i>netmask</i>	(Optional) Bit mask of <i>ip_address</i> .
<i>interface_name</i>	(Optional) Unsecure interface name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To limit access to a single IP address, use 255 in each octet; for example, 255.255.255.255. If you do not specify *netmask*, it defaults to 255.255.255.255 regardless of the class of *source_ip*. Do not use the subnet mask of the internal network. The *netmask* is only a bit mask for the IP address in *ip_address*.

If IPsec is operating, you can specify an unsecure interface name, typically, the outside interface. At a minimum, you must configure the **crypto map** command to specify an interface name with the **telnet** command.

If you do not specify an interface name, the address is assumed to be on an internal interface. The FWSM automatically verifies the IP address against the IP addresses that are specified by the **ip address** commands to ensure that the address that you specify is on an internal interface. If an interface name is specified, the FWSM checks only the host against the interface that you specify.

Up to 16 hosts or networks are allowed access to the FWSM console with Telnet; 5 hosts or networks are allowed access to the console at the same time. Use the **no telnet** or **clear telnet** commands to remove Telnet access from a previously set IP address. Use the **telnet timeout** command to set the maximum time that a console Telnet session can be idle before being logged off by the FWSM. The **clear telnet** command does not affect the **telnet timeout** command duration. You cannot use the **no telnet** command with the **telnet timeout** command.

clear telnet**Examples**

This example shows how to remove the Telnet connection and the idle timeout from the FWSM configuration:

```
fwm/context_name(config)# clear telnet
```

Related Commands

show telnet

telnet

clear terminal

To remove the console terminal line parameter settings, use the **clear terminal** command.

clear terminal

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the console terminal line parameter settings from the FWSM configuration:

```
fwsM/context_name (config) # clear terminal
```

Related Commands **show telnet**
terminal

clear tftp-server

To remove the Trivial File Transfer Protocol (TFTP) server address and directory from the configuration, use the **clear tftp-server** command.

```
clear tftp-server [[interface_name] ip_address path]
```

Syntax Description

<i>interface_name</i>	(Optional) Interface name on which the TFTP server resides.
<i>ip_address</i>	(Optional) IP address or network of the TFTP server.
<i>path</i>	(Optional) Path and filename of the configuration file.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If not specified, an internal interface is assumed. If you specify the outside interface, a warning message informs you that the outside interface is unsecure. The contents of the path are passed directly to the server without interpretation or checking. The format for the path differs by the type of operating system on the server. The configuration file must exist on the TFTP server. Many TFTP servers require the configuration file to be world-writable to write to it and world-readable to read from it.

Examples

This example shows how to remove the TFTP server address and directory from the configuration:

```
fwsm/context_name(config)# clear tftp-server
```

Related Commands

show tftp-server
tftp-server

clear timeout

To remove the maximum idle time durations from the configuration, use the **clear timeout** command.

clear timeout

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the maximum idle time durations from the configuration:

```
fwsM/context_name (config) # clear timeout
```

Related Commands **show timeout**
timeout

clear uauth

To delete all the authorization caches for a user, use the **clear uauth** command.

```
clear uauth [username]
```

Syntax Description	<i>username</i> (Optional) Username to enter, to clear, or view user authentication information.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Security Context Mode: single context mode and multiple context mode Access Location: system and context command line Command Mode: privileged mode Firewall Mode: routed firewall mode and transparent firewall mode
----------------------	--

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines	The clear uauth command deletes one user or all the users' AAA authorization and authentication caches, which forces the user or users to reauthenticate the next time that they create a connection.
-------------------------	--

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. If you attempt to access a service that has been cached from the correct host, the FWSM considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The cache allows up to 16 address and service pairs for each user host.

The output from the **show uauth** command displays the username that is provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is authenticated only or has cached services.



Note

When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPSec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see to the **aaa** commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

This example shows how to cause the user “Pat” to reauthenticate:

```
fws(config)# clear uauth pat
```

Related Commands

show timeout

timeoutaaa authorization

show uauth

timeout

clear url-block

To clear the pending URL block buffer and long URL support usage counters, use the **clear url-block** command.

clear url-block

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines The “Current number of packets held (global)” counter is not cleared.

Examples This example shows how to clear the pending URL block buffer and long URL support usage counters:
`fwsm/context_name(config)# clear url-block`

Related Commands `show url-block`
`url-block`

clear url-cache

To disable URL caching, use the **clear url-cache** command.

clear url-cache

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to disable URL caching:

```
fwsM/context_name (config) # clear url-cache
```

Related Commands **show url-cache stat**
url-cache

clear url-server

To remove the URL filter server from the configuration, use the **clear url-server** command.

clear url-server

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the URL filter server from the configuration:

```
fws(config)# clear url-server
```

Related Commands

show url-server
url-server

clear username

To remove usernames from the user authentication local database, use the **clear username** command.

clear username

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: system and context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove usernames from the user authentication local database:

```
fwsn(config)# clear username
```

Related Commands **show username**
username

clear virtual

To remove the authentication virtual server from the configuration, use the **clear virtual** command.

clear virtual

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to remove the authentication virtual server from the configuration:

```
fwsM/context_name(config)# clear virtual
```

Related Commands **show virtual**
virtual

clear vpngroup

To clear the Easy VPN Remote configuration and security policy that is stored in the Flash partition, use the **clear vpngroup** command.

clear vpngroup

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
Access Location: context command line
Command Mode: configuration mode
Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Examples This example shows how to clear the Easy VPN Remote configuration and security policy that is stored in the Flash partition:

```
fwsm/context_name (config) # clear vpngroup
```

Related Commands **show vpngroup**
vpngroup

clear xlate

To clear the current translation and connection slot information, use the **clear xlate** command.

```
clear xlate [global | local ip1[-ip2] [netmask mask]] {gport | lport port1 [-port2]}
           [interface if1[,ifn]] [state static [,portmap] [,norandomseq] [,identity]] [debug] [count]
```

Syntax Description

global local ip1 -ip2	(Optional) Clears the active translations by global IP address or local IP address using the network mask to qualify the IP addresses.
netmask mask	
interface if1 ,if2 ,ifn	(Optional) Clears the active translations by interface.
gport lport port -port2	(Optional) Clears the active translations by local and global port specifications. See the “Specifying Port Values” section in Appendix B , “Port and Protocol Values,” for a list of valid port literal names.
interface	(Optional) Displays the active translations by interface.
if1 ,if2	(Optional) Specifies the interface.
state static	(Optional) Clears the active translations by state; valid values are static translation (static), dump (cleanup), PAT global (portmap), nat or static translation with the norandomseq setting (norandomseq), or the use of the nat 0 , or identity feature (identity).
,portmap	(Optional) Specifies the port map.
norandomseq	(Optional) Specifies no random sequence.
,identity	(Optional) Specifies the identity.
debug	(Optional) Specifies debugging.
count	(Optional) Specifies the count.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear xlate** command clears the contents of the translation slots. (“xlate” refers to the translation slot.) Always use the **clear xlate** command because translation slots can persist after adding, changing, or removing the **aaa-server**, **access-list**, **alias**, **global**, **nat**, **route**, or **static** commands in the configuration.

Examples

This example shows how to clear the current translation and connection slot information:

```
fwsM/context_name(config)# clear xlate global
```

Related Commands

show conn

show uauth

show xlate

timeout

compatible rfc1583

To restore the method that is used to calculate the summary route costs per RFC 1583, use the **compatible rfc1583** subcommand. To disable RFC 1583 compatibility, use the **no** form of this command.

[no] **compatible rfc1583**

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- OSPF routing is disabled on the FWSM.
- OSPF routing through the FWSM is compatible with RFC 1583.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The Open Shortest Path First (OSPF) protocol is used instead of the Routing Information Protocol (RIP). Do not attempt to configure the FWSM for both OSPF and RIP simultaneously.

The **compatible rfc1583** command is a subcommand of the **router ospf** command. The **router ospf** command is the global configuration command for OSPF routing processes running on the FWSM. The **compatible rfc1583** command is the main command for all of the OSPF configuration commands.

The **show ip ospf** command displays the configured **router ospf** subcommands.

The **compatible rfc1583** subcommand is displayed in the configuration only if it is disabled by the **no compatible rfc1583** subcommand. It displays as “no compatible rfc1583.”

Examples

This example shows how to restore the method that is used to calculate the summary route costs per RFC 1583:

```
fwsM#/context_name(config)# compatible rfc1583
```

Related Commands

router ospf

show ip ospf

configure

To configure from the terminal, Flash partition, or the network, use the **configure** command. To remove configurations, use the **clear configure** command.

configure [**terminal** | **memory**]

configure net [[*tftp_ip*]:*filename*]

Syntax Description

terminal	(Optional) Configures from the terminal connection.
memory	(Optional) Configures memory.
net	Loads the configuration from a TFTP server and the specified path.
<i>tftp_ip</i>	(Optional) IP address or name of the server from which to merge in a new configuration.
<i>filename</i>	(Optional) Filename that you specify to qualify the location of the configuration file on the TFTP server named in <i>server_ip</i> .

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can configure from the terminal, Flash partition, or the network. The new configuration merges with the active configuration.

You must be in privileged mode to use the **configuration** commands, except for the **configure terminal** (**confi t**) command which allows you to start configuration mode from the privileged mode. You can exit configuration mode with the **quit** command. Use the **write memory** command to store the changes in the Flash partition, or use the **write floppy** command to store the configuration on disk.

Each command from the Flash partition (with **configure memory**) and TFTP transfer (with **configure net**) is read and evaluated as follows:

- If the command in the Flash partition or on the disk is identical to an existing command in the current configuration, it is ignored.
- If the command in the Flash partition or on the disk is an additional instance of an existing command, then both commands appear in the current configuration.

- If the command redefines an existing command, the command on the disk or Flash partition overwrites the command in the current configuration in RAM. For example, if you have the **hostname ram** command in the current configuration and the **hostname floppy** command on the disk, the command in the configuration becomes **hostname floppy** and the command line prompt changes to match the new host name when that command is read from disk.

If you set a *filename* with the **tftp-server** command, do not specify it in the **configure** command; instead use a colon (:) without a filename.

The guidelines for the **configure net** command are as follows:

- The **configure net** command allows you to merge the current running configuration with a TFTP configuration stored at the IP address that you specify and from the file that you name. If you specify both the IP address and pathname in the **tftp-server** command, you can specify *server_ip:filename* as a colon (:). For example, you can specify **configure net :**.
- Use the **write net** command to store the configuration in the file.
- If you have an existing FWSM configuration on a TFTP server and store a shorter configuration with the same filename on the TFTP server, some TFTP servers will leave some of the original configuration after the first “:end” mark. This situation does not affect the FWSM because the **configure net** command stops reading when it reaches the first “:end” mark. This situation does not occur if you are using Cisco TFTP Server version 1.1 for Windows NT.



Note Many TFTP servers require the configuration file to be world-readable to be accessible.

The **configure memory** command allows you to merge the configuration in the Flash partition into the current configuration in RAM.

Examples

This example shows how to configure the FWSM using a configuration retrieved with TFTP:

```
fwsM/context_name(config)# configure net 10.1.1.1:tftp/config/fwsMconfig
```

The FWSM configuration file is stored on the TFTP server at 10.1.1.1 in the tftp/config folder.

This example shows how to configure the FWSM from the configuration that is stored in the Flash partition:

```
fwsM/context_name(config)# configure memory
```

Access privileged mode with the **enable** command and configuration mode with the **configure terminal** command. View the current configuration with the **write terminal** command and save the configuration to the Flash partition using the **write memory** command.

```
fwsM> enable
password:
fwsM# configure terminal
fwsM(config)# write terminal
: Saved
[... current configuration ...]
: End
fwsM(config)# write memory
```

When you enter the **configure factory-default** command on a platform other than the FWSM, the FWSM displays a “not supported” error message. On the FWSM, this message is displayed:

```
fws(config)# configure factory default  
'config factory-default' is not supported on FWSM
```

Related Commands **show configure**

config-url (context submode)

To set the URL from which the FWSM downloads the context file, use the **config-url** command.

[no] **config-url** *url*

Syntax Description	<i>url</i>	URL from which the FWSM downloads the context file (text format).
---------------------------	------------	---

Defaults	None.
-----------------	-------

Command Modes	Security Context Mode: multiple context mode Access Location: system command line Command Mode: configuration mode Firewall Mode: routed firewall mode and transparent firewall mode
----------------------	---

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines	When you add a context URL, the system immediately loads the context so that it is running, if the configuration is available.
-------------------------	--



Note

Enter the **allocate-interface (context submode)** command(s) before you enter the **config-url** command. The FWSM must assign interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (**interface**, **nat**, **global**...). If you enter the **config-url** command first, the FWSM loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

See the following URL syntax:

- **disk://[path]/filename**

The disk is a 64-MB partition of Flash that uses a navigable file system. The disk partition is used only for context storage. The system configuration and the software image reside in the Flash partition (called **flash**). The filename does not require a file extension, although we recommend using “.cfg”. If the configuration file is not available, you see the following message:

```
%Error opening disk://filename (File not found)
```

You can then change to the context, configure it at the CLI, and enter the **write memory** command to write the file to Flash memory.



Note

The admin context file must be stored on the internal Flash memory.

- **ftp://[user[:password]@]server/[path/]filename**
The server must be accessible from the admin context. The filename does not require a file extension, although we recommend using “.cfg”.
- **tftp://server/[path/]filename**
The server must be accessible from the admin context. The filename does not require a file extension, although we recommend using “.cfg”.
- **http://server/[path/]filename**
The server must be accessible from the admin context. The filename does not require a file extension, although we recommend using “.cfg”.
- **https://server/[path/]filename**
The server must be accessible from the admin context. The filename does not require a file extension, although we recommend using “.cfg”.

To change the URL, reenter the **config-url** command with a new URL. However, the new configuration does not overwrite the existing one; instead, the FWSM merges the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used.

Examples

This example shows how to set the console timeout to 15 minutes:

```
fws(config)# context cisco
fws/cisco(config)# allocate-interface vlan100 int0
fws/cisco(config)# allocate-interface vlan101 int1
fws/cisco(config)# member gold
fws/cisco(config)# config-url tftp://10.1.1.1/contexts/cisco.cfg
fws/cisco(config)# exit
fws(config)#
```

Related Commands

allocate-interface (context submode)

config-url (context submode)

member (context submode)

Other related commands

class

context

limit-resource (class submode)

context

To create a context and enter the context submode, use the **context** command. To remove the contexts from the running configuration and remove the context entry from the system configuration use the **clear context** command. To delete a single context, use the **no** form of this command.

[no] **context** *name*

Syntax Description

<i>name</i>	Sets the name as a string up to 32 characters long. This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. This name does not have to match the filename that is specified in the URL. “System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.
-------------	---

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode
 Access Location: system command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The FWSM supports 100 contexts.

You cannot enter any context commands until you have created the first context with the **admin-context** command. You cannot remove the current admin context with the **context** command. See the **admin-context** command for more information.

When you enter the context submode, the following commands are available:

- **allocate-interface**—Indicates the interfaces that are assigned to the context.
- **allocate-acl-partition**—Indicates the memory partition to which the context is assigned.
- **member**—Indicates class membership for a context.
- **config-url**—Indicates the URL for a context configuration.
- **description**—Provides a description of the context.

Examples

This example shows how to create a context:

```
fws(config)# context admincontext
fws(config_context)# allocate-interface vlan100 int0
fws(config_context)# allocate-interface vlan101 int1
fws(config_context)# member gold
fws(config_context)# config-url disk:/admin.cfg
fws(config_context)# exit
```

Related Commands

- admin-context
- allocate-interface (context submode)
- changeto
- class
- clear context
- config-url (context submode)
- description (submode)
- member (context submode)
- show context

copy capture

To copy a capture file to a TFTP server, use the **copy capture** command.

copy capture: `[[context-name/] capture_name tftp://server/pathname [pcap]]`

Syntax Description	Parameter	Description
	context-name/	(Optional) Context name.
	<i>capture_name</i>	Unique name that identifies the capture.
	tftp://server	Specifies the TFTP server.
	<i>pathname</i>	Pathname that indicates the last component of the path to the file on the server.
	pcap	(Optional) Specifies the defaults of the preconfigured TFTP server.

Defaults This command has no default settings.

Command Modes

- Security Context Mode: single context mode and multiple context mode
- Access Location: system and context command line
- Command Mode: privileged mode
- Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The FWSM must know how to reach the location (specified by the *tftp_pathname* argument) through its routing table information. This information is determined by the **ip address** command, the **route** command, or the RIP, depending upon the configuration. The *tftp_pathname* can include any directory names in addition to the last component of the path to the file on the server.

The *pathname* can include any directory names in addition to the last component of the path to the file on the server. The pathname cannot contain spaces. If a directory name has spaces, set the directory in the TFTP server instead of in the **copy tftp flash** command.



Note You cannot retrieve images prior to version 2.2 using this feature.

Examples

This example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
fwsM/context_name(config)# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!!
```

You can specify the full path as follows:

```
fwsM/context_name(config)# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap pcap
```

If the TFTP server is already configured, the location or filename can be unspecified as follows:

```
fwsM/context_name(config)# tftp-server outside 171.68.11.129 tftp/cdisk
fwsM/context_name(config)# copy capture:abc tftp:/tftp/abc.cap
```

This example shows how to use the defaults of the preconfigured TFTP server in the **copy capture** command:

```
fwsM/context_name(config)# copy capture:abc tftp:pcap
```

Related Commands

- cd**
- clear flashfs**
- copy disk**
- copy flash**
- copy http(s)**
- copy running-config/copy startup-config**
- copy tftp**
- dir**
- format**
- mkdir**
- more**
- pwd**
- rename**
- rmdir**
- show disk**
- show file**
- show flashfs**
- show http**
- show running-config**
- show startup-config**
- show tftp-server**

copy disk

To copy a file from the disk partition to a TFTP server, another location on the disk partition, to the Flash partition, or to the startup or running configuration, use the **copy disk** command.

```
copy [/noconfirm] disk:[path] tftp:[[/server][[/pathname]]]
```

```
copy [/noconfirm] disk:[path] disk:[path]
```

```
copy [/noconfirm] disk:[path] [flash:[image | pdm]]
```

```
copy [/noconfirm] disk:[path] [startup-config | running-config]
```

```
copy [/noconfirm] disk:[path] ftp://[user[:password]@] server [pathname] [;type=xx]
```

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
<i>path</i>	(Optional) Path to the file location.
tftp	Specifies the TFTP server.
<i>server</i>	(Optional) IP address or name of the server that is set with the name command.
<i>pathname</i>	(Optional) Directory path and filename to which to copy.
disk:	Specifies the disk partition that you are copying.
flash	(Optional) Specifies that the copy target is the Flash partition.
image	(Optional) Specifies that the image is copied.
pdm	(Optional) Specifies that a PDM file is copied to the default Flash partition.
startup-config	(Optional) Specifies that a file is copied to the startup configuration.
running-config	(Optional) Specifies that a file is copied to the running configuration.
ftp	Specifies FTP transactions.
<i>user</i>	(Optional) Username for the FTP transfer.
<i>:password</i>	(Optional) Password for logging into the FTP server.
@	(Optional) Separates the login information from the server address.
;type=xx	(Optional) Specifies the type of transfer. xx is ap , ah , ip (default), or in .

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When you copy the image to Flash on the FWSM, the image is not available until you reboot. The downloaded PDM image files are available to the FWSM immediately without a reboot. If you copy a file to the startup partition, you must either reboot or use the **copy start run** command. If you specify TFTP without the : (colon), you get a prompt.

Examples

This example shows how to copy a file from the disk to a TFTP server:

```
fwsM/context_name(config)# copy disk:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

This example shows how to copy a file from one location on the disk to another location on the disk. The name of the destination file can be either the name of the source file or a different name.

```
fwsM/context_name(config)# copy disk:my_context.cfg disk:my_context/my_context.cfg
```

This example shows how to copy an image or a PDM file from the disk to the Flash partition:

```
fwsM/context_name(config)# copy disk:cdisk flash:image
fwsM/context_name(config)# copy disk:pdm flash:pdm
```

This example shows how to copy a file from the disk to the startup configuration or a running configuration:

```
fwsM/context_name(config)# copy disk:my_context/my_context.cfg startup-config
fwsM/context_name(config)# copy disk:my_context/my_context.cfg running-config
```

Related Commands

- cd
- clear flashfs
- copy capture
- copy flash
- copy http(s)
- copy running-config/copy startup-config
- copy tftp
- copy tftp
- dir
- format
- mkdir
- more
- pwd
- rename
- rmdir
- show disk

show file
show flashfs
show running-config
show startup-config
show tftp-server

copy flash

To copy a file from the Flash partition to a TFTP server, to the disk partition, or to the startup or running configuration, use the **copy flash** command.

```
copy flash[:[image | pdm]] tftp:[[/server][/pathname]]
```

```
copy [/noconfirm] flash:[image | pdm] disk:[path]
```

Syntax Description

image	(Optional) Specifies that the image is copied.
pdm	(Optional) Specifies that a PDM file is copied.
tftp	Specifies the TFTP server.
<i>server</i>	(Optional) IP address or name that you set with the name command.
<i>pathname</i>	(Optional) Directory path and filename.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	Specifies that the copy target is the disk partition.
<i>path</i>	(Optional) Path to the file location.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you specify TFTP without the : (colon), you get a prompt.

Examples

This example show how to copy an image or a PDM file from the Flash partition to a TFTP server:

```
fswm/context_name(config)# copy flash:image tftp://10.7.0.80/image
fswm/context_name(config)# copy flash:pdm tftp://10.7.0.80/FWSM/pdm
```

This example shows how to copy an image or PDM file from the Flash partition to a disk:

```
fswm/context_name(config)# copy flash:image disk:cdisk
fswm/context_name(config)# copy flash:pdm disk:pdm
```

Related Commands

- cd
- clear flashfs
- copy capture
- copy http(s)
- copy running-config/copy startup-config
- copy tftp
- dir
- format
- mkdir
- more
- pwd
- rename
- rmdir
- show disk
- show file
- show flashfs
- show running-config
- show startup-config
- show tftp-server

copy ftp

To copy a file from the Flash partition to a TFTP server, to the disk partition, or to the startup or running configuration, use the **copy flash** command.

```
copy ftp://[user[:password]@] location/pathname [;type=<xx>] [startup-config running-config]
```

```
copy [/noconfirm] ftp://[user[:password]@] location/pathname [;type=<xx>] [startup-config running-config]
```

Syntax Description

<i>user</i>	(Optional) Username for logging into the HTTP server.
<i>password@</i>	(Optional) Password for logging into the HTTP server.
location/pathname	IP address or name that you set with the name command.
;type=xx	(Optional) Specifies the type of transfer. xx is ap , ah , ip (default), or in .
/noconfirm	(Optional) Specifies not to prompt for confirmation.
startup-config	(Optional) Specifies the startup configuration.
running-config	(Optional) Specifies the running configuration.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you specify FTP without the : (colon), you get a prompt.

Examples

This example shows how to copy a file from the disk to the startup configuration or a running configuration:

```
fwsM/context_name(config)# copy ftp:my_context/my_context.cfg startup-config
fwsM/context_name(config)# copy ftp:my_context/my_context.cfg running-config
```

Related Commands

cd
clear flashfs

copy capture
copy http(s)
copy running-config/copy startup-config
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir
show disk
show file
show flashfs
show running-config
show startup-config
show tftp-server

copy http(s)

To copy files from an HTTPS server, use the **copy http[s]** command.

```
copy http[s]://[user:password@] server [:port]/pathname flash:[image | pdm]
```

```
copy [/noconfirm] http[s]://[user:password@]location [:port]/pathname disk:[pathname]
```

```
copy http[s]://[user:password@]server[:port]/pathname {startup-config | running-config}
```

Syntax Description

<i>user</i>	(Optional) Username for logging into the HTTPS server.
<i>password@</i>	(Optional) Password for logging into the HTTPS server.
<i>server</i>	Server name.
<i>location</i>	(Optional) IP address or name that you set with the name command.
<i>port</i>	(Optional) Port to contact on the HTTP server.
<i>pathname</i>	(Optional) Name of the resource that contains the FWSM software image or PDM file to copy.
flash	Specifies the location for the download in the Flash partition.
image	(Optional) Downloads the selected FWSM image to the Flash partition.
pdm	(Optional) Downloads the selected PDM image file to the Flash partition.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk	Specifies the location for the download is to disk.
startup-config	(Optional) Specifies the startup configuration.
running-config	(Optional) Specifies the running configuration.

Defaults

The default *port* is 80 for HTTP and 443 for HTTPS.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	This command was introduced
2.2(1)	Support for this command was modified to add the disk, startup and running configuration on the FWSM.

Usage Guidelines

If you specify TFTP without the : (colon), you get a prompt.

Examples

This example shows how to copy the FWSM software image from a public HTTP server into the Flash partition of the FWSM:

```
fwsM/context_name(config)# copy http://171.68.11.129/auto/cdisk flash:image
```

This example show how to copy the PDM software image through HTTPS (HTTP over SSL), where the SSL authentication is provided by the username “alice” and the password “xyz”:

```
fwsM/context_name(config)# copy https://alice:xyz@171.68.11.129/auto/pdm.bin flash:pdm
```

This example shows how to copy the FWSM software image from an HTTPS server running on a nonstandard port, where the file is copied into the software image space in the Flash partition by default:

```
fwsM/context_name(config)# copy https://alice:zyx@171.68.11.129:8080/auto/cdisk flash
```

**Note**

When entering the “?” character in a URL, press **Ctrl-v** first.

Related Commands

- cd
- clear flashfs
- copy capture
- copy disk
- copy flash
- copy ftp
- copy running-config/copy startup-config
- copy tftp
- dir
- format
- mkdir
- more
- pwd
- rename
- rmdir
- show disk
- show file
- show flashfs
- show running-config
- show startup-config
- show tftp-server

copy running-config/copy startup-config

To copy the running or startup configuration TFTP or FTP server to the disk partition, use the **copy running-config** or **copy startup-config** command.

copy running-config startup-config

copy startup-config running-config

copy [startup-config | running-config] tftp[:[//location][/pathname]]

copy [/noconfirm] [startup-config | running-config] disk:[path]

copy [startup-config | running-config] ftp://[user[:password]@]location/pathname[;type= xx]

Syntax Description		
running-config	(Optional)	Specifies that a file is copied to the running configuration.
startup-config	(Optional)	Specifies that a file is copied to the startup configuration.
tftp		Specifies that the copy is through TFTP.
<i>//location</i>	(Optional)	IP address of the server.
<i>/pathname</i>	(Optional)	Directory where the files are copied.
/noconfirm	(Optional)	Specifies not to prompt for confirmation.
disk:		Specifies the copy target is the disk partition.
<i>path</i>	(Optional)	Path to the file location.
ftp		Specifies that the copy is through FTP.
<i>user</i>	(Optional)	User.
<i>password</i>	(Optional)	User password.
;type=xx	(Optional)	Specifies the type of transfer. xx is ap , ah , ip (default), or in .

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you specify TFTP without the : (colon), you get a prompt.

Examples

This example shows how to copy the running configuration to the startup configuration file:

```
fws(config)# copy running-config startup-config
```

This example shows how to copy a running configuration file to a TFTP server:

```
fws(config)# copy running-config tftp://10.7.0.80/FWSM/my_context/my_context.cfg
```

This example shows how to copy the startup or running configuration to a disk:

```
fws(config)# copy startup-config disk:my_context/my_context.cfg  
fws(config)# copy running-config disk:my_context/my_context.cfg
```

This example shows how to copy the startup configuration to the running configuration:

```
fws(config)# copy startup-config running-config
```

This example shows how to copy the startup or running configuration to a TFTP server:

```
fws(config)# copy startup-config tftp://10.7.0.80/fws/#/my_context/my_context.cfg  
fws(config)# copy running-config tftp://10.7.0.80/fws/#/my_context/my_context.cfg
```

Related Commands

- cd
- clear flashfs
- copy capture
- copy disk
- copy flash
- copy ftp
- copy http(s)
- copy tftp
- dir
- format
- mkdir
- more
- pwd
- rename
- rmdir
- show disk
- show file
- show flashfs
- show running-config
- show startup-config
- show tftp-server

copy tftp

To download the Flash partition software images through TFTP without using monitor mode, use the **copy tftp** command.

```
copy tftp://[location]/[pathname] flash:[image][pdm]
```

```
copy[/noconfirm] tftp://[location]/[pathname] disk:[path]
```

```
copy tftp://server]/[pathname] {startup-config | running-config}
```

Syntax Description

<i>location</i>	(Optional) IP address or name that you set with the name command.
<i>pathname</i>	(Optional) Directory path and filename.
flash	Specifies the Flash partition.
image	(Optional) Downloads the selected FWSM image to the Flash partition.
pdm	(Optional) Downloads the selected PDM image files to the Flash partition.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	Specifies that the copy target is the disk partition.
<i>path</i>	(Optional) Path to the file location.
startup-config	(Optional) Specifies that a file is copied to the startup configuration.
running-config	(Optional) Specifies that a file is copied to the running configuration.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	This command was introduced on the FWSM.
2.2(1)	Support was added for disk, startup and tunning configuration options.

Usage Guidelines

The **copy tftp flash** command allows you to download a PDM software image through TFTP. If you specify TFTP without the **:** (colon), you get a prompt.

If the command is used without the **tftp** keyword or *pathname* optional arguments, you are prompted for the server address and filename.

The *pathname* can include any directory names and the last component of the path to the file on the server. The *pathname* cannot contain spaces.

If you configure the TFTP server to point to a directory on the system from which you are downloading the image, you need to use only the IP address of the system and the image filename.

Examples

This example shows how to make the FWSM prompt you for the filename and server before you start the TFTP download:

```
fwsM(config)# copy tftp flash:
Address or name of remote host [127.0.0.1]? 10.1.1.5
Source file name [cdisk]? fwsM.bin
copying tftp://10.1.1.5/fwsM.bin to Flash
[yes|no|again]? yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
Received 1695744 bytes.
Erasing current image.
Writing 1597496 bytes of image.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
Image installed.
```

```
fwsM(config)# copy tftp://10.0.0.1/fwsM512.bin flash:
```

This example shows how to map an IP address to the TFTP host name with the **name** command and use the **tftp-host** keyword for the *location* argument:

```
fwsM(config)# name 10.1.1.6 tftp-host
fwsM(config)# copy tftp://tftp-host/fwsM512.bin flash:
fwsM(config)# copy tftp://tftp-host/tftpboot/fwsM512.bin flash:
```

This example shows how to copy a file from a TFTP server to a disk. If the file does not fit in the available space, then an error message is printed.

```
fwsM(config)# copy tftp://10.7.0.80/FWSM/my_context.cfg disk:my_context/my_context.cfg
```

Related Commands

- cd
- clear flashfs
- copy capture
- copy disk
- copy flash
- copy ftp
- copy http(s)
- copy running-config/copy startup-config
- dir
- format
- mkdir
- more
- pwd
- rename
- rmdir
- show disk

show file
show flashfs
show running-config
show startup-config
show tftp-server

crashdump force

To force a crash of the FWSM, use the **crashdump** command.

crashdump force [**page-fault** | **watchdog**]

Syntax Description

page-fault	(Optional) Forces a crash of the FWSM with a page fault.
watchdog	(Optional) Forces a crash of the FWSM as a result of watchdogging.

Defaults

The crash information file is saved to the Flash partition.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines



Caution

Be careful entering the **crashdump force** command because it crashes the FWSM and forces it to reload.

The **crashdump force page-fault** command crashes the FWSM as a result of a page fault, and the **crashdump force watchdog** command crashes the FWSM as a result of watchdogging. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashdump force page-fault** or **crashdump force watchdog** command (because these are real crashes). The FWSM reloads after the crash dump is complete.

When you enter the **crashdump force page-fault** command, a warning prompt similar to the following is displayed:

```
fws(config)# crashdump force page-fault
WARNING: This command will force the FWSM to crash and reboot.
Do you wish to proceed? [confirm]:
```

If you enter a carriage return by pressing the Return or enter key, “Y,” or “y,” the FWSM crashes and reloads; all three of these actions are interpreted as confirmation. Any other character is interpreted as a no, and the FWSM returns to the command-line configuration mode prompt.

Related Commands

clear crashdump
failover

show crashdump

crypto dynamic-map

To create a dynamic crypto map entry and enter the crypto dynamic map subcommand mode, use the **crypto dynamic-map** command. Use the **no** form of this command to delete a dynamic crypto map set or entry.

[no] **crypto dynamic-map** *map seq*

Syntax Description

<i>map</i>	Name of the dynamic crypto map set.
<i>seq</i>	Sequence number that corresponds to the dynamic crypto map entry.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

For more detailed help, refer directly to the CLI subcommand in the mode where they are available; for example: **ca ?** or **help ca**.



Note

The **crypto dynamic-map** subcommands are described with the **crypto map client** command. If the peer initiates the negotiation and the local configuration specifies perfect forward secrecy (PFS), the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, a default of group1 is assumed, and an offer of either group1 or group2 is accepted. If the local configuration specifies group2, that group must be part of the peer's offer or the negotiation fails. If the local configuration does not specify PFS, it accepts any offer of PFS from the peer.

The **crypto dynamic-map** subcommands are as follows:

- **match address** *access_list_name*—See the **crypto map set peer** command.
- **set peer** *ip-address*—See the **crypto map set peer** command.
- **set pfs** [**group1** | **group2**]—See the **crypto map set pfs** command.
- **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*—See the **crypto map set security-association lifetime** command.
- **set transform-set** *proposal [proposal ...]*—See the **crypto map set transform-set** command.



Note The **crypto map set transform-set** command is required for dynamic crypto map entries.

The **crypto dynamic-map** command allows you to create a dynamic crypto map entry. The **no crypto dynamic-map** command deletes a dynamic crypto map set or entry. The **clear crypto dynamic-map** removes all of the **crypto dynamic map** commands. Specifying the name of a given crypto dynamic map removes the associated **crypto dynamic map** commands. You can also specify the dynamic crypto map's sequence number to remove all of the associated **crypto dynamic map** commands. The **show crypto engine** command allows you to see a dynamic crypto map set.

Dynamic crypto maps are policy templates that are used when processing negotiation requests for new security associations from a remote IPSec peer, even if you do not know all of the crypto map parameters that are required to communicate with the peer (such as the peer's IP address). For example, if you do not know about all the remote IPSec peers in the network, a dynamic crypto map lets you accept requests for new security associations from previously unknown peers. (However, these requests are not processed until the Internet Key Exchange (IKE) authentication has completed successfully.)

When the FWSM receives a negotiation request through IKE from another peer, the FWSM examines the request to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, the request is rejected unless the crypto map set includes a reference to a dynamic crypto map.

The dynamic crypto map accepts "wildcard" parameters for any parameters that are not explicitly stated in the dynamic crypto map entry. This situation lets you set up IPSec security associations with a previously unknown peer. (The peer still must specify matching values for the "wildcard" IPSec security association negotiation parameters.)

If the FWSM accepts the peer's request, it installs the new IPSec security associations at the same time that it installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. The FWSM performs normal processing, using this temporary crypto map entry as a normal entry, even when it requests new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is removed.

The **crypto dynamic-map** commands are used for determining whether or not traffic should be protected. The only keyword that is required in a **crypto dynamic-map** command is the **set transform-set** keyword. All other keywords are optional.

Examples

This example shows how to configure an IPSec crypto map set:

```
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 101
fwsm/context_name(config)# crypto map mymap 10 set transform-set my_t_set1
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
fwsm/context_name(config)# crypto map mymap 20 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 20 match address 102
fwsm/context_name(config)# crypto map mymap 20 set transform-set my_t_set1 my_t_set2
fwsm/context_name(config)# crypto map mymap 20 set peer 10.0.0.3
fwsm/context_name(config)# crypto dynamic-map mydynamicmap 10 match address 103
fwsm/context_name(config)# crypto dynamic-map mydynamicmap 10 set transform-set my_t_set1
my_t_set2 my_t_set3
fwsm/context_name(config)# crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
```

In the previous example, the crypto map entry **mymap 30** references the dynamic crypto map set **mydynamicmap**, which can be used to process inbound security association negotiation requests that do not match **mymap** entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in **mydynamicmap** for a flow “permitted” by the access list 103, IPSec accepts the request and sets up security associations with the remote peer without previously knowing about the peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings that are specified by the remote peer.

The access list that is associated with **mydynamicmap 10** is also used as a filter. Inbound packets that match a permit entry in this list are dropped for not being IPSec protected. (The same is true for access lists that are associated with static crypto maps entries.) Outbound packets that match a permit entry without an existing corresponding IPSec security association are also dropped.

Related Commands

[clear crypto dynamic-map](#)
[show crypto map](#)

crypto ipsec security-association lifetime

To set global lifetime values used when negotiating IPSec security associations, use the **crypto ipsec security-association lifetime** command. To return to the default values, use the **no** form of this command.

[no] crypto ipsec security-association lifetime {seconds *seconds* | kilobytes *kilobytes*}

Syntax Description	seconds <i>seconds</i>	kilobytes <i>kilobytes</i>
	Specifies the number of seconds that a security association lives before it expires.	Specifies the volume of traffic (in kilobytes) that passes between IPSec peers using a given security association before that security association expires.

Defaults

The defaults are as follows:

- **seconds *seconds*** is 28,800 seconds (8 hours).
- **kilobytes *kilobytes*** is 4,608,000 KB (10 Mbps for one hour).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

For more detailed help, refer directly to the CLI subcommand in the mode where they are available; for example, **ca ?** or **help ca**.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry does not have lifetime values configured, when the FWSM requests new security associations during security association negotiation, it specifies its global lifetime value in the request to the peer. It uses this value as the lifetime of the new security associations. When the FWSM receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after either of these lifetimes is reached.

If you change a global lifetime, the change is applied only when the crypto map entry does not have a lifetime value specified. The change is not applied to existing security associations but is used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the [clear crypto ipsec sa](#) command.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key. Shorter lifetimes require more CPU processing time for establishing new security associations. The lifetime values are ignored for manually established security associations (security associations installed using an **ipsec-manual crypto map** command entry).

The security association (and corresponding keys) expires according to whichever occurs sooner, either after the number of seconds has passed (specified by the **seconds** keyword) or after the amount of traffic in kilobytes has passed (specified by the **kilobytes** keyword).

A new security association is negotiated before the lifetime threshold of the existing security association is reached to ensure that a new security association is ready for use when the old one expires. The new security association is negotiated either 30 seconds before the seconds lifetime expires or when the volume of traffic through the tunnel reaches 256 KB less than the **kilobytes** lifetime (whichever occurs first).

If no traffic passes through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association is negotiated only when IPsec sees another packet that should be protected.

Examples

This example shortens the IPsec SA lifetimes. The time-out lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2,304,000 KB (10 Mbps for 30 minutes).

```
fwsM/context_name(config)# crypto ipsec security-association lifetime seconds 2700
fwsM/context_name(config)# crypto ipsec security-association lifetime kilobytes 2304000
```

Related Commands

[clear crypto ipsec sa](#)
[show crypto ipsec](#)

crypto ipsec transform-set

To create and configure a transform set, use the **crypto ipsec transform-set** command. To delete a transform set or return to the default transport mode, use the **no** form of this command.

```
[no] crypto ipsec transform-set transform-set-name {{transform1 [transform2 [transform3]]} |
mode transport }
```

```
crypto ipsec transform-set transform-set-name [ah-md5-hmac | ah-sha-hmac] [esp-des |
esp-des-192 | esp-des-256 | esp-des | esp-3des | esp-null] [esp-md5-hmac | esp-sha-hmac]
```

Syntax Description

<i>transform-set-name</i>	Name of the transform set to create or modify.
<i>transform1</i> <i>transform2</i> <i>transform3</i>	Up to three transforms to create or modify.
mode transport	Specifies that the FWSM negotiate with a Windows 2000 Layer 2 TP/IPSec client.
ah-md5-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using MD5.
ah-sha-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using SHA.
esp-des	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a 128-bit key.
esp-des-192	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a 192-bit key.
esp-des-256	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a 256-bit key.
esp-null	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a null key.
esp-md5-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a md5 key.
esp-sha-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with an sha key.

Defaults

Tunnel mode

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Transforms define the IPsec security protocol(s) and algorithm(s). Each transform represents an IPsec security protocol (Encapsulating Security Payload (ESP), authenticating header (AH), or both) and the algorithm that you want to use.

The Windows 2000 Layer 2 Tunneling Protocol (L2TP)/IPsec client uses IPsec transport mode, so **transport** mode must be selected on the transform set. For FWSM version 1.1 and later releases, L2TP is the only protocol that can use the IPsec transport mode. All other types of packets using IPsec transport mode are discarded by the FWSM.

**Note**

A transport mode transform can only be used on a **dynamic** crypto map, and the FWSM CLI displays an error if you attempt to tie a transport-mode transform to a **static** crypto map.

Tunnel mode is automatically enabled for a transform set, so you do not have to explicitly configure the **mode** when tunnel mode is desired.

A transform set specifies one or two IPsec security protocols (either ESP or AH or both) and specifies which algorithms to use with the selected security protocol. During the IPsec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

IPsec messages can be protected by a transform set using des and 3des with a 128-bit key, 192-bit key, or 256-bit key.

This example uses the des and 3des 192-bit key transform:

```
fwsM(config)# crypto ipsec transform-set standard esp-des-192 esp-md5-hmac
```

**Note**

Des and 3des support is available on the FWSMs that are licensed for VPN-3DES only.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set that is defined in the crypto map entry is used in the IPsec security association negotiation to protect the data flows specified by that crypto map entry's access list. During the negotiation, the peers search for a transform set that is the same at both peers. When a transform set is found, it is selected and is applied to the protected traffic as part of both peer's IPsec security associations.

When security associations are established manually, you must use a single transform set. The transform set is not negotiated.

Before a transform set can be included in a crypto map entry, you must define it by entering the **crypto ipsec transform-set** command.

To define a transform set, you specify one to three "transforms"—each transform represents an IPsec security protocol (ESP or AH) and the algorithm that you want to use. When the particular transform set is used during negotiations for IPsec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set, you can specify the AH protocol or the ESP protocol. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

Examples of acceptable transform combinations are as follows:

- **ah-md5-hmac**
- **esp-des**
- **esp-des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**

If you specify one or more transforms in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms replace the existing transforms for that transform set.

If you change a transform set definition, the change is applied only to crypto map entries that reference the transform set. The change is not applied to existing security associations but is used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto ipsec sa** command.

Examples

This example defines one transform set (named “standard”), which is used with an IPSec peer that supports the ESP protocol. Both an ESP encryption transform and an ESP authentication transform are specified in this example.

```
fws(config)# crypto ipsec transform-set standard esp-des esp-md5-hmac
```

Related Commands

show crypto ipsec

crypto map client

To create or modify a crypto map entry, use the **crypto map client** command. To return to the default settings, use the **no** form of this command.

crypto map *map-name* **client** [**token**] **authentication** *aaa-server-name*

crypto map *map-name* **client authentication** *aaa-server-name* [**LOCAL**]

crypto map *map-name* **client configuration address** { **initiate** | **respond** }

no crypto map *map-name* **client**

Syntax Description

<i>map-name</i>	Name of the crypto map set.
token	(Optional) Indicates a token-based server for user authentication.
authentication	(Optional) Indicates that the key string is to be used with the ESP authentication transform.
<i>aaa-server-name</i>	Name of the AAA server that will authenticate the user during Internet Key Exchange (IKE) authentication; valid values are TACACS+ , RADIUS , or LOCAL .
LOCAL	(Optional) Specifies a predefined server tag for the AAA local protocol.
configuration address	Configures the IKE mode configuration.
initiate	Indicates that the FWSM will attempt to set IP addresses for each peer.
respond	Indicates that the FWSM will accept requests for IP addresses from any requesting peer.

Defaults

The default settings are as follows:

- Xauth feature is not enabled.
- IKE mode configuration is not enabled.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **crypto map client authentication** command allows you to enable the Extended Authentication (Xauth) feature. This feature lets you prompt for a TACACS+, RADIUS, or LOCAL username and password during IKE authentication. You must first set up the AAA server configuration to use this feature, and be sure to specify the same AAA server name within the **crypto map client authentication** command as was specified in the **aaa-server** command. This command is required only when the crypto map entry's transform set includes an Encapsulation Security Payload (ESP) authentication transform.

You can enter the **LOCAL** optional keyword for the group tag value and use the local FWSM database AAA services such as local command authorization privilege levels. LOCAL is the only second authentication method. The **authorization** command only accepts the LOCAL option when the *server_tag* refers to an existing and valid AAA TACACS+ or RADIUS server group defined in an **aaa-server** configuration command.

This command tells the FWSM during Phase 1 of IKE to use the Xauth (RADIUS, TACACS+, or LOCAL) challenge to authenticate IKE. If the Xauth fails, the IPsec security association is not established, and the IKE security association is deleted. Use the **no crypto map client authentication** command to restore the default value. The Xauth feature is not enabled by default.

**Note**

When Xauth is enabled, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in network extension mode, the IPsec tunnel is created from network to network, so that the users behind the FWSM cannot be associated with a single IP address. A uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the FWSM. For more information on AAA authentication proxies, see the **aaa** commands.

You cannot enable Xauth or IKE mode configuration on an interface when terminating a Layer 2 Tunneling Protocol (L2TP)/IPsec tunnel using the Microsoft L2TP/IPsec client v1.0 (which is available on Windows NT, Windows XP, Windows 98, and Windows ME OS). Instead, you can do either of the following:

- Use a Windows 2000 L2TP/IPsec client.
- Use the **isakmp key keystring address ip-address netmask mask no-xauth no-config-mode** command to exempt the L2TP client from Xauth and IKE mode configuration. However, if you exempt the L2TP client from Xauth or IKE mode configuration, all the L2TP clients must be grouped with the same ISAKMP preshared key or certificate and have the same fully qualified domain name.

The **crypto map client token authentication** command allows you to enable the FWSM to interoperate with a Cisco VPN 3000 Client that is set up to use a token-based server for user authentication. The **token** keyword tells the FWSM that the AAA server uses a token-card system and to prompt the user for the username and password during IKE authentication. Enter the **no crypto map client token authentication** command to restore the default value.

**Note**

The remote user must run Cisco VPN Client version 3.x, Cisco VPN 3000 Client version 2.5/2.6 or higher, or Cisco Secure VPN Client version 1.1 or higher.

The AAA server optional keywords that are available are TACACS+, RADIUS, or LOCAL.

If you specify **LOCAL** and the local user credential database is empty, this message displays:

```
Warning:local database is empty! Use \Qusername' command to define local users.
```

If the local database becomes empty when LOCAL is still present in the command, this message displays:

```
Warning:Local user database is empty and there are still commands using LOCAL for authentication.
```

The **crypto map client configuration address** command allows you to configure IKE mode configuration on the FWSM. IKE mode configuration allows the FWSM to download an IP address to the remote peer (client) as part of an IKE negotiation. When you enter the **crypto map client configuration address** command, you define the crypto map(s) that should attempt to configure the peer.

The **initiate** keyword indicates that the FWSM will attempt to set IP addresses for each peer. The **respond** keyword indicates that the FWSM will accept requests for IP addresses from any requesting peer.



Note

If you use IKE mode configuration on the FWSM, the routers handling the IPsec traffic must also support IKE mode configuration. Cisco IOS Release 12.0(6)T and later releases support IKE mode configuration.

Examples

This example shows how to set up the IPsec rules for VPN encryption IPsec. The **ip**, **nat**, and **aaa-server** commands establish the context for the IPsec-related commands.

```
fwsM/context_name(config)# ip address inside 10.0.0.1 255.255.255.0
fwsM/context_name(config)# ip address outside 168.20.1.5 255.255.255.0
fwsM/context_name(config)# dealer 10.1.2.1-10.1.2.254
fwsM/context_name(config)# nat (inside) 0 access-list 80
fwsM/context_name(config)# aaa-server TACACS+ protocol tacacs+
fwsM/context_name(config)# aaa-server TACACS+ (inside) host 10.0.0.2 secret123
fwsM/context_name(config)# crypto ipsec transform-set pc esp-des esp-md5-hmac
fwsM/context_name(config)# crypto dynamic-map cisco 4 set transform-set pc
fwsM/context_name(config)# crypto map partner-map 20 ipsec-isakmp dynamic cisco
fwsM/context_name(config)# crypto map partner-map client configuration address initiate
fwsM/context_name(config)# crypto map partner-map client authentication TACACS+
fwsM/context_name(config)# crypto map partner-map interface outside
fwsM/context_name(config)# isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
fwsM/context_name(config)# isakmp client configuration address-pool local dealer outside
fwsM/context_name(config)# isakmp policy 8 authentication pre-share
fwsM/context_name(config)# isakmp policy 8 encryption des
fwsM/context_name(config)# isakmp policy 8 hash md5
fwsM/context_name(config)# isakmp policy 8 group 1
fwsM/context_name(config)# isakmp policy 8 lifetime 86400
```

This example shows how to configure IKE mode configuration on the FWSM:

```
fwsM/context_name(config)# crypto map mymap client configuration address initiate
fwsM/context_name(config)# crypto map mymap client configuration address respond
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map interface

To apply a previously defined crypto map set to an interface, use the **crypto map interface** command. To remove the crypto map set from the interface, use the **no** form of this command.

[no] crypto map *map-name* **interface** *interface-name*

Syntax Description

<i>map-name</i>	Name of the crypto map set.
interface <i>interface-name</i>	Specifies the identifying interface to be used by the FWSM to identify itself to peers.

Defaults

The default settings are as follows:

- Xauth feature is not enabled.
- Internet Key Exchange (IKE) mode configuration is not enabled.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **crypto map interface** command allows you to assign a crypto map set to any active FWSM interface. The FWSM supports IPSec termination on any and all active interfaces. You must assign a crypto map set to an interface before that interface can provide IPSec services.

Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same *map-name* but a different *seq-num*, they are considered to be part of the same set and will all be applied to the interface. The crypto map entry with the lowest *seq-num* is considered the highest priority and is evaluated first. A single crypto map set can contain a combination of ipsec-isakmp and ipsec-manual crypto map entries.



Caution

Using the **crypto map interface** command reinitializes the security association database and causes any currently established security associations to be deleted.

If you enable IKE, and you are using a certification authority (CA) to obtain certificates, you must enable IKE with the interface address that is specified in the CA certificates.

Examples

This example assigns the crypto map set “mymap” to the outside interface. When traffic passes through the outside interface, the traffic is evaluated against all the crypto map entries in the “mymap” set. When outbound traffic matches an access list in one of the “mymap” crypto map entries, a security association (if IPsec) is established if no security association or connection already exists.

```
fwsn/context_name(config)# crypto map mymap interface outside
```

Related Commands

- crypto map client**
- crypto map interface**
- crypto map ipsec**
- crypto map set peer**
- crypto map set security-association lifetime**
- crypto map set session-key**
- crypto map set transform-set**
- crypto map set peer**
- show crypto map**

crypto map ipsec

To create or modify a crypto map entry, use the **crypto map ipsec** command. To delete a crypto map entry or set, use the **no** form of this command.

```
[no] crypto map map-name seq-num {ipsec-isakmp | ipsec-manual}
      [dynamic dynamic-map-name]
```

Syntax Description		
<i>map-name</i>		Name of the crypto map set.
<i>seq-num</i>		Number used to rank multiple crypto map entries within a crypto map set.
ipsec-isakmp		Specifies an ipsec-isakmp crypto map entry.
ipsec-manual		Specifies an ipsec-manual crypto map entry.
dynamic	(Optional)	Specifies that a given crypto map entry is to reference a
<i>dynamic-map-name</i>		specified dynamic crypto map.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

After you define crypto map entries, you can use the **crypto map interface** command to assign the crypto map set to interfaces.

Crypto maps can filter or classify traffic to be protected and define the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed through the IKE on behalf of that traffic.

IPSec crypto maps link together definitions of the following:

- What traffic should be protected
- IPSec peer(s) to which the protected traffic can be forwarded—these are the peers with which a security association can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and security associations should be used/managed (or what the keys are if IKE is not used)

A crypto map set is a collection of crypto map entries each with a different *seq-num* but the same *map-name*. For a given interface, you could have certain traffic forwarded to one peer with specified security applied to that traffic, and other traffic forwarded to the same or a different peer with different IPSec security applied. To accomplish this situation, you would create two crypto map entries, each with the same *map-name*, but each with a different *seq-num*.

The number that you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

Use the **crypto dynamic-map** command to create dynamic crypto map entries. After you create a dynamic crypto map set, use the **crypto map ipsec-isakmp dynamic** command to add the dynamic crypto map set to a static crypto map.

Give the lowest priority map entries to the crypto map entries that reference the dynamic map set. This action allows the inbound security association negotiation requests to try to match the static maps first. If the request does not match any of the static maps, set the entries to be evaluated against the dynamic map set.

To make a crypto map entry that references a dynamic crypto map to be set to the lowest priority map entry, give the map entry the highest *seq-num* of all the map entries in a crypto map set.

Examples

This example shows the minimum required crypto map configuration when IKE is used to establish the security associations:

```
fwsM/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsM/context_name(config)# crypto map mymap 10 match address 101
fwsM/context_name(config)# crypto map mymap set transform-set my_t_set1
fwsM/context_name(config)# crypto map mymap set peer 10.0.0.1
```

This example shows the minimum required crypto map configuration when the security associations are manually established:

```
fwsM/context_name(config)# crypto transform-set someset ah-md5-hmac esp-des
fwsM/context_name(config)# crypto map mymap 10 ipsec-manual
fwsM/context_name(config)# crypto map mymap 10 match address 102
fwsM/context_name(config)# crypto map mymap 10 set transform-set someset
fwsM/context_name(config)# crypto map mymap 10 set peer 10.0.0.5
fwsM/context_name(config)# crypto map mymap 10 set session-key inbound ah 256
98765432109876549876543210987654
fwsM/context_name(config)# crypto map mymap 10 set session-key outbound ah 256
fedcbafedcbafedcfedcbafedcbafedc
fwsM/context_name(config)# crypto map mymap 10 set session-key inbound esp 256 cipher
0123456789012345
fwsM/context_name(config)# crypto map mymap 10 set session-key outbound esp 256 cipher
abcdefabcdefabcd
```

This example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows security associations to be established between the FWSM and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” that can be used to process inbound security association negotiation requests that do not match “mymap” entries 10 or 20. If the peer specifies a transform set that matches one of the transform sets that are specified in “mydynamicmap” for a flow “permitted” by the access list 103, IPSec accepts the request and sets up

security associations with the peer without previously knowing about the peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the peer.

The access list that is associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match a permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists that are associated with static crypto maps entries.) Outbound packets that match a permit entry without an existing corresponding IPSec security association are also dropped.

This example shows the configuration using “mydynamicmap”:

```
fwsM/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsM/context_name(config)# crypto map mymap 10 match address 101
fwsM/context_name(config)# crypto map mymap 10 set transform-set my_t_set1
fwsM/context_name(config)# crypto map mymap 10 set peer 10.0.0.1
fwsM/context_name(config)# crypto map mymap 10 set peer 10.0.0.2
fwsM/context_name(config)# crypto map mymap 20 ipsec-isakmp
fwsM/context_name(config)# crypto map mymap 10 match address 102
fwsM/context_name(config)# crypto map mymap 10 set transform-set my_t_set1 my_t_set2
fwsM/context_name(config)# crypto map mymap 10 set peer 10.0.0.3
fwsM/context_name(config)# crypto dynamic-map mydynamicmap 10
fwsM/context_name(config)# crypto dynamic-map mydynamicmap 10 match address 103
fwsM/context_name(config)# crypto dynamic-map mydynamicmap 10 set transform-set my_t_set1
my_t_set2 my_t_set3
fwsM/context_name(config)# crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
```

Related Commands

- crypto map client
- crypto map interface
- crypto map ipsec
- crypto map set peer
- crypto map set security-association lifetime
- crypto map set session-key
- crypto map set transform-set
- crypto map set peer
- show crypto map

crypto map set peer

To specify an IPsec peer in a crypto map entry, use the **crypto map set peer** command. To remove an IPsec peer from a crypto map entry, use the **no** form of this command.

```
[no] crypto map map-name seq-num set peer {hostname | ip-address}
```

Syntax Description

<i>map-name</i>	Name of the crypto map set.
<i>seq-num</i>	Number used to rank multiple crypto map entries within a crypto map set.
<i>hostname</i>	Name of the host.
<i>ip-address</i>	IP address of the host.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is required for all the static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required and in most cases is not used because the peer is unknown.

For ipsec-isakmp crypto map entries, you can specify multiple peers by repeating this command. The peer that packets are actually sent to is determined by the last peer that sent either traffic or a negotiation request for a given data flow to the FWSM. If the attempt fails with the first peer, Internet Key Exchange (IKE) tries the next peer on the crypto map list.

For ipsec-manual crypto entries, you can specify only one peer per crypto map. If you want to change the peer, you must delete the old peer and then specify the new peer.

Examples

This example shows a crypto map configuration when IKE is used to establish the security associations. In this example, a security association could be set up to either the peer at 10.0.0.1 or the peer at 10.0.0.2.

```
fwsM/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsM/context_name(config)# crypto map mymap 10 match address 101
fwsM/context_name(config)# crypto map mymap 10 set transform-set my_t_set1
fwsM/context_name(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map set pfs

To set the IPsec to ask for perfect forward secrecy (PFS) when requesting new security associations or to require PFS when receiving requests for new security associations, use the **crypto map set pfs** command. To specify that IPsec should not request PFS, use the **no** form of this command.

```
[no] crypto map map-name seq-num set pfs [group1 | group2]
```

Syntax Description	
<i>map-name</i>	Name of the crypto map set.
<i>seq-num</i>	Number used to rank multiple crypto map entries within a crypto map set.
set pfs	Specifies PFS.
group1	(Optional) Specifies a Diffie-Hellman prime modulus group.
group2	(Optional) Specifies a Diffie-Hellman prime modulus group.

Defaults

The defaults are as follows:

- PFS is not requested.
- **group1**.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is available only for ipsec-isakmp crypto map entries and dynamic crypto map entries.

With PFS, every time that a new security association is negotiated, a new Diffie-Hellman exchange occurs, which requires additional processing time. PFS adds another level of security. If one key is ever deciphered by an attacker, only the data that is sent with that key is compromised.

During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. The default (group1) is sent if the **set pfs** command does not specify a group.

If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, a default of group1 is assumed, and an offer of either group1 or group2 is accepted. If the local configuration specifies group2, that group must be part of the peer's offer or the negotiation fails. If the local configuration does not specify PFS, it accepts any offer of PFS from the peer.

The 1024-bit Diffie-Hellman prime modulus group, group2, provides more security than group1 but requires more processing time than group1.

**Note**

Internet Key Exchange (IKE) negotiations with a remote peer may hang when a FWSM has numerous tunnels that originate from the FWSM and terminate on a single remote peer. This problem occurs when PFS is not enabled, and the local peer requests many simultaneous rekey requests. If this problem occurs, the IKE security association will not recover until it has timed out or until you manually clear it with the **clear [crypto] isakmp sa** command. The FWSM units that are configured with many tunnels to many peers or many clients sharing the same tunnel are not affected by this problem. If the configuration is affected, enable PFS with the **crypto map *mapname seqnum* set pfs** command.

Examples

This example specifies that PFS should be used whenever a new security association is negotiated for the crypto map “mymap 10”:

```
fwsM/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsM/context_name(config)# crypto map mymap 10 set pfs group2
```

Related Commands

- crypto map client**
- crypto map interface**
- crypto map ipsec**
- crypto map set peer**
- crypto map set security-association lifetime**
- crypto map set session-key**
- crypto map set transform-set**
- crypto map set peer**
- show crypto map**

crypto map set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value that is used when negotiating IPSec security associations, use the **crypto map set security-association lifetime** command. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

```
[no] crypto map map-name seq-num set security-association lifetime {seconds seconds |
kilobytes kilobytes}
```

Syntax Description

<i>map-name</i>	Name of the crypto map set.
<i>seq-num</i>	Number used to rank multiple crypto map entries within a crypto map set.
seconds <i>seconds</i>	Sets the keys and security association to time out after the specified number of seconds have passed.
kilobytes <i>kilobytes</i>	Sets the keys and security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security association's key.

Defaults

The defaults are as follows:

- **seconds** *seconds* is 28,800 seconds (8 hours).
- **kilobytes** *kilobytes* is 4,608,000 KB (10 MBPS for one hour).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

This command is available only for ipsec-isakmp crypto map entries and dynamic crypto map entries.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the FWSM requests new security associations during security association negotiation, it specifies its crypto map lifetime value in the request to the peer; it uses this value as the lifetime of the new security associations. When the FWSM receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The session keys/security association expires after either of these lifetimes is reached.

If you change a lifetime, the change is not applied to existing security associations but is used in subsequent negotiations to establish security associations for data flows that are supported by this crypto map entry. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto ipsec sa** command.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key. Shorter lifetimes require more CPU processing time.

The lifetime values are ignored for manually established security associations (security associations installed through an ipsec-manual crypto map entry).

Examples

This example shortens the timed lifetime for a particular crypto map entry because there is a higher risk that the keys could be compromised for security associations belonging to the crypto map entry. The traffic-volume lifetime is not changed because there is not a high volume of traffic anticipated for these security associations. The timed lifetime is shortened to 2700 seconds (45 minutes).

```
fwsM/context_name(config)# crypto map mymap 10 ipsec-isakmp  
fwsM/context_name(config)# crypto security-association lifetime seconds 2700
```

Related Commands

- crypto map client**
- crypto map interface**
- crypto map ipsec**
- crypto map set peer**
- crypto map set pfs**
- crypto map set session-key**
- crypto map set transform-set**
- crypto map set peer**
- show crypto map**

crypto map set session-key

To manually specify the IPsec session keys within a crypto map entry, use the **crypto map set session-key** command. To remove IPsec session keys from a crypto map entry, use the **no** form of this command.

```
[no] crypto map map-name seq-num set session-key {inbound | outbound} ah spi hex-key-string
```

```
crypto map map-name seq-num set session-key {inbound | outbound} esp spi cipher
hex-key-string [authenticator hex-key-string]
```

Syntax Description	
<i>map-name</i>	Name of the crypto map set.
<i>seq-num</i>	Number used to rank multiple crypto map entries within a crypto map set.
inbound	Specifies inbound traffic.
outbound	Specifies outbound traffic.
ah	Specifies the Authorization Header (AH) protocol.
<i>spi</i>	Security Parameter Index (SPI) number.
<i>hex-key-string</i>	Hexadecimal key string that is associated with the SPI number.
esp	Specifies the Encapsulation Security Payload (ESP) encryption protocol.
cipher	Specifies cipher encoding.
authenticator	(Optional) Specifies ESP authentication.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is available only for ipsec-manual crypto map entries.

If the crypto map's transform set includes an AH protocol, you must define IPsec keys for AH for both inbound and outbound traffic. If the crypto map's transform set includes an ESP encryption protocol, you must define IPsec keys for ESP encryption for both inbound and outbound traffic. If the crypto map's transform set includes an ESP authentication protocol, you must define IPsec keys for ESP authentication for inbound and outbound traffic.

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set pfs
crypto map set security-association lifetime
crypto map set transform-set
crypto map set peer
show crypto map

crypto map set transform-set

To specify a list of transform sets in priority order, use the **crypto map set transform-set** command. To remove all the transform sets from a crypto map entry, use the **no** form of this command.

```
[no] crypto map set transform-set proposal [proposal ...]
```

Syntax Description		
	<i>proposal</i>	Proposal tag.
	<i>proposal...</i>	(Optional) Proposal tag.

Defaults This command has no default settings.

Command Modes Security Context Mode: single context mode and multiple context mode
 Access Location: system and context command line
 Command Mode: configuration mode
 Firewall Mode: routed firewall mode and transparent firewall mode

Command History	Release	Modification
	1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines This command is required for all the static and dynamic crypto map entries.

For an **ipsec-isakmp crypto map** entry, you can list up to six transform sets with this command. List the higher priority transform sets first.

If the local FWSM initiates the negotiation, the transform sets are presented to the peer in the order that is specified in the **crypto map** command. If the peer initiates the negotiation, the local FWSM accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec does not establish a security association and the traffic is dropped.

For an **ipsec-manual crypto map** command, you can specify only one transform set. If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

To change the list of transform sets, respecify the new list of transform sets to replace the old list. This change is applied only to **crypto map** commands that reference this transform set. The change is not applied to existing security associations but is used in subsequent negotiations to establish new security associations. To make the new settings take effect sooner, you can clear all or part of the security association database by using the **clear crypto ipsec sa** command.

Any transform sets that are included in the **crypto map** command must previously have been defined using the **crypto ipsec transform-set** command.

Examples

This example shows how to display the transform sets:

```
fwsM/context_name(config)# crypto map transform-set
```

Related Commands

- crypto map client**
- crypto map interface**
- crypto map ipsec**
- crypto map set peer**
- crypto map set pfs**
- crypto map set security-association lifetime**
- crypto map set session-key**
- crypto map set peer**
- show crypto map**

crypto match address

To specify the match address of packets to encrypt, use the **crypto match address** command. To remove the access list from a crypto map entry, use the **no** form of this command.

[no] crypto match address *access_list_name*

Syntax Description

<i>access_list_name</i>	Name of the access list.
-------------------------	--------------------------

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is required for all the static crypto map entries. If you are defining a dynamic crypto map entry (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use the **access-list extended** command to define this access list.

The access list that is specified with this command is used by IPSec to determine which traffic should be protected by IPSec crypto and which traffic does not need protection. Traffic that is permitted by the access list is protected. Traffic that is denied by the access list is not protected.



Note

The crypto access list is not used to determine whether to permit or deny traffic through the interface. An access list that is applied directly to the interface with the **access-group** command makes that determination.

The crypto access list that is specified by this command is used when evaluating both inbound and outbound traffic. Outbound traffic is evaluated against the crypto access lists that are specified by the interface's crypto map entries to determine if it should be protected by crypto, and if so, which crypto policy applies. For IPSec crypto maps, new security associations are established using the data flow identity that is specified in the permit entry. For dynamic crypto map entries, if no security association exists, the packet is dropped. Inbound traffic is evaluated against the crypto access lists that are specified by the entries of the interface's crypto map set to determine if it should be protected by crypto and, if so, which crypto policy applies. (For IPSec, unprotected traffic is discarded because it should have been protected by IPSec.)

The access list is used to identify the flow for which the IPSec security associations are established. For outbound traffic, the permit entry is used as the data flow identity. For inbound traffic, the data flow identity that is specified by the peer must be “permitted” by the crypto access list.

Examples

This example shows how to specify the match address of packets to encrypt:

```
fwsM/context_name (config) # crypto match address 101
```

Related Commands

- crypto map client**
- crypto map interface**
- crypto map ipsec**
- crypto map set peer**
- crypto map set pfs**
- crypto map set security-association lifetime**
- crypto map set session-key**
- crypto map set transform-set**
- show crypto map**