

# FWSM: Multiple Context Configuration Example

Document ID: 107524

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Background Information

- Context Configuration Files
- Unsupported Features
- Management Access to Security Contexts

### Configure

- Network Diagram
- Enabling or Disabling Multiple Context Mode
- Configure a Security Context
- FWSM: System Execution Space Configuration
- Change Between Contexts and the System Execution Space
- FWSM – ContextA Configuration
- FWSM – ContextB Configuration
- Save Configuration Changes in Multiple Context Mode

### Verify

### Troubleshoot

- Restore Single Context Mode
- Reload a Security Context
- Rename the Context
- Delete Context

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

This document describes the steps used to configure multiple context in Firewall Service Module (FWSM).

You can partition a single FWSM into multiple virtual devices, known as security contexts. Each context has its own security policy, interfaces, and administrators. Multiple contexts are similar to multiple standalone devices. Many features are supported in multiple context mode, which includes routing tables, firewall features, and management. Some features are not supported, which includes dynamic routing protocols.

You can use multiple security contexts in these situations:

- You are a service provider and want to sell security services to many customers. When you enable multiple security contexts on the FWSM, you can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.
- You are a large enterprise or a college campus and want to keep departments completely separate.
- You are an enterprise that wants to provide distinct security policies to different departments.
- You have any network that requires more than one firewall.

Refer to PIX/ASA 7.x and Above: Multiple Context Configuration Example for more information on how to describe the steps used to configure multiple context in security appliances.

# Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on the Firewall Service Module (FWSM) that runs software version 3.2(5).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

# Background Information

## Context Configuration Files

### Context Configurations

The FWSM includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. You can store context configurations on the internal Flash memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

### System Configuration

The system administrator adds and manages contexts with the configuration of each context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the FWSM. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources, such as downloading the contexts from the server, it uses one of the contexts that is designated as the admin context. The system configuration does include a specialized failover interface for failover traffic only.

### Admin Context Configuration

The admin context is just like any other context, except that when you log in to the admin context, then you have system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. But, because logging into the admin context grants you administrator privileges over all contexts, you can possibly need to restrict access to the admin context to appropriate users. The admin context must reside on Flash memory, and not remotely.

If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal Flash memory called `admin.cfg`. This context is named `admin`. If you do not want to use `admin.cfg` as the admin context, you can change the admin context.

## Unsupported Features

Multiple context mode does not support these features:

- Dynamic routing protocols
- Security contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode.
- Multicast

## Management Access to Security Contexts

The FWSM provides system administrator access in multiple context mode as well as access for individual context administrators. These sections describe logging in as a system administrator or as a context administrator:

### System Administrator Access

You can access the FWSM as a system administrator in two ways:

- Session to the FWSM from the switch.
- From the switch, you access the system execution space.
- Access the admin context using Telnet, SSH, or ASDM.

Refer to Configuring Management Access for more information on how to enable Telnet, SSH, and SDM access.

As the system administrator, you can access all contexts.

When you change to a context from admin or the system, your username changes to the default `enable_15` username. If you configured command authorization in that context, you need to either configure authorization privileges for the `enable_15` user, or you can log in as a different name for which you provide sufficient privileges in the command authorization configuration for the context. Enter the **login** command in order to log in with a username. For example, you log in to the admin context with the username `admin`. The admin context does not have any command authorization configuration, but all other contexts include command authorization. For convenience, each context configuration includes a user `admin` with maximum privileges. When you change from the admin context to context A, your username is altered, so you must log in again as `admin` when you enter the **login** command. When you change to context B, you must again enter the **login** command to log in as `admin`.

The system execution space does not support any AAA commands, but you can configure its own enable password, as well as usernames in the local database, in order to provide individual logins.

### Context Administrator Access

You can access a context with Telnet, SSH, or ASDM. If you log in to a non-admin context, you can only access the configuration for that context. You can provide individual logins to the context.

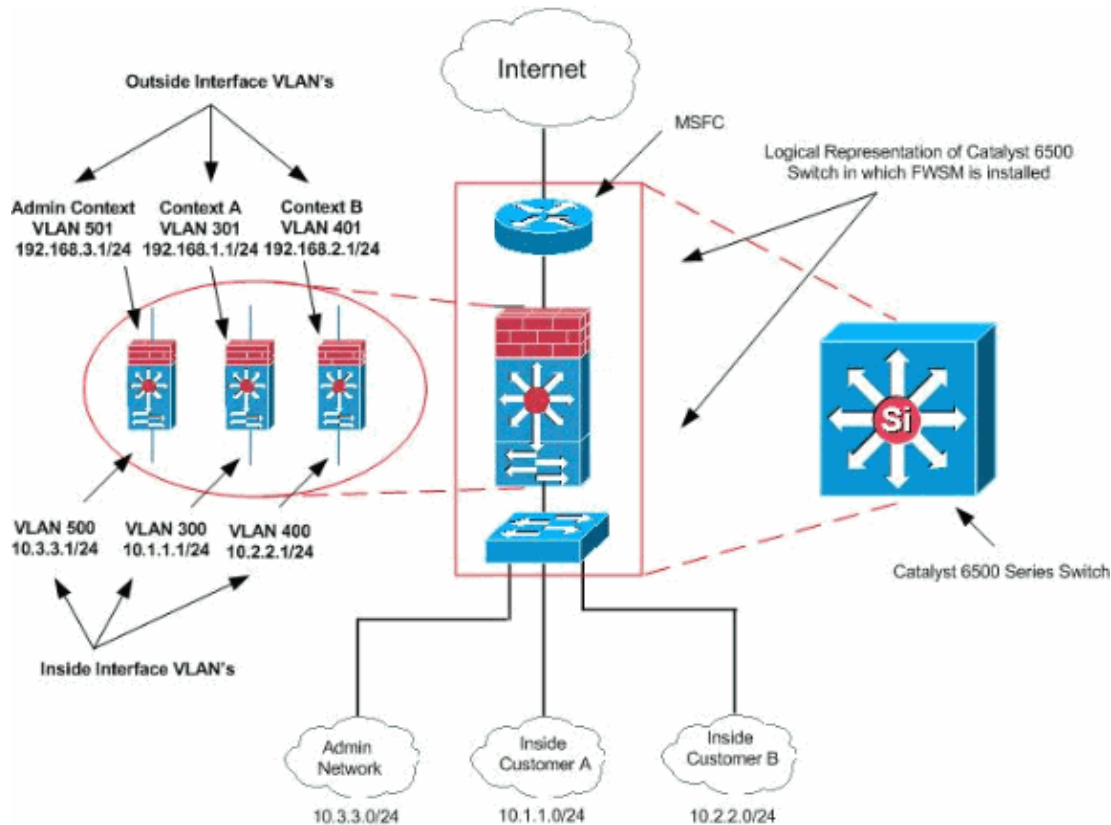
## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:



## Enabling or Disabling Multiple Context Mode

Your FWSM might already be configured for multiple security contexts depending on how you ordered it from Cisco. If you are upgrading, however, you might need to convert from single mode to multiple mode by following the procedures in this section. ASDM does not support changing modes, so you need to change modes using the CLI.

### Backing Up the Single Mode Configuration

When you convert from single mode to multiple mode, the FWSM converts the running configuration into two files. The original startup configuration is not saved, so if it differs from the running configuration, you should back it up before proceeding.

### Enabling Multiple Context Mode

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match with the **mode** command.

When you convert from single mode to multiple mode, the FWSM converts the running configuration into two files:.

1. A new startup configuration that comprises the system configuration
2. An admin.cfg that comprises of the admin context in the root directory of the internal Flash memory

The original running configuration is saved as old\_running.cfg (in the root directory of the internal Flash memory). The original startup configuration is not saved. The FWSM automatically adds an entry for the admin context to the system configuration with the name "admin."

Enter this command in order to enable multiple mode:

```
hostname(config)#mode multiple
```

You are prompted to reboot the FWSM.

```
FWSM(config)#mode multiple
```

```
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
```

```
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

```
Rebooting....
```

```
Booting system, please wait...
*
*
```

```
!--- Output suppressed
```

```
*
*
INFO: Admin context is required to get the interfaces
*** Output from config line 20, "arp timeout 14400"
Creating context 'admin'... Done. (1)
*** Output from config line 23, "admin-context admin"

Cryptochecksum (changed): a219baf3 037b31b4 09289829 1ab9790a

*** Output from config line 25, " config-url flash:/admi..."

Cryptochecksum (changed): d4f0451b 405720e1 bbccf404 86be061c
Type help or '?' for a list of available commands.
FWSM>
```

After reboot, this is the default configuration of the FWSM:

FWSM Default Configuration
----------------------------

```

FWSM#show running-config
: Saved
:
FWSM Version 3.2(5)5 <system>
!
resource acl-partition 12
hostname FWSM
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
!
interface Vlan501
!
interface Vlan502
!
passwd 2KFQnbNIdI.2KYOU encrypted
class default
  limit-resource IPsec 5
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource All 0
!

ftp mode passive
gdb enable
pager lines 24
no failover
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  allocate-interface Vlan501
  allocate-interface Vlan502
  config-url disk:/admin.cfg

!--- admin context is created
!--- by default once you enable
!--- multiple mode

!

prompt hostname context
Cryptochecksum:d62411d2a15f1da35c76fe071b61dcdb
: end
FWSM#

```

## Configure a Security Context

The security context definition in the system configuration identifies the context name, configuration file URL, interfaces that a context can use, and other context parameters.

**Note:** If you do not have an admin context, for example, if you clear the configuration, you must first specify the admin context name when you enter this command:.

```
hostname(config)#admin-context <name>
```

**Note:** Although this context name does not exist yet in your configuration, you can subsequently enter the **context name** command in order to match the specified name to continue the admin context configuration.

In order to add or change a context in the system configuration, complete these steps:

1. In order to add or modify a context, enter this command in the **system execution space**:

```
hostname(config)#context <name>
```

The name is 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.

"System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.

2. (Optional) In order to add a description for this context, enter this command:

```
hostname(config-ctx)#description text
```

3. In order to specify the interfaces you can use in the context, enter this command:

```
hostname(config-ctx)#allocate-interface vlannumber[-vlannumber] [map_name[-map_name]
[invisible | visible]]
```

You can enter this command multiple times in order to specify different ranges. If you remove an allocation with the **no** form of this command, then any context commands that include this interface are removed from the running configuration.

Enter a VLAN number or a range of VLANs, typically from 2 to 1000 and from 1025 to 4094. See the switch documentation for supported VLANs. Use the **show vlan** command in order to see a list of VLANs assigned to the FWSM. You can allocate a VLAN that is not yet assigned to the FWSM, but you need to assign them from the switch if you want them to pass traffic. When you allocate an interface, the FWSM automatically adds the **interface** command for each VLAN in the system configuration.

4. Enter this command in order to identify the URL from which the system downloads the context configuration:

```
hostname(config-ctx)#config-url url
```

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** 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 can possibly include commands that refer to interfaces, for example, interface, nat, global and so forth. 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.

In this scenario, complete the steps in the table in order to configure the multiple context.

There are two customers, Customer A and Customer B. Create three multiple contexts (virtually three FWSMs) in a single FWSM module such as Context A for Customer A, Context B for Customer B, and Admin Context to administrate the FWSM contexts.

**Note:** Create VLANs 300, 301, 400, 401, 500 and 501 in the Catalyst 6500 Series Switch before you use it in the FWSM.

Create the contexts in the system execution space and allocate the respective VLAN's to the each created context and configure the URL path for every context as shown.

```
FWSM Multiple Context Configuration Steps

FWSM(config)#context admin
FWSM(config-ctx)#allocate-interface VLAN500
FWSM(config-ctx)#allocate-interface VLAN501
FWSM(config-ctx)#config-url disk:/admin.cfg

!--- Allocate VLAN 500 and 501 to admin context

FWSM(config)#context contextA

!--- Customer A Context as Context A

FWSM(config-ctx)#allocate-interface VLAN300
FWSM(config-ctx)#allocate-interface VLAN301

!--- Allocate VLAN 300 and 301 to admin context

FWSM(config-ctx)#config-url disk:/contextA.cfg
WARNING: Could not fetch the URL disk:/contextA.cfg
INFO: Creating context with default config

!--- To identify the URL from which the
!--- system downloads the context configuration.

FWSM(config-ctx)#context contextB
Creating context 'contextB'... Done. (3)

!--- Customer B Context as Context B

FWSM(config-ctx)#allocate-interface VLAN400
FWSM(config-ctx)#allocate-interface VLAN401

!--- Allocate VLAN 400 and 401 to admin context

FWSM(config-ctx)#config-url disk:/contextB.cfg
WARNING: Could not fetch the URL disk:/contextB.cfg
INFO: Creating context with default config
FWSM(config-ctx)#exit
```

## FWSM: System Execution Space Configuration

```
FWSM – System Execution Space Configuration

FWSM(config)#show running-config
: Saved
:
FWSM Version 3.2(5)5 <system>
!
```

```

resource acl-partition 12
hostname FWSM
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
!
interface Vlan300
!
interface Vlan301
!
interface Vlan400
!
interface Vlan401
!
interface Vlan501
!
interface Vlan502
!
passwd 2KFQnbNIdI.2KYOU encrypted
class default
  limit-resource IPsec 5
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource All 0
!

ftp mode passive
gdb enable
pager lines 24
no failover
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  allocate-interface Vlan501
  allocate-interface Vlan502
  config-url disk:/admin.cfg
!

context contextA
  allocate-interface Vlan300
  allocate-interface Vlan301
  config-url disk:/contextA.cfg
!

context contextB
  allocate-interface Vlan400
  allocate-interface Vlan401
  config-url disk:/contextB.cfg
!

prompt hostname context
Cryptochecksum:d62411d2a15f1da35c76fe071b61dcdb
: end
FWSM#

```

## Change Between Contexts and the System Execution Space

If you log in to the system execution space (or the admin context using Telnet or SSH), you can change between contexts and perform configuration and monitoring tasks within each context. The running configuration that you edit in a configuration mode, or that is affected by the **copy** or **write** commands,

depends on your location. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) if you enter the **show running-config** command. Only the current configuration displays. You can, however, save all context running configurations from the system execution space if you use the **write memory all** command.

In order to change between the system execution space and a context, or between contexts, see these commands:

- In order to change to a context, enter this command:

```
hostname#changeto context <context name>
```

The prompt changes to this:

```
hostname/name#
```

- In order to change to the system execution space, enter this command

```
hostname/admin#changeto system
```

The prompt changes to this:

```
hostname#
```

## FWSM – ContextA Configuration

In order to configure the contextA, change to the contextA and follow the procedure:

```
!--- From the system execution space,  
!--- enter the changeto context contextA command  
!--- in order to configure the contextA configuration.
```

```
FWSM(config)#changeto context contextA
```

```
FWSM/context1(config)#
```

### FWSM – ContextA Default Configuration

```
FWSM/contextA(config)#show running-config  
  
!--- Default configuration of the context1  
  
: Saved  
:  
FWSM Version 3.2(5)5 <context>  
!  
hostname contextA  
enable password 8Ry2YjIyt7RRXU24 encrypted  
names  
!  
interface Vlan300  
  no nameif  
  no security-level  
  no ip address  
!  
interface Vlan301  
  no nameif
```

```
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
gdb enable
pager lines 24
mtu inside 1500
mtu outside 1500
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 1:00:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect skinny
    inspect smtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
FWSM/contextA#
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
gdb enable
pager lines 24
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 1:00:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
```

```

match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect skinny
inspect smtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:000000000000000000000000000000000000
: end

```

Customer A Configuration for Internet connectivity.

#### FWSM – Configuration of ContextA

```

FWSM/contextA(config)#interface vlan300
FWSM/contextA(config-if)#nameif inside
WARNING: VLAN *300* is not configured.
INFO: Security level for "inside" set to 100 by default.
Access Rules Download Complete: Memory Utilization: 1%
FWSM/contextA(config-if)#ip address 10.1.1.1 255.255.255.0
FWSM/contextA(config-if)#no shut

FWSM/contextA(config-if)#interface vlan 301
FWSM/contextA(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
Access Rules Download Complete: Memory Utilization: 1%
FWSM/contextA(config-if)#ip add 192.168.1.1 255.255.255.0
FWSM/contextA(config-if)#no shut

FWSM/contextA(config)#access-list outbound permit ip any any
FWSM/contextA(config)#nat (inside) 1 access-list outbound
FWSM/contextA(config)#global (outside) 1 interface
INFO: outside interface address added to PAT pool
FWSM/contextA(config)#route outside-context1 0.0.0.0 0.0.0.0 192.168.1.5
FWSM/contextA(config)#exit

```

#### FWSM – ContextA Configuration

```

FWSM/contextA#show running-config
: Saved
:
FWSM Version 3.2(5)5 <context>
!
hostname contextA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan300
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0

```

```

!
interface Vlan301
  nameif outside
  security-level 0
  ip address 192.168.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outbound extended permit ip any any
gdb enable
pager lines 24
mtu inside 1500
mtu outside 1500
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 access-list outbound
route outside 0.0.0.0 0.0.0.0 192.168.1.5 1

!--- Output Suppressed

!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect skinny
    inspect smtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
FWSM/contextA#

```

## FWSM – ContextB Configuration

Customer B Configuration for Internet connectivity.

In order to configure the contextB, change to contextB from contextA:

```

!--- From the system execution space, enter
!--- the changeto context contextB command
--- in orderto configure the contextB configuration.

```

```

FWSM/contextA(config)#changeto context contextB
FWSM/contextB(config)#

```

```

FWSM/contextB(config)#show running-config
: Saved
:
FWSM Version 3.2(5)5 <context>
!
hostname contextB
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan400
  nameif inside
  security-level 100
  ip address 10.2.2.1 255.255.255.0
!
interface Vlan401
  nameif outside
  security-level 0
  ip address 192.168.2.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outbound extended permit ip any any
gdb enable
pager lines 24
mtu inside 1500
mtu outside 1500
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 access-list outbound
route outside 0.0.0.0 0.0.0.0 192.168.2.5 1

!--- Output Suppressed

!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect skinny
    inspect smtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
FWSM/contextB(config)#

```

Similarly configure the admin context to administrate the FWSM and its contexts from the inside and outside interface.

## Save Configuration Changes in Multiple Context Mode

You can save each context (and system) configuration separately, or you can save all context configurations at the same time. This section includes these topics:

### Save Each Context and System Separately

In order to save the system or context configuration, enter this command within the system or context:

```
hostname#write memory
```

**Note:** The copy running-config startup-config command is equivalent to the **write memory** command.

For multiple context mode, context startup configurations can reside on external servers. In this case, the security appliance saves the configuration back to the server that you identified in the context URL, except for an HTTP or HTTPS URL, which does not let you save the configuration to the server.

### Save All Context Configurations at the Same Time

In order to save all context configurations at the same time, as well as the system configuration, enter this command in the system execution space:

```
hostname#write memory all [/noconfirm]
```

If you do not enter the /noconfirm keyword, you see this prompt:

```
Are you sure [Y/N]:
```

## Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show context** Displays the various contexts.

```
FWSM(config)#show context
Context Name      Class      Interfaces      Mode      URL
*admin            default    Vlan501,Vlan502 Routed    disk:/admin.cfg
contextA          default    Vlan300,Vlan301 Routed    disk:/contextA.cfg
contextB          default    Vlan400,Vlan401 Routed    disk:/contextB.cfg
```

```
Total active Security Contexts: 3
```

- **show mode** Verify that the FWSM is configured as a single or multiple mode.

```
FWSM(config)#show mode
Security context mode: multiple
The flash mode is the SAME as the running mode.
```

## Troubleshoot

## Restore Single Context Mode

If you convert from multiple mode to single mode, it is possible to first copy a full startup configuration (if available) to the FWSM; the system configuration inherited from multiple mode is not a completely functional configuration for a single mode device. Because the system configuration does not have any network interfaces as part of its configuration, you must access the security appliance from the console to perform the copy.

In order to copy the old running configuration to the startup configuration and to change the mode to single mode complete these steps in the system execution space:

1. In order to copy the backup version of your original running configuration to the current startup configuration, enter this command in the system execution space:

```
hostname(config)#copy flash:old_running.cfg startup-config
```

2. In order to set the mode to single mode, enter this command in the system execution space:

```
hostname(config)#mode single
```

FWSM reboots.

## Reload a Security Context

You can reload the context in two ways:

1. Clear the running configuration and then import the startup configuration.

This action clears most attributes associated with the context, such as connections and NAT tables.

2. Remove the context from the system configuration.

This action clears additional attributes, such as memory allocation, which can be useful for troubleshooting. But, in order to add the context back to the system requires you to respecify the URL and interfaces.

This section includes these topics:

- Reloading by Clearing the Configuration
- Reloading by Removing and Readding the Context

## Rename the Context

In multiple context mode, to rename a context without changing the configuration is not supported.

You can save the configuration as a firewall configuration, but you need to copy the entire configuration to a new context name and delete the old context configuration.

## Delete Context

Use this command in order to delete the Context. From the system space issue, issue this command:

```
no context contA
```

Also make sure to remove the corresponding config file for the context.

```
dir disk:
```

```
delete disk:/contA.cfg
```

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

---

## Related Information

- [FWSM Basic Configuration Example](#)
- [PIX/ASA 7.x and Above: Multiple Context Configuration Example](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jul 04, 2008

Document ID: 107524

---