Sample Configurations

This chapter illustrates and describes a number of common ways to implement the Firewall Services Module (FWSM). It includes the following topics:

Routed Mode Examples

This section includes the following topics:

Example 1: Security Contexts With Outside Access

This configuration creates three security contexts plus the admin context, each with an inside and an outside interface. The Customer C context includes a DMZ interface where a Websense server for HTTP filtering resides on the service provider premises (see Figure B-1).

Inside hosts can access the Internet through the outside using dynamic NAT or PAT, but no outside hosts can access the inside.

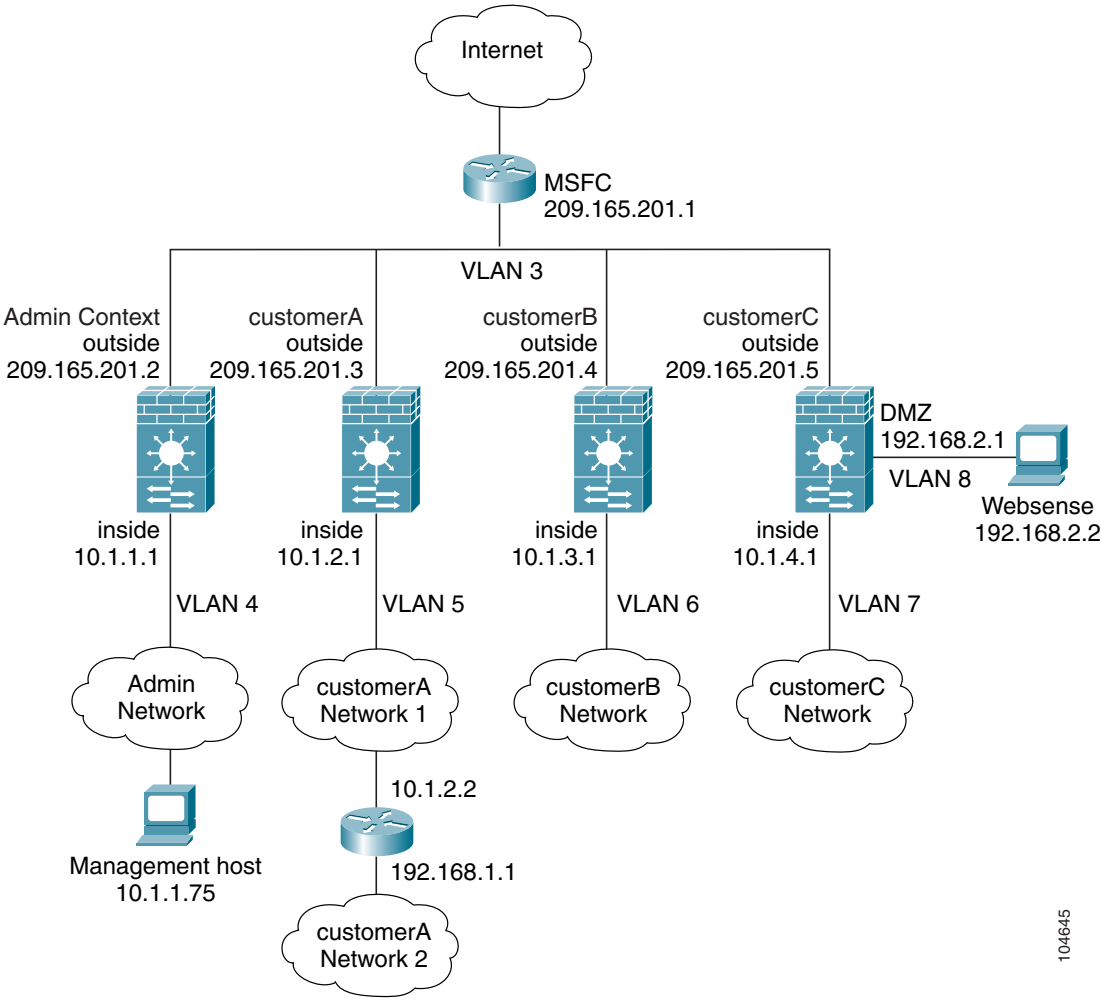
The Customer A context has a second network behind an inside router.

The admin context allows SSH sessions to the FWSM from one host.

Each customer context belongs to a class that limits its resources (gold, silver, or bronze).

Although inside IP addresses can be the same across contexts when the VLANs are unique, keeping them unique is easier to manage.

Figure B-1 Example 1



See the following sections for the configurations for this scenario:

- Example 1: System Configuration, page B-2
- Example 1: Admin Context Configuration, page B-3
- Example 1: Customer A Context Configuration, page B-4
- Example 1: Customer B Context Configuration, page B-4
- Example 1: Customer C Context Configuration, page B-4
- Example 1: Switch Configuration, page B-5

Example 1: System Configuration

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts using the **activation-key** command. The mode and the activation key are not stored in the configuration file, even though they do endure reboots. If you view the configuration on the FWSM using the **write terminal**, **show startup**, or **show running** commands, the mode displays after the FWSM Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
hostname Farscape
password passw0rd
enable password chr1cht0n
admin-context admin
context admin
    allocate-interface vlan3
    allocate-interface vlan4
    config-url disk://admin.cfg
    class default
context customerA
    description This is the context for customer A
    allocate-interface vlan3
    allocate-interface vlan5
    config-url disk://contexta.cfg
    class gold
context customerB
    description This is the context for customer B
    allocate-interface vlan3
    allocate-interface vlan6
    config-url disk://contextb.cfg
    class silver
context customerC
    description This is the context for customer C
    allocate-interface vlan3
    allocate-interface vlan7-vlan8
    config-url disk://contextc.cfg
    class bronze
class gold
    limit-resource all 7%
    limit-resource rate conns 2000
    limit-resource conns 20000
class silver
    limit-resource all 5%
    limit-resource rate conns 1000
    limit-resource conns 10000
class bronze
    limit-resource all 3%
    limit-resource rate conns 500
    limit-resource conns 5000
```

Example 1: Admin Context Configuration

The host at 10.1.1.75 can access the context using SSH, which requires a certificate to be generated using the **ca generate rsa key** *modulus* command and saved using the **ca save all** command. The certificate is saved in Flash memory.

```
hostname Admin
domain isp
nameif vlan3 outside security0
nameif vlan4 inside security100
passwd secret1969
enable password h1andl0
ip address outside 209.165.201.2 255.255.255.224
ip address inside 10.1.1.1 255.255.255.0
route outside 0 0 209.165.201.1 1
ssh 10.1.1.75 255.255.255.255 inside
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 209.165.201.10-209.165.201.29 [This context uses dynamic NAT for inside
users that access the outside]
```

```
static (inside,outside) 209.165.201.30 10.1.1.75 netmask 255.255.255.255 [The host at
10.1.1.75 has access to the Websense server in Customer C, so it needs a static
translation for use in Customer C's ACL]
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
```

Example 1: Customer A Context Configuration

```
nameif vlan3 outside security0
nameif vlan5 inside security100
passwd hell0!
enable password enter55
ip address outside 209.165.201.3 255.255.255.224
ip address inside 10.1.2.1 255.255.255.0
route outside 0 0 209.165.201.1 1
route inside 192.168.1.0 255.255.255.0 10.1.2.2 1 [The Customer A context has a second
network behind an inside router that requires a static route. All other traffic is handled
by the default route pointing to the MSFC.]
nat (inside) 1 10.1.2.0 255.255.255.0
global (outside) 1 interface [This context uses dynamic PAT for inside users that access
that outside. The outside interface address is used for the PAT address]
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
```

Example 1: Customer B Context Configuration

```
nameif vlan3 outside security0
nameif vlan6 inside security100
passwd tenac10us
enable password defen$e
ip address outside 209.165.201.4 255.255.255.224
ip address inside 10.1.3.1 255.255.255.0
route outside 0 0 209.165.201.1 1
nat (inside) 1 10.1.3.0 255.255.255.0
global (outside) 1 209.165.201.9 netmask 255.255.255.255 [This context uses dynamic PAT
for inside users that access the outside]
access-list INTERNET extended permit tcp any any eq http
access-list INTERNET extended permit tcp any any eq https
access-group INTERNET in interface inside [Inside users can only access HTTP and HTTPS
servers on the outside]
```

Example 1: Customer C Context Configuration

```
nameif vlan3 outside security0
nameif vlan7 inside security100
nameif vlan8 dmz security50
passwd fl0wer
enable password treeh0u$e
ip address outside 209.165.201.5 255.255.255.224
ip address inside 10.1.4.1 255.255.255.0
ip address dmz 192.168.2.1 255.255.255.0
route outside 0 0 209.165.201.1 1
url-server (dmz) vendor websense host 192.168.2.2 url-block block 50
url-cache dst 128
```

```
filter url http 10.1.4.0 255.255.255.0 0 0 [When inside users access an HTTP server, the
FWSM consults with a Websense server to determine if the traffic is allowed]
nat (inside) 1 10.1.4.0 255.255.255.0
global (outside) 1 209.165.201.9 netmask 255.255.255.255 [This context uses dynamic NAT
for inside users that access the outside]
static (dmz,outside) 209.165.201.6 192.168.2.2 netmask 255.255.255.255 [A host on the
admin context requires access to the Websense server for management using pcAnywhere, so
the Websense server requires a static translation]
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic. Because there is no NAT from inside to dmz, you do not have to deny
traffic from accessing the dmz.]
access-list MANAGE extended permit tcp host 209.165.201.30 host 209.165.201.6 eq
pcanywhere-data
access-list MANAGE extended permit udp host 209.165.201.30 host 209.165.201.6 eq
pcanywhere-status
access-group MANAGE in interface outside [This ACL allows the management host to use
pcAnywhere on the Websense server]
access-list WEBSENSE extended permit tcp host 192.168.2.2 any eq http [The Websense server
needs to access the Websense updater server on the outside]
access-group WEBSENSE in interface dmz
```

Example 1: Switch Configuration

The following lines in the Cisco IOS switch configuration relate to the FWSM:

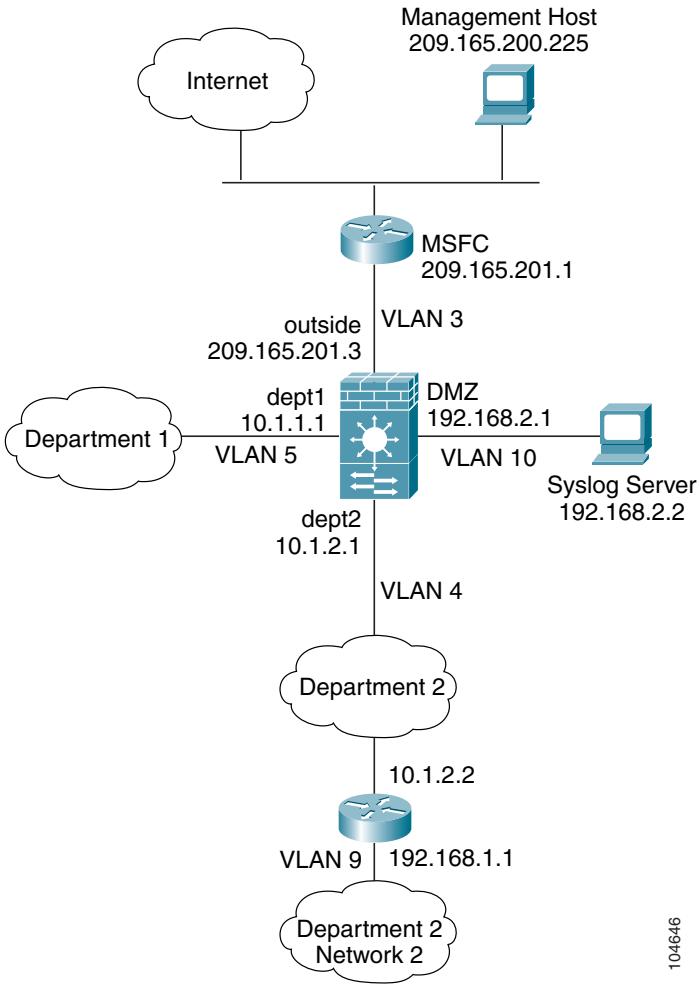
```
...
firewall module 8 vlan-group 1
firewall vlan-group 1 3-8
interface vlan 3
    ip address 209.165.201.1 255.255.255.224
    no shut
...
```

Example 2: Single Mode Using Same Security Level

This configuration creates three internal interfaces. Two of the interfaces connect to departments that are on the same security level, which allows all hosts to communicate without using NAT. The DMZ interface hosts a Syslog server. The management host on the outside needs access to the Syslog server and the FWSM. To connect to the FWSM, the host uses a VPN connection. The FWSM uses RIP on the inside interfaces to learn routes. Because the FWSM does not advertise routes with RIP, the MSFC needs to use static routes for FWSM traffic (see Figure B-2).

The Department networks are allowed to access the Internet, and use PAT.

Figure B-2 Example 2



See the following sections for the configurations for this scenario:

- Example 2: FWSM Configuration, page B-6
- Example 2: Switch Configuration, page B-7

Example 2: FWSM Configuration

```
nameif vlan3 outside security0
nameif vlan4 dept2 security100
nameif vlan5 dept1 security100
nameif vlan10 dmz security50
passwd g00fba11
enable password gen1u$
hostname Buster
same-security-traffic permit inter-interface
ip address outside 209.165.201.3 255.255.255.224
ip address dept2 10.1.2.1 255.255.255.0
ip address dept1 10.1.1.1 255.255.255.0
ip address dmz 192.168.2.1 255.255.255.0
route outside 0 0 209.165.201.1 1
nat (dept1) 1 10.1.1.0 255.255.255.0
nat (dept2) 1 10.1.2.0 255.255.255.0
```

```
global (outside) 1 209.165.201.9 netmask 255.255.255.255 [The dept1 and dept2 networks use
PAT when accessing the outside]
static (dmz,outside) 209.165.201.5 192.168.2.2 netmask 255.255.255.255 [The syslog server
needs a static translation so the outside management host can access the server]
access-list DEPTS extended permit ip any any
access-group DEPTS in interface dept1
access-group DEPTS in interface dept2 [Allows all dept1 and dept2 hosts to access the
outside for any IP traffic]
access-list MANAGE extended permit tcp host 209.165.200.225 host 209.165.201.5 eq telnet
access-group MANAGE in interface outside [This ACL allows the management host to access
the syslog server]
rip dept2 default version 2 authentication md5 scorpius 1 [Advertises the FWSM IP address
as the default gateway for the downstream router. The FWSM does not advertise a default
route to the MSFC.]
rip dept2 passive version 2 authentication md5 scorpius 1 [Listens for RIP updates from
the downstream router. The FWSM does not listen for RIP updates from the MSFC because a
default route to the MSFC is all that is required.]
isakmp policy 1 authentication pre-share [The client uses a pre-shared key to connect to
the FWSM over IPSec. The key is the password in the username command below.]
isakmp policy 1 encryption 3des
isakmp policy 1 group 2
isakmp policy 1 hash sha
isakmp enable outside
crypto ipsec transform-set vpn_client esp-3des esp-sha-hmac
username admin password passw0rd
crypto ipsec transform-set vpn esp-3des esp-sha-hmac
crypto dynamic-map vpn_client 1 set transform-set vpn
crypto map telnet_tunnel 1 ipsec-isakmp dynamic vpn_client
crypto map telnet_tunnel interface outside
crypto map telnet_tunnel client authentication LOCAL
ip local pool client_pool 10.1.1.2
access-list VPN_SPLIT extended permit ip host 209.165.201.3 host 10.1.1.2
vpngroup admin address-pool client_pool
vpngroup admin split-tunnel VPN_SPLIT
vpngroup admin password $ecure23
telnet 10.1.1.2 255.255.255.255 outside
telnet timeout 30
logging trap 5
logging host dmz 192.168.2.2 [System messages are sent to the syslog server on the DMZ
network]
logging on
```

Example 2: Switch Configuration

The following lines in the switch configuration relate to the FWSM:

Catalyst OS on the supervisor:

```
set vlan 3-5,9,10 firewall-vlan 8
```

Cisco IOS software on the MSFC:

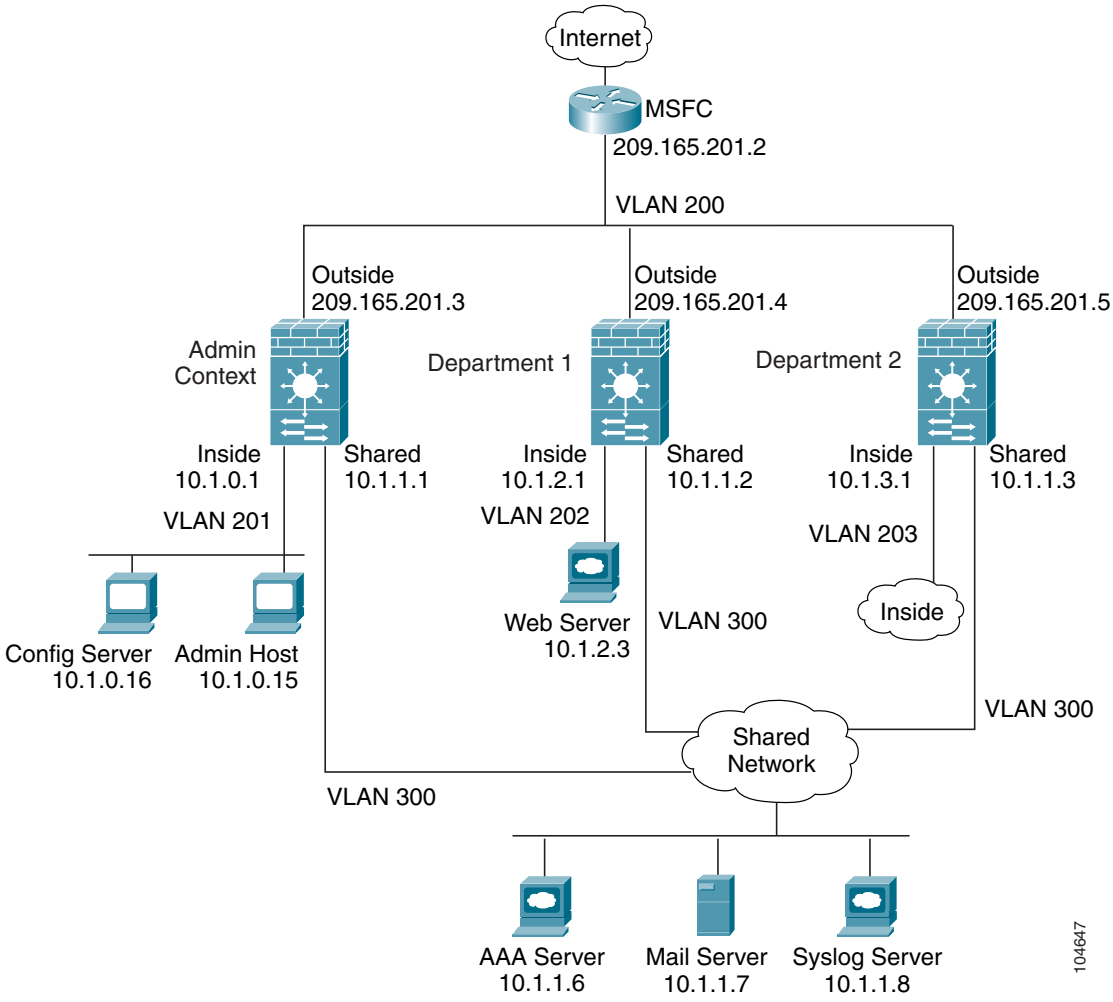
```
interface vlan 3
    ip address 209.165.201.1 255.255.255.224
    no shut
...
```

Example 3: Shared Resources for Multiple Contexts

This configuration includes multiple contexts for multiple departments within a company. Each department has its own security context so that each department can have its own security policy. However, the syslog, mail, and AAA servers are shared across all departments. These servers are placed on a shared VLAN (see Figure B-3).

Department 1 has a web server that outside users who are authenticated by the AAA server can access.

Figure B-3 Example 3



See the following sections for the configurations for this scenario:

- Example 3: System Configuration, page B-9
- Example 3: Admin Context Configuration, page B-9
- Example 3: Department 1 Context Configuration, page B-10
- Example 3: Department 2 Context Configuration, page B-11
- Example 3: Switch Configuration, page B-11

Example 3: System Configuration

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts using the **activation-key** command. The mode and the activation key are not stored in the configuration file, even though they do endure reboots. If you view the configuration on the FWSM using the **write terminal**, **show startup**, or **show running** commands, the mode displays after the FWSM Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
hostname Ubik
password pkd55
enable password deckard69
admin-context admin
context admin
    allocate-interface vlan200
    allocate-interface vlan201
    allocate-interface vlan300
    config-url disk://admin.cfg
context department1
    allocate-interface vlan200
    allocate-interface vlan202
    allocate-interface vlan300
    config-url ftp://admin:passw0rd@10.1.0.16/dept1.cfg
context department2
    allocate-interface vlan200
    allocate-interface vlan203
    allocate-interface vlan300
    config-url ftp://admin:passw0rd@10.1.0.16/dept2.cfg
```

Example 3: Admin Context Configuration

```
hostname Admin
nameif vlan200 outside security0
nameif vlan201 inside security100
nameif vlan300 shared security50
passwd v00d00
enable password d011
ip address outside 209.165.201.3 255.255.255.224
ip address inside 10.1.0.1 255.255.255.0
ip address shared 10.1.1.1 255.255.255.0
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.0.0 255.255.255.0
global (outside) 1 209.165.201.6 netmask 255.255.255.255 [This context uses PAT for inside
users that access the outside]
global (shared) 1 10.1.1.30 [This context uses PAT for inside users that access the shared
network]
static (inside,outside) 209.165.201.7 10.1.0.15 netmask 255.255.255.255 [Because this host
can access the web server in the Department 1 context, it requires a static translation]
static (inside,shared) 10.1.1.78 10.1.0.15 netmask 255.255.255.255 [Because this host has
management access to the servers on the Shared interface, it requires a static translation
to be used in an ACL]
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
and shared network for any IP traffic]
access-list SHARED extended permit ip host 10.1.1.78 any
access-list SHARED extended permit tcp host 10.1.1.30 host 10.1.1.7 eq smtp
access-group SHARED out interface shared [This ACL allows only mail traffic from the
inside network to exit out the shared interface, but allows the admin host to access any
server. Note that the translated addresses are used.]
```

```
telnet 10.1.0.15 255.255.255.255 inside [Allows 10.1.0.15 to access the admin context
using Telnet. From the admin context, you can access all other contexts.]
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6 TheUauthKey
aaa authentication telnet console AAA-SERVER [The host at 10.1.0.15 must authenticate with
the AAA server to log in]
logging trap 6
logging host shared 10.1.1.8 [System messages are sent to the syslog server on the Shared
network]
logging on
```

Example 3: Department 1 Context Configuration

```
nameif vlan200 outside security0
nameif vlan202 inside security100
nameif vlan300 shared security50
passwd cugel
enable password rhialto
ip address outside 209.165.201.4 255.255.255.224
ip address inside 10.1.2.1 255.255.255.0
ip address shared 10.1.1.2 255.255.255.0
nat (inside) 1 10.1.2.0 255.255.255.0
global (outside) 1 209.165.201.8 netmask 255.255.255.255 [The inside network uses PAT when
accessing the outside]
global (shared) 1 10.1.1.31-10.1.1.37 [The inside network uses dynamic NAT when accessing
the shared network]
static (inside,outside) 209.165.201.9 10.1.2.3 netmask 255.255.255.255 [The web server can
be accessed from outside and requires a static translation]
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
and shared network for any IP traffic]
access-list WEBSERVER extended permit ip host 209.165.201.7 host 209.165.201.9 [This ACE
allows the management host (its translated address) on the admin context to access the web
server for management (it can use any IP protocol)]
access-list WEBSERVER extended permit tcp any eq http host 209.165.201.9 eq http [This ACE
allows any outside address to access the web server with HTTP]
access-group WEBSERVER in interface outside
access-list MAIL extended permit tcp host 10.1.1.31 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.32 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.33 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.34 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.35 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.36 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.37 eq smtp host 10.1.1.7 eq smtp
access-group MAIL out interface shared [This ACL allows only mail traffic from the inside
network to exit out the shared interface. Note that the translated addresses are used.]
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6 TheUauthKey
aaa authentication match WEBSERVER outside AAA-SERVER [All traffic matching the WEBSERVER
ACL must authenticate with the AAA server]
logging trap 4
logging host shared 10.1.1.8 [System messages are sent to the syslog server on the Shared
network]
logging on
```

Example 3: Department 2 Context Configuration

```
nameif vlan200 outside security0
nameif vlan203 inside security100
nameif vlan300 shared security50
passwd maz1r1an
enable password ly0ne$$e
ip address outside 209.165.201.5 255.255.255.224
ip address inside 10.1.3.1 255.255.255.0
ip address shared 10.1.1.3 255.255.255.0
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.3.0 255.255.255.0
global (outside) 1 209.165.201.10 netmask 255.255.255.255 [The inside network uses PAT
when accessing the outside]
global (shared) 1 10.1.1.38 [The inside network uses PAT when accessing the shared
network]
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
and shared network for any IP traffic]
access-list MAIL extended permit tcp host 10.1.1.38 host 10.1.1.7 eq smtp
access-group MAIL out interface shared [This ACL allows only mail traffic from the inside
network to exit out the shared interface. Note that the translated PAT address is used.]
logging trap 3
logging host shared 10.1.1.8 [System messages are sent to the syslog server on the Shared
network]
logging on
```

Example 3: Switch Configuration

The following lines in the Cisco IOS switch configuration relate to the FWSM:

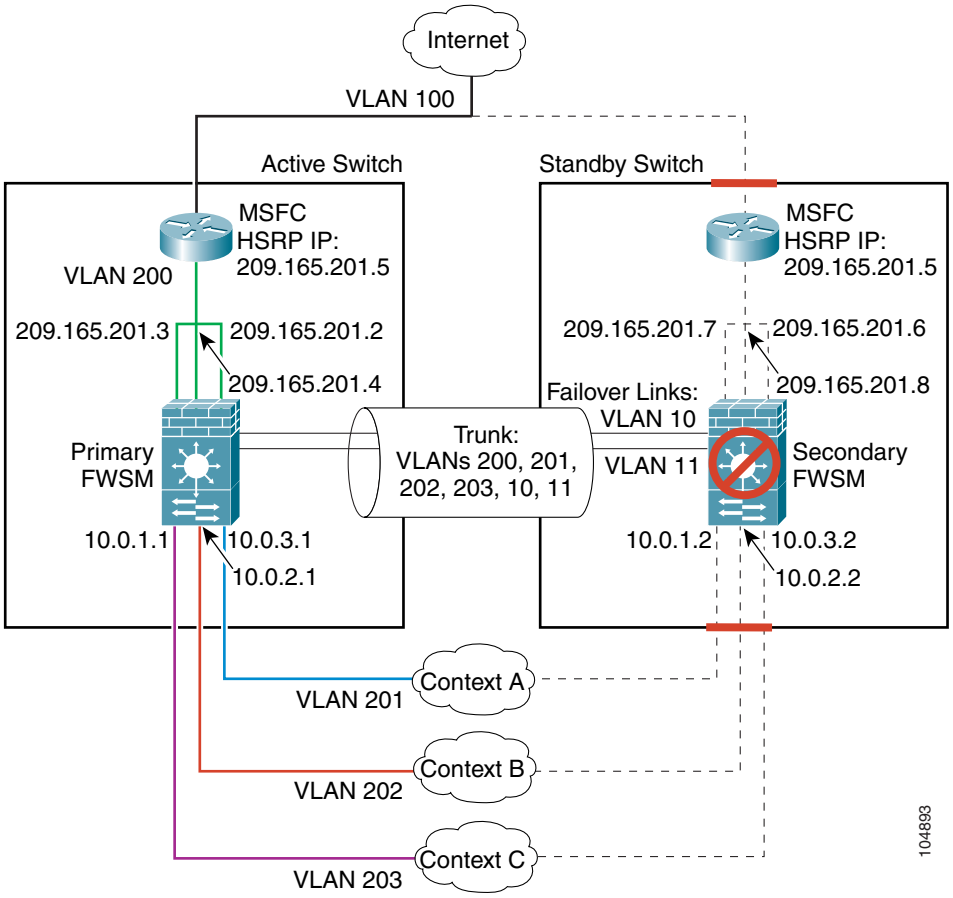
```
...
firewall module 6 vlan-group 1
firewall vlan-group 1 200-203,300
interface vlan 200
    ip address 209.165.201.2 255.255.255.224
    no shut
...
```

Example 4: Failover

This configuration shows a routed, multiple context mode FWSM in one switch, and another FWSM in a second switch acting as a backup (see Figure B-4). Each context (A, B, and C) monitors the inside interface, and context A, which is the admin context, also monitors the outside interface. Because the outside interface is shared among all contexts, monitoring in one context benefits all contexts.

The secondary FWSM is also in routed, multiple context mode, and has the same software version.

Figure B-4 Example 4



See the following sections for the configurations for this scenario:

- Example 4: Primary FWSM Configuration, page B-12
- Example 4: Secondary FWSM System Configuration, page B-14
- Example 4: Switch Configuration, page B-14

Example 4: Primary FWSM Configuration

The following sections include the configuration for the primary FWSM:

- Example 4: System Configuration (Primary), page B-12
- Example 4: Context A Configuration (Primary), page B-13
- Example 4: Context B Configuration (Primary), page B-13
- Example 4: Context C Configuration (Primary), page B-14

Example 4: System Configuration (Primary)

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts using the **activation-key** command. The mode and the activation key are not stored in the configuration file, even though they do endure reboots. If you view

the configuration on the FWSM using the **write terminal**, **show startup**, or **show running** commands, the mode displays after the FWSM Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
hostname primary
enable password farscape
password crichton
failover lan interface faillink vlan 10
failover link statelink vlan 11
failover lan unit primary
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover interface ip statelink 192.168.253.5 255.255.255.252 standby 192.168.253.6
failover interface-policy 50%
failover replication http
failover
admin-context contexta
context contexta
    allocate-interface vlan200
    allocate-interface vlan201
    config-url disk://contexta.cfg
context contextb
    allocate-interface vlan200
    allocate-interface vlan202
    config-url ftp://admin:passw0rd@10.0.3.16/contextb.cfg
context contextc
    allocate-interface vlan200
    allocate-interface vlan203
    config-url ftp://admin:passw0rd@10.0.3.16/contextc.cfg
```

Example 4: Context A Configuration (Primary)

```
nameif vlan200 outside security0
nameif vlan201 inside security100
passwd secret1969
enable password h1and10
ip address outside 209.165.201.2 255.255.255.224 standby 209.165.201.6
ip address inside 10.0.3.1 255.255.255.0 standby 10.0.3.2
monitor-interface inside
monitor-interface outside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 209.165.201.10 netmask 255.255.255.224 [This context uses dynamic PAT
for inside users that access the outside]
route outside 0 0 209.165.201.5 1
telnet 10.0.3.75 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
```

Example 4: Context B Configuration (Primary)

```
nameif vlan200 outside security0
nameif vlan202 inside security100
passwd secret1978
enable password 7samura1
ip address outside 209.165.201.4 255.255.255.224 standby 209.165.201.8
ip address inside 10.0.2.1 255.255.255.0 standby 10.0.2.2
monitor-interface inside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 209.165.201.11 netmask 255.255.255.224 [This context uses dynamic PAT
for inside users that access the outside]
route outside 0 0 209.165.201.5 1
```

```
telnet 10.0.2.14 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
```

Example 4: Context C Configuration (Primary)

```
nameif vlan200 outside security0
nameif vlan203 inside security100
passwd secret0997
enable password strayd0g
ip address outside 209.165.201.3 255.255.255.224 standby 209.165.201.7
ip address inside 10.0.1.1 255.255.255.0 standby 10.0.1.2
monitor-interface inside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 209.165.201.12 netmask 255.255.255.224 [This context uses dynamic PAT
for inside users that access the outside]
route outside 0 0 209.165.201.5 1
telnet 10.0.1.65 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
```

Example 4: Secondary FWSM System Configuration

You do not need to configure any contexts, just the following minimal configuration for the system.

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts using the **activation-key** command. The mode and the activation key are not stored in the configuration file, even though they do endure reboots. If you view the configuration on the FWSM using the **write terminal**, **show startup**, or **show running** commands, the mode displays after the FWSM Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
failover lan interface faillink vlan 10
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover lan unit secondary
failover
```

Example 4: Switch Configuration

The following lines in the Cisco IOS switch configuration on both switches relate to the FWSM. For information about configuring redundancy for the switch, see the switch documentation.

```
...
firewall module 1 vlan-group 1
firewall vlan-group 1 10,11,200-203
interface vlan 200
    ip address 209.165.201.1 255.255.255.224
    standby 200 ip 209.165.201.5
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shut
interface range gigabitethernet 2/1-3
    channel-group 2 mode on
    switchport trunk encapsulation dot1q
    no shut
...
```

Transparent Mode Examples

This section includes the following topics:

Example 5: Security Contexts With Outside Access

This configuration creates three security contexts plus the admin context. Each context allows OSPF traffic to pass between the inside and outside routers (see Figure B-5).

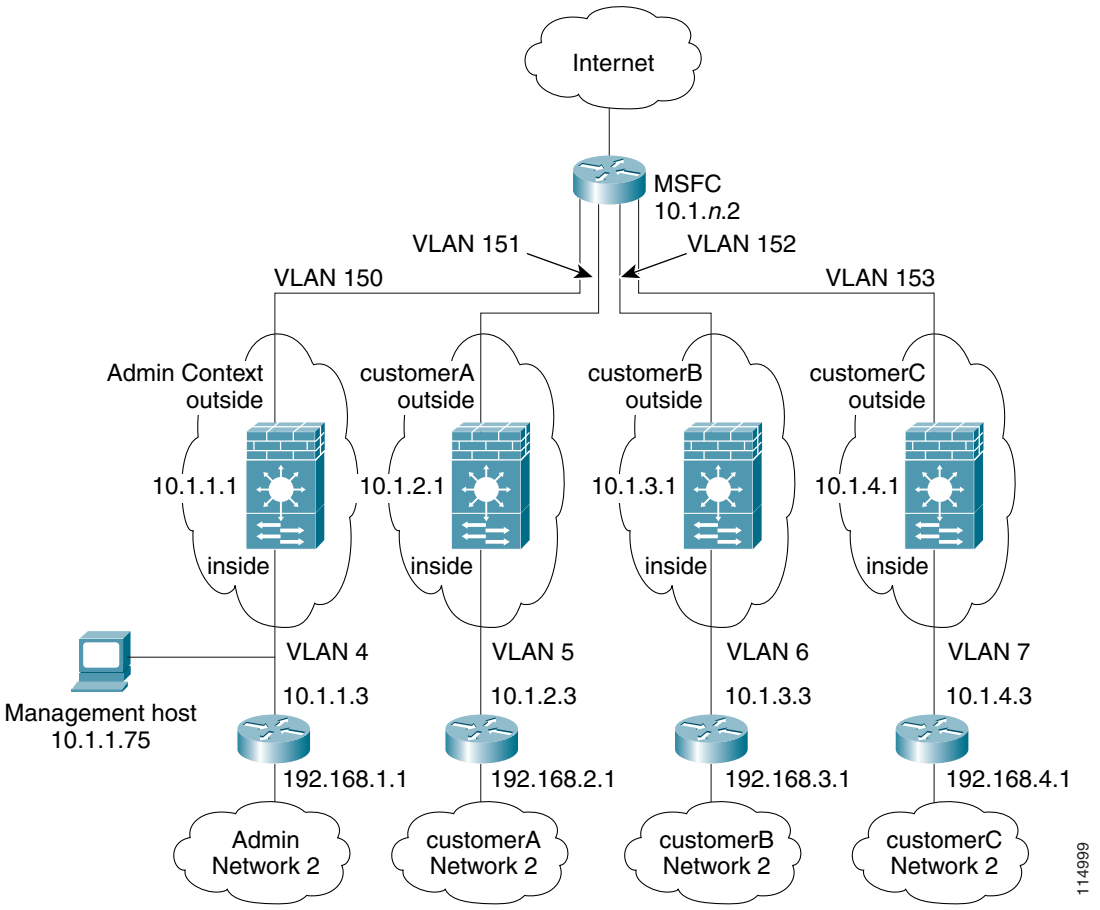
Inside hosts can access the Internet through the outside, but no outside hosts can access the inside.

The admin context allows SSH sessions to the FWSM from one host.

Each customer context belongs to a class that limits its resources (gold, silver, or bronze).

Although inside IP addresses can be the same across contexts, keeping them unique is easier to manage.

Figure B-5 Example 5



See the following sections for the configurations for this scenario:

- Example 1: System Configuration, page B-2
- Example 5: System Configuration, page B-16
- Example 5: Admin Context Configuration, page B-17
- Example 5: Customer A Context Configuration, page B-17
- Example 5: Customer B Context Configuration, page B-17
- Example 5: Customer C Context Configuration, page B-18
- Example 5: Switch Configuration, page B-18

Example 5: System Configuration

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts using the **activation-key** command. The mode and the activation key are not stored in the configuration file, even though they do endure reboots. If you view the configuration on the FWSM using the **write terminal**, **show startup**, or **show running** commands, the mode displays after the FWSM Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
firewall transparent
hostname Farscape
password passw0rd
enable password chr1cht0n
admin-context admin
context admin
    allocate-interface vlan150
    allocate-interface vlan4
    config-url disk://admin.cfg
    class default
context customerA
    description This is the context for customer A
    allocate-interface vlan151
    allocate-interface vlan5
    config-url disk://contexta.cfg
    class gold
context customerB
    description This is the context for customer B
    allocate-interface vlan152
    allocate-interface vlan6
    config-url disk://contextb.cfg
    class silver
context customerC
    description This is the context for customer C
    allocate-interface vlan153
    allocate-interface vlan7
    config-url disk://contextc.cfg
    class bronze
class gold
    limit-resource all 7%
    limit-resource rate conns 2000
    limit-resource conns 20000
class silver
    limit-resource all 5%
    limit-resource rate conns 1000
    limit-resource conns 10000
class bronze
    limit-resource all 3%
    limit-resource rate conns 500
    limit-resource conns 5000
```

Example 5: Admin Context Configuration

The host at 10.1.1.75 can access the context using SSH, which requires a certificate to be generated using the **ca generate rsa key** *modulus* command and saved using the **ca save all** command. The certificate is saved in Flash memory.

```
hostname Admin
domain isp
nameif vlan150 outside security0
nameif vlan4 inside security100
passwd secret1969
enable password h1and10
ip address 10.1.1.1 255.255.255.0
route outside 0 0 10.1.1.2 1
ssh 10.1.1.75 255.255.255.255 inside
access-list INTERNET extended permit 89 any any
access-list INTERNET extended permit ip any any
access-list OSPF extended permit 89 any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic. Also allows OSPF.]
access-group OSPF in interface outside [Allows OSPF.]
```

Example 5: Customer A Context Configuration

```
nameif vlan151 outside security0
nameif vlan5 inside security100
passwd hell0!
enable password enter55
ip address 10.1.2.1 255.255.255.0
route outside 0 0 10.1.2.2 1
access-list INTERNET extended permit 89 any any
access-list INTERNET extended permit ip any any
access-list OSPF extended permit 89 any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic. Also allows OSPF.]
access-group OSPF in interface outside [Allows OSPF.]
```

Example 5: Customer B Context Configuration

```
nameif vlan152 outside security0
nameif vlan6 inside security100
passwd tenac10us
enable password defen$e
ip address 10.1.3.1 255.255.255.0
route outside 0 0 10.1.3.2 1
access-list INTERNET extended permit 89 any any
access-list INTERNET extended permit ip any any
access-list OSPF extended permit 89 any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic. Also allows OSPF.]
access-group OSPF in interface outside [Allows OSPF.]
```

Example 5: Customer C Context Configuration

```
nameif vlan153 outside security0
nameif vlan7 inside security100
passwd fl0wer
enable password treeh0u$e
ip address 10.1.4.1 255.255.255.0
route outside 0 0 10.1.4.2 1
access-list INTERNET extended permit 89 any any
access-list INTERNET extended permit ip any any
access-list OSPF extended permit 89 any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic. Also allows OSPF.]
access-group OSPF in interface outside [Allows OSPF.]
```

Example 5: Switch Configuration

The following lines in the Cisco IOS switch configuration relate to the FWSM:

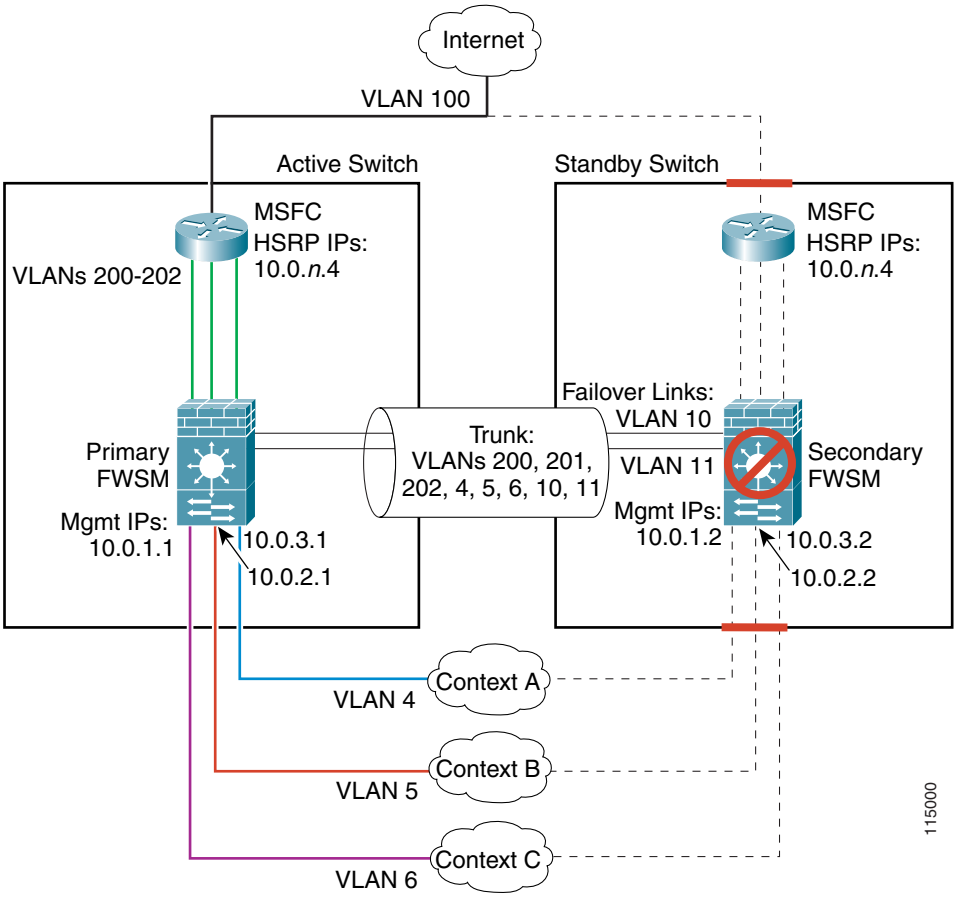
```
...
firewall multiple-vlan-interfaces
firewall module 8 vlan-group 1
firewall vlan-group 1 4-7,150-153
interface vlan 150
    ip address 10.1.1.2 255.255.255.0
    no shut
interface vlan 151
    ip address 10.1.2.2 255.255.255.0
    no shut
interface vlan 152
    ip address 10.1.3.2 255.255.255.0
    no shut
interface vlan 153
    ip address 10.1.4.2 255.255.255.0
    no shut
...
```

Example 6: Failover

This configuration shows a transparent, multiple context mode FWSM in one switch, and another FWSM in a second switch acting as a backup (see Figure B-4). Each context (A, B, and C) monitors the inside interface and outside interface.

The secondary FWSM is also in transparent, multiple context mode, and has the same software version.

Figure B-6 Example 6



See the following sections for the configurations for this scenario:

- Example 6: Primary FWSM Configuration, page B-19
- Example 6: Secondary FWSM System Configuration, page B-21
- Example 6: Switch Configuration, page B-21

Example 6: Primary FWSM Configuration

The following sections include the configuration for the primary FWSM:

- Example 6: System Configuration (Primary), page B-19
- Example 6: Context A Configuration (Primary), page B-20
- Example 6: Context B Configuration (Primary), page B-20
- Example 6: Context C Configuration (Primary), page B-21

Example 6: System Configuration (Primary)

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts using the **activation-key** command. The mode and the activation key are not stored in the configuration file, even though they do endure reboots. If you view

the configuration on the FWSM using the **write terminal**, **show startup**, or **show running** commands, the mode displays after the FWSM Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
firewall transparent
hostname primary
enable password farscape
password crichton
failover lan interface faillink vlan 10
failover link statelink vlan 11
failover lan unit primary
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover interface ip statelink 192.168.253.5 255.255.255.252 standby 192.168.253.6
failover interface-policy 1
failover replication http
failover
admin-context contexta
context contexta
    allocate-interface vlan200
    allocate-interface vlan4
    config-url disk://contexta.cfg
context contextb
    allocate-interface vlan201
    allocate-interface vlan5
    config-url ftp://admin:passw0rd@10.0.3.16/contextb.cfg
context contextc
    allocate-interface vlan202
    allocate-interface vlan6
    config-url ftp://admin:passw0rd@10.0.3.16/contextc.cfg
```

Example 6: Context A Configuration (Primary)

```
nameif vlan200 outside security0
nameif vlan4 inside security100
passwd secret1969
enable password h1andl0
ip address 10.0.3.1 255.255.255.0 standby 10.0.3.2
monitor-interface inside
monitor-interface outside
route outside 0 0 10.0.3.4 1
telnet 10.0.3.75 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside
```

Example 6: Context B Configuration (Primary)

```
nameif vlan201 outside security0
nameif vlan5 inside security100
passwd secret1978
enable password 7samura1
ip address inside 10.0.2.1 255.255.255.0 standby 10.0.2.2
monitor-interface inside
monitor-interface outside
route outside 0 0 10.0.2.4 1
telnet 10.0.2.14 255.255.255.255 inside
access-list INTERNET extended permit ip any any
```

```
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside
```

Example 6: Context C Configuration (Primary)

```
nameif vlan202 outside security0
nameif vlan6 inside security100
passwd secret0997
enable password strayd0g
ip address inside 10.0.1.1 255.255.255.0 standby 10.0.1.2
monitor-interface inside
monitor-interface outside
route outside 0 0 10.0.1.4 1
telnet 10.0.1.65 255.255.255.255 inside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside [Allows all inside hosts to access the outside
for any IP traffic]
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside
```

Example 6: Secondary FWSM System Configuration

You do not need to configure any contexts, just the following minimal configuration for the system.

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts using the **activation-key** command. The mode and the activation key are not stored in the configuration file, even though they do endure reboots. If you view the configuration on the FWSM using the **write terminal**, **show startup**, or **show running** commands, the mode displays after the FWSM Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
firewall transparent
failover lan interface faillink vlan 10
failover interface ip faillink 192.168.253.1 255.255.255.252 standby 192.168.253.2
failover lan unit secondary
failover
```

Example 6: Switch Configuration

The following lines in the Cisco IOS switch configuration on both switches relate to the FWSM. For information about configuring redundancy for the switch, see the switch documentation.

```
...
firewall multiple-vlan-interfaces
firewall module 1 vlan-group 1
firewall vlan-group 1 4-6,10,11,200-202
interface vlan 200
    ip address 10.0.1.3 255.255.255.0
    standby 200 ip 10.0.1.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shut
```

```
interface vlan 201
    ip address 10.0.2.3 255.255.255.0
    standby 200 ip 10.0.2.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shut
interface vlan 202
    ip address 10.0.3.3 255.255.255.0
    standby 200 ip 10.0.3.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shut
interface range gigabitethernet 2/1-3
    channel-group 2 mode on
    switchport trunk encapsulation dot1q
    no shut
...
```