



Sample Configurations

This appendix illustrates and describes a number of common ways to implement FWSM, and includes the following sections:

- [Routed Mode Sample Configurations, page B-1](#)
- [Transparent Mode Sample Configurations, page B-14](#)
- [Failover Example Configurations, page B-18](#)

Routed Mode Sample Configurations

This section includes the following topics:

- [Example 1: Multiple Mode Firewall with Outside Access, page B-1](#)
- [Example 2: Single Mode Firewall Using Same Security Level Example, page B-6](#)
- [Example 3: Shared Resources for Multiple Contexts Example, page B-8](#)
- [Example 4: IPv6 Configuration Example, page B-13](#)

Example 1: Multiple Mode Firewall with Outside Access

The following 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 interface using dynamic NAT or PAT, but no outside hosts can access the inside.

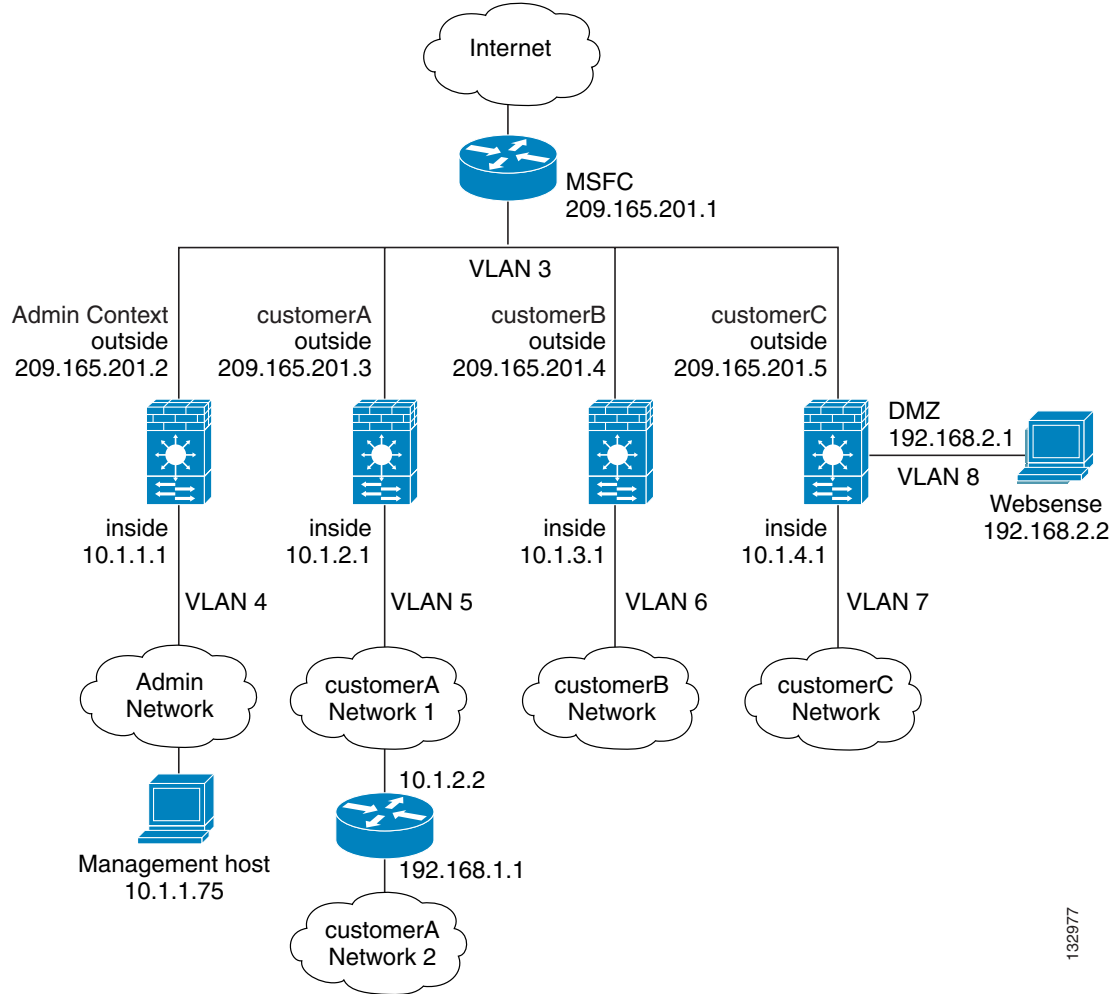
The Customer A context has a second network behind an inside router.

The admin context allows SSH sessions to 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 interfaces are unique, keeping them unique is easier to manage.

Figure B-1 Example 1



132977

See the following sections for the configurations for this scenario:

- [System Configuration \(Example 1\), page B-2](#)
- [Admin Context Configuration \(Example 1\), page B-3](#)
- [Customer A Context Configuration \(Example 1\), page B-4](#)
- [Customer B Context Configuration \(Example 1\), page B-4](#)
- [Customer C Context Configuration \(Example 1\), page B-5](#)
- [Switch Configuration \(Example 1\), page B-5](#)

System Configuration (Example 1)

You must first enable multiple context mode using the **mode multiple** command. Then enter the activation key to allow more than two contexts. The mode and activation key are not stored in the configuration file, even though they endure reboots. If you view the configuration on the FWSM using the **write terminal**, **show startup-config**, or **show running-config** commands, the mode displays after the FWSM Release (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
interface vlan 3
interface vlan 4
interface vlan 5
interface vlan 6
interface vlan 7
interface vlan 8
context admin
    allocate-interface vlan3
    allocate-interface vlan4
    config-url disk://admin.cfg
    member default
context customerA
    description This is the context for customer A
    allocate-interface vlan3
    allocate-interface vlan5
    config-url disk://contexta.cfg
    member gold
context customerB
    description This is the context for customer B
    allocate-interface vlan3
    allocate-interface vlan6
    config-url disk://contextb.cfg
    member silver
context customerC
    description This is the context for customer C
    allocate-interface vlan3
    allocate-interface vlan7-vlan8
    config-url disk://contextc.cfg
    member 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

```

Admin Context Configuration (Example 1)

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

```

interface vlan 3
    nameif outside
    security-level 0
    ip address 209.165.201.2 255.255.255.224
interface vlan 4
    nameif inside
    security-level 100
    ip address 10.1.1.1 255.255.255.0
passwd secret1969
enable password h1andl0

```

```

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
! This context uses dynamic NAT for inside users that access the outside
global (outside) 1 209.165.201.10-209.165.201.29
! The host at 10.1.1.75 has access to the Websense server in Customer C, and
! it needs a static translation for use in Customer C's access list
static (inside,outside) 209.165.201.30 10.1.1.75 netmask 255.255.255.255
access-list INTERNET remark -Allows inside hosts to access the outside for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside

```

Customer A Context Configuration (Example 1)

```

interface vlan 3
  nameif outside
  security-level 0
  ip address 209.165.201.3 255.255.255.224
interface vlan 5
  nameif inside
  security-level 100
  ip address 10.1.2.1 255.255.255.0
passwd hell0!
enable password enter55
route outside 0 0 209.165.201.1 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 router.
route inside 192.168.1.0 255.255.255.0 10.1.2.2 1
nat (inside) 1 10.1.2.0 255.255.255.0
! This context uses dynamic PAT for inside users that access that outside. The outside
! interface address is used for the PAT address
global (outside) 1 interface
access-list INTERNET remark -Allows inside hosts to access the outside for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside

```

Customer B Context Configuration (Example 1)

```

interface vlan 3
  nameif outside
  security-level 0
  ip address 209.165.201.4 255.255.255.224
interface vlan 6
  nameif inside
  security-level 100
  ip address 10.1.3.1 255.255.255.0
passwd tenac10us
enable password defen$e
route outside 0 0 209.165.201.1 1
nat (inside) 1 10.1.3.0 255.255.255.0
! This context uses dynamic PAT for inside users that access the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
access-list INTERNET remark Inside users only access HTTP and HTTPS servers on 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

```

Customer C Context Configuration (Example 1)

```

interface vlan 3
  nameif outside
  security-level 0
  ip address 209.165.201.5 255.255.255.224
interface vlan 7
  nameif inside
  security-level 100
  ip address 10.1.4.1 255.255.255.0
interface vlan 8
  nameif dmz
  security-level 50
  ip address 192.168.2.1 255.255.255.0
passwd fl0wer
enable password treeh0u$e
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, FWSM consults with a
! Websense server to determine if the traffic is allowed
nat (inside) 1 10.1.4.0 255.255.255.0
! This context uses dynamic NAT for inside users that access the outside
global (outside) 1 209.165.201.9 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 uses a static translation for its private address
static (dmz,outside) 209.165.201.6 192.168.2.2 netmask 255.255.255.255
access-list INTERNET remark -Allows all inside hosts to access the outside for any IP
access-list INTERNET remark -traffic, but denies them access to the dmz.
access-list INTERNET extended deny ip any 192.168.2.0 255.255.255.0
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list MANAGE remark -Allows the management host to use pcAnywhere on the
access-list MANAGE remark -Websense server
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
access-list WEBSENSE remark -The Websense server needs to access the Websense updaters
access-list WEBSENSE remark -server on the outside
access-list WEBSENSE extended permit tcp host 192.168.2.2 any eq http
access-group WEBSENSE in interface dmz

```

Switch Configuration (Example 1)

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 shutdown
...

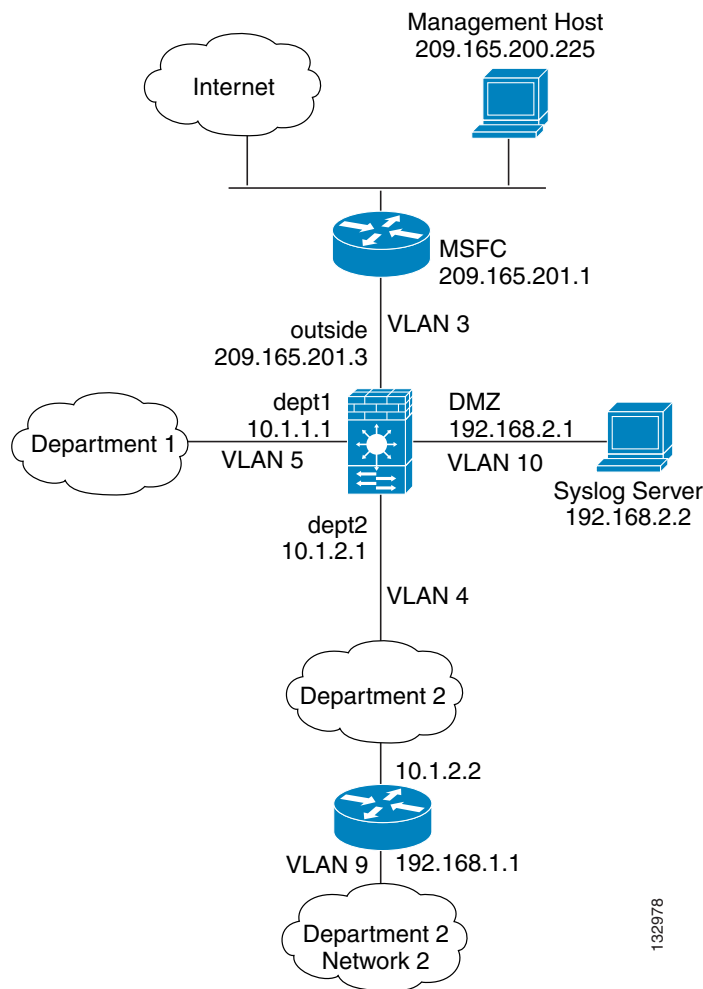
```

Example 2: Single Mode Firewall Using Same Security Level Example

The following configuration creates three internal interfaces. Two of the interfaces connect to departments that are on the same security level. 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. FWSM uses RIP on the inside interfaces to learn routes. Because the FWSM does not advertise routes with RIP, the upstream router 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 section:

- [FWSM Configuration \(Example 2\)](#), page B-7
- [Switch Configuration \(Example 2\)](#), page B-8

FWSM Configuration (Example 2)

```

interface vlan 3
  nameif outside
  security-level 0
  ip address 209.165.201.3 255.255.255.224
interface vlan 4
  nameif dept2
  security-level 100
  ip address 10.1.2.1 255.255.255.0
interface vlan 5
  nameif dept1
  security-level 100
  ip address 10.1.1.1 255.255.255.0
interface vlan 10
  nameif dmz
  security-level 50
  ip address 192.168.2.1 255.255.255.0
passwd g00fball
enable password genlu$
hostname Buster
same-security-traffic permit inter-interface
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
! The dept1 and dept2 networks use PAT when accessing the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
! Because we perform dynamic NAT on these addresses for outside access, we need to perform
! NAT on them for all other interface access. This identity static statement just
! translates the local address to the same address.
static (dept1,dept2) 10.1.1.0 10.1.1.0 netmask 255.255.255.0
static (dept2,dept1) 10.1.2.0 10.1.2.0 netmask 255.255.255.0
! The syslog server uses a static translation so the outside management host can access
! the server
static (dmz,outside) 209.165.201.5 192.168.2.2 netmask 255.255.255.255
access-list DEPTS remark -Allows all dept1 and dept2 hosts to access the
access-list DEPTS remark -outside for any IP traffic
access-list DEPTS extended permit ip any any
access-group DEPTS in interface dept1
access-group DEPTS in interface dept2
access-list MANAGE remark Allows the management host to access the syslog server
access-list MANAGE extended permit tcp host 209.165.200.225 host 209.165.201.5 eq telnet
access-group MANAGE in interface outside
! Advertises the FWSM IP address as the default gateway for the downstream
! router. FWSM does not advertise a default route to the router.
rip dept2 default version 2 authentication md5 scorpius 1
! Listens for RIP updates from the downstream router. FWSM does not
! listen for RIP updates from the router because a default route to the router is all that
! is required.
rip dept2 passive version 2 authentication md5 scorpius 1
! The client uses a pre-shared key to connect to the FWSM over IPsec. The
! key is the password in the username command following.
isakmp policy 1 authentication pre-share
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

```

```
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
telnet 10.1.1.2 255.255.255.255 outside
telnet timeout 30
logging trap 5
! System messages are sent to the syslog server on the DMZ network
logging host dmz 192.168.2.2
logging enable
```

Switch Configuration (Example 2)

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

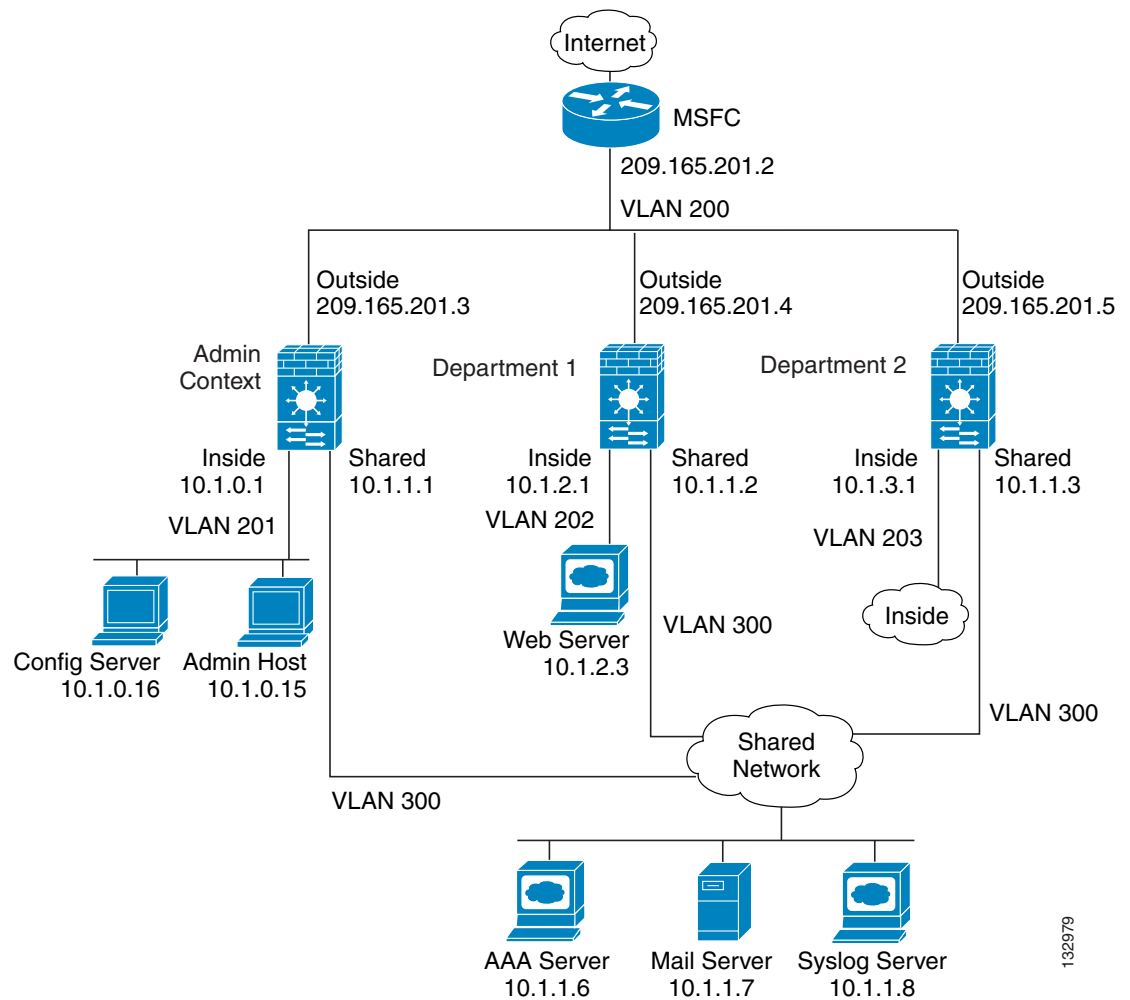
```
interface vlan 3
  ip address 209.165.201.1 255.255.255.224
  no shutdown
...
```

Example 3: Shared Resources for Multiple Contexts Example

The following 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 interface (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



132979

See the following sections for the configurations for this scenario:

- [System Configuration \(Example 3\), page B-9](#)
- [Admin Context Configuration \(Example 3\), page B-10](#)
- [Department 1 Context Configuration \(Example 3\), page B-11](#)
- [Department 2 Context Configuration \(Example 3\), page B-12](#)
- [Switch Configuration \(Example 3\), page B-12](#)

System Configuration (Example 3)

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 endure reboots. If you view the configuration on the FWSM using the **write terminal**, **show startup-config**, or **show running-config** commands, the mode displays after the FWSM Release (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
interface vlan 200
interface vlan 201
interface vlan 202
interface vlan 203
interface vlan 300
admin-context admin
context admin
    allocate-interface vlan200
    allocate-interface vlan201
    allocate-interface vlan300
    config-url disk0://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

```

Admin Context Configuration (Example 3)

```

interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.3 255.255.255.224
interface vlan 201
    nameif inside
    security-level 100
    ip address 10.1.0.1 255.255.255.0
interface vlan 300
    nameif shared
    security-level 50
    ip address 10.1.1.1 255.255.255.0
passwd v00d00
enable password d011
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.0.0 255.255.255.0
! This context uses PAT for inside users that access the outside
global (outside) 1 209.165.201.6 netmask 255.255.255.255
! This context uses PAT for inside users that access the shared network
global (shared) 1 10.1.1.30
! Because this host can access the web server in the Department 1 context, it requires a
! static translation
static (inside,outside) 209.165.201.7 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 access list
static (inside,shared) 10.1.1.78 10.1.0.15 netmask 255.255.255.255
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET remark -and shared network for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list SHARED remark -Allows only mail traffic from inside to exit shared interface
access-list SHARED remark -but allows the admin host to access any server.
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
! Note that the translated addresses are used.

```

```

access-group SHARED out interface shared
! Allows 10.1.0.15 to access the admin context using Telnet. From the admin context, you
! can access all other contexts.
telnet 10.1.0.15 255.255.255.255 inside
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6
    key TheUauthKey
    server-port 16
! The host at 10.1.0.15 must authenticate with the AAA server to log in
aaa authentication telnet console AAA-SERVER
logging trap 6
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging on

```

Department 1 Context Configuration (Example 3)

```

interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.4 255.255.255.224
interface vlan 202
    nameif inside
    security-level 100
    ip address 10.1.2.1 255.255.255.0
interface vlan 300
    nameif shared
    security-level 50
    ip address 10.1.1.2 255.255.255.0
passwd cugel
enable password rhalto
nat (inside) 1 10.1.2.0 255.255.255.0
! The inside network uses PAT when accessing the outside
global (outside) 1 209.165.201.8 netmask 255.255.255.255
! The inside network uses dynamic NAT when accessing the shared network
global (shared) 1 10.1.1.31-10.1.1.37
! The web server can be accessed from outside and requires a static translation
static (inside,outside) 209.165.201.9 10.1.2.3 netmask 255.255.255.255
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET remark -and shared network for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list WEBSERVER remark -Allows the management host (its translated address) on the
access-list WEBSERVER remark -admin context to access the web server for management
access-list WEBSERVER remark -it can use any IP protocol
access-list WEBSERVER extended permit ip host 209.165.201.7 host 209.165.201.9
access-list WEBSERVER remark -Allows any outside address to access the web server
access-list WEBSERVER extended permit tcp any eq http host 209.165.201.9 eq http
access-group WEBSERVER in interface outside
access-list MAIL remark -Allows only mail traffic from inside to exit out the shared int
! Note that the translated addresses are used.
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
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6

```

```

    key TheUauthKey
    server-port 16
    ! All traffic matching the WEBSEVER access list must authenticate with the AAA server
    aaa authentication match WEBSEVER outside AAA-SERVER
    logging trap 4
    ! System messages are sent to the syslog server on the Shared network
    logging host shared 10.1.1.8
    logging on

```

Department 2 Context Configuration (Example 3)

```

interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.5 255.255.255.224
interface vlan 203
    nameif inside
    security-level 100
    ip address 10.1.3.1 255.255.255.0
interface vlan 300
    nameif shared
    security-level 50
    ip address 10.1.1.3 255.255.255.0
passwd mazlrlan
enable password ly0ne$$e
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.3.0 255.255.255.0
! The inside network uses PAT when accessing the outside
global (outside) 1 209.165.201.10 netmask 255.255.255.255
! The inside network uses PAT when accessing the shared network
global (shared) 1 10.1.1.38
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET remark -and shared network for any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list MAIL remark -Allows only mail traffic from inside to exit out the shared int
access-list MAIL extended permit tcp host 10.1.1.38 host 10.1.1.7 eq smtp
! Note that the translated PAT address is used.
access-group MAIL out interface shared
logging trap 3
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging on

```

Switch Configuration (Example 3)

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 shutdown
...

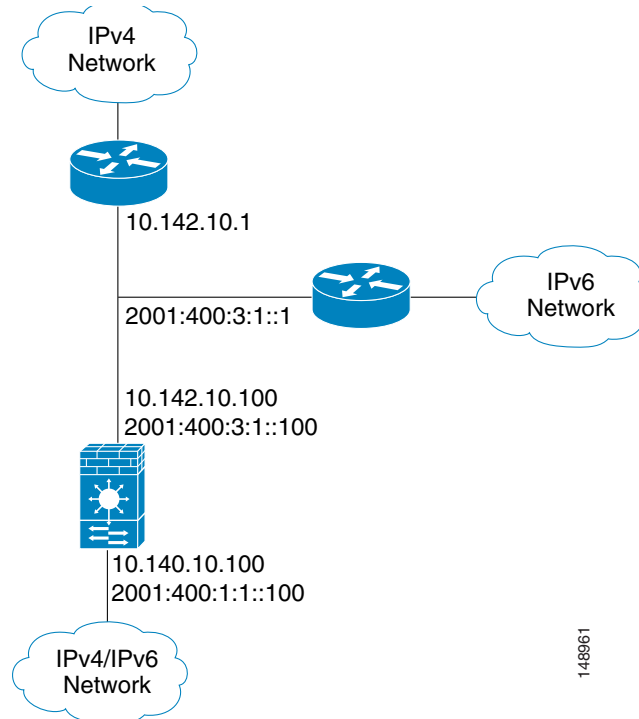
```

Example 4: IPv6 Configuration Example

The following configuration (see [Figure B-4](#)) shows several features of IPv6 configured on the FWSM:

- Each interface is configured with both IPv6 and IPv4 addresses.
- The IPv6 default route is set with the **ipv6 route** command.
- An IPv6 access list is applied to the outside interface.

Figure B-4 Example 4: IPv4 and IPv6 Dual Stack Configuration



```

password pkd
enable password happy
hostname ubik
interface vlan 100
    nameif outside
    security-level 0
    ip address 10.142.10.100 255.255.255.0
    ipv6 address 2001:400:3:1::100/64
    ipv6 nd suppress-ra
interface vlan 101
    nameif inside
    security-level 100
    ip address 10.140.10.100 255.255.255.0
    ipv6 address 2001:400:1:1::100/64
route outside 0.0.0.0 0.0.0.0 10.142.10.1 1
access-list INTERNET remark -Allows all inside IPv4 hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
ipv6 route outside ::/0 2001:400:3:1::1
ipv6 access-list IPV6INTERNET permit ip any any
access-group IPV6INTERNET in interface inside
ipv6 access-list OUTACL permit icmp6 2001:400:2:1::/64 2001:400:1:1::/64

```

```
ipv6 access-list OUTACL permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq telnet
ipv6 access-list OUTACL permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq ftp
ipv6 access-list OUTACL permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq www
access-group OUTACL in interface outside
```

Transparent Mode Sample Configurations

This section includes the following topics:

- [Example 5: Multiple Mode, Transparent Firewall with Outside Access Example, page B-14](#)

Example 5: Multiple Mode, Transparent Firewall with Outside Access Example

The following 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](#)).

Also, DHCP packets can pass through the transparent firewall, because the transparent firewall does not support the DHCP relay feature.

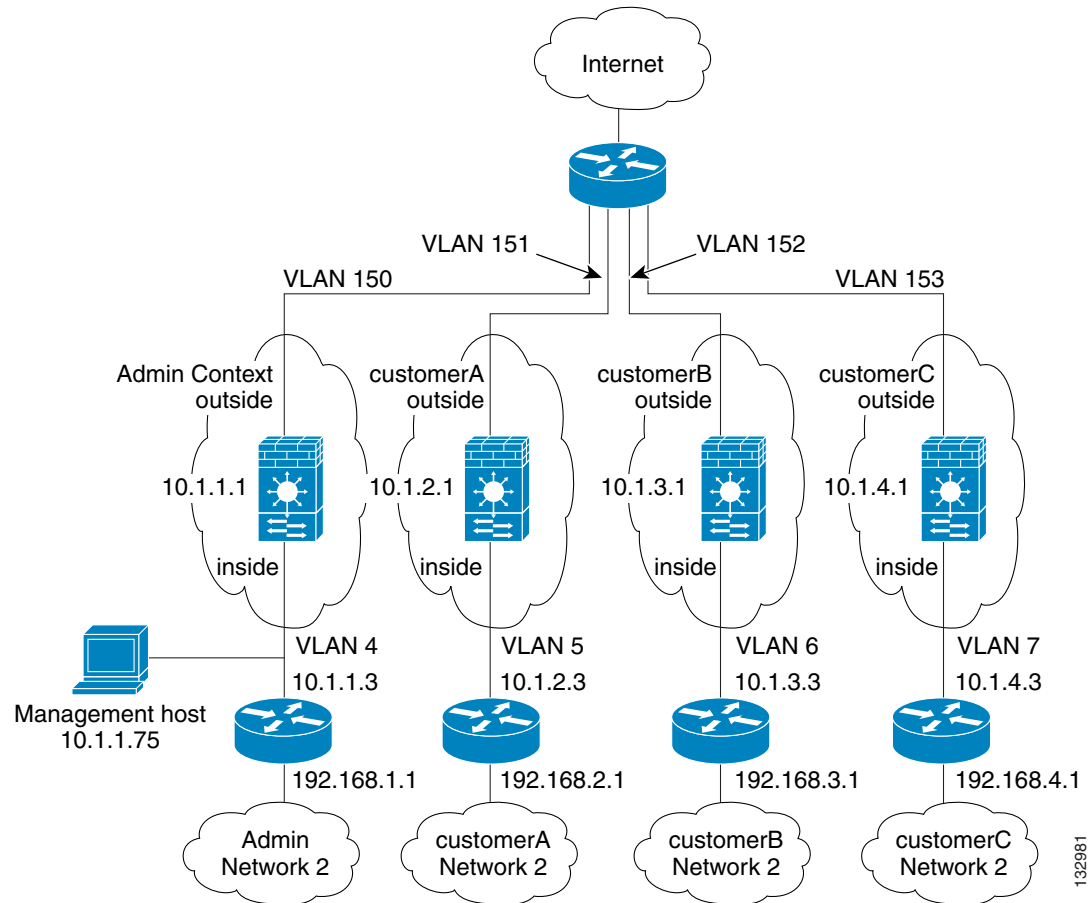
Inside hosts can access the Internet through the outside, but no outside hosts can access the inside.

The admin context allows SSH sessions to the FWSM from one host. It also uses ARP inspection to prevent IP spoofing of the upstream and downstream routers.

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:

- [System Configuration \(Example 5\), page B-15](#)
- [Admin Context Configuration \(Example 5\), page B-16](#)
- [Customer A Context Configuration \(Example 5\), page B-17](#)
- [Customer B Context Configuration \(Example 5\), page B-17](#)
- [Customer C Context Configuration \(Example 5\), page B-18](#)

System Configuration (Example 5)

You must first enable multiple context mode using the **mode multiple** command. The mode is not stored in the configuration file, even though it endures reboots. If you view the configuration on FWSM using the **write terminal**, **show startup-config**, or **show running-config** commands, the mode displays after the FWSM Release (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
interface vlan 4
interface vlan 5
interface vlan 6
```

```

interface vlan 7
interface vlan 150
interface vlan 151
interface vlan 152
interface vlan 153
admin-context admin
context admin
    allocate-interface vlan150
    allocate-interface vlan4
    config-url disk://admin.cfg
    member default
context customerA
    description This is the context for customer A
    allocate-interface vlan151
    allocate-interface vlan5
    config-url disk://contexta.cfg
    member gold
context customerB
    description This is the context for customer B
    allocate-interface vlan152
    allocate-interface vlan6
    config-url disk://contextb.cfg
    member silver
context customerC
    description This is the context for customer C
    allocate-interface vlan153
    allocate-interface vlan7
    config-url disk://contextc.cfg
    member 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

```

Admin Context Configuration (Example 5)

The host at 10.1.1.75 can access the context using SSH, which requires a key pair to be generated using the **crypto key generate** command.

```

firewall transparent
passwd secret1969
enable password h1andl0
interface vlan 150
    nameif outside
    security-level 0
    bridge-group 1
interface vlan 4
    nameif inside
    security-level 100
    bridge-group 1
interface bvi 1
    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
arp outside 10.1.1.2 0009.7cbe.2100
arp inside 10.1.1.3 0009.7cbe.1000
arp-inspection inside enable flood
arp-inspection outside enable flood
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back
access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside

```

Customer A Context Configuration (Example 5)

```

firewall transparent
passwd hell0!
enable password enter55
interface vlan 151
    nameif outside
    security-level 0
    bridge-group 45
interface vlan 5
    nameif inside
    security-level 100
    bridge-group 45
interface bvi 45
    ip address 10.1.2.1 255.255.255.0
route outside 0 0 10.1.2.2 1
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back
access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside

```

Customer B Context Configuration (Example 5)

```

firewall transparent
passwd tenac10us
enable password defen$e
interface vlan 152
    nameif outside
    security-level 0
    bridge-group 1
interface vlan 6
    nameif inside
    security-level 100
    bridge-group 1
interface bvi 1
    ip address 10.1.3.1 255.255.255.0
route outside 0 0 10.1.3.2 1
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back

```

```

access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside

```

Customer C Context Configuration (Example 5)

```

firewall transparent
passwd f10wer
enable password treeh0u$e
interface vlan 153
    nameif outside
    security-level 0
    bridge-group 100
interface vlan 7
    nameif inside
    security-level 100
    bridge-group 100
interface bvi 100
    ip address 10.1.4.1 255.255.255.0
route outside 0 0 10.1.4.2 1
access-list INTERNET remark -Allows all inside hosts to access the outside
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list RETURN remark -Allows OSPF back
access-list RETURN extended permit 89 any any
access-list RETURN remark -Allows DHCP back
access-list RETURN extended permit udp any any eq 68
access-group RETURN in interface outside

```

Failover Example Configurations

This section includes the following topics:

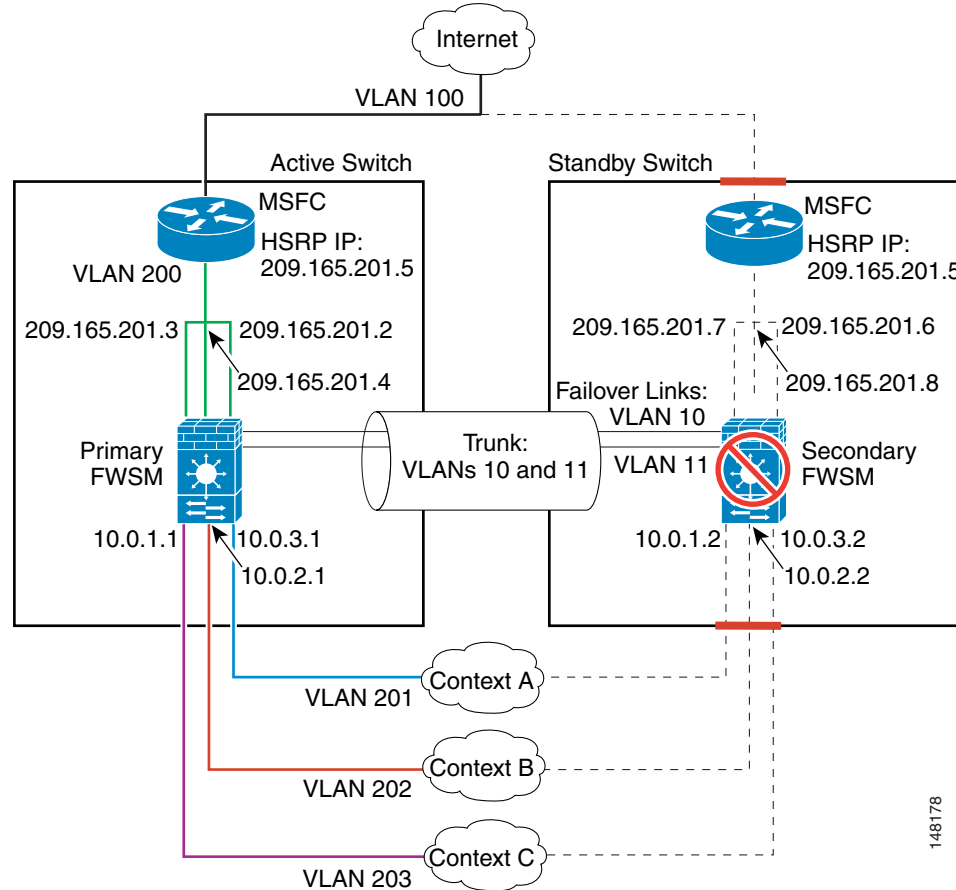
- [Example 6: Routed Mode Failover, page B-18](#)
- [Example 7: Transparent Mode Failover, page B-22](#)
- [Example 8: Active/Active Failover with Asymmetric Routing Support, page B-26](#)

Example 6: Routed Mode Failover

The following configuration shows a multiple context mode FWSM with each context in routed mode in one switch, and another FWSM in a second switch acting as a backup (see [Figure B-6](#)). 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 multiple context mode, and has the same software release.

Figure B-6 Example 6



See the following sections for the configurations for this scenario:

- [Primary FWSM Configuration \(Example 6\), page B-19](#)
- [Secondary FWSM System Configuration \(Example 6\), page B-21](#)
- [Switch Configuration \(Example 6\), page B-22](#)

Primary FWSM Configuration (Example 6)

The following sections include the configuration for the primary FWSM:

- [System Configuration \(Primary Unit—Example 6\), page B-19](#)
- [Context A Configuration \(Primary Unit—Example 6\), page B-20](#)
- [Context B Configuration \(Primary Unit—Example 6\), page B-21](#)
- [Context C Configuration \(Primary Unit—Example 6\), page B-21](#)

System Configuration (Primary Unit—Example 6)

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 Release (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
!The vlan 10 and 11 interfaces are created when you enter the failover lan interface and failover link commands.
interface vlan 10
    description LAN Failover interface
interface vlan 11
    description STATE Failover interface
interface vlan 200
interface vlan 201
interface vlan 202
interface vlan 203
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
```

Context A Configuration (Primary Unit—Example 6)

```
interface vlan 200
    nameif outside
    security-level 0
    ip address 209.165.201.2 255.255.255.224 standby 209.165.201.6
interface vlan 201
    nameif inside
    security-level 100
    ip address 10.0.3.1 255.255.255.0 standby 10.0.3.2
passwd secret1969
enable password hlandl0
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
```

Context B Configuration (Primary Unit—Example 6)

```

interface vlan 200
  nameif outside
  security-level 0
  ip address 209.165.201.4 255.255.255.224 standby 209.165.201.8
interface vlan 202
  nameif inside
  security-level 100
  ip address 10.0.2.1 255.255.255.0 standby 10.0.2.2
passwd secret1978
enable password 7samura1
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

```

Context C Configuration (Primary Unit—Example 6)

```

interface vlan 200
  nameif outside
  security-level 0
  ip address 209.165.201.3 255.255.255.224 standby 209.165.201.7
interface vlan 203
  nameif inside
  security-level 100
  ip address 10.0.1.1 255.255.255.0 standby 10.0.1.2
passwd secret0997
enable password strayd0g
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

```

Secondary FWSM System Configuration (Example 6)

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 Release line (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
```

Switch Configuration (Example 6)

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.

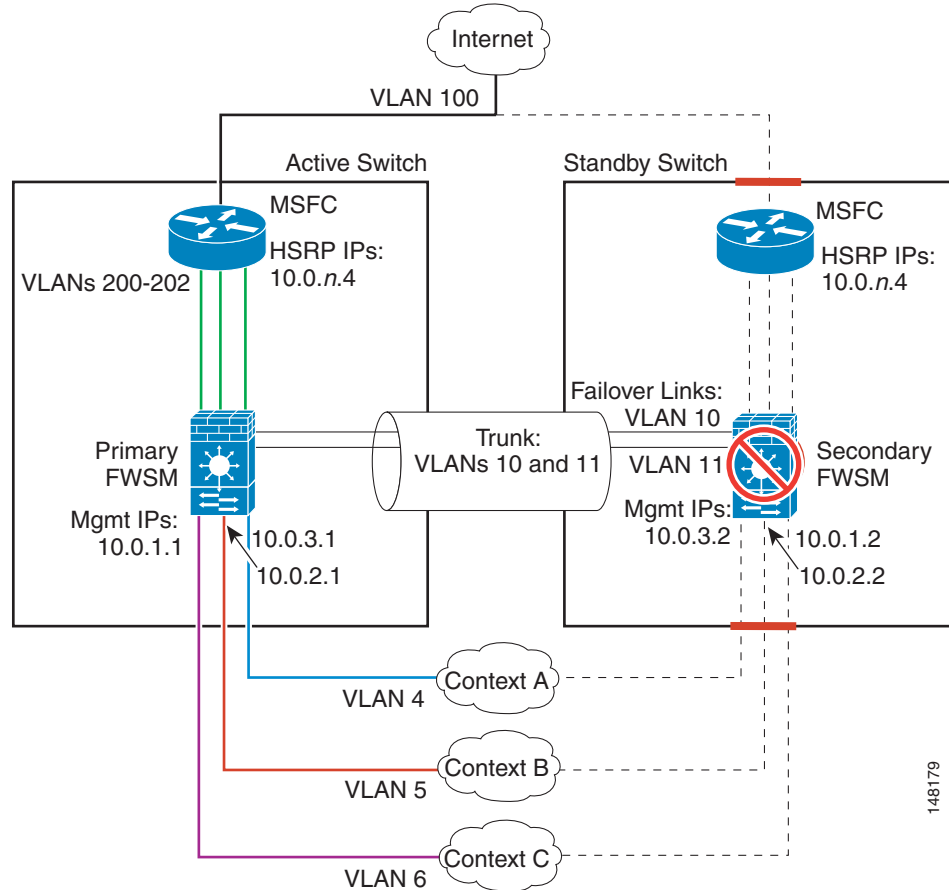
```
...
firewall module 1 vlan-group 1
firewall vlan-group 1 10,11,200-203
interface vlan 200
  ip address 209.165.201.1 255.255.255.224
  standby 200 ip 209.165.201.5
  standby 200 priority 110
  standby 200 preempt
  standby 200 timers 5 15
  standby 200 authentication Secret
  no shutdown
interface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

Example 7: Transparent Mode Failover

The following configuration shows a multiple context mode FWSM with transparent mode contexts in one switch, and another FWSM in a second switch acting as a backup (see [Figure B-6](#)). Each context (A, B, and C) monitors the inside interface and outside interface.

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

Figure B-7 Example 7



See the following sections for the configurations for this scenario:

- [Primary FWSM Configuration \(Example 7\), page B-23](#)
- [Secondary FWSM System Configuration \(Example 7\), page B-26](#)
- [Switch Configuration \(Example 7\), page B-26](#)

Primary FWSM Configuration (Example 7)

The following sections include the configuration for the primary FWSM:

- [System Configuration \(Primary Unit—Example 7\), page B-23](#)
- [Context A Configuration \(Primary Unit—Example 7\), page B-24](#)
- [Context B Configuration \(Primary Unit—Example 7\), page B-25](#)
- [Context C Configuration \(Primary Unit—Example 7\), page B-25](#)

System Configuration (Primary Unit—Example 7)

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 Release (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
interface vlan 4
interface vlan 5
interface vlan 6
!The vlan 10 and 11 interfaces are created when you enter the failover lan interface and
failover link commands.
interface vlan 10
    description LAN Failover interface
interface vlan 11
    description STATE Failover interface
interface vlan 200
interface vlan 201
interface vlan 202
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
```

Context A Configuration (Primary Unit—Example 7)

```
firewall transparent
passwd secret1969
enable password hlandl0
interface vlan 200
    nameif outside
    security-level 0
    bridge-group 56
interface vlan 4
    nameif inside
    security-level 100
    bridge-group 56
interface bvi 56
    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 remark -Allows all inside hosts to access the outside for
access-list INTERNET remark -any IP traffic
```

```

access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside

```

Context B Configuration (Primary Unit—Example 7)

```

firewall transparent
passwd secret1978
enable password 7samurai
interface vlan 201
    nameif outside
    security-level 0
    bridge-group 2
interface vlan 5
    nameif inside
    security-level 100
    bridge-group 2
interface bvi 2
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 remark -Allows all inside hosts to access the outside for
access-list INTERNET remark -any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside

```

Context C Configuration (Primary Unit—Example 7)

```

firewall transparent
passwd secret0997
enable password strayd0g
interface vlan 202
    nameif outside
    security-level 0
    bridge-group 1
interface vlan 6
    nameif inside
    security-level 100
    bridge-group 1
interface bvi 1
    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 remark -Allows all inside hosts to access the outside for
access-list INTERNET remark -any IP traffic
access-list INTERNET extended permit ip any any
access-group INTERNET in interface inside
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside

```

Secondary FWSM System Configuration (Example 7)

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

```
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
```

Switch Configuration (Example 7)

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 10.0.3.3 255.255.255.0
  standby 200 ip 10.0.1.4
  standby 200 priority 110
  standby 200 preempt
  standby 200 timers 5 15
  standby 200 authentication Secret
  no shutdown
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 shutdown
interface vlan 202
  ip address 10.0.2.3 255.255.255.0
  standby 200 ip 10.0.3.4
  standby 200 priority 110
  standby 200 preempt
  standby 200 timers 5 15
  standby 200 authentication Secret
  no shutdown
interface range gigabitethernet 2/1-3
  channel-group 2 mode on
  switchport trunk encapsulation dot1q
  no shutdown
...
```

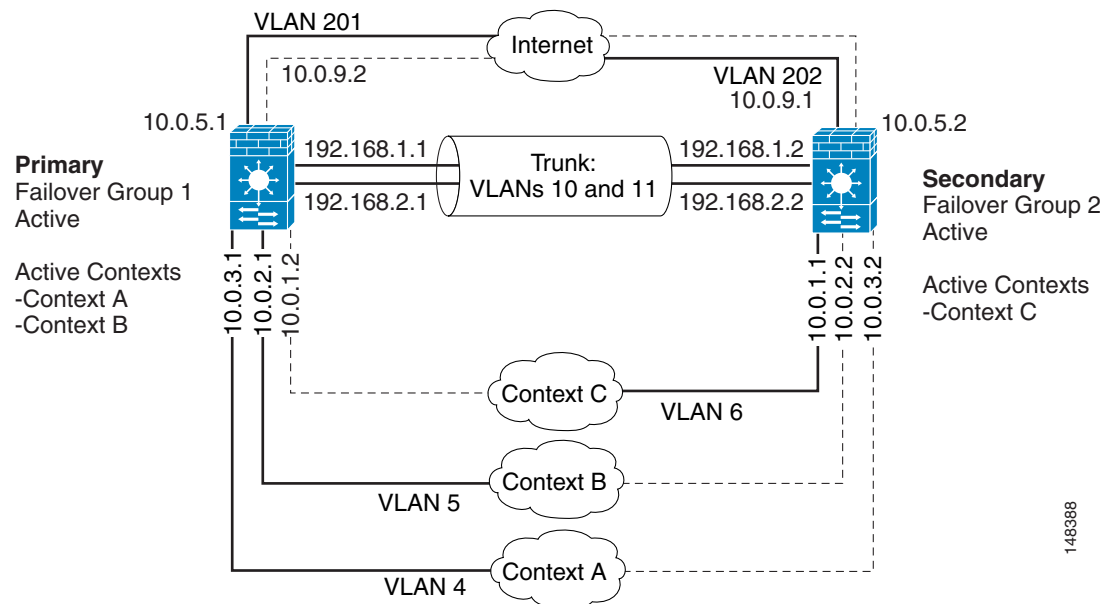
Example 8: Active/Active Failover with Asymmetric Routing Support

The following example shows how to configure Active/Active failover. In this example there are three contexts: Context A (the admin context), Context B, and Context C.

- The failover groups are configured with the **preempt** command.
- The admin context only has one interface.

Figure B-8 shows the network diagram for the example.

Figure B-8 Active/Active Failover Configuration



148388

Prerequisites

Both units must be in multiple context mode. Use the **mode multiple** command to switch the primary and secondary FWSMs to multiple context mode. You must enter the **mode multiple** command on both the primary and secondary unit to change modes; the **mode multiple** command is not replicated to the secondary unit even in existing Active/Standby failover configurations.

Both FWSMs must be licensed for the same number of security contexts.

Primary FWSM Configuration (Example 8)

The following sections include the configuration for the primary FWSM:

- [System Context Configuration \(Primary FWSM—Example 8\)](#), page B-27
- [Context A Configuration \(Primary FWSM—Example 8\)](#), page B-28
- [Context B Configuration \(Primary FWSM—Example 8\)](#), page B-29
- [Context C Configuration \(Primary FWSM—Example 8\)](#), page B-29

System Context Configuration (Primary FWSM—Example 8)

The failover groups and the failover and Stateful Failover VLANs are configured in the system context.

```
hostname cisco-primary
enable password farscape
password crichton
interface vlan 4
interface vlan 5
interface vlan 6
```

```

!The vlan 10 and 11 interfaces are created when you enter the failover lan interface and
failover link commands.
interface vlan 10
    description LAN Failover interface
interface vlan 11
    description STATE Failover interface
interface vlan 201
interface vlan 202
failover
failover lan unit primary
failover lan interface faillink vlan 10
failover key MySecretKey
failover link statelink vlan 11
failover interface ip faillink 192.168.1.1 255.255.255.0 standby 192.168.1.2
failover interface ip statelink 192.168.2.1 255.255.255.0 standby 192.168.2.2
failover group 1
    preempt
    replication http
    interface-policy 50%
failover group 2
    secondary
    preempt
    replication http
    interface-policy 50%
admin-context contexta
context contexta
    description administrative context
    allocate-interface vlan4
    config-url disk://contexta.cfg
    join-failover-group 1
context contextb
    allocate-interface vlan201
    allocate-interface vlan5
    config-url ftp://admin:passw0rd@10.0.3.16/contextb.cfg
    join-failover-group 1
context contextc
    allocate-interface vlan202
    allocate-interface vlan6
    config-url ftp://admin:passw0rd@10.0.3.16/contextc.cfg
    join-failover-group 2

```

Context A Configuration (Primary FWSM—Example 8)

Context A is the admin context. In this example the admin context contains only one interface, the inside interface, for administrative access. Because the context contains only one interface, you cannot use Telnet to access the FWSM through the interface. Telnet access is not permitted to the lowest security level interface in a context, and because Context A has only one interface, it is the lowest level interface by default. Instead, you must define an SSH connection to manage the FWSM through this interface.

```

interface vlan 4
    nameif mgmt
    security-level 5
    ip address 10.0.3.1 255.255.255.0 standby 10.0.3.2
passwd secret1969
enable password hlandl0
monitor-interface inside
crypto key generate rsa modulus 1024
ssh 10.0.3.0 255.255.255.0 inside
ssh version 2

```

Context B Configuration (Primary FWSM—Example 8)

```

interface vlan 201
  nameif outside
  security-level 0
  ip address 10.0.5.1 255.255.255.0 standby 10.0.5.2
  asr-group 1
interface vlan 5
  nameif inside
  security-level 100
  ip address 10.0.2.1 255.255.255.0 standby 10.0.2.2
passwd secret1978
enable password 7samural
monitor-interface inside
monitor-interface outside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 10.0.5.1 netmask 255.255.255.0
! This context uses dynamic PAT for inside users that access the outside
route outside 0 0 10.0.5.5 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

```

Context C Configuration (Primary FWSM—Example 8)

```

interface vlan 202
  nameif outside
  security-level 0
  ip address 10.0.9.1 255.255.255.224 standby 10.0.9.2
  asr-group 1
interface vlan 6
  nameif inside
  security-level 100
  ip address 10.0.1.1 255.255.255.0 standby 10.0.1.2
passwd secret0997
enable password strayd0g
monitor-interface inside
monitor-interface outside
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 10.0.9.1 netmask 255.255.255.0
! This context uses dynamic PAT for inside users that access the outside
route outside 0 0 10.0.9.5 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

```

The Secondary FWSM Configuration (Example 8)

You only need to configure the secondary FWSM to recognize the failover link. The secondary FWSM obtains the context configurations from the primary FWSM upon booting or when **failover** is first enabled. The **preempt** commands in the failover group configurations cause the failover groups to become active on their designated unit after the configurations have been synchronized and the preempt delay has passed.

Note that you must configure the **failover key** command on the secondary FWSM so that it can receive the configuration from the primary FWSM.

```

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

```

When you enable failover with the failover command, the secondary FWSM obtains the configuration from the primary FWSM.

Switch Configuration (Example 8)

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 4-6,10,11,201,202
interface vlan 201
    ip address 10.0.5.3 255.255.255.0
    standby 200 ip 10.0.5.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface vlan 202
    ip address 10.0.9.3 255.255.255.0
    standby 200 ip 10.0.9.4
    standby 200 priority 110
    standby 200 preempt
    standby 200 timers 5 15
    standby 200 authentication Secret
    no shutdown
interface range gigabitethernet 2/1-3
    channel-group 2 mode on
    switchport trunk encapsulation dot1q
    no shutdown
...

```