APPENDIX A

Sample Configurations

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

Example 1: Multiple Mode Firewall With Outside Access

This configuration creates three security contexts plus the admin context, each with an inside and an outside interface. Both interfaces are configured as redundant interfaces.

The Customer C context includes a DMZ interface where a Websense server for HTTP filtering resides on the service provider premises (see Figure A-1).

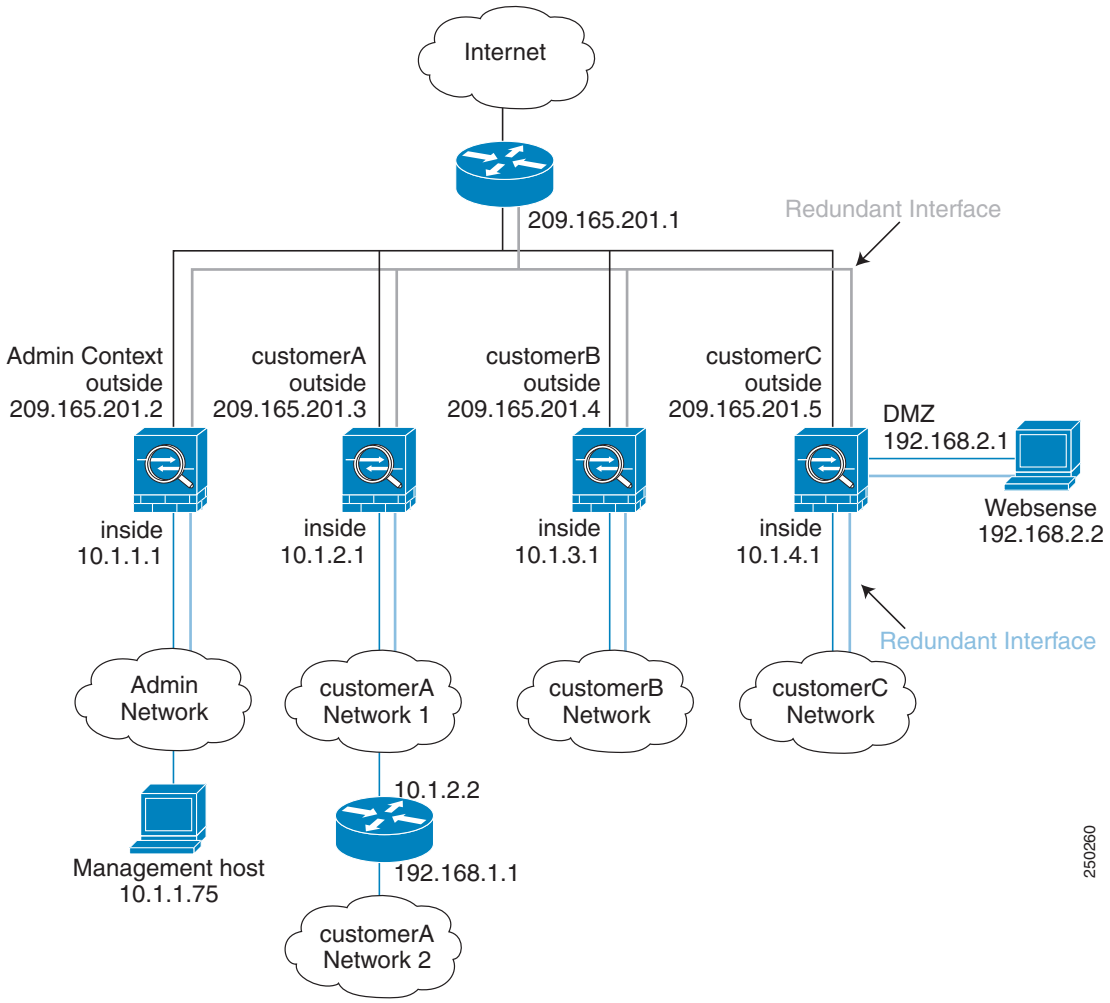
Inside hosts can access the Internet through the outside using dynamic NAT or PAT, but no outside hosts can access the inside.

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

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

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

Figure A-1 Example 1



See the following sections for the configurations for this scenario:

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

System Configuration for Example 1

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. Enter the **show mode** command to view the current mode.

```
hostname Farscape
password passw0rd
enable password chr1cht0n
mac-address auto
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
admin-context admin
interface gigabitethernet 0/0
   no shutdown
interface gigabitethernet 0/1
   no shutdown
interface gigabitethernet 0/2
   no shutdown
interface gigabitethernet 0/3
   no shutdown
interface redundant 1
   member-interface gigabitethernet 0/0
   member-interface gigabitethernet 0/1
interface redundant 2
   member-interface gigabitethernet 0/2
   member-interface gigabitethernet 0/3
interface redundant 1.3
   vlan 3
   no shutdown
interface redundant 2.4
   vlan 4
   no shutdown
interface redundant 2.5
   vlan 5
   no shutdown
interface redundant 2.6
   vlan 6
   no shutdown
interface redundant 2.7
   vlan 7
   no shutdown
interface redundant 2.8
   vlan 8
   no shutdown
class gold
   limit-resource rate conns 2000
   limit-resource conns 20000
class silver
   limit-resource rate conns 1000
   limit-resource conns 10000
class bronze
   limit-resource rate conns 500
   limit-resource conns 5000
context admin
   allocate-interface redundant1.3 int1
   allocate-interface redundant2.4 int2
   config-url disk0://admin.cfg
   member default
context customerA
   description This is the context for customer A
   allocate-interface redundant1.3 int1
   allocate-interface redundant2.5 int2
```

```
   config-url disk0://contexta.cfg
   member gold
context customerB
   description This is the context for customer B
   allocate-interface redundant1.3 int1
   allocate-interface redundant2.6 int2
   config-url disk0://contextb.cfg
   member silver
context customerC
   description This is the context for customer C
   allocate-interface redundant1.3 int1
   allocate-interface redundant2.7-redundant2.8 int2-int3
   config-url disk0://contextc.cfg
   member bronze
```

Admin Context Configuration for Example 1

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

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.

```
hostname Admin
domain example.com
interface int1
   nameif outside
   security-level 0
   ip address 209.165.201.2 255.255.255.224
   no shutdown
interface int2
   nameif inside
   security-level 100
   ip address 10.1.1.1 255.255.255.0
   no shutdown
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, so
! 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
```

Customer A Context Configuration for Example 1

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface int1
   nameif outside
   security-level 0
   ip address 209.165.201.3 255.255.255.224
   no shutdown
interface int2
   nameif inside
```

```
   security-level 100
   ip address 10.1.2.1 255.255.255.0
   no shutdown
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
```

Customer B Context Configuration for Example 1

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface int1
   nameif outside
   security-level 0
   ip address 209.165.201.4 255.255.255.224
   no shutdown
interface int2
   nameif inside
   security-level 100
   ip address 10.1.3.1 255.255.255.0
   no shutdown
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 for Example 1

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface int1
   nameif outside
   security-level 0
   ip address 209.165.201.5 255.255.255.224
   no shutdown
interface int2
   nameif inside
   security-level 100
   ip address 10.1.4.1 255.255.255.0
   no shutdown
interface int3
   nameif dmz
   security-level 50
```

```
   ip address 192.168.2.1 255.255.255.0
   no shutdown
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, the ASA 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 MANAGE remark Allows the management host to use pcAnywhere on the 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
```

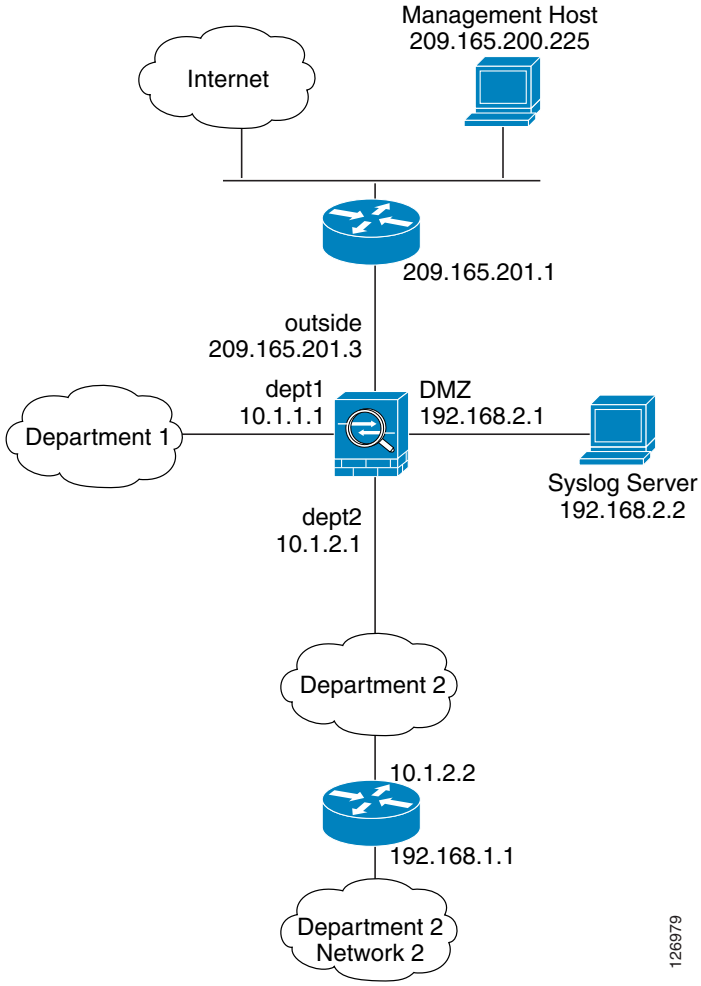
Example 2: Single Mode Firewall Using Same Security Level

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 access lists. The DMZ interface hosts a syslog server. The management host on the outside needs access to the Syslog server and the ASA. The ASA uses RIP on the inside interfaces to learn routes. The ASA does not advertise routes with RIP; the upstream router needs to use static routes for ASA traffic (see Figure A-2).

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

Threat detection is enabled.

Figure A-2 Example 2




```
passwd g00fba11
enable password gen1u$
hostname Buster
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
interface gigabitethernet 0/0
   nameif outside
   security-level 0
   ip address 209.165.201.3 255.255.255.224
   no shutdown
interface gigabitethernet 0/1
   nameif dept2
   security-level 100
   ip address 10.1.2.1 255.255.255.0
   mac-address 000C.F142.4CDE standby 000C.F142.4CDF
   no shutdown
   rip authentication mode md5
   rip authentication key scorpius key_id 1
interface gigabitethernet 0/2
   nameif dept1
   security-level 100
   ip address 10.1.1.1 255.255.255.0
   no shutdown
```

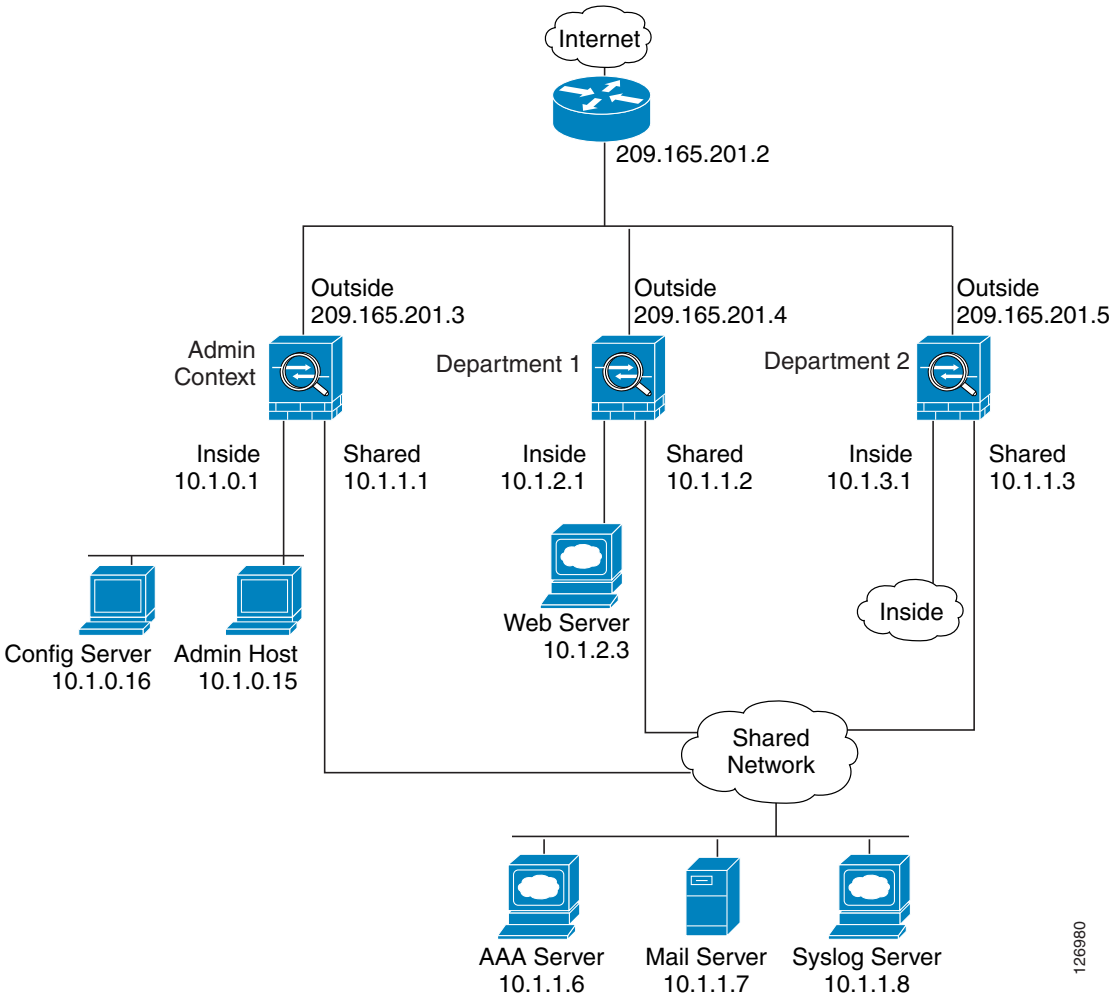
```
interface gigabitethernet 0/3
   nameif dmz
   security-level 50
   ip address 192.168.2.1 255.255.255.0
   no shutdown
same-security-traffic permit inter-interface
route outside 0 0 209.165.201.1 1
nat (dept1) 1 10.1.1.0 255.255.255.0
nat (dept2) 1 10.1.2.0 255.255.255.0
! The dept1 and dept2 networks 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 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 ssh
access-group MANAGE in interface outside
! Advertises the ASA IP address as the default gateway for the downstream
! router. The ASA does not advertise a default route to the upstream
! router. Listens for RIP updates from the downstream router. The ASA does
! not listen for RIP updates from the upstream router because a default route to the
! upstream router is all that is required.
router rip
   network 10.0.0.0
   default information originate
   version 2
ssh 209.165.200.225 255.255.255.255 outside
logging trap 5
! System messages are sent to the syslog server on the DMZ network
logging host dmz 192.168.2.2
logging enable
! Enable basic threat detection:
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
! Enables scanning threat detection and automatically shun attackers,
! except for hosts on the 10.1.1.0 network:
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
! Enable statistics for access-lists:
threat-detection statistics access-list
```

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 interface (see Figure A-3).

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

Figure A-3 Example 3



See the following sections for the configurations for this scenario:

- System Configuration for Example 3, page A-9
- Admin Context Configuration for Example 3, page A-10
- Department 1 Context Configuration for Example 3, page A-11
- Department 2 Context Configuration for Example 3, page A-12

System Configuration for Example 3

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. Enter the **show mode** command to view the current mode.

```
hostname Ubik
password pkd55
enable password deckard69
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
```

```
mac-address auto
admin-context admin
interface gigabitethernet 0/0
   no shutdown
interface gigabitethernet 0/0.200
! This is the shared outside interface
   vlan 200
   no shutdown
interface gigabitethernet 0/1
   no shutdown
interface gigabitethernet 0/1.201
! This is the inside interface for admin
   vlan 201
   no shutdown
interface gigabitethernet 0/1.202
! This is the inside interface for department 1
   vlan 202
   no shutdown
interface gigabitethernet 0/1.203
! This is the inside interface for department 2
   vlan 203
   no shutdown
interface gigabitethernet 0/1.300
! This is the shared inside interface
   vlan 300
   no shutdown
context admin
   allocate-interface gigabitethernet 0/0.200
   allocate-interface gigabitethernet 0/1.201
   allocate-interface gigabitethernet 0/1.300
   config-url disk0://admin.cfg
context department1
   allocate-interface gigabitethernet 0/0.200
   allocate-interface gigabitethernet 0/1.202
   allocate-interface gigabitethernet 0/1.300
   config-url ftp://admin:passw0rd@10.1.0.16/dept1.cfg
context department2
   allocate-interface gigabitethernet 0/0.200
   allocate-interface gigabitethernet 0/1.203
   allocate-interface gigabitethernet 0/1.300
   config-url ftp://admin:passw0rd@10.1.0.16/dept2.cfg
```

Admin Context Configuration for Example 3

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
hostname Admin
interface gigabitethernet 0/0.200
   nameif outside
   security-level 0
   ip address 209.165.201.3 255.255.255.224
   no shutdown
interface gigabitethernet 0/0.201
   nameif inside
   security-level 100
   ip address 10.1.0.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/0.300
   nameif shared
   security-level 50
```

```
   ip address 10.1.1.1 255.255.255.0
   no shutdown
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 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
aaa authorization command AAA-SERVER LOCAL
aaa accounting command 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 enable
```

Department 1 Context Configuration for Example 3

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface gigabitethernet 0/0.200
   nameif outside
   security-level 0
   ip address 209.165.201.4 255.255.255.224
   no shutdown
interface gigabitethernet 0/0.202
   nameif inside
   security-level 100
   ip address 10.1.2.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/0.300
   nameif shared
   security-level 50
   ip address 10.1.1.2 255.255.255.0
   no shutdown
passwd cugel
enable password rhialto
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 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 WEBSERVER access list must authenticate with the AAA server
aaa authentication match WEBSERVER 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 enable
```

Department 2 Context Configuration for Example 3

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface gigabitethernet 0/0.200
   nameif outside
   security-level 0
   ip address 209.165.201.5 255.255.255.224
   no shutdown
interface gigabitethernet 0/0.203
   nameif inside
   security-level 100
   ip address 10.1.3.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/0.300
   nameif shared
   security-level 50
   ip address 10.1.1.3 255.255.255.0
   no shutdown
passwd maz1r1an
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 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 enable
```

Example 4: Multiple Mode, Transparent Firewall 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 A-4).

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

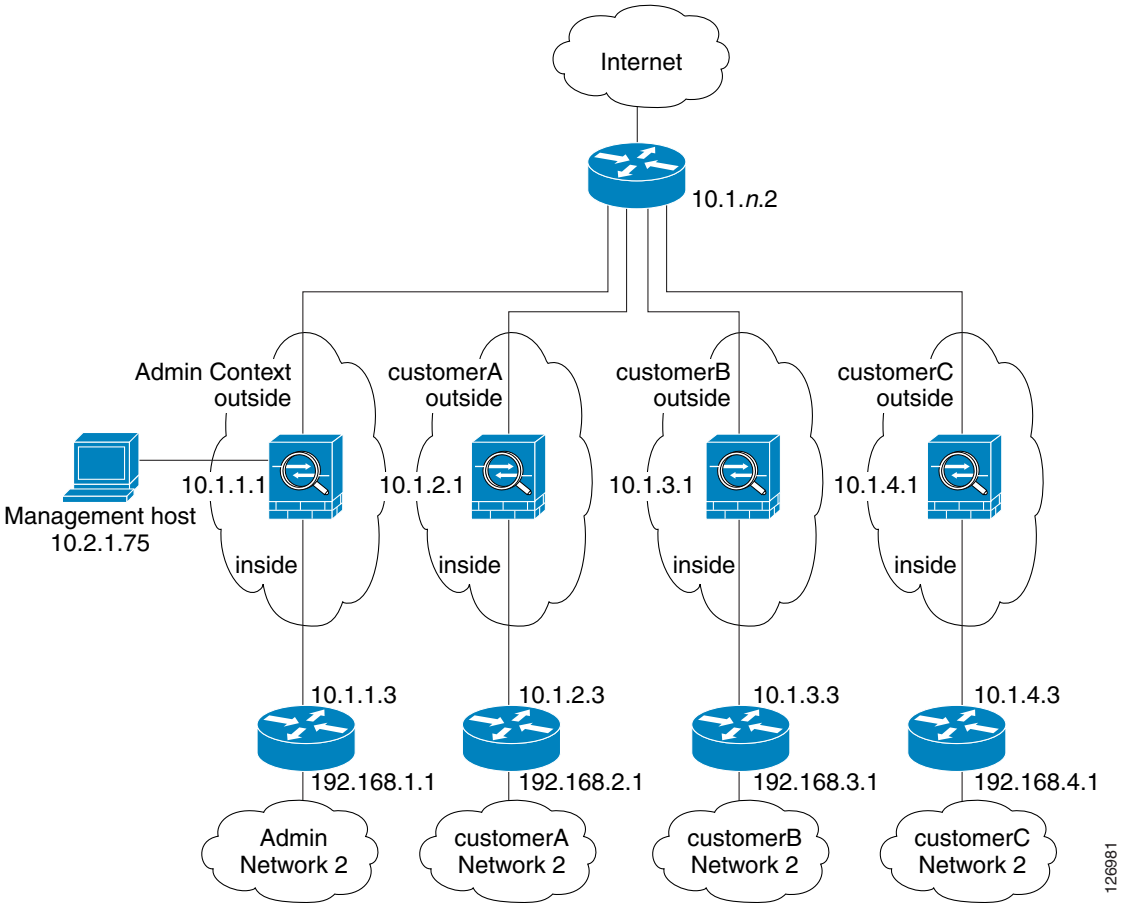
An out-of-band management host is connected to the Management 0/0 interface.

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

Connection limit settings for each context, except admin, limit the number of connections to guard against DoS attacks.

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

Figure A-4 Example 4



See the following sections for the configurations for this scenario:

- System Configuration for Example 4, page A-14
- Admin Context Configuration for Example 4, page A-15
- Customer A Context Configuration for Example 4, page A-16
- Customer B Context Configuration for Example 4, page A-16
- Customer C Context Configuration for Example 4, page A-17

System Configuration for Example 4

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. Enter the **show mode** command to view the current mode.

```
firewall transparent
hostname Farscape
password passw0rd
enable password chr1cht0n
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
mac-address auto
admin-context admin
```

```
interface gigabitethernet 0/0
   no shutdown
interface gigabitethernet 0/0.150
   vlan 150
   no shutdown
interface gigabitethernet 0/0.151
   vlan 151
   no shutdown
interface gigabitethernet 0/0.152
   vlan 152
   no shutdown
interface gigabitethernet 0/0.153
   vlan 153
   no shutdown
interface gigabitethernet 0/1
   shutdown
interface gigabitethernet 0/1.4
   vlan 4
   no shutdown
interface gigabitethernet 0/1.5
   vlan 5
   no shutdown
interface gigabitethernet 0/1.6
   vlan 6
   no shutdown
interface gigabitethernet 0/1.7
   vlan 7
   no shutdown
interface management 0/0
   no shutdown
context admin
   allocate-interface gigabitethernet 0/0.150
   allocate-interface gigabitethernet 0/1.4
   allocate-interface management 0/0
   config-url disk0://admin.cfg
context customerA
   description This is the context for customer A
   allocate-interface gigabitethernet 0/0.151
   allocate-interface gigabitethernet 0/1.5
   config-url disk0://contexta.cfg
context customerB
   description This is the context for customer B
   allocate-interface gigabitethernet 0/0.152
   allocate-interface gigabitethernet 0/1.6
   config-url disk0://contextb.cfg
context customerC
   description This is the context for customer C
   allocate-interface gigabitethernet 0/0.153
   allocate-interface gigabitethernet 0/1.7
   config-url disk0://contextc.cfg
```

Admin Context Configuration for Example 4

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

The host at 10.2.1.75 can access the context using SSH, which requires a key pair to be generated using the **crypto key generate** command.

```
hostname Admin
domain example.com
```

```
interface gigabitethernet 0/0.150
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1.4
   nameif inside
   security-level 100
   no shutdown
interface management 0/0
   nameif manage
   security-level 50
! Unlike other transparent interfaces, the management interface
! requires an IP address:
   ip address 10.2.1.1 255.255.255.0
   no shutdown
passwd secret1969
enable password h1andl0
ip address 10.1.1.1 255.255.255.0
route outside 0 0 10.1.1.2 1
ssh 10.2.1.75 255.255.255.255 manage
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

Customer A Context Configuration for Example 4

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface gigabitethernet 0/0.151
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1.5
   nameif inside
   security-level 100
   no shutdown
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 OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

Customer B Context Configuration for Example 4

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface gigabitethernet 0/0.152
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1.6
   nameif inside
   security-level 100
   no shutdown
```

```
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 OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
! The following commands add connection limits to the global policy.
class-map conn_limits
 match any
policy-map global_policy
   class conn_limits
      set connection conn-max 5000 embryonic-conn-max 2000
      set connection timeout tcp 2:0:0 reset half-close 0:5:0 embryonic 0:0:20 dcd 20 3
service-policy global_policy global
```

Customer C Context Configuration for Example 4

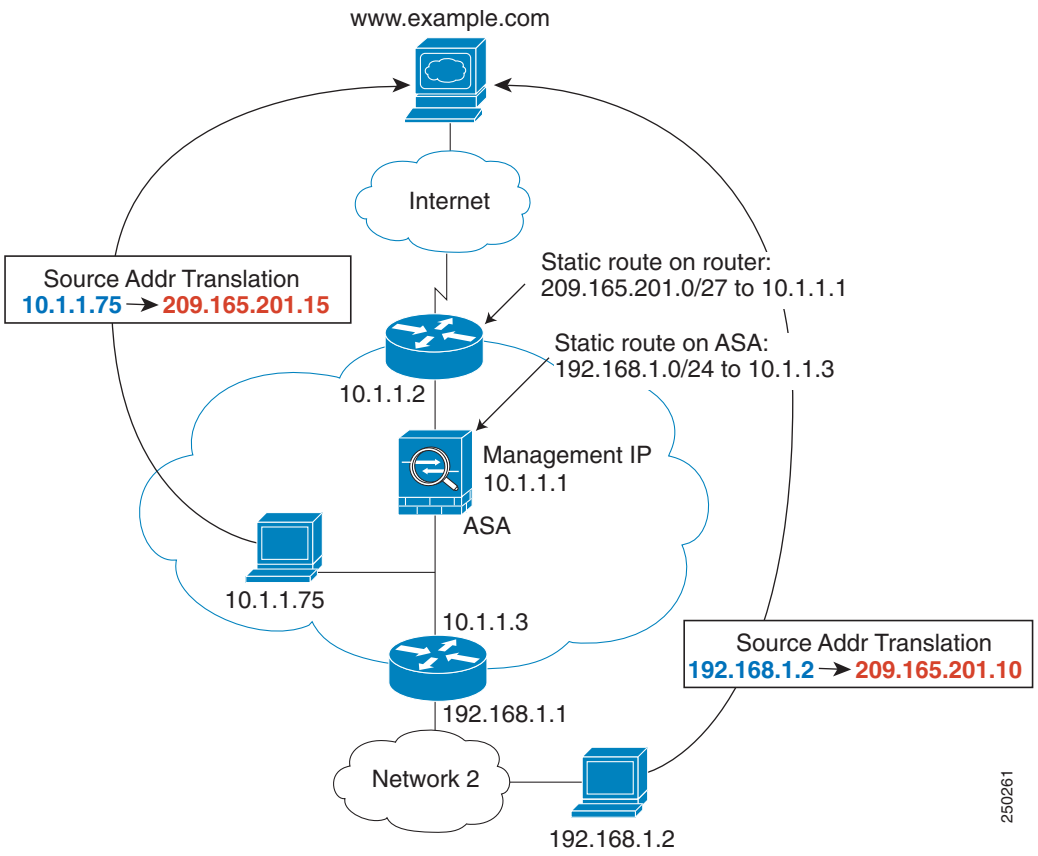
To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
interface gigabitethernet 0/0.153
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1.7
   nameif inside
   security-level 100
   no shutdown
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 OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
! The following commands add connection limits to the global policy.
class-map conn_limits
 match any
policy-map global_policy
   class conn_limits
      set connection conn-max 5000 embryonic-conn-max 2000
      set connection timeout tcp 2:0:0 reset half-close 0:5:0 embryonic 0:0:20 dcd 20 3
service-policy global_policy global
```

Example 5: Single Mode, Transparent Firewall with NAT

This configuration shows how to configure NAT in transparent mode (see Figure A-5).

Figure A-5 Example 5



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

```
firewall transparent
hostname Farscape
password passw0rd
enable password chr1cht0n
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
hostname Moya
domain example.com
interface gigabitethernet 0/0
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1
   nameif inside
   security-level 100
   no shutdown
ip address 10.1.1.1 255.255.255.0
route outside 0 0 10.1.1.2 1
! The following route is required when you perform NAT
```

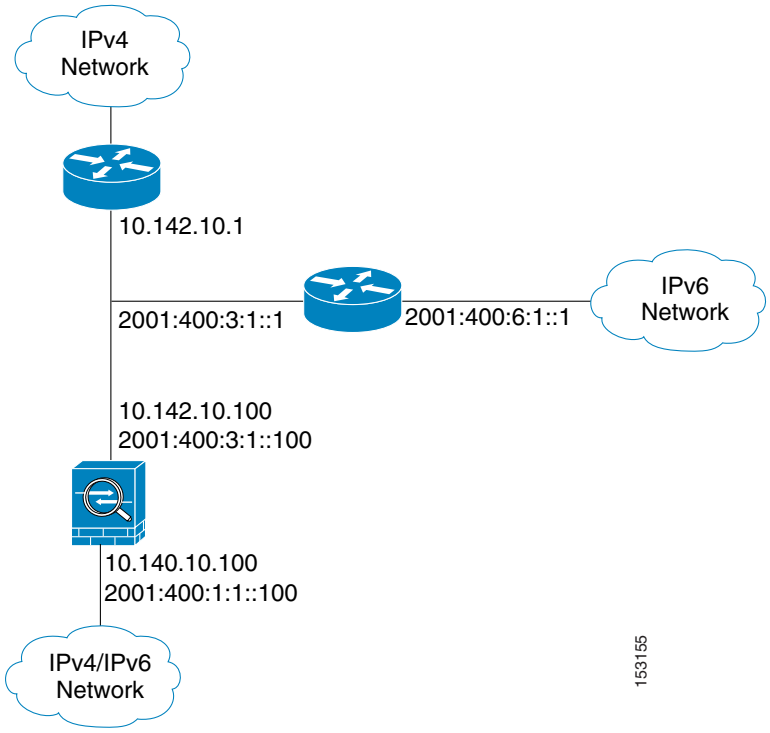
```
! on non-directly-connected networks:
route inside 192.168.1.0 255.255.255.0 10.1.1.3 1
ssh 10.1.1.75 255.255.255.255 inside
nat (inside) 1 10.1.1.0 255.255.255.0
nat (inside) 1 198.168.1.0 255.255.255.0
global (outside) 1 209.165.201.1-209.165.201.15
```

Example 6: IPv6 Configuration

This sample configuration shows several features of IPv6 support on the ASA:

- 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.
- The enforcement of Modified-EUI64 format interface identifiers in the IPv6 addresses of hosts on the inside interface.
- The outside interface suppresses router advertisement messages.
- An IPv6 static route.

Figure A-6 IPv6 Dual Stack Configuration



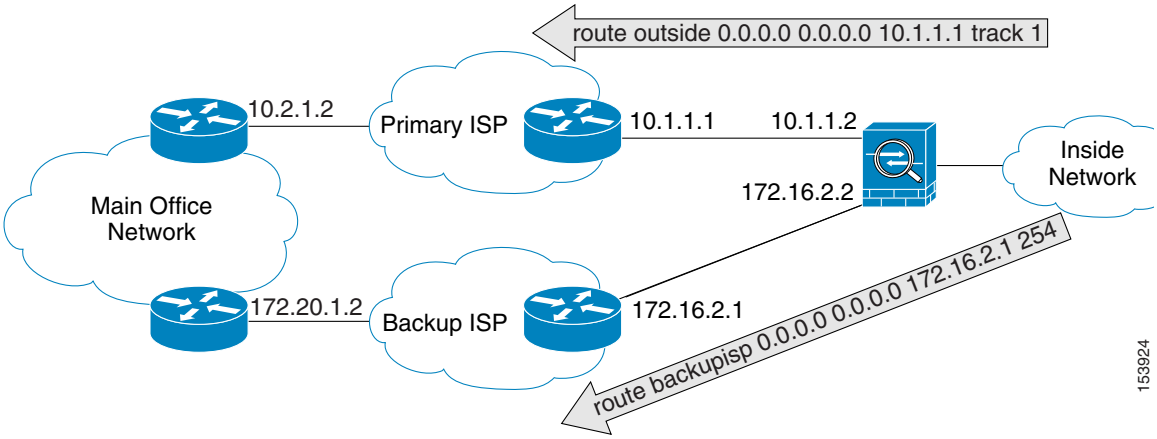

```
enable password myenablepassword
passwd mypassword
hostname coyupix
asdm image flash:/asdm.bin
boot system flash:/image.bin
```

```
interface gigabitethernet0/0
   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
   ospf mtu-ignore auto
   no shutdown
interface gigabitethernet0/1
   nameif inside
   security-level 100
   ip address 10.140.10.100 255.255.255.0
   ipv6 address 2001:400:1:1::100/64
   ospf mtu-ignore auto
   no shutdown
access-list allow extended permit icmp any any
ssh 10.140.10.75 255.255.255.255 inside
logging enable
logging buffered debugging
ipv6 enforce-eui64 inside
ipv6 route outside 2001:400:6:1::/64 2001:400:3:1::1
ipv6 route outside ::/0 2001:400:3:1::1
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 allow in interface outside
access-group outacl in interface outside
route outside 0.0.0.0 0.0.0.0 16.142.10.1 1
```

Example 7: Dual ISP Support Using Static Route Tracking

This configuration shows a remote office using static route tracking to use a backup ISP route if the primary ISP route fails. The ASA in the remote office uses ICMP echo requests to monitor the availability of the main office gateway. If that gateway becomes unavailable through the default route, the default route is removed from the routing table and the floating route to the backup ISP is used in its place.

Figure A-7 Dual ISP Support

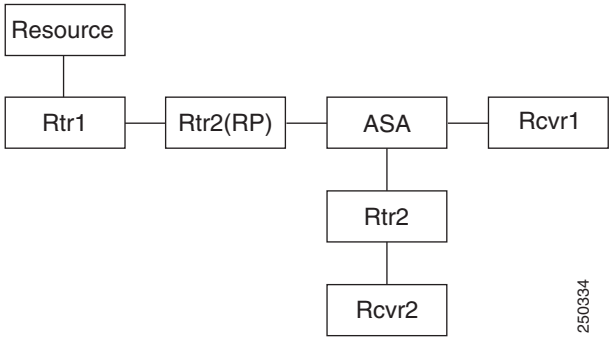


```
passwd password1
enable password password2
hostname myfirewall
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
!
interface gigabitethernet 0/0
   nameif outside
   security-level 0
   ip address 10.1.1.2 255.255.255.0
   no shutdown
!
interface gigabitethernet 0/1
   description backup isp link
   nameif backupisp
   security-level 100
   ip address 172.16.2.2 255.255.255.0
   no shutdown
!
sla monitor 123
   type echo protocol ipIcmpEcho 10.2.1.2 interface outside
   num-packets 3
   timeout 1000
   frequency 3
sla monitor schedule 123 life forever start-time now
!
track 1 rtr 123 reachability
!
route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
! The above route is used while the tracked object, router 10.2.1.2
! is available. It is removed when the router becomes unavailable.
!
route backupisp 0.0.0.0 0.0.0.0 172.16.2.1 254
! The above route is a floating static route that is added to the
! routing table when the tracked route is removed.
```

Example 8: Multicast Routing

This configuration shows a source that is sending out multicast traffic with two listeners that are watching for messages. A network lies between the source and the receivers, and all devices need to build up the PIM tree properly for the traffic to flow. This includes the ASA 5505 adaptive security appliance, and all IOS routers.

Figure A-8 Multicast Routing Configuration



Note Multicast routing only works in single routed mode.

- For PIM Sparse Mode, page A-22
- For PIM bidir Mode, page A-23

For PIM Sparse Mode

This configuration enables multicast routing for PIM Sparse Mode.

```
hostname asa
multicast-routing

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.1.2.1 255.255.255.0

interface GigabitEthernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.3.1 255.255.255.0
 igmp join-group 227.1.2.3

! Specify the RP
pim rp-address 10.1.1.2

! Specify ACL configuration on the interfaces
access-list mcast permit pim any any
access-list mcast permit igmp any any
access-list mcast permit ospf any any
access-list mcast permit icmp any any
access-list mcast permit tcp any any eq 80
access-list mcast permit udp any 224.0.0.0 240.0.0.0

no failover
access-group mcast in interface outside
access-group mcast in interface inside
```

```
access-group mcast in interface dmz

!   Configures unicast routing
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.2.0 255.255.255.0 area 0
 network 10.1.3.0 255.255.255.0 area 0
 log-adj-changes
!
```

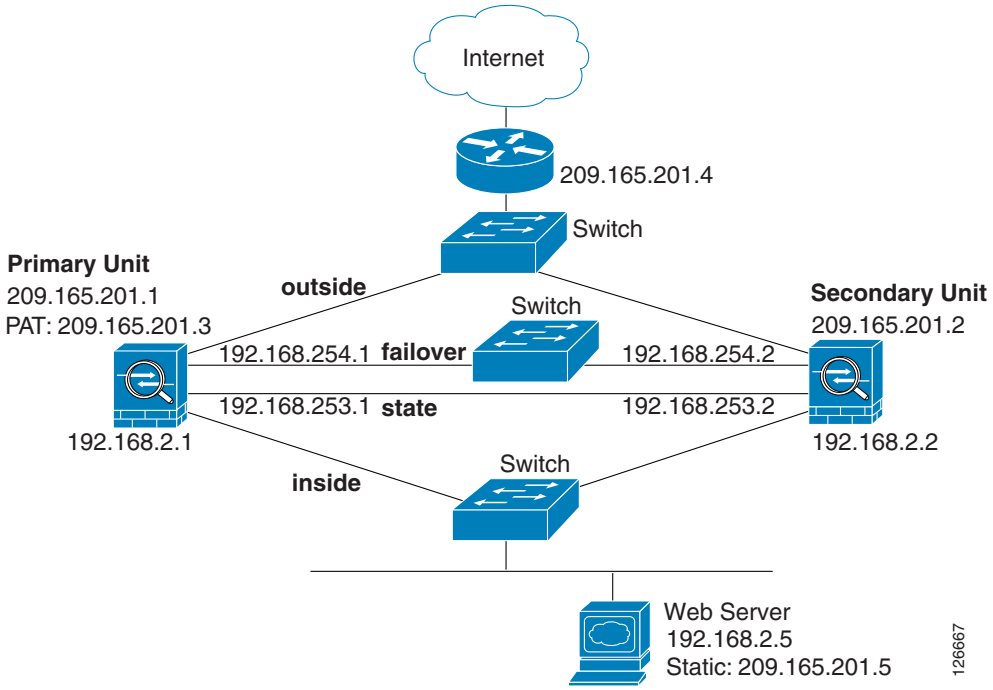
For PIM bidir Mode

```
hostname asa
multicast-routing
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.1.2.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.3.1 255.255.255.0
 igmp join-group 227.1.2.3

! Specify the RP
pim rp-address 10.1.1.2 bidir


! Specify ACL configuration on the interfaces
access-list mcast permit pim any any
access-list mcast permit igmp any any
access-list mcast permit ospf any any
access-list mcast permit icmp any any
access-list mcast permit tcp any any eq 80
access-list mcast permit udp any 224.0.0.0 240.0.0.0

no failover
access-group mcast in interface outside
access-group mcast in interface inside
access-group mcast in interface dmz

!   Configures unicast routing
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.2.0 255.255.255.0 area 0
 network 10.1.3.0 255.255.255.0 area 0
 log-adj-changes
```

Example 9: LAN-Based Active/Standby Failover (Routed Mode)

Figure A-9 shows the network diagram for a failover configuration using an Ethernet failover link. The units are configured to detect unit failures and to fail over in under a second (see the **failover polltime unit** command in the primary unit configuration).

Figure A-9 LAN-Based Failover Configuration



See the following sections for primary or secondary unit configuration scenarios:

- Primary Unit Configuration for Example 9, page A-24
- Secondary Unit Configuration for Example 9, page A-25

Primary Unit Configuration for Example 9

```
hostname pixfirewall
enable password myenablepassword
password mypassword
interface gigabitethernet0/0
   nameif outside
   ip address 209.165.201.1 255.255.255.224 standby 209.165.201.2
   no shutdown
interface gigabitethernet0/1
   nameif inside
   ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
   no shutdown
interface gigabitethernet0/2
   description LAN Failover Interface
   no shutdown
interface gigabitethernet0/3
   description STATE Failover Interface
```

```
telnet 192.168.2.45 255.255.255.255 inside
access-list acl_out permit tcp any host 209.165.201.5 eq 80
failover
failover lan unit primary
failover lan interface failover gigabitethernet0/2
failover lan enable
! The failover lan enable command is required on the PIX ASA only.
failover polltime unit msec 200 holdtime msec 800
failover key key1
failover link state gigabitethernet0/3
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
failover interface ip state 192.168.253.1 255.255.255.0 standby 192.168.253.2
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

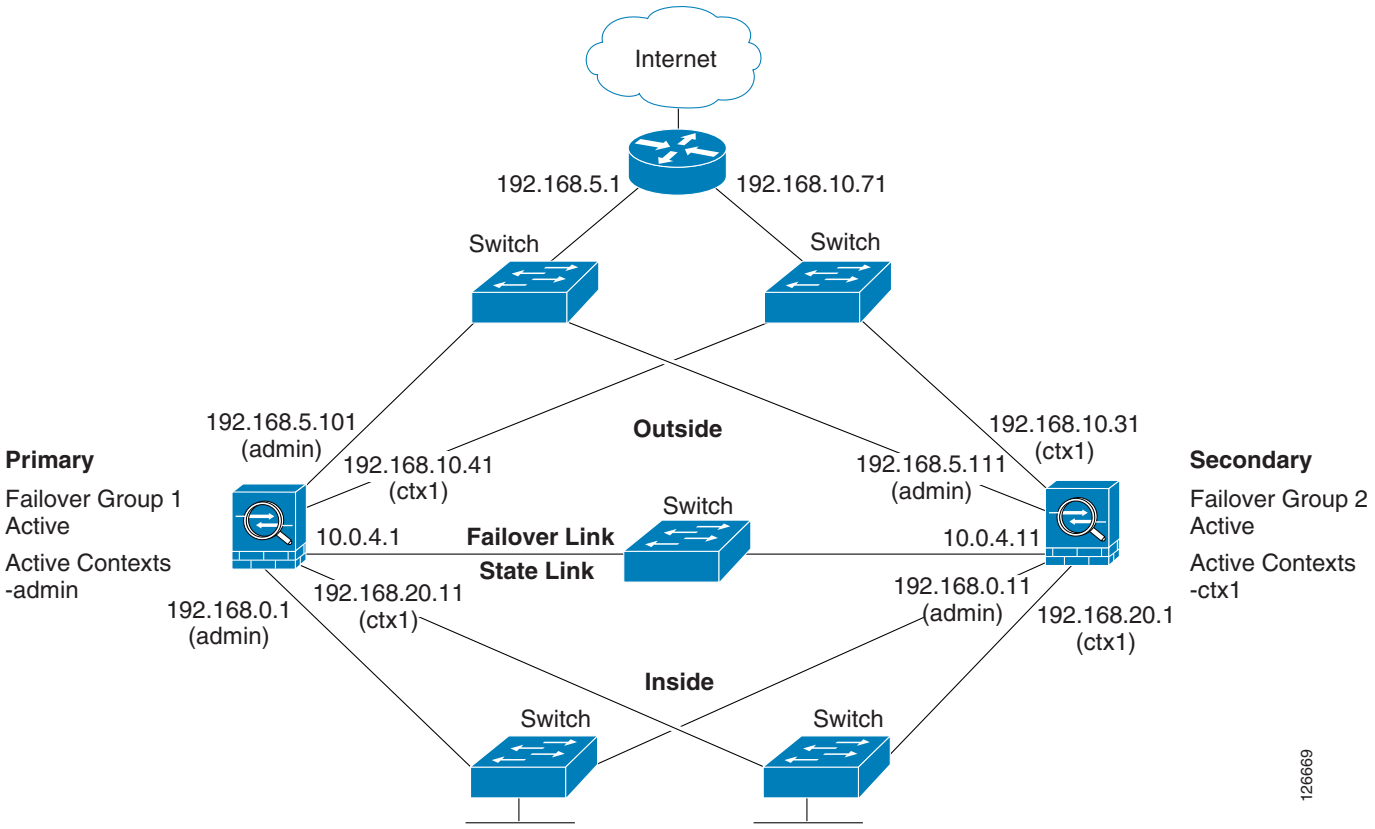
Secondary Unit Configuration for Example 9

```
failover
failover lan unit secondary
failover lan interface failover gigabitethernet0/2
failover lan enable
failover key key1
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
```

Example 10: LAN-Based Active/Active Failover (Routed Mode)

The following example shows how to configure Active/Active failover. In this example there are 2 user contexts, named admin and ctx1. Figure A-10 shows the network diagram for the example.

Figure A-10 Active/Active Failover Configuration



See the following sections for the configurations for this scenario:

- Primary Unit Configuration for Example 10, page A-26
- Secondary Unit Configuration for Example 10, page A-28

Primary Unit Configuration for Example 10

See the following sections for the primary unit configuration:

- Primary System Configuration for Example 10, page A-26
- Primary admin Context Configuration for Example 10, page A-27
- Primary ctx1 Context Configuration for Example 10, page A-28

Primary System Configuration for Example 10

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. Enter the **show mode** command to view the current mode.

```
hostname ciscopix
enable password farscape
password crichton
asdm image flash:/asdm.bin
```

```
boot system flash:/cdisk.bin
mac-address auto
interface gigabitethernet0/0
   description LAN/STATE Failover Interface
interface gigabitethernet0/1
   no shutdown
interface gigabitethernet0/2
   no shutdown
interface gigabitethernet0/3
   no shutdown
interface gigabitethernet1/0
   no shutdown
interface gigabitethernet1/1
   no shutdown
interface gigabitethernet1/2
   no shutdown
interface gigabitethernet1/3
   no shutdown
failover
failover lan unit primary
failover lan interface folink gigabitethernet0/0
failover link folink gigabitethernet0/0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
   primary
   preempt 60
failover group 2
   secondary
   preempt 60
admin-context admin
context admin
   description admin
   allocate-interface gigabitethernet0/1
   allocate-interface gigabitethernet0/2
   config-url flash:/admin.cfg
   join-failover-group 1
context ctx1
   description context 1
   allocate-interface gigabitethernet0/3
   allocate-interface gigabitethernet1/0
   config-url flash:/ctx1.cfg
   join-failover-group 2
```

Primary admin Context Configuration for Example 10

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
enable password frek
password elixir
hostname admin
interface gigabitethernet0/1
   nameif outside
   security-level 0
   ip address 192.168.5.101 255.255.255.0 standby 192.168.5.111
interface gigabitethernet0/2
   nameif inside
   security-level 100
   ip address 192.168.0.1 255.255.255.0 standby 192.168.0.11
monitor-interface outside
monitor-interface inside
route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
```

```
ssh 192.168.0.2 255.255.255.255 inside
```

Primary ctx1 Context Configuration for Example 10

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
enable password quadrophenia
password tommy
hostname ctx1
interface gigabitethernet0/3
   nameif inside
   security-level 100
   ip address 192.168.20.1 255.255.255.0 standby 192.168.20.11
interface gigabitethernet1/0
   nameif outside
   security-level 0
   ip address 192.168.10.31 255.255.255.0 standby 192.168.10.41
   asr-group 1
access-list 201 extended permit ip any any
access-group 201 in interface outside
logging enable
logging console informational
monitor-interface inside
monitor-interface outside
route outside 0.0.0.0 0.0.0.0 192.168.10.71 1
```

Secondary Unit Configuration for Example 10

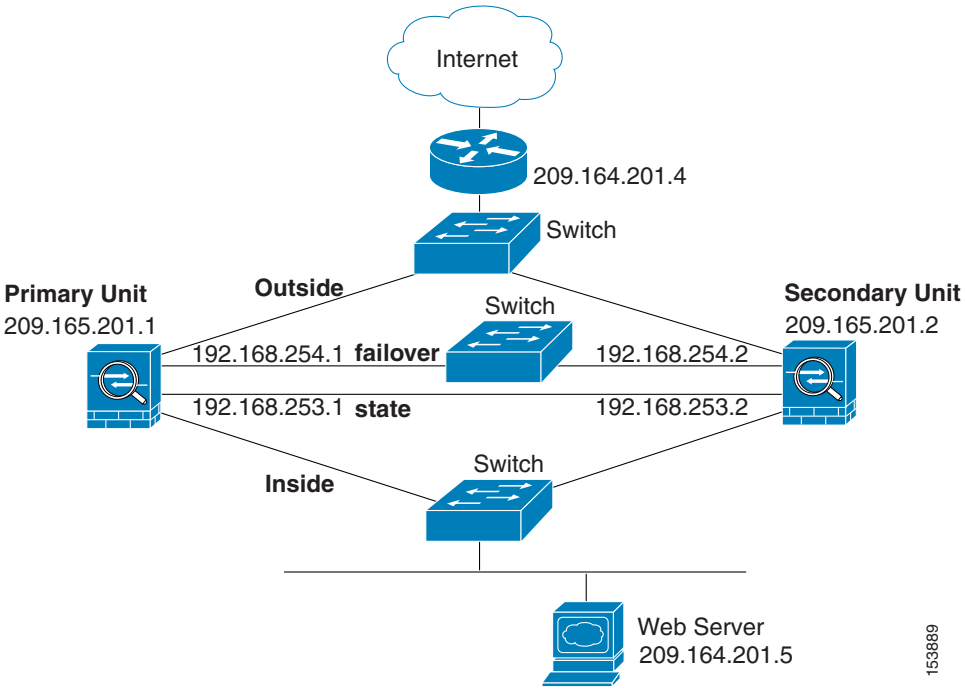
You only need to configure the secondary ASA to recognize the failover link. The secondary ASA obtains the context configurations from the primary ASA upon booting or when failover is first enabled. The **preempt** commands in the failover group configurations cause the failover groups to become active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

```
failover
failover lan unit secondary
failover lan interface folink gigabitethernet0/0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
```

Example 11: LAN-Based Active/Standby Failover (Transparent Mode)

Figure A-11 shows the network diagram for a transparent mode failover configuration using an Ethernet failover link. The units are configured to detect unit failures and to fail over in under a second (see the **failover polltime unit** command in the primary unit configuration).

Figure A-11 Transparent Mode LAN-Based Failover Configuration



See the following sections for the configurations for this scenario:

- Primary Unit Configuration for Example 11, page A-29
- Secondary Unit Configuration for Example 11, page A-30

Primary Unit Configuration for Example 11

```
firewall transparent
hostname pixfirewall
enable password myenablepassword
password mypassword
interface gigabitethernet0/0
   nameif outside
   no shutdown
interface gigabitethernet0/1
   nameif inside
   no shutdown
interface gigabitethernet0/2
   description LAN Failover Interface
   no shutdown
interface gigabitethernet0/3
   description STATE Failover Interface
telnet 192.168.2.45 255.255.255.255 inside
access-list acl_out permit tcp any host 209.165.201.5 eq 80
ip address 209.165.201.1 255.255.255.0 standby 209.165.201.2
failover
failover lan unit primary
failover lan interface failover gigabitethernet0/2
failover lan enable
! The failover lan enable command is required on the PIX ASA only.
failover polltime unit msec 200 holdtime msec 800
```

```
failover key key1
failover link state gigabitethernet0/3
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
failover interface ip state 192.168.253.1 255.255.255.0 standby 192.168.253.2
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

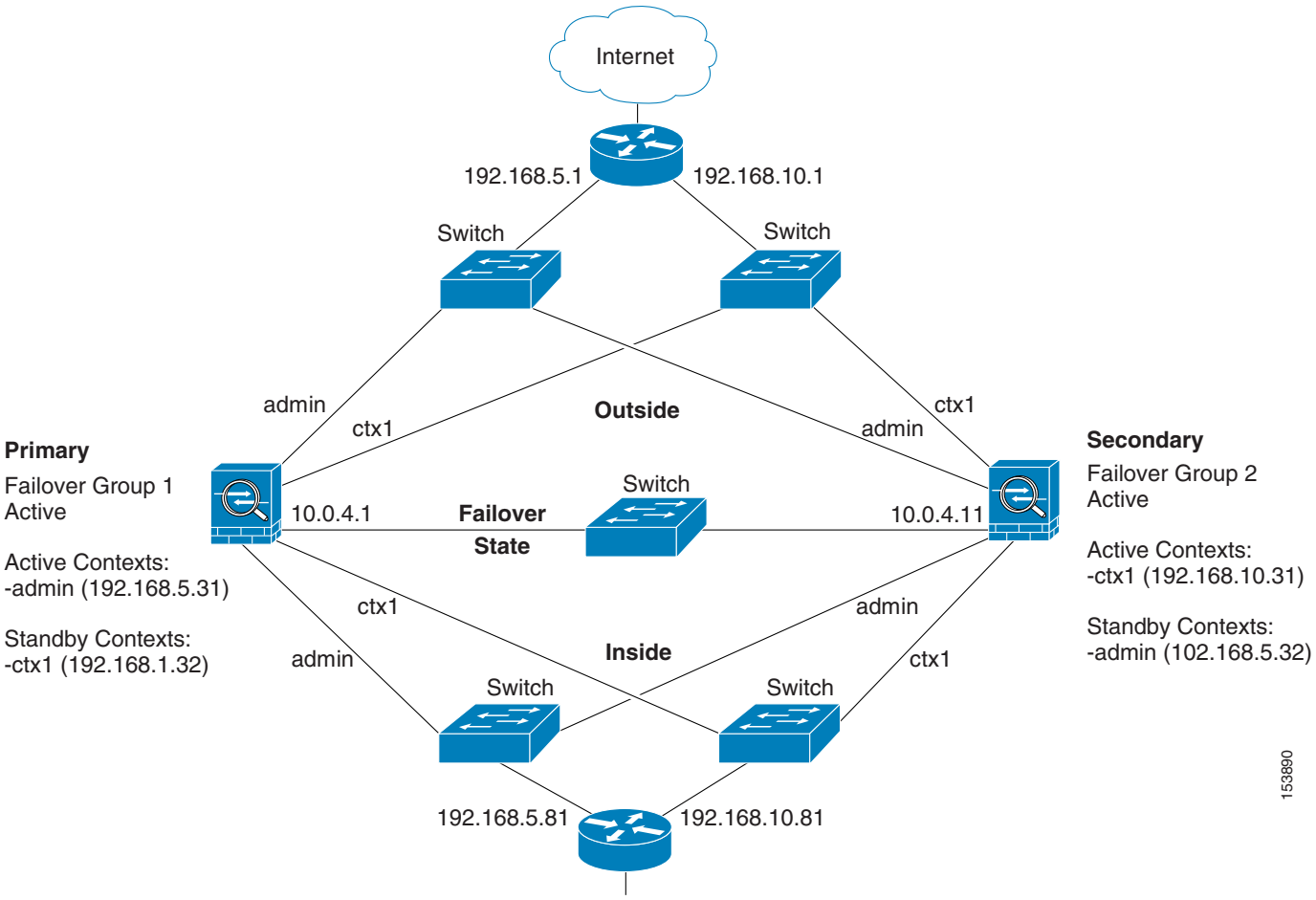
Secondary Unit Configuration for Example 11

```
firewall transparent
failover
failover lan unit secondary
failover lan interface failover gigabitethernet0/2
failover lan enable
failover key key1
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
```

Example 12: LAN-Based Active/Active Failover (Transparent Mode)

The following example shows how to configure transparent mode Active/Active failover. In this example there are 2 user contexts, named admin and ctx1. Figure A-12 shows the network diagram for the example.

Figure A-12 Transparent Mode Active/Active Failover Configuration



See the following sections for the configurations for this scenario:

- Primary Unit Configuration for Example 12, page A-31
- Secondary Unit Configuration for Example 12, page A-33

Primary Unit Configuration for Example 12

See the following sections for the primary unit configuration:

- Primary System Configuration for Example 12, page A-31
- Primary admin Context Configuration for Example 12, page A-32
- Primary ctx1 Context Configuration for Example 12, page A-33

Primary System Configuration for Example 12

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. Enter the **show mode** command to view the current mode.

```
firewall transparent
```

```
hostname ciscopix
enable password farscape
password crichton
asdm image flash:/asdm.bin
boot system flash:/cdisk.bin
mac-address auto
interface gigabitethernet0/0
   description LAN/STATE Failover Interface
interface gigabitethernet0/1
   no shutdown
interface gigabitethernet0/2
   no shutdown
interface gigabitethernet0/3
   no shutdown
interface gigabitethernet1/0
   no shutdown
interface gigabitethernet1/1
   no shutdown
interface gigabitethernet1/2
   no shutdown
interface gigabitethernet1/3
   no shutdown
failover
failover lan unit primary
failover lan interface folink gigabitethernet0/0
failover link folink gigabitethernet0/0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
   primary
   preempt
failover group 2
   secondary
   preempt
admin-context admin
context admin
   description admin
   allocate-interface gigabitethernet0/1
   allocate-interface gigabitethernet0/2
   config-url flash:/admin.cfg
   join-failover-group 1
context ctx1
   description context 1
   allocate-interface gigabitethernet0/3
   allocate-interface gigabitethernet1/0
   config-url flash:/ctx1.cfg
   join-failover-group 2
```

Primary admin Context Configuration for Example 12

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
enable password frek
password elixir
hostname admin
interface gigabitethernet0/1
   nameif outside
   security-level 0
interface gigabitethernet0/2
   nameif inside
   security-level 100
ip address 192.168.5.31 255.255.255.0 standby 192.168.5.32
```

```
monitor-interface outside
monitor-interface inside
route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
ssh 192.168.5.72 255.255.255.255 inside
```

Primary ctx1 Context Configuration for Example 12

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
enable password quadrophenia
password tommy
hostname ctx1
interface gigabitethernet0/3
   nameif inside
   security-level 100
interface gigabitethernet1/0
   nameif outside
   security-level 0
access-list 201 extended permit ip any any
access-group 201 in interface outside
logging enable
logging console informational
ip address 192.168.10.31 255.255.255.0 standby 192.168.10.32
monitor-interface inside
monitor-interface outside
route outside 0.0.0.0 0.0.0.0 192.168.10.1 1
```

Secondary Unit Configuration for Example 12

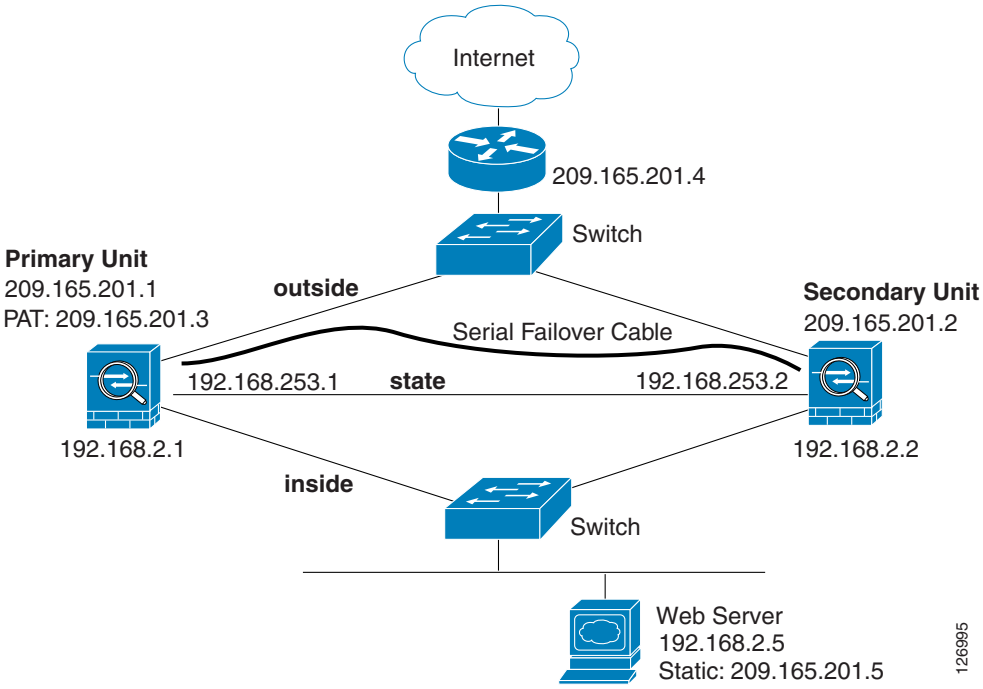
You only need to configure the secondary ASA to recognize the failover link. The secondary ASA obtains the context configurations from the primary ASA upon booting or when failover is first enabled. The **preempt** commands in the failover group configurations cause the failover groups to become active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

```
firewall transparent
failover
failover lan unit secondary
failover lan interface folink gigabitethernet0/0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
```

Example 13: Cable-Based Active/Standby Failover (Routed Mode)

Figure A-13 shows the network diagram for a failover configuration using a serial Failover cable. This configuration is only available on the PIX ASA. This example also specifies a stateful failover configuration.

Figure A-13 Cable-Based Failover Configuration



The following are the typical commands in a cable-based failover configuration.

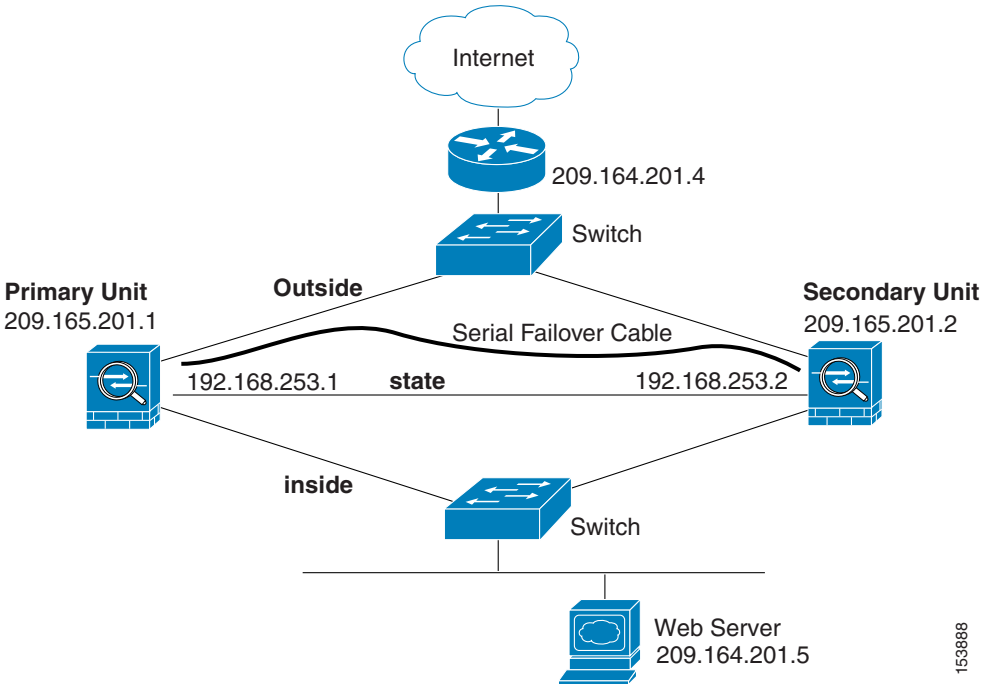
```
enable password myenablepassword
passwd mypassword
hostname pixfirewall
asdm image flash:/asdm.bin
boot system flash:/image.bin
interface Ethernet0
   nameif outside
   security-level 0
   speed 100
   duplex full
   ip address 209.165.201.1 255.255.255.224 standby 209.165.201.2
   no shutdown
interface Ethernet1
   nameif inside
   security-level 100
   speed 100
   duplex full
   ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
   no shutdown
interface Ethernet3
   description STATE Failover Interface
```

```
telnet 192.168.2.45 255.255.255.255 inside
access-list acl_in permit tcp any host 209.165.201.5 eq 80
access-group acl_in in interface outside
failover
! Enables cable-based failover on the PIX security appliance
failover link state Ethernet3
failover interface ip state 192.168.253.1 255.255.255.252 standby 192.168.253.2
! The previous two lines are necessary for a stateful failover
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

Example 14: Cable-Based Active/Standby Failover (Transparent Mode)

Figure A-14 shows the network diagram for a transparent mode failover configuration using a serial Failover cable. This configuration is only available on the PIX 500 series ASA.

Figure A-14 Transparent Mode Cable-Based Failover Configuration



The following are the typical commands in a cable-based, transparent firewall failover configuration.

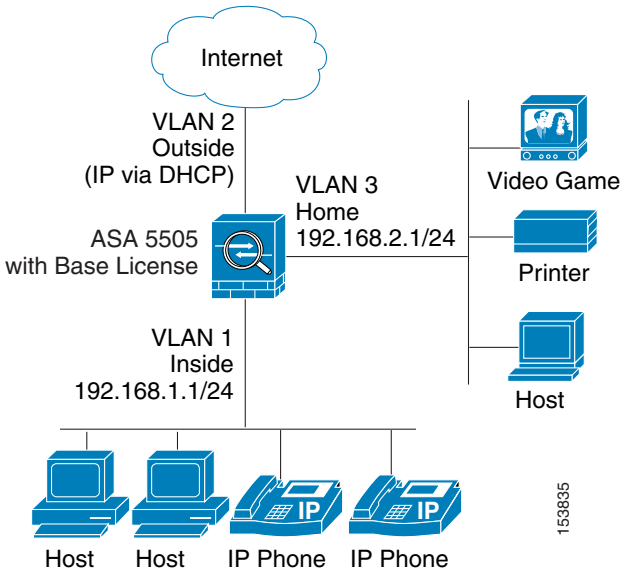
```
enable password myenablepassword
passwd mypassword
hostname pixfirewall
asdm image flash:/asdm.bin
boot system flash:/image.bin
firewall transparent
interface Ethernet0
```

```
   speed 100
   duplex full
   nameif outside
   security-level 0
   no shutdown
interface Ethernet1
   speed 100
   duplex full
   nameif inside
   security-level 100
   no shutdown
interface Ethernet3
   description STATE Failover Interface
telnet 192.168.2.45 255.255.255.255 mgmt
access-list acl_in permit tcp any host 209.165.201.5 eq 80
access-group acl_in in interface outside
ip address 209.165.201.1 255.255.255.0 standby 209.165.201.2
failover
failover link state Ethernet3
failover interface ip state 192.168.253.1 255.255.255.0 standby 192.168.253.2
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

Example 15: ASA 5505 Base License

This configuration creates three VLANs: inside (business), outside (Internet), and home (see Figure A-15). Both the home and inside VLANs can access the outside, but the home VLAN cannot access the inside VLAN. The inside VLAN can access the home VLAN so both VLANs can share a printer. Because the outside IP address is set using DHCP, the inside and home VLANs use interface PAT when accessing the Internet.

Figure A-15 ASA 5505 Base License



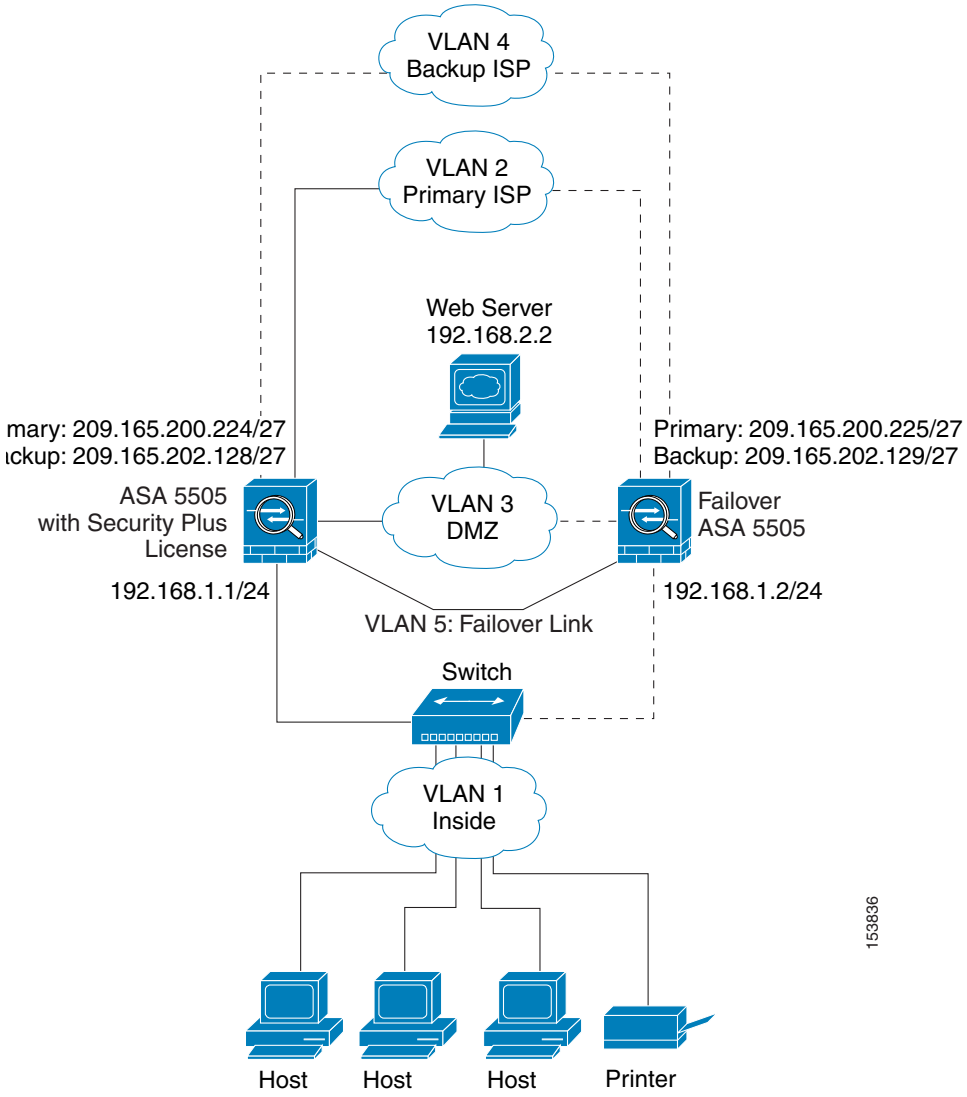

```
passwd g00fba11
enable password gen1u$
hostname Buster
```

```
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
interface vlan 2
   nameif outside
   security-level 0
   ip address dhcp setroute
   no shutdown
interface vlan 1
   nameif inside
   security-level 100
   ip address 192.168.1.1 255.255.255.0
   no shutdown
interface vlan 3
! This interface cannot communicate with the inside interface. This is required using
! the Base license
   no forward interface vlan 1
   nameif home
   security-level 50
   ip address 192.168.2.1 255.255.255.0
   no shutdown
interface ethernet 0/0
   switchport access vlan 2
   no shutdown
   interface ethernet 0/1
   switchport access vlan 1
   no shutdown
interface ethernet 0/2
   switchport access vlan 1
   no shutdown
interface ethernet 0/3
   switchport access vlan 3
   no shutdown
interface ethernet 0/4
   switchport access vlan 3
   no shutdown
interface ethernet 0/5
   switchport access vlan 3
   no shutdown
interface ethernet 0/6
   description PoE for IP phone1
   switchport access vlan 1
   no shutdown
interface ethernet 0/7
   description PoE for IP phone2
   switchport access vlan 1
   no shutdown
nat (inside) 1 0 0
nat (home) 1 0 0
global (outside) 1 interface
! The previous NAT statements match all addresses on inside and home, so you need to
! also perform NAT when hosts access the inside or home networks (as well as the outside).
! Or you can exempt hosts from NAT for inside <--> home traffic, as effected by the
! following:
access-list natexmpt-inside extended permit ip any 192.168.2.0 255.255.255.0
access-list natexmpt-home extended permit ip any 192.168.1.0 255.255.255.0
nat (inside) 0 access-list natexmpt-inside
nat (home) 0 access-list natexmpt-home
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
ssh 192.168.1.0 255.255.255.0 inside
```

Example 16: ASA 5505 Security Plus License with Failover and Dual-ISP Backup

This configuration creates five VLANs: inside, outside, dmz, backup-isp and faillink (see Figure A-16).

Figure A-16 ASA 5505 Security Plus License with Failover and Dual-ISP Backup



See the following sections for the configurations for this scenario:

- Primary Unit Configuration for Example 16, page A-38
- Secondary Unit Configuration for Example 16, page A-40

Primary Unit Configuration for Example 16

```
passwd g00fba11
enable password gen1u$
```

```
hostname Buster
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
interface vlan 2
   description Primary ISP interface
   nameif outside
   security-level 0
   ip address 209.165.200.224 standby 209.165.200.225
   backup interface vlan 4
   no shutdown
interface vlan 1
   nameif inside
   security-level 100
   ip address 192.168.1.1 255.255.255.0
   no shutdown
interface vlan 3
   nameif dmz
   security-level 50
   ip address 192.168.2.1 255.255.255.0
   no shutdown
interface vlan 4
   description Backup ISP interface
   nameif backup-isp
   security-level 0
   ip address 209.168.202.128 standby 209.168.202.129
   no shutdown
interface vlan 5
   description LAN Failover Interface
interface ethernet 0/0
   switchport access vlan 2
   no shutdown
interface ethernet 0/1
   switchport access vlan 4
   no shutdown
interface ethernet 0/2
   switchport access vlan 1
   no shutdown
interface ethernet 0/3
   switchport access vlan 3
   no shutdown
interface ethernet 0/4
   switchport access vlan 5
   no shutdown
failover
failover lan unit primary
failover lan interface faillink vlan5
failover lan faillink vlan5
failover polltime unit 3 holdtime 10
failover key key1
failover interface ip faillink 10.1.1.1 255.255.255.0 standby 10.1.1.2
nat (inside) 1 0 0
nat (home) 1 0 0
global (outside) 1 interface
! The previous NAT statements match all addresses on inside and home, so you need to
! also perform NAT when hosts access the inside or home networks (as well as the outside).
! Or you can exempt hosts from NAT for inside <--> home traffic, as effected by the
! following:
access-list natexmpt-inside extended permit ip any 192.168.2.0 255.255.255.0
access-list natexmpt-home extended permit ip any 192.168.1.0 255.255.255.0
nat (inside) 0 access-list natexmpt-inside
nat (home) 0 access-list natexmpt-home
sla monitor 123
 type echo protocol ipIcmpEcho 209.165.200.234 interface outside
 num-packets 2
```

```
 frequency 5
sla monitor schedule 123 life forever start-time now
track 1 rtr 123 reachability
route outside 0 0 209.165.200.234 1 track 1
! This route is for the primary ISP.
route backup-isp 0 0 209.165.202.154 2
! If the link goes down for the primary ISP, either due to a hardware failure
! or unplugged cable, then this route will be used.
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
ssh 192.168.1.0 255.255.255.0 inside
```

Secondary Unit Configuration for Example 16

You only need to configure the secondary ASA to recognize the failover link. The secondary ASA obtains the context configurations from the primary ASA upon booting or when failover is first enabled.

```
interface ethernet 0/4
   switchport access vlan 5
   no shutdown
failover
failover lan unit secondary
failover lan interface faillink vlan5
failover polltime unit 3 holdtime 10
failover key key1
failover interface ip faillink 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

Example 17: AIP SSM in Multiple Context Mode

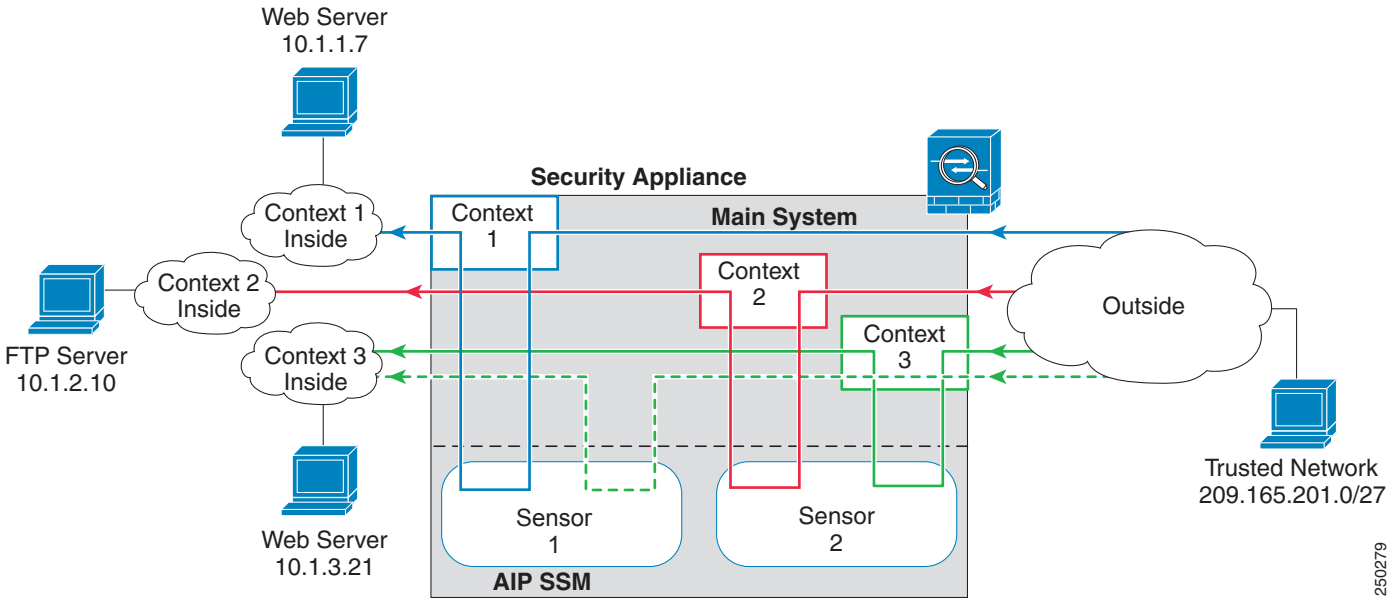
This configuration assigns two virtual IPS sensors to three contexts. Context 1 uses sensor 1, context 2 uses sensor 2 (for greater security), and context 3 uses sensor 2 for most traffic, but uses sensor 1 for a more trusted outside network (see Figure A-17).

For Context 1, only the trusted network is allowed to access a web server and manage the context using SSH.

For Context 2, any outside user can access the FTP server.

For Context 3, any outside user can access the web server, but the trusted network can access anything on the inside network.

Figure A-17 Security Contexts and Virtual Sensors



See the following sections for the configurations for this scenario:

- System Configuration for Example 17, page A-41
- Context 1 Configuration for Example 17, page A-42
- Context 2 Configuration for Example 17, page A-42
- Context 3 Configuration for Example 17, page A-43

System Configuration for Example 17

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. Enter the **show mode** command to view the current mode.

```
hostname Farscape
password passw0rd
enable password chr1cht0n
mac-address auto
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
admin-context context 1
interface gigabitethernet 0/0
   no shutdown
interface gigabitethernet 0/1
   no shutdown
interface gigabitethernet 0/2
   no shutdown
interface gigabitethernet 0/3
   no shutdown
context 1
   allocate-interface gigabitethernet0/0
   allocate-interface gigabitethernet0/3
   allocate-ips sensor1
   config-url ftp://user1:passw0rd@10.1.1.1/configlets/context1.cfg
context 2
```

```
   allocate-interface gigabitethernet0/1
   allocate-interface gigabitethernet0/3
   allocate-ips sensor2
   config-url ftp://user1:passw0rd@10.1.1.1/configlets/context2.cfg
context 3
   allocate-interface gigabitethernet0/2
   allocate-interface gigabitethernet0/3
   allocate-ips sensor1
   allocate-ips sensor2 default
   config-url ftp://user1:passw0rd@10.1.1.1/configlets/context3.cfg
```

Context 1 Configuration for Example 17

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
hostname context1
domain example.com
interface gigabitethernet 0/3
   nameif outside
   security-level 0
   ip address 209.165.200.225 255.255.255.224
   no shutdown
interface gigabitethernet 0/0
   nameif inside
   security-level 100
   ip address 10.1.1.1 255.255.255.0
   no shutdown
passwd seaandsand
enable password pinballwizard
route outside 0 0 209.165.200.230 1
ssh 209.165.201.0 255.255.255.224 outside
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 209.165.200.252
! Trusted network can access the web server at 10.1.1.7
access-list INBOUND extended permit tcp 209.165.201.0 255.255.255.224 host 10.1.1.7 eq
http
access-group INBOUND in interface outside
! Any traffic allowed to the inside of context 1 must go through
! the IPS sensor assigned to the context.
! Traffic is in promiscuous mode (a separate stream is sent
! to the IPS sensor. If the sensor fails, traffic continues.
access-list IPS extended permit ip any any
class-map my-ips-class
   match access-list IPS
policy-map my-ips-policy
   class my-ips-class
      ips promiscous fail-open
service-policy my-ips-policy interface outside
```

Context 2 Configuration for Example 17

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
hostname context2
domain example.com
interface gigabitethernet 0/3
   nameif outside
```

```
   security-level 0
   ip address 209.165.200.226 255.255.255.224
   no shutdown
interface gigabitethernet 0/1
   nameif inside
   security-level 100
   ip address 10.1.2.1 255.255.255.0
   no shutdown
passwd drjimmy
enable password acidqueen
route outside 0 0 209.165.200.230 1
ssh 10.1.2.67 255.255.255.255 inside
nat (inside) 1 10.1.2.0 255.255.255.0
global (outside) 1 209.165.200.253
! All users can access the FTP server at 10.1.2.10
access-list FTP extended permit tcp any any eq ftp
access-group FTP in interface outside
! Any traffic allowed to the inside of context 2 must go through
! the IPS sensor assigned to the context.
! Traffic is in inline mode (traffic is sent
! to the IPS sensor before continuing to the inside.)
! If the sensor fails, traffic stops.
access-list IPS permit ip any any
class-map my-ips-class
   match access-list IPS
policy-map my-ips-policy
   class my-ips-class
      ips inline fail-close
service-policy my-ips-policy interface outside
```

Context 3 Configuration for Example 17

To change to a context configuration, enter the **changeto context** *name* command. To change back to the system, enter **changeto system**.

```
hostname context3
domain example.com
interface gigabitethernet 0/3
   nameif outside
   security-level 0
   ip address 209.165.200.227 255.255.255.224
   no shutdown
interface gigabitethernet 0/1
   nameif inside
   security-level 100
   ip address 10.1.3.1 255.255.255.0
   no shutdown
passwd lovereign
enable password underture
route outside 0 0 209.165.200.230 1
ssh 209.165.201.0 255.255.255.224 outside
nat (inside) 1 10.1.3.0 255.255.255.0
global (outside) 1 209.165.200.254
! All users can access the web server at 10.1.3.21
! The trusted network 209.165.201.0/27 can access all of the inside nw.
access-list IN_CONTEXT3 extended permit ip 209.165.201.0 255.255.255.224 any
access-list IN_CONTEXT3 extended permit tcp any host 10.1.3.21 eq http
access-group IN_CONTEXT3 in interface outside
! Traffic from 209.165.201.0/27 goes through IPS sensor 1.
! Traffic is in promiscuous mode (a separate stream is sent
! to the IPS sensor. If the sensor fails, traffic continues.
```

```
! All other traffic allowed to the inside of context 1 must go
! through sensor 2. Traffic is in inline mode (traffic is sent
! to the IPS sensor before continuing to the inside.)
! If the sensor fails, traffic stops.
access-list my-ips-acl permit ip 209.165.201.0 255.255.255.224 any
class-map my-ips-class
   match access-list my-ips-acl
access-list my-ips-acl2 permit ip any any
class-map my-ips-class2
   match access-list my-ips-acl2
policy-map my-ips-policy
   class my-ips-class
      ips promiscuous fail-open sensor sensor1
   class my-ips-class2
      ips inline fail-close sensor sensor2
service-policy my-ips-policy interface outside
```