



# APPENDIX **B**

## Sample Configurations

---

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

- [Example 1: Multiple Mode Firewall With Outside Access, page B-1](#)
- [Example 2: Single Mode Firewall Using Same Security Level, page B-6](#)
- [Example 3: Shared Resources for Multiple Contexts, page B-8](#)
- [Example 4: Multiple Mode, Transparent Firewall with Outside Access, page B-13](#)
- [Example 5: Single Mode, Transparent Firewall with NAT, page B-18](#)
- [Example 6: IPv6 Configuration, page B-19](#)
- [Example 7: Dual ISP Support Using Static Route Tracking, page B-20](#)
- [Example 8: MultiCast Routing \(Routed Mode\), page B-21](#)
- [Example 9: Active/Standby Failover \(Routed Mode\), page B-23](#)
- [Example 10: Active/Active Failover \(Routed Mode\), page B-25](#)
- [Example 11: Active/Standby Failover \(Transparent Mode\), page B-28](#)
- [Example 12: Active/Active Failover \(Transparent Mode\), page B-30](#)

### 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 B-1](#)).

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

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

The admin context allows SSH sessions to the adaptive security appliance from one host.

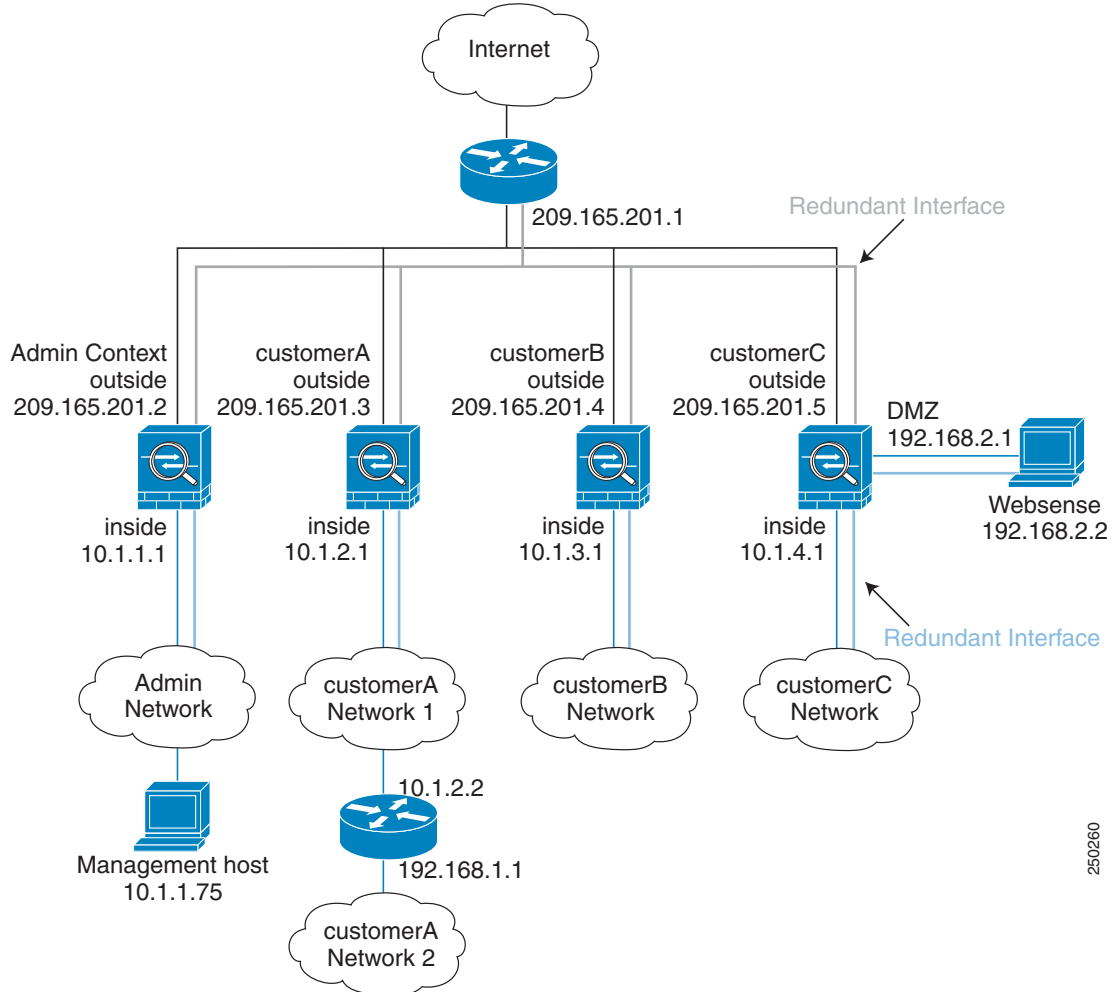


#### Note

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

---

Figure B-1 Example 1



250260

See the following sections for the configurations for this scenario:

- [System Configuration for Example 1, page B-2](#)
- [Admin Context Configuration for Example 1, page B-4](#)
- [Customer A Context Configuration for Example 1, page B-4](#)
- [Customer B Context Configuration for Example 1, page B-5](#)
- [Customer C Context Configuration for Example 1, page B-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 hlandl0
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 tenac1ous
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 adaptive security appliance 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
```

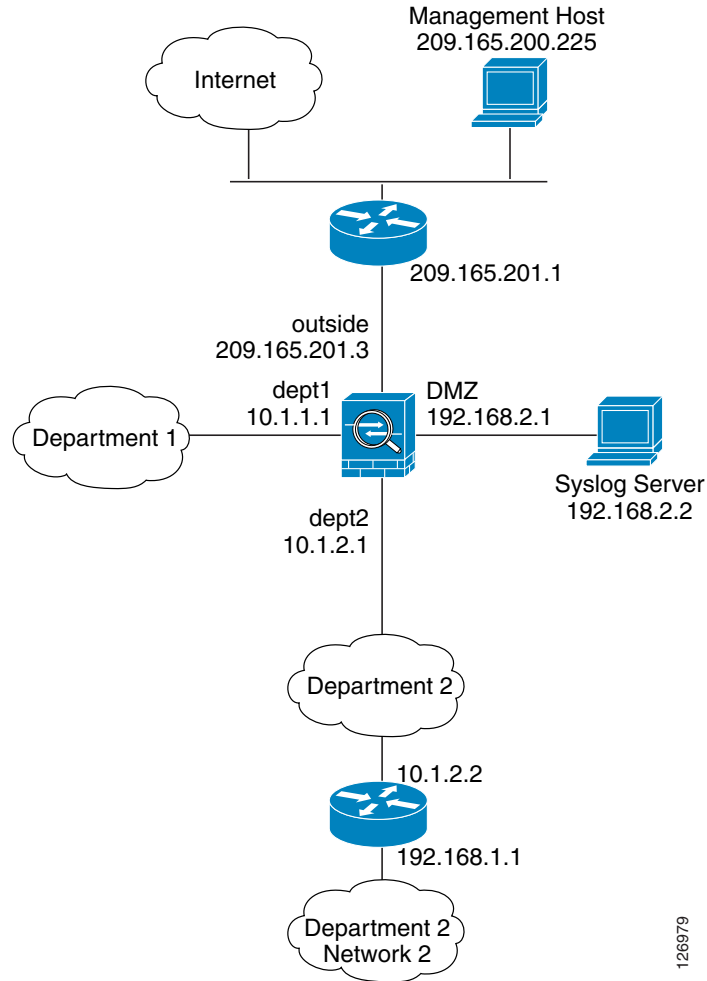
## Example 2: Single Mode Firewall Using Same Security Level

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 adaptive security appliance. The adaptive security appliance uses RIP on the inside interfaces to learn routes. The adaptive security appliance does not advertise routes with RIP; the upstream router needs to use static routes for adaptive security appliance traffic (see [Figure B-2](#)).

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

Threat detection is enabled.

Figure B-2 Example 2



126979

```

passwd g00fba11
enable password genlu$
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 adaptive security appliance IP address as the default gateway for the
! downstream
! router. The adaptive security appliance does not advertise a default route to the
! upstream
! router. Listens for RIP updates from the downstream router. The adaptive security
! appliance 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

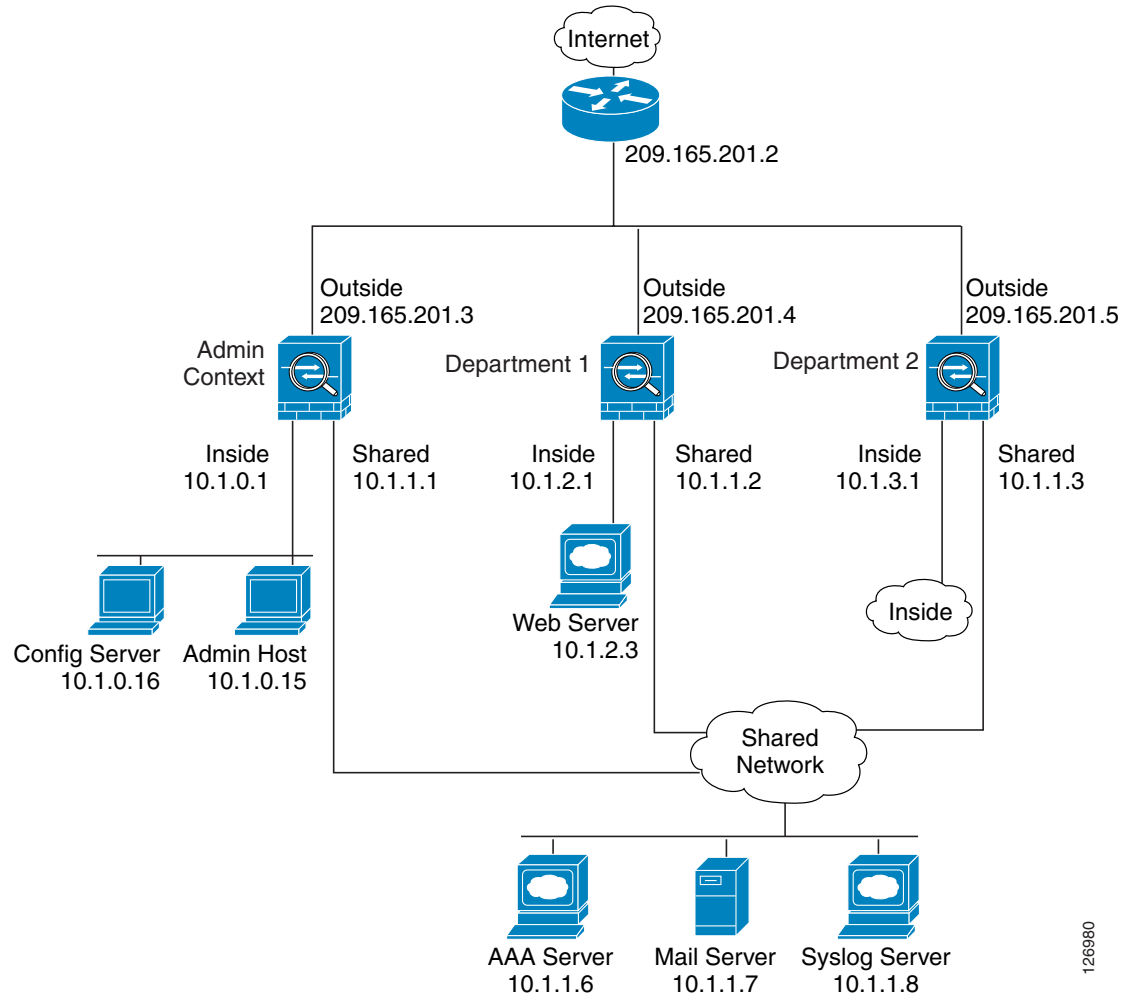
```

## 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 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



126980

See the following sections for the configurations for this scenario:

- [System Configuration for Example 3, page B-9](#)
- [Admin Context Configuration for Example 3, page B-10](#)
- [Department 1 Context Configuration for Example 3, page B-11](#)
- [Department 2 Context Configuration for Example 3, page B-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 rhalto
nat (inside) 1 10.1.2.0 255.255.255.0

```

## Example 3: Shared Resources for Multiple Contexts

```

! 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 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 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 B-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 adaptive security appliance from one host.

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

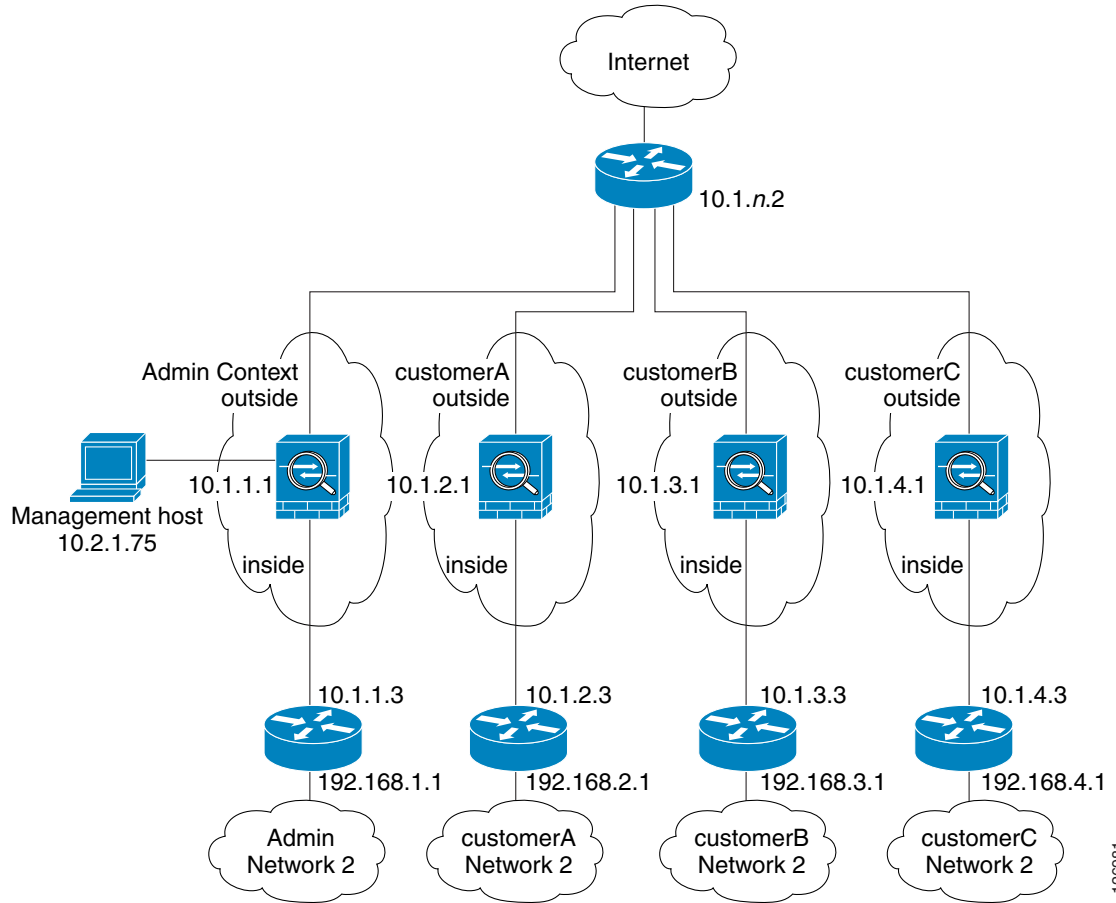
**Note**

---

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

---

Figure B-4 Example 4



See the following sections for the configurations for this scenario:

- [System Configuration for Example 4, page B-14](#)
- [Admin Context Configuration for Example 4, page B-15](#)
- [Customer A Context Configuration for Example 4, page B-16](#)
- [Customer B Context Configuration for Example 4, page B-16](#)
- [Customer C Context Configuration for Example 4, page B-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 hlandl0
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**.

```

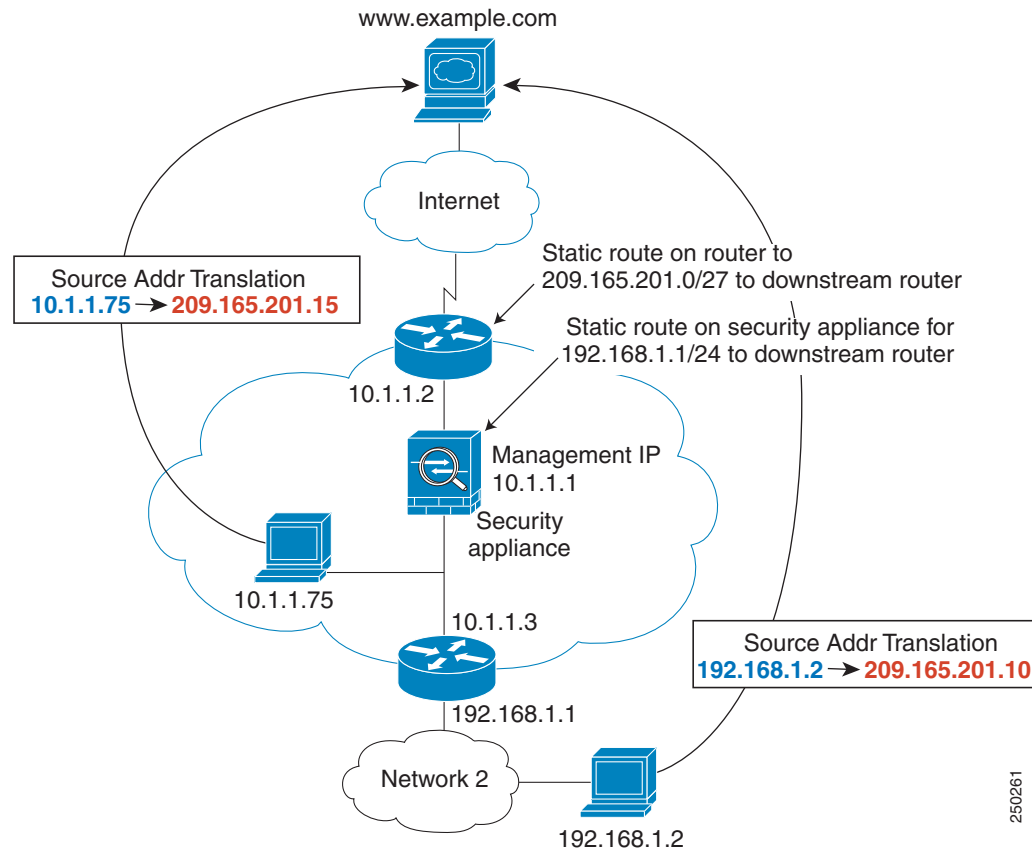
interface gigabitethernet 0/0.153
  nameif outside
  security-level 0
  no shutdown
interface gigabitethernet 0/1.7
  nameif inside
  security-level 100
  no shutdown
passwd fl0wer
enable password treeh0u$e
ip address 10.1.4.1 255.255.255.0
route outside 0 0 10.1.4.2 1
access-list OSPF remark -Allows 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 B-5](#)).

Figure B-5 Example 5



The host at 10.1.1.75 can access the adaptive security appliance 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

```

250261

```

! 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

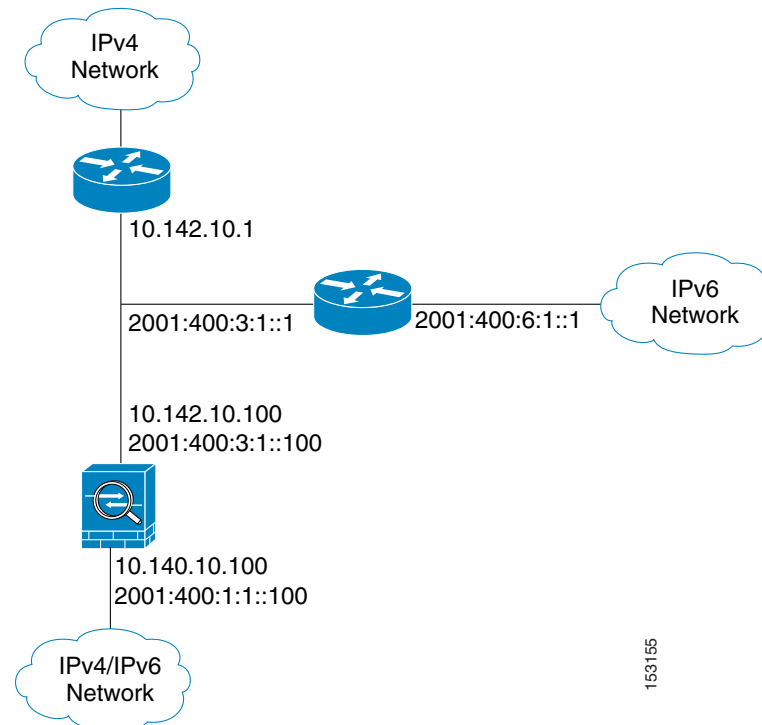
```

## Example 6: IPv6 Configuration

This sample configuration shows several features of IPv6 support on the adaptive security appliance:

- 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 B-6** IPv6 Dual Stack Configuration



```

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

```

## Example 7: Dual ISP Support Using Static Route Tracking

```

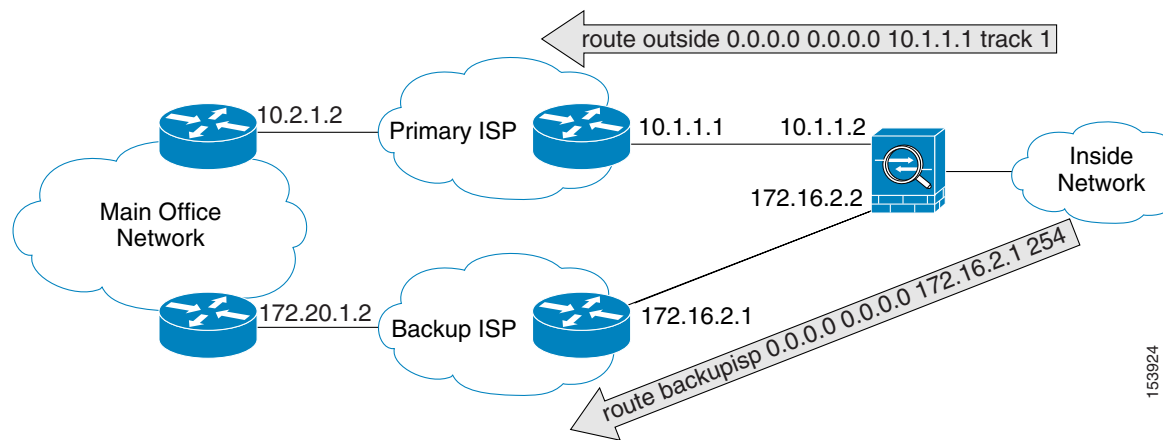
interface Ethernet0
  nameif outside
  security-level 0
  ip address 10.142.10.100 255.255.255.0
  ipv6 address 2001:400:3:1::100/64
  ipv6 nd suppress-ra
  ospf mtu-ignore auto
  no shutdown
interface Ethernet1
  nameif inside
  security-level 100
  ip address 10.140.10.100 255.255.255.0
  ipv6 address 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 adaptive security appliance 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 B-7** Dual ISP Support



```

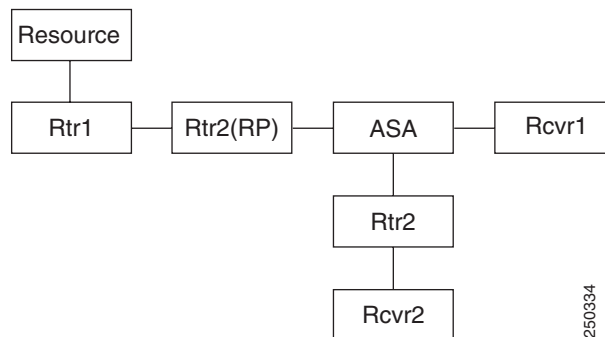
passwd password1
enable password password2
hostname myfirewall
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
!
interface gigabitethernet 0/0
  nameif outside
  security-level 0
  ip address 10.1.1.2 255.255.255.0
  no shutdown
!
interface gigabitethernet 0/1
  description backup isp link
  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 10.2.1.1 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 (Routed Mode)

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 all IOS routers.

**Figure B-8** Multicast Routing Configuration



**Note**


---

Multicast routing only works in single routed mode.

---

- [For PIM Sparse Mode, page B-22](#)
- [For PIM bidir Mode, page B-22](#)

## 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

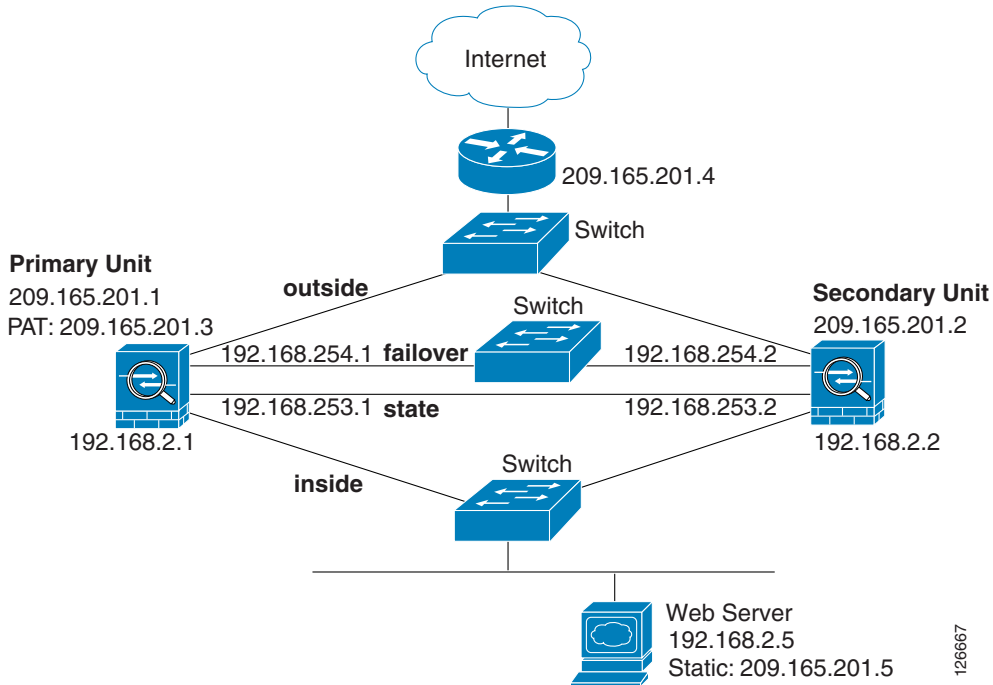
no failover
access-group mcast in interface outside
access-group mcast in interface inside
access-group mcast in interface dmz

! 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: Active/Standby Failover (Routed Mode)

Figure B-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 B-9 Failover Configuration



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

- [Primary Unit Configuration for Example 9, page B-24](#)
- [Secondary Unit Configuration for Example 9, page B-25](#)

## Primary Unit Configuration for Example 9

```
hostname pixfirewall
enable password myenablepassword
password mypassword
interface Ethernet0
  nameif outside
  ip address 209.165.201.1 255.255.255.224 standby 209.165.201.2
  no shutdown
interface Ethernet1
  nameif inside
  ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
  no shutdown
interface Ethernet2
  description LAN Failover Interface
  no shutdown
interface ethernet3
  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 Ethernet2
failover lan enable
! The failover lan enable command is required on the PIX adaptive security appliance only.
failover polltime unit msec 200 holdtime msec 800
failover key key1
```

```
failover link state Ethernet3
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
```

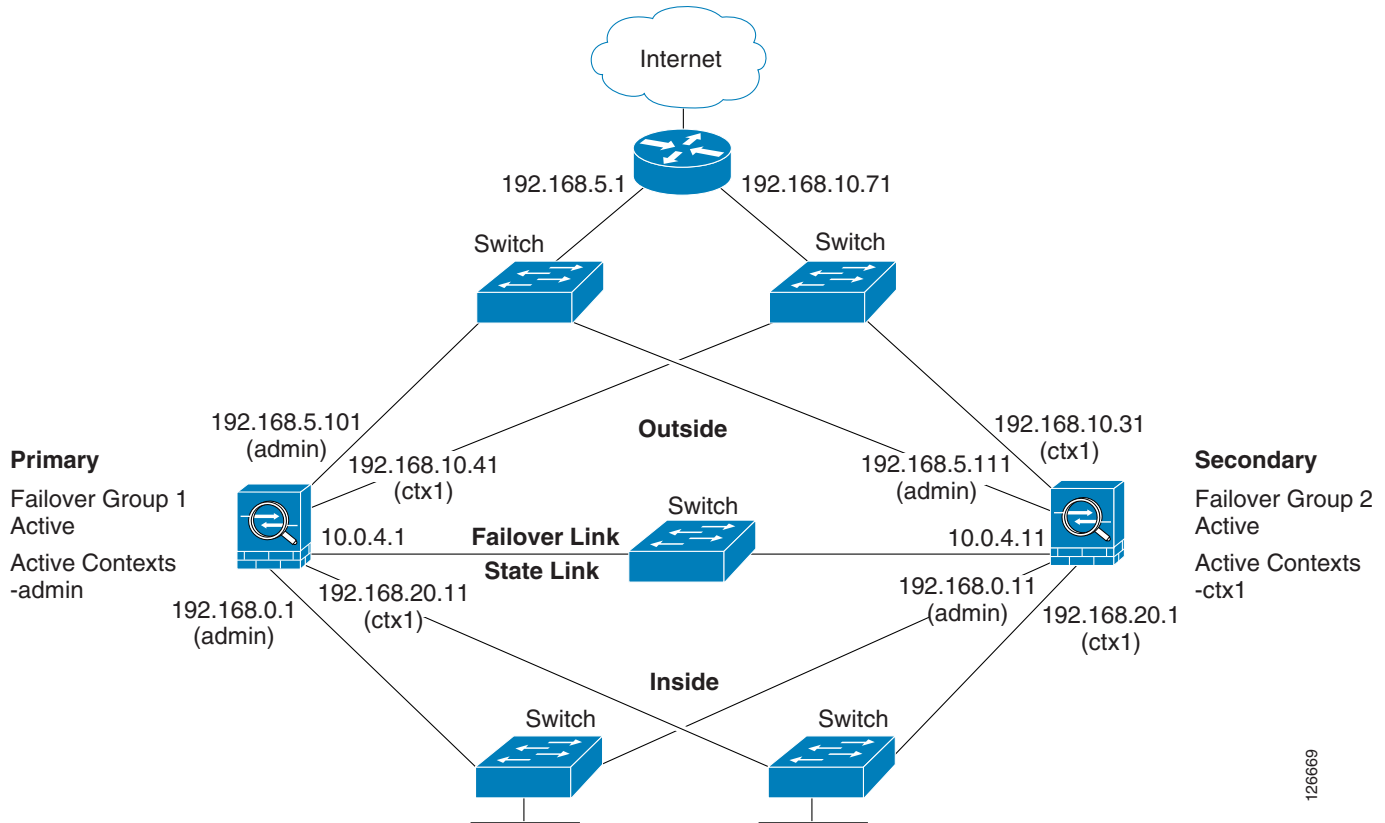
## Secondary Unit Configuration for Example 9

```
failover
failover lan unit secondary
failover lan interface failover ethernet2
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: 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 B-10](#) shows the network diagram for the example.

Figure B-10 Active/Active Failover Configuration



126669

See the following sections for the configurations for this scenario:

- [Primary Unit Configuration for Example 10, page B-26](#)
- [Secondary Unit Configuration for Example 10, page B-28](#)

## Primary Unit Configuration for Example 10

See the following sections for the primary unit configuration:

- [Primary System Configuration for Example 10, page B-26](#)
- [Primary admin Context Configuration for Example 10, page B-27](#)
- [Primary ctx1 Context Configuration for Example 10, page B-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 Ethernet0
  description LAN/STATE Failover Interface
interface Ethernet1
  no shutdown
interface Ethernet2
  no shutdown
interface Ethernet3
  no shutdown
interface Ethernet4
  no shutdown
interface Ethernet5
  no shutdown
interface Ethernet6
  no shutdown
interface Ethernet7
  no shutdown
interface Ethernet8
  no shutdown
interface Ethernet9
  no shutdown
failover
failover lan unit primary
failover lan interface folink Ethernet0
failover link folink Ethernet0
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 Ethernet1
  allocate-interface Ethernet2
  config-url flash:/admin.cfg
  join-failover-group 1
context ctx1
  description context 1
  allocate-interface Ethernet3
  allocate-interface Ethernet4
  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 Ethernet1
  nameif outside
  security-level 0
  ip address 192.168.5.101 255.255.255.0 standby 192.168.5.111
interface Ethernet2
  nameif inside
  security-level 100

```

### Example 11: Active/Standby Failover (Transparent Mode)

```

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 Ethernet3
  nameif inside
  security-level 100
  ip address 192.168.20.1 255.255.255.0 standby 192.168.20.11
interface Ethernet4
  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 adaptive security appliance to recognize the failover link. The secondary adaptive security appliance obtains the context configurations from the primary adaptive security appliance 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.

```

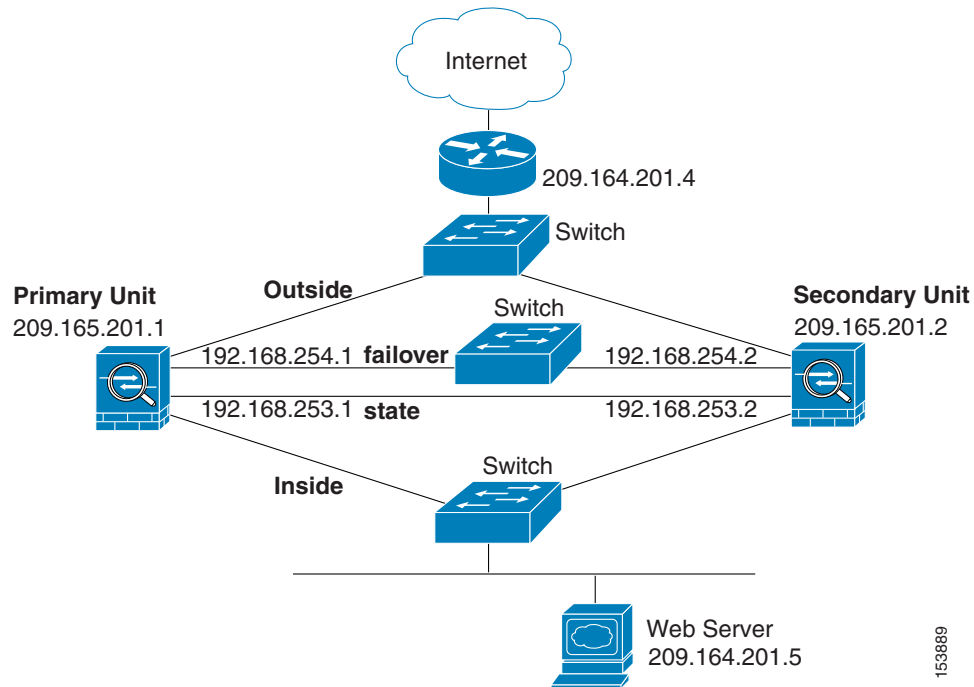
failover
failover lan unit secondary
failover lan interface folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11

```

## Example 11: Active/Standby Failover (Transparent Mode)

Figure B-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 B-11 Transparent Mode Failover Configuration



See the following sections for the configurations for this scenario:

- [Primary Unit Configuration for Example 11, page B-29](#)
- [Secondary Unit Configuration for Example 11, page B-30](#)

## Primary Unit Configuration for Example 11

```

firewall transparent
hostname pixfirewall
enable password myenablepassword
password mypassword
interface Ethernet0
  nameif outside
  no shutdown
interface Ethernet1
  nameif inside
  no shutdown
interface Ethernet2
  description LAN Failover Interface
  no shutdown
interface ethernet3
  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 Ethernet2
failover lan enable
! The failover lan enable command is required on the PIX adaptive security appliance only.
failover polltime unit msec 200 holdtime msec 800

```

## ■ Example 12: Active/Active Failover (Transparent Mode)

```
failover key key1
failover link state Ethernet3
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
```

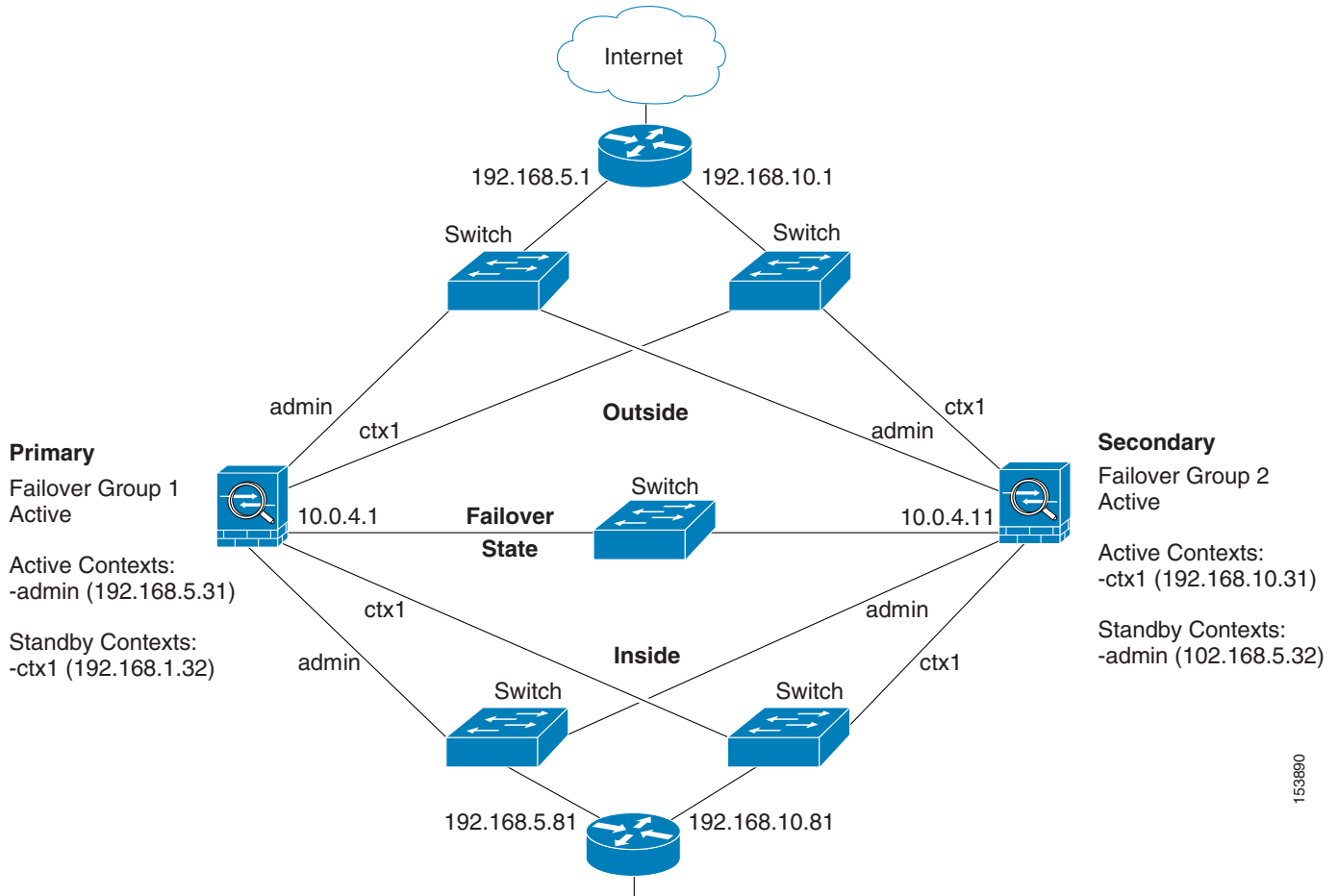
## Secondary Unit Configuration for Example 11

```
firewall transparent
failover
failover lan unit secondary
failover lan interface failover ethernet2
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: 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 B-12](#) shows the network diagram for the example.

Figure B-12 Transparent Mode Active/Active Failover Configuration



See the following sections for the configurations for this scenario:

- [Primary Unit Configuration for Example 12, page B-31](#)
- [Secondary Unit Configuration for Example 12, page B-33](#)

## Primary Unit Configuration for Example 12

See the following sections for the primary unit configuration:

- [Primary System Configuration for Example 12, page B-31](#)
- [Primary admin Context Configuration for Example 12, page B-32](#)
- [Primary ctx1 Context Configuration for Example 12, page B-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
```

## Example 12: Active/Active Failover (Transparent Mode)

```

hostname ciscopix
enable password farscape
password crichton
asdm image flash:/asdm.bin
boot system flash:/cdisk.bin
mac-address auto
interface Ethernet0
    description LAN/STATE Failover Interface
interface Ethernet1
    no shutdown
interface Ethernet2
    no shutdown
interface Ethernet3
    no shutdown
interface Ethernet4
    no shutdown
interface Ethernet5
    no shutdown
interface Ethernet6
    no shutdown
interface Ethernet7
    no shutdown
interface Ethernet8
    no shutdown
interface Ethernet9
    no shutdown
failover
failover lan unit primary
failover lan interface folink Ethernet0
failover link folink Ethernet0
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 Ethernet1
    allocate-interface Ethernet2
    config-url flash:/admin.cfg
    join-failover-group 1
context ctx1
    description context 1
    allocate-interface Ethernet3
    allocate-interface Ethernet4
    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 Ethernet1
    nameif outside
    security-level 0

```

```

interface Ethernet2
  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 Ethernet3
  nameif inside
  security-level 100
interface Ethernet4
  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 adaptive security appliance to recognize the failover link. The secondary adaptive security appliance obtains the context configurations from the primary adaptive security appliance 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 Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11

```

## ■ Example 12: Active/Active Failover (Transparent Mode)