Cisco Systems Networking Academy

Cisco.com

# Network Security 2

# Module 8 – PIX Security Appliance Contexts, Failover

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

# Learning Objectives


Cisco.com

–8.1 Configure a PIX Security Appliance to Perform in Multiple Context Mode

–8.2 Configure PIX Security Appliance Failover

–8.3 Configure Transparent Firewall Mode


Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems Networking Academy

Cisco.com

# Module 8 – PIX Security Appliance Contexts, Failover, and Management

## 8.1 Configure a PIX Security Appliance to Perform in Multiple Context Mode

CCNA CISCO CERTIFIED™

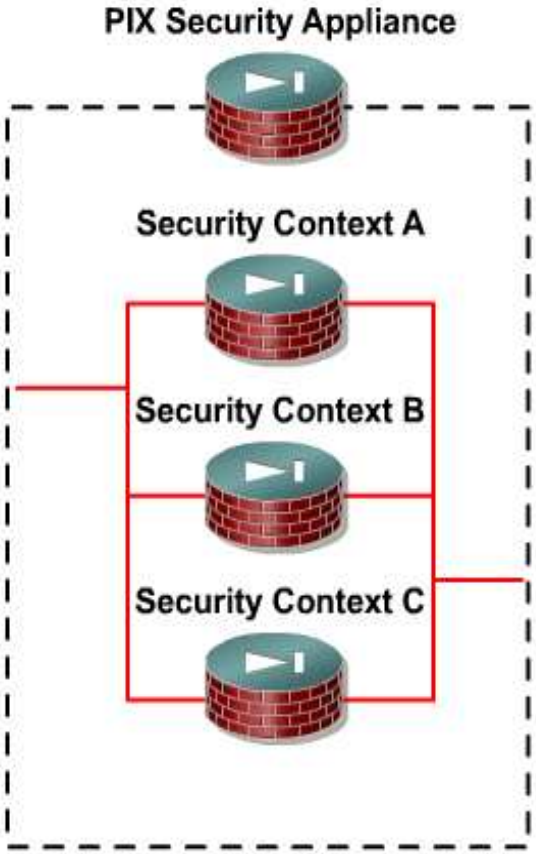
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

HÖGSKOLAN HALMSTAD

# Security Contexts

Cisco.com

- You can partition a single firewall appliance into multiple virtual firewalls, known as security contexts.
- Each context has its own configuration that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone firewall.
- The system administrator adds and manages contexts by configuring them in the system configuration, which identifies basic settings for the firewall appliance.
- When the system needs to access network resources, it uses one of the contexts that is designated as the admin context.

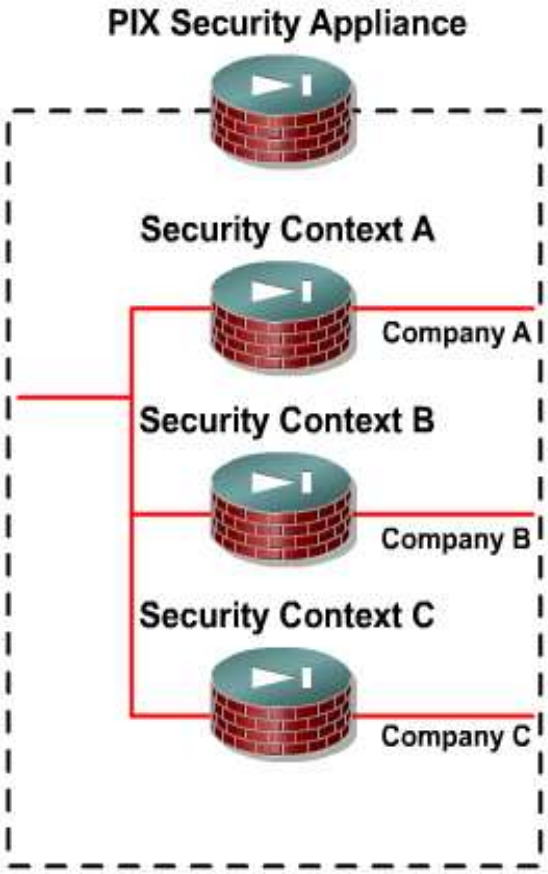



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Common Uses for Security Contexts

Cisco.com

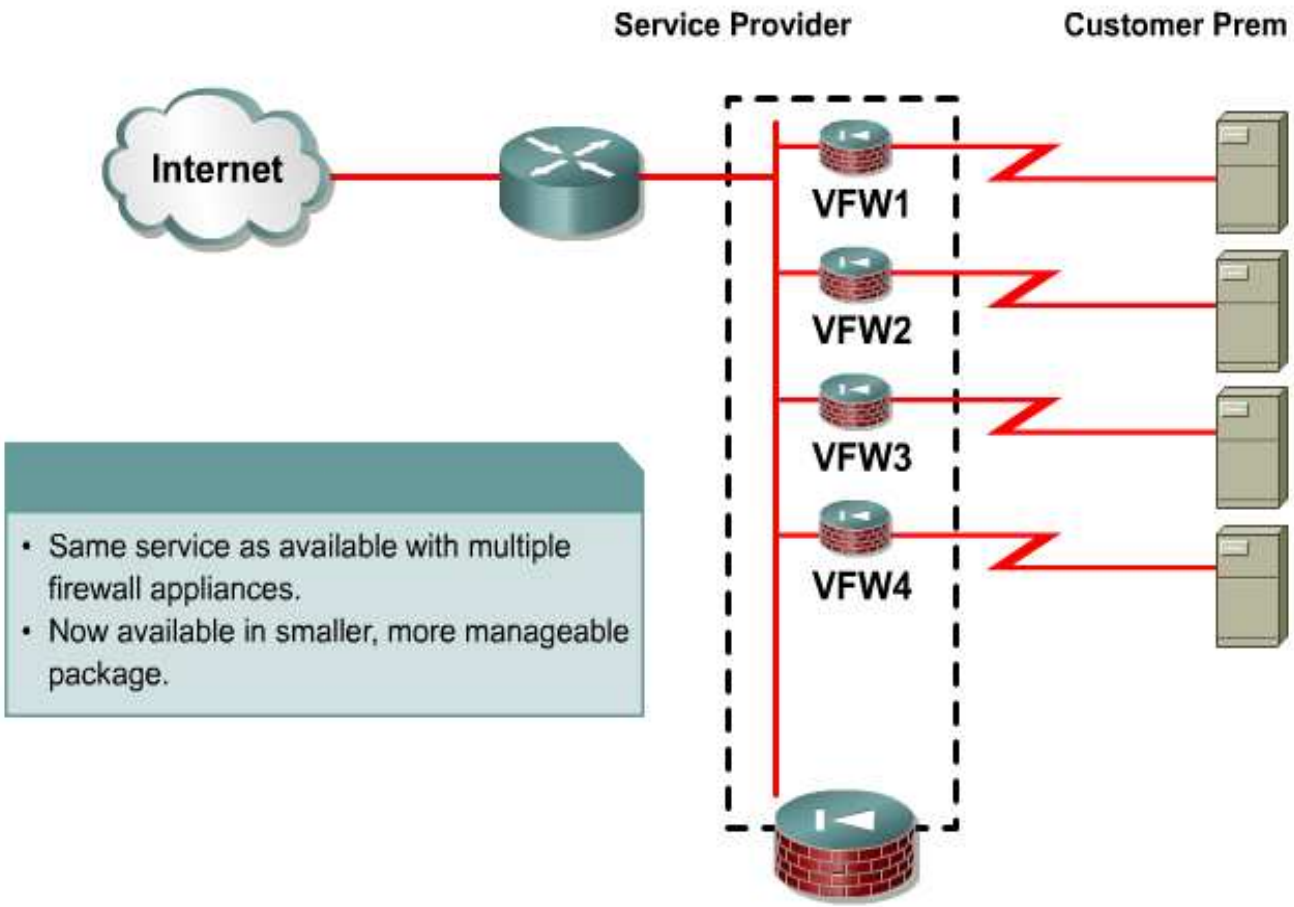
- Service provider wanting to sell firewall services to many customers.
- Large enterprise or a college campus wanting to keep departments completely separate.
- Enterprise that wanting to provide distinct security policies to different departments.
- Any network that requires more than one firewall.




Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Multiple Contexts Example






- Same service as available with multiple firewall appliances.
- Now available in smaller, more manageable package.

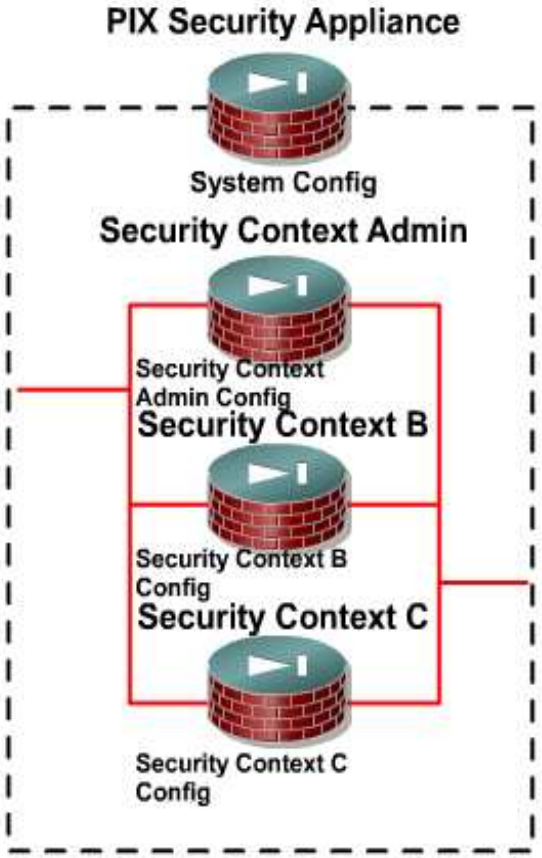
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Context Configuration Files

Cisco.com

**Context configuration files have the following characteristics:**

- Each context has its own configuration file.
- The firewall appliance also includes a system configuration that identifies basic settings for the firewall appliance, including a list of contexts.




Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Packet Classification

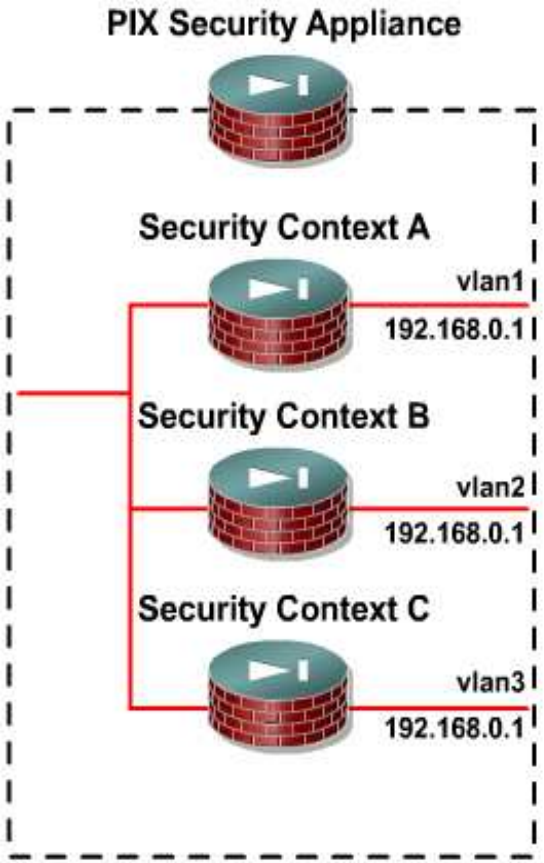
Cisco.com

**Each packet that enters the firewall appliance must be classified, so that the firewall appliance can determine to which context to send a packet. The firewall appliance checks for the following characteristics:**

- Source interface (VLAN)
- Destination address

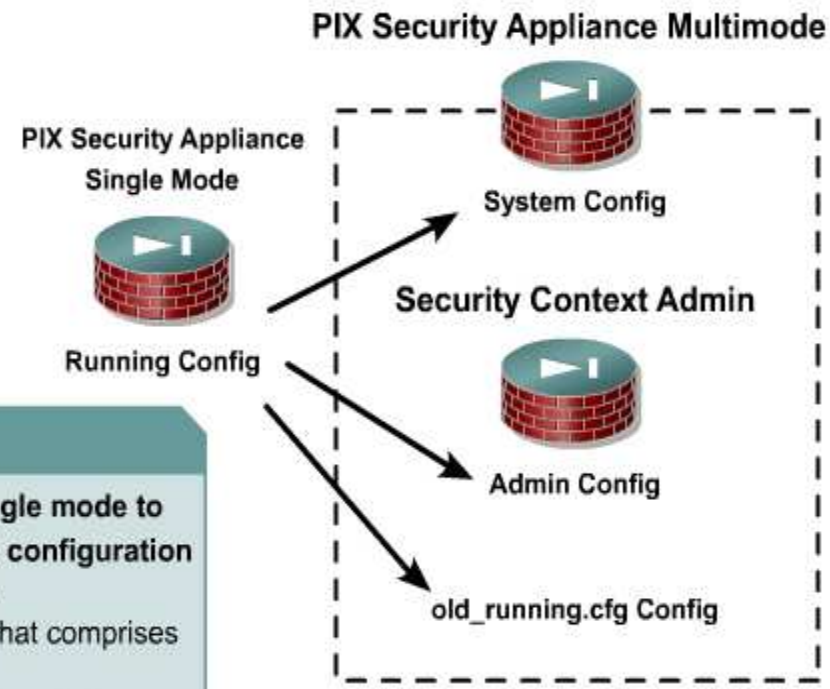
**The firewall appliance uses the characteristic that is unique and not shared across contexts.**

- You can share a VLAN interface so long as each IP address space on that VLAN is unique. You can have overlapping IP addresses so long as the VLANs are unique.




Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Backing up the Single Mode Configuration




**When you convert from single mode to multiple mode, the running configuration is converted into two files:**

- New startup configuration that comprises the system configuration.
- Admin.cfg that comprises the admin context.

**The original running configuration is saved as old_running.cfg (in disk).**

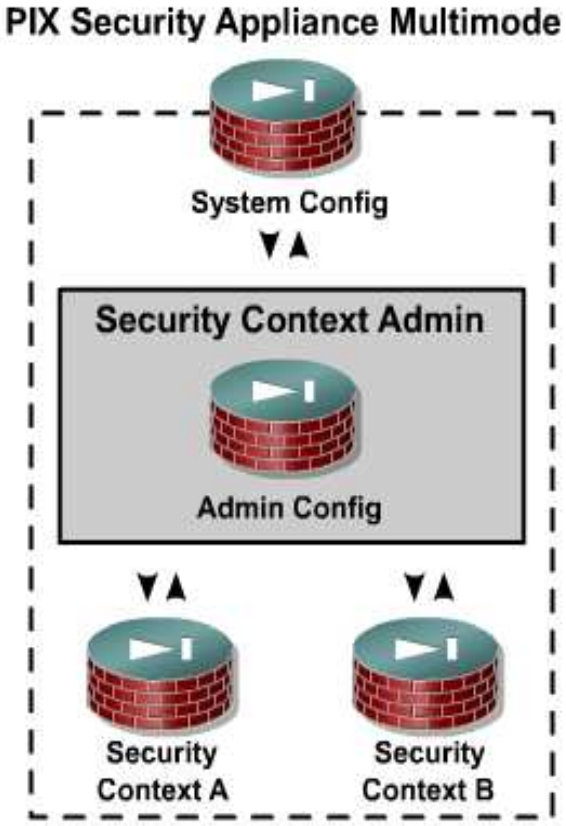
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Admin Context

Cisco.com

The Admin Context has the following characteristics:

- The system execution space has no traffic passing interfaces, and uses the policies and interfaces of the admin context to communicate with other devices.
- Used to fetch configs for other contexts and send system level syslogs.
- Users logged in to the admin context are able to change to the system context and create new contexts.
- Since the admin context is special, it doesn't count against the licensed firewall count.
- Aside from it's significance to the system, it could be used as a regular context.




Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Enabling Multiple Context Mode

Cisco.com

**pixfirewall(config)#**

```
mode {single | multiple} [noconfirm]
```

Selects the Context Mode as follows:

- multiple—Sets multiple context mode; mode with security contexts
- single—Sets single context mode; mode without security contexts
- noconfirm—Sets the mode without prompting you for confirmation.

Before you convert from multiple mode to single mode, you must copy the backup version of the original running configuration to the current startup configuration.

```
pixfirewall(config)# mode multiple
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Adding a Context

Cisco.com

pixfirewall(config)#

```
context name
```

Adds or modifies a context.

- name—A string up to 32 characters long (case sensitive).
  Note:
  - "System" is a reserved name, and cannot be used.

```
pixfirewall(config)# context context1
Creating context 'context1'... Done. (4)
pixfirewall(config-ctx)#
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Removing a Context

Cisco.com

**pixfirewall(config)#**

```
no context name
```

- You can only remove a context by editing the system configuration.
- You cannot remove the current admin context, unless you remove all contexts.
- Contexts can be removed or created on the fly, no reboot is required

```
pixfirewall(config)# no context context3
WARNING: Removing context 'context3'
Proceed with removing the context? [confirm]
```

**pixfirewall(config)#**

```
clear configure context
```

- Removes all contexts, including the admin context.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Changing the Admin Context

Cisco.com

pixfirewall(config)#

```
admin-context name
```

- You can set any context to be the admin context.

```
pixfirewall(config)# admin-context context2
pixfirewall(config)# wr t
...
admin-context context2
context context2
allocate-interface GigabitEthernet0/0
allocate-interface GigabitEthernet0/1
allocate-interface GigabitEthernet0/3
config-url disk0:/context2.cfg
...
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Changing Between Contexts

Cisco.com

**pixfirewall(config)#**

```
changeto {system | context name}
```

- Changes the environment to the context specified.

```
pixfirewall(config)# changeto context context1
pixfirewall/context1(config)#
```

- Also changes the environment to the system execution space.

```
pixfirewall/context1(config)# changeto context system
pixfirewall(config)#
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Viewing Context Information

Cisco.com

pixfirewall(config)#

```
show context [name [detail]| count]
```

- View all contexts.
- An "*" designates an admin context.

```
pixfirewall(config)# show context
Context Name Interfaces URL
*admin GigabitEthernet0/0,GigabitEthernet0/1
disk0:/admin.cfg
context1
GigabitEthernet0/0,GigabitEthernet0/1,GigabitEthernet0/
3 disk0
:/context1.cfg
context2
GigabitEthernet0/0,GigabitEthernet0/1,GigabitEthernet0/
3 disk0
:/context2.cfg
Total active Security Contexts: 3…
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems Networking Academy

Cisco.com

# Module 8 – PIX Security Appliance Contexts, Failover, and Management

## 8.2 Configure PIX Security Appliance Failover

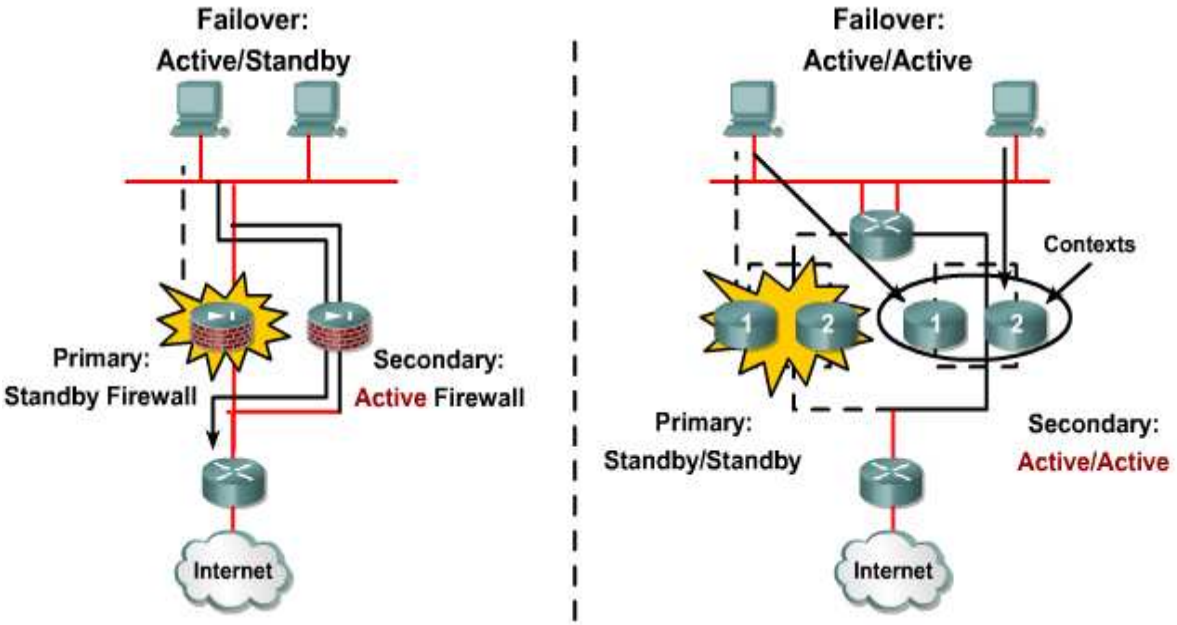
CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

HÖGSKOLAN HALMSTAD

# Hardware Failover

Cisco.com

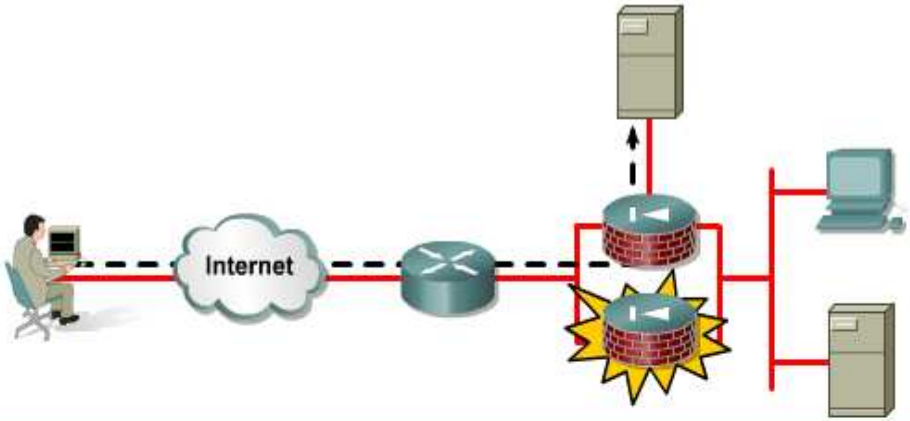



- Hardware failover protects the network should the primary go offline.
  - Active/Standby—only one unit can be actively processing traffic while other is hot standby.
  - Active/Active—both units can process traffic and serve as backup units.
- Stateful failover maintains session state during failover.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Hardware and Stateful Failover

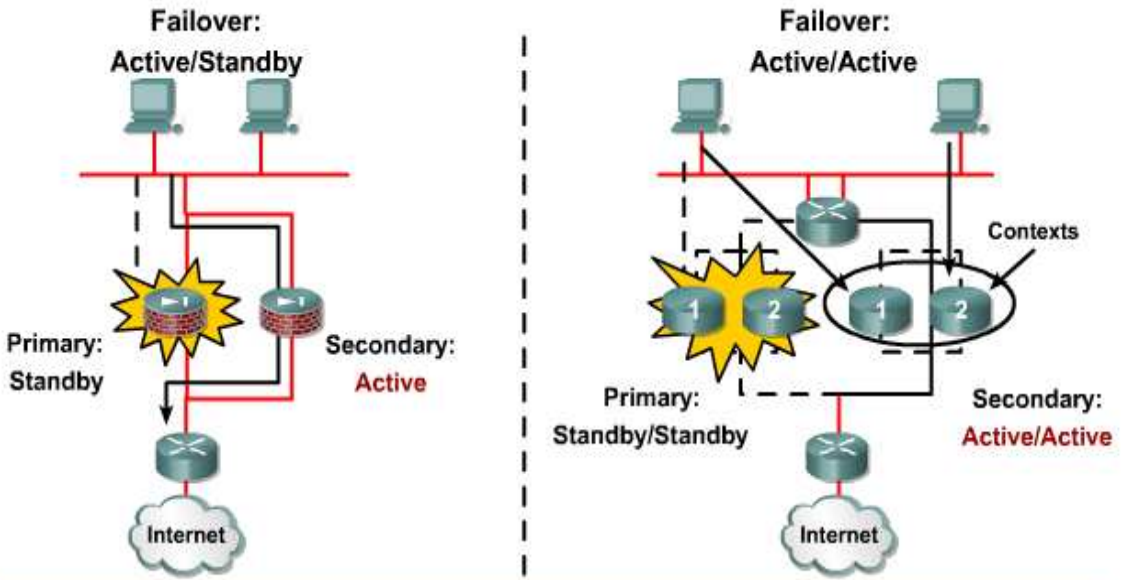





- Hardware Failover
  - Connections are dropped.
  - Client applications must reconnect.
  - Provides hardware redundancy.
  - Provided by serial or LAN-based cabling.
- Stateful failover
  - TCP connections remain active.
  - No client applications need to reconnect.
  - Provides redundancy and stateful connection.
  - Provided by LAN-based failover.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Failover Requirements

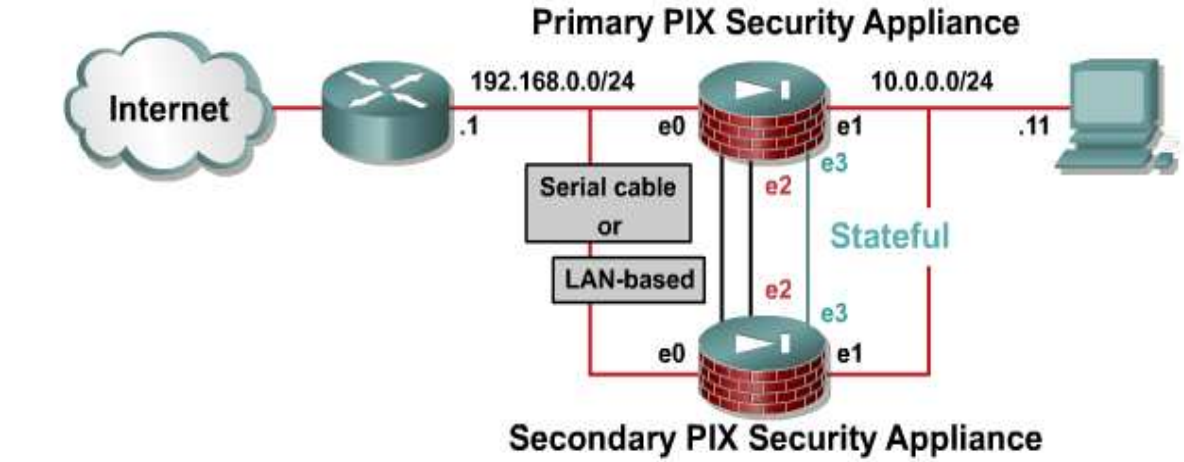


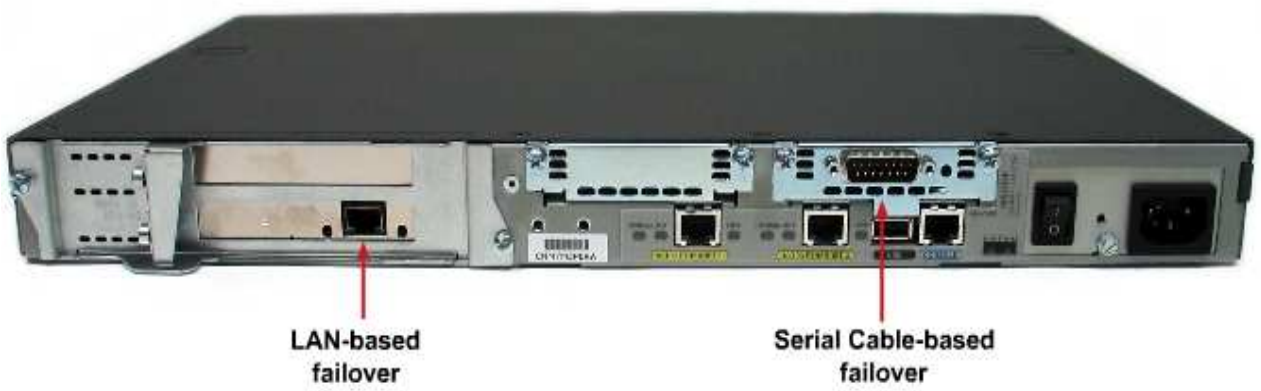

The primary and secondary PIX Security Appliances must be identical in the following requirements:

- Same model number
- Identical software versions
- Same activation keys (DES or 3DES)
- Same amount of Flash memory and RAM
- Proper licensing

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Types of Failover Cabling

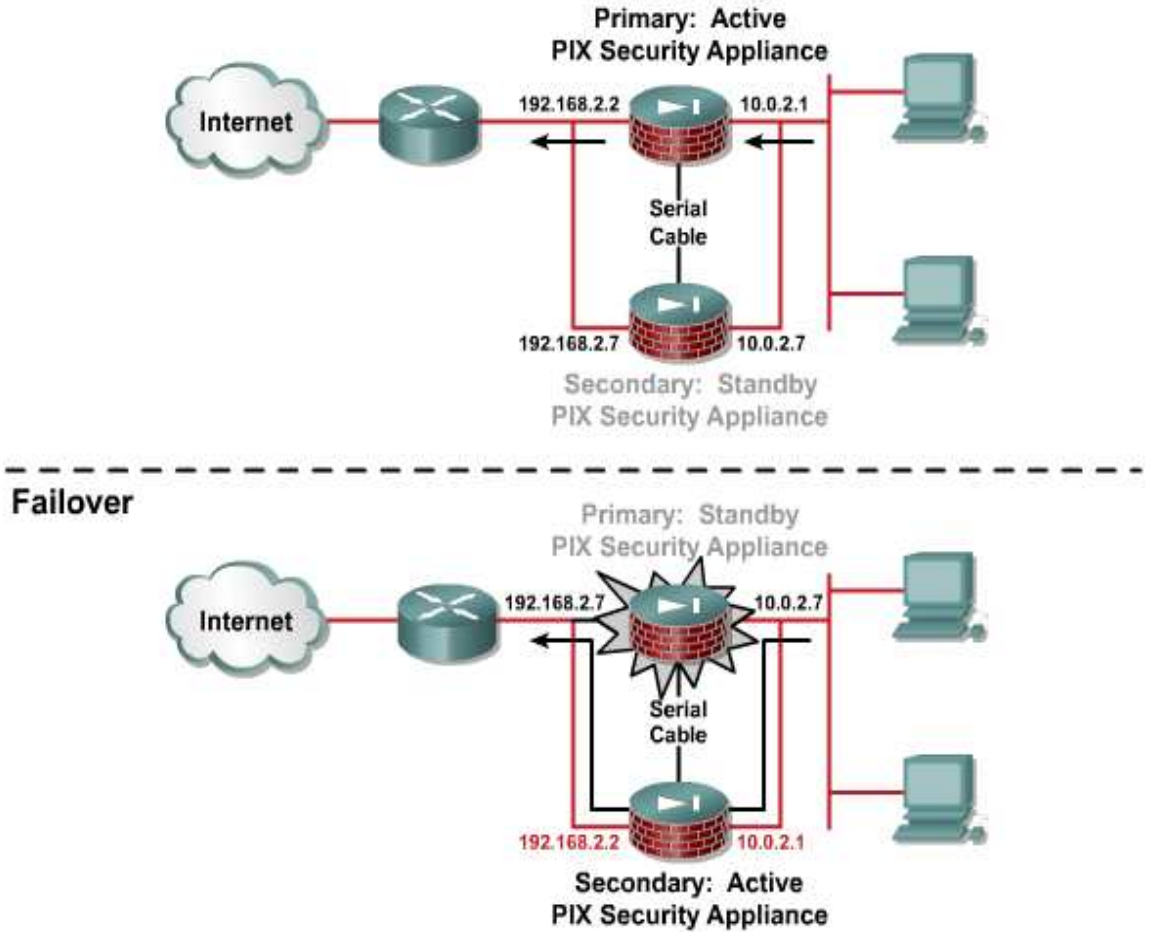



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Serial Cable – Active/Standby Failover

Cisco.com




Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# LAN-Based Failover

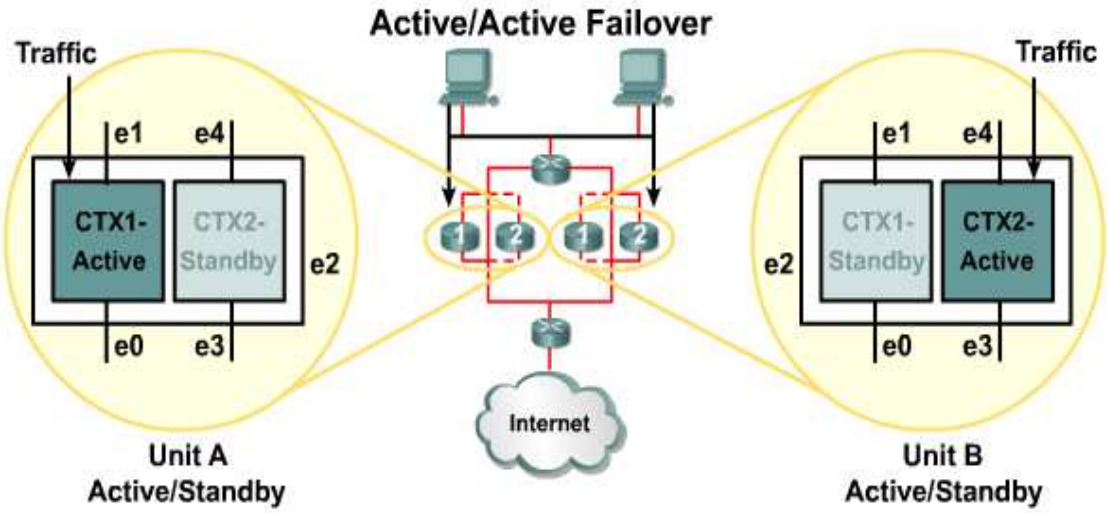


- Provides long-distance failover functionality
- Uses an Ethernet cable rather than the serial failover cable
- Requires a dedicated LAN interface, but the same interface can be used for stateful failover
- Requires a dedicated switch, hub, or VLAN
- Uses message encryption and authentication to secure failover transmissions

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Active/Active Failover






Active/active failover requires the use of contexts

- For example, two security appliances with 2 contexts each
  - CTX1
  - CTX2

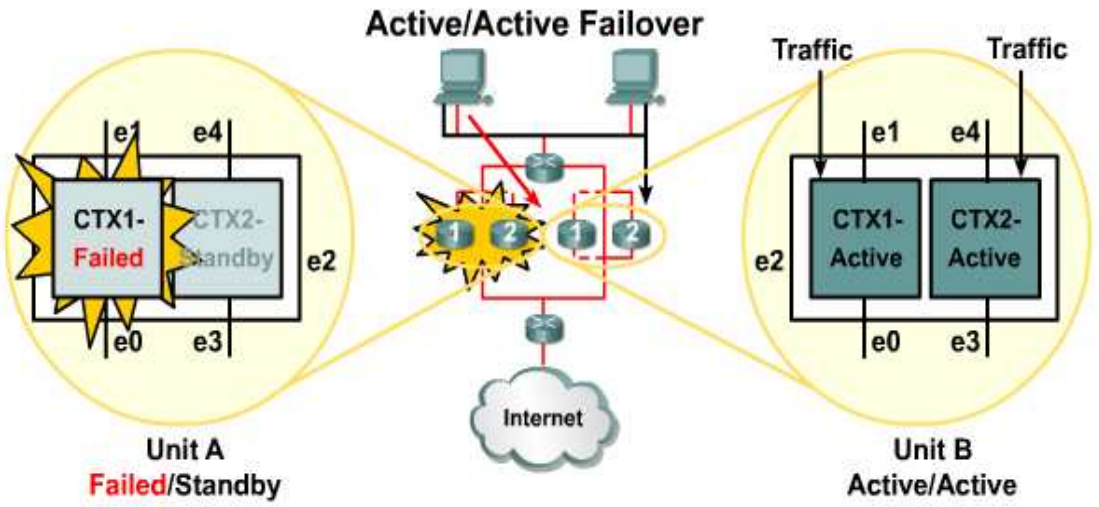
Normal Conditions,

- Each security appliance has one active and one standby context
  - Active context processes traffic.
  - Standby context is located in the peer security appliance.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Active/Active Failover






**Under failed conditions,**

- Unit A determines outside interface on CTX1 has failed.
  - CTX1 is placed in failed state.
  - Unit A has one failed and one standby context.
- Unit B, CTX1 becomes active.
  - Unit B has two active contexts.
  - Both active contexts pass traffic.

**Failover can be context-based or unit based.**

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems Networking Academy

Cisco.com

# Module 8 – PIX Security Appliance Contexts, Failover, and Management

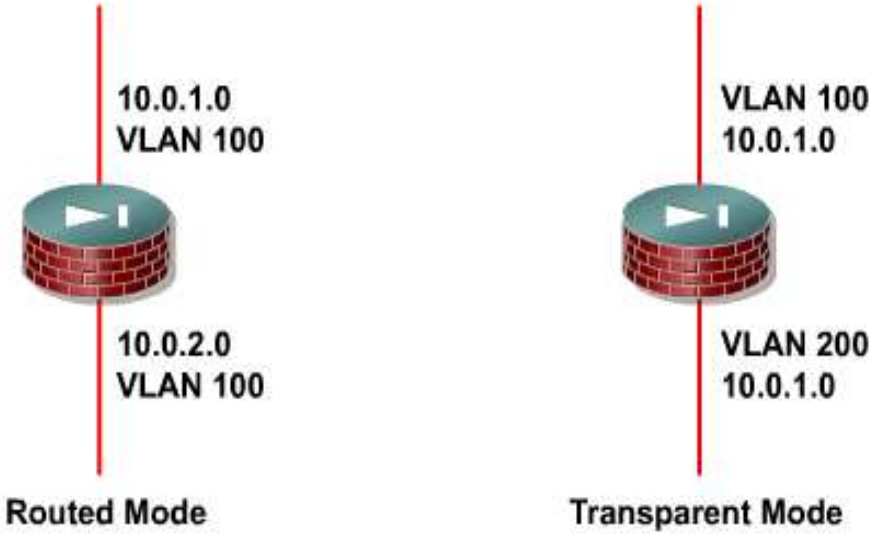
# 8.3 Configure Transparent Firewall Mode

CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Högskolan Halmstad

# Transparent Versus Routed Firewall




**The PIX Security Appliance can run in two firewall settings:**

- Routed–Based on IP Address
- Transparent–Based on MAC Address

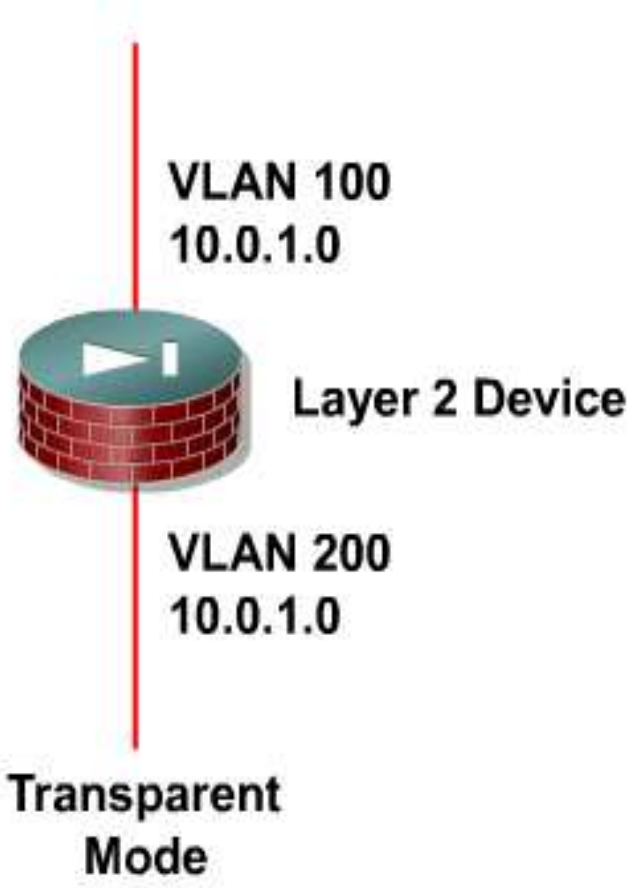
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Transparent Firewall Benefits

Cisco.com

Easily integrated and maintained in existing network:

- IP readdressing not necessary.
- No NAT to configure.
- No IP routing to troubleshoot.

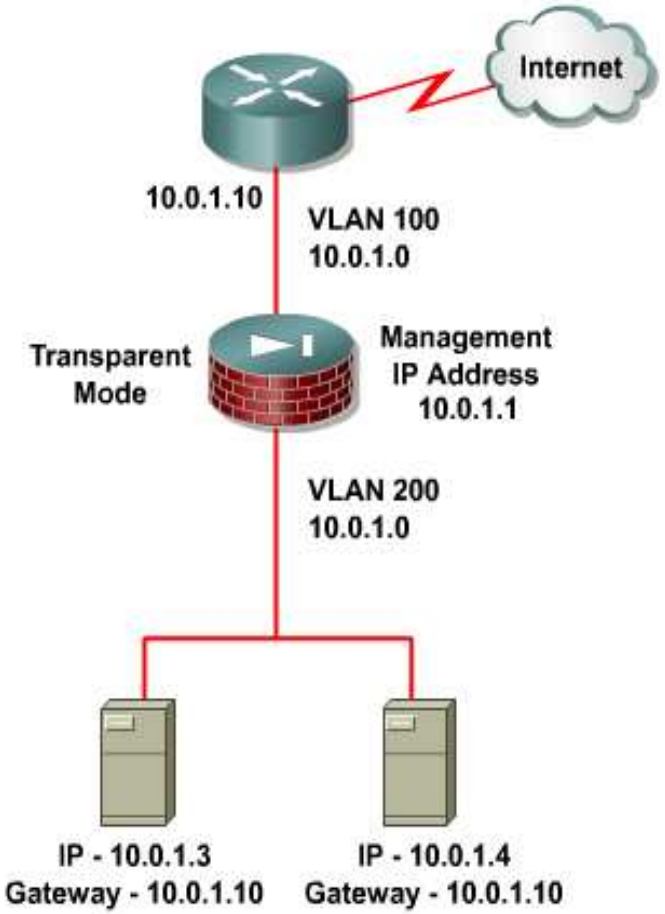



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Transparent Firewall Guidelines



- Layer 3 traffic must be explicitly permitted.
- Each directly connected network must be on the same subnet.
- A management IP address is required for each context, even if you do not intend to use Telnet to the context.
- The management IP address must be on the same subnet as the connected network.
- Do not specify the PIX management IP address as the default gateway for connected devices.
- Devices need to specify the router on the other side of the PIX as the default gateway.
- Each interface must be a different VLAN interface



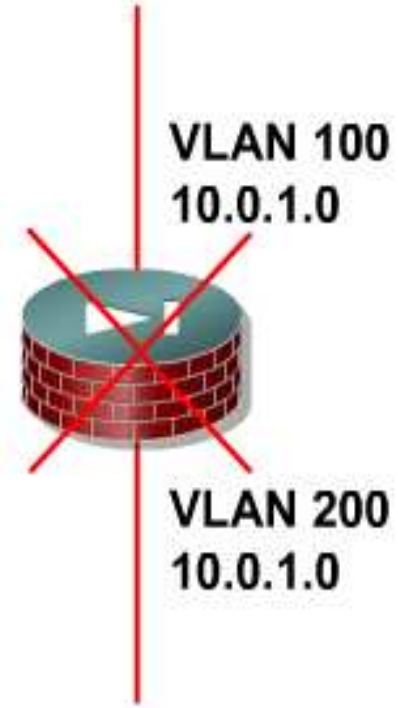

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Unsupported Features

Cisco.com

The following features are not supported in transparent firewall mode:

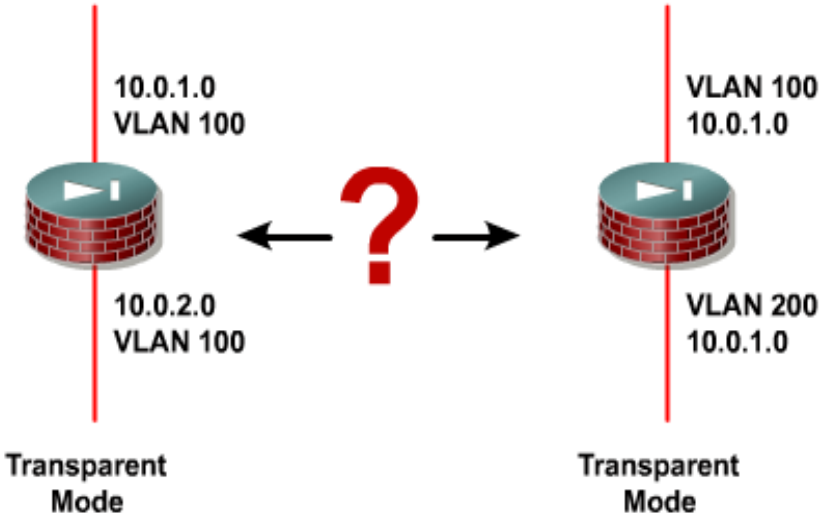
- NAT
- Dynamic routing protocols
- IPv6
- DHCP relay
- Quality of Service
- Multicast
- VPN termination for through traffic




Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# View the Current Firewall Mode






**pixfirewall(config)#**

```
show firewall
```

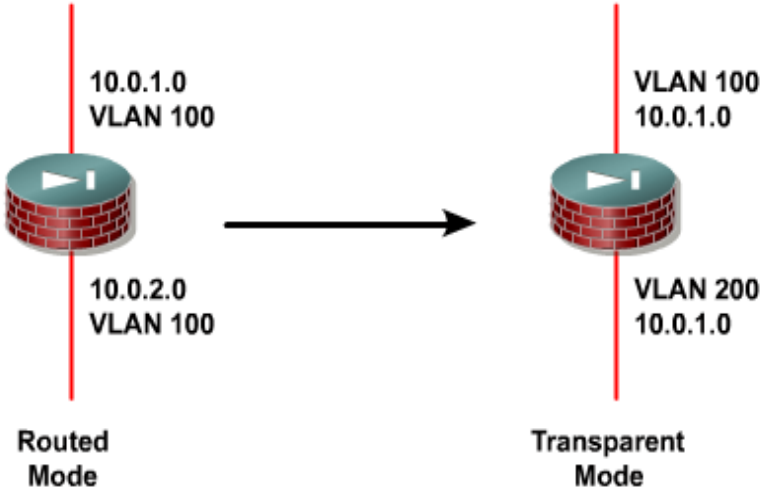
- Shows the current firewall transparent mode.

```
pixfirewall(config)# show firewall
Firewall mode: Transparent
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Enable Transparent Firewall Mode






pixfirewall(config)#

```
firewall transparent
```

- Use no firewall transparent command to return to router

```
pixfirewall(config)# firewall transparent
Switched to transparent mode
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Assigning the Management IP Address

Cisco.com

**pixfirewall(config)#**

```
ip address ip_address [mask] [standby ip_address]
```

- Sets the IP address for an interface (in routed mode) or for the management address (transparent mode).
- Note the following:
  - For routed mode, enter this command in interface configuration mode.
  - In transparent mode, enter this command in global configuration mode.

```
pixfirewall(config)# ip address 10.0.1.1 255.255.255.0
pixfirewall(config)# show ip address
Management System IP Address:
   ip address 10.0.1.1 255.255.255.0
Management Current IP Address:
   ip address 10.0.1.1 255.255.255.0
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Configure ACLs

Cisco.com


**pixfirewall(config)#**

```
access-list id [line line-number] [extended] {deny |
permit} {object-group network_obj_grp_id |
protocol} source_address mask dest_address mask
```

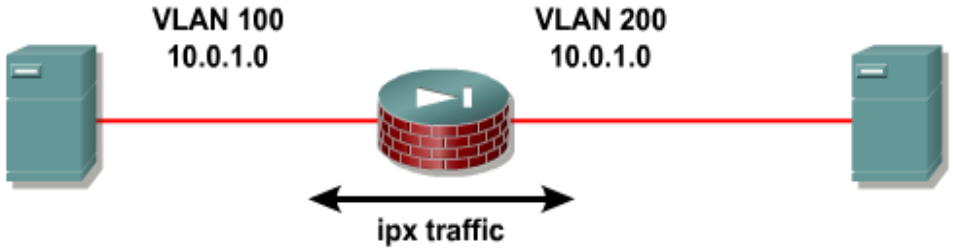
- Determine what traffic should be allowed through the firewall.
- Remember that by default, no traffic is allowed through the firewall – regardless of the security level assigned to the interfaces.

```
pixfirewall(config)# access-list ACLIN permit icmp 10.0.1.0
255.255.255.0 10.0.1.0 255.255.255.0
pixfirewall(config)# access-group ACLIN in interface inside
pixfirewall(config)# access-group ACLIN in interface outside
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Ethertype ACLs






**pixfirewall(config)#**

```
access-list id ethertype {deny | permit} {ipx | bpdu |
mpls-unicast | mpls-multicast | any | hex_number}
```

Treatment of non-IP packets:

- The transparent firewall introduces a new type of access-list: the ethertype access-list.
- Ethertype access-lists allow an administrator can allow specific non-IP packets through the firewall.

```
pixfirewall(config)# access-list ETHER ethertype permit ipx
pixfirewall(config)# access-group ETHER in interface inside
pixfirewall(config)# access-group ETHER in interface outside
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# ARP Inspection

Cisco.com

**pixfirewall(config)#**

```
arp interface_name ip_address mac_address [alias]
```

- A static ARP entry maps a MAC address to an IP address and identifies the interface through which the host is reached.

```
pixfirewall(config)# arp outside 10.0.1.1 0009.7cbe.2100
```

**pixfirewall(config)#**

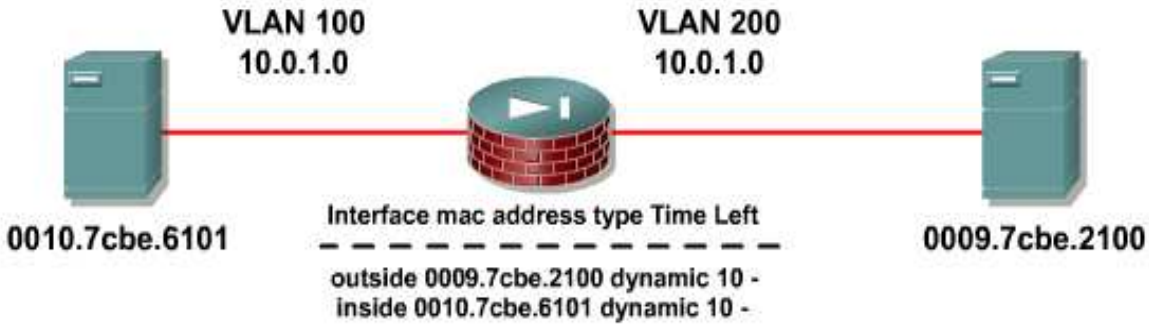
```
arp-inspection intereface_name enable [flood | no-flood]
```

- ARP inspection checks all ARP packets against static ARP entries and blocks mismatched packets.
- This feature prevents ARP spoofing.

```
pixfirewall(config)# arp-inspection outside enable
arp inspection enabled on outside
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# MAC Address Table




**The MAC address table is used to find out the outgoing interface based on destination MAC address.**

- Built on the fly, learned from source mac address.
- No flooding if MAC address not found.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Disable MAC Address Learning




pixfirewall(config)#

```
mac-learn interface_name disable
no mac-learn interface_name disable
```

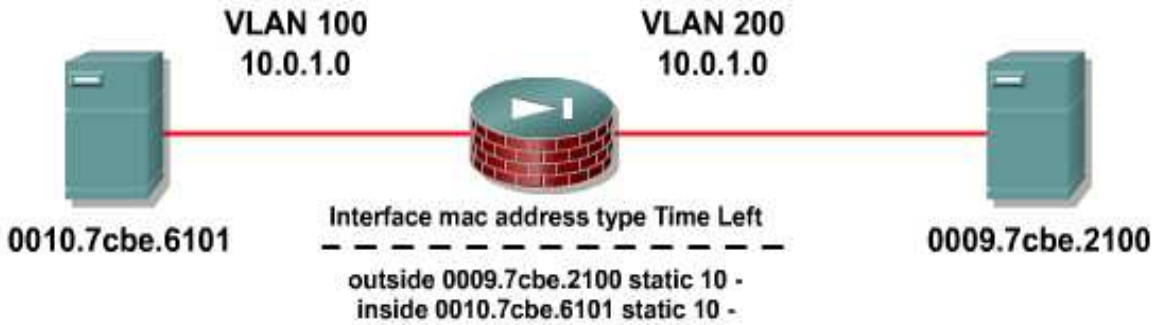
- Disables MAC address learning for an interface.
- To reenable MAC address learning, use the `no` form of this command.
- By default, each interface automatically learns the MAC addresses of entering traffic, and the pix security appliance adds corresponding entries to the MAC address table.

```
pixfirewall(config)# mac-learn outside disable
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Adding a Static MAC Address

Cisco.com




pixfirewall(config)#

```
mac-address-table static interface_name mac_address
```

- Adds a static entry to the MAC address table,
- Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface.
- Guard against MAC spoofing.

```
pixfirewall(config)# mac-address-table static inside
0010.7cbe.6101
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# Viewing the MAC Address Table

Cisco.com

pixfirewall(config)#

```
show mac-address-table [interface_name]
```

- Shows the MAC address table.

```
pixfirewall(config)# show mac-address-table
interface mac address type Time Left
------------------------------------------------------
-
outside 0009.7cbe.2100 static -
inside 0010.7cbe.6101 dynamic 10
fw1# show mac-address-table inside
interface mac address type Time Left
------------------------------------------------------
--
inside 0010.7cbe.6101 dynamic -
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

# debug Commands



**Debug Support:**

- **`debug arp-inspection`**—To track code path of arp forwarding and arp inspection module in transparent firewall.
- **`debug mac-address-table`**—To track insert/delete/update to the bridge table maintained for transparent firewall.

```
pixfirewall(config)# debug arp-inspection
pixfirewall(config)# debug mac-address-table
```

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se