Cisco Systems
Networking Academy

Cisco.com

Module 3 – Security Devices

3.4 Getting Started with the PIX Security Appliance

CCNA CISCO CERTIFIED™

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

User Interface

- Unprivileged mode – This mode is available when the PIX is first accessed. The > prompt is displayed. This mode provides a restricted, limited, view of PIX settings.
- Privileged mode – This mode displays the # prompt and enables users to change the current settings. Any unprivileged command also works in privileged mode.
- Configuration mode – This mode displays the (config)# prompt and enables users to change system configurations. All privileged, unprivileged, and configuration commands work in this mode.
- Monitor mode – This is a special mode that enables users to update the image over the network or to perform password recovery. While in the monitor mode, users can enter commands specifying the location of the TFTP server and the PIX software image or password recovery binary file to download.

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

Security Levels

- Higher security level interface to a lower security level interface – For traffic originating from the inside interface of the PIX with a security level of 100 to the outside interface of the PIX with a security level of 0, all IP-based traffic is allowed unless it is restricted by ACLs, authentication, or authorization.
- Lower security level interface to a higher security level interface – For traffic originating from the outside interface of the PIX with a security level of 0 to the inside interface of the PIX with a security level of 100,all packets are dropped unless specifically allowed by an `access-list` command. The traffic can be restricted further if authentication and authorization is used.
- Same secure interface to a same secure interface – No traffic flows between two Interfaces with the same security level.

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

Basic Commands

- `hostname` – assigns a hostname to the PIX.
- `interface` – Configures the type and capability of each perimeter interface.
- `nameif` – Assigns a name to each perimeter interface.
- `ip address` – Assigns an IP address to each interface.
- `security level` – Assigns the security level for the perimeter interface.
- `speed` – Assigns the connection speed.
- `duplex` – Assigns the duplex communications.

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

Additional Commands

- `nat-control` – Enable or disable NAT configuration requirement.
- `nat` – Shields IP addresses on the inside network from the outside network.
- `global` – Creates a pool of one or more IP addresses for use in NAT and PAT.
- `route` – Defines a static or default route for an interface.

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

Cisco Systems
Networking Academy

Cisco.com

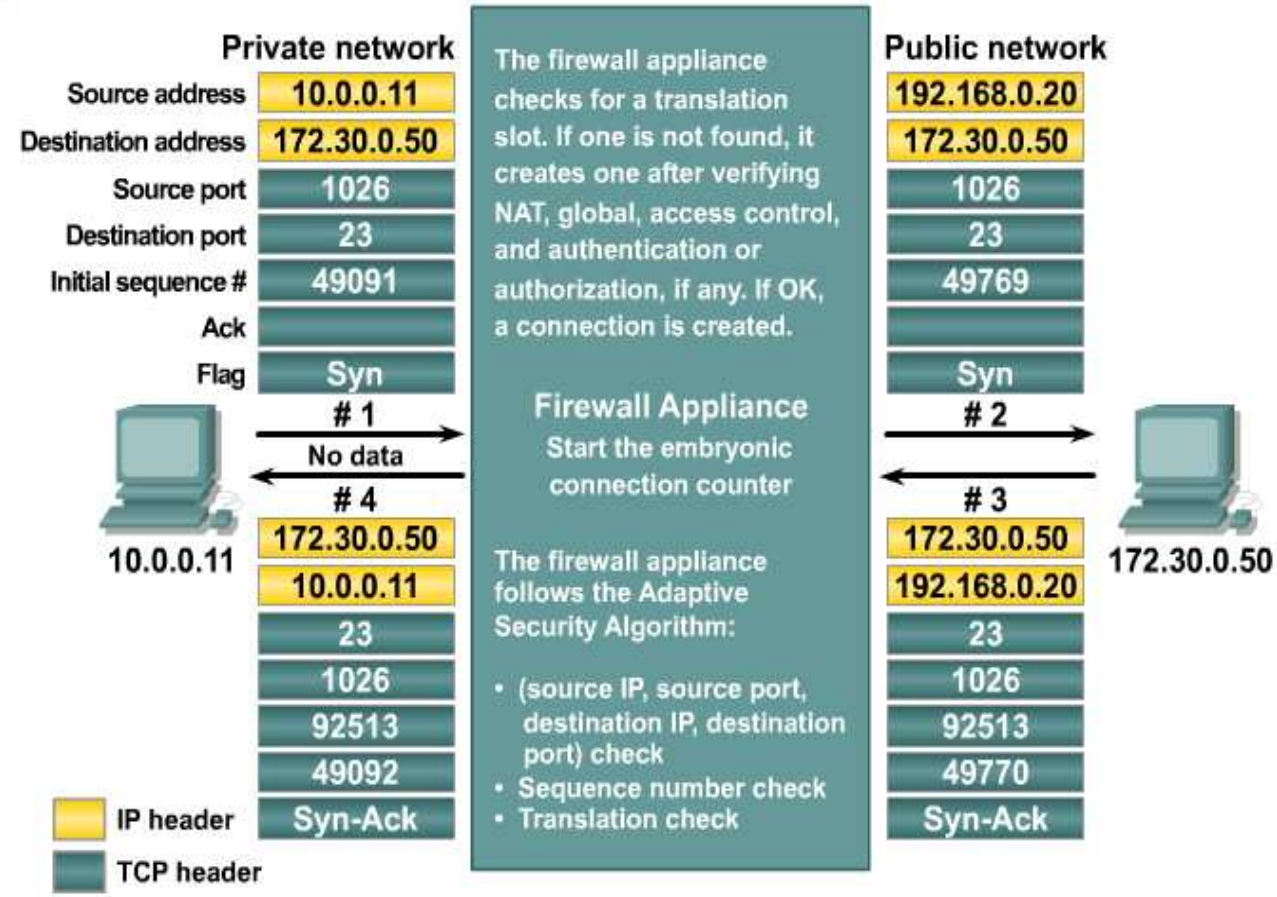
Module 3 – Security Devices

3.5 PIX Security Appliance Translations and Connections

CCNA CISCO CERTIFIED™

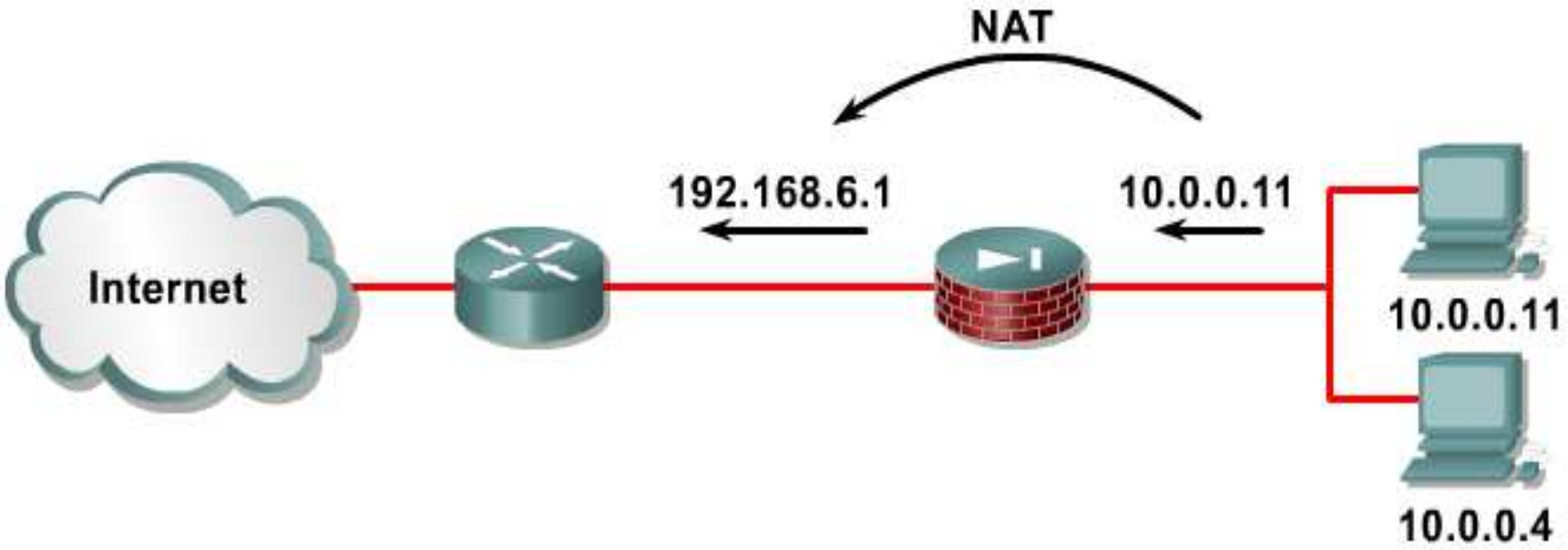
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

UDP



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

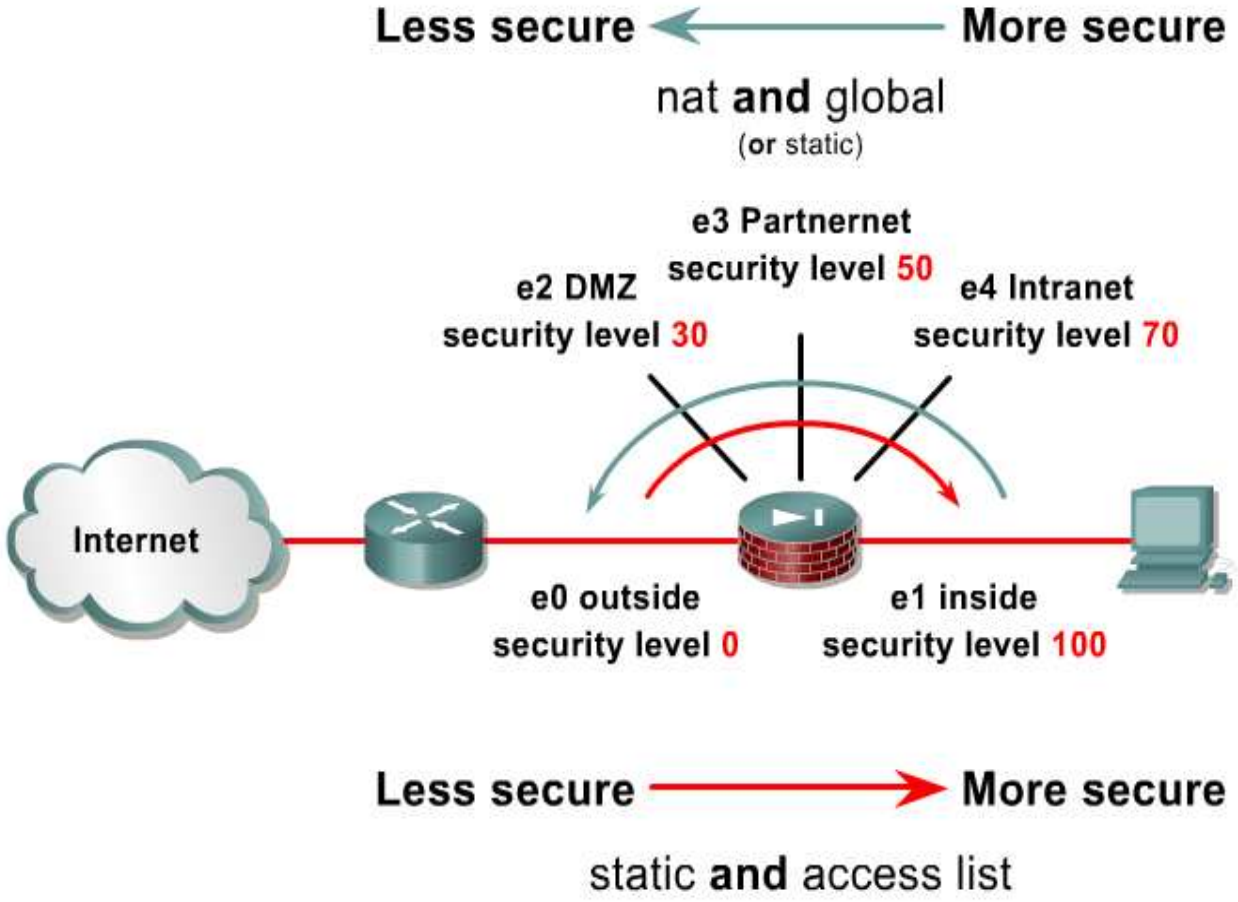
NAT



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

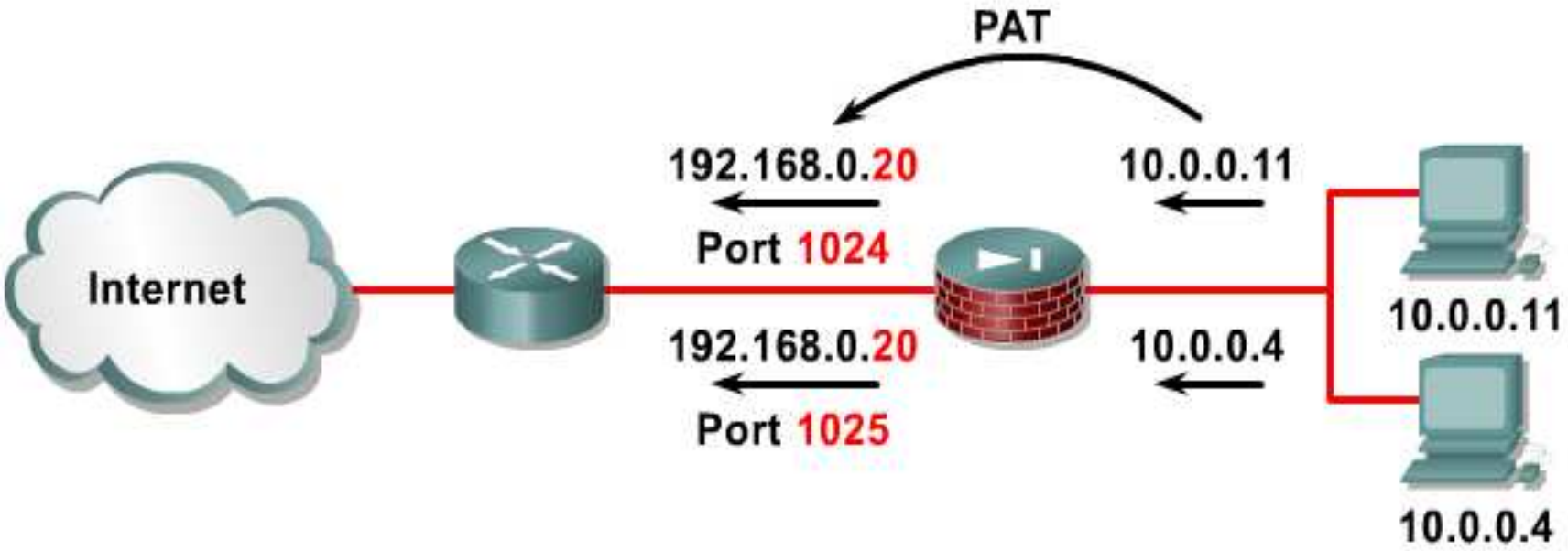
Access through the PIX Security Appliance

Cisco.com



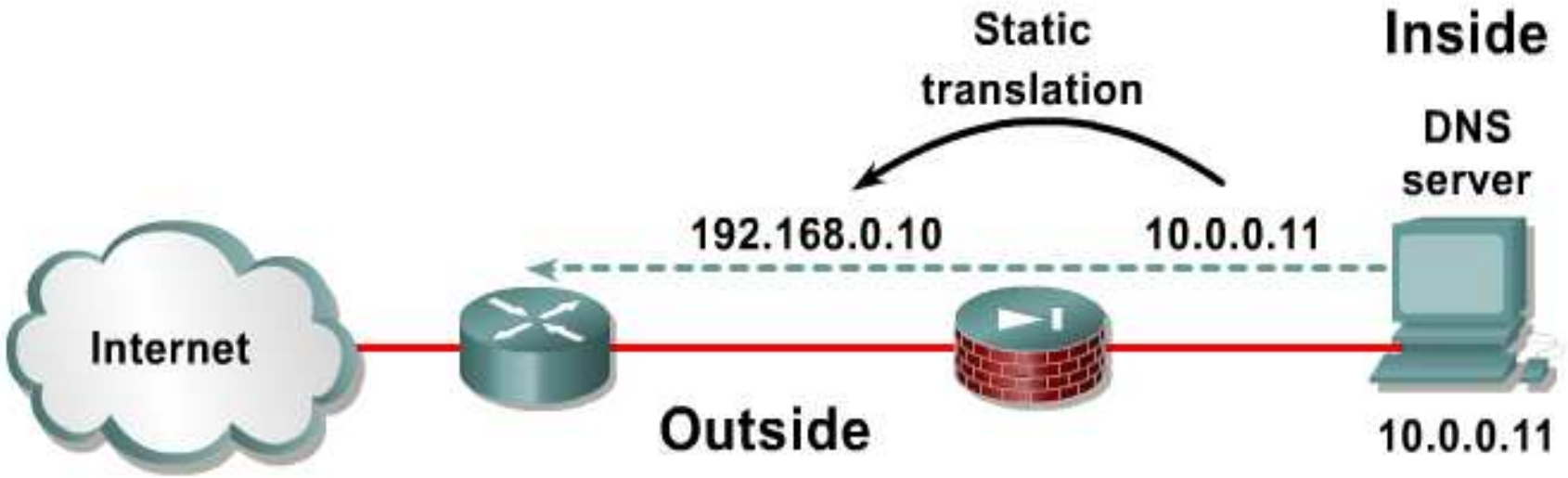
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

PAT



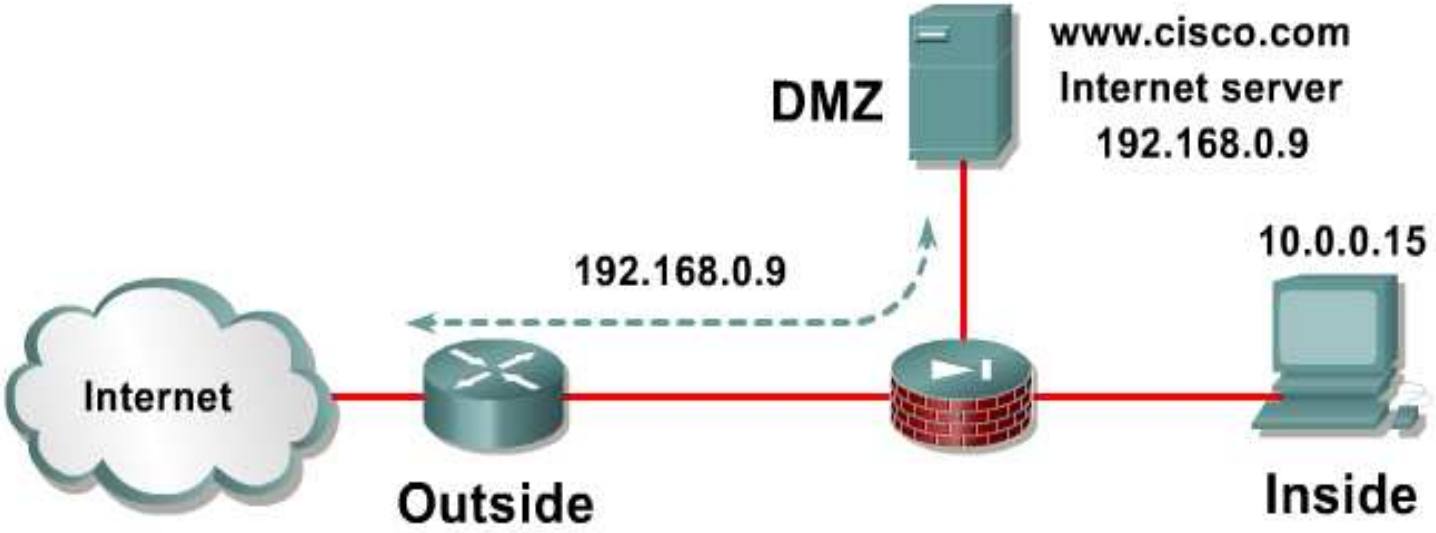
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Static Translation



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

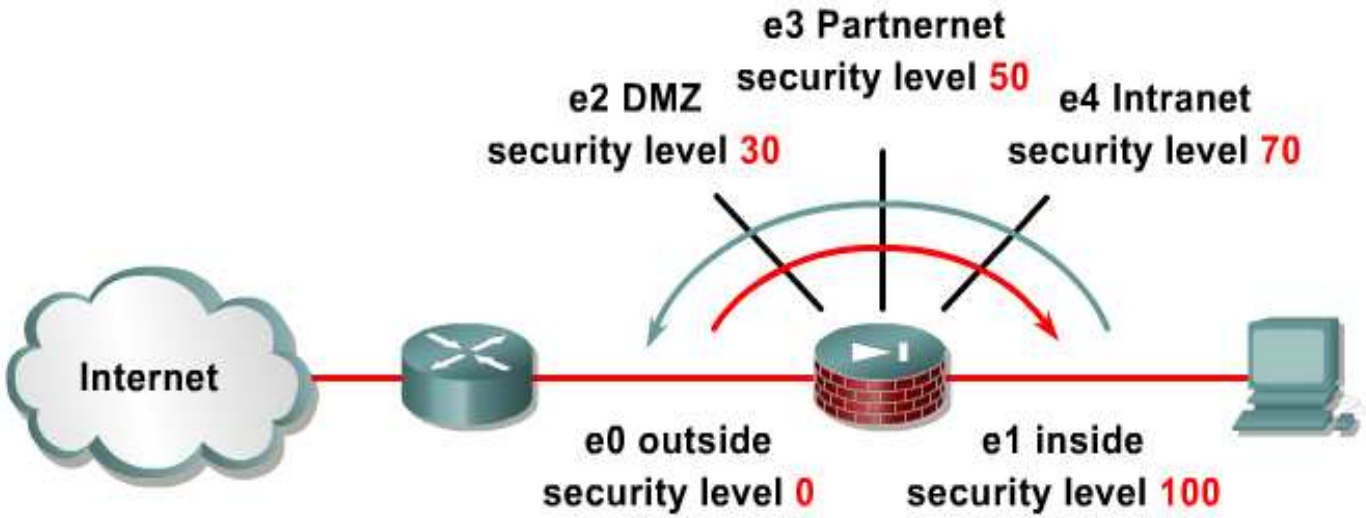
Identity NAT



- Identity NAT is used to create a transparent mapping.
- IP addresses on the high security interface translate to themselves on ALL lower security interfaces.

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

Multiple Interfaces



- Supports additional interfaces.
- Increases the security of publicly available services.
- Easily interconnects multiple extranets or partner networks.
- Easily configured with standard firewall appliance commands.

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

Cisco Systems
Networking Academy

Cisco.com

Module 3 – Security Devices

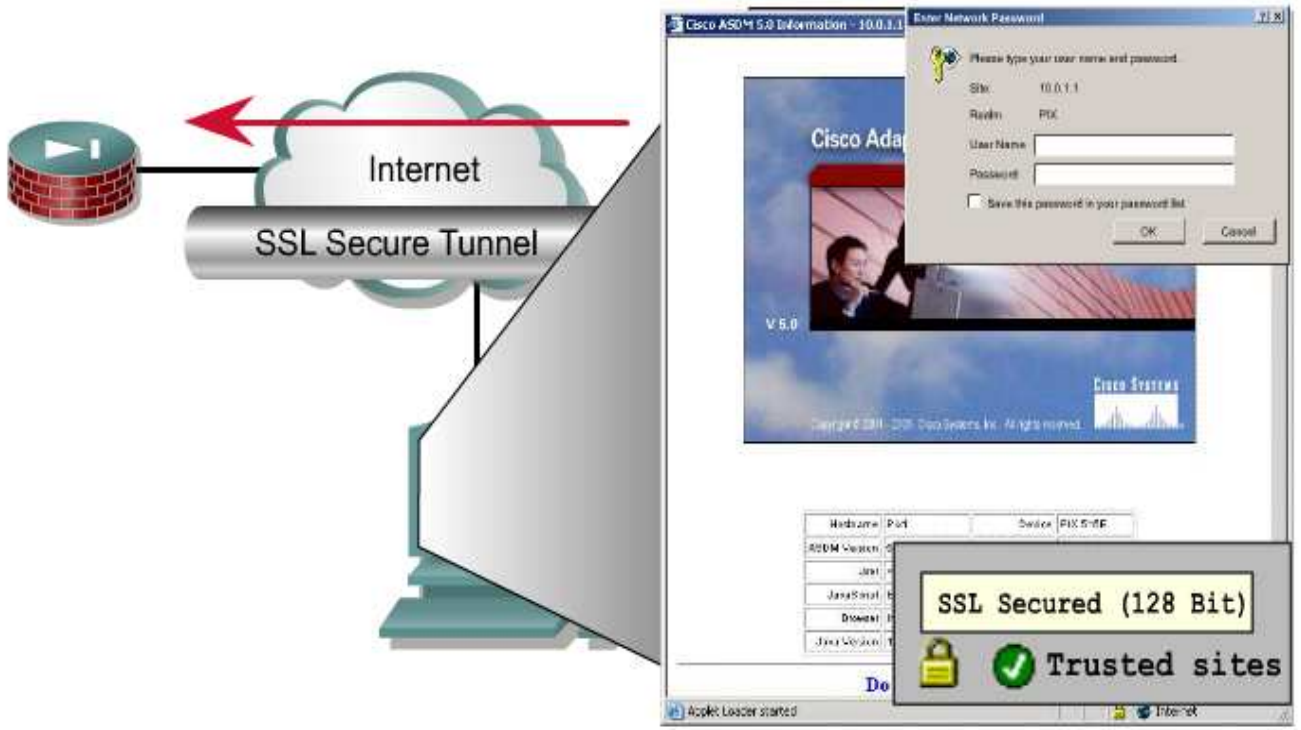
3.6 Manage a PIX Security Appliance with Adaptive Security Device Manager

CCNA CISCO CERTIFIED™

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

Adaptive Security Device Manager (ASDM)

Cisco.com



ASDM is a browser-based configuration tool designed to help configure and monitor the security appliance.

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

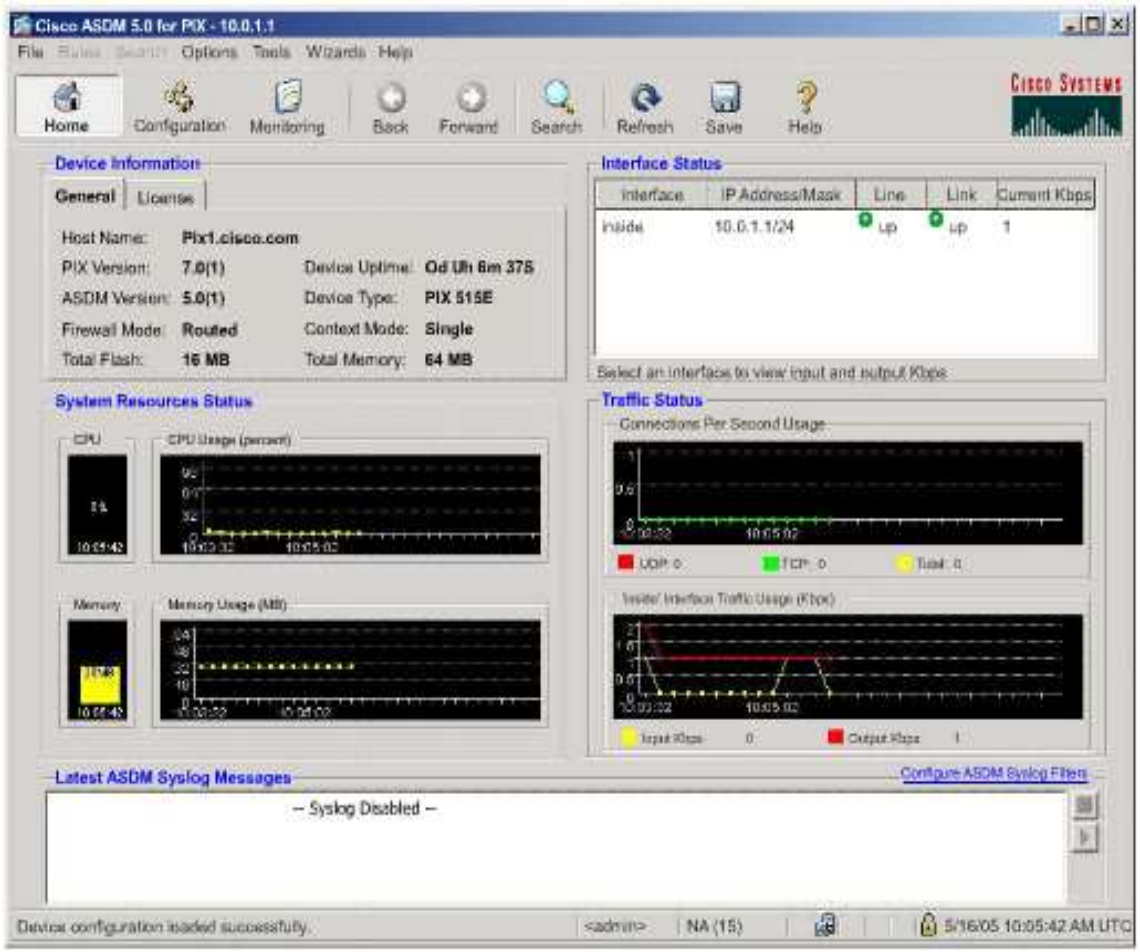
ASDM Compatibility

Cisco.com

DM Version	Security Appliance SW Version	Security Appliance Model
PDM 1.0	6.0 or 6.1	506, 515, 520, 525, 535
PDM 1.1	6.0 or 6.1	506, 515, 520, 525, 535
PDM 2.0	6.2	501,506/506E, 515/515E, 520, 525, 535
PDM 2.1	6.2	501,506/506E, 515/515E, 520, 525, 535
PDM 3.0	6.3	501,506/506E, 515/515E, 520, 525, 535
ASDM 5.0	**7.0**	515/515E, 520, 525, 535, 5510, 5520, 5540

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

ASDM Home Window



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

Cisco Systems
Networking Academy

Cisco.com

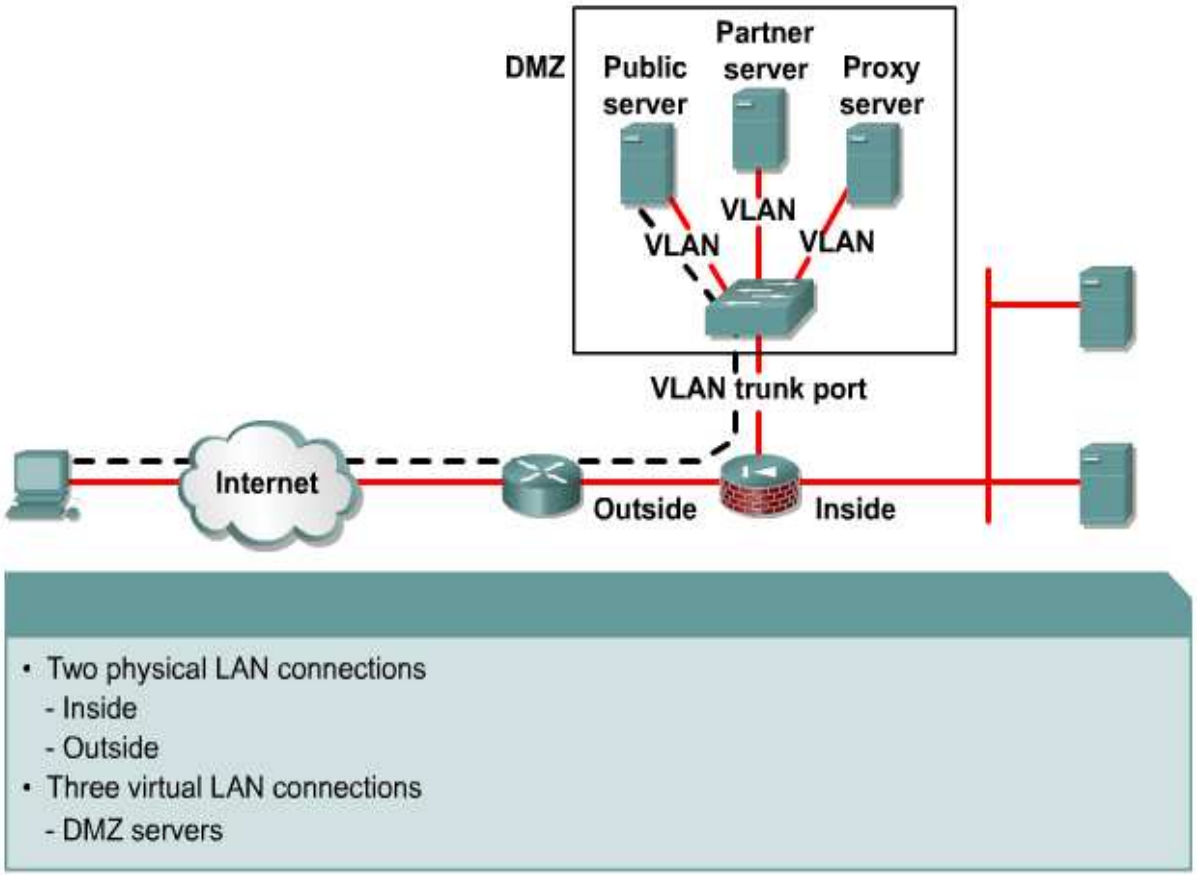
Module 3 – Security Devices

3.7 PIX Security Appliance Routing Capabilities

CCNA CISCO CERTIFIED™

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

VLANs

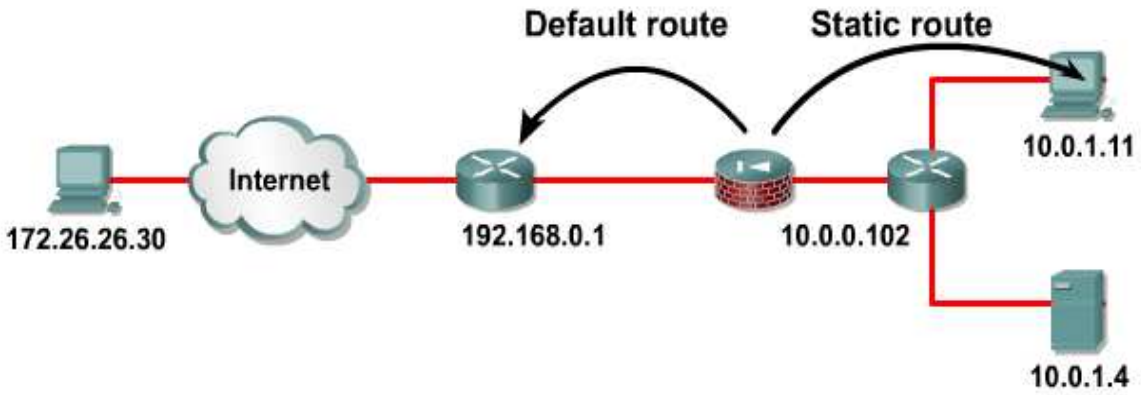


- Two physical LAN connections
  - Inside
  - Outside
- Three virtual LAN connections
  - DMZ servers

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

Static Routes

Cisco.com



pixfirewall(config)#

```
route interface_name ip_address netmask gateway_ip
  [metric]
```

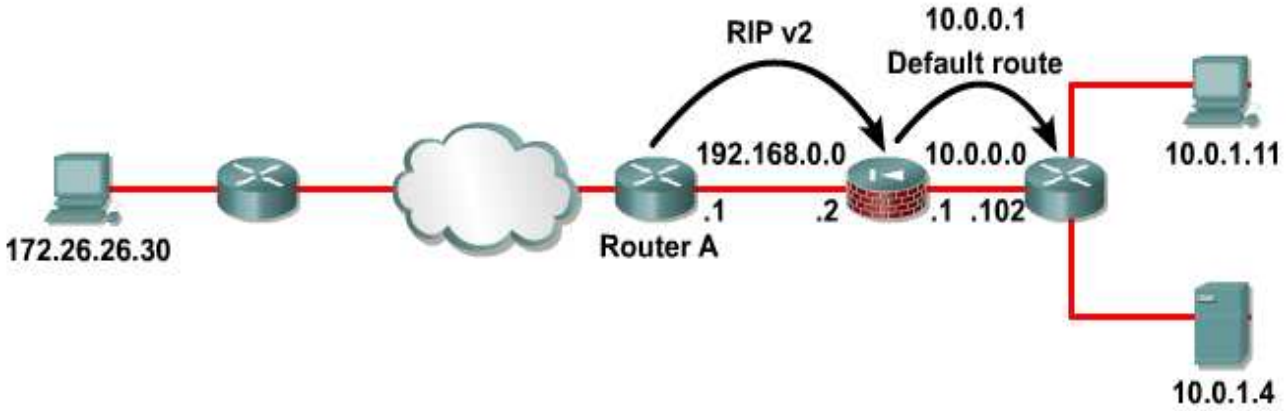
- Defines a static or default route for an interface

```
pixfirewall(config)# route outside 0.0.0.0 0.0.0.0
  192.168.0.1 1
pixfirewall(config)# route inside 10.0.1.0 255.255.255.0
  10.0.0.102 1
```

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

Routing with RIP

Cisco.com



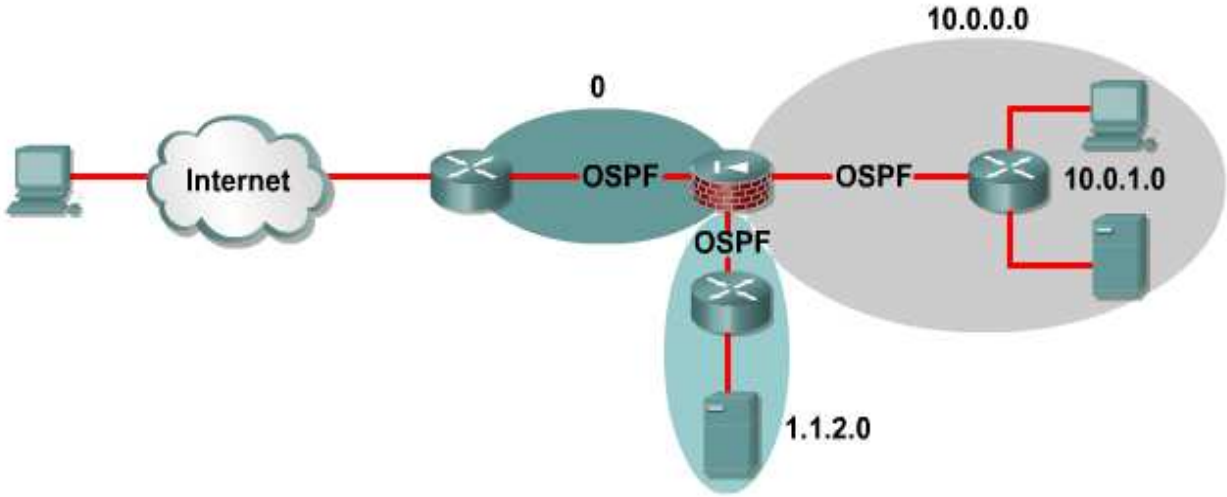

```
pix1(config)# rip outside passive version 2 authentication md5 MYKEY 2
pix1(config)# rip inside default
```

- The PIX Firewall accepts encrypted RIP version 2 multicast updates. For example, it could learn the route to network 172.26.26.0 from router A.
- The PIX Firewall broadcasts IP address 10.0.0.1 as the default route for devices on the inside interface.

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

Routing with OSPF

Cisco.com



PIX Security Appliance OSPF two-process criteria:

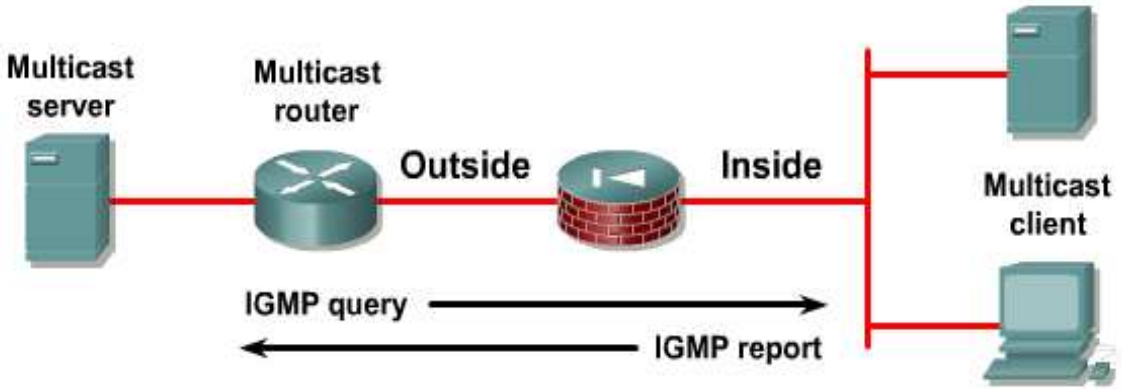
- NAT is used.
- OSPF is operating on public and private areas.
- LSA type 3 filtering is required.

Run two OSPF processes:

- One process is for public areas.
- One process is for the private areas.

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

Multicast Routing



- An IP datagram is transmitted to a set of hosts identified by a single IP destination address.
- Clients that wish to receive multicasts must join a multicast host group.
- Multicast router discovers group hosts by sending IGMP query messages.
- Host group members respond with IGMP reports.
- The PIX Security Appliance supports Stub Multicast Routing—IGMP proxying.

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