

PIX and ASA 7.x

A guide to the new features



- ▶ Getting 7.x software up and running
- ▶ Overview of the changes between version 6.3 and 7.x
- ▶ Practical examples using 7.x features

Getting 7.x Software Up and Running



- ▶ Hardware Platforms:
 - PIX 515/515E
 - PIX 525
 - PIX 535
 - ASA 5500 series (5510, 5520, 5540)
- ▶ PIX 501 and 506e are not supported



Memory Requirements for PIX 515e

- ▶ 6.3 software can only see 8mb Flash
- ▶ 7.x software 'unlocks' Flash to 16mb
- ▶ RAM requirements depend on license:
 - Restricted 32mb must become 64mb
 - Unrestricted and/or Failover 64mb must become 128mb
- ▶ Software upgrade is free (SmartNet)
- ▶ Memory upgrade must be purchased



Upgrade Procedures

- ▶ **To upgrade PIX 515e or 535 with PDM installed, upgrade must be done from monitor mode**
 - This is due to flash size restrictions

- ▶ **Verify memory sizes and ensure minimum requirements are met**
 - For PIX, examine current license for minimum requirements

- ▶ **PIX 515e, 525 and 535 can be upgraded from CLI while old software is running**
 - Less downtime, ensure 515e and/or 535 does NOT have PDM

- ▶ **Older PIX versions (5.x, 4.x) must be upgraded to version 6.2 or 6.3 and then converted to 7.x**

- ▶ **Conduits must be migrated to ACL syntax**



Upgrade Procedures for PIX 515, 525 and 535 without PDM

- ▶ **Recommended terminal session is serial console**
 - Logging during reboot
 - Network connectivity not required

- ▶ **Save config to the TFTP server**
 - *write net <tftp ip address>:<filename>*
 - **example: write net 192.168.1.1:v6-3config.txt**

- ▶ **Copy new software from TFTP to flash**
 - *copy tftp flash:image*
 - You will be asked for the IP address and filename
 - Ensure the 'image installed' message appears after the copy procedure completes

- ▶ **After copy is complete, perform a reload**
 - *reload*



Upgrade Procedures for PIX 515, 525 and 535 without PDM (cont.)

- ▶ **Once the PIX reloads, examine the running configuration**
 - *show run* [[]] <beg-incl-excl-grep>
 - Perform a side by side comparison if necessary
 - *write net 192.168.1.1:v7-Xconfig.txt*

- ▶ **Assuming your config is valid, save new config**
 - *write mem* (or *copy run start*)
 - Be aware the your old config will be overwritten. Ensure is has been saved to backup

- ▶ **If you do not save your config, PIX will convert file for each reboot**
 - Until the new config is saved, the previous 6.3 config is still saved as the startup config



Upgrade Procedures for PIX 515 and 535 with PDM

- ▶ **If the PIX 515e and/or 535 contains a PDM image in flash, it must be upgraded from monitor mode**
 - Not enough room in flash all the files
 - Monitor mode does not process traffic, extra downtime will be incurred

- ▶ **Enter into monitor mode**
 - Using serial console connection, break into boot sequence during a reload



Upgrade Procedures for PIX 515 and 535 with PDM (cont.)

- ▶ Proceed with reload? [confirm] [Press the enter key]
- ▶ Rebooting....
- ▶ Cisco Secure PIX Firewall BIOS (4.0) #0:Thu Mar 2 22:59:20 PST 2000
- ▶ Platform PIX-515
- ▶ Flash=i28F640J5 @ 0x300
- ▶ Use BREAK or ESC to interrupt flash boot.
- ▶ Use SPACE to begin flash boot immediately.
- ▶ Flash boot interrupted.
- ▶ 0:i8255X @ PCI(bus:0 dev:13 irq:10)
- ▶ 1:i8255X @ PCI(bus:0 dev:14 irq:7)
- ▶ 2:i8255X @ PCI(bus:1 dev:0 irq:11)
- ▶ 3:i8255X @ PCI(bus:1 dev:1 irq:11)
- ▶ 4:i8255X @ PCI(bus:1 dev:2 irq:11)
- ▶ 5:i8255X @ PCI(bus:1 dev:3 irq:11)
- ▶ Using 1:i82559 @ PCI(bus:0 dev:14 irq:7), MAC:0021.1234.efc7
- ▶ Use ? for help.
- ▶ monitor>



Upgrade Procedures for PIX 515 and 535 with PDM (cont.)

- ▶ From monitor mode, you must manually copy the new software (NOT saved to flash)

- ▶ Determine where the TFTP server is and set the appropriate parameters
 - *monitor> interface 1 (inside)*
 - *monitor> address x.x.x.x*
 - *monitor> gateway x.x.x.x (optional)*
 - *monitor> server x.x.x.x (where x.x.x.x is the TFTP server)*
 - *monitor>file <7.x filename)*
 - *monitor>tftp*

- ▶ The new software will copy into RAM, load and execute, and convert your old config to a new one
 - Time to wait will be from 2 to 12 minutes
 - 2-4 minutes for 525/535, 10-12 minutes for 515e



Upgrade Procedures for PIX 515 and 535 with PDM (cont.)

- ▶ **Once the PIX has rebooted and you see the normal prompt, the software needs to be copied to flash**
 - ***copy tftp://192.168.1.1/pix704.bin flash:***
 - *Address or name of remote host [192.168.1.1]?*
 - *Source filename [pix704.bin]?*
 - *Destination filename [pix704.bin]?*

- ▶ **The new software will be copied into flash**



Upgrade Procedures for PIX 515 and 535 with PDM (cont.)

- ▶ **The previous 6.x configuration will be saved in flash**
 - *PIX(config)#show flash*
 - *Directory of flash:/*
 - *-rw- 1983 02:22:23 Apr 16 2005 downgrade.cfg*
 - *-rw- 4644864 02:22:53 Apr 17 2005 pix704.bin*

- ▶ **From config mode, use the *boot system* command to specify which file to load**
 - 7.x code supports multiple versions in flash
 - defaults to first valid image file
 - Versions can be toggled with the *boot system* command
 - example: *PIX(config)#boot system flash:pix704.bin*



Upgrade Procedure Caveats

- ▶ **If you are using a 'real' interface for stateful failover, your config must be changed**
 - Using an interface that processes traffic flows is not allowed to share the stateful failover interface in 7.x (allowed in 6.x)
 - Removal of stateful failover might be required if there are not spare interfaces

- ▶ **If your config is not changed and you perform an upgrade, your shared 'real' interface will become non-operational**
 - 7.x software treats the failover interfaces as 'special' interfaces and traffic flows cannot occur over them
 - Whichever interface was sharing the failover interface will become non-operational and traffic flows will stop



Upgrade Procedure Caveats (cont.)

- ▶ **During the copy procedure, you might see messages regarding ‘invalid flash blocks’ or ‘relinked orphaned X’**
 - This is normal behavior
 - Ignore these errors

- ▶ **The only way to downgrade the system to have a backup copy of the previous config**
 - Copy the old config into the system as the ‘startup-config’
 - Copy the old version of software that matches the config file you have into flash using **downgrade** command
 - Delete new version of software that already exists in flash
 - Reload

Overview of the Changes Between Version 6.3 and 7.x



- ▶ **Underlying technologies have NOT changed**
 - Adaptive Stateful Algorithm
 - Security levels and default trust levels
 - Translations and Connections
 - TCP Sequence numbering
 - Stateful engine
 - Named interfaces
 - Must be named
 - names are still used in config
 - Cut-through Authentication
 - Same technologies, same configurations
 - Default protocol inspection rules
 - Even though the commands have changed, default 'fixups' are still enabled
 - ESMTP inspection is now supported

7.X Technology Changes

- ▶ **CLI has changed**
 - CLI is designed to behave more like IOS
 - TAB key, context-sensitive help
 - New Interface Config mode
 - 'Clear' command not as risky

- ▶ **7.x software supports the new Modular Policy Framework (MPF)**
 - Build upon the MQC in IOS
 - Leverages known configurations
 - Allows for granular and global policies
 - Policies in 6.x are always global (fixup, max-conn, etc)
 - New L5/7 support
 - Can control access to IM, P2P, mime-type, URI length, specific FTP commands



7.X Technology Changes (cont.)

▶ **VPN CLI and features have Changed**

➤ VPN CLI

- Tunnel-group config
- Group-policy config

➤ VPN Features

- WebVPN (SSL VPN's) on ASA platform
- Hub and Spoke VPN's (hair-pinning)
- IPSec/TCP
- Activate/control VPN Client firewall or CSA

▶ **FWSM Contexts have been added**

➤ Firewall Contexts included in 7.x

- Number of contexts is based upon license and platform
- Contexts allow for multi-tenant and/or multi-interface configs



7.X Technology Changes (cont.)

▶ **Transparent Firewalls**

- 'Bump in the wire' technology
- Multiple transparent contexts can be used to create multi-tenant 'bump in the wire' firewalls

▶ **Can disable 6.x 'forced' NAT policy**

- (config)#no nat-control

▶ **Active/Active Failover**

- 6.x code allowed for only Active/Standby failover
- Active/Active solutions now are 'in the box'
 - Based upon new context technology
 - Still only one 'active' firewall (context) for given subnet/VLAN



7.X Technology Changes (cont.)

- ▶ **Improved Multicast support**
 - via PIM-SM
- ▶ **SSHv2 supported**
 - Allows AES encryption
- ▶ **SCP and FTP transfers**
 - For image and config file management
- ▶ **Multiple Image and Config files in flash**
 - Boot image and/or config file can be specified
- ▶ **Extended Ping capability**
 - Same features as IOS – no 'trace' command (yet)
- ▶ **IPv6 supported**
 - Full stateful inspection support and policy control



7.X Technology Changes (cont.)

▶ **Intrusion Prevention System**

- The ASA 5500 series appliances support a new card called the AIP-SSM (Advanced Inspection and Prevention Security Services Module)
- Hardware based IPS blade
 - Runs it's own OS

▶ **AIP-SSM has two flavors**

- AIP-SSM 10
 - 2Ghz Processor / 1.0 Gig RAM (5510 and 5520)
- AIP-SSM 20
 - 2.4Ghz Processor / 2.0 Gig RAM (5540 only)

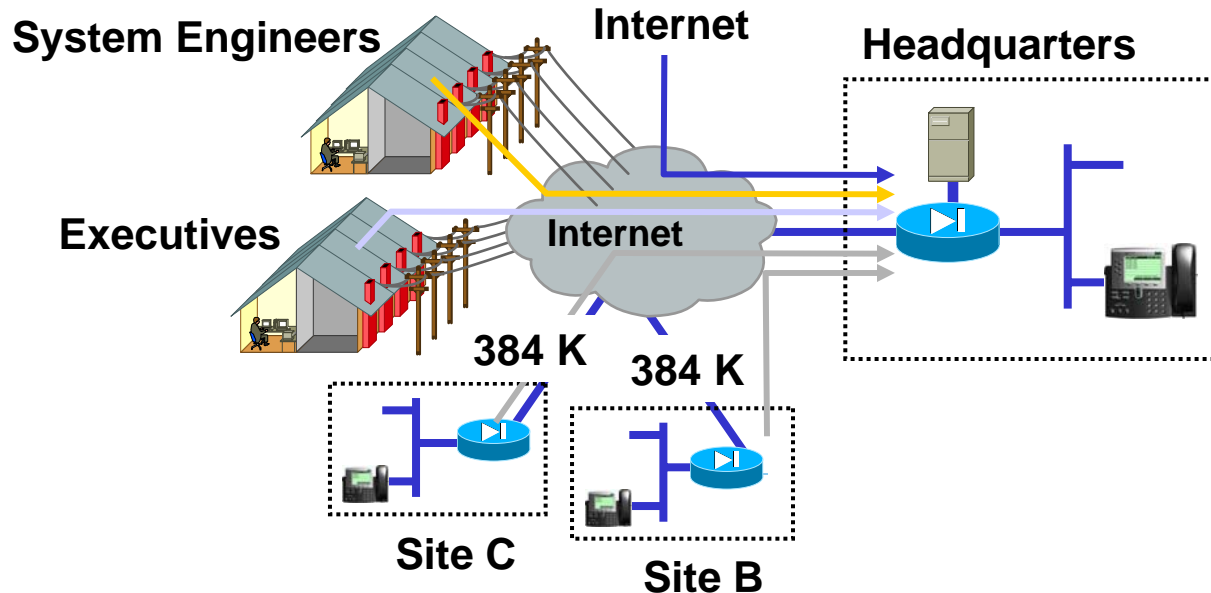


7.X Command Line Interface

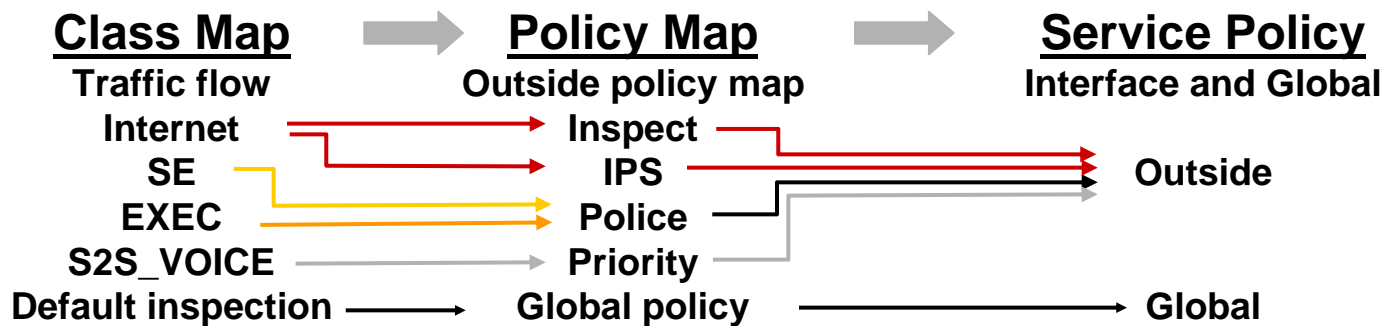
- ▶ **New CLI interface for Interface config**
 - *pix(config)# interface ethernet0*
 - *pix(config-if)# nameif outside*
 - *pix(config-if)# ip address 192.168.1.2 255.255.255.0*
 - *pix(config-if)# security-level 0*
 - *pix(config-if)# speed 100*
 - *pix(config-if)# duplex full*
 - *pix(config-if)# no shut*

- ▶ **Once the interfaces are named, names are used throughout the configuration**
 - *pix(config)# nat (inside) 1 10.0.0.0 255.0.0.0*
 - *pix(config)# static (inside,outside) 192.168.1.3 10.1.1.3 0 0*
 - *pix(config)# telnet 10.1.1.1 255.255.255.255 inside*

Modular Policy Framework (MPF)



Modular policy provides greater granularity and more flexibility





Modular Policy Framework (cont.)

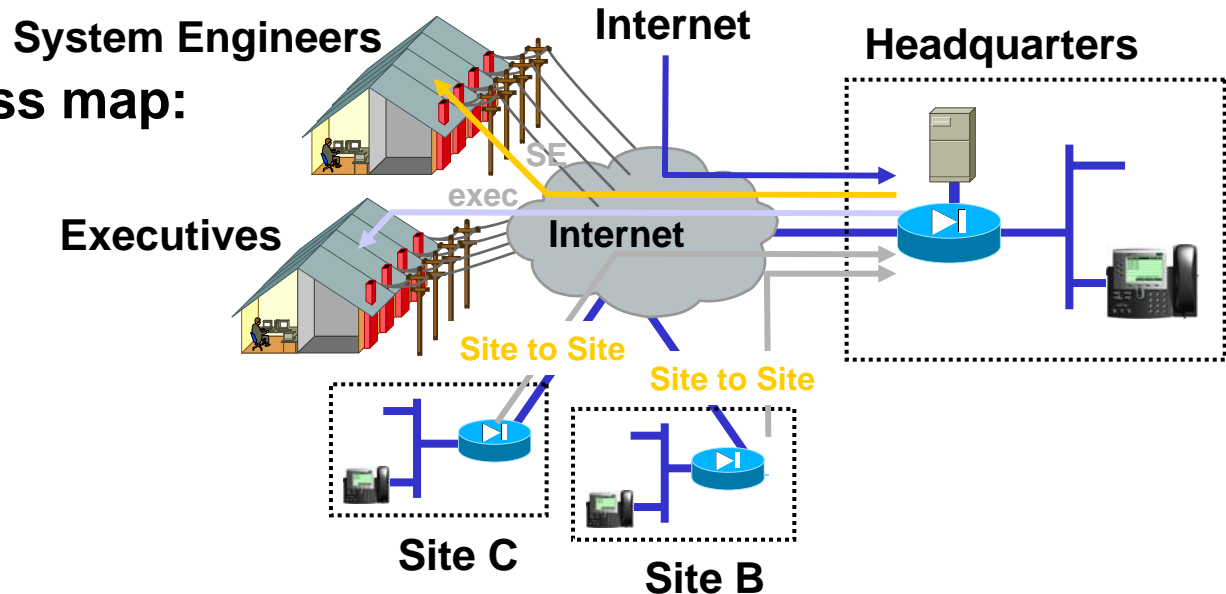
- ▶ **Modular Policy Framework uses the same building blocks at the IOS Modular QoS CLI (MQC)**
 - Class-Maps
 - Who are you / what type of traffic (Classification)
 - Policy-Maps
 - What do I do with you / traffic treatment (PHB)
 - Service-Policies
 - Where / when does this apply

- ▶ **Modular Policy Framework allows for**
 - Granular Policies applied to specific traffic and/or interfaces
 - New per flow behavior that 6.x could not support
 - Basic QoS, Inspection (fixup), Connection limits

Modular Policy Framework (cont.)

To configure a class map:

- Name a class
- Define matching attributes



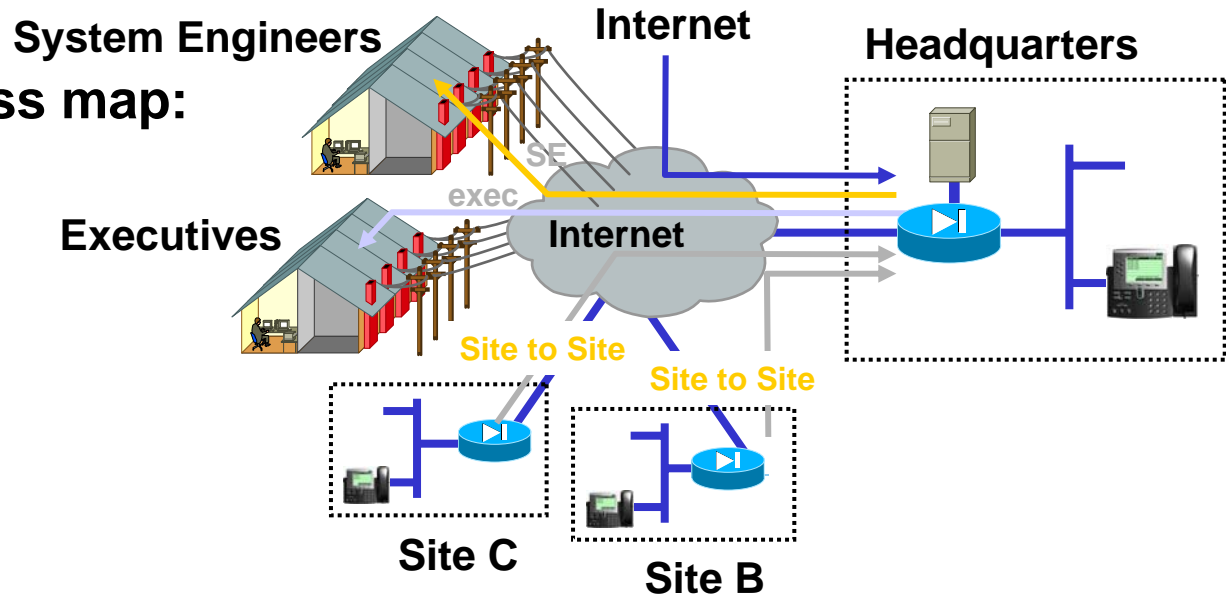
```

pix1(config)# class-map SE
pix1(config-cmap)# match port tcp eq 23
pix1(config-cmap)# match tunnel-group S2S
pix1(config)# class-map S2S_VOICE
pix1(config-cmap)# match dscp ef
pix1(config)# class-map EXEC
pix1(config-cmap)# match access-list 102
    
```

Modular Policy Framework (cont.)

To configure a class map:

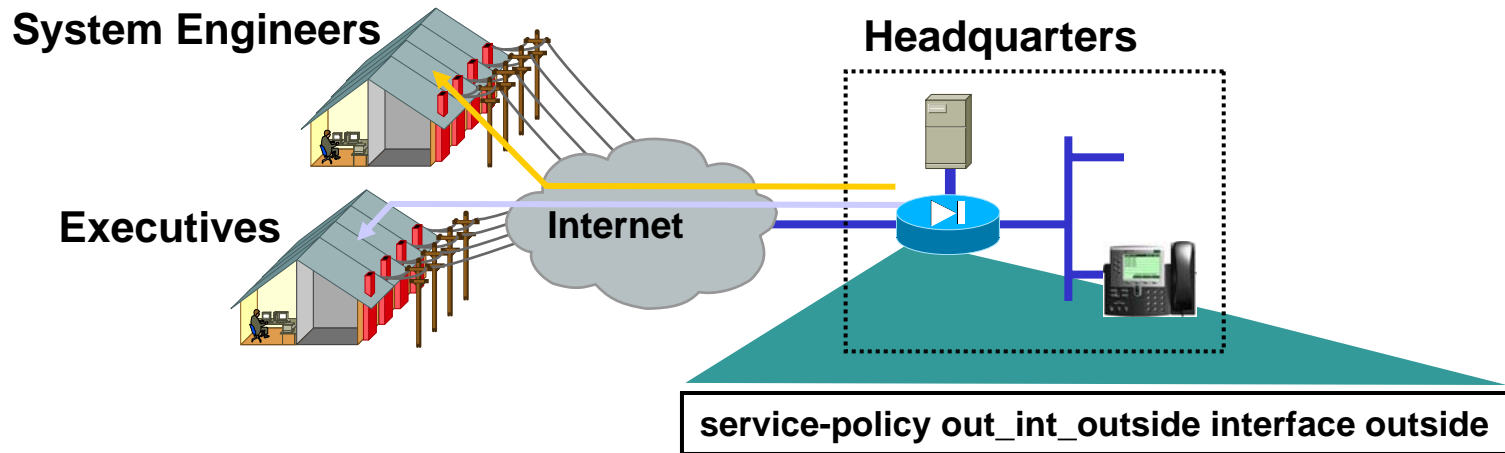
- Name a class
- Define matching attributes



```

pix1(config)# policy-map OUT_INT_OUTSIDE
pix1(config-pmap)# class SE
pix1(config-pmap-c)# MPF Parameter (inspect, IPS, police,
priority, set connection, etc)
pix1(config-pmap-c)# police 56000 1000
pix1(config-pmap-c)# class S2S_VOICE
pix1(config-pmap-c)# priority
pix1(config-pmap-c)# class EXEC
pix1(config-pmap-c)# set connection conn-max 200
    
```

Modular Policy Framework (cont.)



```
pix1(config)# service-policy OUT_INT_OUTSIDE interface  
outside
```



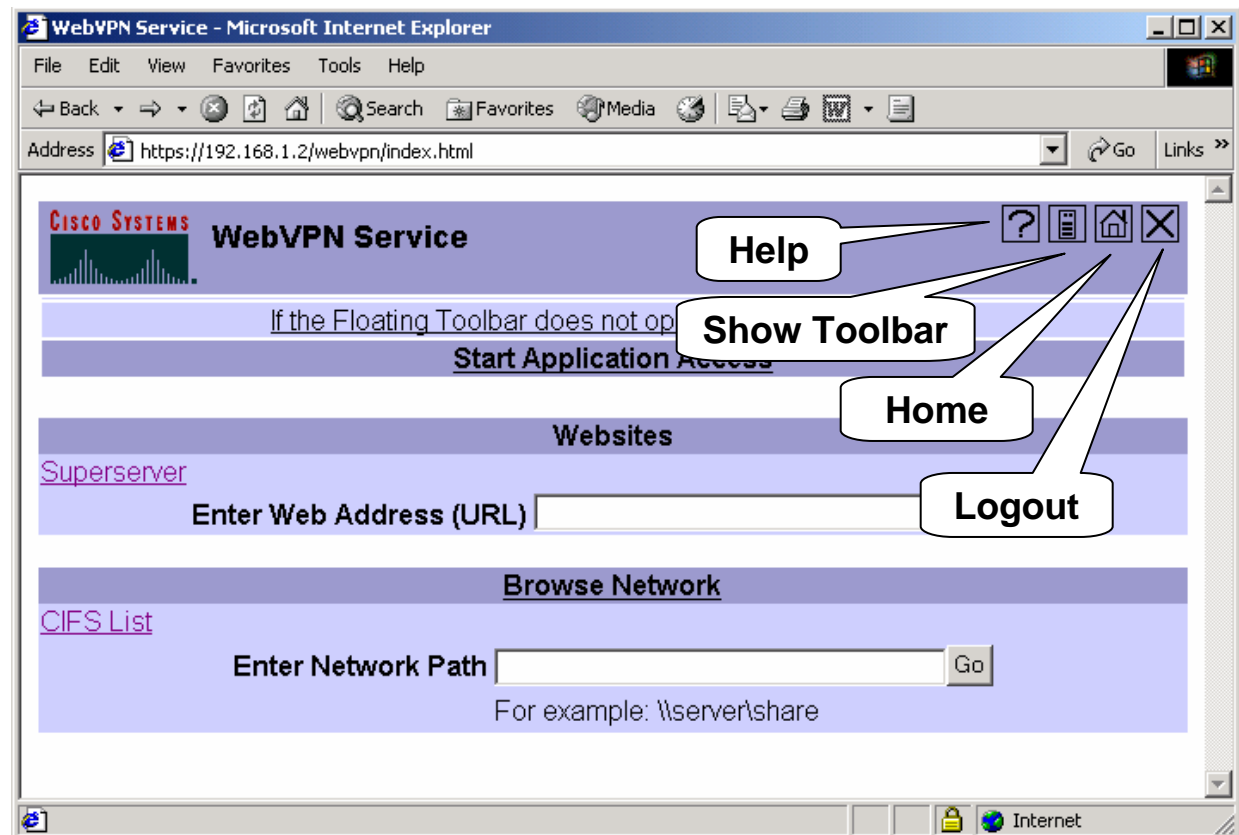
Web VPN

- ▶ **Prior to 7.x software, VPN's could only be established using the IPSec protocol suite**
 - Includes site-to-site VPN's and remote access VPN's
 - Some locations did not support IPSec (NAT & PAT), and NAT-traversal can be blocked

- ▶ **Web VPN allows for VPN tunnel over SSL**
 - SSL to the ASA head end unit
 - Allows for Basic VPN services
 - Web, Windows File Shares, Email, etc
 - Specific application may require IPSec VPN

Web VPN Home Page

- ▶ The home page is the end user's customized access point.



- ▶ **Contexts allows for multiple virtual firewalls**
 - Used for installations where renumbering would cause an issue
 - Used for multi-tenant applications
 - Used for 'extra' security between interfaces

- ▶ **Each context is a separate firewall**
 - Context is associated with either subnets or VLAN's
 - Each context uses it's own config file and has a virtual file system
 - Contexts do NOT 'see' each other



Contexts (cont.)

- ▶ **Graphical Management of Contexts is supported**
 - Via ASDM (PDM replacement for 7.x)
 - Can manage multiple contexts (admin) or single contexts

- ▶ **Contexts do not support**
 - Dynamic Routing
 - Only static routes
 - VPN termination
 - Multicast

- ▶ **Convert the firewall to context mode**
 - Previous startup-config should be saved onto a TFTP server for downgrade path
 - *pix(config)# **mode multiple [no confirm]***
 - Current running-config is renamed and saved into flash as old_running.cfg
 - Forces reload

- ▶ **Once the firewall is converted to multiple mode the following occurs**
 - Running-config is split and 2 new files are created
 - Startup-config for the system
 - Admin.cfg for the admin context

▶ **System configuration file**

- Includes system wide settings
 - software version
 - location of context configuration files
 - Uses Admin Context interfaces

▶ **Admin context**

- The admin context is created automatically
 - System wide configuration
 - Place to create/delete contexts
 - Only context that 'sees' the others
 - Can be used to login/logout of other contexts

- ▶ **All other contexts need to be created**
 - From the admin context:
 - ***pix(config)# context name***
 - ***pix(config)# context context1***
 - ***Creating context 'context1'... Done.***
 - ***pix(config-ctx)#***

- ▶ **Once the context is created, you associate the context with interfaces**
 - ***pix(config-ctx)# allocate-interface [physical | .subif]***
 - ***pix(config-ctx)# allocate-interface gigabitethernet0/1.100 int1***
 - 'int1' will be the interface name within the context

- ▶ **Each context has its own configuration file**
 - MUST configure location of config file
 - pix(config)# **config-url URL**
 - pix(config-ctx)# **config-url flash:/context3.cfg**
 - FTP, TFTP or SSL can also be used
 - Enables the context (disabled before config-url)
 - Ensure the interfaces have been allocated before this command is entered
 - Config changes within the context are saved to this file
 - i.e. write mem, copy run start



Contexts (cont.)

- ▶ **Contexts can be managed multiple ways**
 - From the admin context
 - ***pix(config)# changeto context1***
 - ***pix/context1(config)#***
 - Normal management
 - Once the context config is in place, normal management applies (telnet, SSH, etc)

- ▶ **Management commands apply only to the specific context**
 - write, show, and clear will only affect the local context (unless it is the admin context)



Contexts (cont.)

- ▶ **To remove a context, perform the following tasks**
 - Connect to the system context
 - *pix/context1(config)# changeto context system*
 - *pix(config)# no context NAME*

- ▶ **To remove ALL context configuration**
 - Connect to the system context
 - *pix/context1(config)# changeto context system*
 - *pix(config)# clear configure context*
 - Be careful with the clear command



Transparent Firewall

- ▶ **A transparent firewall operates at layer 2**
 - Instead of 'routing' at layer 3, it 'switches' at layer 2
 - Transparent firewall 'connects' VLAN's not subnets
 - Allows arp-inspection

- ▶ **A transparent firewall does not support**
 - NAT, QoS, DHCP relay
 - Cannot change L3 header
 - Routing, multicast, IPv6
 - Does not have L3 services running
 - VPN tunnel termination
 - Requires NAT and basic routing services



Transparent Firewall (cont.)

- ▶ **Transparent firewall mode must be enabled**
 - Issue the 'firewall transparent' command
 - Affects the entire firewall
 - Reload not forced

- ▶ **Transparent contexts can be created and used**
 - All contexts on appliance are either routed or transparent
 - Cannot mix and match

- ▶ **Example**
 - ***pix(config)# firewall transparent***
 - **Switched to transparent mode**
 - ***pix(config)# context NAME***

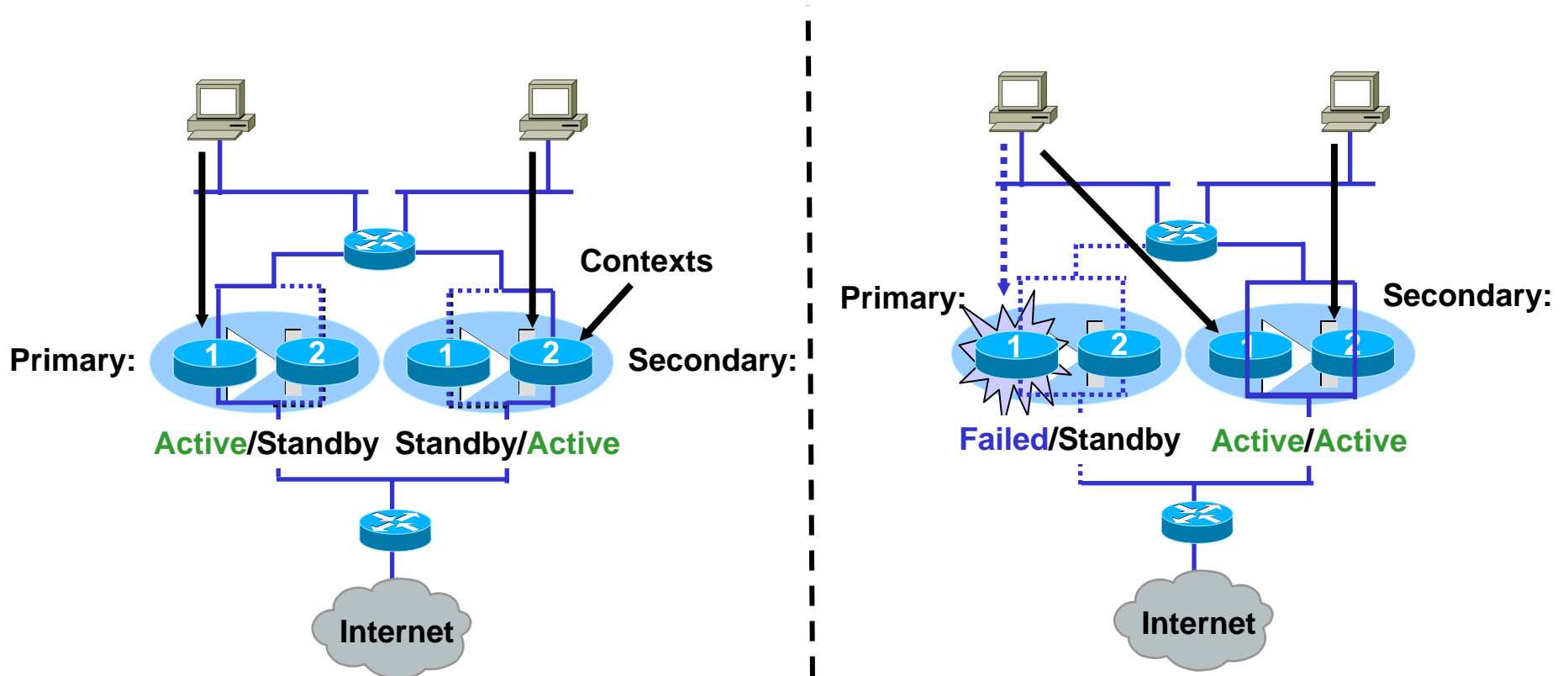


Transparent Firewall (cont.)

- ▶ To manage the L2 (transparent) firewall remotely, a management IP address must be configured
 - ***pix(config)# ip address x.x.x.x y.y.y.y***
 - Configures the MGMT IP address for the PIX
 - Done in global config mode
 - Must be an IP in the controlled subnet
 - ***fw1(config)# ip address 192.168.1.1 255.255.255.0***
 - ***fw1(config)# show ip address***
 - ***Management System IP Address:***
 - ip address 192.168.1.1 255.255.255.0***

- ▶ To manage contexts, configure a MGMT IP address for the system and then use the 'changeto' command

Active/Active Failover



- **Active/Active:** Both units can process traffic and serve as backup units



Active/Active Failover (cont.)

- ▶ **Active/Active failover requires the following**
 - Same Hardware models/configurations
 - Same software revs
 - The use of contexts
 - Proper licensing

- ▶ **Active/Active supports stateful failover**
 - Unlike 6.x software, stateful interface cannot be shared with a traffic passing interface (inside, outside, DMZ, etc)
 - With stateful Active/Active, you get stateful 'pairs' of firewalls
 - Does not support load balancing



Active/Active Failover (cont.)

- ▶ **Active/Active technology does not differ from standard active/standby failover**
 - Based upon active contexts
 - Active/standby contexts are reciprocal on other physical firewall

- ▶ **Contexts are 'grouped' into redundant pairs**
 - ***pix(config)# context NAME***
 - ***pix/NAME(config)# join-failover-group X***



ASA Intrusion Prevention System

- ▶ **AIP-SSM blade allows for wire-speed IPS**
 - Can be ran in promiscuous or inline mode
 - Promiscuous copies all traffic to card
 - Inline mode sees all flows
 - Firewall can forward or block all traffic based upon failure of card/service
 - Fail-open permits on failure
 - Fail-closed denies on failure

- ▶ **MPF can be used to specify which traffic (users) will use the AIP-SSM**
 - *pix(config)# policy-map IPS*
 - *pix(config-pmap)# class Internet*
 - *pix(config-pmap-c)# IPS*

Practical examples using 7.x features





7.X Command Line Interface

- *firewall(config)# hostname pix*
- *pix(config)# interface ethernet0*
- *pix(config-if)# nameif **outside***
- *pix(config-if)# ip address 192.168.1.1 255.255.255.0*
- *pix(config-if)# **security-level 0***
- *pix(config-if)# speed 100*
- *pix(config-if)# duplex full*
- *pix(config-if)# no shut*
- *pix(config)# interface ethernet1*
- *pix(config-if)# nameif **inside***
- *pix(config-if)# ip address 10.1.1.1 255.255.255.0*
- *pix(config-if)# **security-level 100***
- *pix(config-if)# speed 100*
- *pix(config-if)# duplex full*
- *pix(config-if)# no shut*
- *pix(config-if)# route outside 0.0.0.0 0.0.0.0 192.168.1.254 1*
- *pix(config)# **nat control** (NAT does NOT have to be enabled in 7.x)*
- *pix(config)# nat (**inside**) 1 10.1.1.0 255.255.255.0*
- *pix(config)# global (**outside**) 1 192.168.1.10*



Using the MPF for Voice / QoS

- ***pix(config)# class-map voice***
- ***pix(config-cmap)# match dscp ef***
- ***pix(config-cmap)# class-map voice-signal***
- ***pix(config-cmap)# match dscp af31***
- ***pix(config-cmap)# ...other classes (internet, vpn, etc)***
- ***pix(config)# policy-map QoS-Voice***
- ***pix(config-pmap)# class voice***
- ***pix(config-pmap-c)# priority***
- ***pix(config-pmap-c)# class voice-signal***
- ***pix(config-pmap-c)# priority***
- ***pix(config-pmap-c)# class ...other classes***
- ***pix(config)# interface ethernet0***
- ***pix(config-if)# service-policy out QoS-Voice***



Adding IPS for Internet traffic

- ***pix(config)# access-list extended 101 permit ip any any***
- ***pix(config)# class-map Internet***
- ***pix(config-cmap)# match access-list 101***
- ***pix(config)# policy-map QoS-Voice***
- ***pix(config-pmap)# class Internet***
- ***pix(config-pmap-c)# IPS***
- ***pix(config)# interface ethernet0***
- ***pix(config-if)# service-policy out QoS-Voice***

- **Internet class happens after the voice and voice-signal classes**
- **All traffic after voice classes goes to IPS blade for inspection**

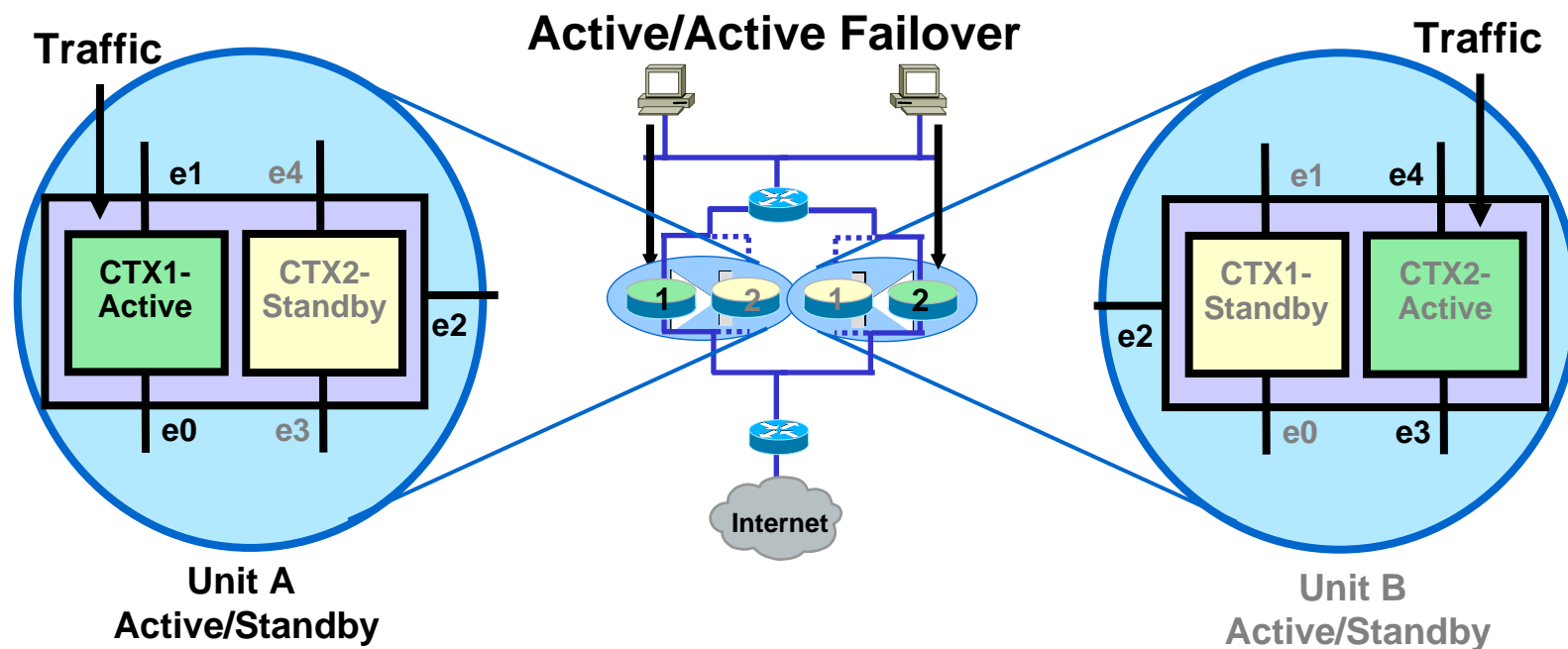


Using the MPF for BGP MD5

- ***pix(config)# class-map BGP-MD5***
- ***pix(config-cmap)# match port tcp eq 179 (or ACL)***
- ***pix(config)# tcp-map BGP-MD5***
- ***pix(config-tcp-map)# tcp-options range 19 19 allow***
- ***pix(config-tcp-map)# policy-map global_policy***
- ***pix(config-pmap)# class BGP-MD5***
- ***pix(config-pmap-c)# set connection advanced-options BGP-MD5***
- ***pix(config)# service-policy global_policy global***

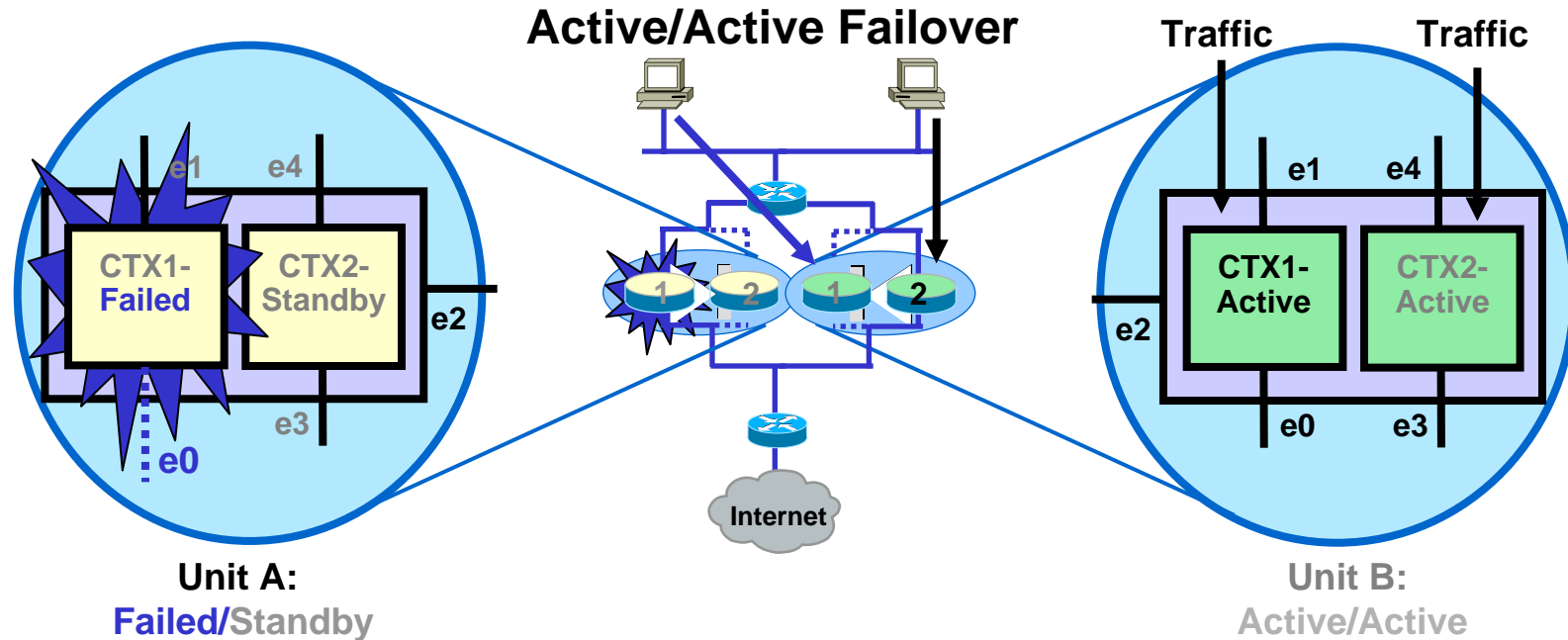
- **Default policy 'global_policy' is built and enabled by default**
- **Editing the 'global_policy' affects all interfaces and all flows**

Active/Active Failover



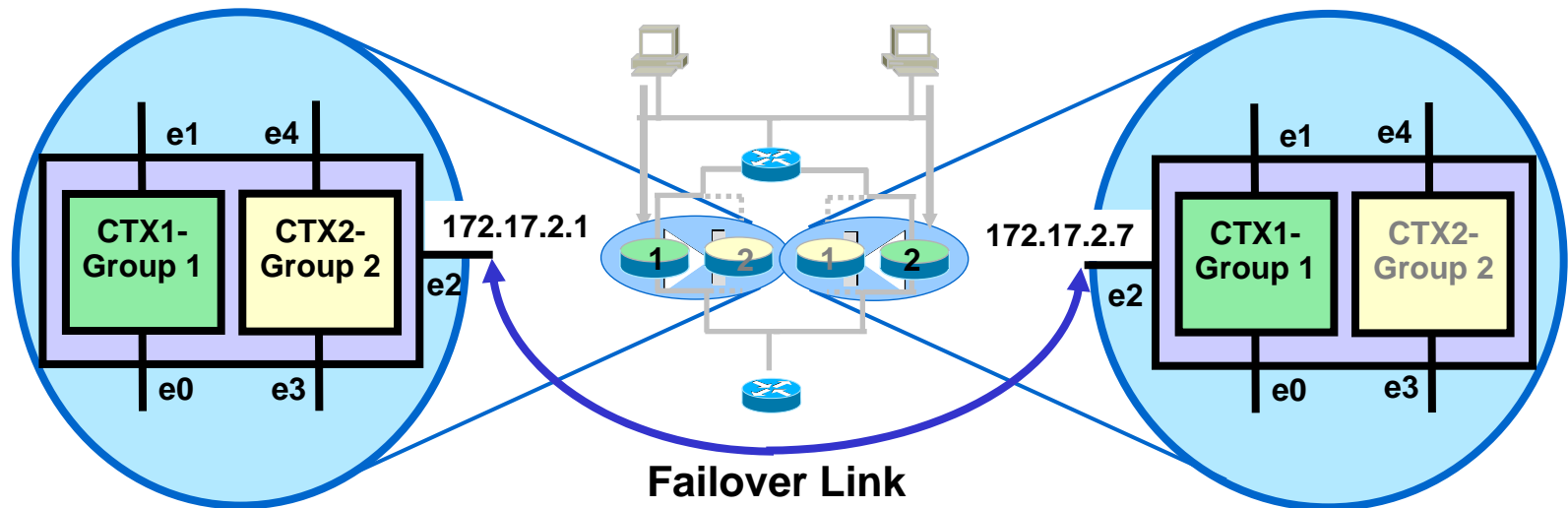
- ▶ **Active/active failover requires the use of contexts. For example, two security appliances with 2 contexts each**
 - **CTX1**
 - **CTX2**
- ▶ **Under normal conditions, each security appliance has one active and one standby context**
 - **Active context processes traffic**
 - **Standby context is located in the peer security appliance**

Active/Active Failover (Cont.)



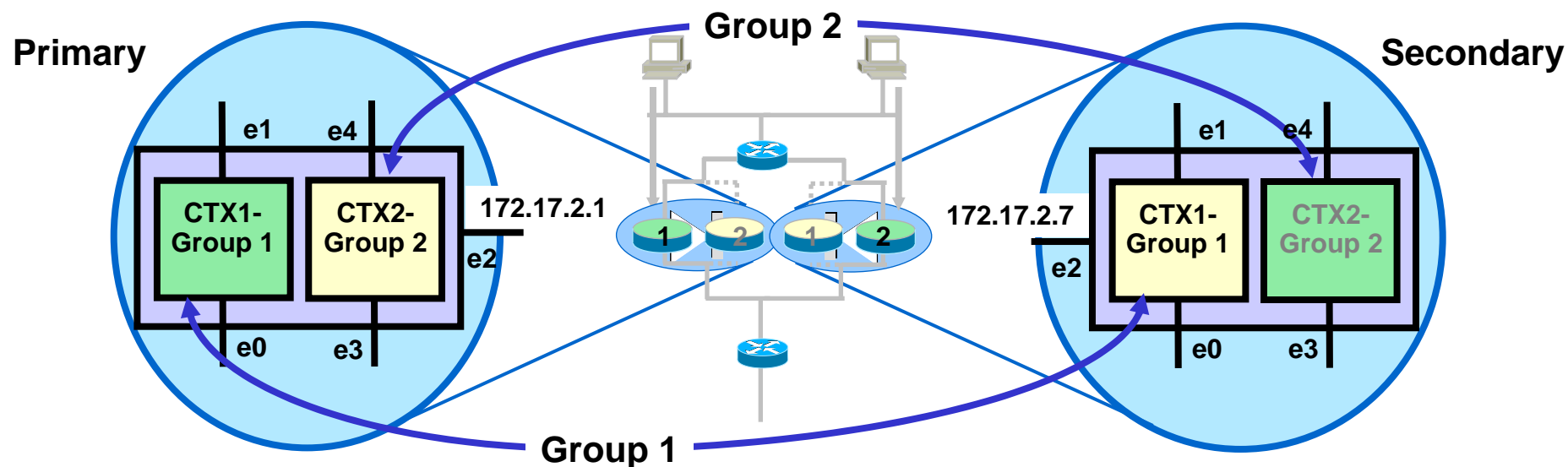
- ▶ Under failed conditions, Unit A determines outside interface on CTX1 has failed
 - CTX1 is placed in failed state
 - Unit A has one failed and one standby context
- ▶ Unit B, CTX1 becomes active
 - Unit B has two active contexts
 - Both active contexts pass traffic
- ▶ Failover can be context-based or unit-based

Active/Active Failover (Cont.)



```
fw2(config)# interface ethernet2
fw2(config-if)# no shut
fw2(config)# failover lan interface LANFAIL ethernet2
fw2(config)# failover interface ip LANFAIL 172.17.2.1 255.255.255.0 standby
172.17.2.7
fw2(config)# failover lan enable
fw2(config)# failover link LANFAIL ethernet2
fw2(config)# failover lan key 1234567
```

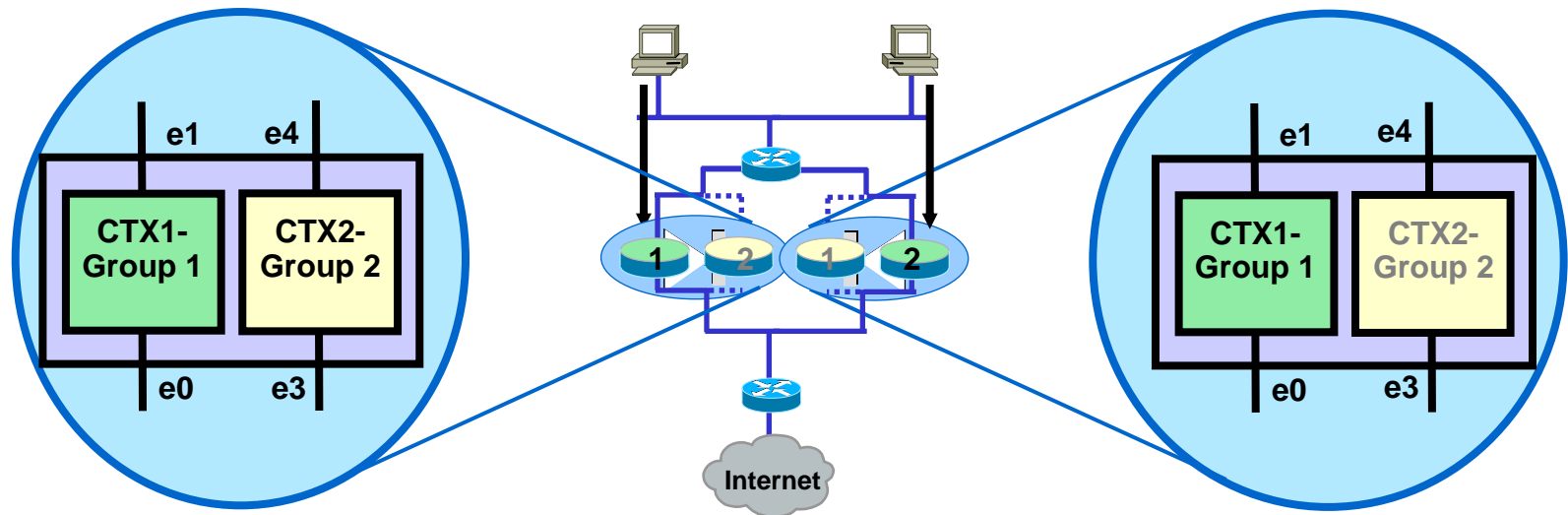
Active/Active Failover (Cont.)



- Active/active failover adds support for failover group.
- Failover is performed on a unit or group level.
- A group is comprised of one or more contexts.
- Each failover group contains separate state machines to keep track of the group failover state.

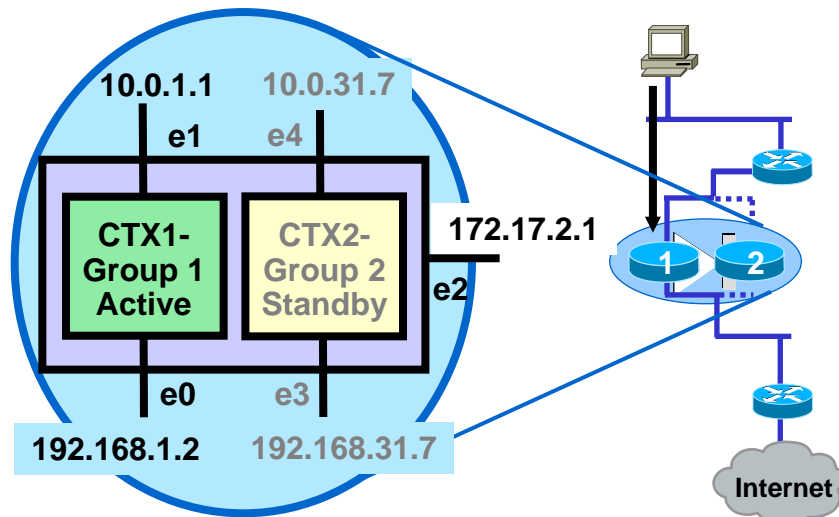
```
fw2(config)# failover group 1
fw2(config-fover-group)# primary
fw2(config)# failover group 2
fw2(config-fover-group)# secondary
```

Active/Active Failover (Cont.)



```
fw2(config)# context ctx1
fw2(config-ctx)# allocate-interface ethernet0
fw2(config-ctx)# allocate-interface ethernet1
fw2(config-ctx)# config-url flash:/ctx1.cfg
fw2(config-ctx)# join-failover-group 1
fw2(config)# context ctx2
fw2(config-ctx)# allocate-interface ethernet3
fw2(config-ctx)# allocate-interface ethernet4
fw2(config-ctx)# config-url flash:/ctx2.cfg
fw2(config-ctx)# join-failover-group 2
```

Active/Active Failover (Cont.)



▶ Context 1

➤ Interface e0

- IP address 192.168.1.2
- Standby 192.168.1.7

➤ Interface e1

- IP Address 10.0.1.1
- Standby 10.0.1.7

▶ Context 2

➤ Interface e3

- IP address 192.168.31.7
- Standby 192.168.31.1

➤ Interface e4

- IP address 10.0.31.7
- Standby 10.0.31.1

```
fw2(config)# changeto context ctx1
fw2/ctx1(config)# interface ethernet0
fw2/ctx1(config-if)# ip address 192.168.1.2 255.255.255.0 standby
192.168.1.7
fw2/ctx1(config-if)# nameif outside
fw2/ctx1(config-if)# exit
fw2/ctx1(config)# interface ethernet1
fw2/ctx1(config-if)# ip address 10.0.1.1 255.255.255.0 standby 10.0.1.7
fw2/ctx1(config-if)# nameif inside
fw2/ctx1(config-if)# exit
```

Thank You

Rick Williams

rick.williams@oasis-network.com

<http://www.sunsetlearning.com>

1.800.569.1894

