Catalyst 6500, Cisco 7600 Firewall Service Module, FWSM

3.1 újdonságok

ÁCS GYÖRGY
GACS@CISCO.COM

Agenda

FWSM3.1 licensing and overview

ASDM 5.0(1)F overview

FWSM/ASDM feature discussions

FWSM3.1 Licensing

FWSM3.1 Licensing Changes

- **Additional 250 Virtual Firewall Tier of Licensing**

  FR-SVC-FWM-VC-T4 **(250 Virtual Firewalls)**

  FW-SVC-FWM-UPGR3 **(Upgrade 100 to 250 Virtual Firewalls)**

- **Additional GTP license (same as PIX 7.0)**

  FR-SVC-FWM-GTP

FWSM Licensing Information

Licensed features

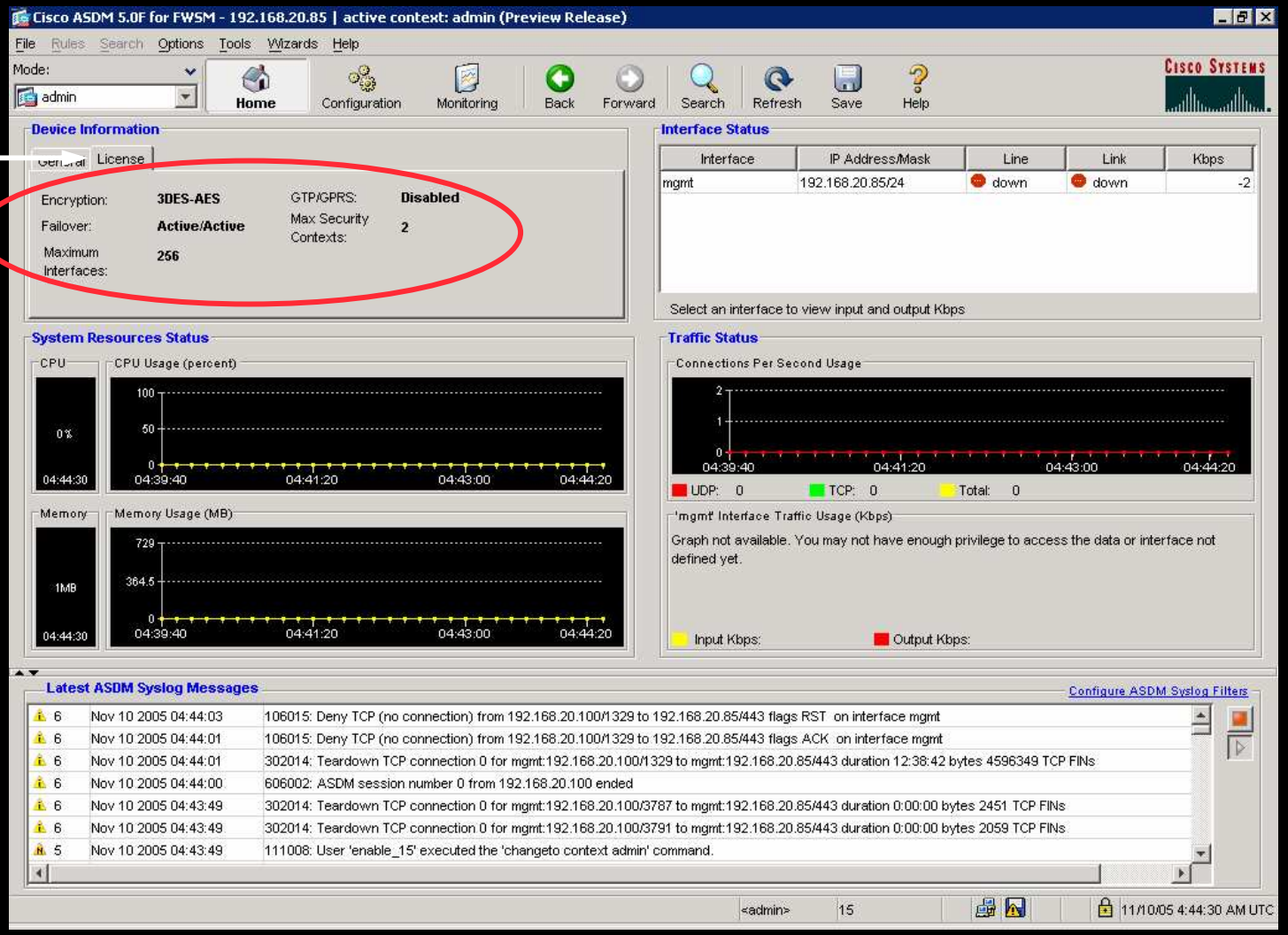
```
FWSM# show activation-key
Serial Number:  SAD065102T5
Running Activation Key: 0x00000000 0x00000000 0x00000000
0x00000000
The Running Activation Key is not valid, using default
settings:

Licensed features for this platform:
Maximum Interfaces          : 256
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 2
GTP/GPRS                    : Disabled
VPN Peers                   : Unlimited

The flash activation key is the SAME as the running key.
```

ASDM 5.0(1)F Licensing Screen

Licensing tab



FWSM3.1 & ASDM 5.0(1)F

Overview

FWSM 3.1 újdonságok

- **Higher Scalability:** 250 contexts
- **High Availability:** Active/Active
- **Stronger Defense Against Threats: PIX OS 7.0 Features**
- **-** Modular Policy CLI
- - Advanced App Inspection (Port 80 Misuse)
- - Additional Protocols
- **-** Mobile Wireless Security (GTP/GPRS)
- - VoIP Enhancements, Skinny Video
- **Network Integration:**
- **-** IPv6 (SW)
- - PIM-Sparse Mode Multicast (Single Mode)
- - **Multiple L2 Interfaces per Context**
- - **Mixed L2 & L3**, Private VLANs
- - Asymmetric Routing
- **Management:**
- **-** CVDM, ASDM 5.0, VMS, MARS

FWSM Feature Summary

- **Major FWSM3.1 features are summarized in terms of**
  - **feature description**
  - **feature available in L2 or L3 firewall**
  - **feature available in single or multi mode**
  - **PIX feature parity information**

Legends

Mode

L2: feature is available in transparent mode firewall
L3: feature is available in routed mode firewall
N/A: feature is not applicable in this mode
(blank): presently, feature is not supported in this mode

Context

S: feature is available in single mode
M: feature is available in multi mode
N/A: feature is not applicable in this mode
(blank): presently, feature is not supported in this mode

PIX Parity

n.n: feature was implemented in PIX version n.n
(blank): feature is not supported on PIX platform

Usability, Scalability & Performance

	Mode		Context		PIX Parity
	L2	L3	S	M	
CLI improvements	✓	✓	✓	✓	7.0
250 virtual context	✓	✓	N/A	✓	
ACL memory enhancement	✓	✓	✓	✓	
Sessionizing non TCP/UDP packets	✓	✓	✓	✓	
Applying “write mem” to all context	✓	✓	N/A	✓	
global statements up to 4,000		✓	✓	✓	

Network Integration

	Mode		Context		PIX Parity
	L2	L3	S	M	
Mixed L2 & L3 mode	✓	✓	N/A	✓	
Multi pairs of L2 interfaces per TFW	✓	N/A	✓	✓	
Private vlan support	✓	✓	✓	✓	

Address translation and ACL Enhancements

	Mode		Context		PIX Parity
	L2	L3	S	M	
NAT control		✓	✓	✓	7.0
Overlapping static configuration	✓	✓	✓	✓	7.0
Time based ACL	✓	✓	✓	✓	7.0
ACL editing	✓	✓	✓	✓	6.3
Interface as address in ACL	✓	✓	✓	✓	6.3

Deep Packet Inspection (HTTP)

	Mode		Context		PIX Parity
	L2	L3	S	M	
Detect & block tunneled app + attacks	✓	✓	✓	✓	7.0
RFC compliant checking	✓	✓	✓	✓	7.0
HTTP command filtering	✓	✓	✓	✓	7.0
MIME type filtering	✓	✓	✓	✓	7.0
Min/Max size check on msg, hdr len & URI	✓	✓	✓	✓	7.0
Content validation	✓	✓	✓	✓	7.0
Keyword based HTTP msg filtering	✓	✓	✓	✓	7.0

Inspection Engines Enhancements

	Mode		Context		PIX Parity
	L2	L3	S	M	
Enhanced FTP inspection	✓	✓	✓	✓	7.0
ESMTP inspection	✓	✓	✓	✓	7.0
TCP stream reassembly for inspection engines	✓	✓	✓	✓	7.0
Connection optimization for URL filtering	✓	✓	✓	✓	7.0
ActiveX/Java filtering	✓	✓	✓	✓	6.0
PPTP Enhancements	✓	✓	✓	✓	6.3
Fixup to inspection enhancements	✓	✓	✓	✓	7.0

Modular Policy Framework

High Availability

	Mode		Context		PIX Parity
	L2	L3	S	M	
Active/Active	✓	✓		✓	7.0
Active/Active pre-empt option	✓	✓		✓	
Asymmetric Routing (w and w/o A/A)	✓	✓	✓	✓	

Core (IP) Enhancements

	Mode		Context		PIX Parity
	L2	L3	S	M	
Multicast support	*	✓	✓		7.0
IPv6 phase I		✓	✓	✓	7.0
dNAT for multicast		✓	✓		
OSPF neighbor	N/A	✓	✓		7.0
TCP Normalizer	✓	✓	✓	✓	7.0

* FWSM2.x bridges multicast traffic in L2 mode.

VoIP and Multimedia

	Mode		Context		PIX Parity
	L2	L3	S	M	
H.323 enhancement – T.38	✓	✓	✓	✓	7.0
H.323 enhancement - GKRCS	✓	✓	✓	✓	7.0
MGCP NAT		✓	✓	✓	7.0
GTP fixup	✓	✓	✓	✓	7.0
SIP instant messaging fixup	✓	✓	✓	✓	7.0
TAPI/CTIQBE fixup	✓	✓	✓	✓	6.3
Skinny video support	✓	✓	✓	✓	

Authentication, Authorization & Accounting

	Mode		Context		PIX Parity
	L2	L3	S	M	
Simultaneous RADIUS accounting servers	✓	✓	✓	✓	7.0
Accounting for management traffic	✓	✓	✓	✓	7.0
FTP authentication challenge	✓	✓	✓	✓	
MAC based AAA exempt	✓	✓	✓	✓	6.3
Cut through proxy authen using local DB	✓	✓	✓	✓	6.3

Monitoring and Management Improvements

	Mode		Context		PIX Parity
	L2	L3	S	M	
SSHv2	✓	✓	✓	✓	7.0
Ping, logging & memory mgt enhancements	✓	✓	✓	✓	7.0
Syslog server failure policy (TCP transport)	✓	✓	✓	✓	7.0
SNMPv2C and Additional MIBs	✓	✓	✓	✓	7.0
Out of band management		✓	✓	✓	7.0
Prompt with slot/status/… reporting	✓	✓	✓	✓	

ASDM 5.0(1)F Overview

- **What is ASDM (Adaptive Security Device Manager)**

  A browser based tool designed to help configure and monitor the firewall service module.

FWSM – ASDM Requirements

- Minimum ASDM and FWSM software compatibility version (ASDM: 5.0(1)F & FWSM3.1)
- Supported Java 1.4.2 and 5.0 (also known as 1.5)

  IBM Java (not officially supported)
- To access ASDM through a browser following must be met:

  JavaScript and Java must be enabled

  Browser support for SSL must be enabled

  Pop-up blockers may prevent ASDM from starting (ASDM will notify you)
- Supported Browsers

  – Windows 2000 (Service Pack 4), Windows XP (English or Japanese version of Windows)

  Internet Explorer 6.0 with Java Plug-in 1.4.2 or 5.0 (also known as 1.5.0)

  Firefox 1.0 with Java Plug-in 1.4.2 or 5.0 (or 1.5.0)

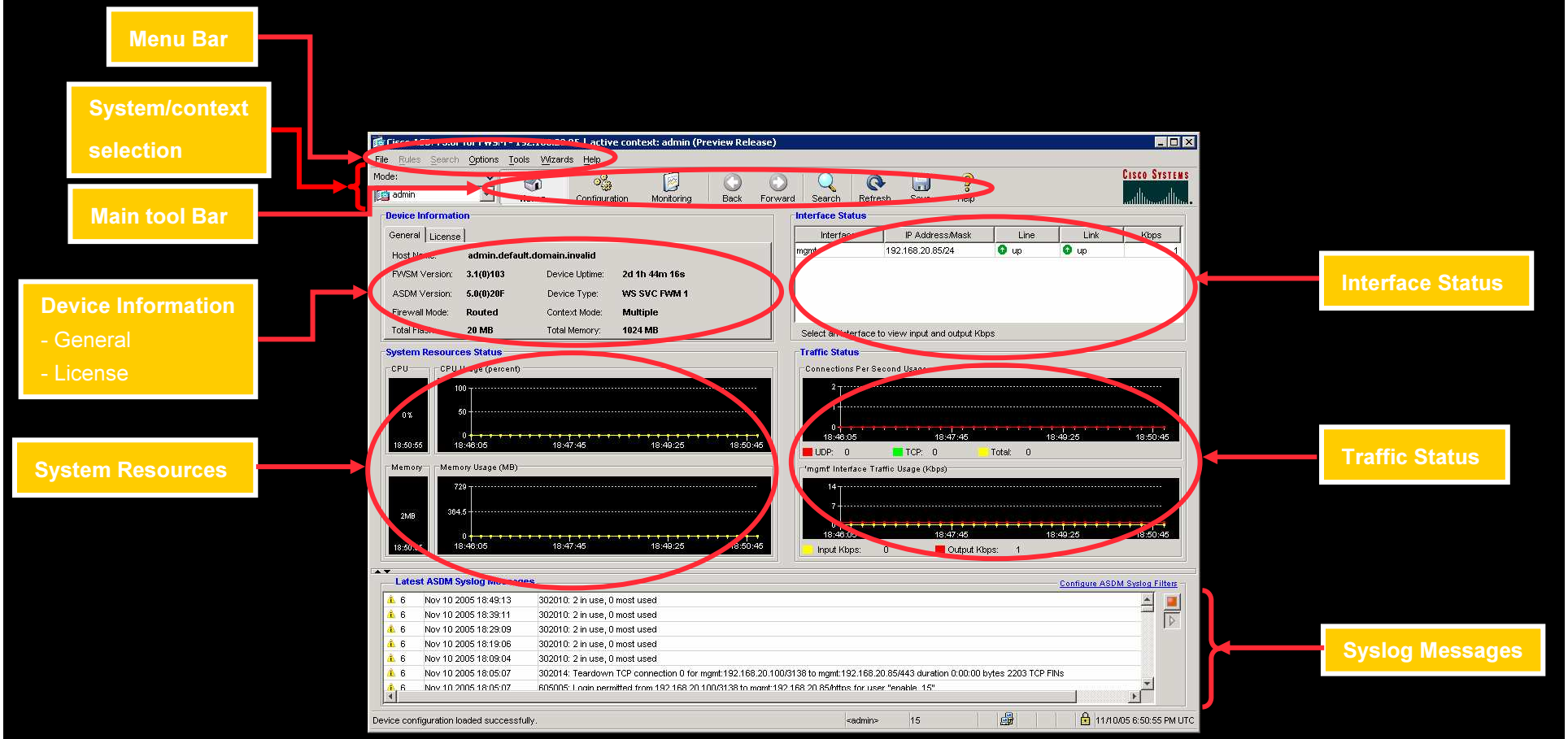
  – Sun SPARC Solaris 8 or Solaris 9

  Firefox 1.0 with Java Plug-in 1.4.2 or 5.0 (or 1.5.0)

  – Red Hat Desktop, Red Hat Enterprise Linux WS version 3

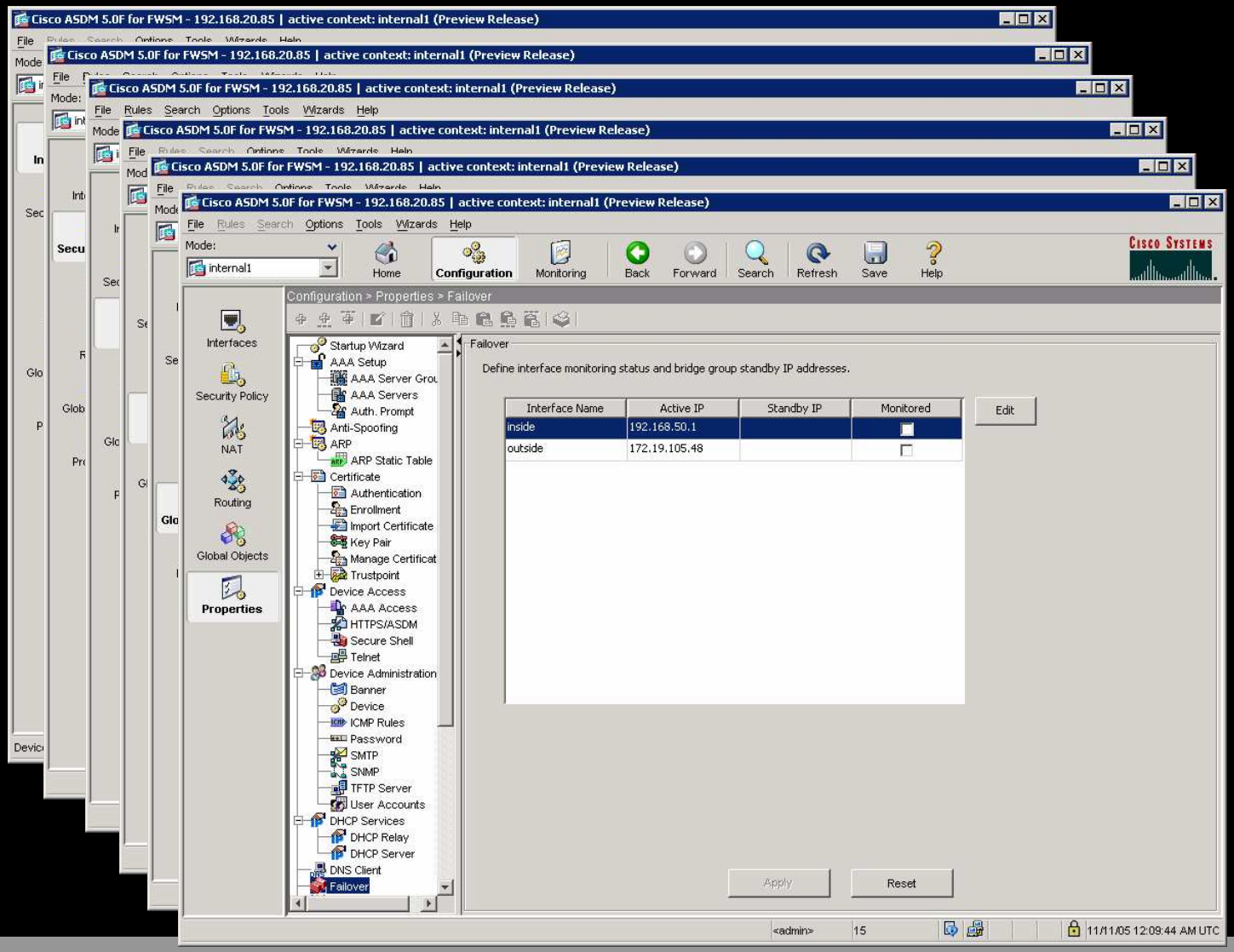
  Firefox 1.0 with Java Plug-in 1.4.2 or 5.0 (or 1.5.0)

ASDM 5.0(1)F – FWSM Home Window



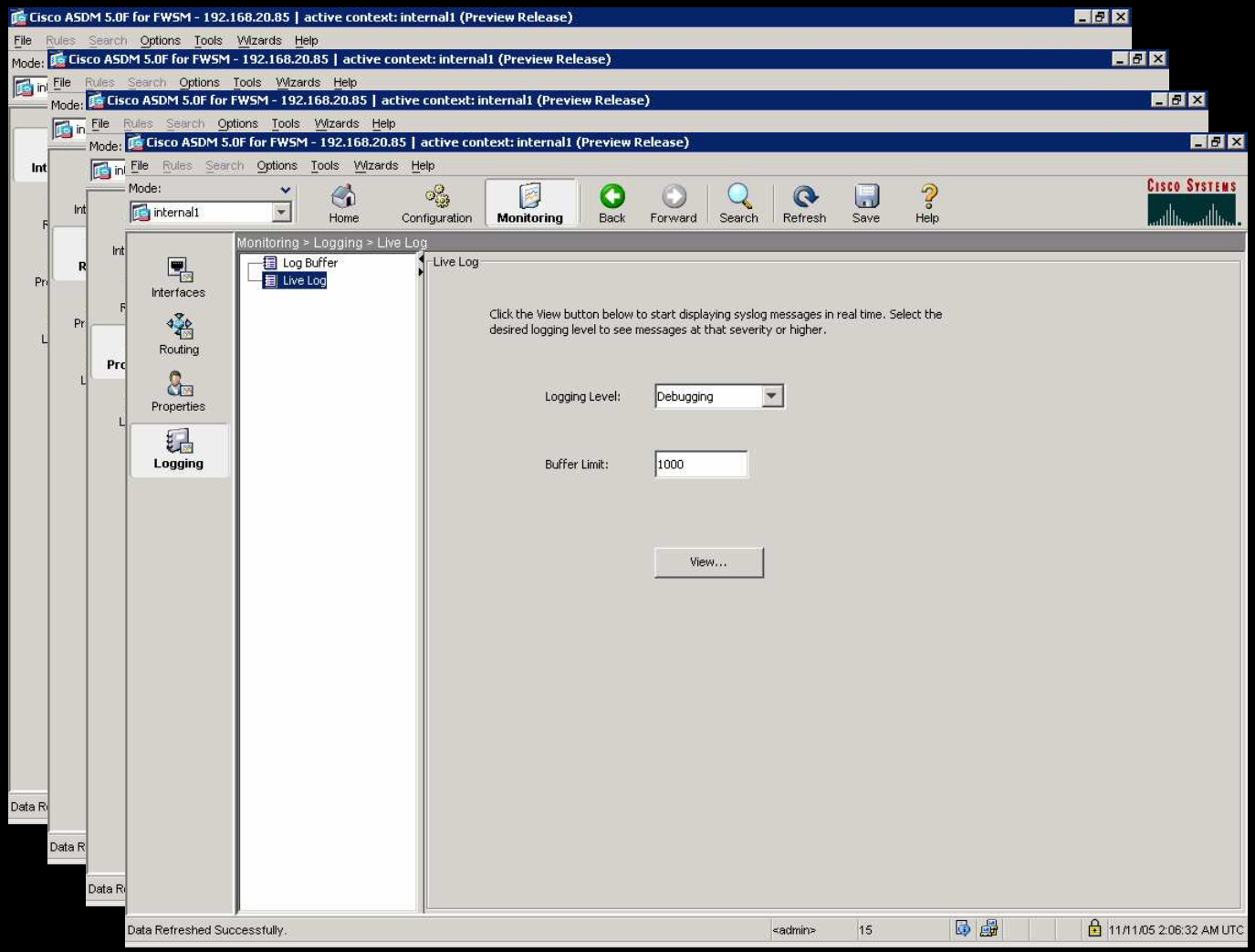
ASDM 5.0(1)F Configuration

- Interfaces
- Security Policy
- NAT
- Routing
- Global Objects
- Properties



ASDM 5.0(1)F Monitoring

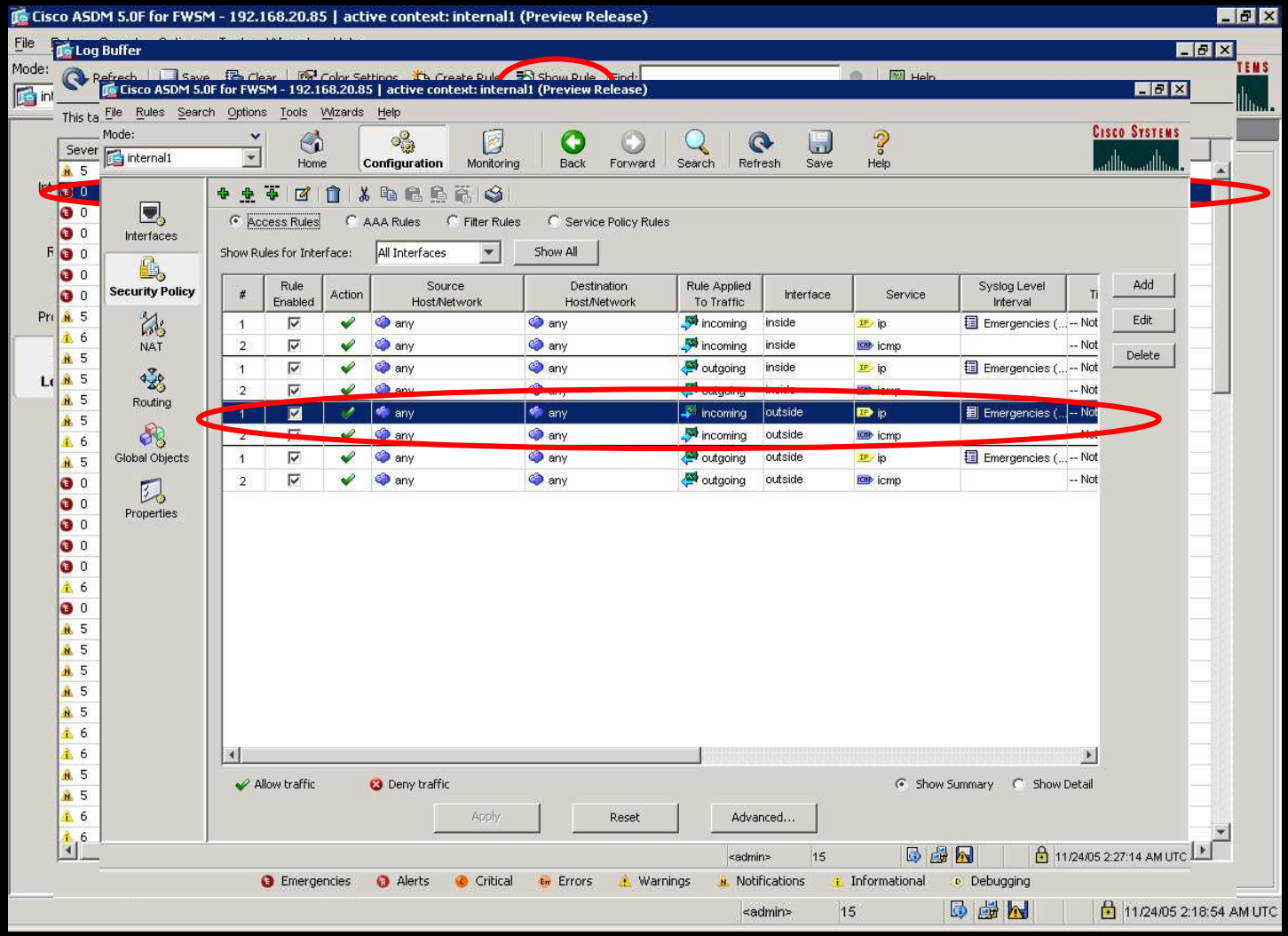
- Interfaces
- Routing
- Properties
- Logging



ASDM 5.0(1)F Support of FWSM3.1

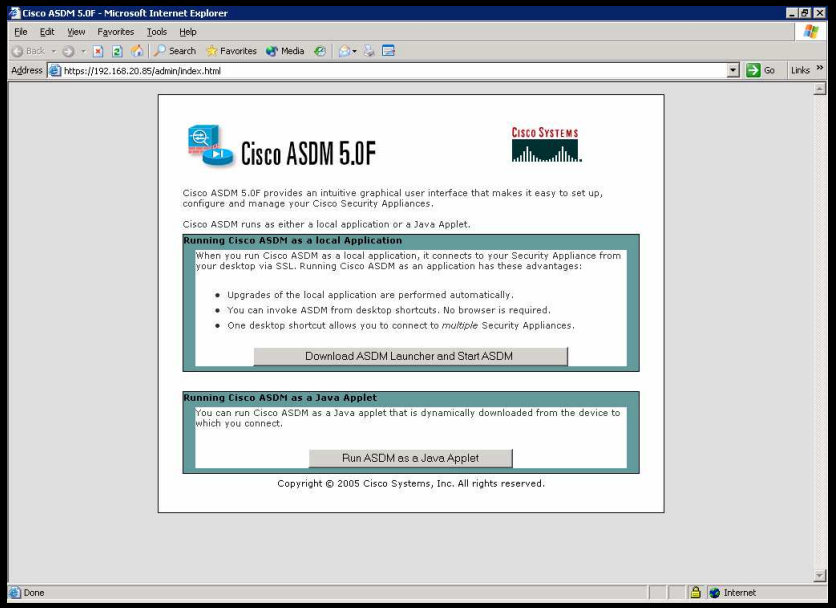
- Supports all the new configuration features of FWSM 3.1 (IPv6 excluded)
- Includes the new management features in ASDM 5.0 for ASA/PIX such as Live Log, Service Policy Rules Table, File Management, Upgrade Software, and a new GUI look-and-feel
- Syslog to ACE Correlation
- Create the opposite ACE rule to permit or deny traffic
- Identify the ACE that generated the syslog
- Set different color for different syslog levels
- Search on any text in the syslog table
- Better support for handling many contexts – context caching and display a list of contexts
- Run ASDM in demo mode which doesn't require a live FWSM
- Number of ASDM sessions in multi mode is increased to 80 from 32

ASDM 5.0(1)F Syslog Correlation Feature



ASDM 5.0(1)F Launcher

- Windows
  - browser mode
  - local mode
- Solaris and Linux
  - browser mode
- To run ASDM in local mode, you must first install the ASDM Launcher on your PC. You will only need to do this once



ASDM Launcher: no more dependency on browser - only need to install the Java Plug-in

ASDM 5.0(1)F Demo Mode

- allows you to see what ASDM looks like without having a live FWSM
- simulate the monitoring data!
- Limitations
  - File/Disk operations will not be supported
  - monitoring and logging data are simulated. Historical monitoring data is not available

FWSM3.1 & ASDM 5.0(1)F Training

Usability, Scalability and Performance

CLI Changes

- Make FWSM3.1 CLI more like IOS
  - Command completion
  - Command syntax check
  - Context sensitive help
  - Lower level command execution
  - Command line editing
    - ^K - delete from cursor to the end of the line
    - ^U - delete from cursor to the start of the line
    - ^E - Move the cursor to the end of the line
    - ^Y - recall the most recent delete
    - ^L - redisplay the current line
  - Command-alias

FWSM3.1 CLI Screen Snapshots

```
FWSM# dir disk:?
  disk:/internal1.cfg    disk:/internal2.cfg
FWSM# dir disk:
```

```
FWSM# changeto contest admin
                    ^
ERROR: % Invalid input detected at '^' marker.
```

```
FWSM(config)# show run
: Saved
:
FWSM Version 3.1(0)103 <system>
!
resource acl-partition 12
hostname FWSM
…
```

```
FWSM(config)# help logout
USAGE:
        logout

DESCRIPTION:
logout          Exit from current user profile to unprivileged mode
```

```
FWSM(config)# command-alias exec ctx show context

FWSM(config)# ctx
Context Name      Class      Interfaces            Mode         URL
*admin            default    Vlan10                Routed       disk:/admin.cfg
 internal1        default    Vlan105,Vlan50        Routed       disk:/internal1.cfg
```

New Inspect Architecture

- Significant change from 2.3
- “fixup” now is referred to as “inspect”
- fixup CLI (fixup protocol xxx <port>) is supported but is deprecated and MPC mechanism should be used going forward

Extend Packet Capture Support

FWSM3.1 Packet Capture consists of

- Capabilities for packet sniffing and network fault isolation
- FWSM can track packet information for traffic that passes through it, including management traffic and inspection engines
- IPv6 support
- Configuration example
  - capture <name> type <data_format> [access-list <access-list_name>] interface <interface>

"Sessions" for non TCP/UDP Flows

- All non TCP/UDP packets were handled by Session Management and not Fast Path prior to 3.1
- FWSM3.1 inserts sessions in Fast Path for these type of traffic resulting in performance improvements
- Use following when debugging non tcp/udp sessions (see next slide)
  - show connection
  - show np 3 stats

Debugging Non TCP/UDP "Sessions"

Note non tcp/udp connections

```
FWSM# sh conn
2 in use, 3 most used
 Network Processor 1 connections
PROT:80 out 50.1.1.1 in 50.1.2.1 idle 0:00:30 Bytes 94
TCP out 50.1.1.1:39390 in 50.1.2.1:23 idle 0:00:02 Bytes 1701 FLAGS - UBOI
 Network Processor 2 connections
Multicast sessions:
 Network Processor 1 connections
 Network Processor 2 connections
IPv6 connections:
```

"Other Fixup" field will increment due to 1st packet hitting session management

```
FWSM# sh np 3 stats
-------------------------------------------------------------
                    Slow Path Statistics
-------------------------------------------------------------
  Packets from Fast Path
…
Session Management Statistics
  ----------------------------
  Session Mgmt Inserts   : 4
  TCP Fixups             : 1
  UDP Fixups             : 0
  ICMP Fixups            : 33
  Other Fixups           : 3
```

Miscellaneous Scalability Improvements

- 250 virtual context (from 100)
  - maximum number of context (250) should be managed properly amongst available resources
- Overall ACL memory usage improvements
  - Includes filters, fixup rules, regular ACLs, AAA rules, …
  - Early expectations are over 10% and 30% improvements of overall ACL memory usage in best case scenarios for single and multi mode respectively
- SIP fixup improvements
  - SIP signaling implementation will use regular pin-holes rather than “established rules” (NP3 limited resource)
  - Total concurrent SIP call should improve above 5000 (depending on available system resources)

FWSM3.1 & ASDM 5.0(1)F Training

Network Integration

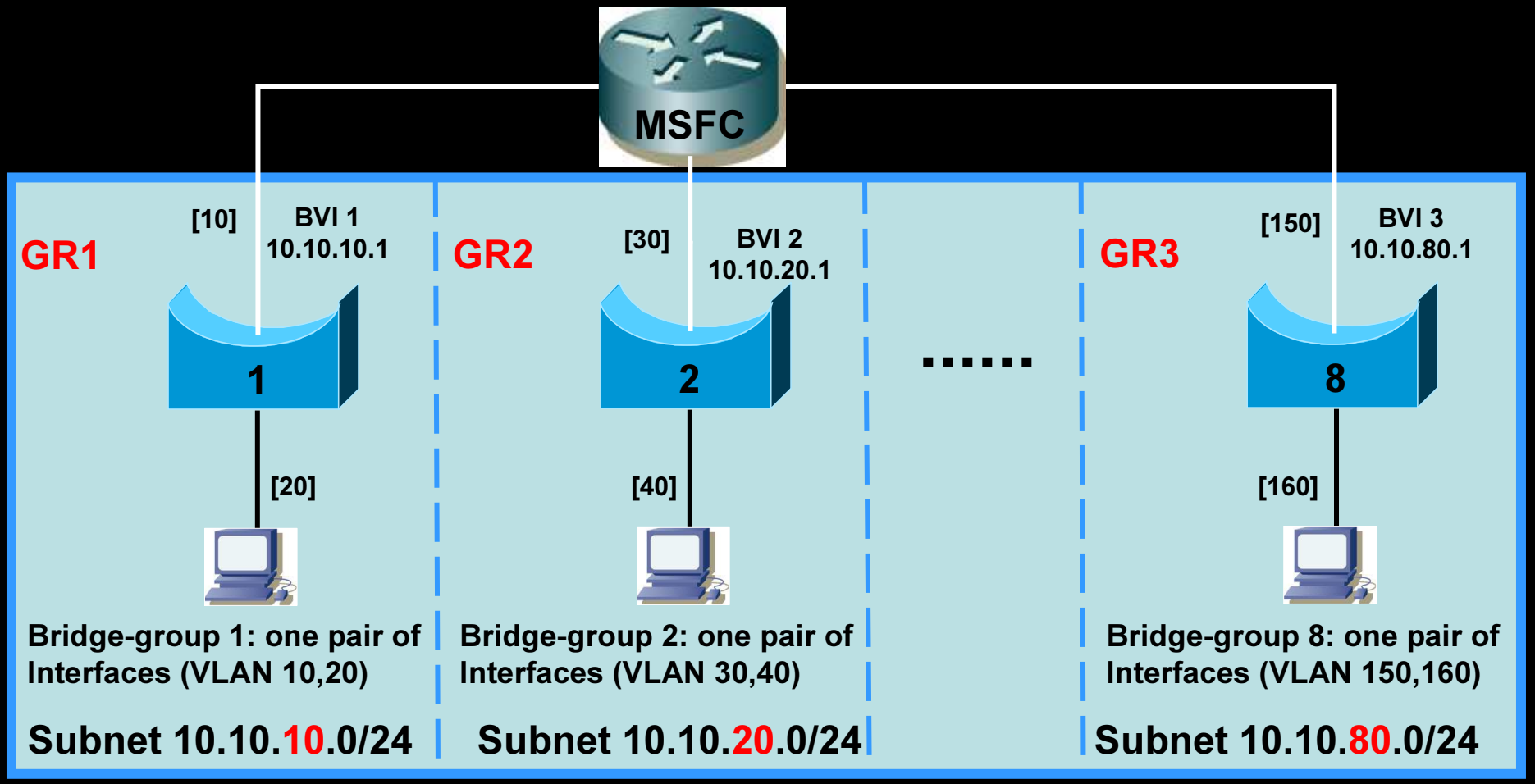
Transparent Firewall Multi Pair Interface

- Pre FWSM3.1 issues: maximum of 2 interfaces per transparent firewall. Made scalability and managing the firewall cumbersome.
- FWSM3.1: No extra license necessary to benefit from increased number of interfaces
- FWSM3.1 Notes
  - Interface names unique within one context.
  - Inter-group Interfaces can not talk to each other
  - Max number of 8 pairs (groups) allowed per context
  - Each interface group will have its own IP address, and there is one default route per context. The IP address can be set through “interface BVI”.
  - No overlapping subnet between groups

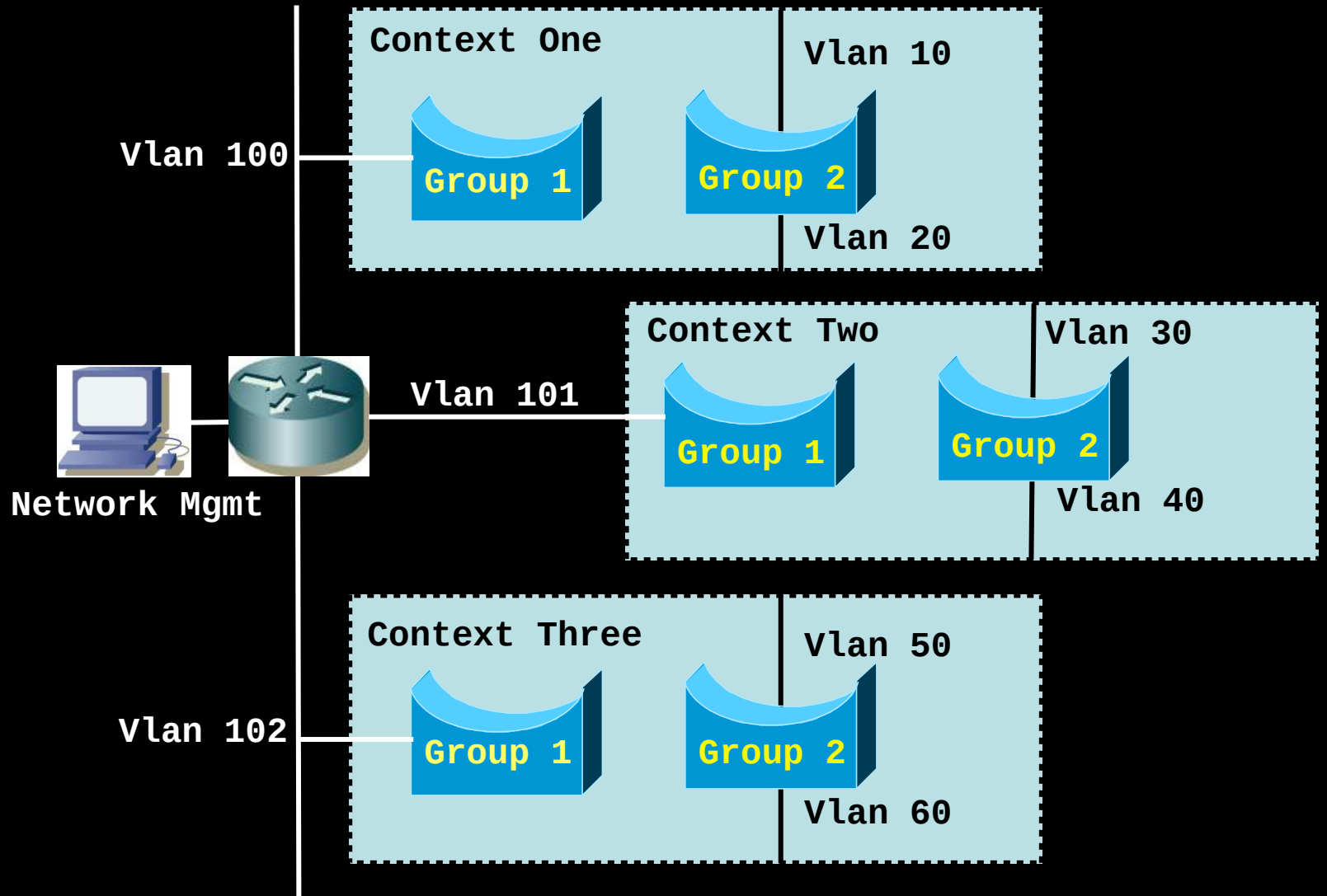
Significant Transparent Firewall Enhancements

- Availability of up to 8 pairs of interfaces within a transparent firewall, including in virtual firewall mode
- Sessions are created in the network processors' fast path for non UDP or TCP protocol (example: GRE) as well as IP multicast traffic

Multi Pair Interfaces in TFW



Practical Application (TFW management)

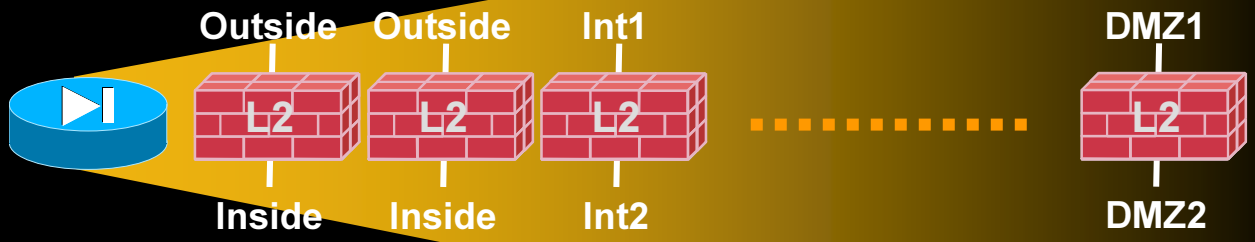


FWSM3.1 Multi Mode

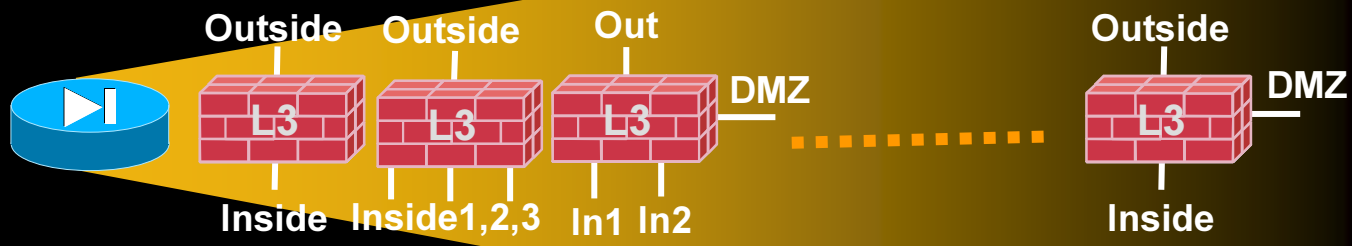
- Scales up to 250 contexts per blade
- Transparent and Routed mode virtual contexts can coexist on the same blade

FWSM2.x Multimode: L2 XOR L3

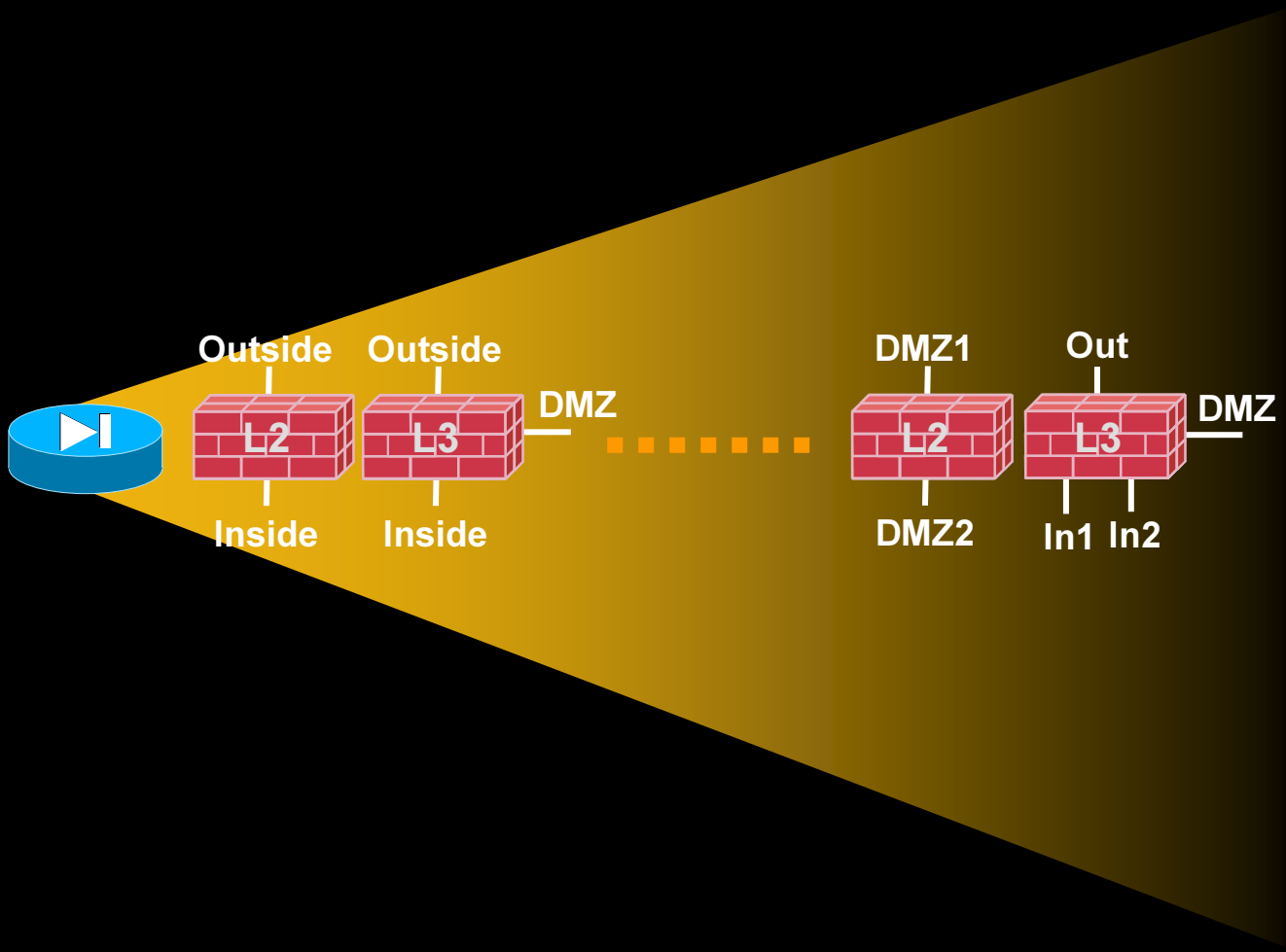
Multimode Transparent



Multimode Routed



FWSM3.1 Multi Mode (MIXED L2 & L3 VFW!)



FWSM3.1 Multi Mixed Mode

Context mode can be set in individual context's configuration and can be Transparent or Routed Mode

```
FWSM/internal2(config)# firewall ?
configure mode commands/options:
  transparent  Switch to transparent mode
FWSM(config)# show context
Context Name      Class      Interfaces            Mode         URL
*admin            default    Vlan10                Routed       disk:/admin.cfg
 internal1        default    Vlan105,Vlan50        Routed       disk:/int1.cfg
 internal2        default    Vlan106,Vlan51        Transparent  disk:/int2.cfg
```

Shared Interfaces: Do not share interfaces between transparent and routed contexts. As before no sharing between transparent contexts!

FWSM3.1 & ASDM 5.0(1)F Training

Address Translation and ACL enhancements

Nat-control options

- FWSM3.1 has nat-control disabled by default that allows inside hosts to communicate with outside network without NAT
- A flag is set in the slow path for each virtual firewall.
- This flag is used while allocating Xlates

```
[no] nat-control
```

Debugging NAT Control Issues

- ‘show np 3 vft vfw_id’ will show the status of nat-control

```
FWSM/internal1# show np 3 vft 2
--------------------------------
Slow Path Virtual Firewall Table
--------------------------------
Context Name                  : internal1 (#2)

   Xlate Timeout              : 3:00:00 sec
   AAA Absolute Timeout       : 0:05:00 sec
   AAA Inactivity Timeout     : 0:00:00 sec
   TCP MSS Min                : 0 Bytes
   TCP MSS Max                : 0 Bytes
   Syslog Mask (Bits 96-127)  : 0x0
   Syslog Mask (Bits 64-95)   : 0x7f
   Syslog Mask (Bits 32-63)   : 0xffffffff
   Syslog Mask (Bits 00-31)   : 0xffffffff
   Virtual Http Address       : 0.0.0.0
   Virtual Telnet Address     : 0.0.0.0
   ACL Deny Flow Max          : 4096
   ACL Alert Interval         : 300 sec
   MAC List                   : None
   Syslog Level               : 7
```

```
   Flags                      : 0x80000
         |- Nat Control           : Disabled
         |- VF                    : Enabled
         |- ICMP Fixup            : Disabled
         |- ICMP Fixup Error      : Disabled
         |- Firewall Mode         : Router
         |- Same Security Traffic : Disabled
         |- Intra Ifc Traffic     : Disabled
         |- New Connections       : Allowed
         |- Fixup Packets         : Allowed
         |- No DNS Alias Inbound  : Disabled
         |- No DNS Alias Outbound : Disabled
         |- HTTP Redirect Warning : Disabled
         |- Reset Inbound         : Disabled
         |- AAA Telnet Challenge  : Enabled
         |- AAA FTP Challenge     : Enabled
         |- AAA HTTP Challenge    : Enabled
         |- AAA HTTPS Challenge   : Enabled
         `- AAA Config Style      : Not Configured
   ----------------------------------------------
```

Increase Number of Global Statements

- Number of global statements is increased form 1,000 (FWSM2.x) to 4,000
- Global statements includes both NAT and PAT
- Global PAT support
  - extremely memory consuming
  - in case of PAT, scale up to 2,000

Overlapping Static Configuration

- Overlapping static configurations were allowed in initial versions of FWSM 1.x
- In FWSM 2.x code the actual root cause of the tree handling code was fixed
- In FWSM 3.1, overlapping configurations are supported again
- Sample Configuration
  - static (inside,outside) 41.1.1.10 40.1.1.2 netmask 255.255.255.255
  - static (inside,outside) 41.0.0.0 40.0.0.0 netmask 255.0.0.0 0 0

Time-range

- Provides a way to specify a time interval when connectivity to the specified destinations is permitted or denied. Multiple time-ranges can be defined. The command allows easy and routine control of traffic connectivity through the firewall device
  - define the time range
  - specify time-range option on access-list to describe the allowed access time

Time based ACL

- Configure time-range and apply it to ACL

```
FWSM(config)# show run time-range
!
time-range weekdays
 periodic weekdays 8:00 to 16:59
!
FWSM(config)# show run access-list
access-list outside_mpc_in remark Only www traffic during weekdays
access-list outside_mpc_in extended permit tcp any any eq www time-
range weekdays
```

- Debugging may be done via:
  - debug acl config
  - show access-list

ACL Options

- Useful new options
  - "time-range"
  - "inactive" to turn off the ACL

```
access-list outside_in extended permit tcp any object-group mail-servers
eq smtp inactive
```

Debugging ACL issues

- show access-list will give ACEs status in the PC side (inactive ACE does not increase its hit count)
- NP key flag indicating active/inactive status of ACL can be obtained from [no] debug acl config

```
FWSM/internal1# show clock
21:04:49.590 UTC Tue Nov 22 2005
FWSM/internal1# sh access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list ALLOW; 2 elements
access-list ALLOW line 1 extended permit ip any any (hitcnt=176)
access-list ALLOW line 2 extended permit icmp any any (hitcnt=0)
access-list outside_weekend; 1 elements
access-list outside_weekend line 1 extended permit ip any any time-range weekends
(hitcnt=0) (inactive)
```

ACL Editing

- Provides ability to change the order of ACEs by specifying the line number
- Note that reordering ACEs has a performance hit
- Debugging may be done via:
  - debug acl config
  - debug acl error
  - show access list

ACL Interface Parameter

- Provides ability to configure an ACE with interface name. The ACE will get updated with proper IP addresses
- Configuration may be done by specifying “interface <if_name> in access-list definition
- Debugging may be done via:
  - debug acl config
  - debug acl error

FWSM3.1 & ASDM 5.0(1)F Training

Modular Policy Framework

Modular Policy CLI

- Based on Modular Policy Framework (MPF)
- Addresses the need to have greater granularity and flexibility in configuring network policies.
- Examples
  - Create timeout configuration that is specific to a particular TCP application as opposed to setting timeouts that is applied globally
  - Set maximum connection limits that are specific to a particular TCP/UDP application

Modular Policy CLI paradigm

Immediate benefit: IOS like CLI

FWSM 1.x, 2.2, 2.3

```
nameif vlan315 users security80
nameif vlan316 outside security0
nameif vlan298 fover security50
nameif vlan326 extranet security20
nameif vlan324 inside security100
fixup protocol http
ip address users 137.222.250.186
    255.255.255.240
ip address outside 137.222.250.218
    255.255.255.240
ip address fover 137.222.251.126
    255.255.255.252
ip address scumnet 193.60.198.2
    255.255.255.192
ip address inside 137.222.249.251
    255.255.255.224
```

FWSM 3.1

```
interface VLAN315
    ip address 137.222.250.186
            255.255.255.240
    nameif users
    security 80
    no shut
!
class-map test
    match access-list 100
!
Policy-map test
    class test
            inspect http
```

MPC Paradigm

Distinct domains between configuration and runtime data

```
FWSM-6K4(config)# sh nameif
Interface                  Name                       Security
Vlan822                    mgmt                        82
FWSM-6K4(config)# sh run nameif
!
interface Vlan822
 nameif mgmt
 security-level 82
!
FWSM-6K4(config)#
```

Automatic conversion of Pre FWSM3.1 configurations

```
FWSM-6K4(config)# sh run fixup
INFO: All 'fixup' commands have been converted to 'inspect' commands.
Please use 'show running-config service-policy' in conjunction
with 'show running-config policy-map' to view the new configuration.
```

Modular Policy CLI Definitions

- Class-map: Specify traffic class through specific traffic identification based on its packet contents
- Policy-map: Associate actions to each of the above class of traffic in order to formulate policies
- Service-policy: Activate policies through associating policy-map with one or more interfaces

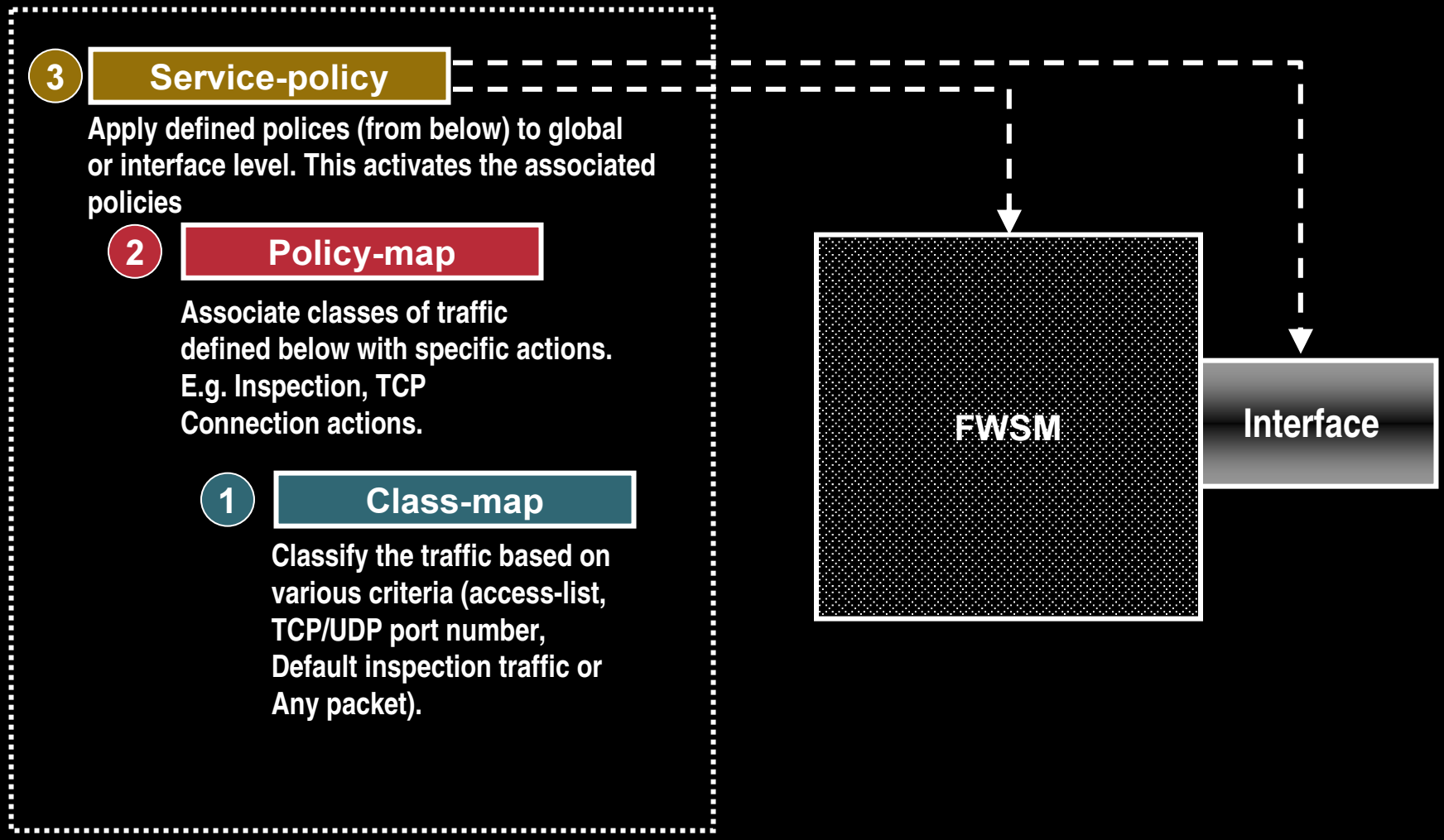
class-map matching criteria

- Access list using IP 5-tuple (protocol, Source/Destination IP address, Source/Destination port)
- TCP/UDP port number
- Default inspection traffic
- any packet

Policy-map and service-policy

- Policy-map action options are:
  - Inspection (fixup)
  - Set maximum number of connections.
  - Other connection actions such as setting maximum number of embryonic connections will not be done in the first release of MPC (3.1)
- Service-policy may activate the above policy on global basis or on per interface basis

MPC Logical View



MPC Example

Set connection idle timeout for a given TCP stream

1. Create an ACL that catches the traffic subject to the custom idle timeout

```
access-list custom permit tcp host 10.1.1.1 host 192.168.1.1 eq 865
```

2. Define a class-map whose match criteria is the ACL we just defined

```
class-map custom-timeout
    match access-list custom
```

3. Create a policy map to apply connection-related parameters to the custom class

```
policy-map timeout
    class custom-timeout
        set connection timeout tcp 0:18:55
```

MPF Constraints

- The interface “service-policy” takes precedence over global service-policy if both are configured
- Only “class inspection_default”may have multiple inspects under it. Other user defined classes can only have one “inspect <service> per class.

Debugging MPC Issues

- **No explicit show/debug commands related to MPC**
  - **use inspect related show/debug**
  - **use show “conn” or “xlate” as before**

FWSM3.1 & ASDM 5.0(1)F Training

Deep Packet Inspection (HTTP)

Application Firewall (deep packet inspection)

- enhanced HTTP inspection feature, is also known as an application firewall (AFW) provides deep analysis of web traffic
- AFW enables granular control over HTTP sessions to prevent abuse of the HTTP protocol
- AFW allows administrative control over applications that attempt to tunnel over port 80, such as applications like gotomypc and the various forms of Instant Messenger
- AFW features known as deep inspection or application intelligence

Application Firewall Feature Summary

- RFC compliance enforcement
- HTTP request method authorization and enforcement
- Response message validation
- Port Misuse and enforcement
- MIME type enforcement
- Transfer encoding type validation
- Content control based on message data content and type
- URI length enforcement
- Message size enforcement
- NO application awareness (web services, XML)
- NO flow decryption through the box

Application Firewall Configuration Components

- class-map
  - Identify the traffic for inspection. The port to use for traffic inspection is identified here …
- http-map
  - Describes the parameters that http inspection will use for processing
- Keywords
  - (and parameters) specific to the function they perform. e.g. content-length has minimum and maximum acceptable size limits. Out of range values initiates specified actions
- Actions
  - allow, drop, reset, and log

Application Firewall Keywords and Functions

- **content-length:** Inspection based on the length of the HTTP content
- **content-type-verification:** Inspection based on the type of HTTP content
- **max-header-length:** Inspection based on the length of the HTTP header
- **max-uri-length:** Inspection based on the length of the URI
- **port-misuse:** Inspection of p2p, IM, and tunneled applications
- **request-method:** Inspection based on the HTTP request method
- **strict-http:** Enables strict HTTP inspection
- **transfer-encoding:** Inspection based on the transfer encoding type

Application Firewall Configuration Steps

- **Create a class-map for http inspection**

```
sh run class-map http-port
!
class-map http-port
 match port tcp eq www
!
```

- **Create http map to define parameters for http inspect**

```
sh run http-map inbound-http
!
http-map inbound-http
 content-length min 100 max 200 action reset log
 content-type-verification match-req-rsp action reset log
 max-header-length request 100 action reset log
 max-uri-length 100 action reset log
 port-misuse p2p action drop
 port-misuse im action drop
 port-misuse default action allow
```

Application Firewall Configuration Steps

- **Create a policy map for http inspection**

```
sh run policy-map outside_policy
!
policy-map outside_policy
 class http-port
  inspect http inbound-http
```

- **Create service policy to define scope of inspection**

```
sh run service-policy
service-policy global_policy global
service-policy outside_policy interface outside
service-policy inside-policy interface inside
```

Deep Packet Inspection Example (MPC)

Deny FTP get command

1. Create an ACL that catches the traffic

```
access-list custom permit tcp any any eq ftp
```

2. Define a FTP map that denies GET commands

```
ftp-map nogetforyou
    request-command deny get
```

3. Create a class map to catch FTP traffic

```
class-map ftp
    match access-list custom
```

4. Create a policy map that uses the FTP-map

```
policy-map ftp
 class ftp
  inspect ftp strict nogetforyou
```

5. Apply the policy-map to an interface

```
service-policy ftp interface inside
```

Show and Debug Commands

- Verify configuration via
  - show running-config http-map
  - show running-config ftp-map
  - show running-config class-map
  - show running-config policy-map
  - show running-config service-policy
- Perform debugging via
  - show service-policy

FWSM3.1 & ASDM 5.0(1)F Training

Inspection Engines Enhancements

Inspection Engines Enhancements

- “fixup” command is now replaced with “inspect”
- Each of the inspection engines may be enabled and disabled through CLI

Enhanced FTP Inspection

- Enhance existing strict FTP inspection
- Include FTP request command filtering
- Include additional security checks

FTP Inspection

- **Basic FTP inspection**

  FWSM/internal1(config)# policy-map global_policy

  FWSM/internal1(config-pmap)# class inspection_default

  FWSM/internal1(config-pmap-c)# inspect ftp

- **Strict FTP inspection**

  – When FTP Tunneled over HTTP it Prevents web browsers from sending embedded commands. It will also contain the Basic FTP Inspection

  – If FTP request does contain commands which is not RFC compliant, connection will be closed and syslog will be generated

  FWSM/internal1(config-pmap-c)# inspect ftp strict

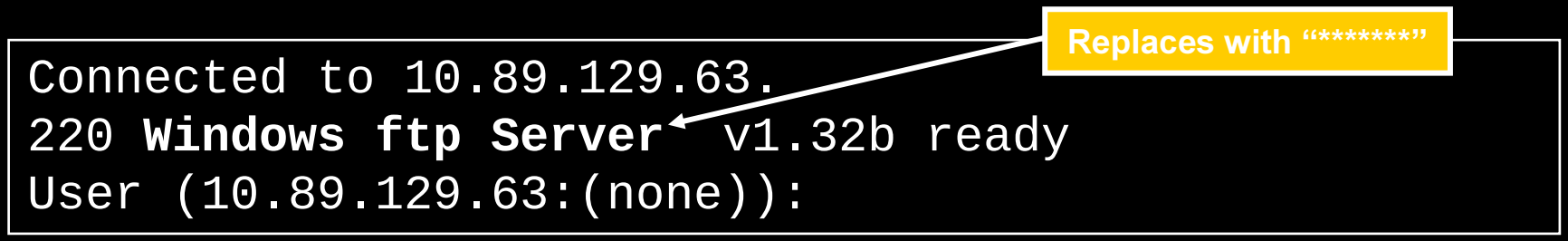
FTP Command Filtering Configurations

- **Allow or disallow specific ftp commands. If disallowed, connection will be closed and syslog will be generated.**

```
sh run ftp-map
!
ftp-map ftp-in
 request-command deny appe cdup
 ! [dele get help mkd put rmd rnfr rnto site stou]
!
```

Additional FTP Inspection Security Checks

- **Prevent from displaying server system type**




```
FWSM(config-ftp-map)# ?
Ftp-map configuration commands:
  mask-syst-reply  Mask reply to syst command
  no               Negate a command or set its defaults
  request-command  FTP request command inspection
```

- **Prevent a client guessing valid User name (RFC2577)**
  - **(Not Configurable) Will not allow the Server to return a "Invalid Username" For Older FTP Servers**

Show and Debug CLIs

- Configuration
  - show running-config http-map
  - show running-config ftp-map
  - show running-config class-map
  - show running-config policy-map
  - show running-config service-policy
- Debugging
  - show service-policy

ESMTP Inspection

- Currently, FWSM supports SMTP inspection
- Customers use Mail Servers that leverage SMTP Extensions that were defined in follow-on RFCs
- These extensions are commonly used with Microsoft Exchange
- FWSM3.1 inspects additional supported ESMTP commands for RFC compliance
  - Adds support for eight extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET)
  - Other extended SMTP commands, such as ATRN, STARTLS, ONEX, VERB, CHUNKING, and private extensions are not supported
- Since SMTP and ESMTP fixups operate on the same port, only one of them can be active (first configured)

ESMTP Inspection Configuration

- **Specified as part of policy-map criteria**

```
FWSM/internal2(config-pmap-c)# inspect ?
mpf-policy-map-class mode commands/options:
  ctiqbe
  dns
  esmtp
  ftp
  …
  smtp
  snmp
  sqlnet
  sunrpc
  tftp
  xdmcp
```

TCP Stream Reassembly

- Application Inspections (fixup/inspect) cannot reliably inspect application data when the data is segmented by TCP. The problem is especially acute with inspections that filter application data. In such cases, a failure to reject segmented data or failure to reassemble and inspect the data is a breach of security.
- This feature will allow fixups to process TCP streams rather than packets
- specific fixups that will leverage this feature are SIP, FTP, Skinny and ESMTP

TCP Stream Reassembly

- There are no configuration CLI/ASDM for this feature
- Debug
  - debug fixup tcp (useful if log messages are reported)
- Logging outputs
  - Default log level: 4/Warning
  - 507001: TCP Proxy terminated connection from <src> to <dst> - reassembly limit of <limit> bytes exceeded
- Caveats/Limitation
  - When the reassembly limit is exceeded, the log message is sent and the connection reset

ActiveX/Java Filtering

- Remove ActiveX objects from HTTP traffic as it passes through FWSM
- Remove Java applets from HTTP traffic as it passes through FWSM
- Configuration may be done via:
  - [no] filter activex | java <port>[-<port>] | except <lcl_ip> <mask> <frgn_ip> <mask>

Connection Optimization for URL Filtering

- Currently, FWSM creates a new TCP connection to the url-server for each HTTP request it needs to validate
- This feature enhances performance by creating the TCP connection once and using it for many requests. Instead of just one persistent connection per url-server, the system will create a pool of connections (the default is 5 connections and can be set from 1 to 100) and round-robins between each connection
- Both Websense and N2H2 are supported
- [connections <number>] is added too url-server CLI

PPTP Enhancements

- Uses GRE tunnels to encapsulate packets between client and server
- Stateful inspection will be added
- “sessionizing non TCP/UDP traffic” improvement will be used for creating data channels
- Configuration may be done via:
  - “inspect pptp” configuration in policy-map
- Debugging may be done via:
  - “show connection” will reflect the GRE tunnels for PPTP sessions on the NPU side.

FWSM3.1 & ASDM 5.0(1)F Training

Core IP Enhancements

IPv6 Support

- Dual IP stack supporting IPv4 and IPv6
- Neighbor discovery. This is the IPv6 equivalent of ARP
- IPv6 static routing
- IPv6 ACLs
- Security checks of IPv6 header, including extension headers
- ICMPv6 support
- Separate IPv6 access list, conn, fragment database, host, routing (static only) and xlate tables. These would only be allocated if IPv6 is configured.
- Fixups modified to support IPv6:
  - TCP (sequence number randomization, open and close state transition enforcement, and TCP option policing)
  - UDP
  - FTP
  - HTTP
  - ICMP
  - SMTP
- Management access to the device using HTTP, SSHv1, SSHv2 and Telnet will be supported for both IPv4 and IPv6. Ping to and from the device will also be supported for both IPv4 and IPv6
- Only software based and not accelerated!
- ONLY IN ROUTED

IPv6 Configurations

- IPv6 Address
  - [no] ipv6 address autoconfig
  - [no] ipv6 address [ipv6-prefix/ prefix-length [eui-64]]
  - [no] ipv6 address [ipv6-address link-local]
- IPv6 neighbor discovery (duplicate address detection, neighbor solicitation, router advertisement parameters)
  - [no] ipv6 nd dad attempts attempts-value
  - [no] ipv6 nd ns-interval [ns-interval]
  - [no] ipv6 nd prefix ipv6-prefix/ prefix-length|default [[valid-lifetime preferred-lifetime]|[at valid-date preferred-date]|infinite|noadvertise| off-link|no-autoconfig]]
  - [no] ipv6 nd ra-interval [ra-interval]
  - [no] ipv6 nd ra-lifetime [ra-lifetime]
  - [no] ipv6 nd reachable-time [reachable-time]
  - [no] ipv6 nd suppress-ra

IPv6 Commands

- Following commands will be added for IPv6 support
  - IPv6 access-list
  - IPv6 route
  - IPv6 neighbor
  - IPv6 ICMP
  - show NP <N> stats
  - show commands

```
FWSM/internal2# show ipv6 ?
  access-list  Show hit counters for access policies
  icmp         Show ICMPv6 access rules configured on all interfaces
  interface    IPv6 interface status and configuration
  neighbor     Show IPv6 neighbor cache entries
  route        Show IPv6 routes
  routers      Show local IPv6 routers
  traffic      IPv6 traffic statistics
```

IPv6 Commands

- Debug commands/output will be changed to reflect IPv6 support
- [no] debug ipv6 icmp | interface | nd | packet | routing
  - icmp: Display debug messages for IPv6 Internet Control Message Protocol (ICMP) transactions (excluding IPv6 ICMP neighbor discovery transactions).
  - interface: Display debug messages for IPv6 interfaces.
  - nd: Display debug messages for IPv6 Internet Control Message Protocol (ICMP) neighbor discovery transactions.
  - packet: Display debug messages for IPv6 packets.
  - routing: Display debug messages for IPv6 routing table updates and route cache updates.
  - Sysloging: Existing syslog messages are changed to support IPv6 addresses in addition to IPv4 addresse

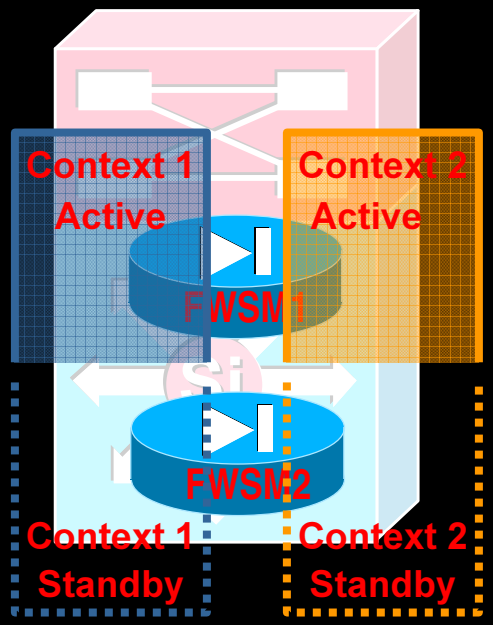
IPv6 Limitations and Caveats

- No IPv6 multicast support
- No support on Failover and Transparent Firewall
- ASDM 5.0(1)F does not support IPv6 management
- No IPv6 support on shared interfaces (multi mode)

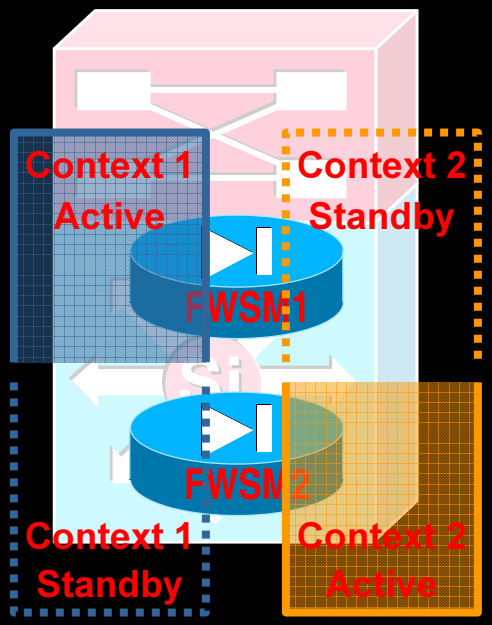
FWSM3.1 & ASDM 5.0(1)F Training

High Availability Enhancements

Active/Standby vs. Active/Active



Active/Standby



Active/Active

Active/Standby and Active/Active

Intra and Inter chassis High Availability

Active/Active Features

- When FWSM is running in virtual firewall mode it is possible to use active/active redundancy
- No special license necessary for failover
- Similar to HSRP (two failover groups are available)
- The group's status is either active or standby
- Virtual firewalls are mapped to a failover group
- Redundancy always functions with a pair of FWSM (one primary, one secondary – both can be active for given virtual firewalls)

Active/Active HA: “primary” vs. “active”

- Just like before, one FWSM is designated primary while the other one is secondary – however, at the failover group level it is now possible to elect the unit which should become active or standby

```
FWSM-6K1/pri/9/act(config-fover-group)# ?
Failover User Group configuration mode:
  help              Help for user Failover Group configuration commands
  interface-policy  Set the policy for failover due to interface failures
  no                Remove user failover group configuration
  polltime          Configure failover interface polling interval
  preempt           Allow preemption of lower priority active unit
  primary           Primary unit has higher priority
  replication       Configure the replication option
  secondary         Secondary unit has higher priority
  <cr>
FWSM-6K1/pri/9/act(config-fover-group)#
```

Active/Active: quick config overview

```
FWSM-6K1/pri/9/act(config-ctx)# sh run context
admin-context Cluster-1-admin
context Cluster-1-admin
  allocate-interface Vlan822
  config-url disk:/transparent.cfg
  join-failover-group 1
!
context one
  allocate-interface Vlan1448
  allocate-interface Vlan448
  config-url disk:/one
  join-failover-group 1
!
context two
  allocate-interface Vlan1121
  allocate-interface Vlan121
  config-url disk:/two
  join-failover-group 2
!
```

Now properties of the failover Group are no longer global!

```
FWSM-6K1/pri/9/act(config-ctx)# sh run failover
| beg group

failover group 1
  preempt
  replication http
  polltime interface 3
  interface-policy 100
failover group 2
  secondary
  preempt 10
  replication http
  polltime interface 3
  interface-policy 52
```

Active/Active: Preemption in action

PRIMARY

```
FWSM-6K1/pri/9/act(config-fover-group)#
Dec 19 2005 09:39:46 system : %FWSM-1-103001: (Primary) No response from other
firewall (reason code = 1).
Dec 19 2005 09:39:46 system : %FWSM-1-104001: (Primary_group_2) Switching to
ACTIVE - HELLO not heard from mate.
Dec 19 2005 09:42:37 system : %FWSM-1-709003: (Primary) Beginning configuration
replication: Send to mate.
Dec 19 2005 09:43:18 system : %FWSM-1-709004: (Primary) End Configuration
Replication (ACT)
Dec 19 2005 09:43:41 system : %FWSM-1-104002: (Primary_group_2) Switching to
STNDBY - Other unit want me Standby
```

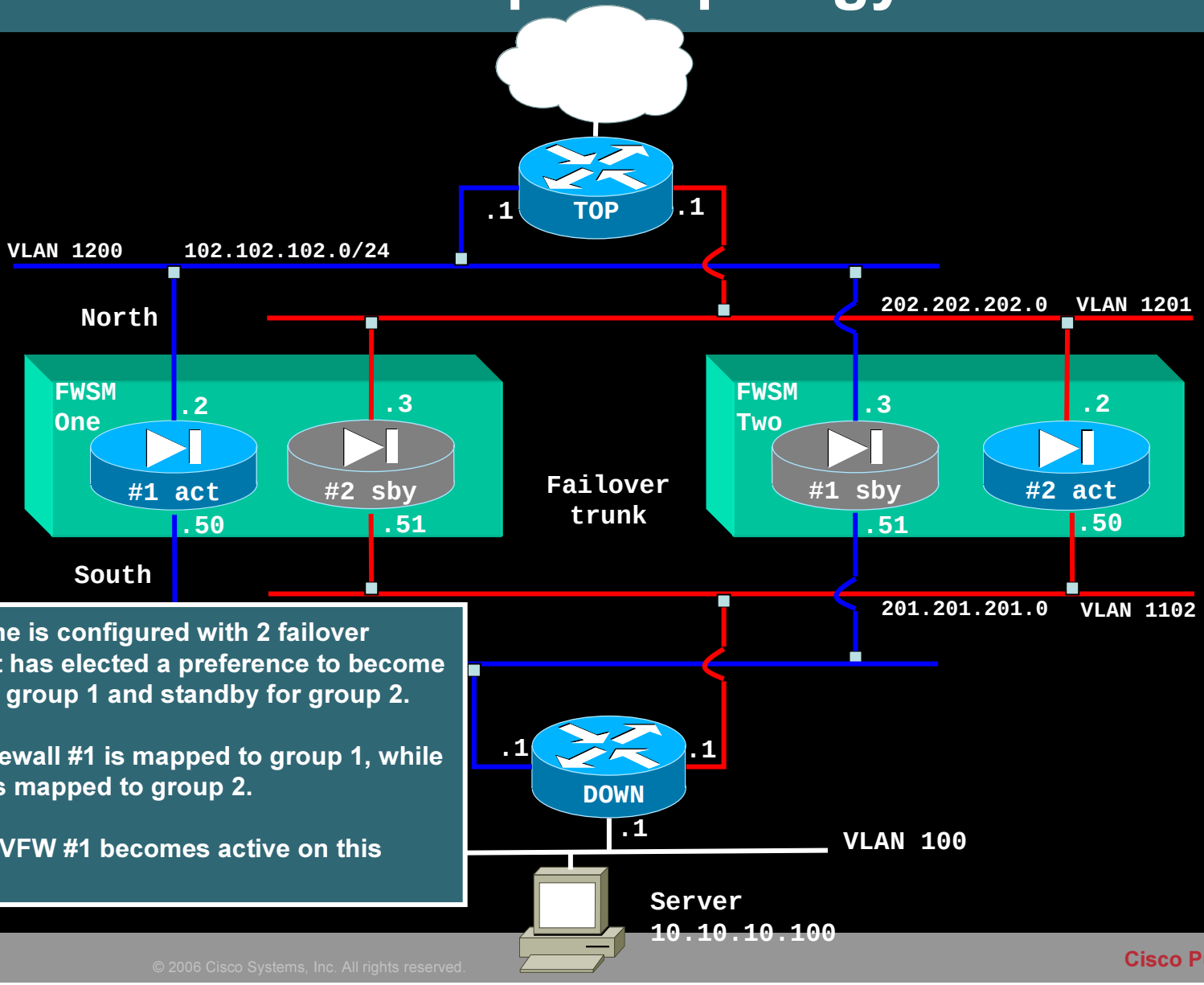
SECONDARY

```
Group 1 Detected Active mate
        Group 2 Detected Active mate
Access Rules Download Complete: Memory Utilization: < 1%
End configuration replication from mate.
        Group 2 preempt mate
Dec 19 2005 11:22:46 system : %FWSM-1-104001: (Secondary_group_2) Switching to
ACTIVE - Failover state check.
```

Active/Active Features (cont)

- Failover is configured by the system administrator. Individual contexts see nothing special regarding failover, except for interface monitoring which remains available as in previous releases
- An entire failover group can be flipped over to the other FWSM if necessary
- Failover is now preemptive if configured to do so – should the other FWSM advertise a higher priority for a given failover group, the FWSM with the lower priority can give up its active role

Active/Active Sample Topology



FWSM One is configured with 2 failover groups. It has elected a preference to become active for group 1 and standby for group 2.

Virtual firewall #1 is mapped to group 1, while VFW #2 is mapped to group 2.

As such, VFW #1 becomes active on this FWSM.

MAC address allocation

- One physical MAC per FWSM (2 MACs total per failover setup, whether act/sby or act/act)
- In active/standby, the active FWSM uses MAC A while standby uses MAC B; if standby takes over it borrows MAC A
- In active/active, the same process exists on per failover-group basis:

  Group 1:

  MAC A used by active, B by standby

  Group 2:

  MAC A used by active, B by standby
- Corollary: don't share interfaces between failover groups

Asymmetric Routing

- 2 options for asymmetric routing on FWSM
  - a) Single FWSM (or within a virtual firewall)
  - b) While in active/active mode
- Option “a” is achieved using a new concept called “ASR group”
- Option “b” is achieved using “ASR group” with active/active redundancy

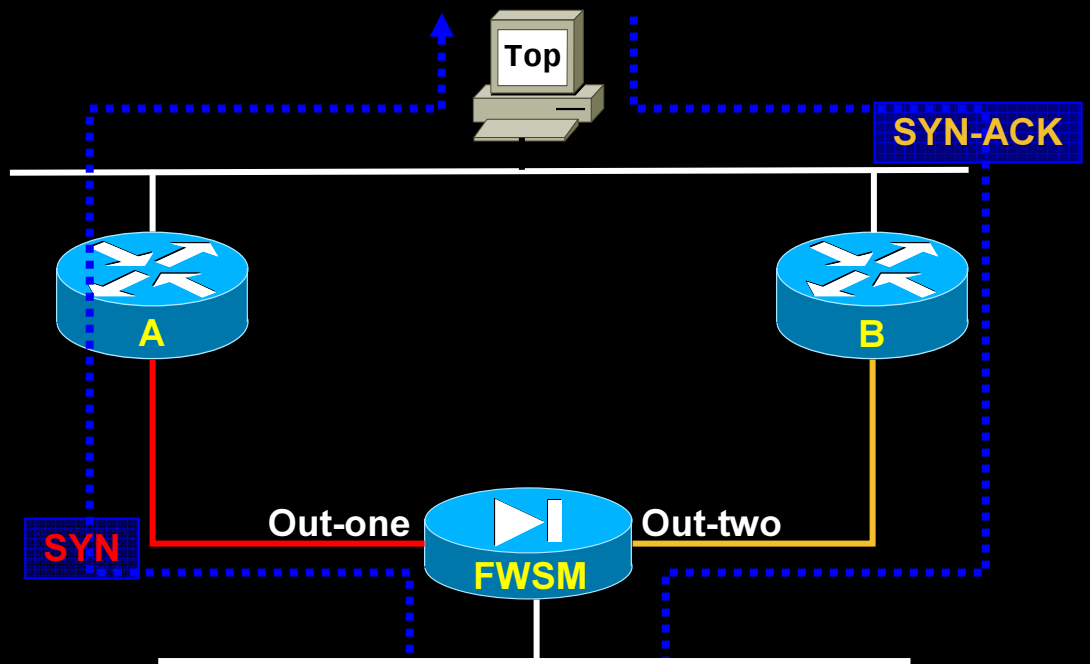
Asymmetric Routing

- Up to 8 interfaces in an ASR group
- 32 groups per FWSM
- Allows traffic to arrive on a different unit or interface than the traffic originated and will be forwarded to the unit or interface where the traffic originally passed through
- Operates in both Multimode and Singlemode
- Operates in both Routed and Transparent mode
- Operates in Failover and Non-failover configuration

Asymmetric Routing (ASR Group)

Client initiates a connection to Top. The initial SYN could take the Router A route, while the SYN-ACK could come back via the Router B route. This is normally not a supported configuration, because connection entries in FWSM are tied to the original source and destination interfaces.

Using the new ASR group concept it is possible for the FWSM to accept the returning SYN-ACK segment even though no corresponding SYN was ever seen on that interface.



Keep in mind that before a session is created, one valid initial packet must have crossed the FWSM. This means that ASR does not disable the state machine. A SYN-ACK will be permitted on a different interface than the original one if and only if a valid SYN matches the returning SYN-ACK!

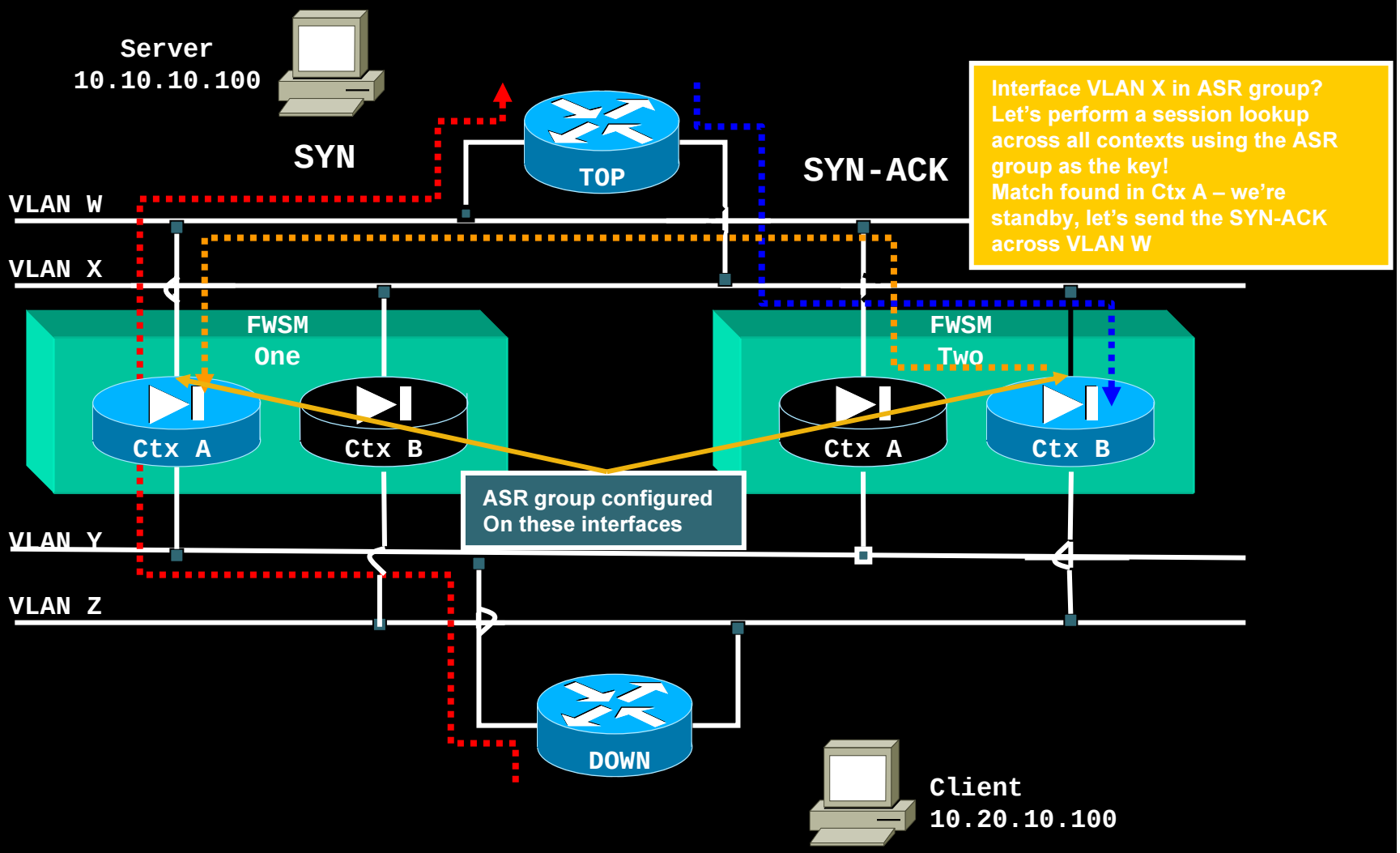
Asymmetric Routing with Active/Active

- With active-active network designs, it is fairly easy to run into an asymmetric routing condition
- Traffic could leave via one FWSM, context A and come back through the other FWSM in the failover pair using a different active context
- With no special provision to take care of this particular condition, traffic would be left out in the dark and dropped
- The active-active code automatically handles traffic wandering off the beaten path and “reroutes” it back to the appropriate context

Symmetric Routing with Active/Active

- TCP and UDP sessions are automatically rerouted using ASR
- ICMP connections are not replicated, therefore ASR can’t help asymmetric ICMP traffic
- ASR is supported both in routed and transparent mode

Asymmetric Routing – Active/Active HA (Only forwarded by Layer2)



FWSM3.1 & ASDM 5.0(1)F Training

Miscellaneous Improvements

SSHv2

- SSH2 is implemented to help increase the compatibility to support wide range of SSH clients.
- Only server side support is implemented.
- The following features are supported:
  - 3DES, AES symmetric ciphers
  - hmac-(sha, md5) algorithms for packet integrity
  - RSA public key algorithm for host authentication
  - Diffie-Hellman-group1-sha1 key exchange method
  - Password based user authentication

SSHv2 Configuration and Debug

- **Configuration may be done via:**
  - **[no] ssh <local_ip> <mask> <if_name>**
  - **[no] ssh timeout <number>**
  - **[no] ssh version 1|2**
- **Debugging maybe done via:**
  - **show ssh sessions [<client_ip>]**
  - **Show debug ssh <debug level>**

Limitations and Caveats

- The user authentication attempt limit is set to 3 – it is not configurable
- Requires 3DES License for SSH V2 to work.
- The cryptographic algorithms used by SSH2 is limited to 3DES and AES. Only SHA and MD5 are available for the integrity.
- SSH2 is limited to a maximum of 100 sessions per physical device, with a further limitation of 5 sessions per security context.
- Several features of the SSH2 drafts will not be implemented. These include
  - X11 Forwarding
  - Port Forwarding
  - SFTP support
  - Kerberos and AFS Ticket Passing
  - Data Compression

Syslog server Failure Policy (TCP transport)

- allow new network access sessions for a TCP-based system log server that is not operational – default is FWSM denies new connections for failed server.

```
hostname(config)# logging permit-hostdown
hostname# show running-config logging
```

VPN Enhancements

- To the box management connections
- Maximal 5 connections for Single Mode and 10 connections for Multiple Mode
- Virtualized

VPN Implementation and Deviations

- Implementation
  - All processing done on PC side
  - NPs punt all control and data packets to PC
- Deviations from PIX7.0
  - no support NAT-T, IPSEC over UDP, cTCP
  - no transport mode except L2L answer mode
  - no inheritance in SA (VPN3k)

SNMPv2c and Additional MIBs

- SNMP v2c is implemented to support 64bit counters preventing “rapid counter rollover” on high bandwidth media
- SNMP v2c is essentially SNMP v1 with 64bit counters. The context and security features of SNMP v2 are not present
- The RFCs that define SNMPv2c are 1901-1907
- MIBs will be on par with PIX7.0

Out of Band Management

- Allows only management traffic to be allowed on configured interfaces.
- This is only allowed in routed mode and not transparent mode
- Configuration via

```
FWSM/admin(config)# int vlan10
FWSM/admin(config-if)# management-only
```

Prompt Display Configuration

- FWSM prompt maybe changed to display available status
- Usage:

  prompt <keyword> [<keyword> ...]
- Syntax:

  keywords:

Hostname	Configures the prompt to display the hostname
Domain	Configures the prompt to display the domain
Context	Configures the prompt to display the current context (multimode only)
Priority	Configures the prompt to display the 'failover lan unit' setting
State	Configures the prompt to display the current traffic handling state
Slot	Configures the prompt to display the slot location (when applicable)
- Example:

  FWSM/internal1/sec/actNoFailover/4(config)#

Miscellaneous Improvements

- **Ping, logging and memory management enhancements**

  Extended ping, logging of memory depletion conditions, and improved checks for detecting memory corruptions

  – Extended ping

  FWSM# ping

  Interface: mgmt

  Target IP address: 10.10.10.2

  Repeat count: [5]

  Datagram size: [100]

  Timeout in seconds: [2]

  Extended commands [n]:

  Sweep range of sizes [n]:

  Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

- **Increase current number of HTTPS to ASDM form 32 to 80**

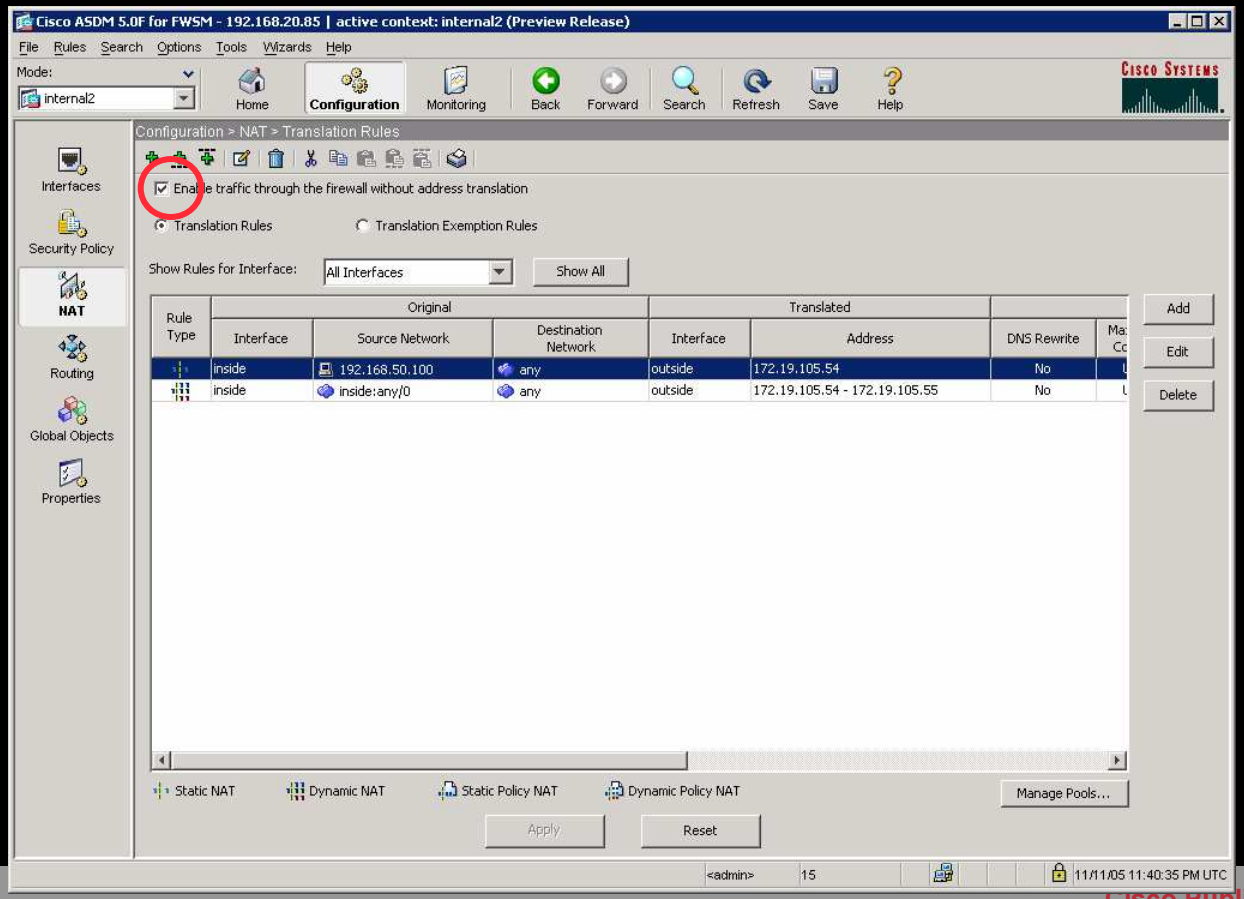
FWSM3.1 & ASDM 5.0(1)F Training

ASDM 5.0(1)F

Nat-control options

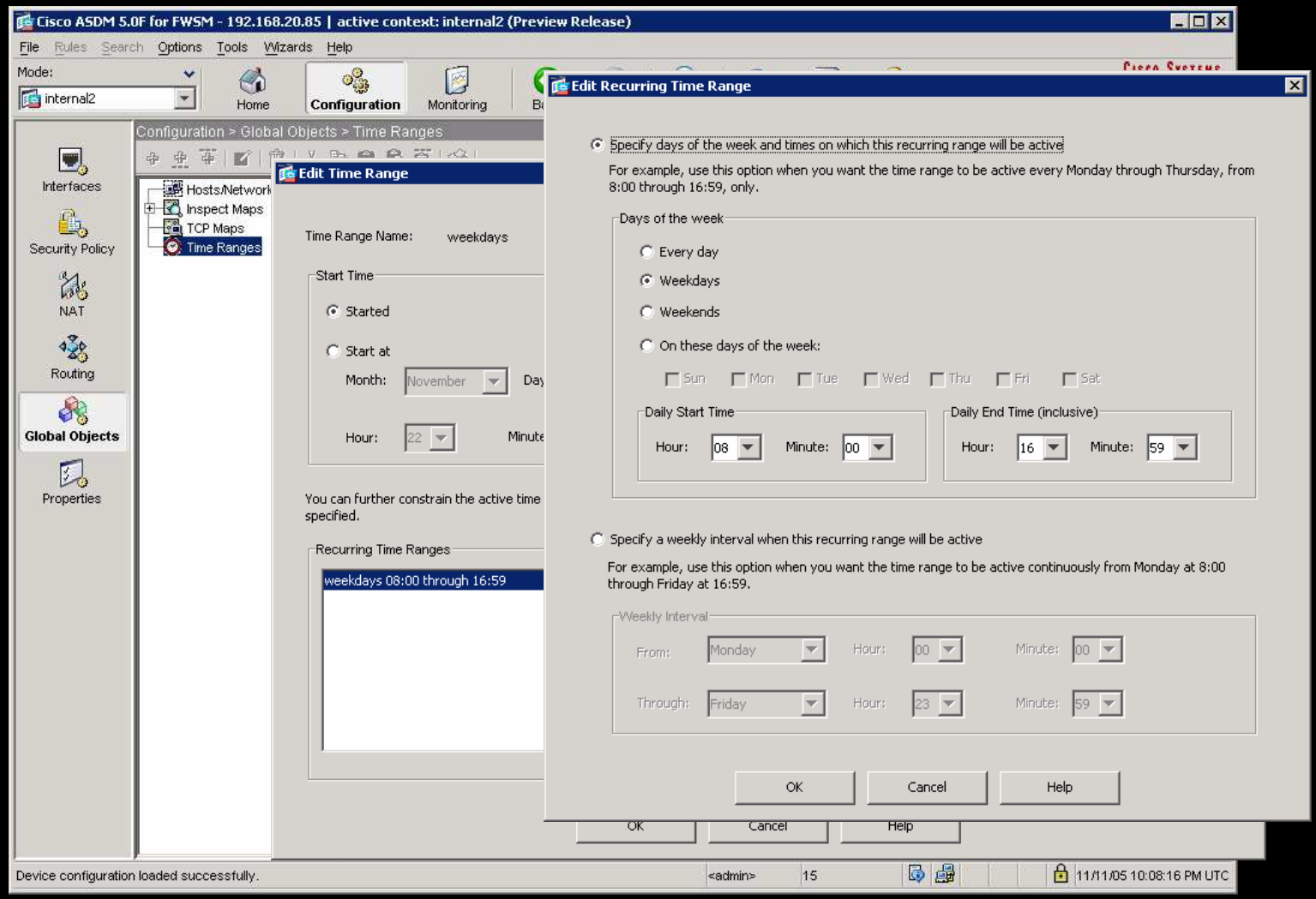
- **FWSM3.1 has nat-control disabled by default that allows inside hosts to communicate with outside network without NAT**

Remove checkmark to enable NAT requirement



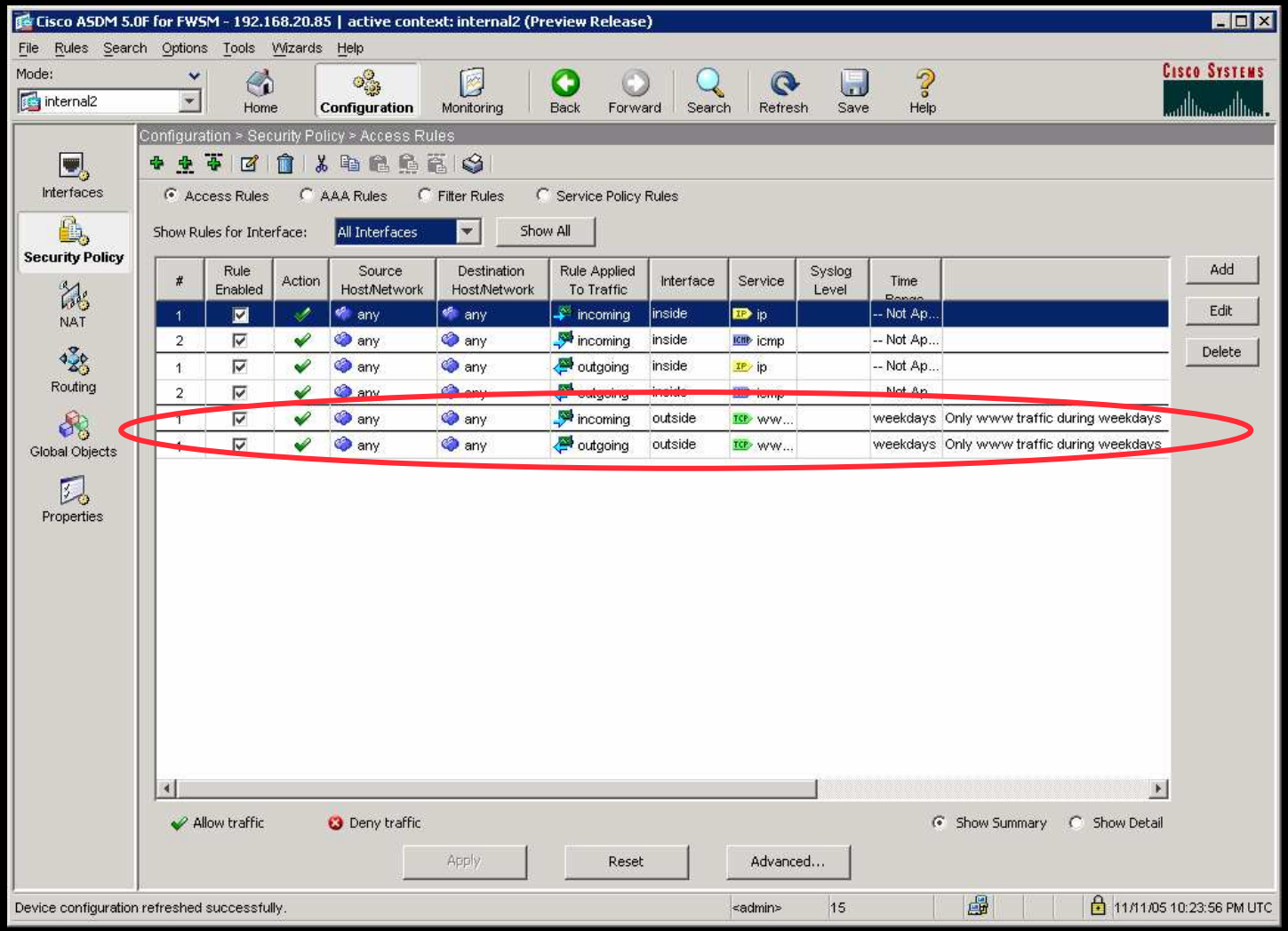
Time-range – ASDM 5.0(1)F

Define time-range



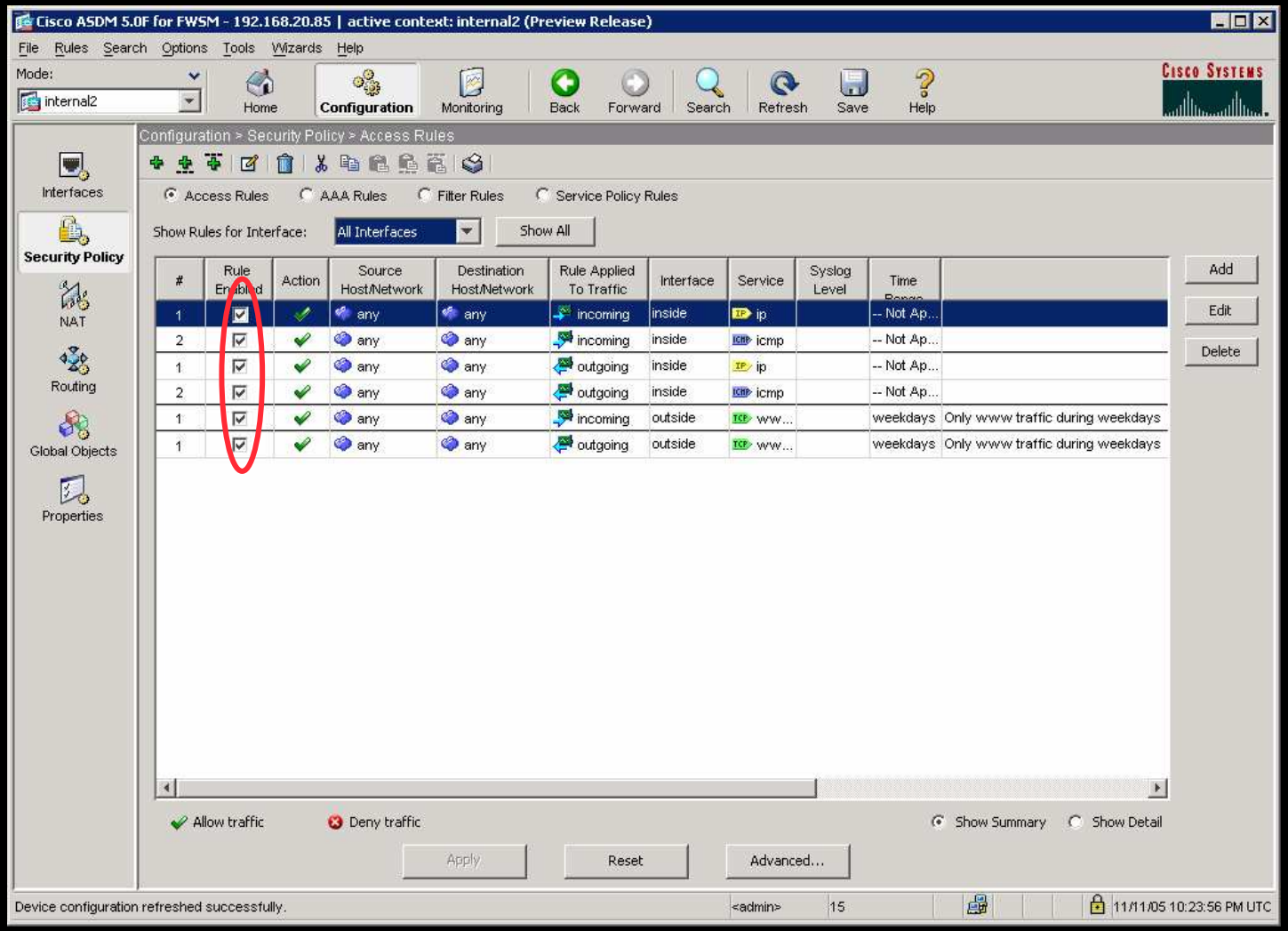
Time-range - ASDM 5.0(1)F

Apply to access-list & access-group



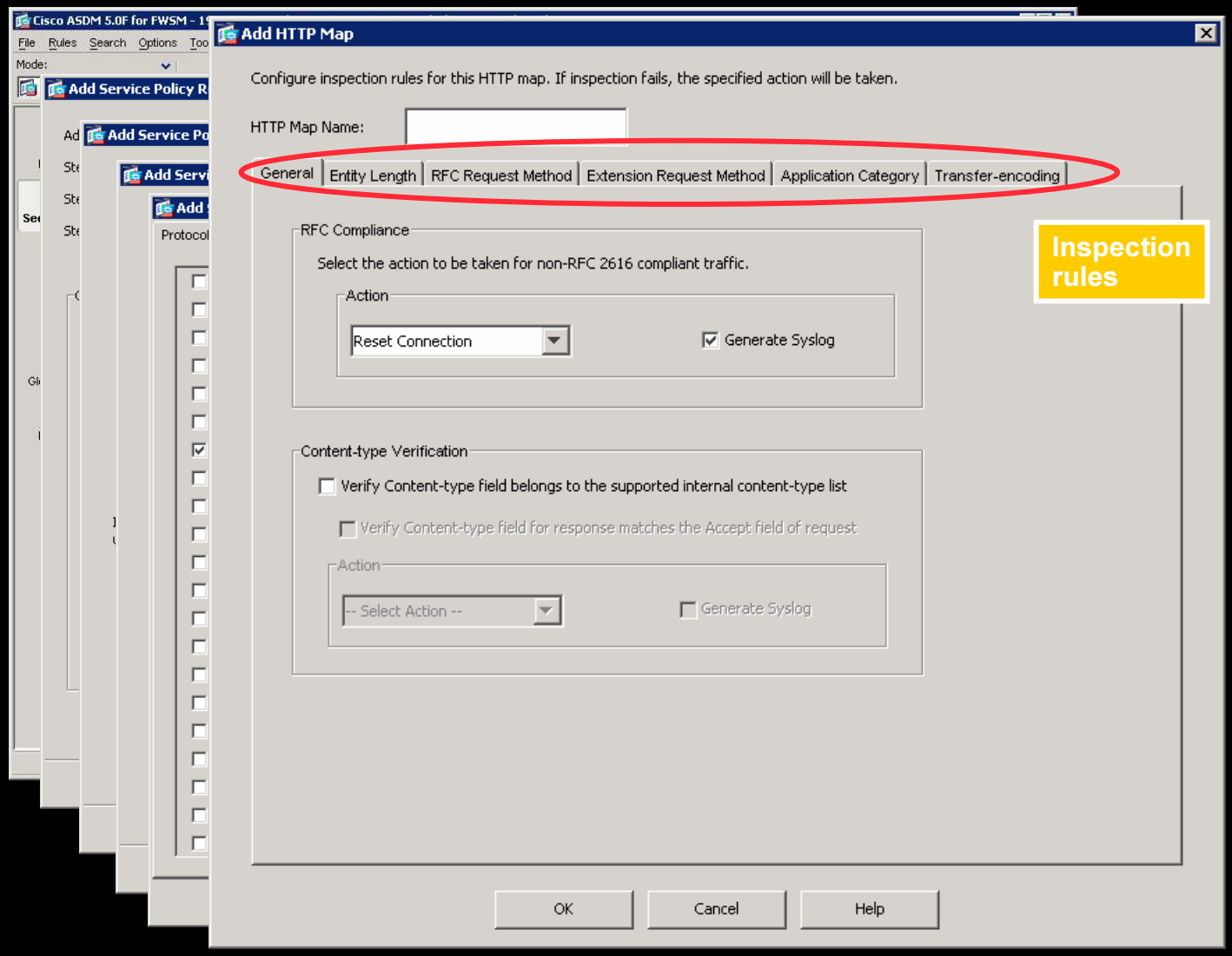
ACL Inactive option

Remove checkmark to disable



Application Firewall – ASDM 5.0(1)F

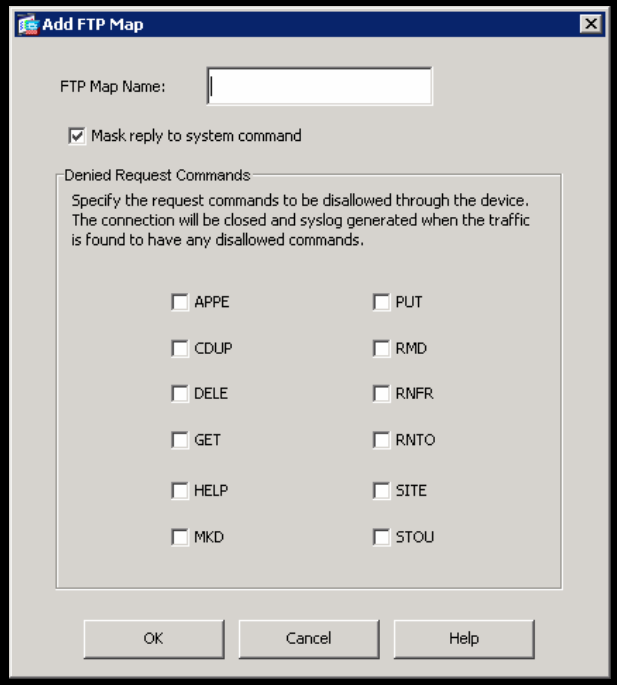
Service Policy Wizards



Inspection rules

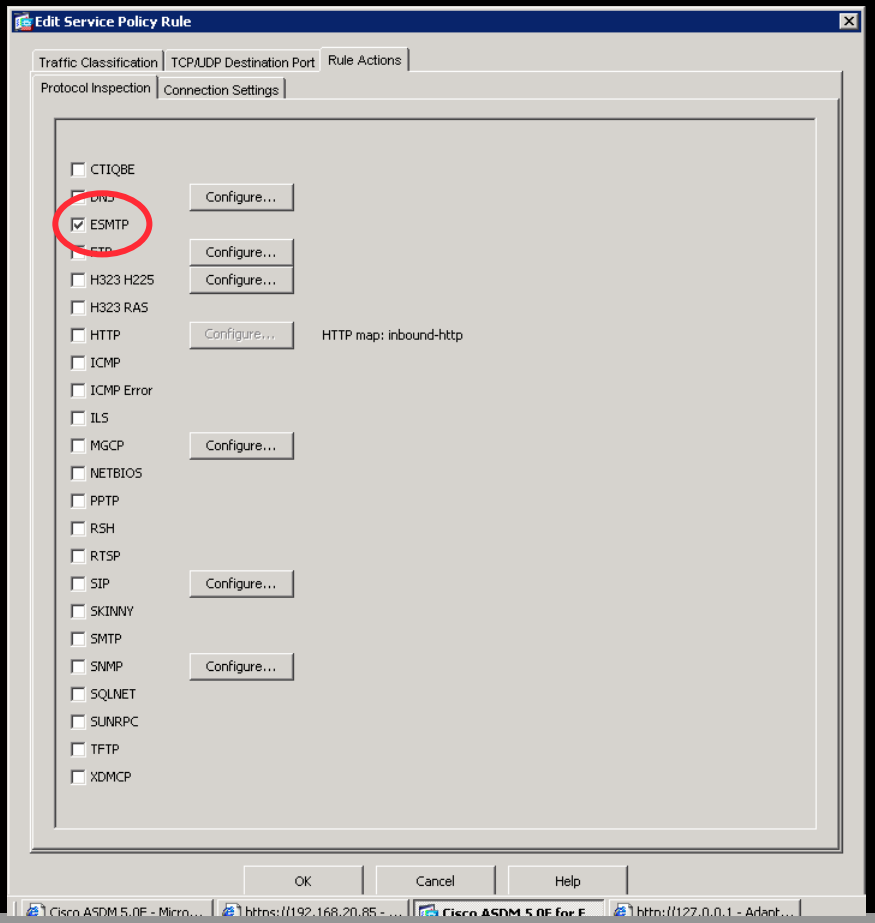
FTP Command Filtering Configurations

- Allow or disallow specific ftp commands. If disallowed, connection will be closed and syslog will be generated.
- ASDM: global objects ->Inspect maps -> ftp

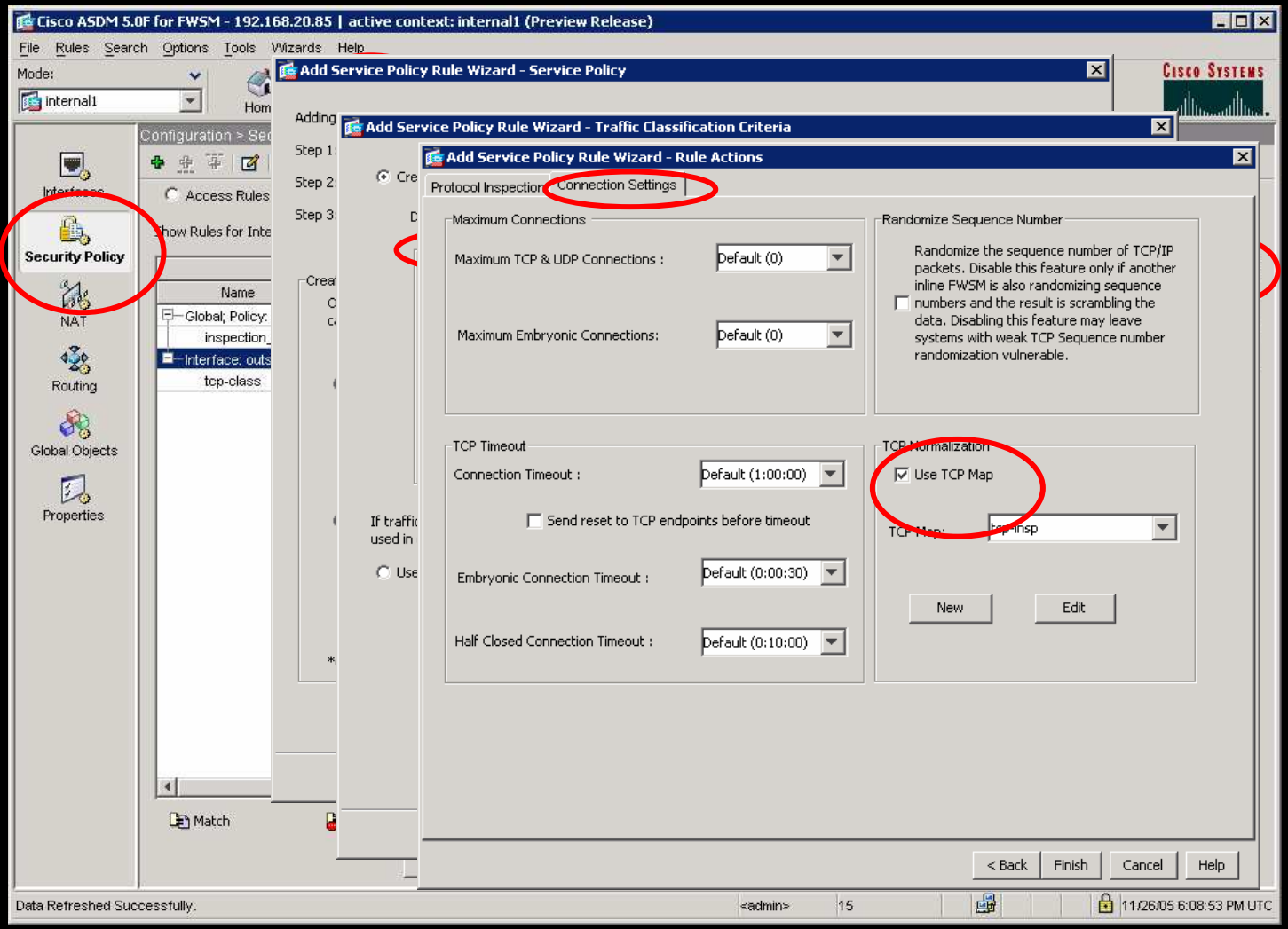


ESMTP Inspection Configuration

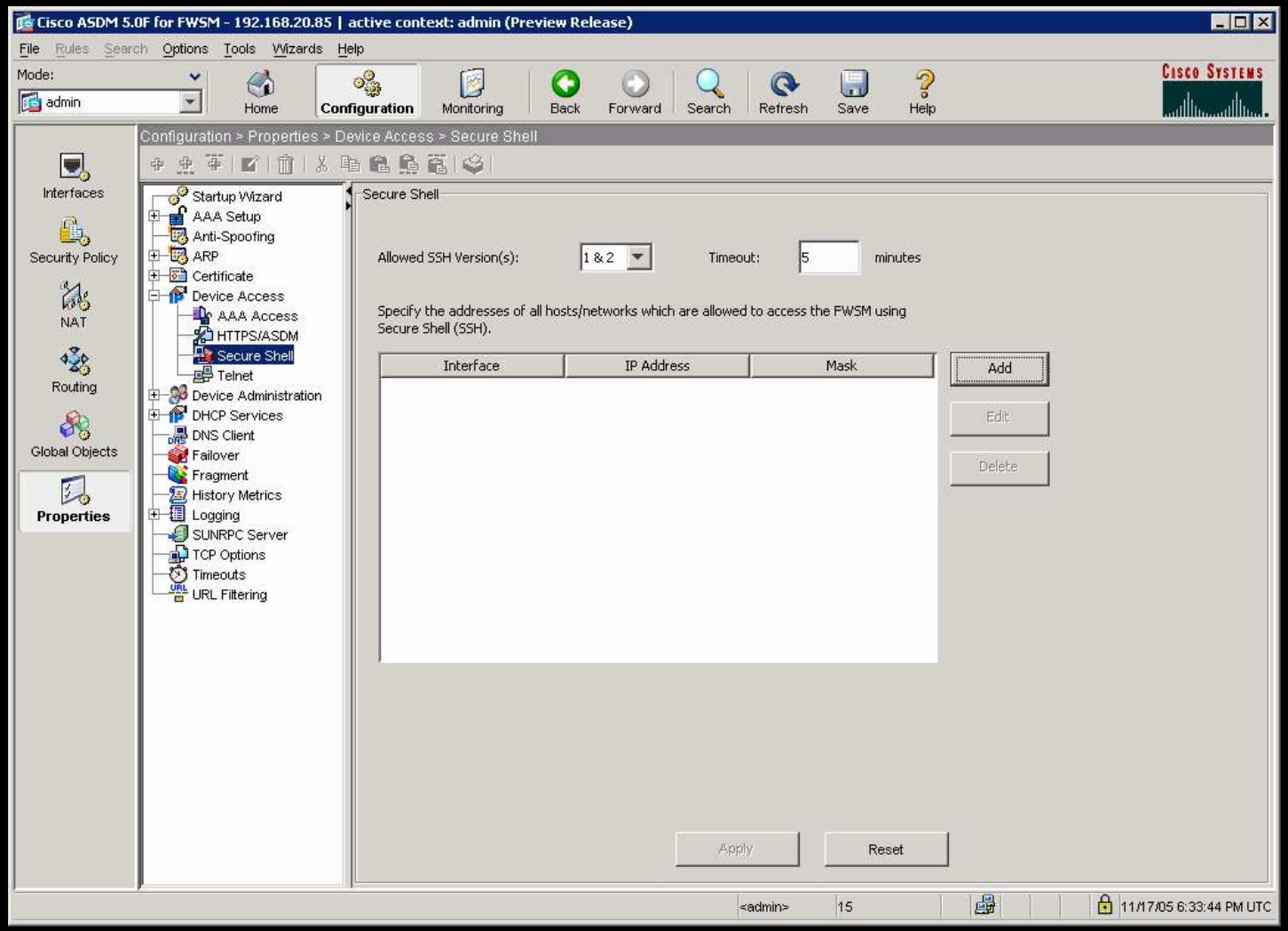
- **Specified as part of policy-map criteria**
  ASDM: Security Policy -> Rule Actions



TCP Advanced Options (tcp-map)

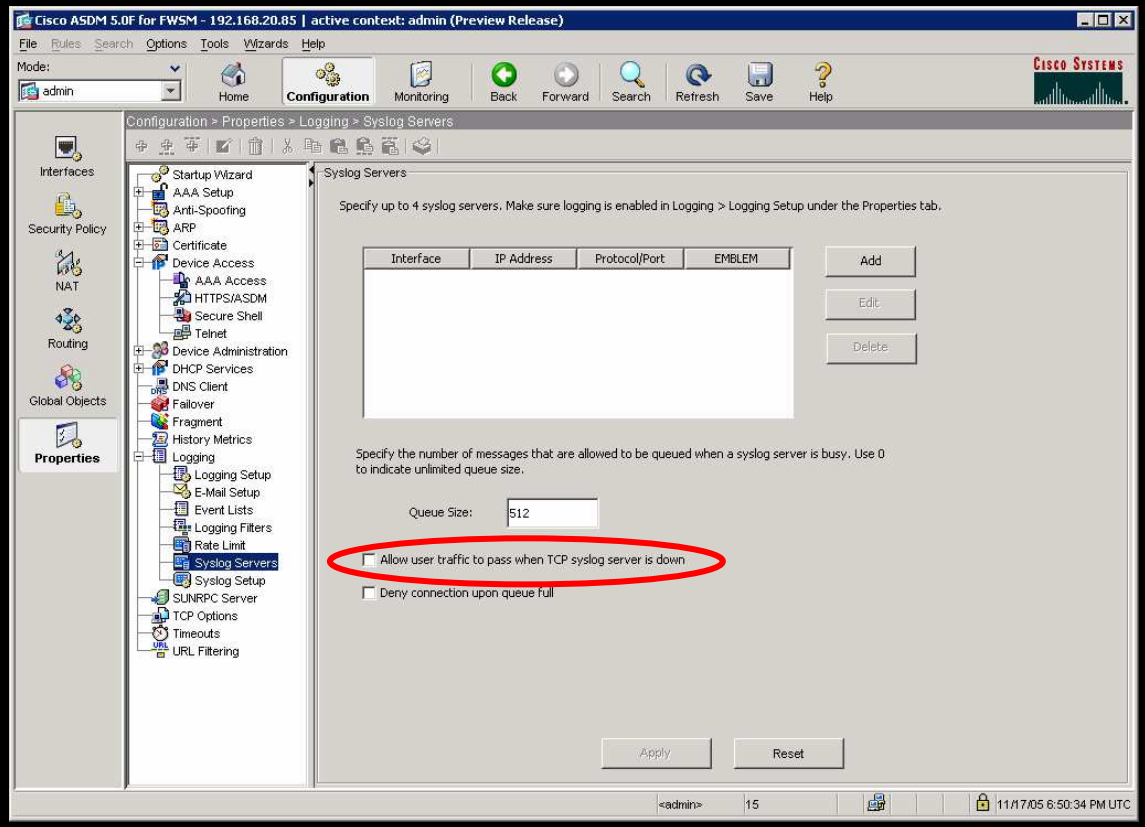


Secure Shell Configuration – ASDM 5.0(1)F



Syslog Server Failure Policy (TCP transport)

- allow new network access sessions for a TCP-based system log server that is not operational – default is FWSM denies new connections for failed server.



Out of Band Management

- Allows only management traffic to be allowed on configured interfaces.
- ASDM: Configuration-> Interface