Content:

FWSM introduction

Requirements for FWSM 3.2

How the Firewall Services Module Works with the Switch

Using the MSFC

Firewall Mode Overview

Stateful Inspection Overview

Security Context Overview

FWSM introduction

Cisco Firewall Services Module (FWSM)

- A high-speed, integrated firewall module for Cisco Catalyst 6500 switches and Cisco 7600 Series routers—provides the fastest firewall data rates in the industry: 5-Gbps throughput, 100,000 CPS, and 1M concurrent connections.
- Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis.
- Based on Cisco PIX Firewall technology, the Cisco FWSM offers large enterprises and service providers unmatched security, reliability, and performance.

End-of-Sale and End-of-Life has been reached for Cisco IOS Firewall Feature Set on the Cisco Catalyst 6500
The recommended replacement for the Cisco IOS Firewall Feature Set on the Cisco Catalyst 6500 is the Cisco Catalyst 6500 Firewall Services Module (FWSM).

Source:
http://cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_end-of-life_notice0900aecd8067a132.html

FWSM main site (Thats contains informations on one webpage):
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

6500 Series switches main site (info for modules as well):
http://cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

SW versions available:
4.0(1) – new!
3.2(6) - 3.2(1)
3.1(10) - 3.1(4)

ASDM:
6.1F -for 4.X
5.2(1)F - 5.2(4)F for 3.2 and 3.1 (not all 3.1 compatible.)

End-of-Sale and End-of-Life has been reached for the Cisco Catalyst OS Release 8.x
The recommended replacement for the Cisco Catalyst OS 8.x is Cisco IOS release 12.2SX.

Source:
http://cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_end-of-life_notice0900aecd80699e1a.html

Requirements for FWSM 3.2

The switch models that support the FWSM include the following platforms:

Catalyst 6500 series switches, with the following required components:
–Supervisor engine with Cisco IOS software (known as supervisor IOS) or Catalyst operating system (OS).
–MSFC 2 with Cisco IOS software.

Cisco 7600 series routers, with the following required components:
–Supervisor engine with Cisco IOS software.
–MSFC 2 with Cisco IOS software.

Support for FWSM 3.2

	Supervisor Engines*
Cisco IOS Software Release	
12.2(18)SXF and higher	720, 32
12.2(18)SXF2 and higher	2, 720, 32
Cisco IOS Software Modularity Release	
12.2(18)SXF4	720, 32
Catalyst Software Release[2]	
8.5(3) and higher	2. 720, 32

* The FWSM does not support the supervisor 1 or 1A.

The connection between the FWSM and the switch is a 6-GB 802.1Q trunking EtherChannel

How the Firewall Services Module Works with the Switch

The Catalyst 6500 series switches supports two software modes:

–Cisco IOS software on both the switch supervisor and the integrated MSFC (known as “supervisor IOS”).

–Catalyst Operating System (OS) on the supervisor, and Cisco IOS software on the MSFC.

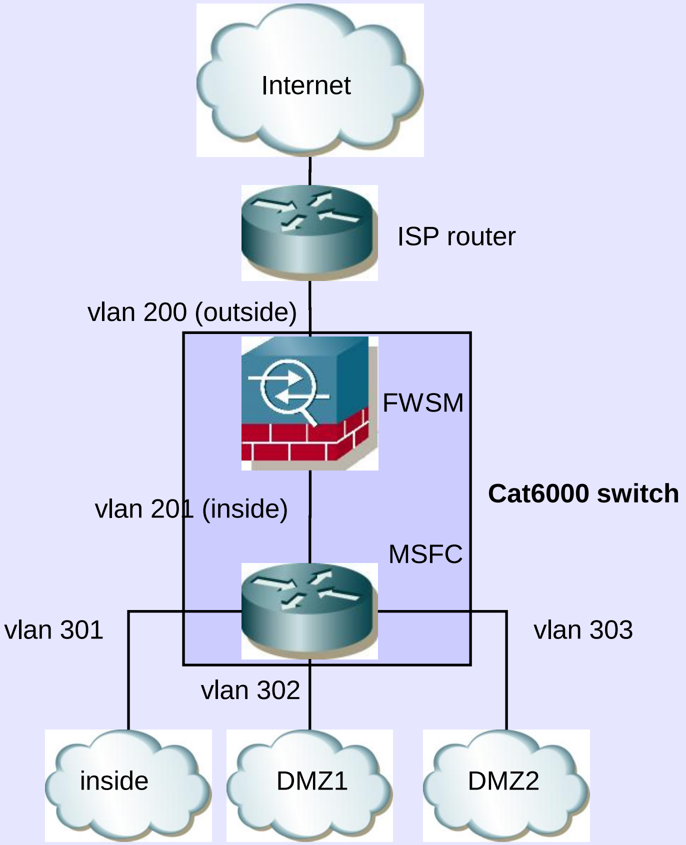
The Cisco 7600 series routers support only Cisco IOS software.

The FWSM runs its own operating system.

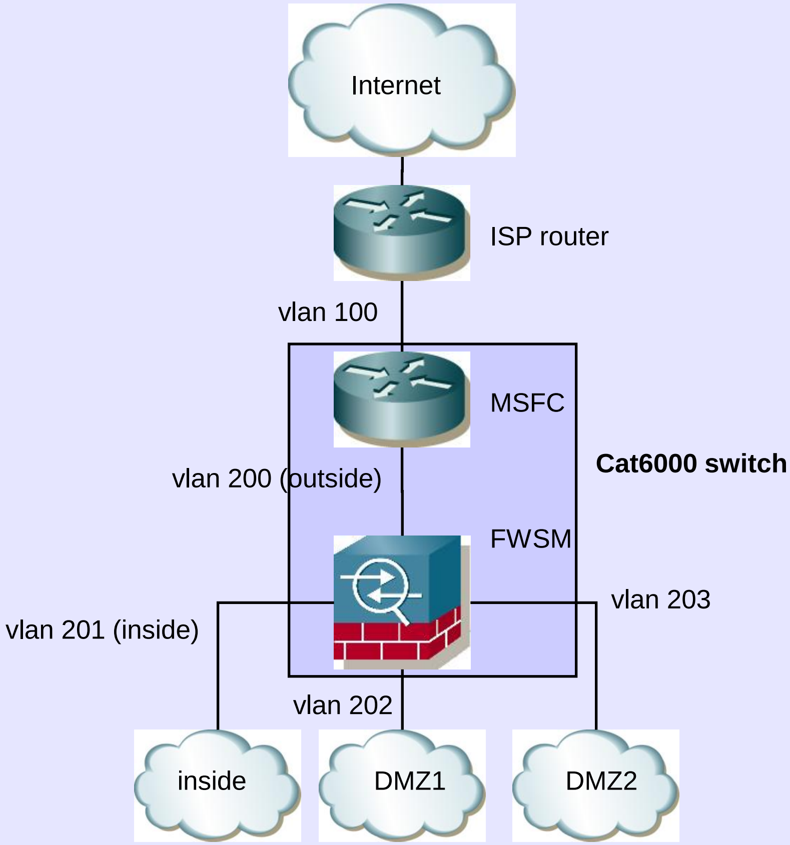
Using the MSFC

MSFC placements variations in single mode setup:

MSFC behind the FWSM



MSFC in front of the FWSM



The VLAN 201 is assigned to the inside interface of the FWSM

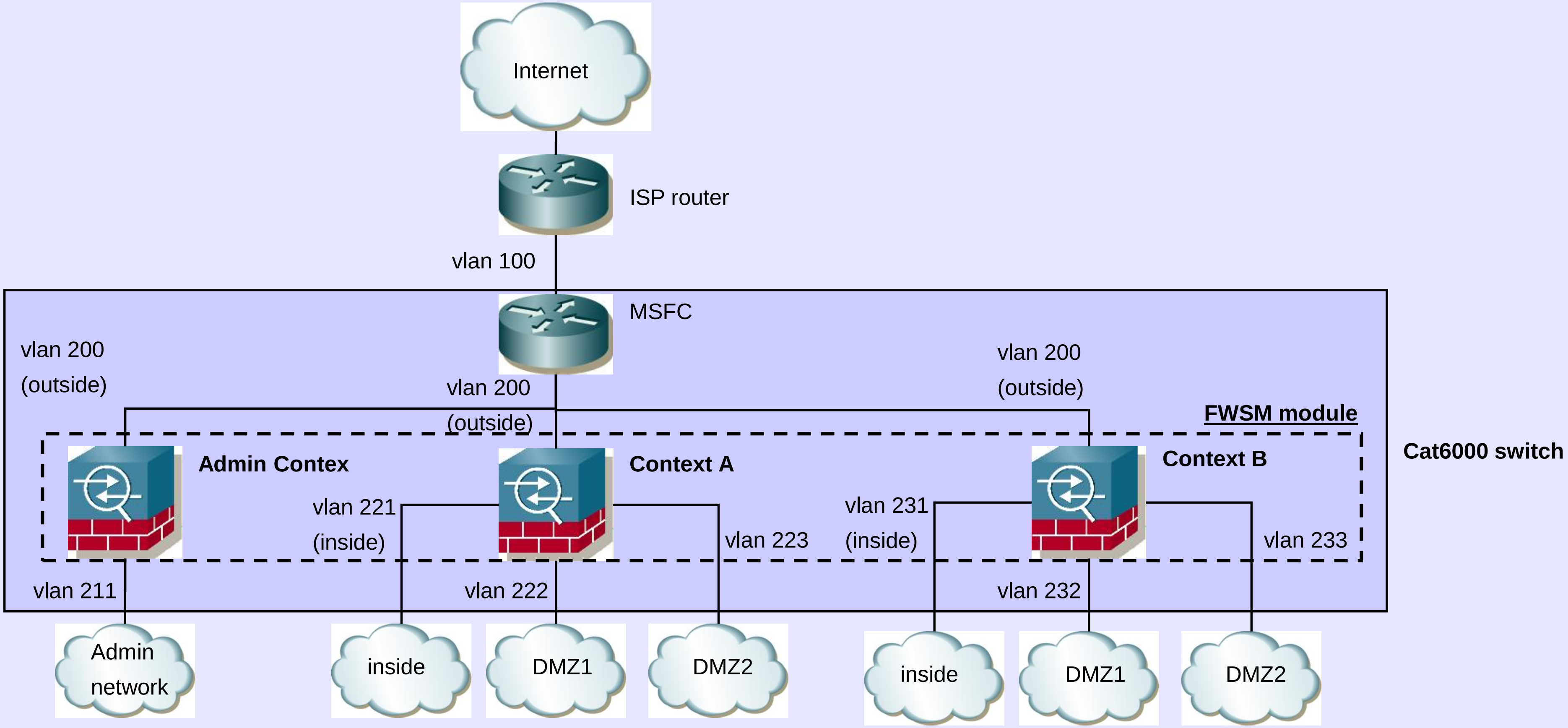
The MSFC routes between VLANs 201, 301, 302, and 303, and no inside traffic goes through the FWSM unless it is destined for the Internet

The VLAN 200 is assigned to the outside interface of the FWSM

The FWSM processes and protects all traffic between the inside VLANs 201, 202, and 203

Using the MSFC

MSFC placement in multimode setup:



Use the **MSFC in front of all the contexts** to route between the Internet and the switched networks

If the MSFC is behind FWSM, then MSFC will route between the contexts, that should be done by FWSM.

Firewall Mode Overview

The FWSM runs in two different firewall modes:

Routed
- The FWSM is considered to be a router hop in the network

Transparent
- FWSM acts like a "bump in the wire," or a "stealth firewall," and is not considered a router hop
- The FWSM connects to the same network on its inside and outside interfaces.
- You can configure up to eight pairs of interfaces (called bridge groups) to connect to eight different networks, per context.

In multiple context mode, you can choose the mode for each context independently, so some contexts can run in transparent mode while others can run in routed mode.

Stateful Inspection Overview

All traffic that goes through the firewall is inspected using the **Adaptive Security Algorithm** and is either allowed through or dropped.

Security Context Overview

Same as ASA, but **hibrid solutions** are supported (1 context can be in transparent, while other can be in routed mode.

No VPN support! Use IOS for minimal performance request or VPN SPA module or SSL VPN module for higher performance request.

Content:

Assigning VLANs to the Firewall Services Module

SVI – Switched virtual interface

Customizing the FWSM Internal Interface

The FWSM Internal Architecture

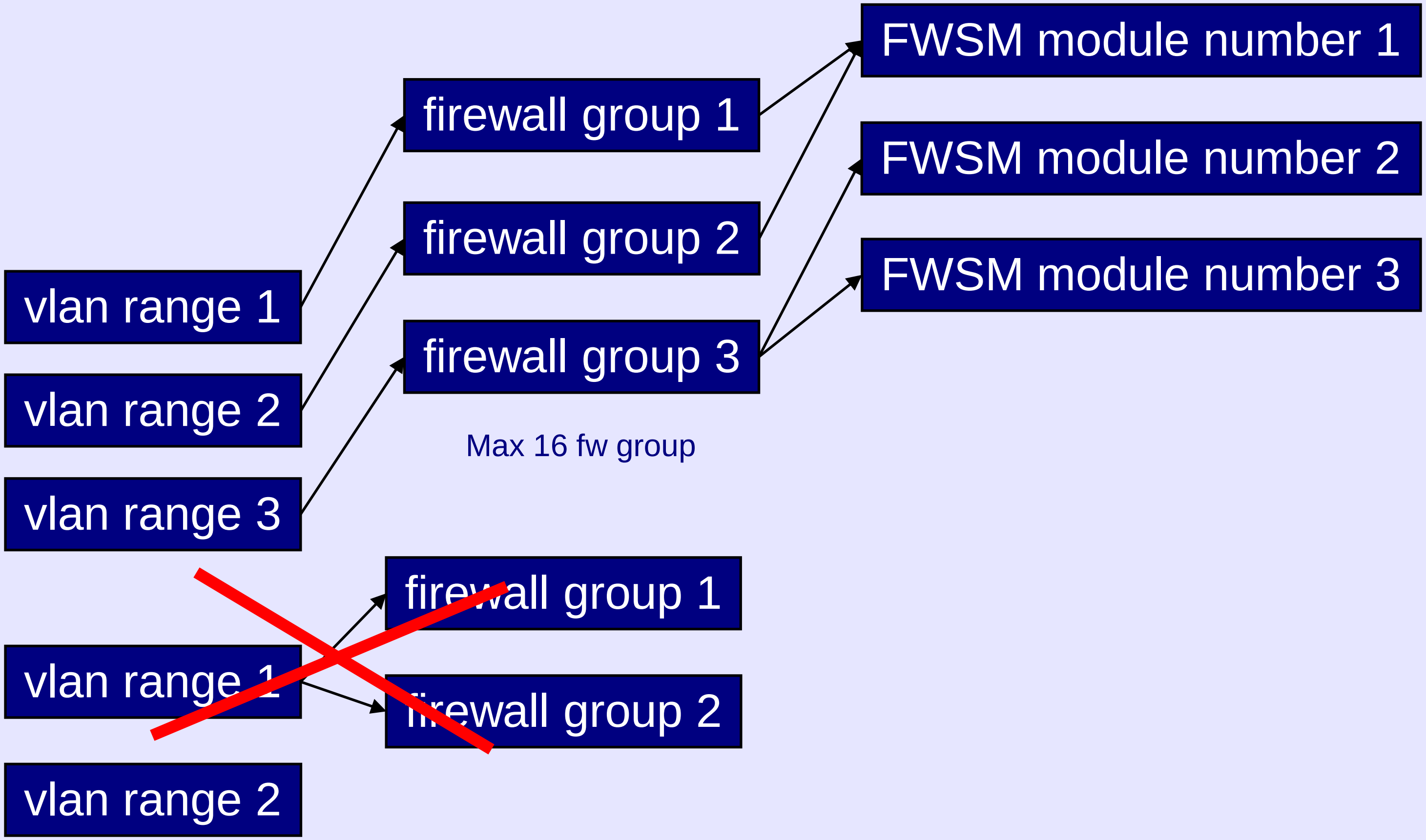
Packet Flows on FWSM

State checking for FWSM

Managing the Firewall Services Module Boot Partitions

Resetting the FWSM in Cisco IOS Software

Assigning VLANs to the Firewall Services Module



vlan range 1

vlan range 2

vlan range 3

firewall group 1

firewall group 2

firewall group 3

FWSM module number 1

FWSM module number 2

FWSM module number 3

Max 16 fw group

vlan range 1

vlan range 2

firewall group 1

firewall group 2

Commands (IOS only):

```
Router# firewall vlan-group <firewall_group> <vlan_range>
Router# firewall module <module_number> vlan-group <firewall_group>

Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100

Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Assigning VLANs to the Firewall Services Module

VLAN Guidelines:

- You can use private VLANs with the FWSM. Assign the primary VLAN to the FWSM; the FWSM automatically handles secondary VLAN traffic.
- You cannot use reserved VLANs.
- You cannot use VLAN 1.
- If you use FWSM failover within the same switch chassis, do not assign the VLAN(s) you reserved for failover and stateful communications to a switch port. But, if you use failover between chassis, you must include the VLANs in the trunk port between the chassis.
- If you do not add the VLANs to the switch before you assign them to the FWSM, the VLANs are stored in the supervisor engine database and are sent to the FWSM as soon as they are added to the switch.
- Assign VLANs to the FWSM before you assign them to the MSFC.
- VLANs that do not satisfy this condition are discarded from the range of VLANs that you attempt to assign on the FWSM.

SVI – Switched virtual interface

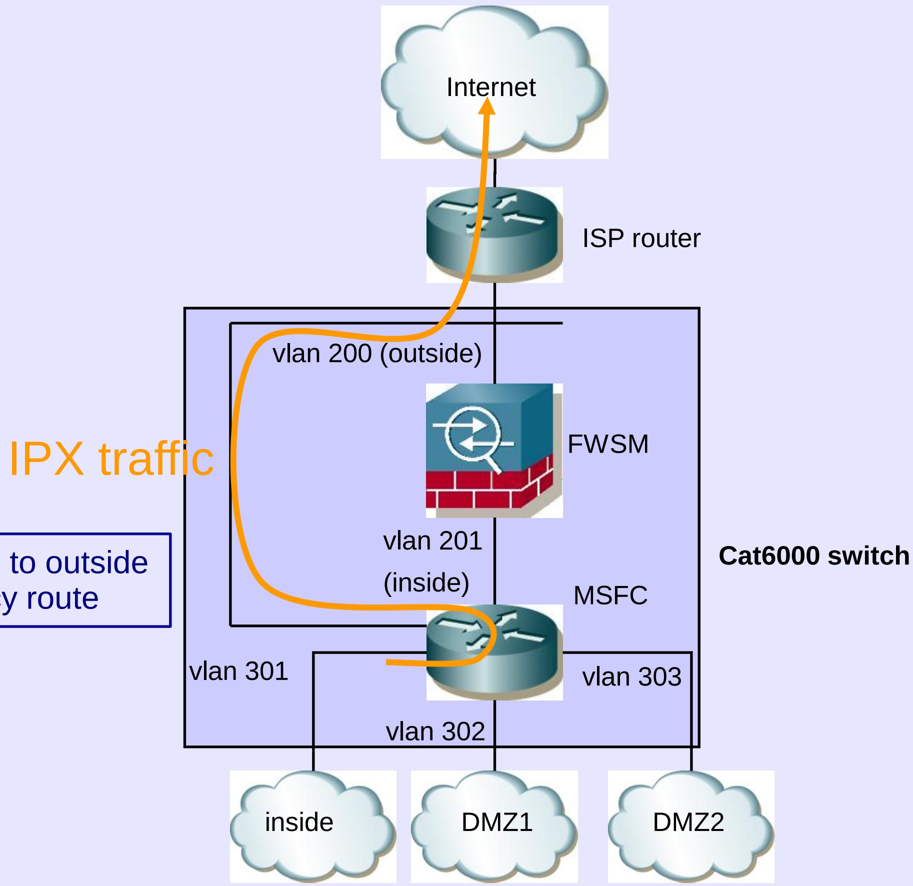
- A VLAN defined on the MSFC is called a switched virtual interface, that is a logical Layer 3 interface on a switch.
- If you assign the VLAN used for the SVI to the FWSM, then the MSFC routes between the FWSM and other Layer 3 VLANs.
- Creating multiple SVI can cause misconfiguration and can bypass the FWSM by misconfiguration.
- From the other side, multiple SVI can help bypass FWSM in specific case (like IPX bypass for FWSM).

To enable support for multiple SVI as part of FWSM vlan use the following command:

Required commands:

```
Router(config)# firewall multiple-vlan-interfaces
```

MSFC behind the FWSM

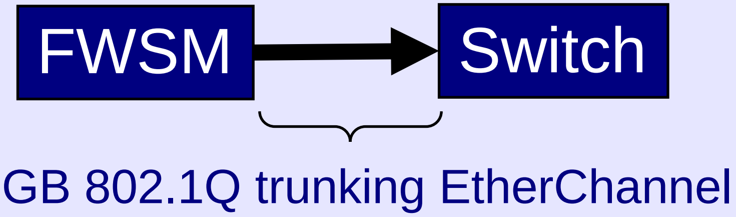


On MSFC the IPX traffic from inside to outside can be routed on vlan 200 with policy route

Basic example configuration link:

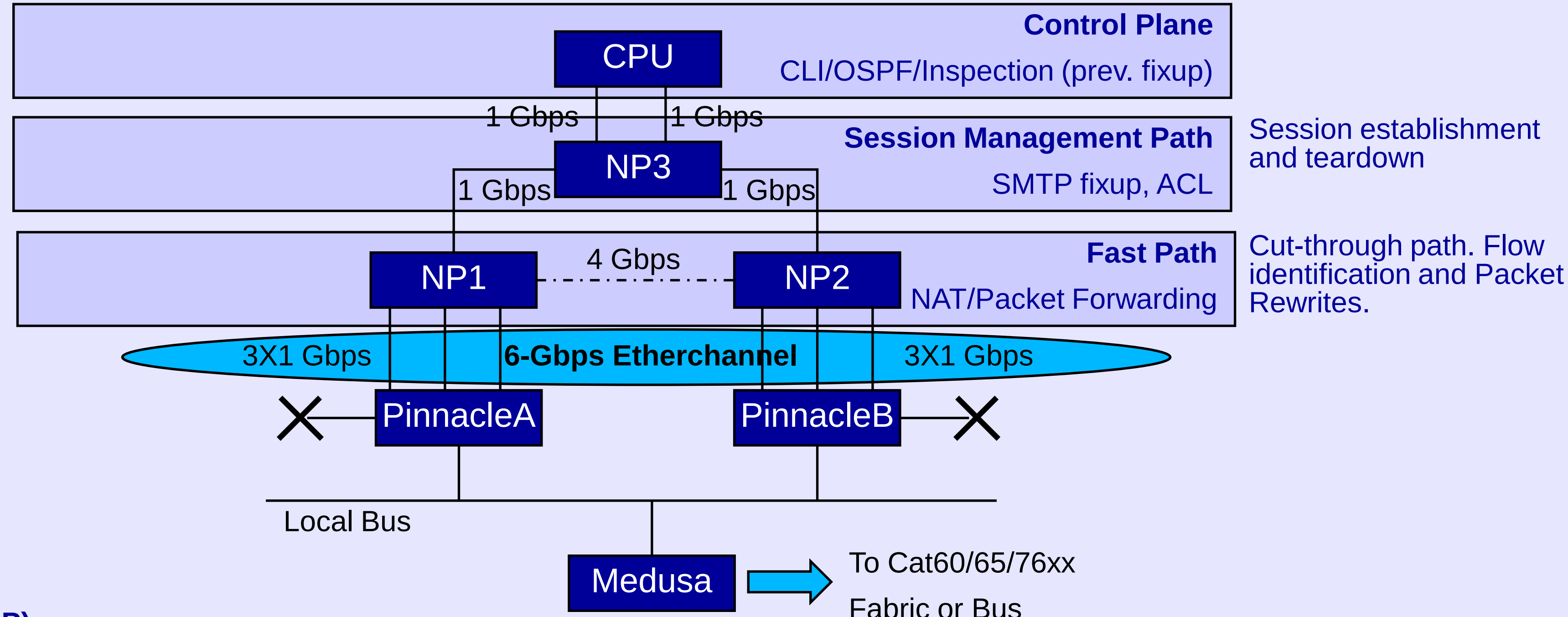
http://cisco.com/en/US/products/hw/modules/ps2706/products_configuration_example09186a00808b4d9f.shtml

Customizing the FWSM Internal Interface



- 6-GB 802.1Q trunking EtherChannel
- On FWSM 2 NPs connect to three Gigabit Ethernet interfaces each.
- The traffic distribution to the interfaces in the EtherChannel made according to a distribution algorithm based on session information.

The FWSM Internal Architecture



Control Plane (CP)

Most of the memory-intensive tasks and complex operations are performed in the CP.
The frequently used simple tasks within the packet processing are moved to the Network Processors.

CP Tasks:

- Layer 7 fixups (It is on NP3 as well). Multi Channel Protocols (FTP, VOIP) and others like esmtp inspections are here.
- Overall management of the blade
- Supervisory functions for each NP
- Running of routing protocols
- Preliminary compilation of the access rules before downloading them into the slow NP

CP has two Gigabit Ethernet ports connected to the Session Management Path NP (NP3).

Network Processors (NP)

Each NP has four Gigabit Ethernet interfaces.

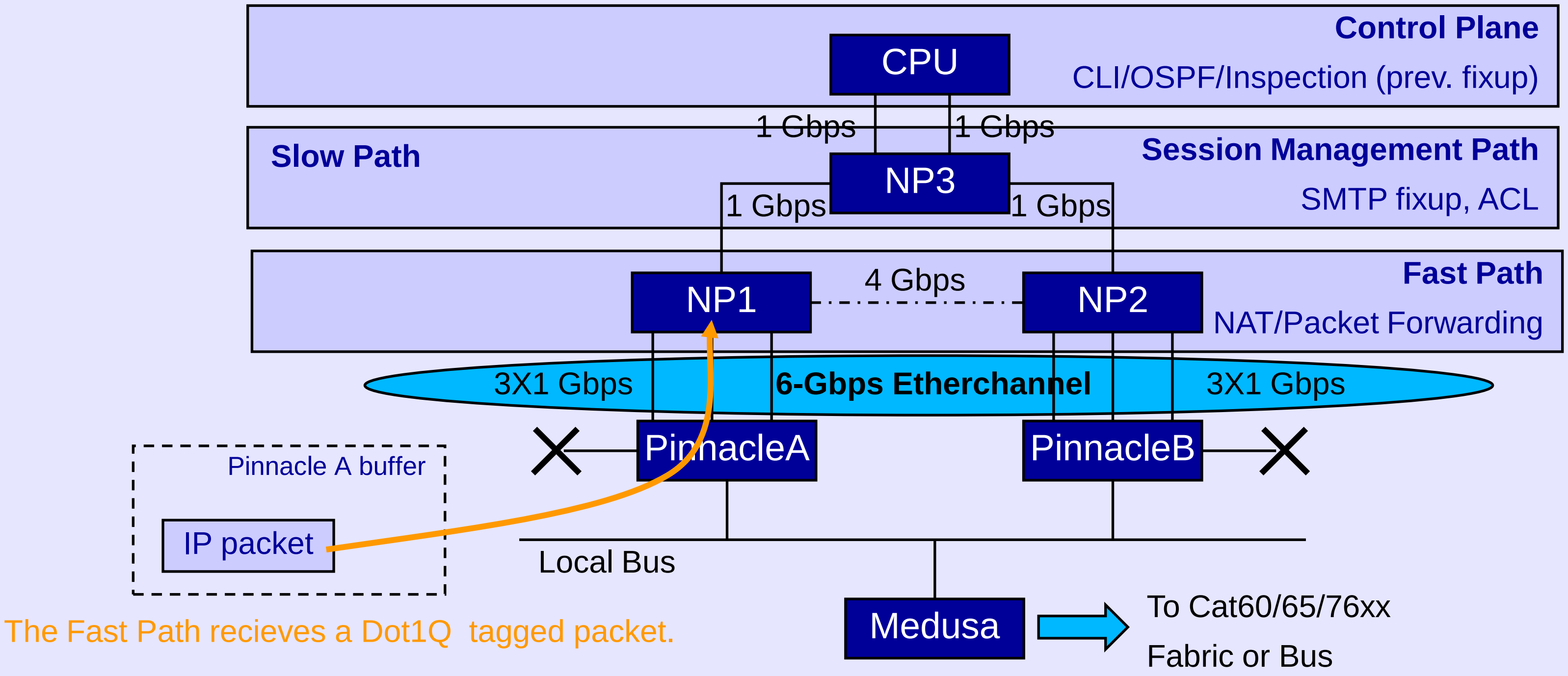
Session Management Path Network Processor (NP3)

- It has 4 Gigabit Ethernet port.
- NP3 connects to the CP using two Gigabit Ethernet ports (port 3 and 4).
- NP3 connects to the NP1 and NP2 using two Gigabit Ethernet ports (port 1 and 2).

Fast Path Network processors (NP1 and NP2)

- It has 4 Gigabit Ethernet port.
- Each NP connects to Port 1 and 2 of NP3 with their fourth Gigabit Ethernet port.
- Each NP connect with the Catalyst 6500/7600 switching crossbar-SFM (offers 256 GBps) or backplane (offers 32 GBps) with their remained Gigabit Ethernet ports.
- This 3 remained Gigabit Ethernet ports per NP (total 6) used in 802.1Q trunking EtherChannel.

Packet Flows on FWSM



Session establishment and teardown

Cut-through path. Flow identification and Packet Rewrites.

The Fast Path recieves a Dot1Q tagged packet.

Step 1. Destination MAC address
- one of Firewall MAC Addresses?
- Broadcast?
- Multicast?

→ Step 2.

Step 2. Destination IP address — one of Firewall IP Addresses? → Forward packet to CP

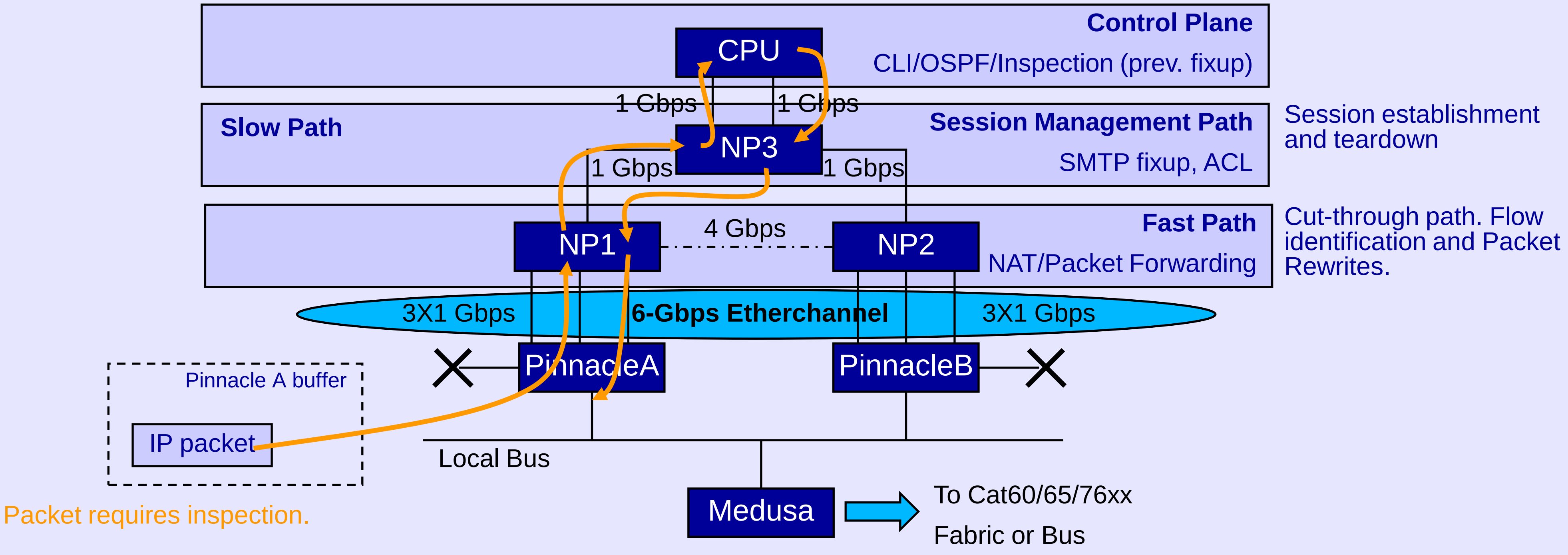
Step 3. Packet type — routing packets (for example, RIP/OSPF packets → Forward packet to CP

Step 4. Packet fragment — is fragmented? → Forward packet to IP Virtual Reassembly Module.

Step 5. Protocol type — Non-TCP/UDP protocol packets? → Forward packet to CP or NP

TCP/UDP protocol packets? → Step 6. (Session Lookup begins)

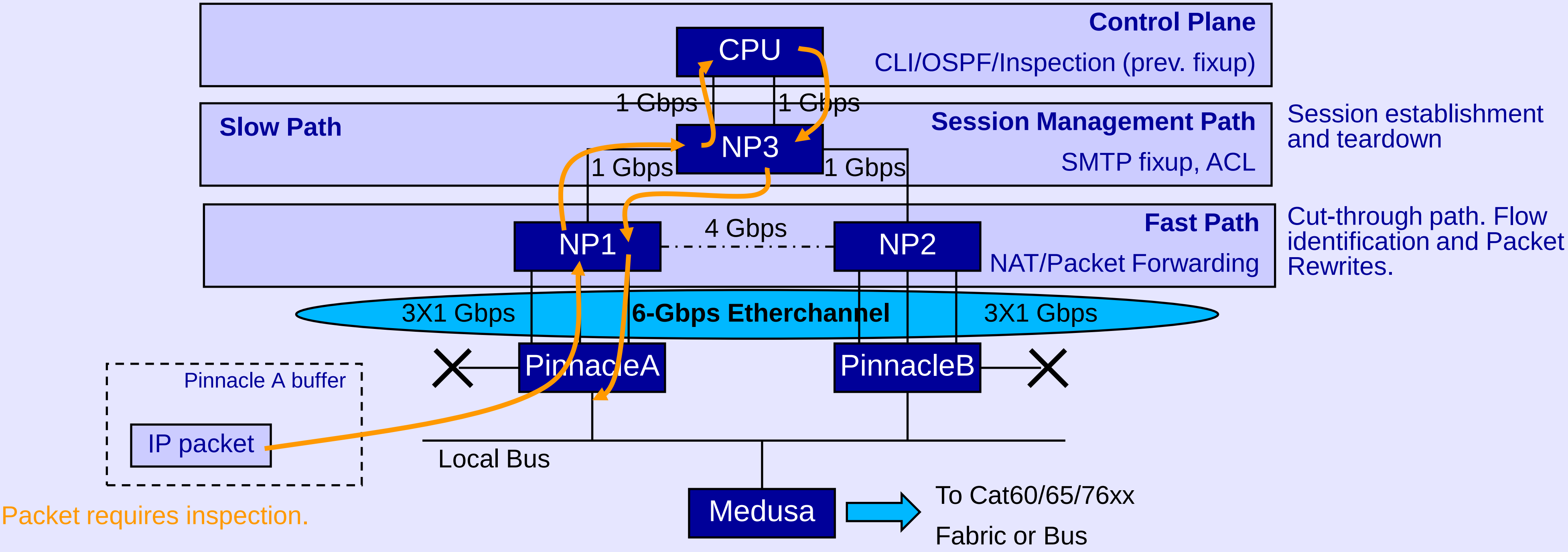
Packet Flows on FWSM



Packet requires inspection.

Step 6. Session lookup	1 succesful	→	State retrieved from the session lookup. Step 6/1.
	2 failed	→	Protocol type of packet specifies the action. Step 6/2.
Step 6/1. State table check	fragmentation frag?	→	Forward packet to IP Virtual Reassembly Module.
	process in the Fast Path?	→	Apply NAT, update state.
	intercepted Session / AAA Session?	→	Forward packet to NP3
	inspection required?	→	Forward packet to NP3
Step 6/2. „Protocol type check”	Not TCP SYN	→	Packet drop.
	Not ICMP echo request	→	Packet drop – if ACL check result is deny
	TCP SYN	→	Forward packet to NP3. Step 7.

Packet Flows on FWSM



Step 7. NP3 tasks

If required → Acl check, AAA, etc...

Existing session - Session ID attached from Fast Path → Actions taken by the Session ID (TCP intercept, AAA timestamp update)

New session (TCP SYN, UDP, ICMP echo request) → Acl check, forward to CP in case of Layer 7 Application Inspections* or mgmt traffic

* Smtp inspection occurs in fast path processing while Esmtp inspection occurs in control-plane path processing.

State checking for FWSM

Usefull comands:

```
show np {number item | all}
show np acl-notification
show np block
show np pc

show conn long 3
show pc conn

show nic
show console-output

show permon detail
```

Understanding access-list memory utilization

Managing the Firewall Services Module Boot Partitions

FWSM has a 128-MB Flash memory card:

- Six partitions (cf:n)
- Contains Configuration, Operating System, etc..

Partitions:

Maintenance partition (cf:1)—Contains the maintenance software. Use the maintenance software to upgrade or install application images if you cannot boot into the application partition, to reset the application image password, or to display the crash dump information.

Network configuration partition (cf:2)—Contains the network configuration of the maintenance software. The maintenance software requires IP settings so that the FWSM can reach the TFTP server to download application software images.

Crash dump partition (cf:3)—Stores the crash dump information.

Application partitions (cf:4 and cf:5)—Stores the application software image, system configuration, and ASDM. By default, Cisco installs the images on cf:4. You can use cf:5 as a test partition. For example, if you want to upgrade your software, you can install the new software on cf:5, but maintain the old software as a backup in case you have problems. Each partition includes its own startup configuration.

Security context partition (cf:6)—64 MB are dedicated to this partition, which stores security context configurations (if desired) and RSA keys in a navigable file system. Other partitions do not have file systems that allow you to perform common tasks such as listing files. This partition is called disk when using the copy command.

Administrating boot partitions:

Set Boot Partition:

```
Router(config)# boot device module mod_num cf:n
```

view the current boot partition:

```
Router# show boot device [mod_num]
```

Resetting the FWSM in Cisco IOS Software

To reset the FWSM, enter the following command:

```
Router# hw-module module mod_num reset [cf:n] [mem-test-full]
```

The **cf:**n argument is the partition, either 1 (maintenance), 4 (application), or 5 (application). If you do not specify the partition, the default partition is used (typically cf:4).

The **mem-test-full** option runs a full memory test, which takes approximately 6 minutes.