Catalyst Switch Security Update
Business-Ready Campus

2004.12

Cisco Systems, Korea

Bang, Hang Mo (banha@cisco.com)

Agenda

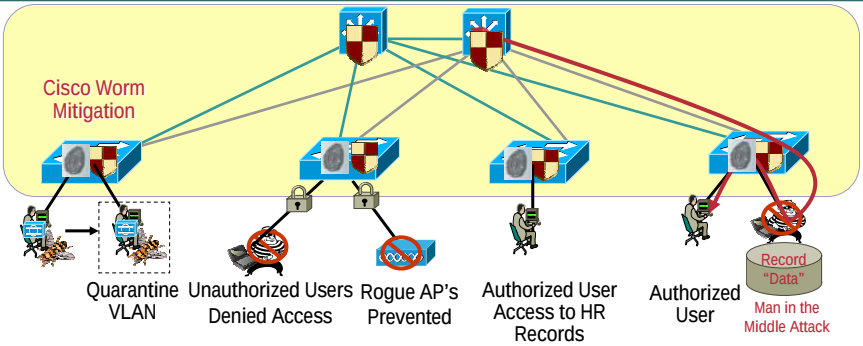
- Catalyst Integrated Security Features (CISF)
- Mitigating the Worm Impact
- Catalyst 6500 Integrated Security Service Modules
- Catalyst 6500 Security Module Reference Design
- Q/A

Cisco.com

Catalyst Integrated Security Features (CISF)

What are the Components of Campus Security?

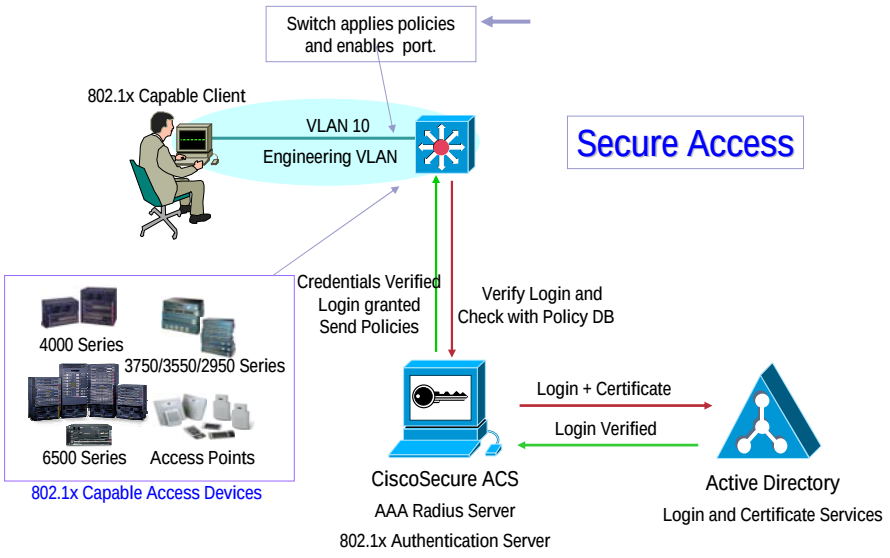
Cisco.com



Host IPS (CSA) with Network Admission Control (NAC)	Cisco Identity Based Networking Services (IBNS)	Cisco Catalyst Integrated Security
Detects and Isolates Infected Users	"Controlling Who/What Gets Access to the Network and What They Can Do"	Protects Against Today's Emerging Attacks: "Man-in-the-Middle" "DHCP Server Spoofing" "IP Address Spoofing"

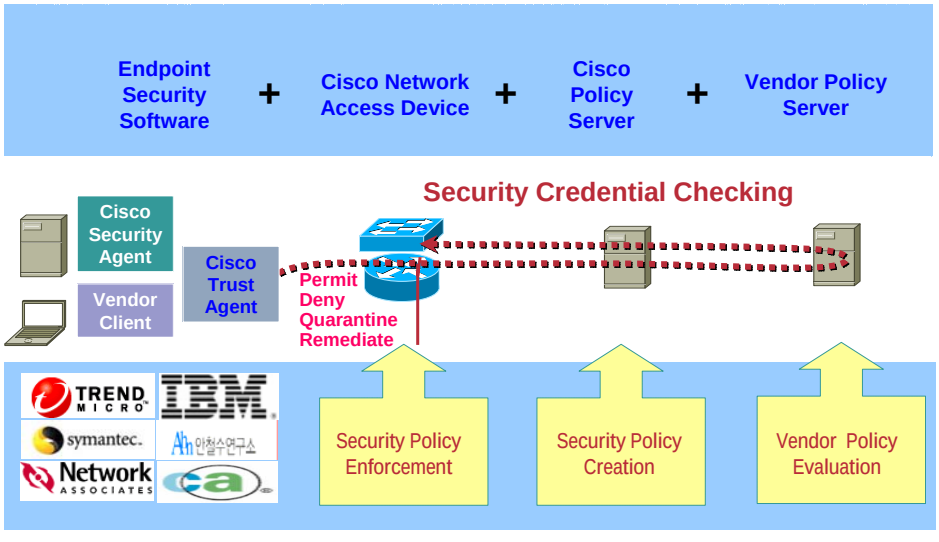
IBNS (Identity-based Networking Service)
802.1x Access Control

Cisco.com



Network Admission Control
Cisco NAC Program

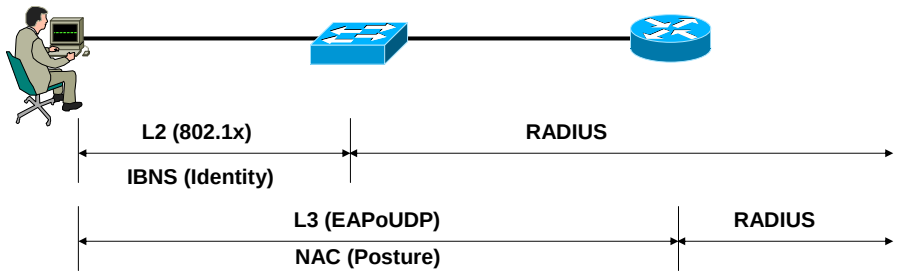
Cisco.com



IBNS & NAC Phase 1

Gateway IP Operation (Current)

Cisco.com

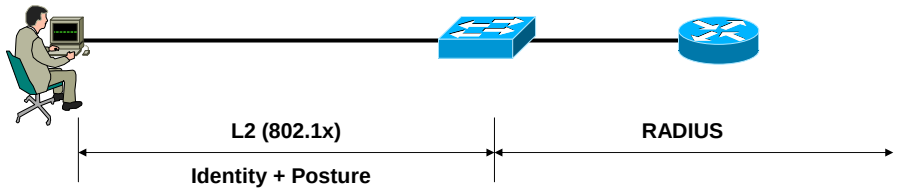


1. 802.1x Authentication
2. Optional 802.1x Policy assignment
3. DHCP
4. NAC at first L3 Gateway

IBNS & NAC Phase 2

LAN Port 802.1x Operation (Q2 CY05)

Cisco.com



1. 802.1x Authentication
2. Single Tunnel, Multiple Transactions
3. Identity Authentication
4. NAC Posture Validation
5. Policy Assignment
6. DHCP

Why Do We Care So Much About CISF?

Cisco.com

- CSI/FBI Survey shows Information Theft as the #1 growing trend
- 99% of all enterprises network ports are OPEN
- Any laptop can plug into the network and gain access to the network
- 75% of attacks that caused monetary loses were from the inside.
- Highest source of loss was theft of proprietary information – with a average of 2.7 million per incident
- Insider attack by disgruntled employees was listed as likely source by 77% of respondents

S²

LAN Security Threats

Cisco.com

- MAC Address Flooding Attack
  - Hacking Tool: macof (part of dsniff package)
  - SYN floods with random src and dst MAC, random src and dst IP
  - After CAM Table Fills, Traffic Flooding Occurs (32K entries)
  - Random IP addresses include multicast address space and will eventually cause distribution layer to fail due to excessive processing of multicast routes
- DHCP Rogue Server Attack
  - Hacking Tool: gobbler or actual rogue DHCP server
  - Man in the middle attacks via DNS or IP default GW forging
- DHCP Starvation
  - Hacking Tool: gobbler
  - Depletion of DHCP address space
- ARP Spoofing or ARP Poisoning Attack
  - Hacking Tool: ettercap, dsniff, arpspoof
  - Menu driven discovery of MAC level topology with ARPs and DNS Reverse Name Lookup
  - Man in the middle attacks with integrated packet capture and password sniffing

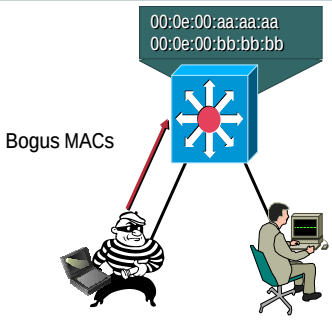
Catalyst Integrated Security Features

Cisco.com

- Port security to limit the number of MAC addresses per port to prevent CAM flooding attacks
- DHCP Snooping to prevent DHCP rogue server attacks and build a DHCP snooping binding table
- Dynamic ARP inspection to restrict ARP responses and gratuitous ARP to only the address(es) found in the DHCP binding table
- IP Source Guard to restrict IP traffic sourced from a particular interface to only address(es) from in the DHCP binding table

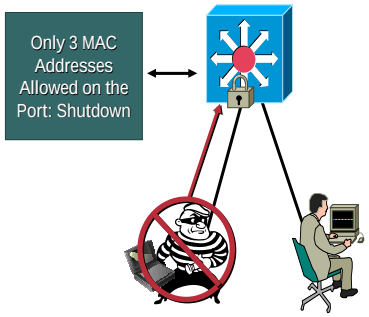
Port Security
against MAC Address Flooding Attack

Cisco.com



Problem:

"Script Kiddie" Hacking Tools Enable Attackers Flood Switch CAM Tables with Bogus Macs; Turning the VLAN into a "Hub" and Eliminating Privacy

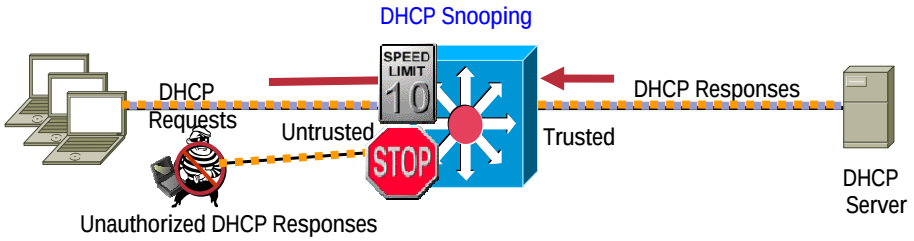


Solution:

CISF Recognizes MAC Flooding Attack and Locks down Port and Sends an SNMP Trap

DHCP Snooping
against Rogue / Malicious DHCP Server

Cisco.com

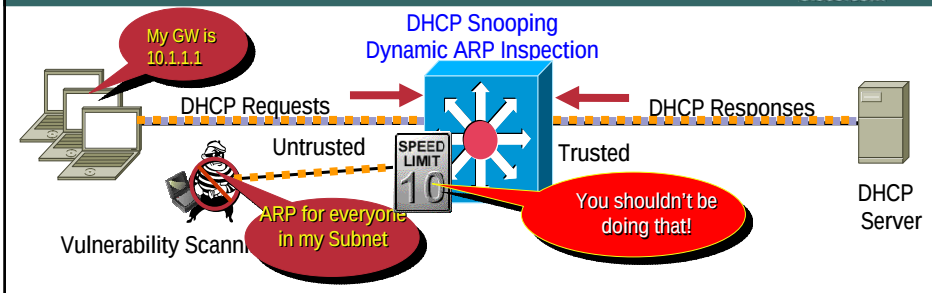


DHCP Snooping

1. Track the Request (Discover)
2. Track the Response (Offer)
3. Rate limit Requests on Trusted Interfaces. Limit DOS attacks on DHCP Server
4. Deny Responses (Offers) on non trusted interfaces. Stop Malicious or errant DHCP Server

Dynamic ARP Inspection
against Recognizance / ARP Scan's

Cisco.com



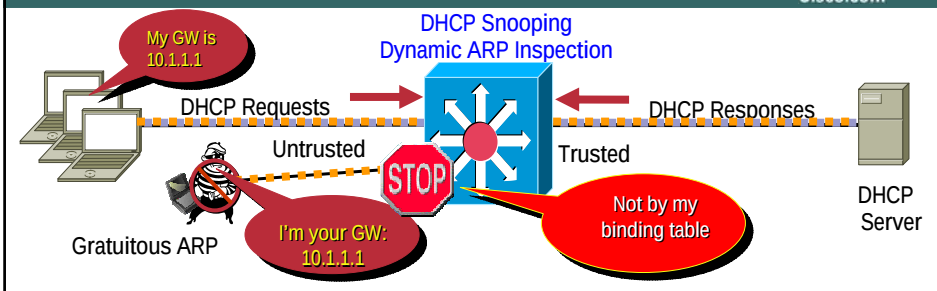
Dynamic ARP Inspection

1. Use DHCP Snooping Binding Table
2. Track MAC to IP from DHCP transactions
3. Rate limit ARP Requests from client ports. Stop port scanning Recognizance thwarted…

Dynamic ARP Inspection

against ARP poisoning (ettercap, dsnif, arpspoof)

Cisco.com



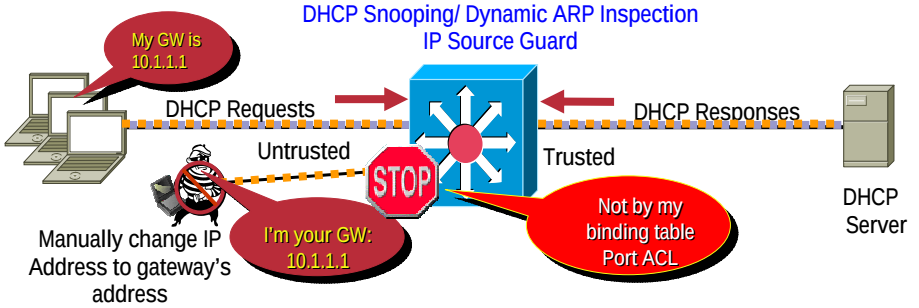
Dynamic ARP Inspection

1. Use DHCP Snooping Binding Table
2. Track MAC to IP from DHCP transactions
3. Rate limit ARP Requests from client ports. Stop port scanning
4. Drop BOGUS Gratuitous ARP's. Stop ARP Poisoning/ MITM attacks

IP Source Guard

against incorrect/malicious hard coded IP Address

Cisco.com

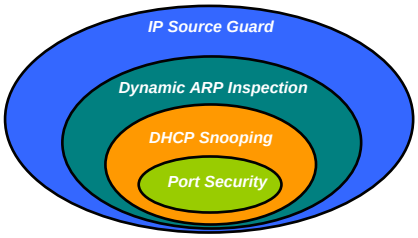


IP Source Guard

1. Use DHCP Snooping Binding Table
2. Track IP Address to Port associations
3. Dynamically Program Port ACL to drop traffic not originating from IP Address assigned via DHCP

CISF Summary

Cisco.com



- Port Security prevents MAC flooding attacks
- DHCP snooping prevents client attack on the switch and server
- Dynamic ARP Inspection adds security to ARP using DHCP snooping table
- IP Source Guard adds security to IP source address using DHCP snooping table
- All features work on switchports

```
ip dhcp snooping
ip dhcp snooping vlan 2-10
ip arp inspection vlan 2-10
!
interface fa3/1
swithport port-security
switchport port-security max 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
!
Interface gigabit1/1
ip dhcp snooping trust
ip arp inspection trust
```


Matrix for Security Features 1/2

Cisco.com

Feature/ Platform	6500/ CatOS	6500/ IOS	4500/ CatOS	4500/ IOS
Dynamic Port Security	Now 7.6(1)	Now 12.1(13)E	Now 5.1(1)	Now 12.1(13)EW
DHCP Snooping	8.3(1)	Q1CY05 12.2(18)SXD2	N/A	Now** 12.1(12c)EW
DAI	8.3(1)	Q1CY05 12.2(18)SXD2	N/A	Now ** 12.1(19)EW
IP Source Guard	8.3(1)*	Q1CY05* 12.2(18)SXD2	N/A	Now ** 12.1(19)EW

* Requires Sup720

** For the Catalyst 4500/IOS-based platforms, this requires Sup2+, Sup3, Sup4, Sup 5. These Sups are supported on the Catalyst 4006, 4503, 4506, and 4507R chassis.

NOTE: There are no plans to support these features for any Catalyst 4000/4500 platform running CatOS, or any 2900 platform.

Matrix for Security Features 2/2

Cisco.com

Feature/ Platform	3750 EMI/SMI	3550 EMI/SMI	2970 EI	2950 EI	2950 SI
Dynamic Port Security	Now 12.1(11)AX	Now 12.1(4)EA1	Now 12.1(11)AX	Now 12.0(5.2)WC1	Now 12.0(5.2)WC1
DHCP Snooping	Now 12.1(19)EA1	Now 12.1(19)EA1	Now 12.1(19)EA1	Now 12.1(19)EA1	N/A
DAI	Q2CY04 **** 12.2(20)SE	Q4CY04 *** 12.2(XX)SE	N/A	N/A	N/A
IP Source Guard	Q2CY04 **** 12.2(20)SE	Q4CY04 *** 12.2(XX)SE	N/A	N/A	N/A

*** Current target. Also, 3750/3550 will support DAI and Source Guard on EMI image only.

**** 3550 EMI only

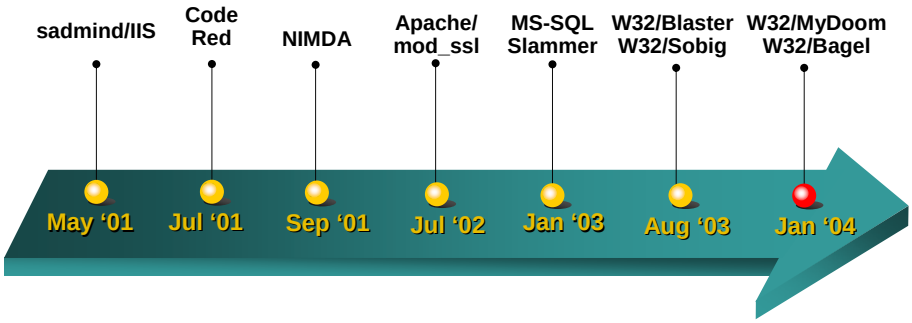
NOTE: There are no plans to support these features for any Catalyst 4000/4500 platform running CatOS, or any 2900 platform.

Cisco.com

Mitigating the Worm Impact

What Are the Other Top of Mind Issues With Security?

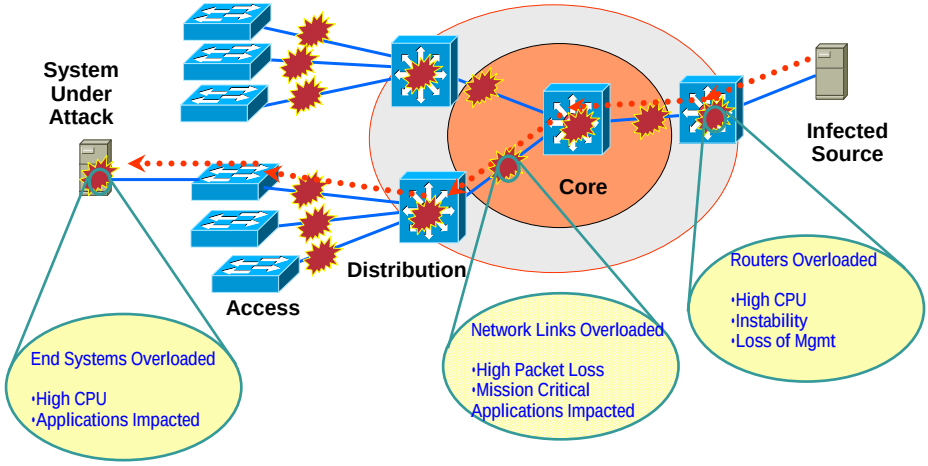
Cisco.com



The Progression of Worm Development

Impact of an Internet Worm

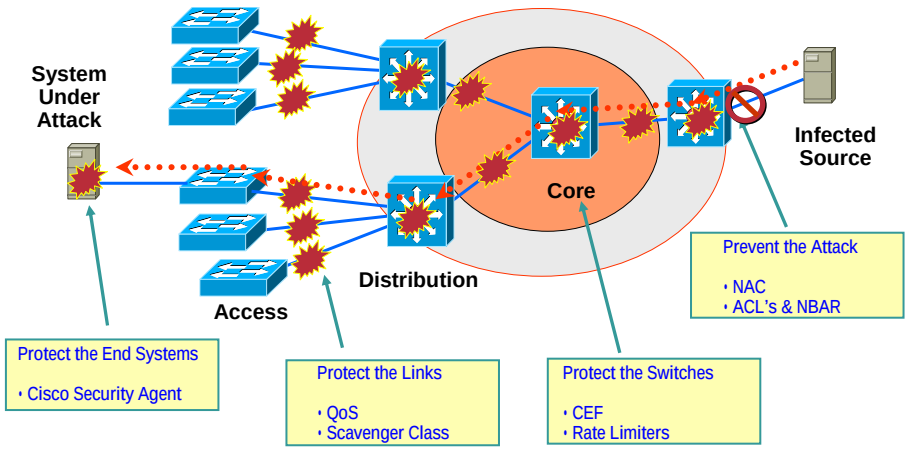
Cisco.com



Attacks targeted to end systems CAN and DO affect the infrastructure

Mitigating the Impact

Cisco.com



Comprehensive Enterprise Security Strategy directed at protecting the *entire* network

Nimda (Code Red)
Aggressive Network Scanning

Cisco.com

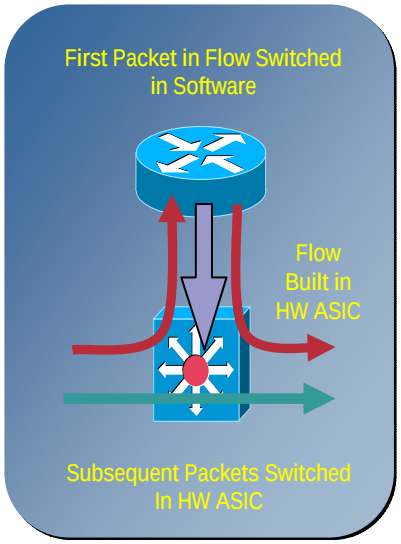
- Nimda, Slammer and similar worms send packets to a very large number of random addresses looking for vulnerable end systems to attack
- Code Red chose a random destination address for every scan attempt
- Nimda improved on Code Red:
  - 50% of the time, an address with the same first two octets will be chosen
  - 25% of the time, an address with the same first octet will be chosen
  - 25% of the time, a random address will be chosen
- Problem: Code Red and Nimda disabled many networks that used Flow or 'on-demand' based switching
- Solution: Cisco Express Forwarding [CEF]

Catalyst Cisco Express Forwarding

Before CEF…Flow-Based Switching

Cisco.com

- Flow-Based Switching is Limited by the ability of the CPU to setup initial flows
- Flow Based HW Caches may overflow when an abnormally high number of flows established
- Ability of CPU to process control plane traffic (EIGRP, OSPF, BPDU) suffers when flow rate is abnormally high

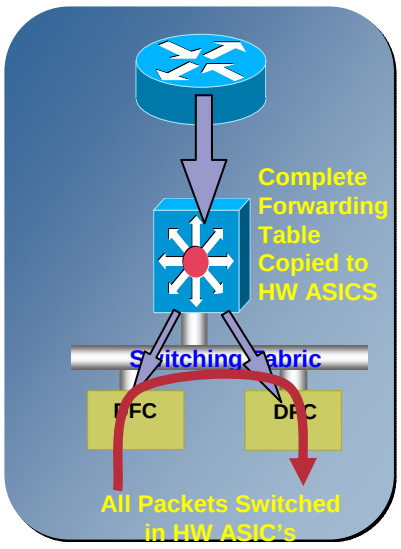


Catalyst Cisco Express Forwarding

CEF - Topology-Based Switching

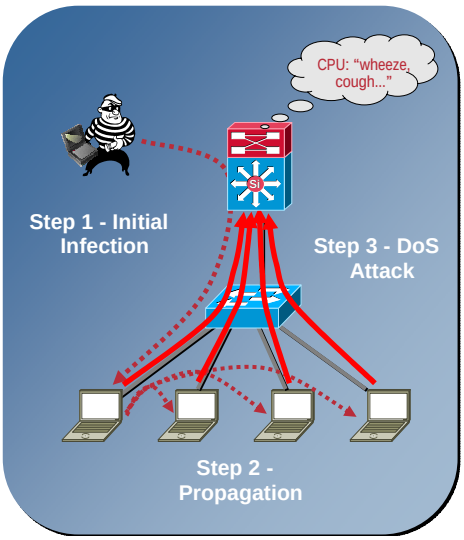
Cisco.com

- Route Processor builds a Forwarding Information Base (FIB) calculated based on routing table entries, not traffic flows
- Hardware forwarding of first packet in each flow, whether there are one or one million new flows
- Control plane unburdened by traffic forwarding - dedicated to protocol processing



Control Plane Attacks

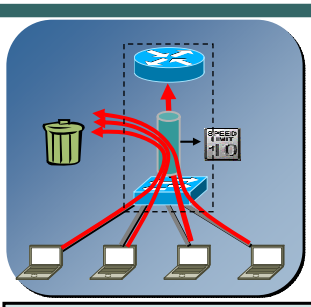
Cisco.com



- Intentional attacks can also attempt to cause resource constraints on switches and routers
  - Certain types of IP Packets with are always sent to the CPU for processing
- Fully loading the RP to 100% utilization can result in
  - 1. Routing protocols getting out of sync with the rest of the network causing network flaps and major network transitions
  - 2. High load on the RP can cause the console to lock up and make
  - 3. Other RP based processes to cease operation or run with unpredictable results

Control Plane Protection
RP Rate-Limiting

Cisco.com



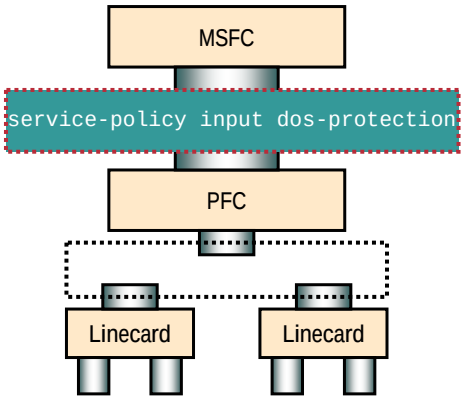
- Control-plane rate-limiting throttles the amount of traffic forwarded to the RP in a given interval
- Both Unicast and Multicast Rate-limiters are avail on the Sup720

Unicast RP Rate Limiters		Multicast RP Rate Limiters
ACL Input	ICMP Redirect	FIB Miss
ACL Output	ICMP Unreachable	Partial
ACL VACL Log	RPF Failure	Connected
CEF Glean	Layer 2 PDU	
CEF Receive	Layer 2 Protocol Tunneling	
IP Errors	TTL Failure	
IP Features	MTU Failure	
Unicast RP Rate Limiters		Multicast RP Rate Limiters

Control Plane Protection
Control Plane Policing

Cisco.com

- Introduce a new interface: the control-plane interface
- Provides QoS control for Control Plane packets
- Leverages MQC
- Preserves existing interface configuration
- Is easy to configure (clear and simple)
- Provides significant protection against DoS



Slammer (Sapphire)
Exponential Growth in Network Traffic

Cisco.com

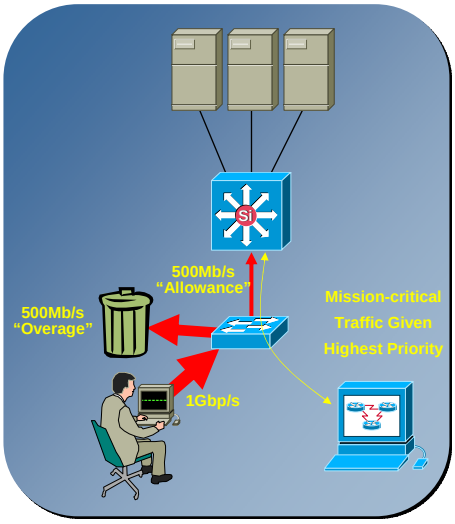
- **Code Red had an initial infection rate of about 2 new infected systems per hour**
- **Slammer had an initial infection rate of 7 systems per minute**
- **The rapid rate of infection and aggressive scan rate of Slammer resulted in extreme traffic loads**
- **Problem: High packet loss rates disrupted mission critical systems**
- **Solution: Protect mission critical applications using QoS with Scavenger class marking and source based policers**

Cisco Solution - Scavenger Class QoS

Mitigate the Impact of Worms

Cisco.com

- Utilizes QoS and Rate Limiting
- Ensures that Mission Critical Traffic gets through
  - High priority traffic like VoIP and Business Systems Traffic already configured for biased queuing
- Maintains Management traffic so that IT Managers can place ACLs and track down infections
- Keeps network devices from being overrun

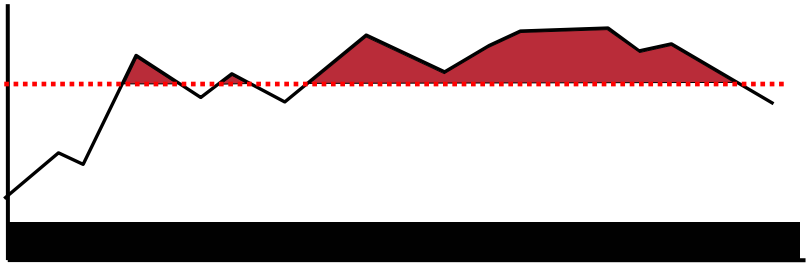


Scavenger Class QoS

Protection from a Turbo-Worm

Cisco.com

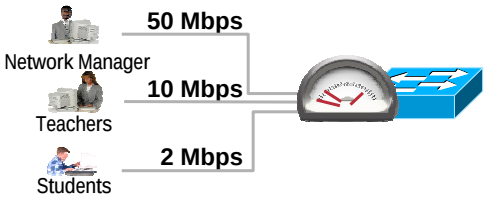
- **During 'abnormal' worm traffic conditions traffic marked as Scavenger is aggressively dropped**
- **Priority Queuing ensuring low latency and jitter for VoIP**
- **Stations not generating abnormal traffic volumes continue to receive network service**



Protecting Against Denial of Service

Using the tools Cisco IOS Has Built in

Cisco.com



- PROBLEM:

  Many denial of services tools "Blast" the network or host ports with huge streams of traffic

- SOLUTION:

  Rate limiting allows network managers to set bandwidth thresholds to prevent the deliberate or accidental flooding of the network; keeps traffic flowing smoothly

Catalyst 6500-Sup720
Per User Rate Limiting

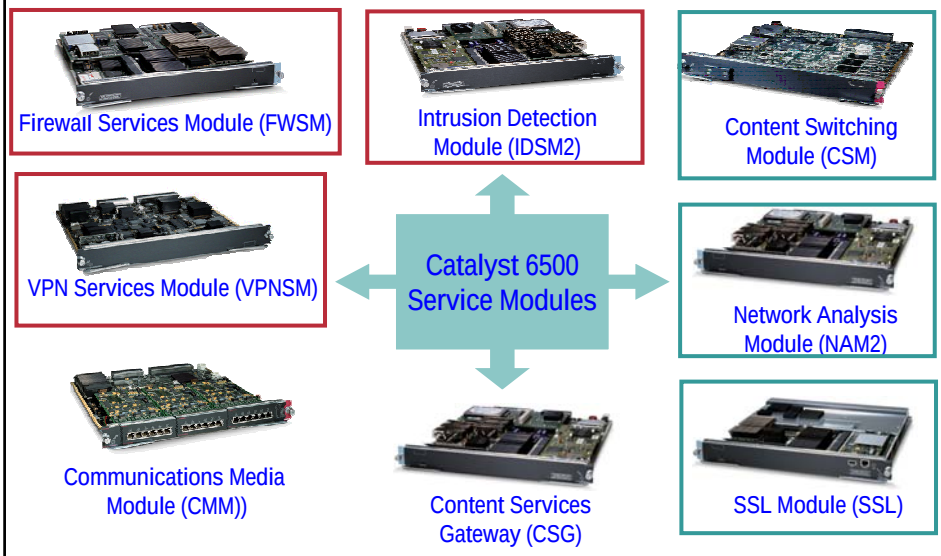
```
class-map match-all User
 match access-group name User
!
policy-map User
     class User
          police flow mask src-only 100000000 3125000
     conform-action transmit exceed-action drop
interface GigabitEthernet4/1
 ip address 10.1.1.1 255.255.255.0
 logging event link-status
 speed nonegotiate
 service-policy input User
 no cdp enable
!
ip access-list extended User
permit ip any any
```


Catalyst 6500 Integrated Security Service Modules

Catalyst 6500

Integrated High-Performance Service Modules

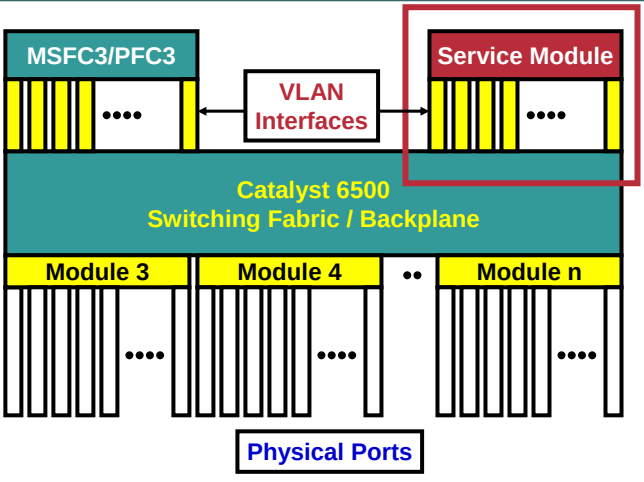
Cisco.com



Catalyst 6500 Service Modules

How it is viewed?

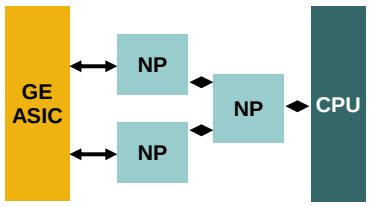
Cisco.com



Interface of Service Module = VLAN ← Physical Ports

Firewall Services Module (FWSM)

Cisco.com



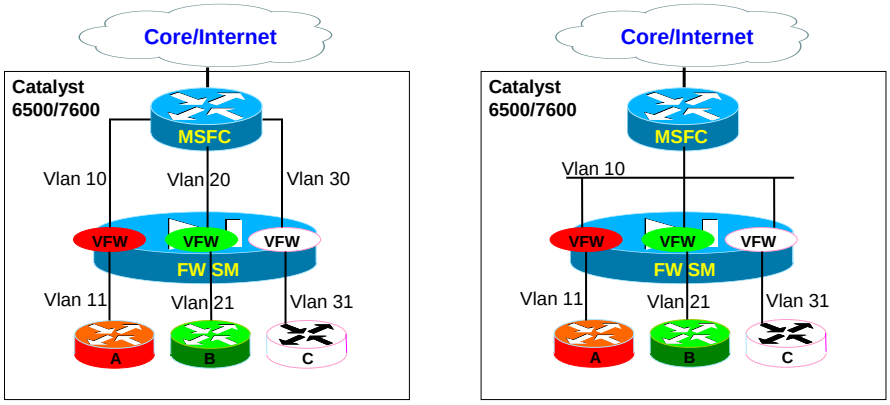
THE WS-SVC-FWM-1-K9 Supports:

- Fabric line card
- Supported in Cisco IOS and Catalyst OS
- Network-processor based hardware
- Up to 5Gb aggregate throughput
- Up to 3Mpps aggregate performance
- Up to 1M TCP concurrent connections
- Up to 100K new connections per second for HTTP, DNS and enhanced SMTP
- Support for 100 Virtual Firewalls
- Transparent Firewall support
- Intra and Inter chassis failover in Active/Standby mode
- Dynamic Routing with RIP and OSPF

Firewall Services Module (FWSM)

Virtual Firewall Support

Cisco.com

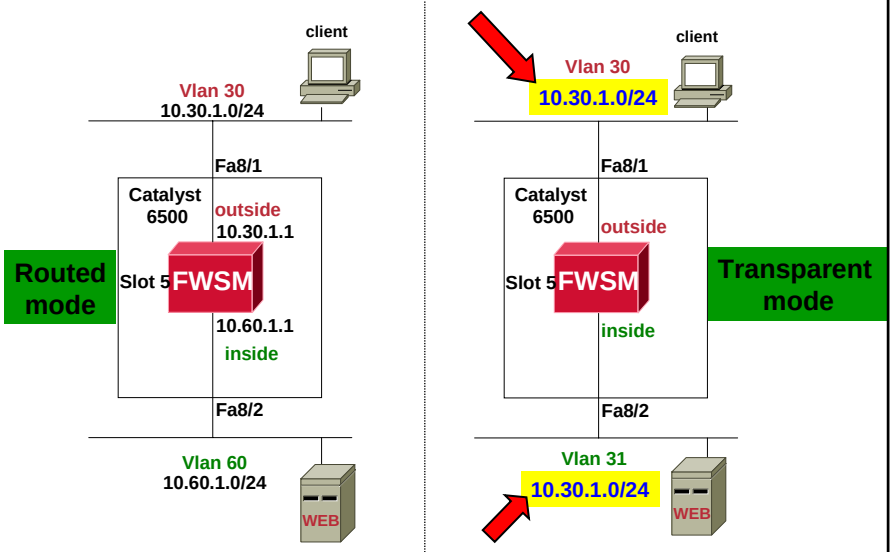


- **E.g. three customers ⇨ three security contexts – scales up to 100**
- **VLANs can be shared if needed (VLAN 10 on the right-hand side example**
- **Each context has its own policies (NAT, access-lists, fixups, etc.)**

Firewall Services Module (FWSM)

Transparent Firewall Support

Cisco.com



Intrusion Detection Module 2 (IDSM2)

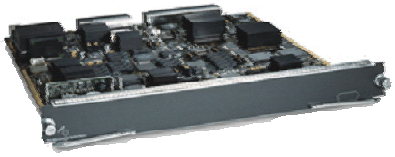
Cisco.com

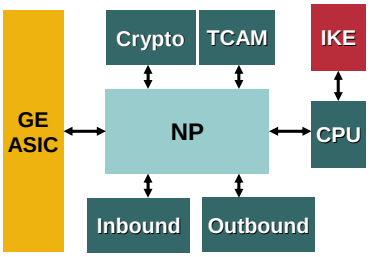
The WS-SVC-IDSM2 Supports:

- Supports connection to 32-Gbps shared bus
- Supports single 8-Gbps fabric connection
- Comprehensive attack recognition
- Same code base as Cisco IDS appliances
- Monitors up to 600Mbps of traffic (@ 450 byte Packet)
- Supports arrival rate of up to 100 flows/sec
- Passive monitoring / In-Line Mode (beta)
- Extensive signature database
- Built in web-based management (IDM)
- Support IDS Event Viewer
- Sensor stateful failover
- Supports Alarms, Shunning and TCP resets, Drop(beta)

VPN Service Module (VPNSM)

Cisco.com



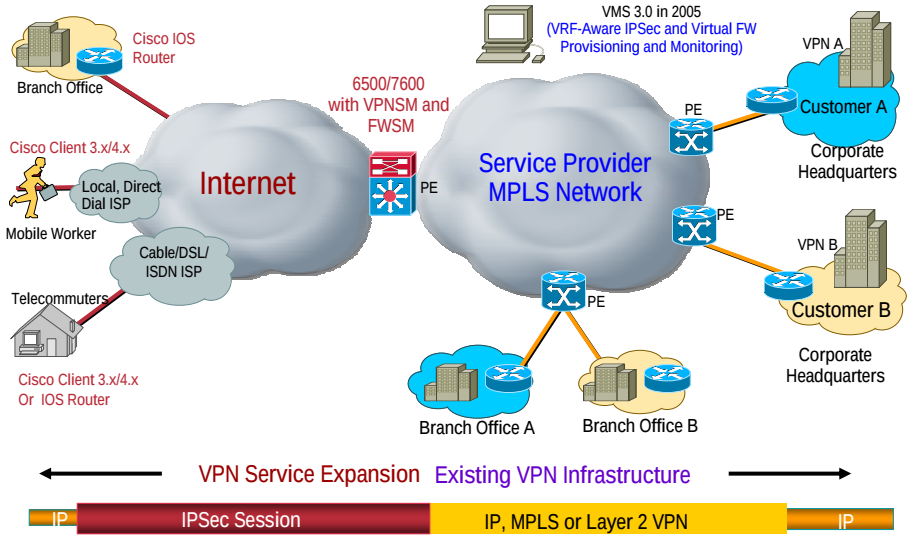


The WS-SVC-IPSEC-1 Supports:

- Supports connection to 32-Gbps shared bus
- Supports single 8-Gbps fabric connection
- Cisco IOS® support only
- Sup2 and Sup720 support
- IPSec site to site VPN
- EZ-VPN Client support
- Up to 8000 tunnels supported
- 1.9Gbps 3DES performance (500+ byte packets)
- 1.6Gbps 3DES performance (300+ byte packets)
- Up to 10 VPNSM per platform (14 Gbps or 5 Mpps)
- Tunnel setup rate 60 tunnels/sec
- IKE, IKE-XAUTH, MD5, SHA-1, SSH
- Kerberos Telnet, X.509 Digital signatures
- Shared Secrets
- ESP DES and 3DES

Network Based IPSec VPN Services Aswan Solution Architecture – Phase 2.0

Cisco.com



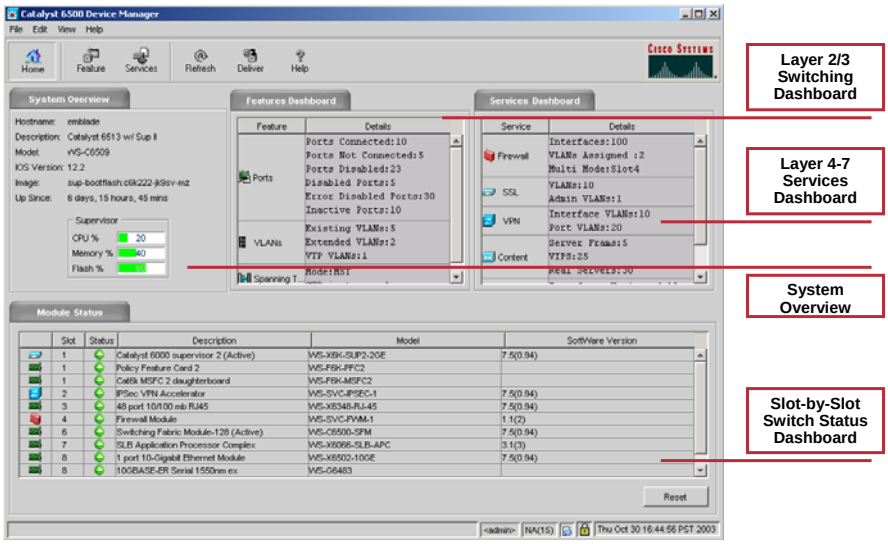
New Features in 12.2(18)SXD1

Cisco.com

- Sup720 VRF-aware IPsec
  - Overlapping IP Addresses per VRF/Customer
  - Crypto Maps per VRF
  - RADIUS is global (or per VRF via proxy)
  - Single Public IP for Mapping IPsec into All VRFs
- Inter Chassis Active/Standby IPSec Stateful HA only for VRF-Aware IPSec
- Max of 512 VRFs suppoted per platform in this release
- Tunnel Scalability in this Release:
  - 4K max for native IPSec site-to-site or remote access
  - 1K max for IPSec+GRE (Tunnel Prot.) with VRF-Lite
  - 512 max for IPSec+GRE (TP) with MPLS in VRFs

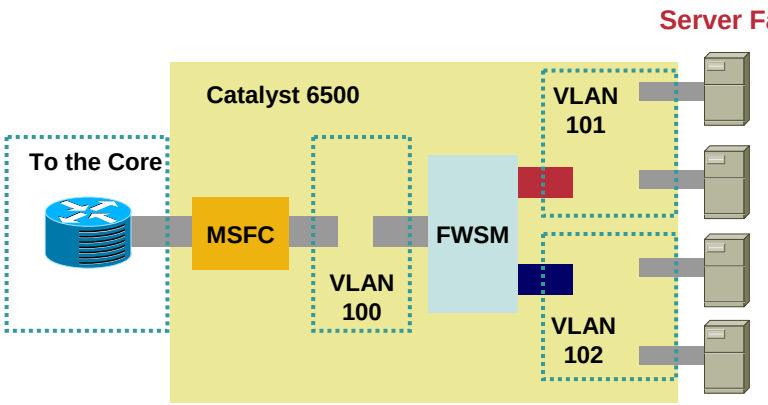
CiscoView Device Manager (CVDM)

Cisco.com



Catalyst 6500 Security Module Reference Design

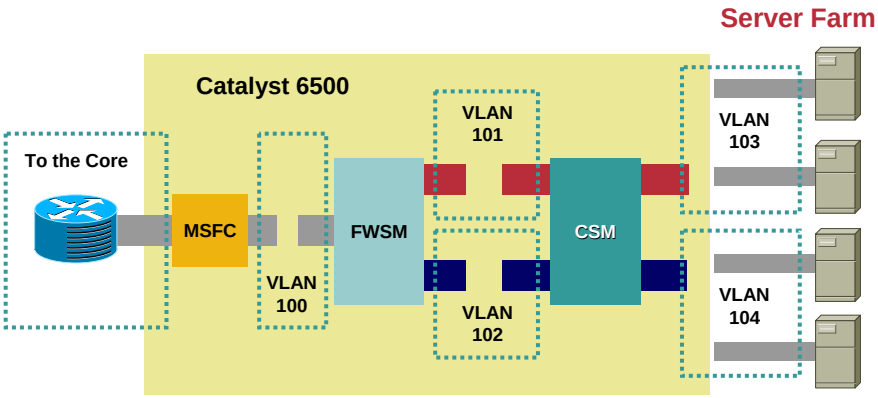
Service Module Reference Designs
FWSM in Server Farm



Service Module Reference Designs

FWSM + CSM in Server Farm

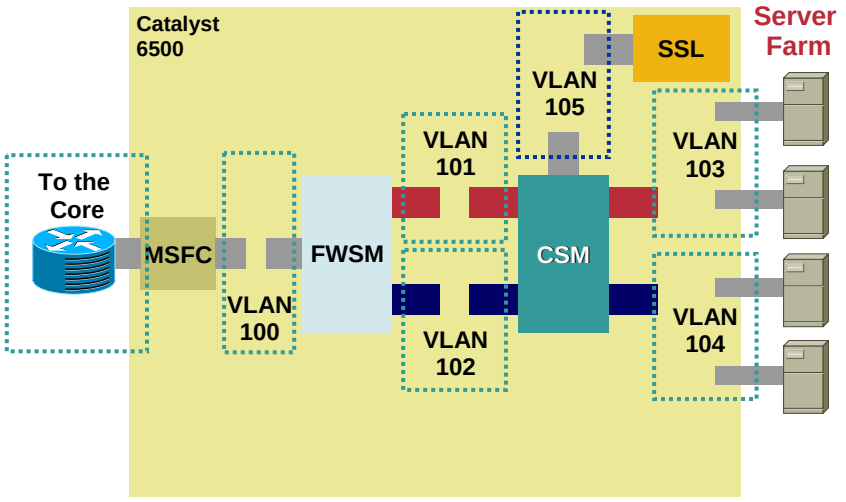
Cisco.com



Service Module Reference Designs

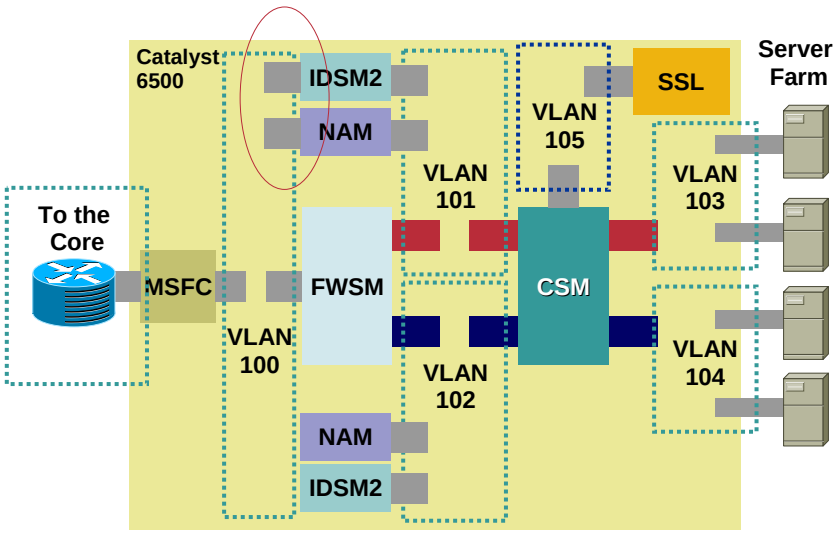
FWSM + CSM+SSL in Server Farm

Cisco.com



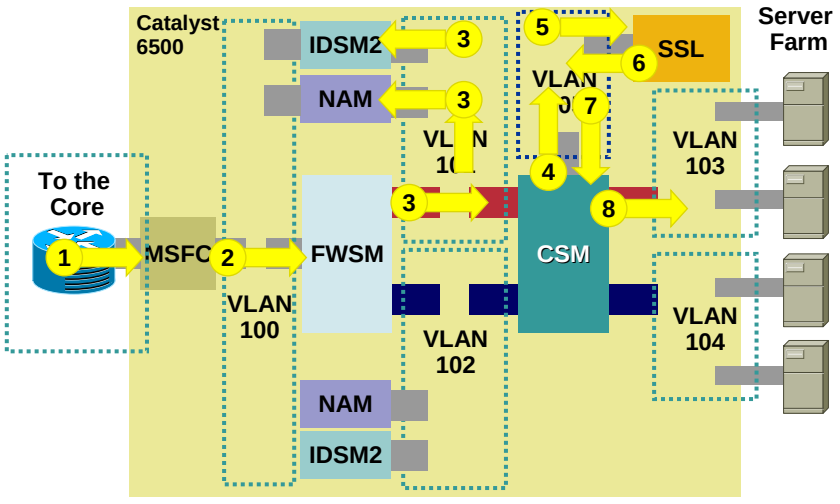
Service Module Reference Designs
FWSM + CSM + SSL + IDSM + NAM in Server Farm

Cisco.com



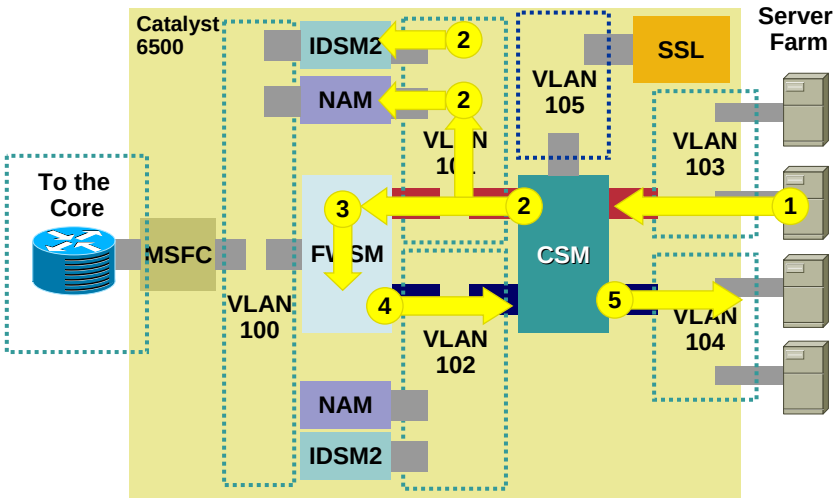
Service Module Reference Designs
Client Packet Flow

Cisco.com



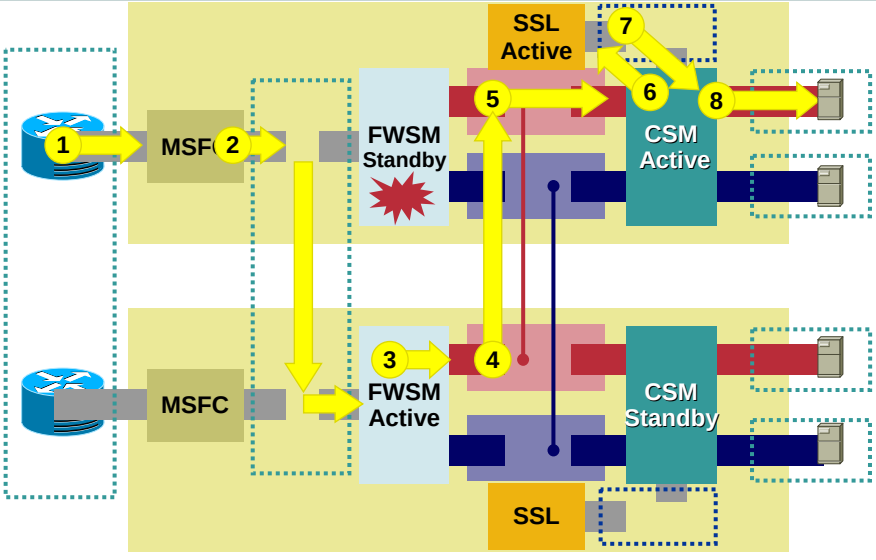
Service Module Reference Designs
Server Packet Flow

Cisco.com



Service Module Reference Designs
Packet Flow – Redundancy / Failover Configuration

Cisco.com



Q and A

CISCO SYSTEMS