Cisco.com

SP Security

2004년 10월 20일

Cisco Systems Korea
성일용(iyseong@cisco.com)

Agenda

Cisco.com

What are SP Security Threats

- General SP Security Threats
- Internet Worm Threats
- P2P Security Threats

What are SP Security Solutions

SP Specific Solutions

- Black Hole / Sink Hole
- BCP 38 Filtering
- BGP Security Solutions
- Infrastructure ACLs / Control plane Protections

De-Worming Tools

- Cisco Guard/ Traffic anomaly Detector
- Netflow / RMON / Anomaly Detection Tool
- Firewall
- Network IDS/IPS
- Host IDS/IPS

SP Managed Security

- Managed Firewall
- Managed VPN service
- Managed Security Provisioning & Management
- Managed Security Report

SP Security Threats

• Se

The Internet Health Report (Last Hour)

About this site

	UUNET	C&W	QWEST	VERIO	SPRINT	GENUITY	LEVEL3	AT&T	INTERNAP
UUNET	289	62	74	81	77	102	88	100	143
C&W	62	29	21	37	29	36	28	39	58
QWEST	74	21	49	28	35	33	38	33	88
VERIO	81	37	28	86	41	40	34	31	43
SPRINT	77	29	35	41	35	35	37	37	46
GENUITY	102	36	33	40	35	45	37	47	43
LEVEL3	88	28	38	34	37	37	61	36	48
AT&T	100	39	33	31	37	47	36	37	55
INTERNAP	143	58	88	43	46	43	48	55	35

LAST DAY

Generated Sat Jan 25 08:02:53 2003 GMT

Healthy < 80ms Latency. Stable < 120ms Latency.

Severe < 180ms Latency. Critical > 180ms Latency.

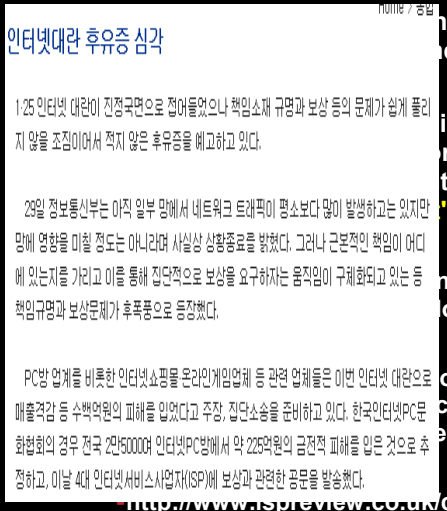
The colored square indicates the largest geometric mean within the area specified, over the time period.

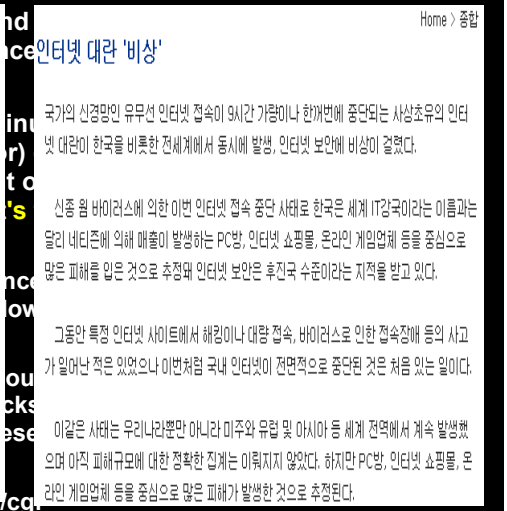
The colored number indicates the overall geometric mean over the time period.

11 8 6 2 0

News—January 22, 2002
Cloud-Nine Officially Closes ISP!

By:mark.j @ 10:44:AM—Comments (35)—SendNews [HERE]/PrintNews [HERE]

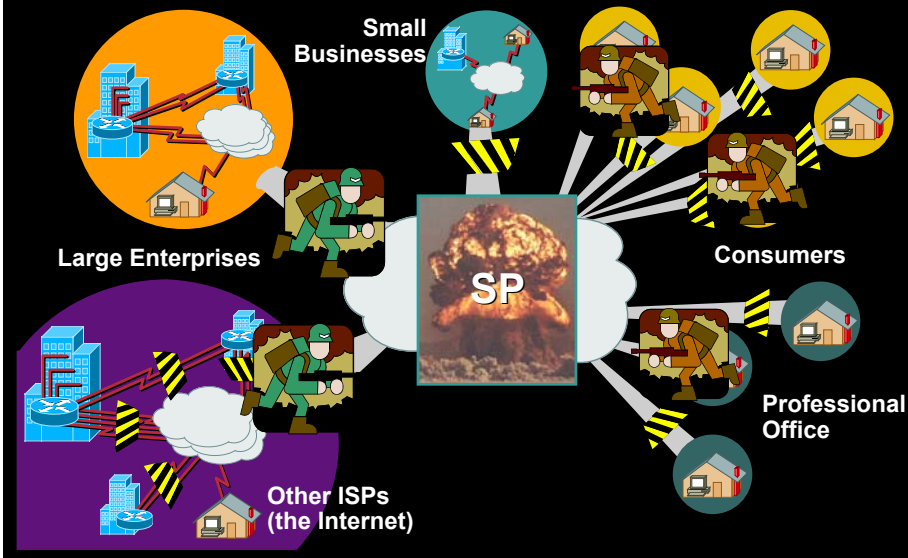




http://www.ispreview.co.uk/cgi-bin/ispnews/printnews.cgi?newsid1011696274,91619

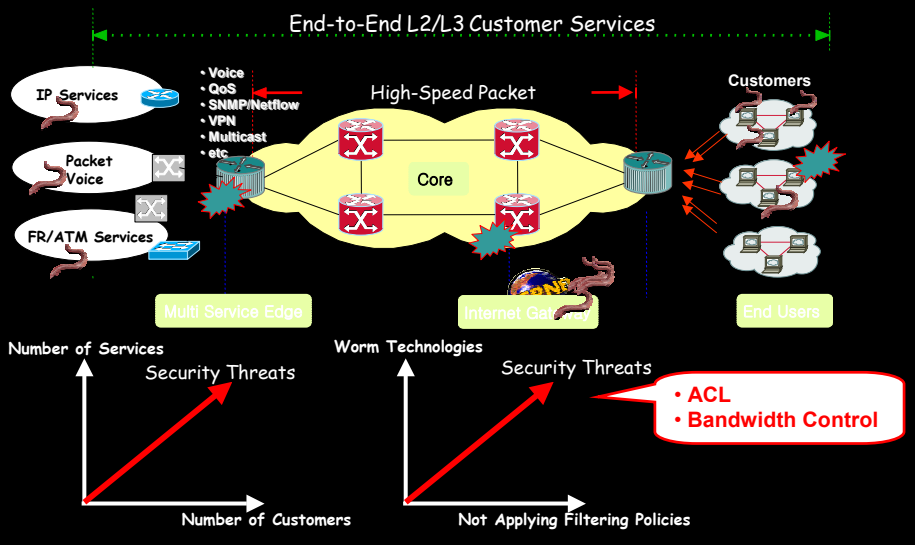
SP's Are Today's New Battle Grounds

Cisco.com



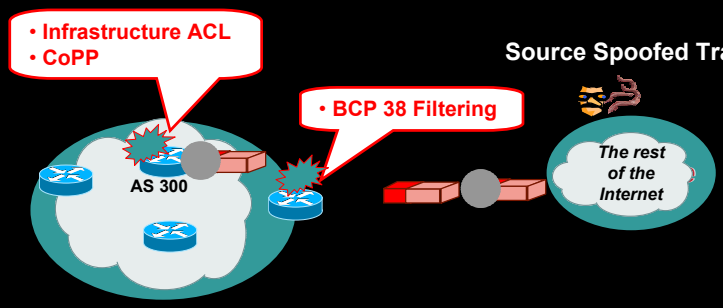
General SP Security Threats

Cisco.com



General SP Security Threats

Cisco.com

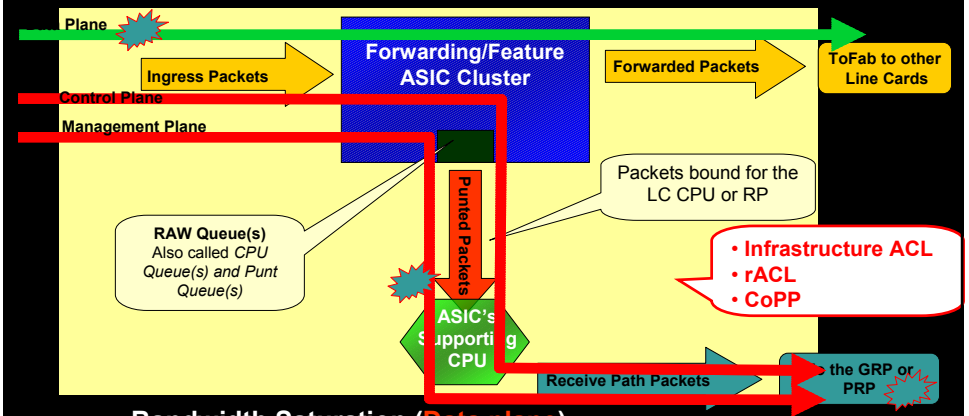


Most of the source spoofed traffics are for

- DoS attacks
- Traffic that do not want to be traced (= not trusted)
- May be targeted to the SP network Infra and cause SP resource consuming

General SP Security Threats

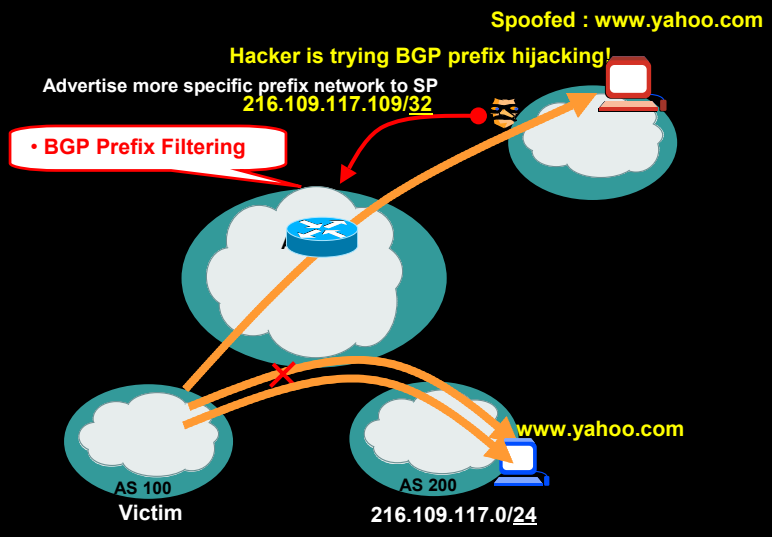
Cisco.com



- Bandwidth Saturation (Data plane)
- Target the Control or Management Plane (Receive Path traffic on the Control and Management Plane)
- Saturate the Punt path out of the forwarding/feature ASIC by abusing the TCP/IP standards (Data plane traffic that is punted from the forwarding/feature ASIC)

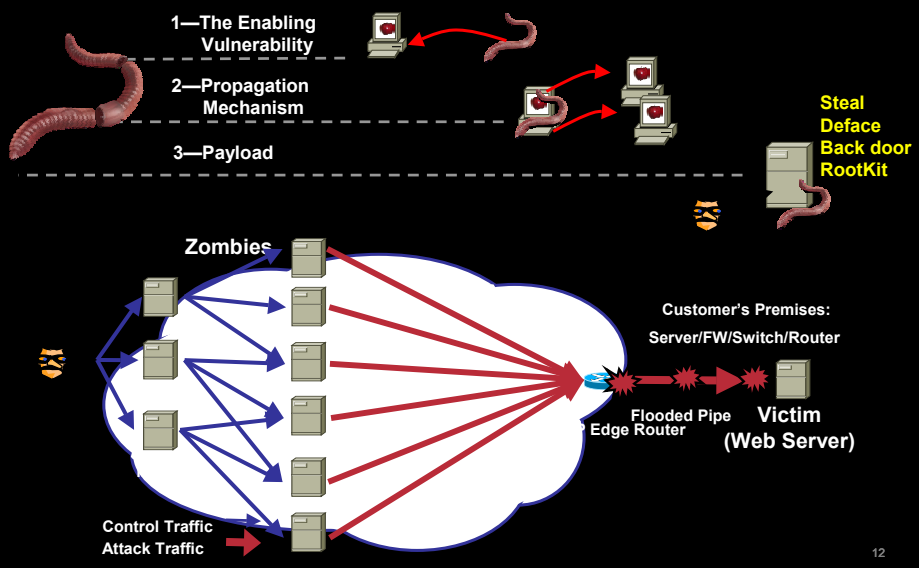
General SP Security Threats

Cisco.com



Internet Worm Threats

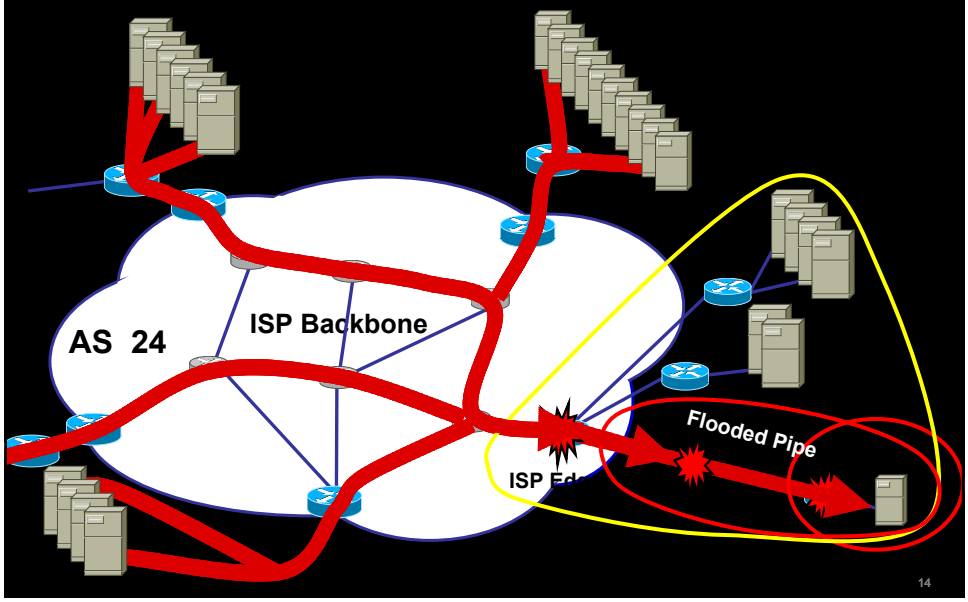
Cisco.com



Internet Worm Threats (BOTNET)

- BOTNETs are better than DDOS Kits:
  - BOTNETs allow for all the types of DDOS. 1Gbps
  - ICMP attacks, TCP Attacks, and UDP Attacks are easy to craft and launched
  - BOTNETs allow for http overload attacks—where every machine in the BOTNET pulls down the same page—refresh—pulls down the same page—refresh again—etc.
  - This sort of HTTP abuse is in its infant stages; load balancers thinking they provide "DOS protection" beware
- Of course the key advantage of the BOTNET is the ability to hide the real controller of the BOTNET
- www.megasecurity.org
- Controlled via IRC channels

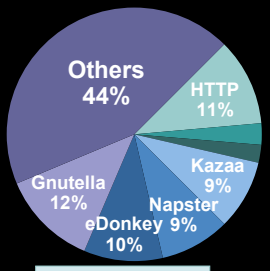
Internet Worm Threats (DDoS)



P2P Security Threats

Cisco.com

JULY 2002 IN A LARGE EUROPEAN ISP



P2P = 40%

P2P App	Connection properties
Gnutella	Connection is a simple TCP connection to some peers (called servents—servers-clients)
eDonkey	With a single TCP connection to one server (to publish file and retrieve the server list) and multiple UDP 'connections' to all servers (for search)
Kazaa	All peers register to a single 'tracker' (IP address, dynamic TCP port, local chunks, …) All peers connect to some peers from tracker

P2P Security Threats

Cisco.com

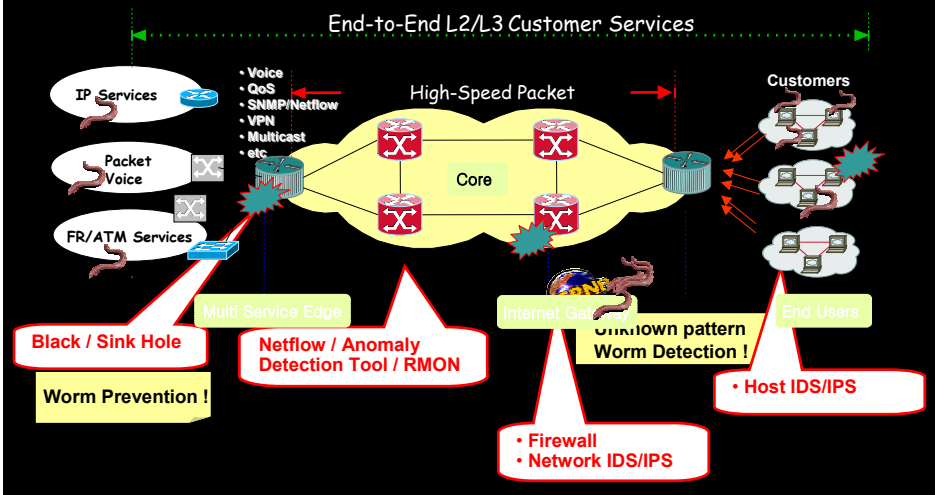
- Retrieving executable content
- P2P provides anonymity on purpose
- Naive users will download and execute
- Buffer Overflow
  - Peers are listening on a couple of UDP or TCP ports
  - This may open a door to a buffer overflow attack
- Attractive target:
  - Million of peers
  - Always connected
- Most of P2P protocols do not have authentication
- Easy to write a pseudo peer or server program

P2P Security Threats

- The ‘push’ operations could be diverted to launch DoS attack on a victim even behind a firewall
- Registering victims as peers will force other peers to try to connect
- Kazaa (and perhaps others) can use the P2P network in order to automatically install
  the next version, this mechanism could be used to install thousands of Trojans
- P2P Adware/Spyware (when click banner)
  - Lost of time and resources
  - Door to hostile code on the clicked URL
- SP is wasting the Bandwidth

  The most visible sign: Upstream is utilized 100% even during nights

How to defense from SP Security Threats

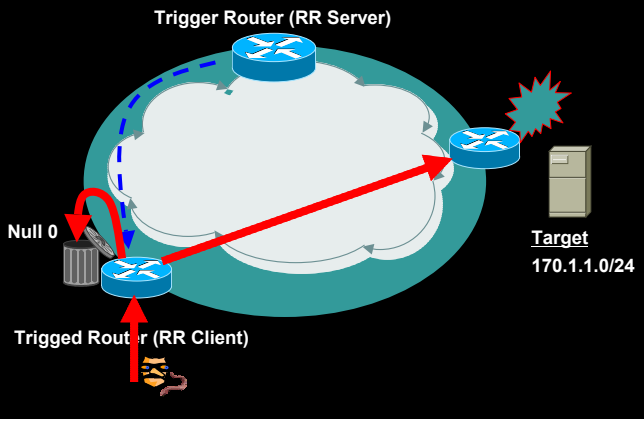


SP Security Solutions
Black Hole / Sink Hole

Black Hole

Overview

- Black hole filtering will route packets to Null 0 (black hole = CEF pseudo interface)
- Filter packets based on destination
- SP is running iBGP with RR Server(Trigger router) and Client(Triggered router)



Black Hole

Preparing

BGP Network

- iBGP RR Server & Client
- No-export BGP community
- Block prefixes less than /24 (iBGP trigger advertises between /25 and /32)

Triggered Router

- All triggered routers should configure a black hole static route
- Black hole Test-Net : 192.0.2.0/24

```
ip route 192.0.2.0  255.255.255.0  Null0
```

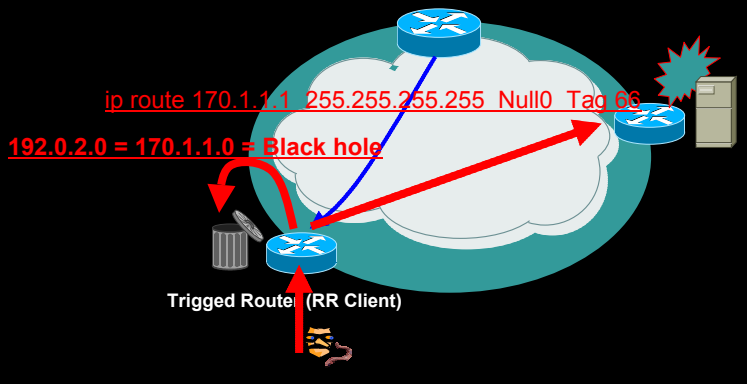
- If (packet tag=66) then (drop this packet)

```
router bgp 109
   redistribute static route-map static2bgp
!
route-map static2bgp permit 10
   match tag 66
   set ip next-hop  192.0.2.1
route-map static2bgp permit 20
```


Black Hole

Activation

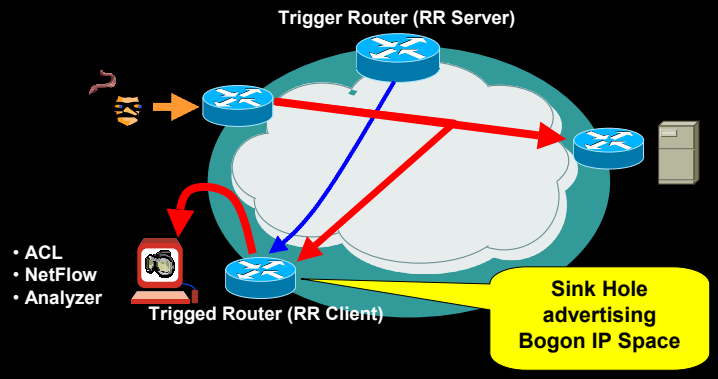
- Trigger Router(RR Server) advertises the victim network to all the triggered routers(RR Clients)
- Triggered router(RR Client) gets this black holed prefix advertisements and drop packets forwarding this network



Sink Hole

Cisco.com

- Sink Hole works the same method with Black Hole
- Sink Hole method does not drop packet but inspect and analysis these packets
- Sink Hole analyzer monitors
  - DoS Attack / Worm traffic
  - Security Scanning traffic
  - Backscatter(Random source spoofing) traffic



How to monitor

Cisco.com

Netflow Monitoring

```
router_A# sh ip cache (verbose) flow
IP packet size distribution (85435 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2728 active, 1368 inactive, 85310 added
  463824 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec      /Flow     /Flow
TCP-X                2      0.0         1   1440      0.0       0.0       9.5
TCP-other        82580     11.2         1   1440     11.2       0.0      12.0
Total:           82582     11.2         1   1440     11.2       0.0      12.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         132.122.25.60   Se0/0         192.168.1.1     06 9AEE 0007     1
Et0/0         139.57.220.28   Se0/0         192.168.1.1     06 708D 0007     1
Et0/0         165.172.153.65  Se0/0         192.168.1.1     06 CB46 0007     1
```

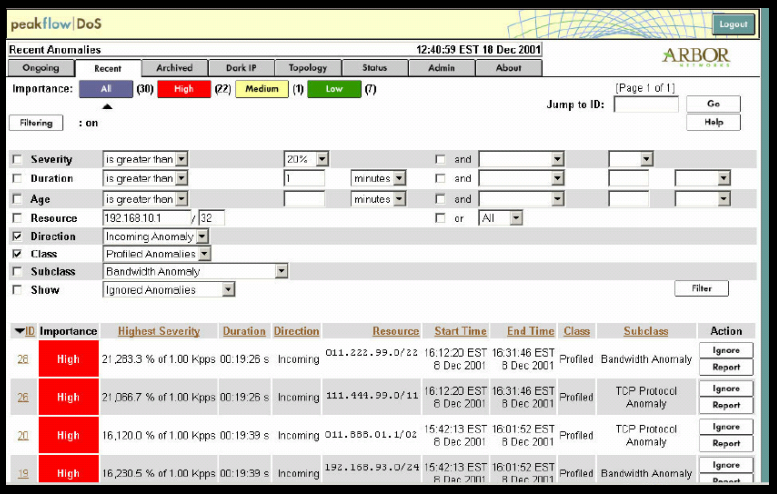
Protocol

Flow info summary

Flow details

How to monitor

- 3rd party analyzer tool (Arbor peakFlow)
  Attack detection/Analysis/Filtering



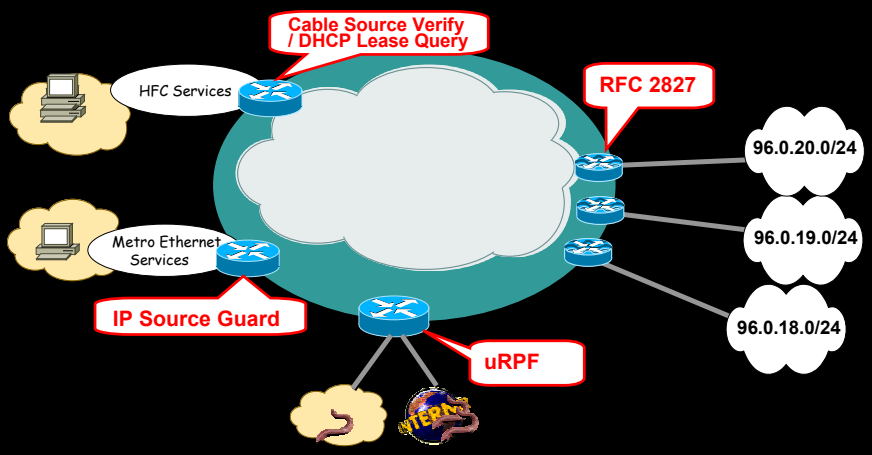
SP Security Solutions

BCP38 Filtering (Source Address Validation)

BCP 38 Ingress Packet Filtering

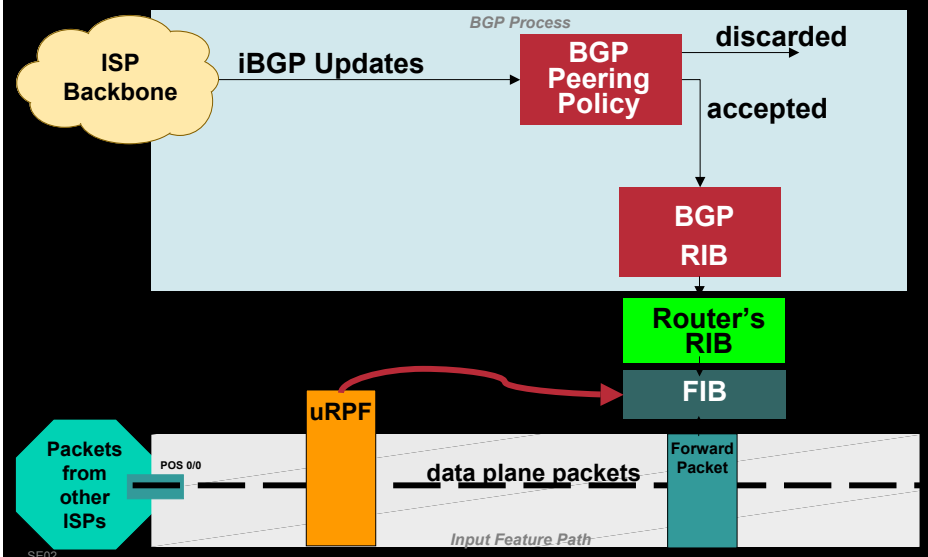
Cisco.com

Defeating Denial of Service Attacks which employ IP Source Address Spoofing



BCP 38 Ingress Packet Filtering (uRPF)

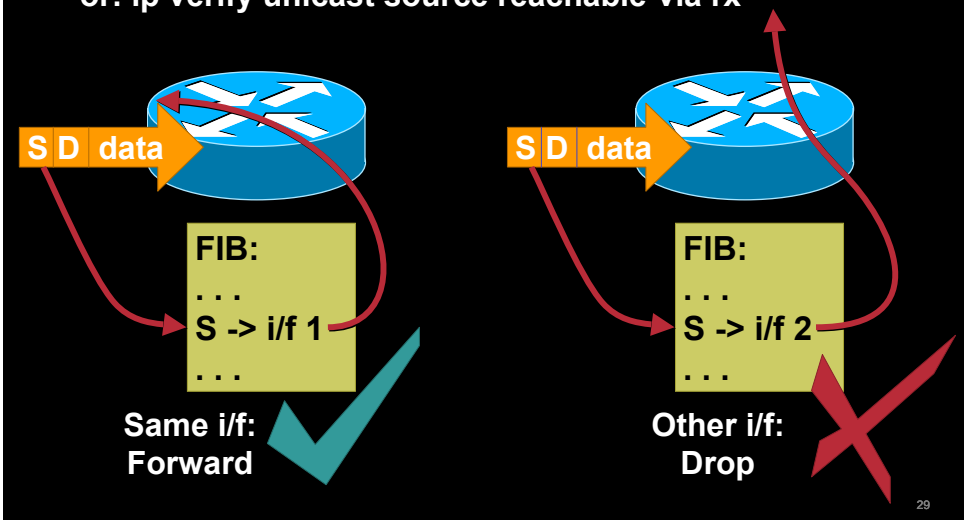
Cisco.com



BCP 38 Ingress Packet Filtering (Strict uRPF)

Cisco.com

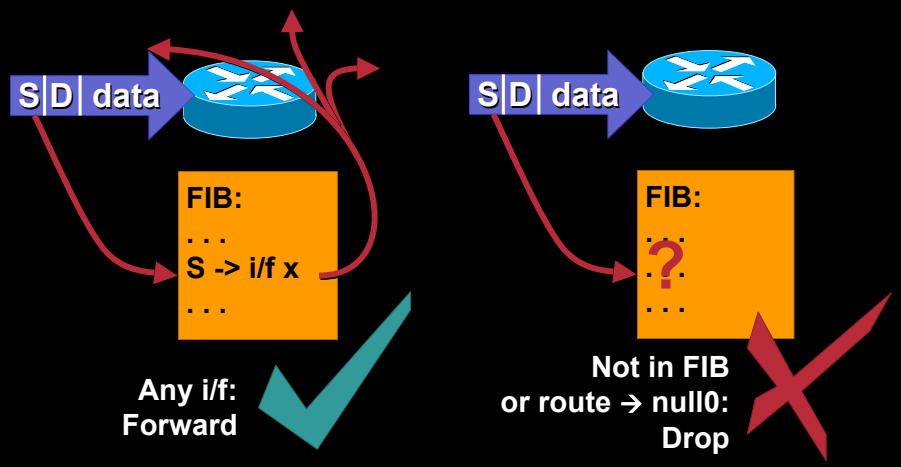
router(config-if)# ip verify unicast reverse-path
or: ip verify unicast source reachable-via rx



BCP 38 Ingress Packet Filtering (Loose uRPF)

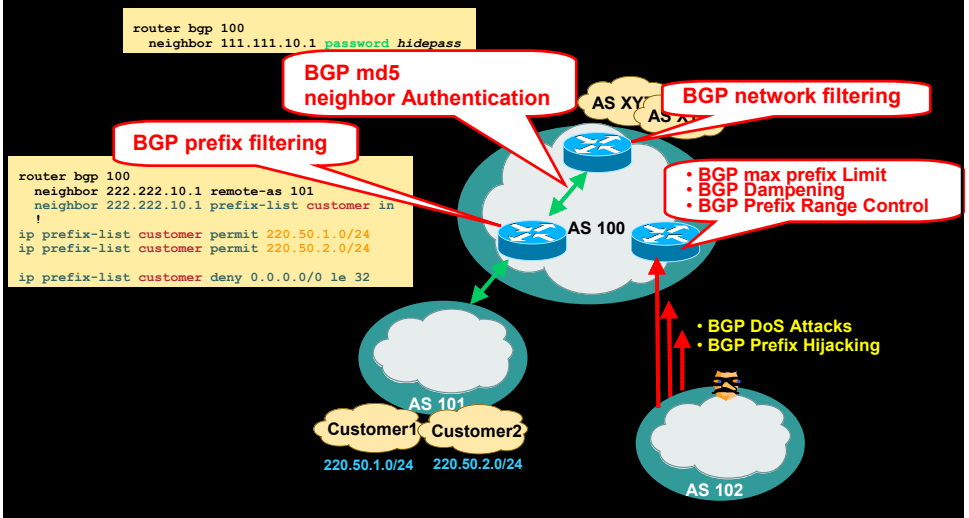
Cisco.com

router(config-if)# ip verify unicast source reachable-via any



SP Security Solutions
BGP Security Solutions

BGP Security Solutions



SP Security Solutions
Infrastructure ACLs

Infrastructure ACLs

- Basic premise: filter traffic destined TO your core routers
- Develop list of required protocols that are sourced from outside your AS and access core routers
  - eBGP, IPSec, GRE
- Identify core address block(s)
  - This is the protected address space
  - Summarization is critical → simpler and shorter ACLs
- Infrastructure ACL will permit only required protocols and deny ALL others to infrastructure space
- ACL should also provide anti-spoof filtering
  - Deny your space from external sources
  - Deny RFC1918 space
  - Deny multicast sources addresses (224/4)
  - RFC3330 defines special use IPv4 addressing

Infrastructure ACLs

- Infrastructure ACL must permit transit traffic
  - Traffic passing through routers must be allowed via permit ip any any
- ACL is applied inbound on ingress interfaces
- Fragments destined to the core can be filtered via fragments keyword
  - Fragments pose a security risk: by default they are not filtered by ACLs

Infrastructure ACLs

Example

```
! Deny our internal space as a source of external packets
access-list 101 deny ip our_CIDR_block any
! Deny src addresses of 0.0.0.0 and 127/8
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
! Deny RFC1918 space from entering AS
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.15.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
! The only protocol that require infrastructure access is eBGP.
WE have defined both src and dst addresses
access-list 101 permit tcp host peerA host peerB eq 179
access-list 101 permit tcp host peerA eq 179 host peerB
! Deny all other access to infrastructure
access-list 101 deny ip any core_CIDR_block
! Permit all data plane traffic
access-list 101 permit ip any any
```

SP Security Solutions
Control Plane Protections

General SP Security Threats

- Excessive traffic destined to GRP can lead to high CPU → DoS
- Receive ACLs filter traffic destined to the GRP via receive adjacencies
- rACLs explicitly permit or deny traffic destined to the GRP
- rACL do NOT affect transit traffic
- Traffic is filtering on the ingress LC, prior to GRP processing
- rACLs enforce security policy by filtering who/what can access the router

Receive ACLs

Cisco.com

- LC CPU handles rACL processing
- Under attack, LC CPU utilization increases
- Impact depends on LC engine type
- rACL always improves resiliency to attack

Control Plane Policing

Cisco.com

- rACLs are great but
  - Only available on GSR/7500
  - Limited granularity—permit/deny only
- Need to protect all platforms
  - To achieve protection today, need to apply ACL to all interfaces
  - Some platform implementation specifics
- Some packets need to be permitted but at limited rate
- CoPP leverages Modular QoS CLI (MQC) for QoS policy definition
- Dedicated control-plane “interface”
  - Single point of application

Control Plane Policing

- CoPP policy is applied to the control-plane itself
  - `Router(config)# control-plane`
  - `Router(config-cp)# service-policy input  control-plane-policy`
- 3 step process:
  - Class-map

    Setup class of traffic
  - Policy-map

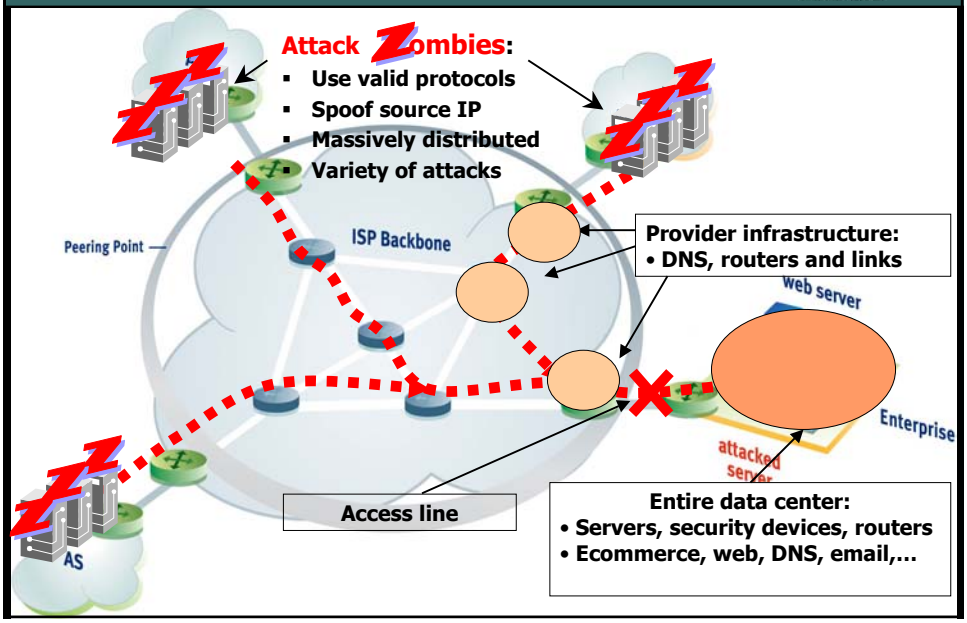
    Define the actual QoS policy: rate limiting and actions
  - Apply CoPP policy to control plane “interface”

De-worming Tools

Cisco Guard/ Traffic anomaly Detector

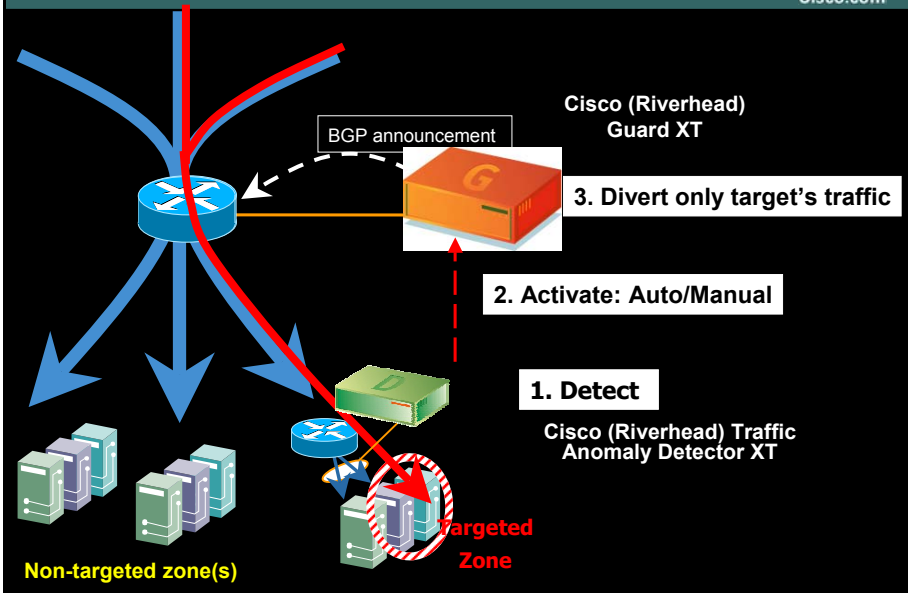
DDoS Vulnerabilities
Multiple Threats and Targets

Cisco.com



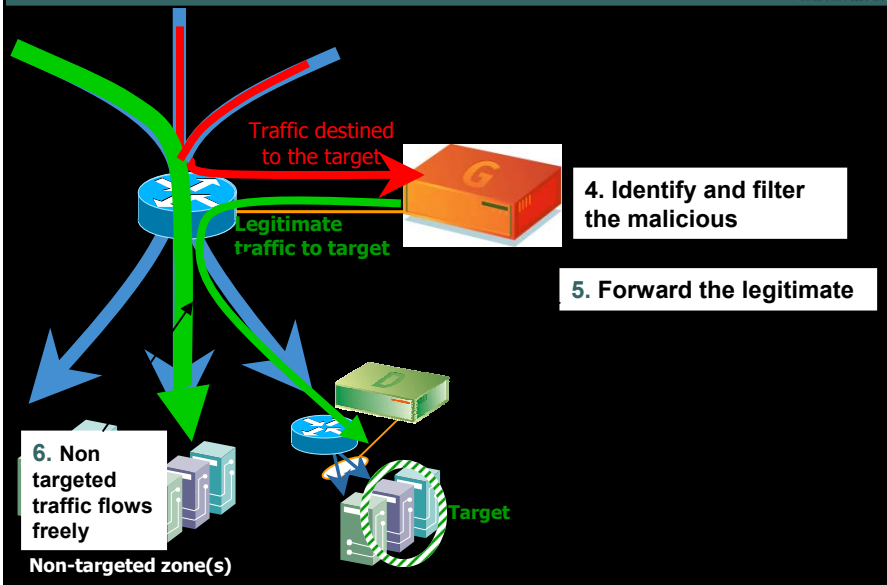
Dynamic Diversion Architecture

Cisco.com



Dynamic Diversion Architecture

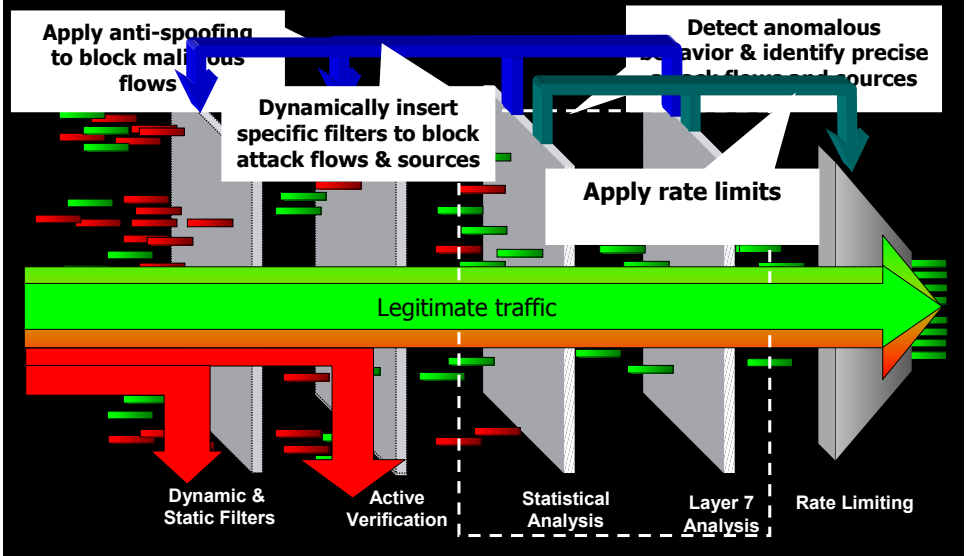
Cisco.com



Multi-Verification Process (MVP)

Integrated Defenses in the Guard XT

Cisco.com



Current Product Suite

Cisco.com

Cisco Guard XT 5650

Cisco Traffic Anomaly Detector XT 5600

Common Features
- Two Gigabit interfaces – MMF or GE-TX
- Two management interfaces
- Dual Xeon control plane, Broadcom
- Sibyte data plane
- Redundant power, RAID 1 dual drives

Attack *analysis & mitigation*

Diverts traffic flows for *on-demand scrubbing*

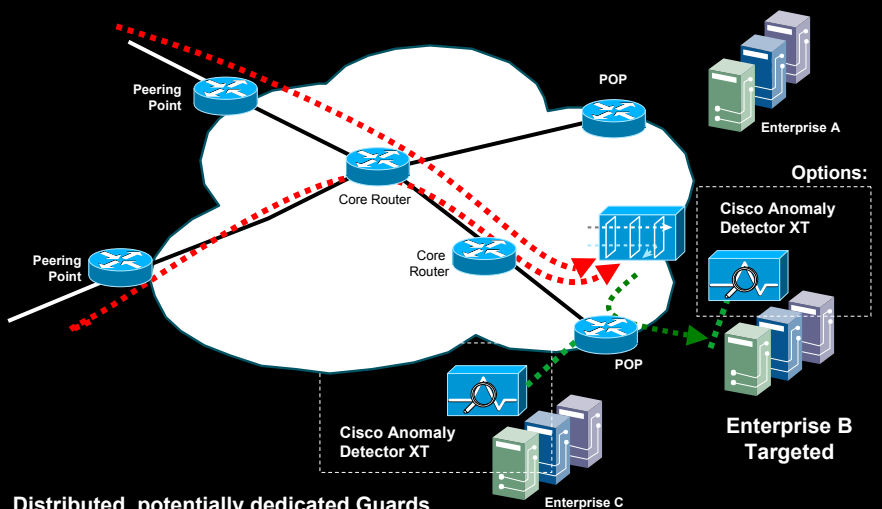
Attack *detection* to support on-demand, shared scrubbing

Monitors *copy of traffic*

Guard / Detector SP Versions
- dual SMF interfaces
- DC power and NEBS server

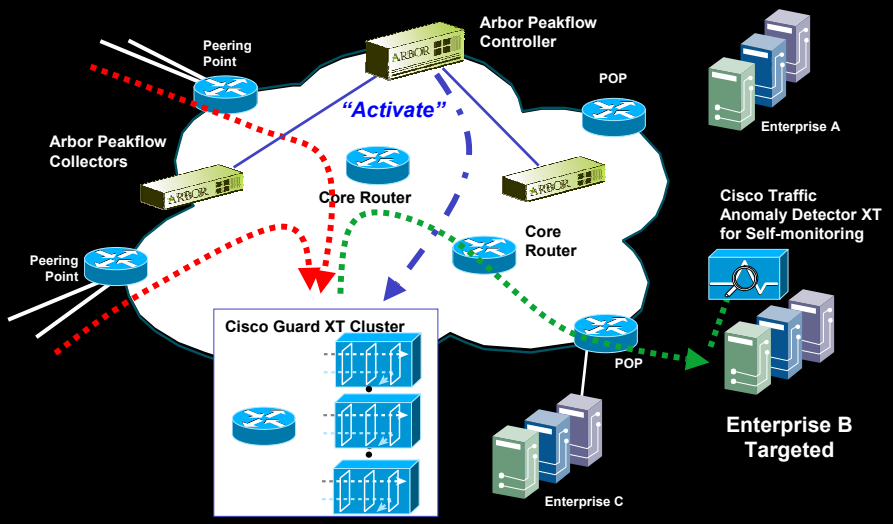
Service Provider Distributed Protection

Cisco.com



Distributed, potentially dedicated Guards
Detector CPE for monitoring and potentially activation
Potentially Detector at SP for monitoring, or Netflow…

Service Provider Centralized Protection

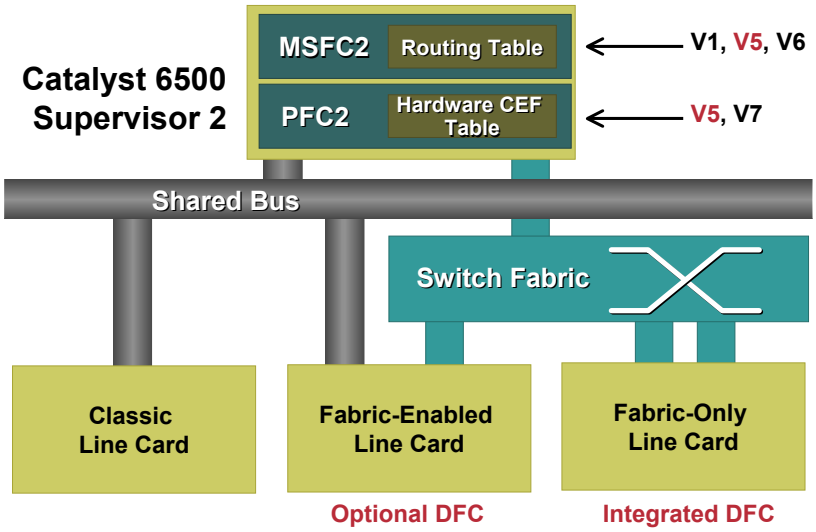


Illustrating interoperability with third party monitoring, such as Arbor Networks or in-house Netflow based system

De-worming Tools

Netflow / Anomaly Detection Tool / RMON

NetFlow (NetFlow Architecture)



NetFlow (functional sequence)

1. Create and update flows in NetFlow Cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	SrcPort	SrcMsk	SrcAS	DstPort	DstMsk	DstAS	NextHop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Expiration

- **Inactive timer** expired (15 sec is default)
- **Active timer** expired (30 min (1800 sec) is default)
- NetFlow **cache is full** (oldest flows are expired)

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	SrcPort	SrcMsk	SrcAS	DstPort	DstMsk	DstAS	NextHop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Aggregation?

No

Yes

e.g. Protocol-Port Aggregation Scheme becomes

Protocol	Pkts	SrcPort	DstPort	Bytes/Pkt
11	11000	00A2	00A2	1528

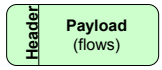
4. Export Version

Non-Aggregated Flows – export **Version 5 or 9**

Aggregated Flows – export **Version 8 or 9**

5. Transport Protocol

Export Packet

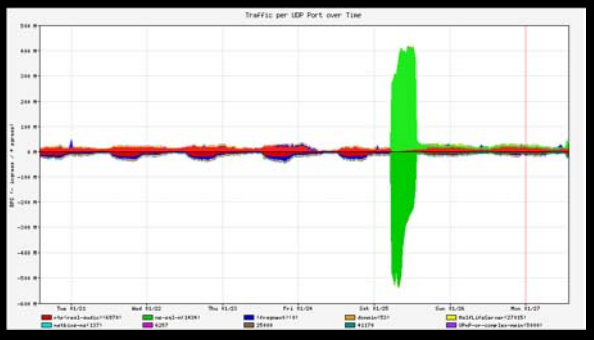


NetFlow (Versions)

NetFlow Version	Comments
1	Original
5	Standard and most common
7	Specific to Cisco Catalyst 6500 and 7600 Series Switches Similar to Version 5, but does not include AS, interface, TCP Flag & TOS information
8	Choice of eleven aggregation schemes Reduces resource usage
9	Flexible, extensible file export format to enable easier support of additional fields & technologies; coming out now are MPLS, Multicast, & BGP Next-Hop

Netflow (Detect DoS Anomaly traffic)

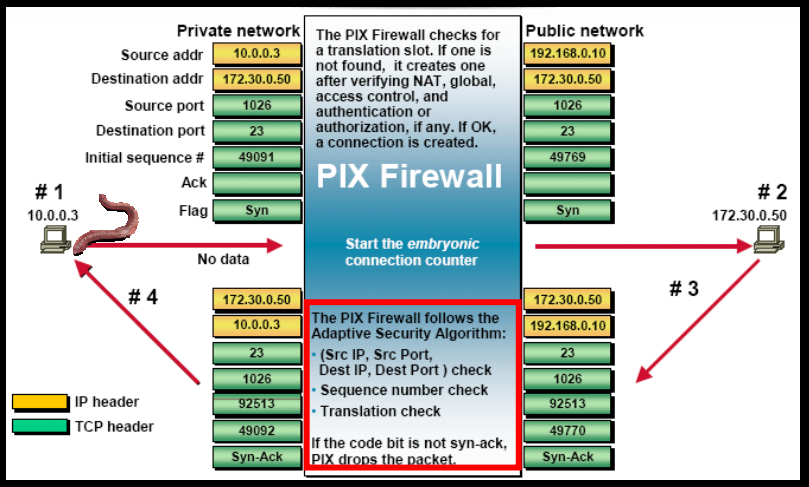
- **An event or condition in the network that is identified as a statistical abnormality when compared to typical traffic patterns gleaned from previously collected profiles and baselines.**



De-worming Tools
Firewall

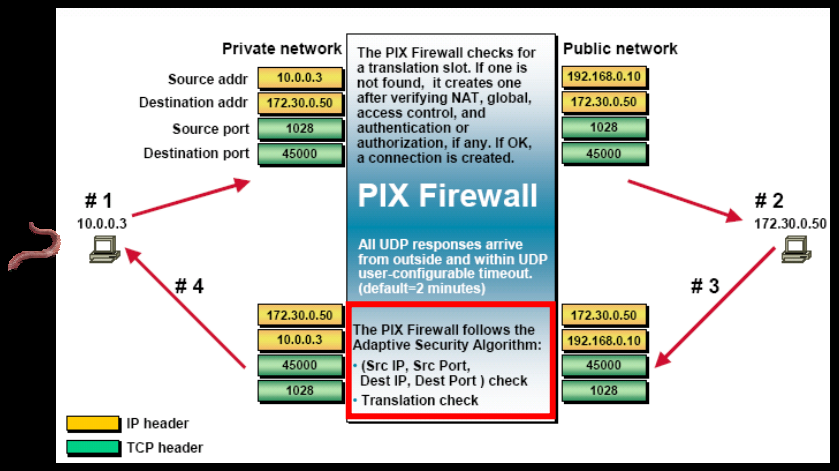
Firewall (Cisco Firewall)

ASA (Adaptive Security Algorithm): De-Worming TCP based attacks

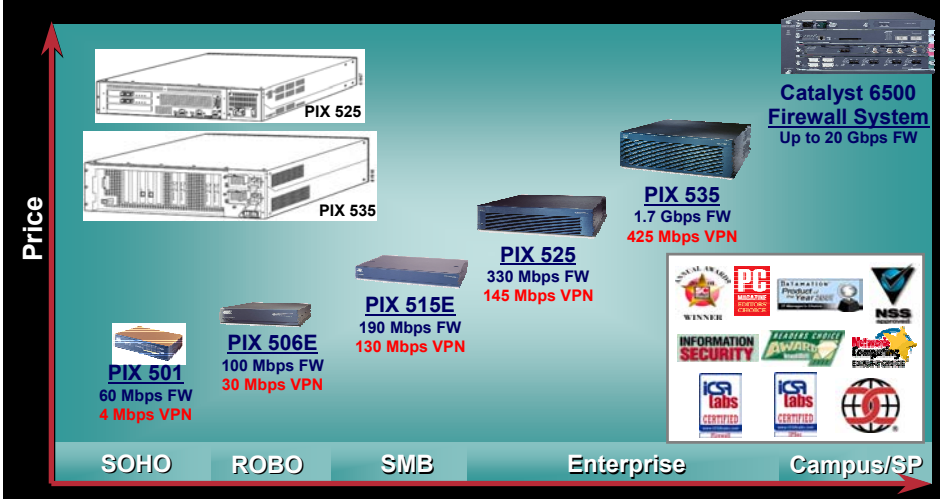


Firewall (Cisco Firewall)

ASA (Adaptive Security Algorithm): De-Worming UDP based attacks



Cisco Firewall Product



* ROBO : Remote Office Branch Office

De-worming Tools
Network IDS/IPS

Network IDS

Detect Exploits

Activity indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking

Detect DoS

Activity indicative of someone attempting to consume bandwidth or computing resources to disrupt normal operations, such as Trinoo, TFN, and SYN floolds

Detect Reconnaissance

Activity indicative of someone probing or mapping the network to identify “targets of opportunity,” such as ping sweeps and port sweeps - usually a precursor to an actual exploit attempt

Detect Misuse

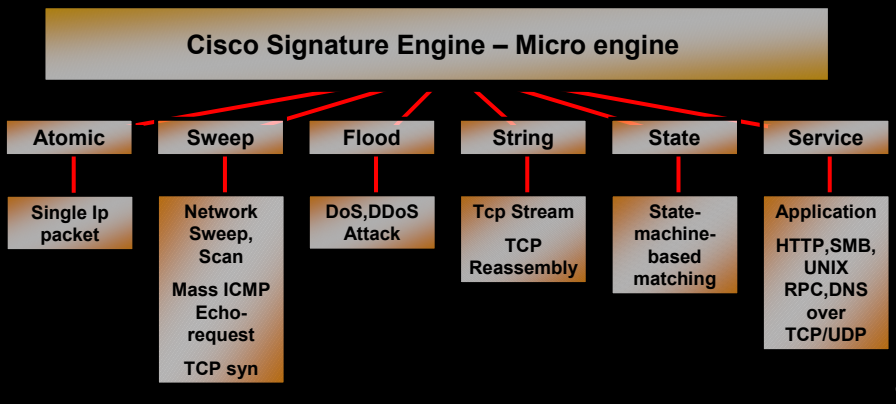
Activity indicative of someone attempting to violate corporate policy. This can be detected by configuring the sensor to look for a custom Text strings in the network traffic

Network IDS

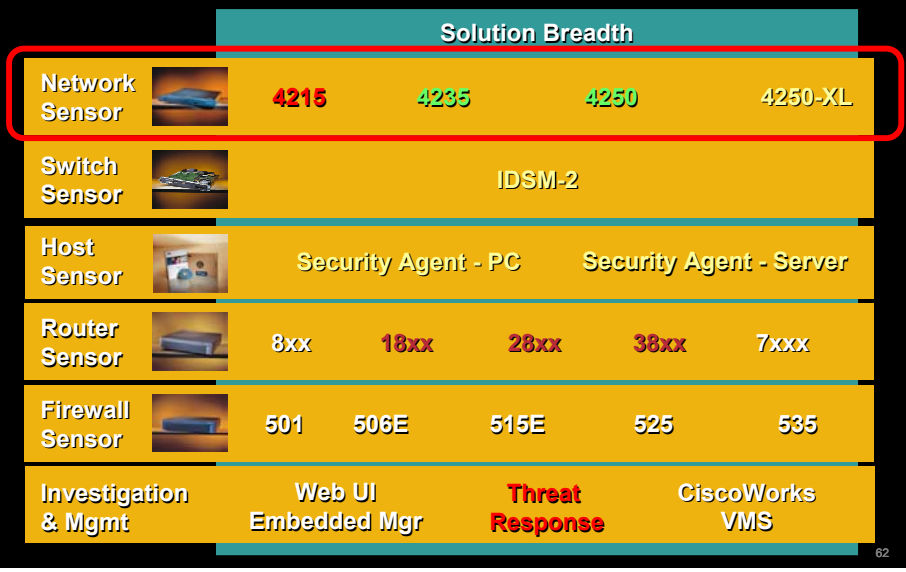
Prevention methods

- tcp reset (to the attack system)
- Provisioning filtering rules to Active system (ex. provision acl rules to Cisco routers)

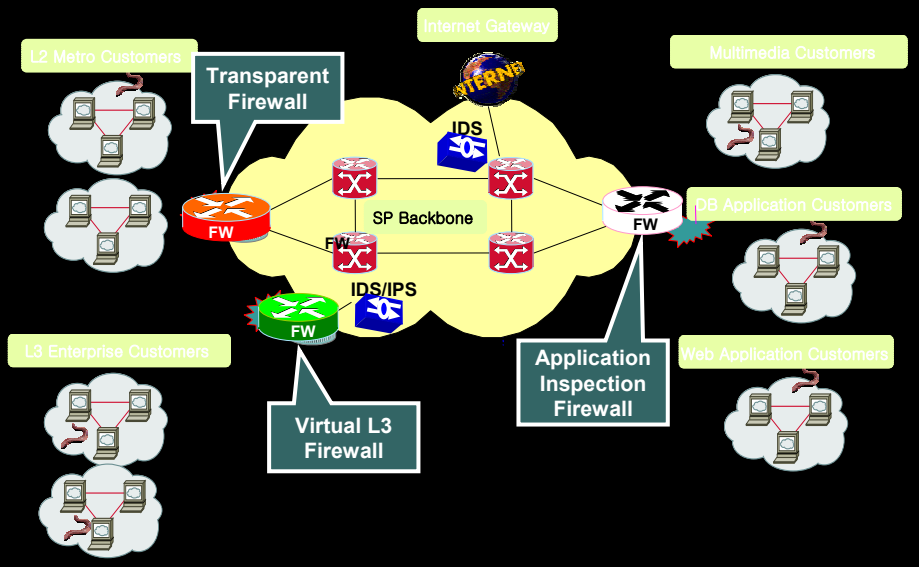
Cisco NIDS Engine



Cisco IDS/IPS



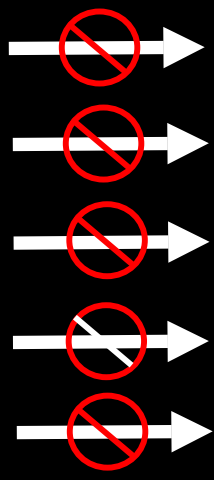
How to apply Firewall & IDS in SP

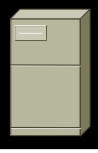


De-worming Tools
Host IDS/IPS

CSA (Cisco Security Agent)

- **Probe** phase
  - Ping scans
  - Port scans
- **Penetrate** phase
  - Transfer exploit code to target
- **Persist** phase
  - Install new code
  - Modify configuration
- **Propagate** phase
  - Attack other targets
- **Paralyze** phase
  - Erase files
  - Crash system
  - Steal data

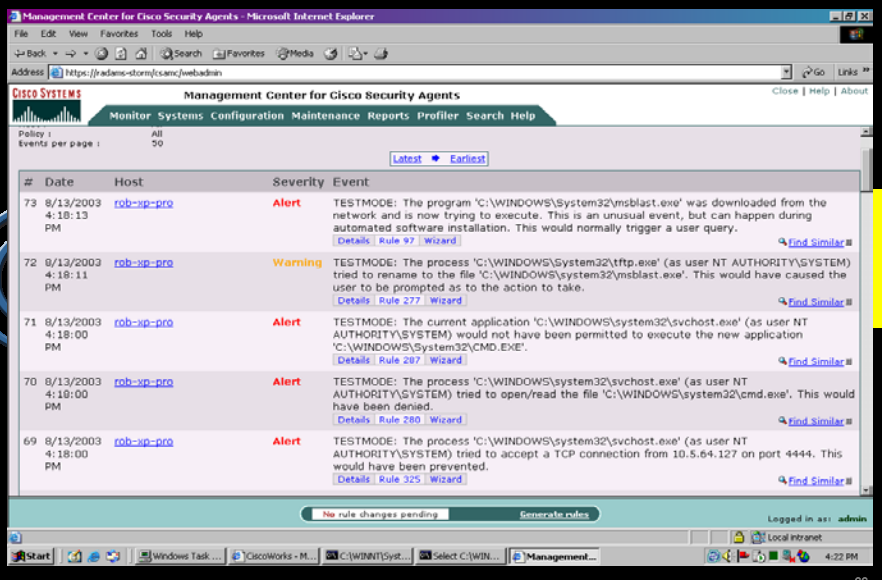




Server protected by CSA

- File system interceptor
- Network interceptor
- Configuration interceptor
- Execution space interceptor

CSA in Action: Protection Against Blaster



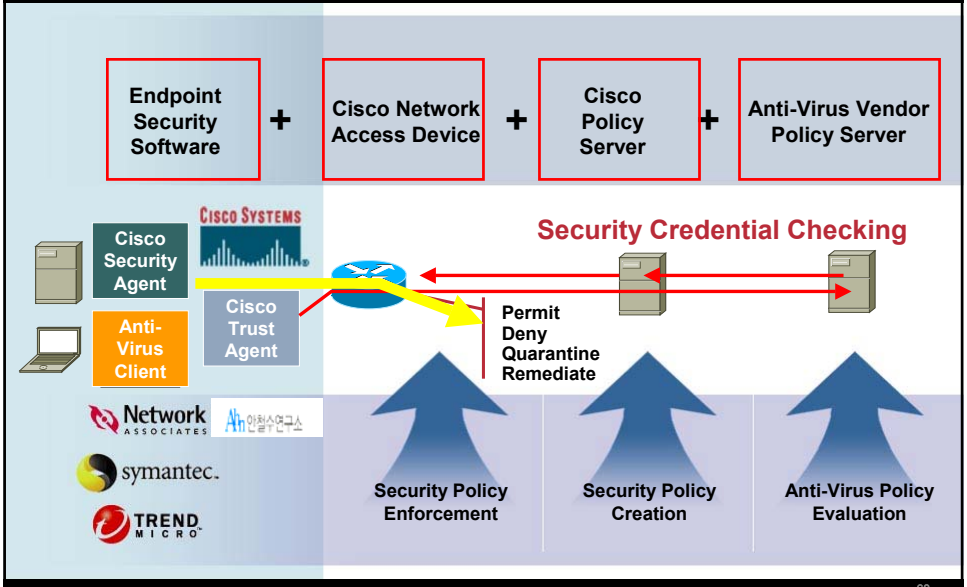
CSA DayZero ScoreCard

CSA successfully blocked the following known attacks with a default installation

- Partial List -

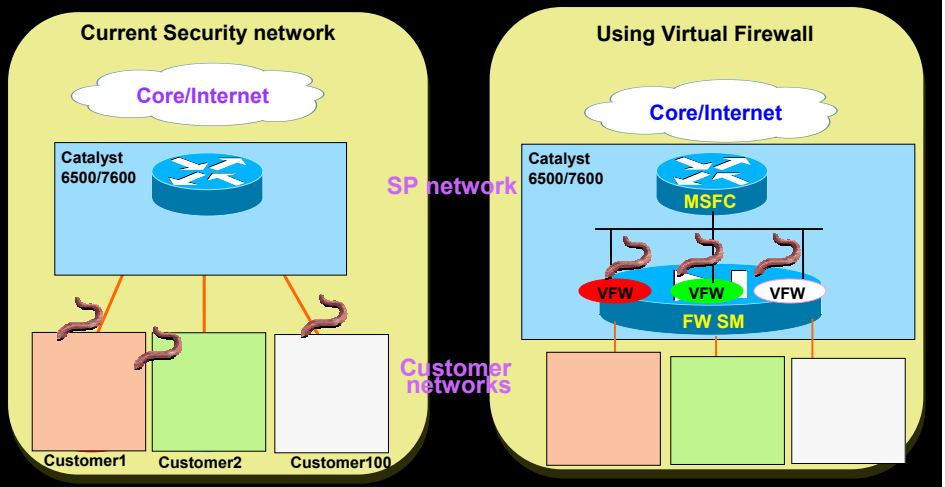
- Mydoom
- W32.Blaster
- Fizzer
- Bugbear
- Sobig.E
- SQL Slammer
- Sircam.A
- WebDav Vulnerability
- Code Red
- Nimda

Network Admission Control



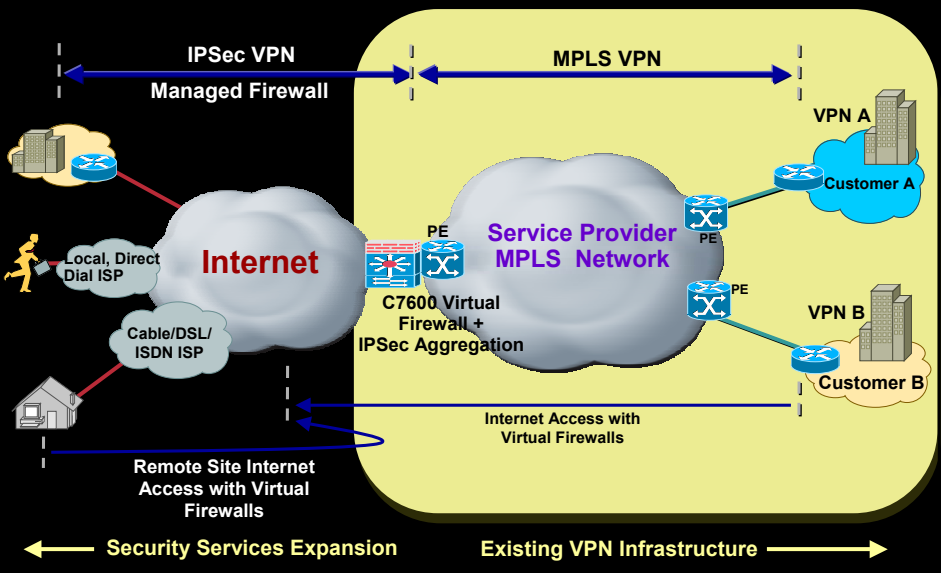
SP Managed Security

Managed Firewall



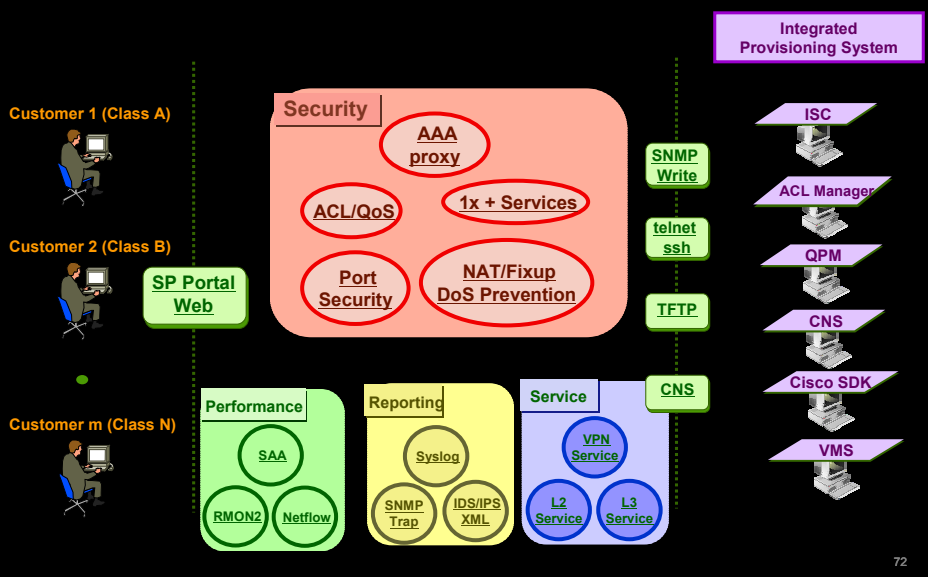
Managed VPN service

Cisco.com

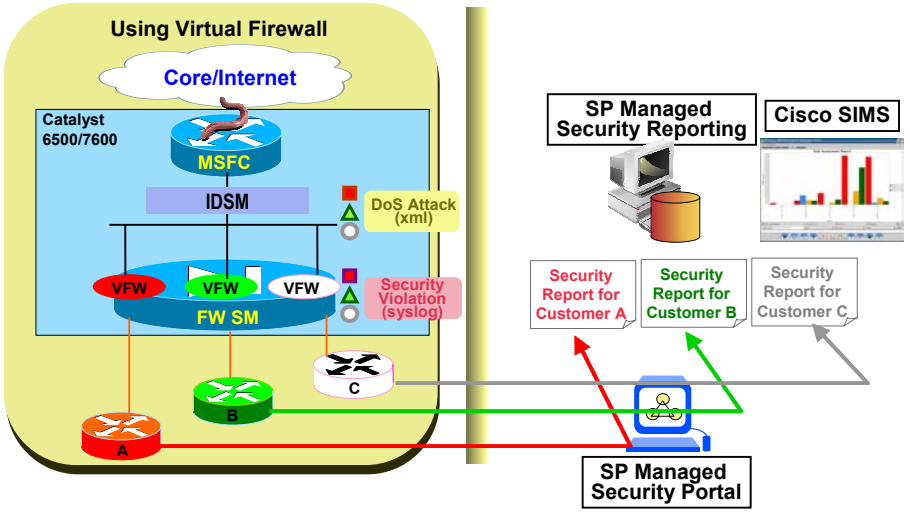


Managed Security Provisioning & Management

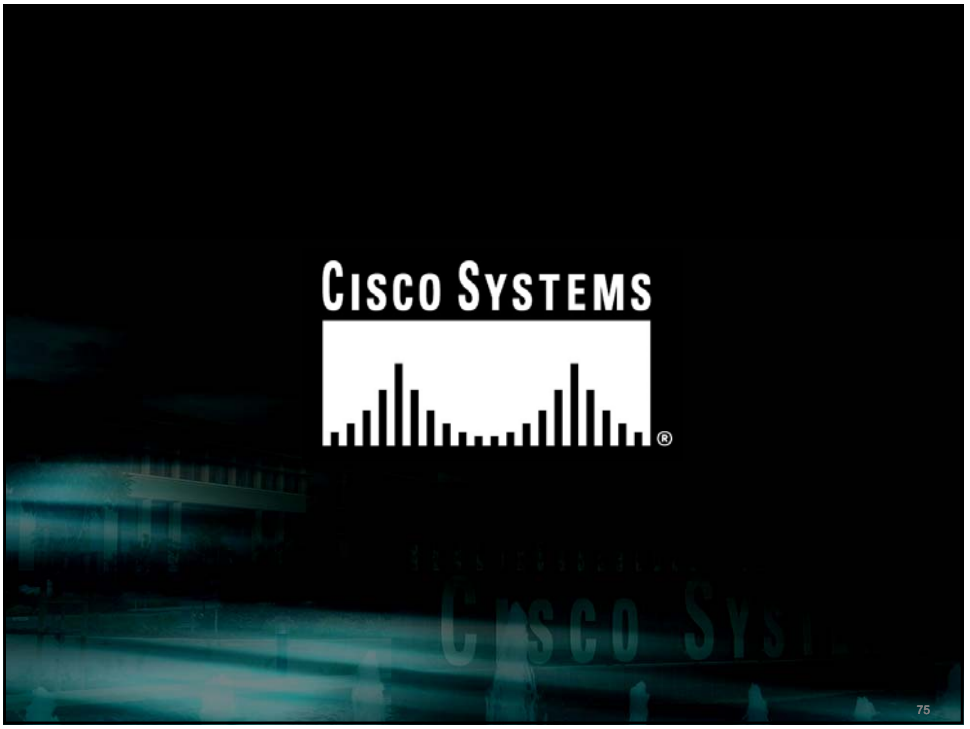
Cisco.com



Managed Security Report



Q and A


CISCO SYSTEMS