

SP Security

2004년 10월 20일

Cisco Systems Korea
성일용(iyseong@cisco.com)

1

Agenda

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

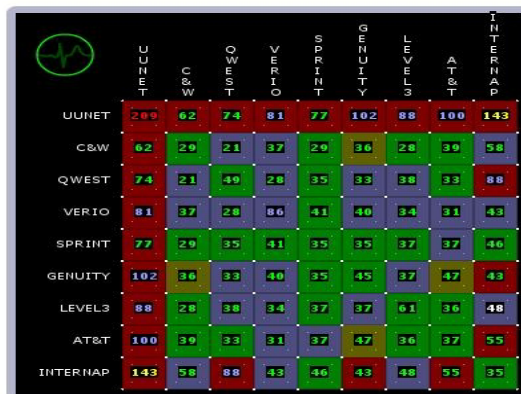
2

SP Security Threats



The Internet Health Report (Last Hour)

About this site:



LAST DAY

Generated Sat Jan 25 08:02:53 2003 GMT



Healthy < 80ms Latency.



Severe < 180ms Latency.



Stable < 120ms 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!

Cisco.com

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

인터넷대란 후유증 심각

1.25 인터넷 대란이 진정국면으로 접어들었으나 책임소재 규명과 보상 등의 문제가 쉽게 풀리지 않을 조짐이어서 적지 않은 후유증을 예고하고 있다.

29일 정보통신부는 아직 일부 망에서 네트워크 트래픽이 평소보다 많이 발생하고는 있지만 망에 영향을 미칠 정도는 아니라며 사실상 상황종료를 밝혔다. 그러나 근본적인 책임이 어디에 있는지를 가리고 이를 통해 집단적으로 보상을 요구하는 움직임이 구체화되고 있는 등 책임규명과 보상문제가 후폭풍으로 등장했다.

PC방 업체를 비롯한 인터넷쇼핑몰 온라인게임업체 등 관련 업체들은 이번 인터넷 대란으로 매출격감 등 수백억원의 피해를 입었다고 주장, 집단소송을 준비하고 있다. 한국인터넷PC문화협회의 경우 전국 2만5000여 인터넷PC방에서 약 225억원의 금전적 피해를 입은 것으로 추정하고, 이날 4대 인터넷서비스사업자(ISP)에 보상과 관련한 공문을 발송했다.

<http://www.ispnews.co.kr/cgi-bin/ispnews/printnews.cgi?newsid1011696274,91619>

인터넷 대란 '비상'

국가의 신경망인 유무선 인터넷 접속이 9시간 가량이나 한꺼번에 중단되는 사상초유의 인터넷 대란이 한국을 비롯한 전세계에서 동시에 발생, 인터넷 보안에 비상이 걸렸다.

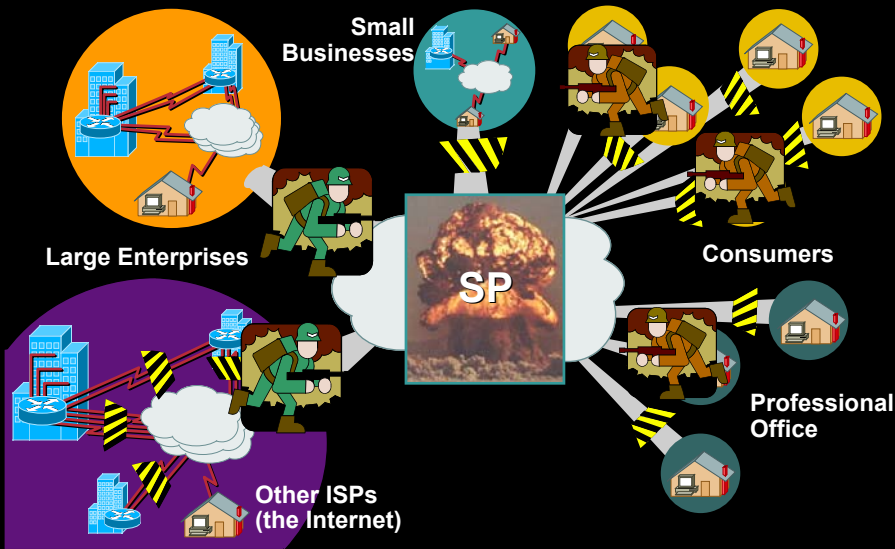
신종 웹 바이러스에 의한 이번 인터넷 접속 중단 사태로 한국은 세계 IT강국이라는 이름과는 달리 네티즌에 의해 매혹이 발생하는 PC방, 인터넷 쇼핑몰, 온라인 게임업체 등을 중심으로 많은 피해를 입은 것으로 추정돼 인터넷 보안은 후진국 수준이라는 지적을 받고 있다.

그동안 특정 인터넷 사이트에서 해킹이나 대량 접속, 바이러스로 인한 접속장애 등의 사고가 일어난 적은 있었으나 이번처럼 국내 인터넷이 전면적으로 중단된 것은 처음 있는 일이다.

이같은 사태는 우리나라뿐만 아니라 미주와 유럽 및 아시아 등 세계 전역에서 계속 발생했으며 아직 피해규모에 대한 정확한 집계는 이뤄지지 않았다. 하지만 PC방, 인터넷 쇼핑몰, 온라인 게임업체 등을 중심으로 많은 피해가 발생한 것으로 추정된다.

SP's Are Today's New Battle Grounds

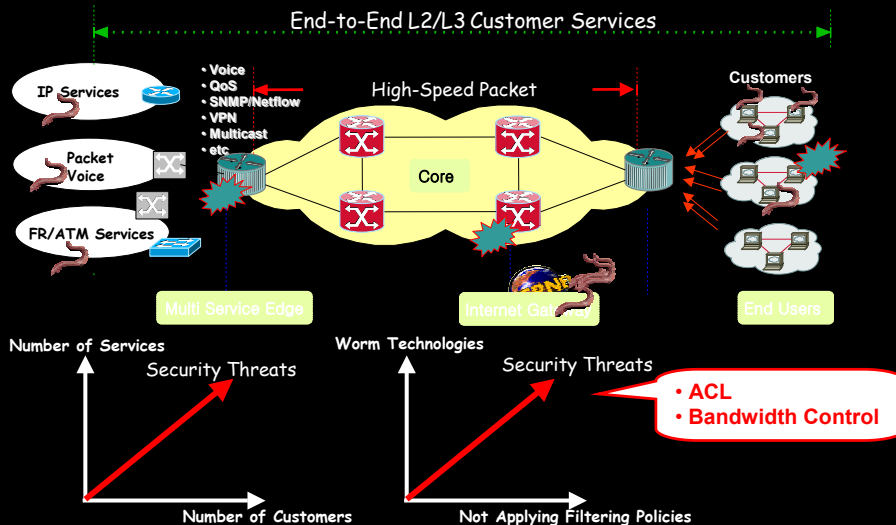
Cisco.com



7

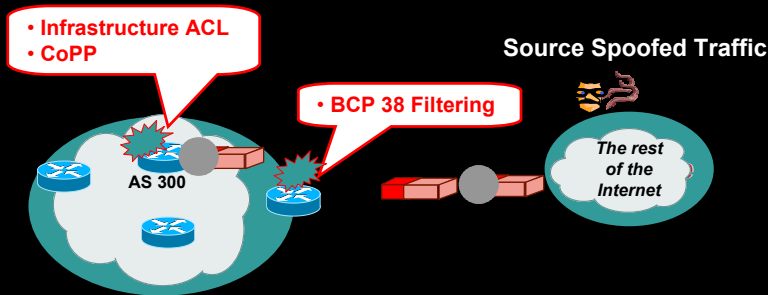
General SP Security Threats

Cisco.com



8

General SP Security Threats

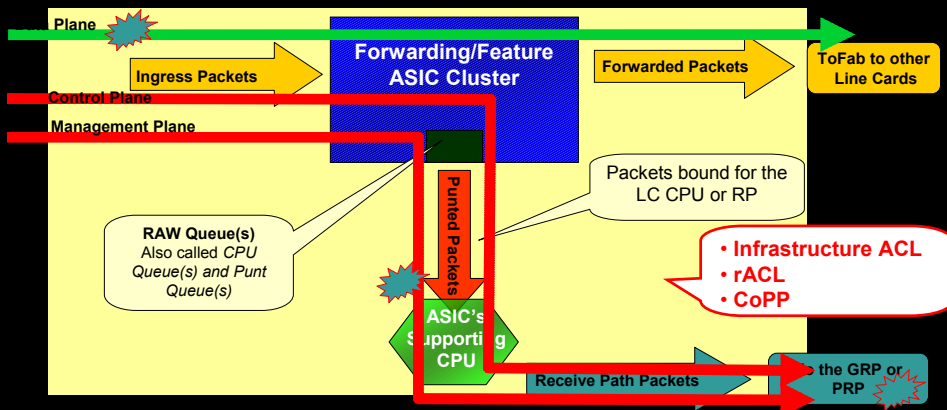


Most of the source spoofed traffics are for

- 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

9

General SP Security Threats

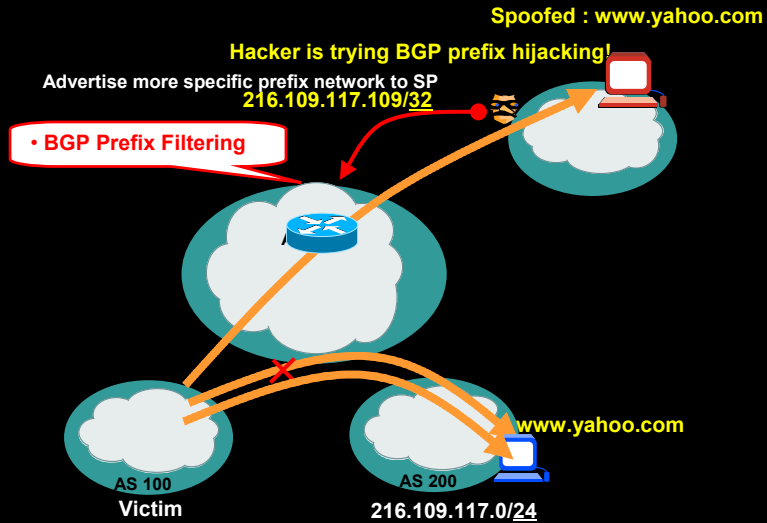


- **Bandwidth Saturation (Data plane)**
- **Target the Control or Management Plane (Receive Path traffic on the Control and Management Plane)**
- **Saturate the Punt path out of the forwarding/feature ASIC by abusing the TCP/IP standards (Data plane traffic that is punted from the forwarding/feature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

10

General SP Security Threats

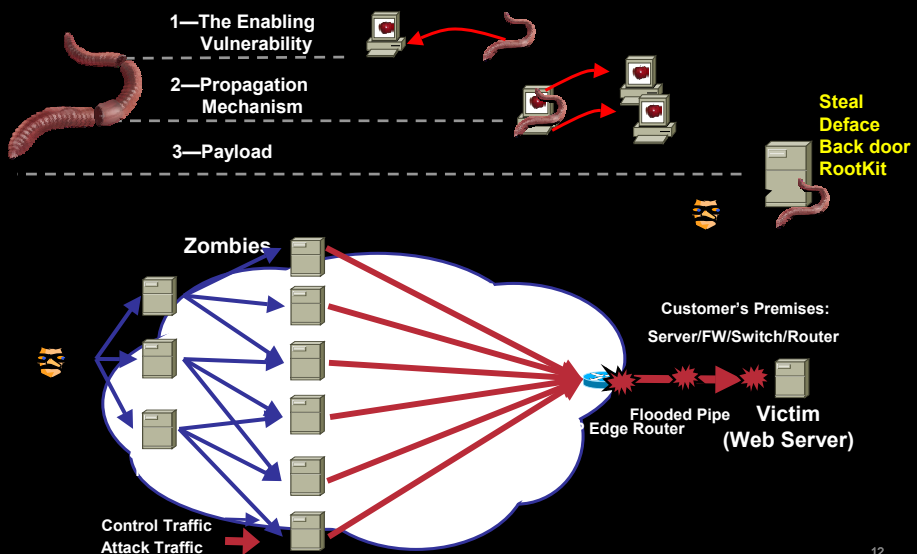
Cisco.com



11

Internet Worm Threats

Cisco.com



12

Internet Worm Threats (BOTNET)

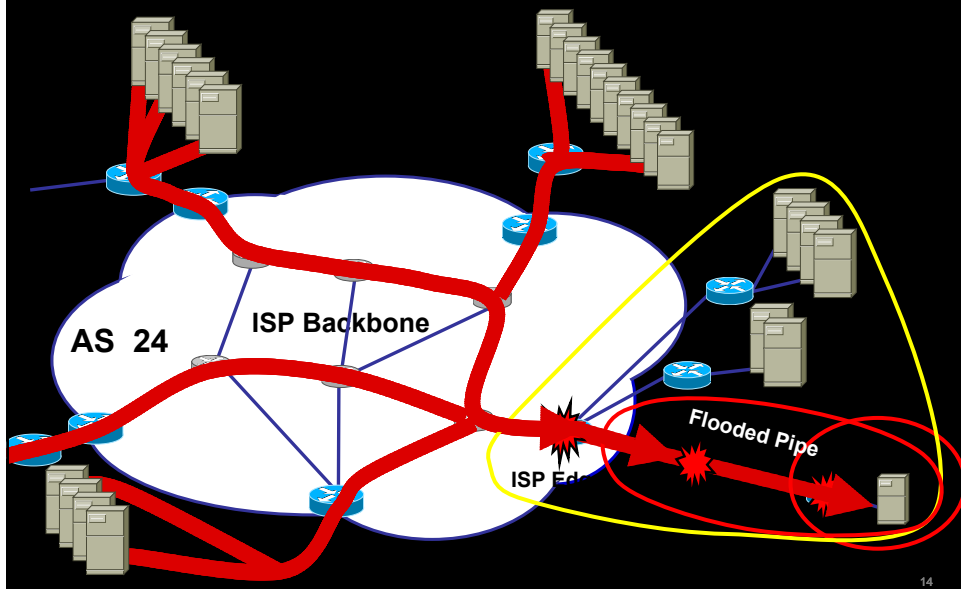
Cisco.com

- **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

13

Internet Worm Threats (DDoS)

Cisco.com

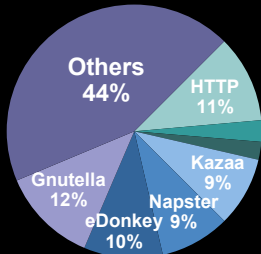


14

P2P Security Threats

Cisco.com

**JULY 2002 IN A
LARGE EUROPEAN ISP**



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

15

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

16

P2P Security Threats

Cisco.com

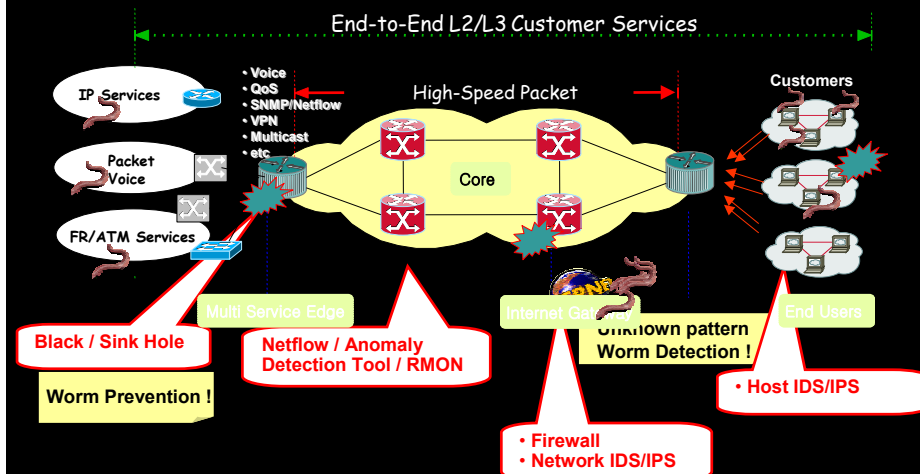
- The 'push' operations could be diverted to launch DoS attack on a victim even behind a firewall
- Registering victims as peers will force other peers to try to connect
- Kazaa (and perhaps others) can use the P2P network in order to automatically install the next version, this mechanism could be used 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

17

How to defense from SP Security Threats

Cisco.com



18

SP Security Solutions

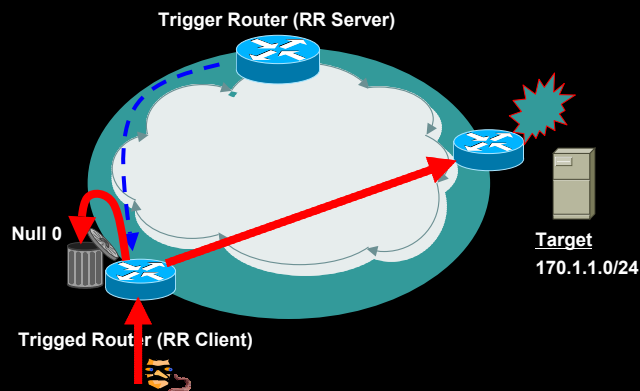
Black Hole / Sink Hole



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

Cisco.com

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
```

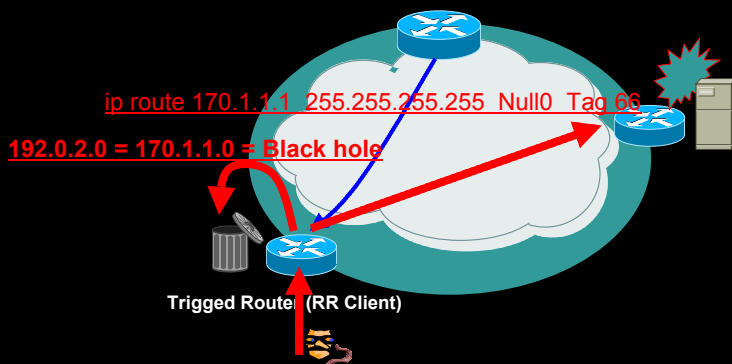
21

Black Hole

Cisco.com

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

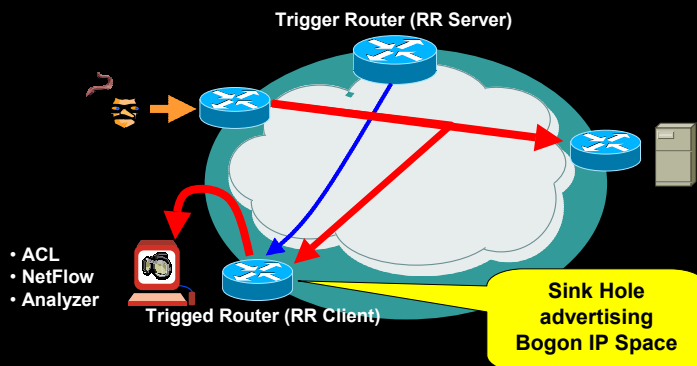


22

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



23

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
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 aged 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	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active (Sec) /Flow	Idle (Sec) /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
Eto/0	132.122.25.60	Se0/0	192.168.1.1	06	9AEE	0007	1
Eto/0	139.57.220.28	Se0/0	192.168.1.1	06	708D	0007	1
Eto/0	165.172.153.65	Se0/0	192.168.1.1	06	CB46	0007	1

Flow details

24

How to monitor

Cisco.com

- 3rd party analyzer tool (Arbor peakFlow)

Attack detection/Analysis/Filtering

The screenshot displays the Arbor peakFlow DoS web interface. At the top, it shows the title 'peakflow DoS' and a 'Logout' button. Below this is a navigation bar with tabs: 'Recent Anomalies', 'Archived', 'Dark IP', 'Topology', 'Status', 'Admin', and 'About'. The current date and time are '12:40:59 EST 10 Dec 2001'. The 'Importance' section shows a distribution: All (30), High (22), Medium (1), and Low (7). A 'Filtering' section is on the left with various criteria like Severity, Duration, Age, Resource, Direction, Class, Subclass, and Show. A table of recent anomalies is shown below, with columns for ID, Importance, Highest Severity, Duration, Direction, Resource, Start Time, End Time, Class, Subclass, and Action. The table lists four anomalies, all marked as 'High' severity.

ID	Importance	Highest Severity	Duration	Direction	Resource	Start Time	End Time	Class	Subclass	Action
28	High	21,283.3 % of 1.00 Kpps	00:19:26 s	Incoming	011.222.99.0/22	16:12:20 EST 8 Dec 2001	16:31:46 EST 9 Dec 2001	Profiled	Bandwidth Anomaly	Ignore Report
28	High	21,066.7 % of 1.00 Kpps	00:19:26 s	Incoming	111.444.99.0/11	16:12:20 EST 8 Dec 2001	16:31:46 EST 9 Dec 2001	Profiled	TCP Protocol Anomaly	Ignore Report
20	High	16,120.0 % of 1.00 Kpps	00:19:39 s	Incoming	011.555.01.1/02	15:42:13 EST 8 Dec 2001	16:01:52 EST 8 Dec 2001	Profiled	TCP Protocol Anomaly	Ignore Report
19	High	16,230.5 % of 1.00 Kpps	00:19:39 s	Incoming	192.168.93.0/24	15:42:13 EST 8 Dec 2001	16:01:52 EST 8 Dec 2001	Profiled	Bandwidth Anomaly	Ignore Report

25

Cisco.com

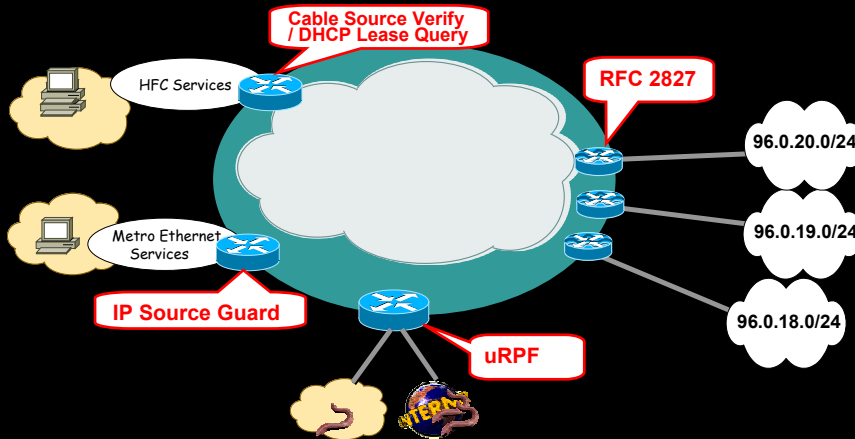
SP Security Solutions BCP38 Filtering (Source Address Validation)



BCP 38 Ingress Packet Filtering

Cisco.com

Defeating Denial of Service Attacks which employ IP Source Address Spoofing



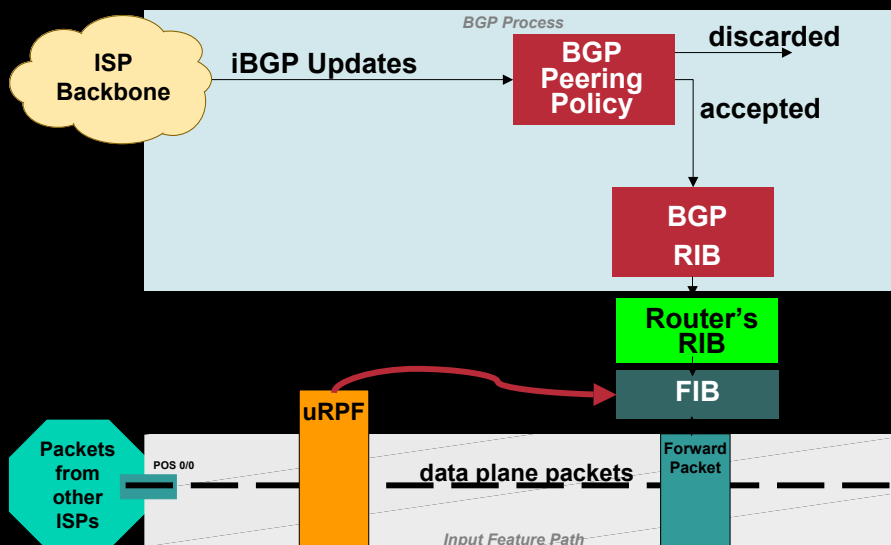
SE02
10118_08_2004_c1

© 2004 Cisco Systems, Inc. All rights reserved.

27

BCP 38 Ingress Packet Filtering (uRPF)

Cisco.com



SE02
10118_08_2004_c1

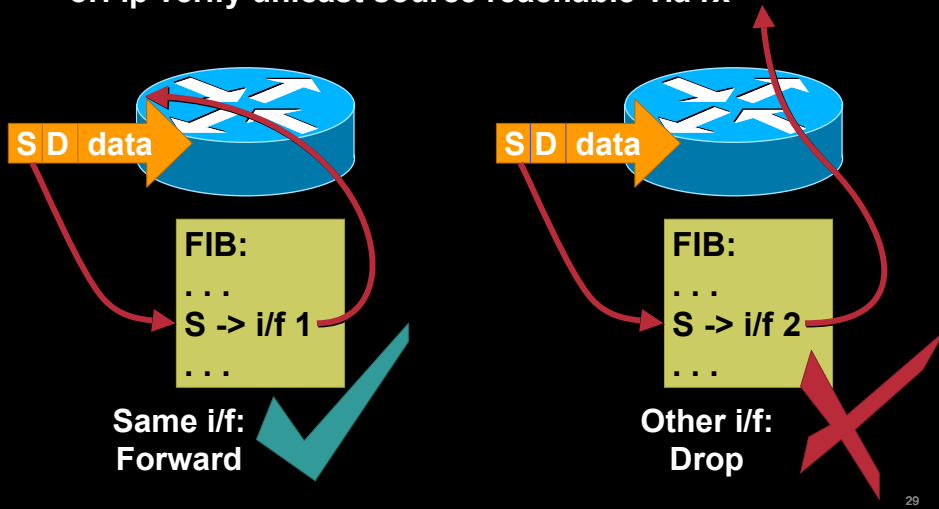
© 2004 Cisco Systems, Inc. All rights reserved.

28

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

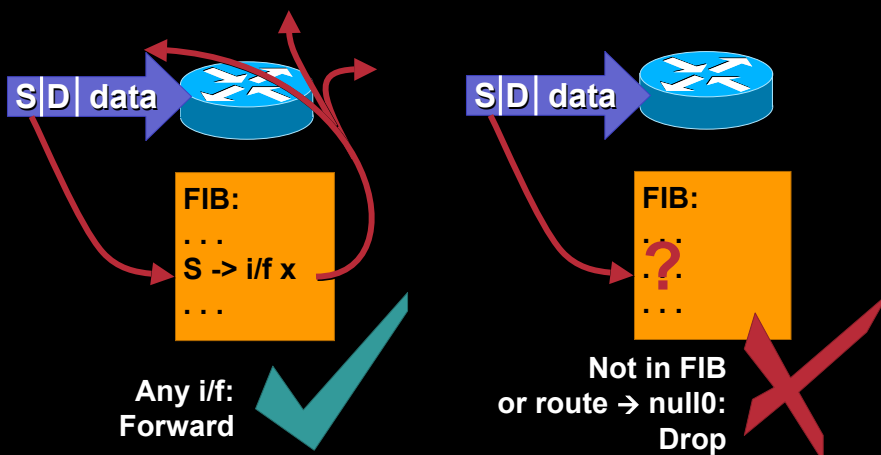


29

BCP 38 Ingress Packet Filtering (Loose uRPF)

Cisco.com

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



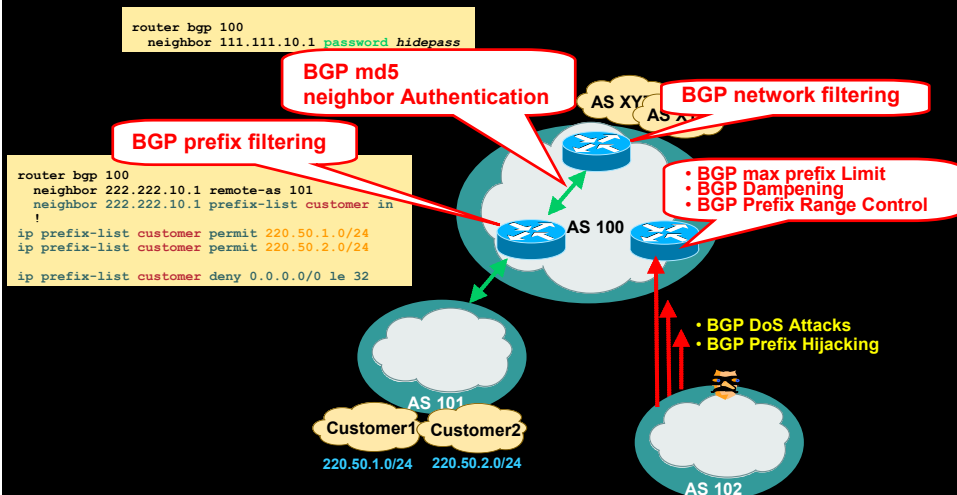
30

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

Cisco.com

- **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

35

Infrastructure ACLs

Cisco.com

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
```

36

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**

39

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**

40

- **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”**

41

De-worming Tools

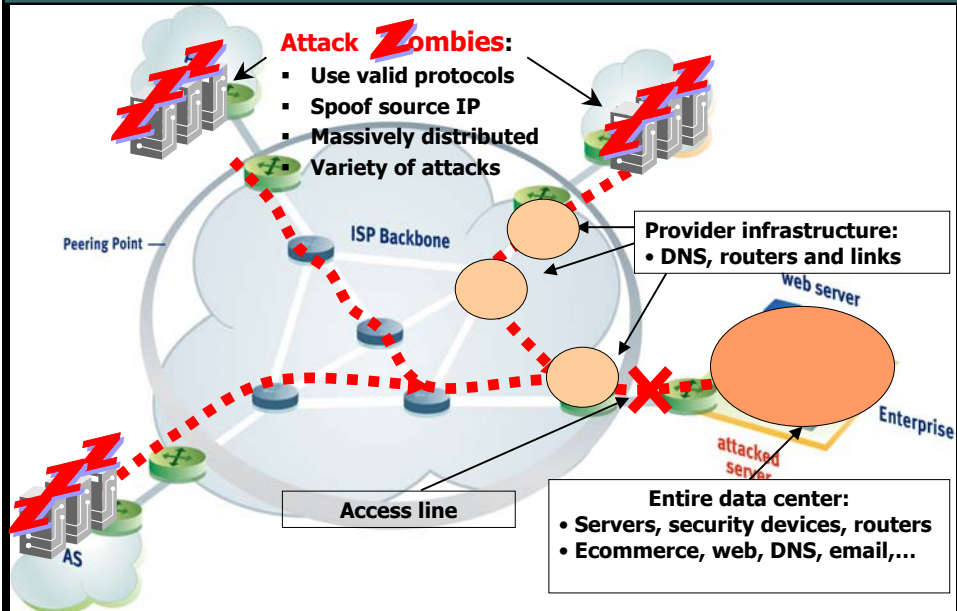
Cisco Guard/ Traffic anomaly Detector



DDoS Vulnerabilities

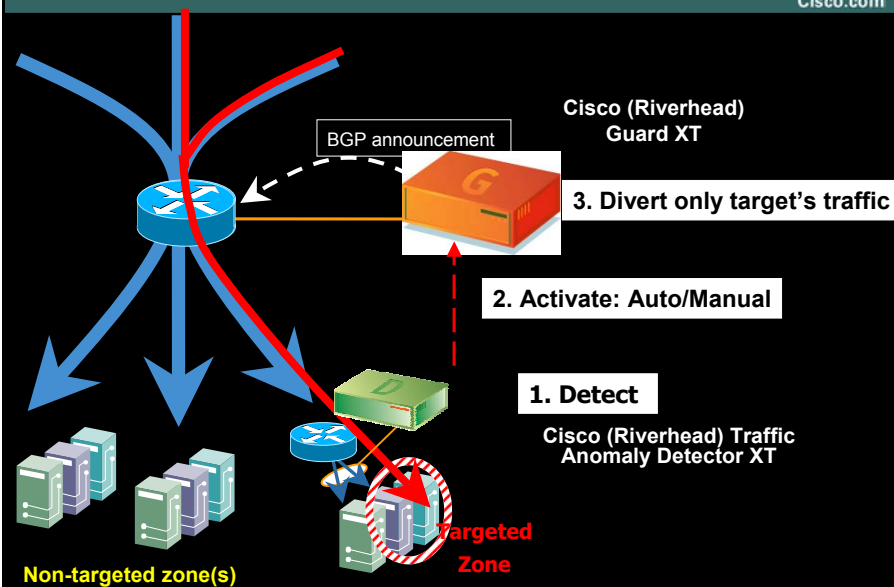
Multiple Threats and Targets

Cisco.com



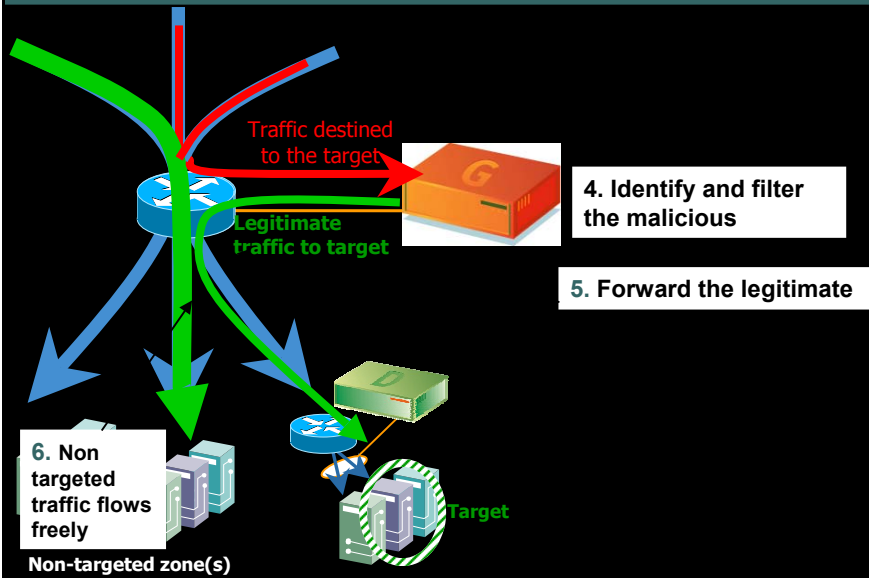
Dynamic Diversion Architecture

Cisco.com



Dynamic Diversion Architecture

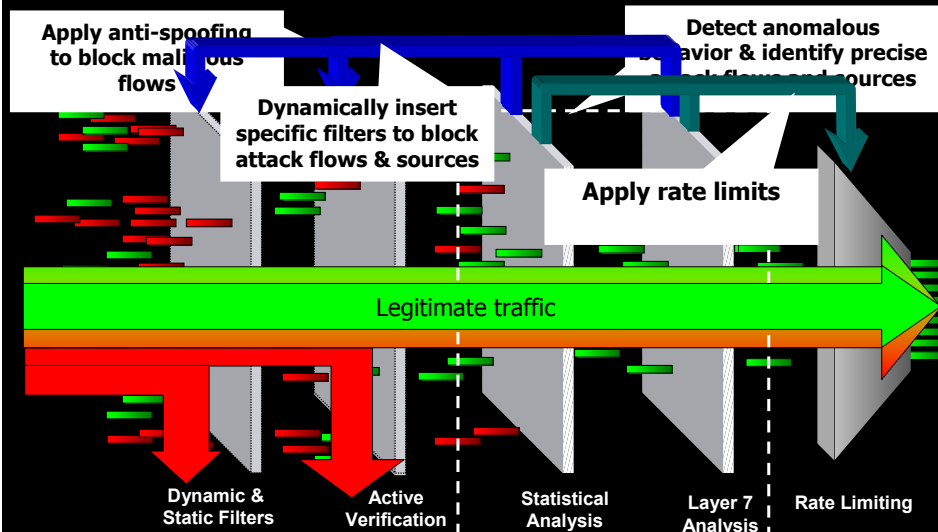
Cisco.com



45

Multi-Verification Process (MVP) Integrated Defenses in the Guard XT

Cisco.com



46

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*

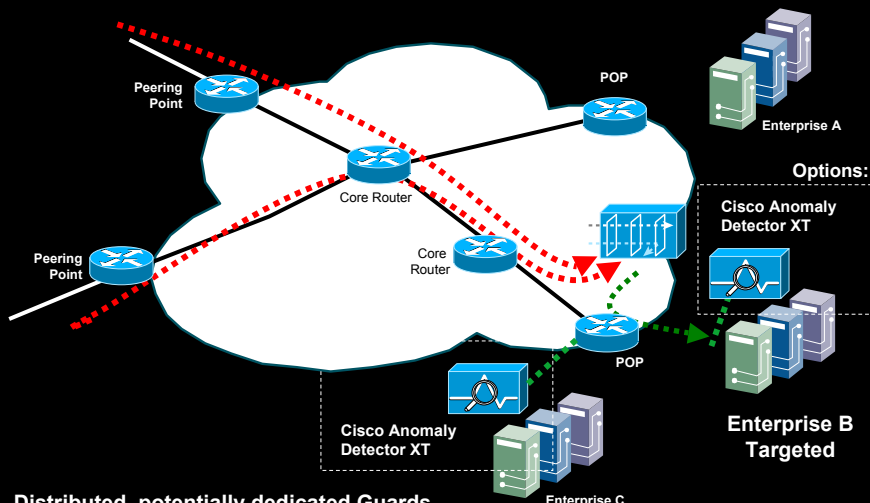
Guard / Detector SP Versions

- dual SMF interfaces
- DC power and NEBS server

47

Service Provider Distributed Protection

Cisco.com

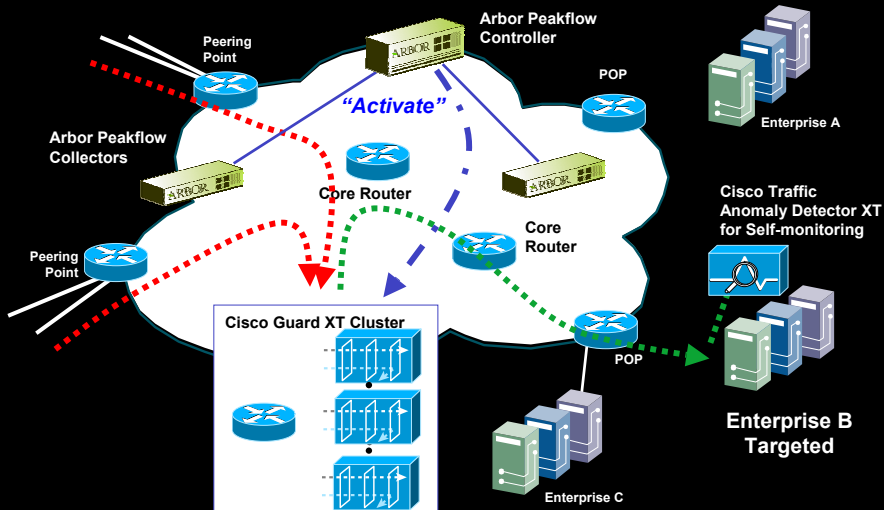


Distributed, potentially dedicated Guards
Detector CPE for monitoring and potentially activation
Potentially Detector at SP for monitoring, or Netflow...

48

Service Provider Centralized Protection

Cisco.com



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

49

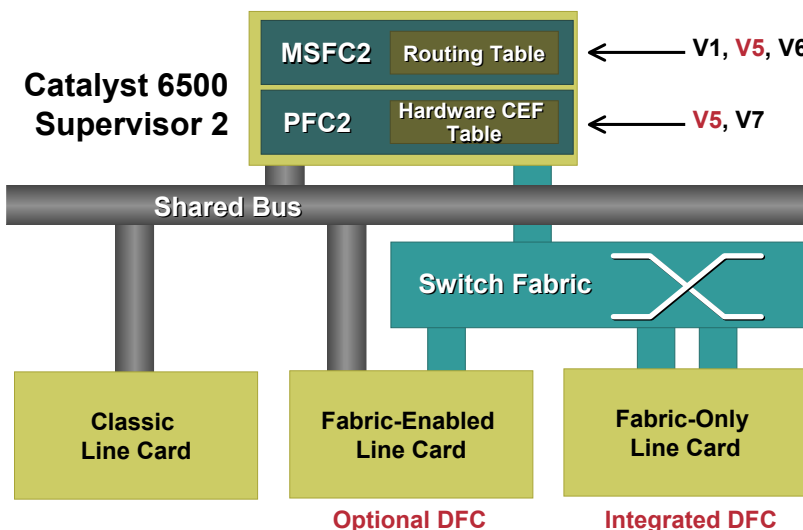
Cisco.com

De-worming Tools Netflow / Anomaly Detection Tool / RMON



NetFlow (NetFlow Architecture)

Cisco.com



51

NetFlow (functional sequence)

Cisco.com

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?



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



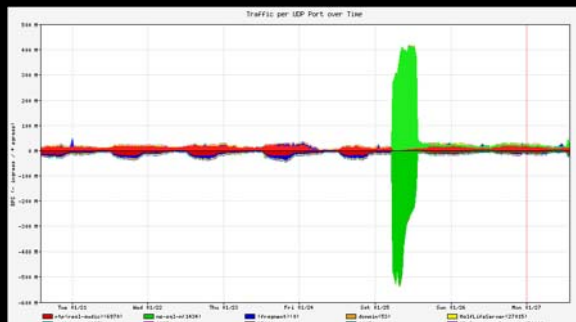
52

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.**



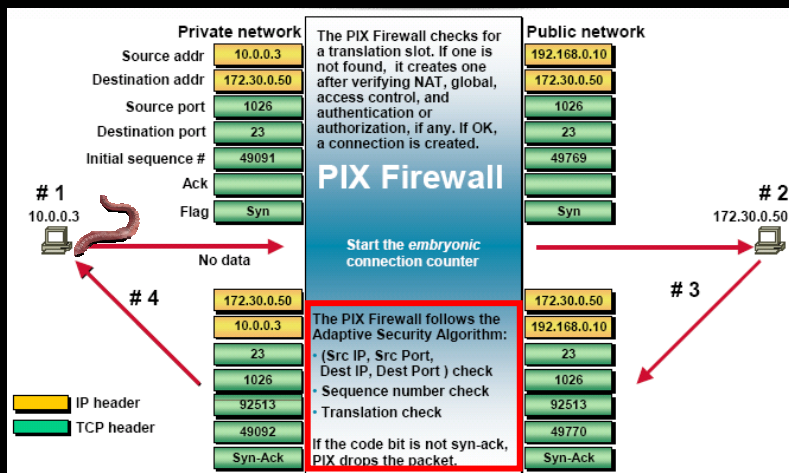
54

De-worming Tools Firewall



Firewall (Cisco Firewall)

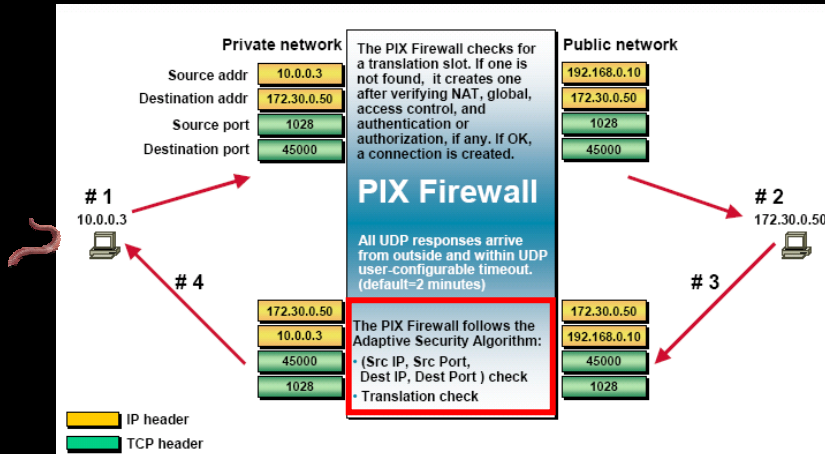
ASA (Adaptive Security Algorithm): De-Worming TCP based attacks



Firewall (Cisco Firewall)

Cisco.com

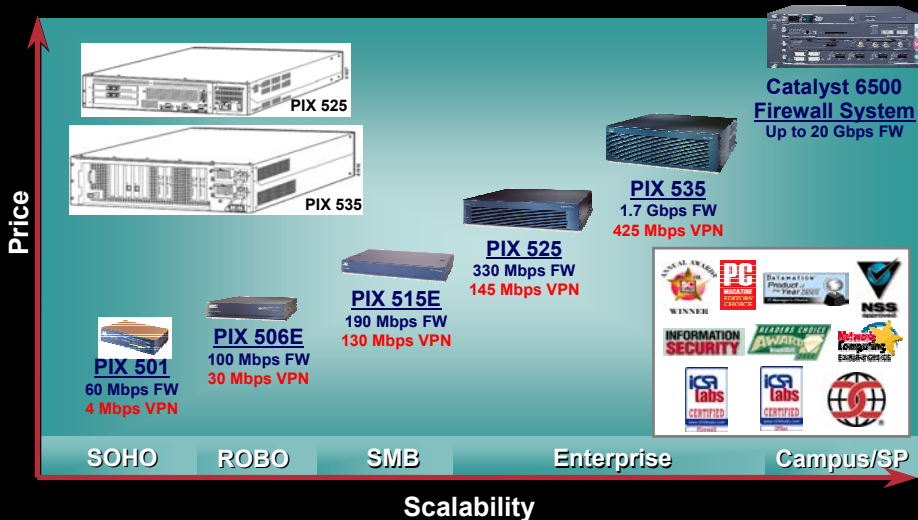
ASA (Adaptive Security Algorithm): De-Worming UDP based attacks



57

Cisco Firewall Product

Cisco.com



* ROBO : Remote Office Branch Office

58

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 floods

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

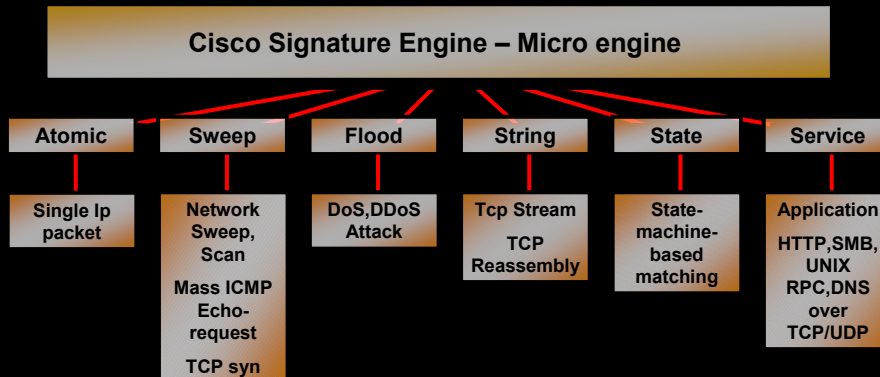
Network IDS

Cisco.com

Prevention methods

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

Cisco NIDS Engine



61

Cisco IDS/IPS

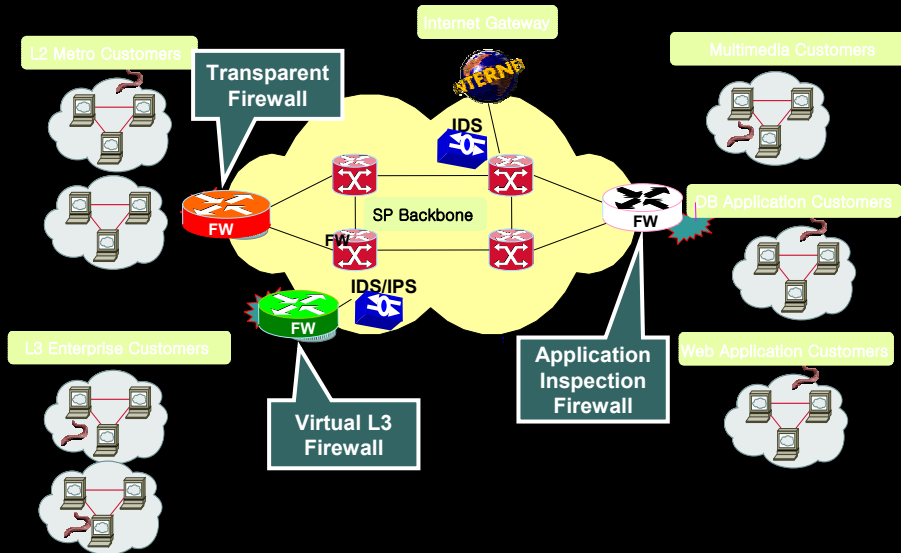
Cisco.com

		Solution Breadth				
Network Sensor		4215	4235	4250	4250-XL	
Switch Sensor		IDSM-2				
Host Sensor		Security Agent - PC		Security Agent - Server		
Router Sensor		8xx	18xx	28xx	38xx	7xxx
Firewall Sensor		501	506E	515E	525	535
Investigation & Mgmt		Web UI Embedded Mgr		Threat Response	CiscoWorks VMS	

62

How to apply Firewall & IDS in SP

Cisco.com



63

Cisco.com

De-worming Tools Host IDS/IPS



CSA (Cisco Security Agent)

Cisco.com

Probe phase

Ping scans

Port scans

Penetrate phase

Transfer exploit code to target

Persist phase

Install new code

Modify configuration

Propagate phase

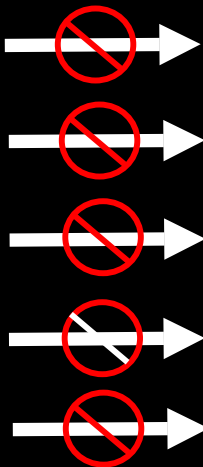
Attack other targets

Paralyze phase

Erase files

Crash system

Steal data



Server
protected
by CSA

File system interceptor

Network interceptor

Configuration interceptor

Execution space interceptor

65

CSA in Action: Protection Against Blaster

Cisco.com

Management Center for Cisco Security Agents - Microsoft Internet Explorer

Address: https://adams-dorm/csa/mcwebadmin

Management Center for Cisco Security Agents

Monitor Systems Configuration Maintenance Reports Profiler Search Help

Policy: All
Events per page: 50

#	Date	Host	Severity	Event
73	8/13/2003 4:18:13 PM	rob-xp-pro	Alert	TESTMODE: The program 'C:\WINDOWS\system32\msblast.exe' was downloaded from the network and is now trying to execute. This is an unusual event, but can happen during automated software installation. This would normally trigger a user query. Details Rule 97 Wizard Find Similar
72	8/13/2003 4:18:11 PM	rob-xp-pro	Warning	TESTMODE: The process 'C:\WINDOWS\system32\cmd.exe' (as user NT AUTHORITY\SYSTEM) tried to rename to the file 'C:\WINDOWS\system32\msblast.exe'. This would have caused the user to be prompted as to the action to take. Details Rule 277 Wizard Find Similar
71	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The current application 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) would not have been permitted to execute the new application 'C:\WINDOWS\system32\CMD.EXE'. Details Rule 287 Wizard Find Similar
70	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) tried to open/read the file 'C:\WINDOWS\system32\cmd.exe'. This would have been denied. Details Rule 280 Wizard Find Similar
69	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) tried to accept a TCP connection from 10.5.64.127 on port 4444. This would have been prevented. Details Rule 325 Wizard Find Similar

No rule changes pending [Generate rules](#)

Logged in as: admin

Start Windows Taskbar CiscoWorks - M... C:\WINNT\Syst... Select C:\WIN... Management... 4:22 PM

66

CSA DayZero ScoreCard

Cisco.com

CSA successfully blocked the following known attacks with a default installation

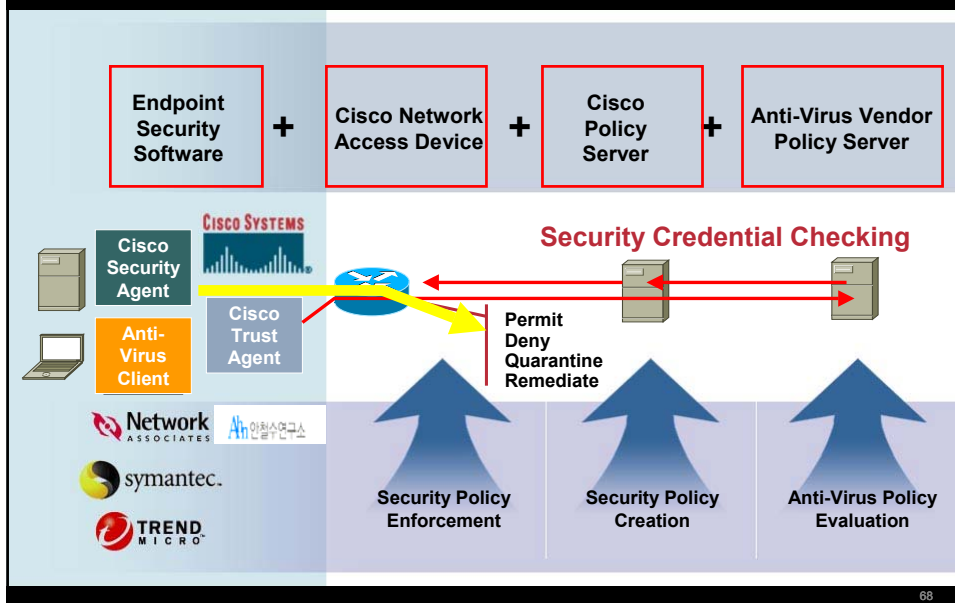
- Partial List -

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

67

Network Admission Control

Cisco.com

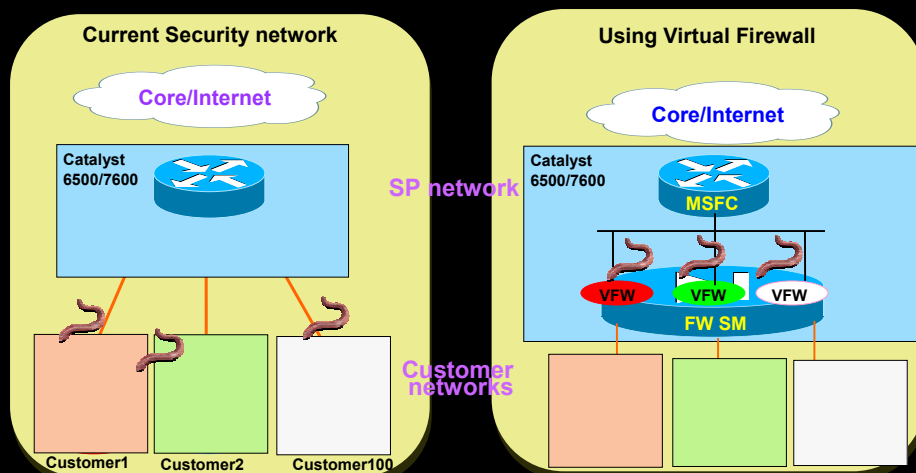


68

SP Managed Security

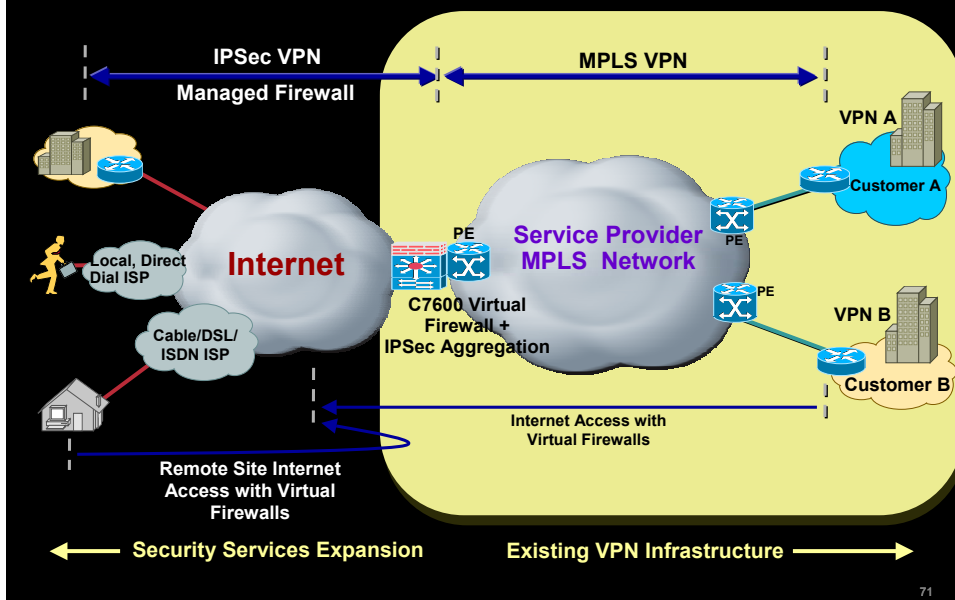


Managed Firewall



Managed VPN service

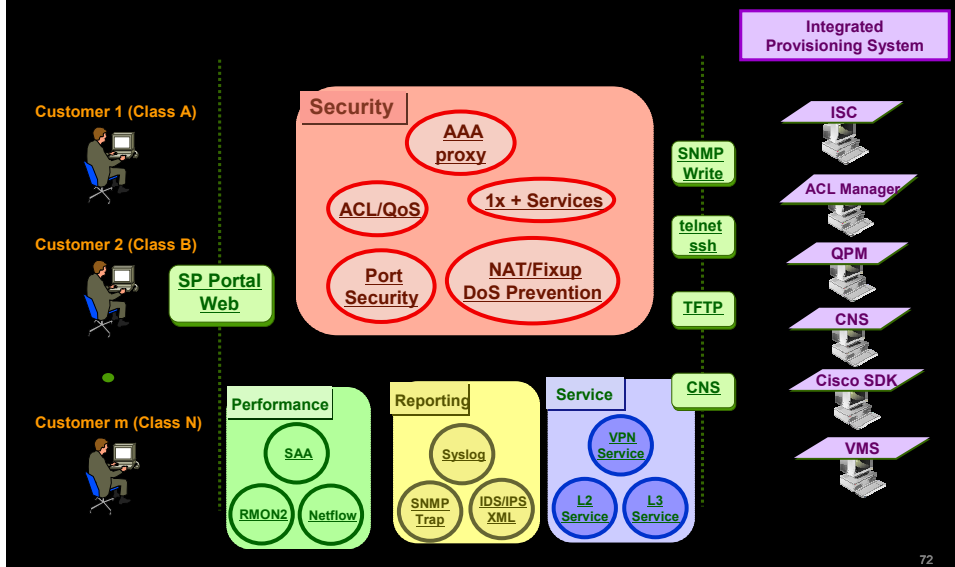
Cisco.com



71

Managed Security Provisioning & Management

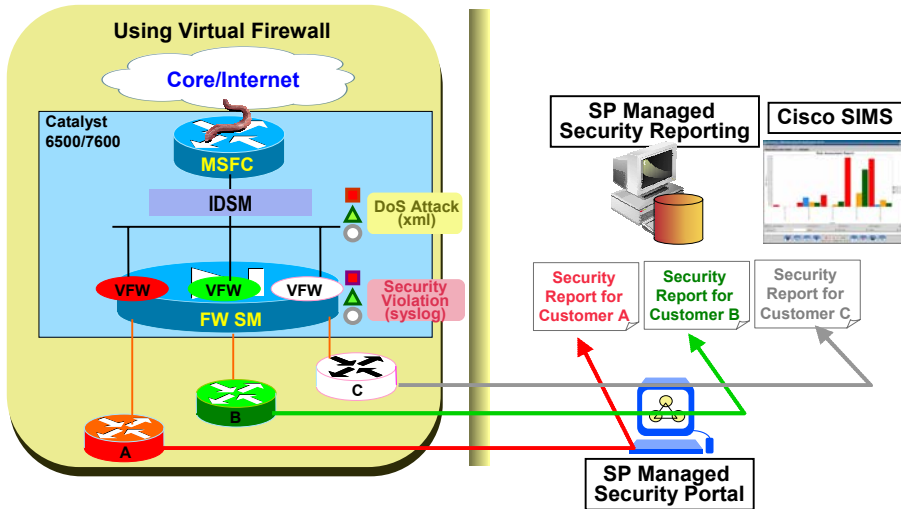
Cisco.com



72

Managed Security Report

Cisco.com



Cisco.com

Q and A



CISCO SYSTEMS

