



Touch Cisco

Cisco ASA Appliance



Touch Cisco - Webinare für Kunden

Michael Vassigh
Consulting System Engineer



Webinar “Thema Security”

Cisco ASA Security Appliance

Nach dem Webinar sollte der Zuhörer in der Lage sein:

- Die vielfältigen Security-Funktionen der ASA zu kennen
- Die Design-Optionen für High-Availability zu nutzen
- Die verfügbaren Firewall-Techniken der ASA für seine Umgebung auszuwählen und zu betreiben
- Den erfolgreichen Einsatz neuer Firewall-Funktionen zum verstärkten Schutz des Datenverkehrs zu planen

Agenda

- ASA Hardware & Options
 - Short Introduction
- ASA Software
 - High-Availability/Redundancy
- ASA Advanced Firewall-Functions
 - Inspection Engines
 - Connection-Management
- Summary

Hardware-Overview



Cisco ASA 5500 Series Adaptive Security Appliances

Solutions Ranging from Desktop to Data Center

Cisco ASA 5500 Platforms

- Integrates, market-proven firewall, SSL/IPsec, IPS, and content security technologies
- Extensible multi-processor architecture delivers high concurrent services performance and significant investment protection
- Flexible management lowers cost of ownership
- Easy-to-use Web-based user interface
- Numerous certifications and awards
- And much more...



ASA 5505



ASA 5510



ASA 5520



ASA 5540



ASA 5550



ASA 5580-20



ASA 5580-40



Teleworker

Branch
Office

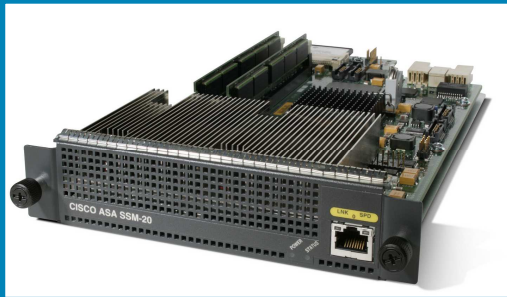
Internet
Edge

Campus

Data Center

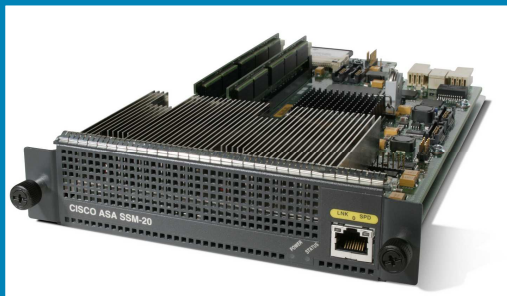
Wide-Range of Cisco ASA 5500 Series Security Service Modules (SSMs)

IPS Security Services Module (AIP-SSM)



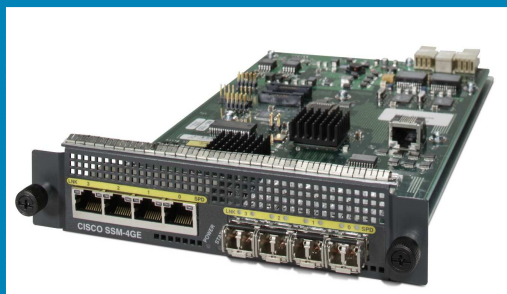
- Provides **full-featured IPS and IDS services** for protection of critical network assets
- Available in 3 models: SSM-10, SSM-20, SSM-40
- Delivers up to 650 Mbps of IPS throughput

Content Security Services Module (CSC-SSM)



- Provides **full-featured Anti-X services** (anti-virus, anti-spyware, anti-spam, anti-phishing, URL filtering, and more)
- Available in two models SSM-10 and SSM-20

4-Port GE Services Module (4GE-SSM)



- I/O module offers **four copper 10/100/1000 ports** in addition to **four SFP ports** for improved flexibility and network segmentation
- Customers can use up-to four ports total out of these eight ports, with the ability to mix and match copper and optical GE ports

High-Availability



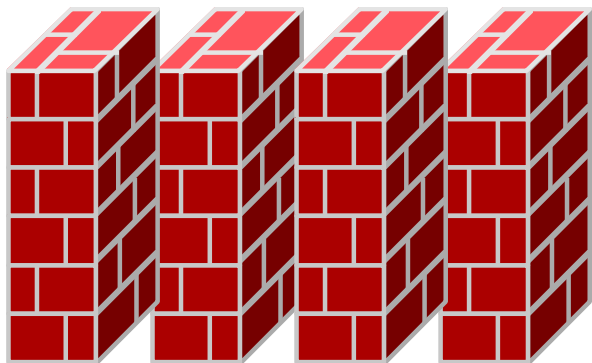
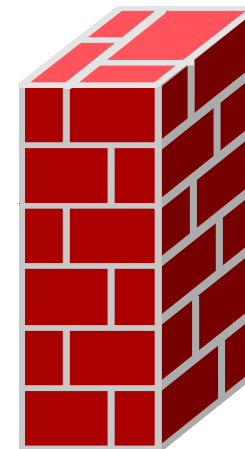
High Availability

Different people, different opinions ...

- „Needs a redundant Chassis !“
- „Needs a redundant Power-Supply !“
- „Data-Plane or Control Plane ?“
- „Use a Loadbalancer !“
- „Are you asking for Failover ?“
- „Is covered by our 24x7x2h Support-Service“

Firewall Design - Virtualization

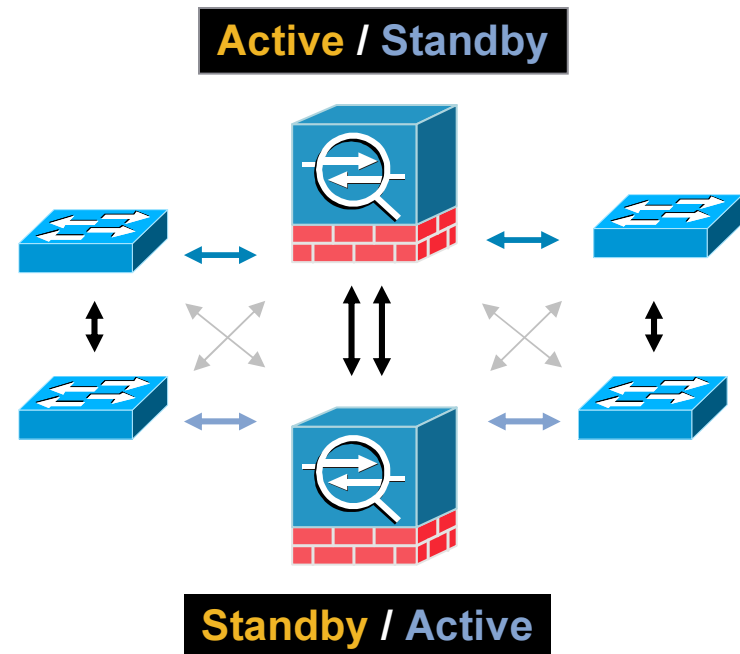
- Virtualization provides a way to create multiple firewalls in the same physical chassis
- Maximum number of virtual firewalls is 50 for the ASA (not supported on ASA 5505)



- Virtualization is a licensed feature
- Within the ASA a Virtual-Firewall-Instance is called a "Context"

Redundant Chassis

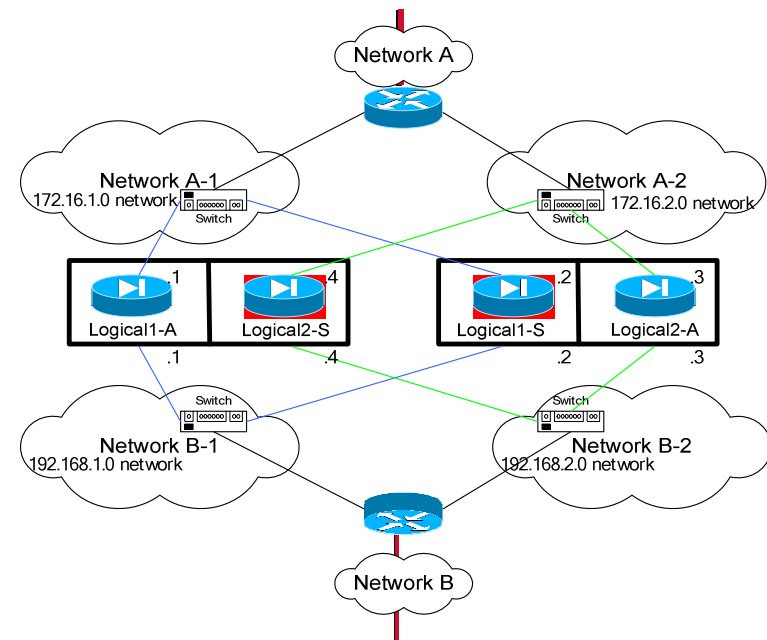
- 2x Identical chassis
- Identical SW-Releases
- Identical Service-Modules
- Dedicated Sync-Interfaces for „Config“ & „Session-State“ recommended
- „State“-Interface speed should follow „Data-Interface“ speeds*
- Cross-Over cable between ASA not recommended
- From 5505 to 5580
(Plus license on smaller model)



*ASA5580: 1x GE-performance is sufficient for 10GE-Installations

Deployment Options

- Active - Standby Mode
 - Single-Context-Mode option
 - Most SW features available
 - Single Data-Path at any time
 - Stateful-Failover Optional*
- Active – Active Mode
 - Multi-Context required*
 - Limits available SW features
 - Multiple Data-Paths possible
 - Stateful-Failover Optional*



*Not on ASA5505

Failover Requirements

- Software Image and Operation-Mode must be identical
 - Major and Minor Release Version e.g. 7.2*
 - Both units in Routed-Mode/Transparent-Mode
 - Both units in Single-Mode/Multi-Context-Mode
 - Flash-Size can be different
- Failover IP Configuration required on both units
 - Failover-Link-Interface (Control-Plane = Config)
 - Failover-State-Interface (Data-Plane = active Sessions)
 - Monitored Interfaces (Health-Check/Probing)
- Failover Timing can be adjusted
 - Sub-Second Failover scenario (polltime unit msec xxx)

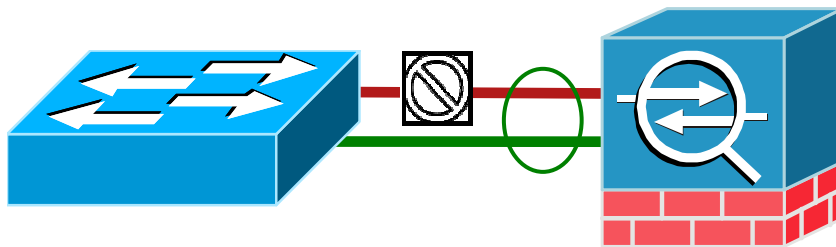
*Minor Releases can be upgraded during failover

Redundant Interface (8.0)*

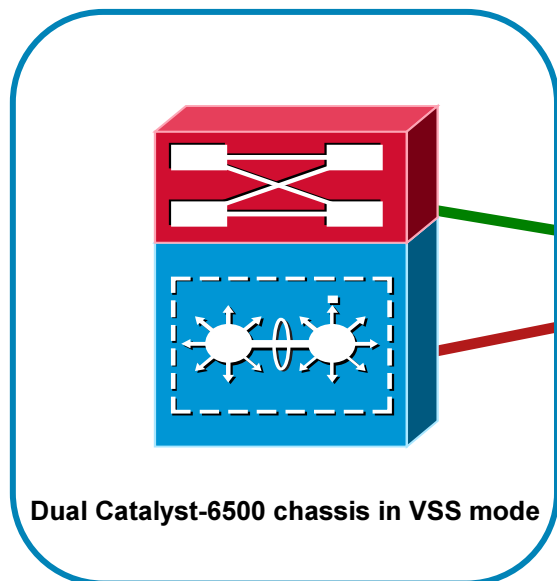
- Single Chassis Option
- Logical Interface represents physical interface-pair
- All configuration refers to Logical-Interface
 - Nameif
 - Security-Level
 - IP-Address
- Failover is less than 500ms
- Passes traffic when member interface is enabled
- Active interface can be moved between „pairs“
- Maximum 8 interface pairs

*Not on ASA5505

Interface redundancy design



Simple Deployment Option



„VSS“-Deployment Option

Redundant-Route/“Backup-ISP”

- Single Chassis Option
- Uses 2 Interfaces
- Supported Interfaces
 - DHCP-Client
 - PPPoE-Client
 - Regular Interface
- Tracking of connectivity with SLA-Monitor
 - Failover monitoring can be tuned
- Failover result is „Routing“ change
- No Load-Balancing/Sharing

Sample Setup

- 2 „Routes“ required

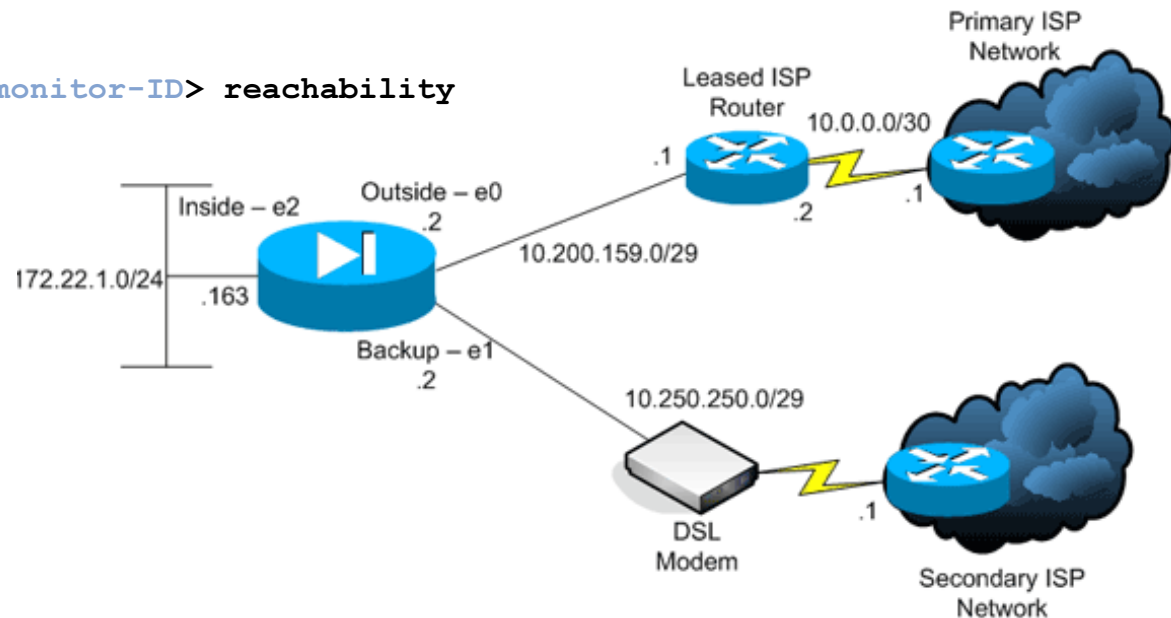
```
route outside 0.0.0.0 0.0.0.0 10.200.159.1 1 track <track-ID>
route backup 0.0.0.0 0.0.0.0 10.250.250.1 254
```

- SLA-Monitor + Timing

```
sla monitor <monitor-ID>
  type echo protocol ipIcmpEcho 10.0.0.1 interface outside
sla monitor schedule <monitor-ID> life forever start-time now
```

- Activate Tracking

```
track <track-ID> rtr <monitor-ID> reachability
```



VPN Redundancy (Remote Access)

- 2 or more systems build a cluster (tested = 10)
 - ASA5510, ASA5520, ASA5540, ASA5580
 - Mix of VPN3000 and ASA possible (not recommended)
 - SW-Mix possible (not recommended)
- Supports both IPSEC and SSL-VPN clients
 - Cisco VPN Client
 - Cisco AnyConnect Client
 - Cisco IOS EzVPN (HW-Client)
 - Cisco VPN 3002
 - Cisco PIX 501
 - Cisco ASA5505
 - „some Third Party Clients“
- Cluster-Master distributes traffic
 - Loadsharing is done automatically
 - Member-Failure requires new connection setup

External Loadbalancer (not ASA specific)

- No special requirements on ASA
- Multiple Systems can be active
- Loadbalancer distributes traffic
- Loadbalancer monitors availability
- Loadbalancer ensures correct traffic-flow
- Loadbalancer ensures failover
- Loadbalances Firewall or VPN or both

Advanced Firewalling Options



Application Inspection & Control Engines

Provide Control over Application Usage & Network Access

- Application and protocol-aware inspection services provide strong application-layer security and detailed policy controls
- Perform **conformance checking, state tracking, security checks**, NAT/PAT, dynamic port allocation, and **offer a wide range of controls** for businesses to set application-layer policies

Media/Voice over IP

SIP
SCCP (Skinny)
H.323 v1–4
GTP (3G Mobile Wireless)
MGCP
TRP/RTCP/RTSP
TAPI/JTAPI

**Over 30
Engines**

Database/OS Services

ILS/LDAP
Oracle/SQL*Net (V1/V2)
Microsoft RPC/DCE RPC
Microsoft Networking
NFS
RSH
SunRPC/NIS+
X Windows (XDMCP)

Specific Applications

Microsoft Windows Messenger
Microsoft NetMeeting
Real Player
Cisco IP Phones
Cisco Softphones

Core Internet Protocols

HTTP
FTP
TFTP
SMTP/ESMTP
DNS/EDNS
ICMP
TCP
UDP

Security Services

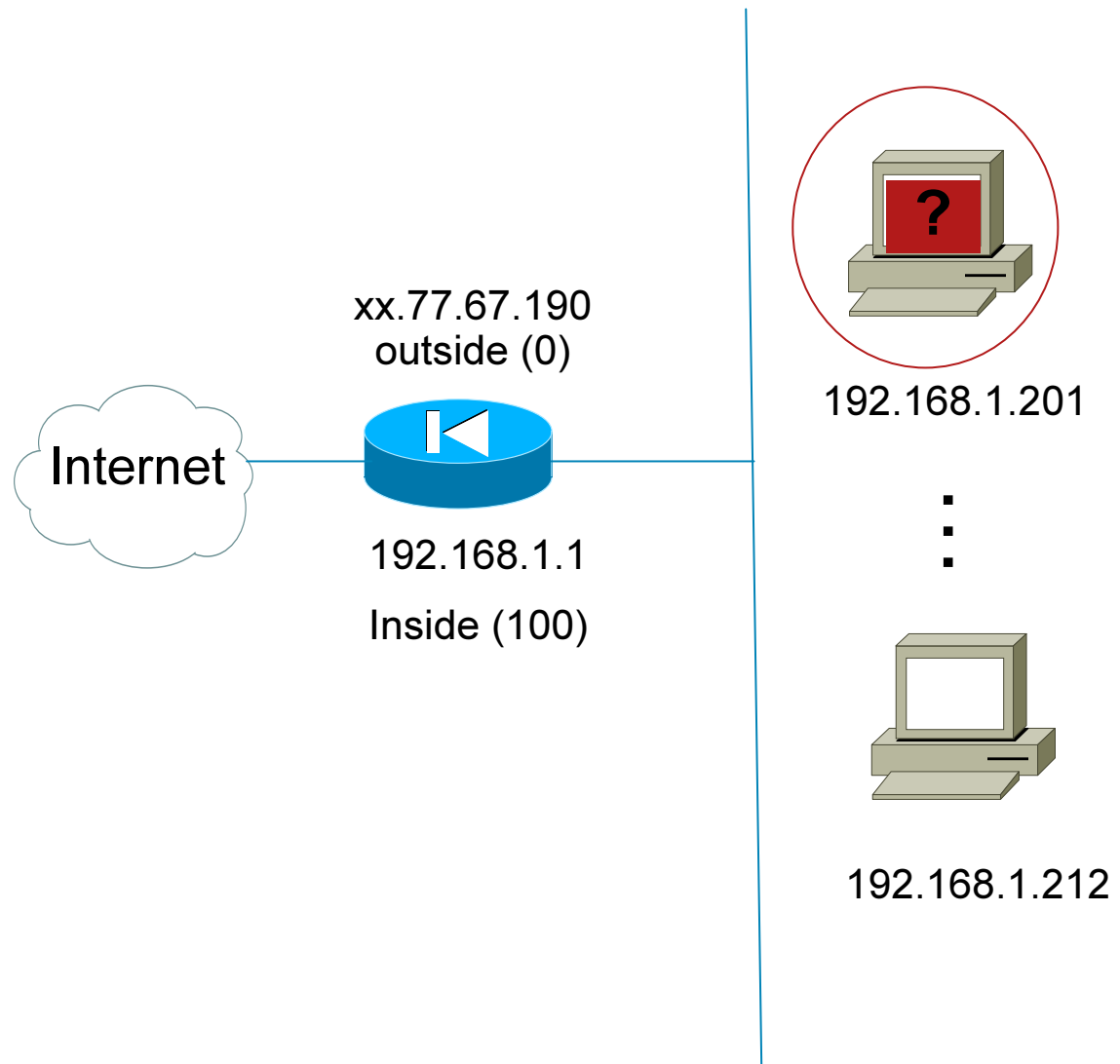
IKE
IPSec
PPTP

HTTP Inspection Evolution on PIX/ASA

- New default inspection policies for IM, P2P and tunneling protocols (use **show run all** to display in config)
- 7.2 added more inspection features (partial list):
 - Permit/deny packets with multiple content-type headers
 - Granular control over protocols tunneled inside of HTTP
 - Permit/deny null HTTP encodings
 - Permit/deny non-ASCII request headers, forms parameters, and response headers
 - HTTP Server Banner Masking
 - Java, ActiveX, and other applet/script filtering capabilities to improve upon existing filter commands

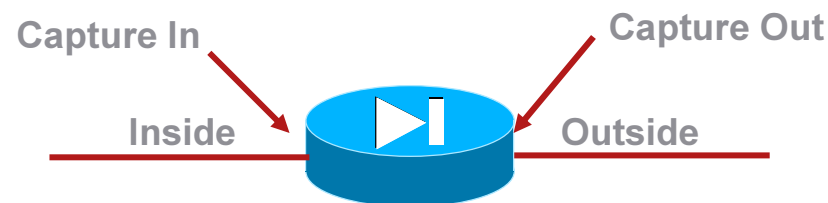
Case Study: Block GoToMyPC Application

- Problem:
After implementing filtering, we noticed host 192.168.1.201 talking via tcp/80 to Go2myPC.com
- Goal:
Using HTTP inspection engine to implement a policy that blocks users from using that service, while allowing access to tcp/80 for allowed traffic



ASDM-Tool: Packet Capture

- Traffic can be captured both before and after it passes through the firewall; one capture on the inside interface, one capture on the outside interface
- Capture buffer saved in RAM (default size 512KB)
- Default is to stop capturing when buffer is full
- Default packet length is 1518 bytes
- Copy captures off via TFTP or HTTPS



Capture viewed in Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a packet capture of a file named 'first.pcap'. The filter is set to '(ip.addr eq 198.133.219.25 and ip.addr eq 10.1.15.32) and (tcp.port eq 80)'. The packet list shows several packets, with packet 30 selected. The packet details pane shows the following information:

- Frame 30 (54 bytes on wire (54 bytes captured))
- Ethernet II, Src: Cisco_92:61:a4 (00:0e:84:92:61:a4), Dst: Cisco_0f:9a:44 (00:19:56:0f:9a:44)
- Internet Protocol, Src: 198.133.219.25 (198.133.219.25), Dst: 10.1.15.32 (10.1.15.32)
- Transmission Control Protocol, Src Port: http (80), Dst Port: netview-aiX-4 (1664), Seq: 896,

The packet bytes pane shows the raw data of the selected packet. The 'Follow TCP Stream' window is open, displaying the stream content. The stream content shows a series of HTTP 304 Not Modified responses, each with a 'Connection: Keep-Alive' header. The responses are from the same server (198.133.219.25) to the same client (10.1.15.32). The responses are for different resources, as indicated by the 'Etag' values: '443b', '21e', '196', '557c', and '32d'.

Stream Content:

```
HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Date: wed, 07 May 2008 17:04:14 GMT
Last-Modified: Fri, 12 Jan 2007 20:21:56 GMT
Etag: "443b"

HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Date: wed, 07 May 2008 17:04:15 GMT
Last-Modified: Tue, 26 Sep 2006 00:03:57 GMT
Etag: "21e"

HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Date: wed, 07 May 2008 17:04:15 GMT
Last-Modified: Tue, 19 Dec 2006 20:00:33 GMT
Etag: "196"

HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Date: wed, 07 May 2008 17:04:15 GMT
Last-Modified: Thu, 03 Apr 2008 18:10:19 GMT
Etag: "557c"

HTTP/1.1 304 Not Modified
Connection: Keep-Alive
Date: wed, 07 May 2008 17:04:16 GMT
Last-Modified: Tue, 19 Dec 2006 19:59:13 GMT
Etag: "32d"
```

ASDM-Tool: HTTP Inspection

Cisco ASDM 5.2 for ASA - 192.168.1.72 (Preview Release)

File Options Tools Wizards Help Search: Find

Home Configuration Monitoring Back Forward Packet Tracer Refresh Save Help

Configuration > Global Objects > Class Maps > HTTP

Network Object Groups

IP Names

Service Groups

Class Maps

DNS

FTP

H.323

HTTP

Instant Messaging (IM)

SIP

Inspect Maps

DCERPC

DNS

ESMTP

FTP

GTP

H.323

HTTP

Instant Messaging (IM)

IPSec Pass Through

MGCP

NetBIOS

RADIUS Accounting

SCCP (Skinny)

SIP

SNMP

Regular Expressions

TCP Maps

Time Ranges

HTTP

HTTP class maps with names starting with "_default" are default class maps and cannot be modified or deleted.

Name	Match Conditions			Description
	Match	Criterion	Value	
_default_GoTo...		Request Arguments	_default_GoToMyP...	
		Request URI	_default_GoToMyP...	
_default_aim-m...		Request Header Field (...)	_default_aim-mess...	
_default_firethr...		Request Header Field (...)	_default_firethru-t...	
		Request URI	_default_firethru-t...	
_default_gator		Request Header Field (...)	_default_gator	
_default_gnu-h...		Request Arguments	_default_gnu-http-t...	
		Request URI	_default_gnu-http-t...	
_default_http-tu...		Request URI	_default_http-tunnel	
_default_httpport...		Request Header Field (...)	_default_httpport-tu...	
_default_kazaa		Response Header Field...	> 0	
_default_msn-m...		Response Header Field...	_default_msn-mes...	
_default_shout...		Request Header Field (...)	_default_shoutcas...	
_default_windo...		Request Header Field (...)	_default_windows...	
_default_yahoo...		Request Body	_default_yahoo-m...	

Match
 No match
 Regular expression
 Regular expression class

Apply Reset

tester 2 5/3/06 6:09:51 AM UTC

ASDM-Tool: Regex Build Wizard

- This is the string to match on
- We chose to ignore case resulting in this string match

Build Regular Expression

Build a regular expression snippet and insert it into the regular expression below.

Build Snippet

☐ Starts at the beginning of the line (^)

Specify Pattern

☒ Specify character string

Character String: .ercbroker

☐ Escape special characters

☒ Ignore case

☐ Specify character

☐ Negate the character

Choose Character

☒ Any character (.)

☐ Character set: 0-9A-Za-z

☐ Special character: \

☐ Whitespace character: \s

☐ Three digit octal number: [0-7]

☐ Two digit hexadecimal number: [0-9A-F]

☐ Specified Character: []

Snippet Preview: [Ee][Rr][Cc][Bb][Rr][Oo][Kk][Ee][Rr]

Append Snippet Append Snippet as Alternate Insert Snippet at Cursor

Regular Expression

.ercbroker Test...

Selection Occurrences

☒ Zero or one times (?) ☐ At least [] times {n,}

☐ One or more times (+) ☐ Exactly [] times {n}

☐ Any number of times (*)

Apply to Selection

OK Cancel Help

Final HTTP Inspect

Edit HTTP Inspect

Match Criteria

☒ Single Match

Match Type: ☒ Match ☐ No Match

Criterion: Request URI

Value

☒ Regular Expression: MH-Go2MyPC_2

☐ Regular Expression Class: go2mypc_class

☐ Multiple matches

HTTP Traffic Class: _default_GoToMyPC-tunnel

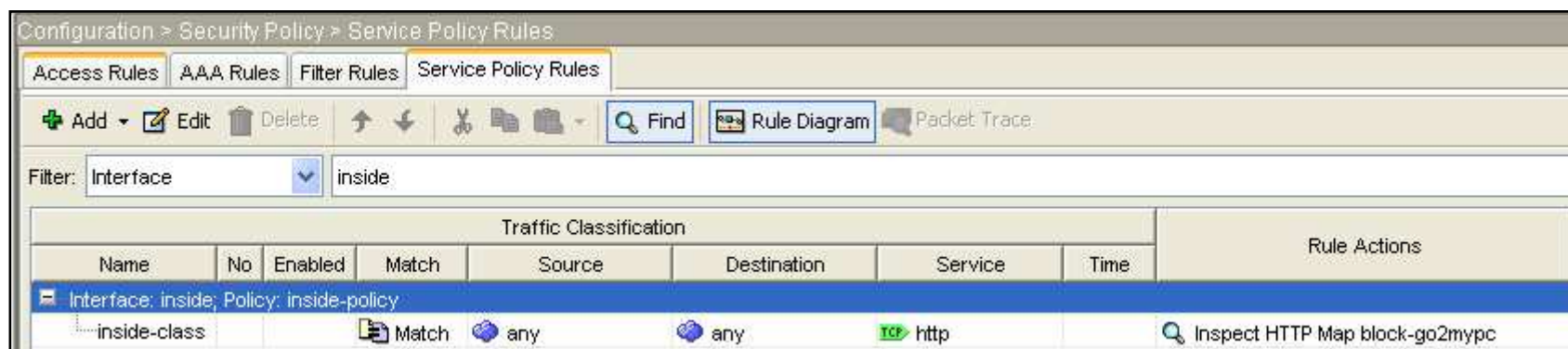
Actions

Action: ☒ Drop Connection ☐ Reset ☐ Log

Log: ☒ Enable ☐ Disable

- Our match criteria is to inspect the URI being sent by the client
- Note that this HTTP inspect policy can be set to drop the connection, reset client and server (TCP RST) or just log the connection
- Because our security policy does not allow for remote PC management, we are going to drop the connection and log

Final Service Policy on Interface



- In this example, note that the service policy is only inspecting tcp/80. All other traffic is not bound to this particular policy
- We could have also selected more granular source and destination L3 addresses, if necessary

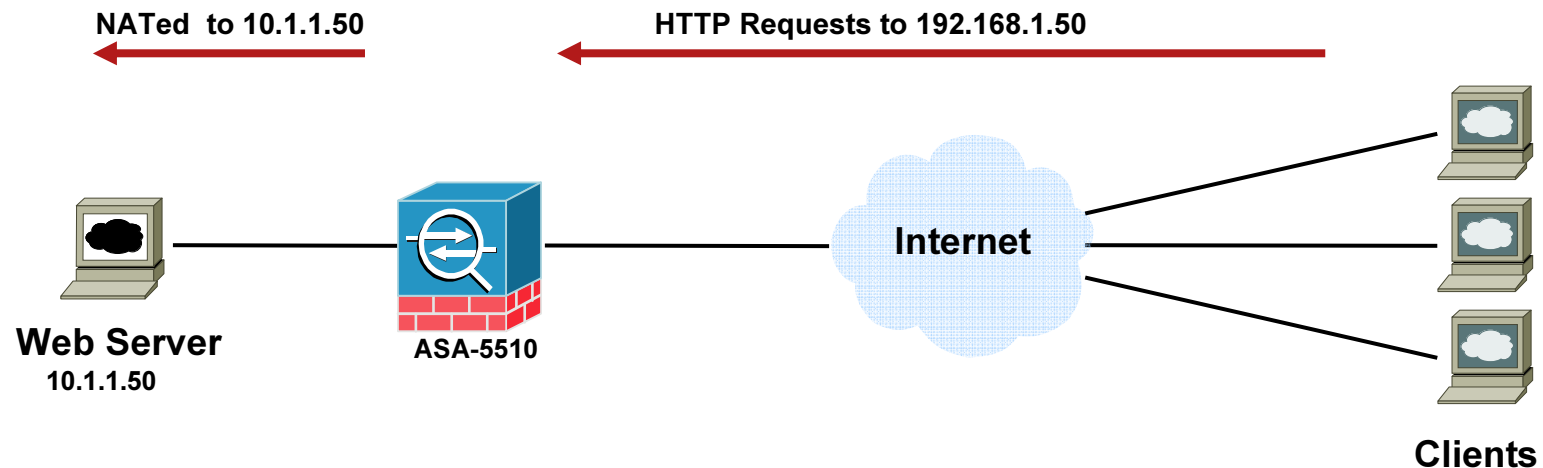
Connection Management



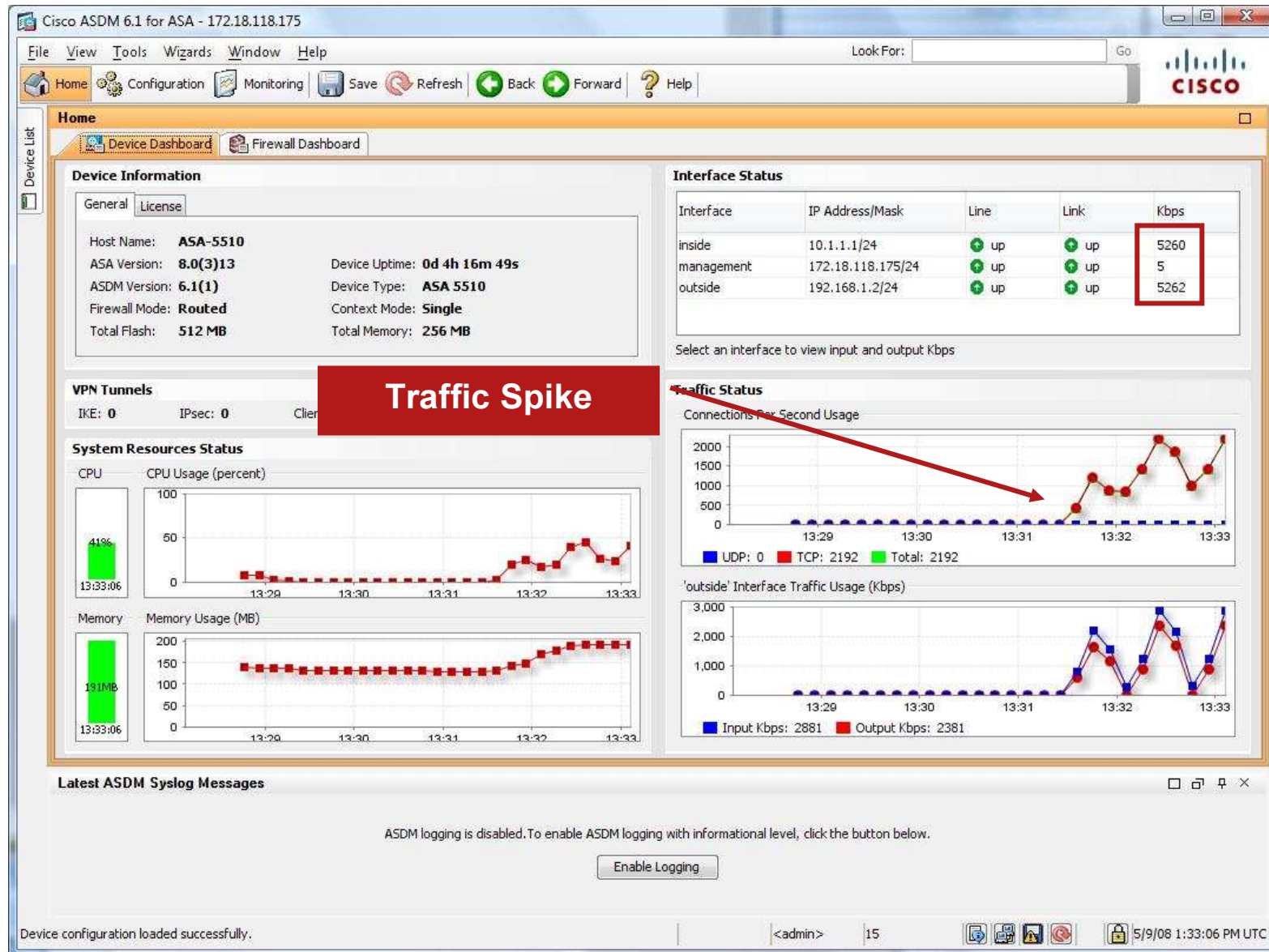
Case Study: Intermittent Access to Web Server

Problem

- Most external clients are not able to load company's web page



Case Study: Intermittent Access to Web Server



Case Study: Intermittent Access to Web Server

- **show perfmon** indicates high number of embryonic connections

```
ASA-5510# show perfmon
```

PERFMON STATS:	Current	Average
Xlates	0/s	0/s
Connections	2059/s	299/s
TCP Conns	2059/s	299/s
UDP Conns	0/s	0/s
URL Access	0/s	0/s
URL Server Req	0/s	0/s
TCP Fixup	0/s	0/s
TCP Intercept Established Conns	0/s	0/s
TCP Intercept Attempts	0/s	0/s
TCP Embryonic Conns Timeout	1092/s	4/s
HTTP Fixup	0/s	0/s
FTP Fixup	0/s	0/s
AAA Authen	0/s	0/s
AAA Author	0/s	0/s
AAA Account	0/s	0/s

VALID CONNS RATE in TCP INTERCEPT:	Current	Average
	N/A	95.00%

```
ASA-5510#
```

Show Conn and Show Conn Detail

Idle Time,
Bytes Transferred

Connection
Flags

```
ASA# show conn
2 in use, 64511 most used
```

```
TCP out 198.133.219.25:23 in 10.9.9.3:11068 idle 0:00:06 Bytes 127 flags UIO
UDP out 172.18.124.1:123 in 10.1.1.9:123 idle 0:00:13 flags -
```

“detail” Adds
Interface Names

```
ASA# show conn detail
2 in use, 64511 most used
```

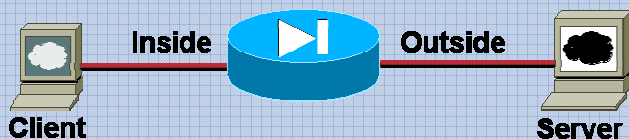
```
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
        B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
        E - outside back connection, F - outside FIN, f - inside FIN,
        G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data, i - incomplete,
        k - Skinny media, M - SMTP data, m - SIP media, O - outbound data,
        P - inside back connection, q - SQL*Net data, R - outside acknowledged FIN,
        R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
        s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
```

```
TCP outside:198.133.219.25/23 inside:10.9.9.3/11068 flags UO
UDP outside:172.18.124.1/123 inside:10.1.1.9/123 flags -
```

Connection Flags—Quick Reference

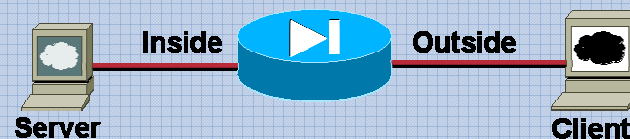
Outbound Connection

<u>TCP Flags</u>	<u>FW Flags</u>
SYN	saA
SYN+ACK	A
ACK	U
Inbound Data	UI
Outbound Data	UIO
FIN	Uf
FIN+ACK	UfFR
ACK	UfFRr



Inbound Connection

<u>TCP Flags</u>	<u>FW Flags</u>
SYN	SaAB
SYN+ACK	aB
ACK	UB
Inbound Data	UIB
Outbound Data	UIOB
FIN	UBF
FIN+ACK	UBfFR
ACK	UBfFRr



Case Study: Intermittent Access to Web Server

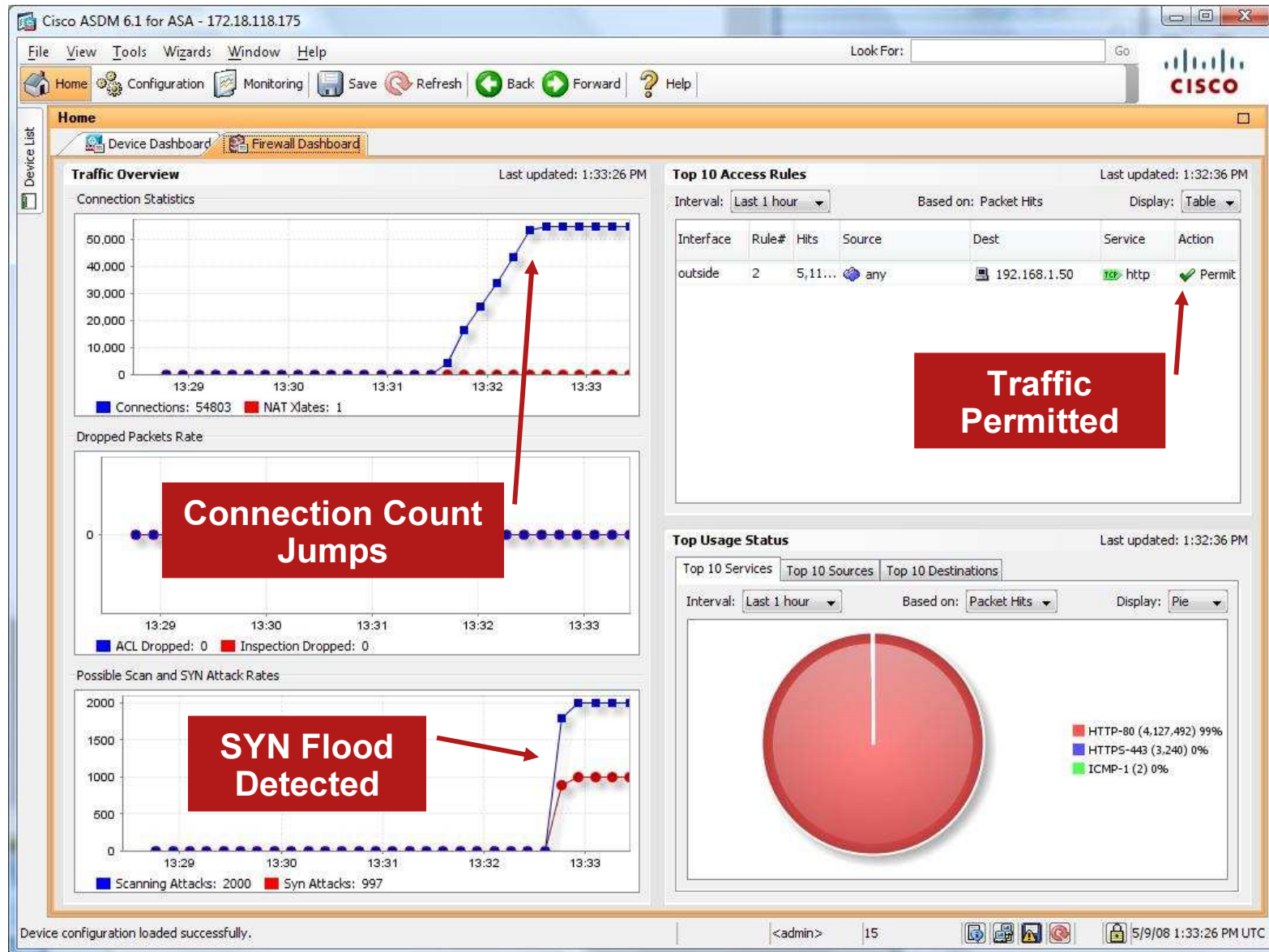
- Issue **show conn** to see 'who' is creating the connections

Random Sources

Embryonic Conns

```
ASA-5510# show conn
54764 in use, 54764 most used
TCP outside 17.24.101.118:26093 inside 10.1.1.50:80, idle 0:00:23, bytes 0, flags aB
TCP outside 111.76.36.109:23598 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 24.185.110.202:32729 inside 10.1.1.50:80, idle 0:00:25, bytes 0, flags aB
TCP outside 130.203.2.204:56481 inside 10.1.1.50:80, idle 0:00:29, bytes 0, flags aB
TCP outside 39.142.106.205:18073 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 75.27.223.63:51503 inside 10.1.1.50:80, idle 0:00:03, bytes 0, flags aB
TCP outside 121.226.213.239:18315 inside 10.1.1.50:80, idle 0:00:04, bytes 0, flags aB
TCP outside 66.187.75.192:23112 inside 10.1.1.50:80, idle 0:00:06, bytes 0, flags aB
TCP outside 13.50.2.216:3496 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 99.92.72.60:47733 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
TCP outside 30.34.246.202:20773 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 95.108.110.131:26224 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 76.181.105.229:21247 inside 10.1.1.50:80, idle 0:00:06, bytes 0, flags aB
TCP outside 82.210.233.230:44115 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 134.195.170.77:28138 inside 10.1.1.50:80, idle 0:00:12, bytes 0, flags aB
TCP outside 70.133.128.41:22257 inside 10.1.1.50:80, idle 0:00:15, bytes 0, flags aB
TCP outside 124.82.133.172:27391 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
TCP outside 26.147.236.181:37784 inside 10.1.1.50:80, idle 0:00:07, bytes 0, flags aB
TCP outside 98.137.7.39:20591 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 37.27.115.122:24542 inside 10.1.1.50:80, idle 0:00:12, bytes 0, flags aB
. . .
```

Case Study: Intermittent Access to Web Server

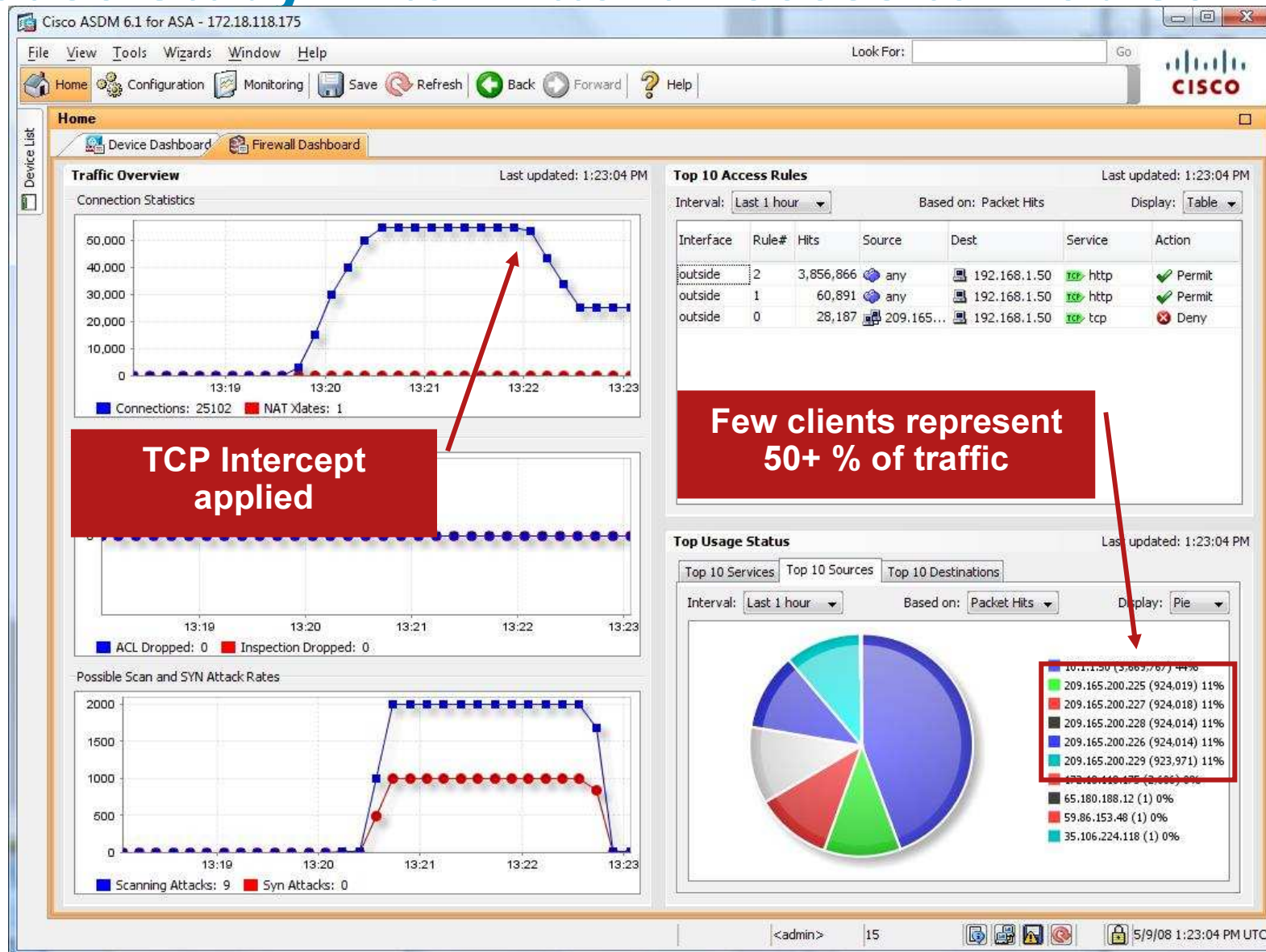


Case Study: Intermittent Access to Web Server

- Apply TCP Intercept to stop the SYN flood attack

```
access-list 140 extended permit tcp any host 192.168.1.50 eq www
!
class-map protect
  description Protect web server from attacks
  match access-list 140
!
policy-map interface_policy
  class protect
    set connection embryonic-conn-max 100
!
service-policy interface_policy interface outside
```

Case Study: Intermittent Access to Web Server

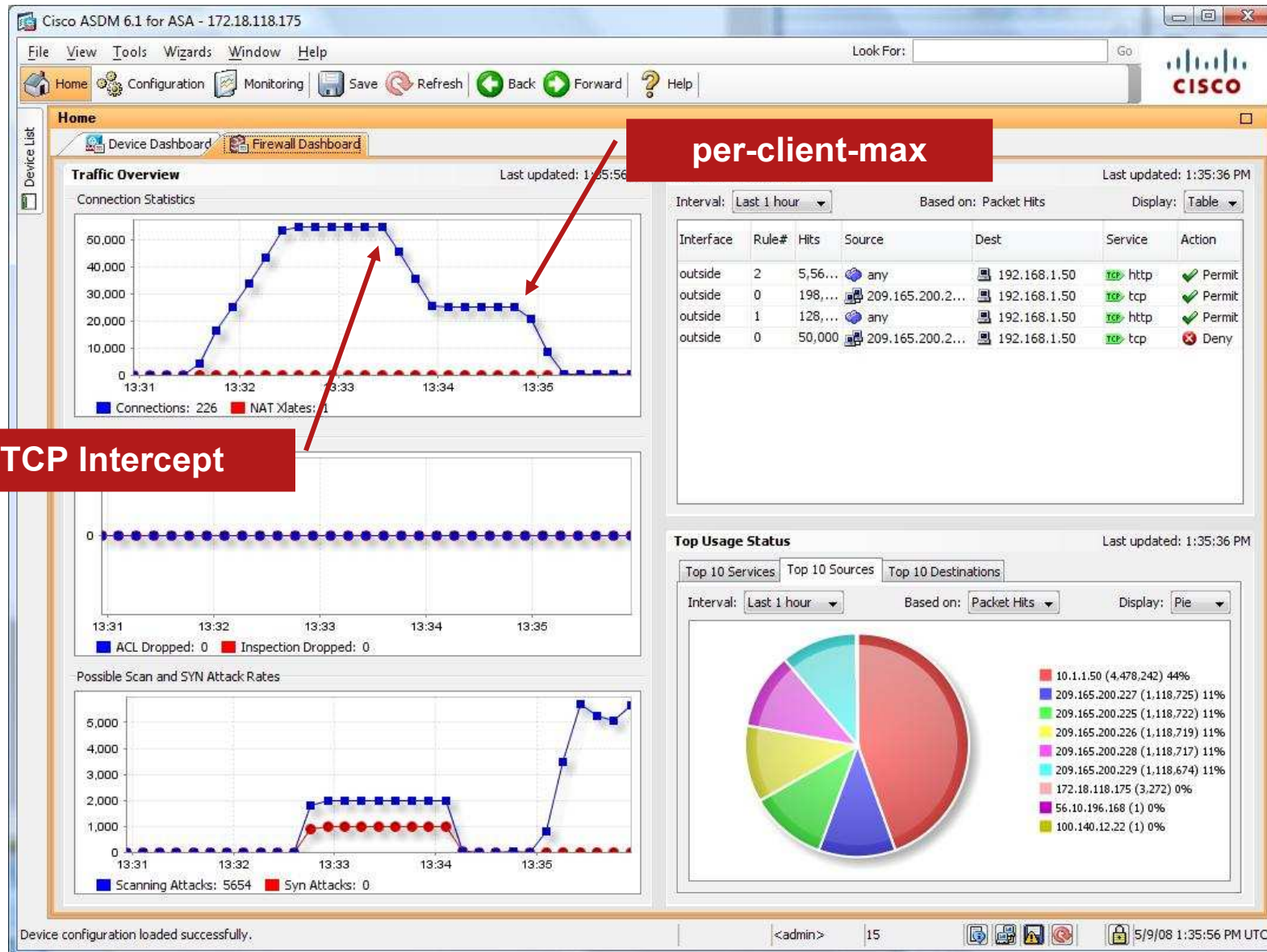


Case Study: Intermittent Access to Web Server

- Apply **per-client-max** option to limit the number of connections any single client can establish

```
access-list 140 extended permit tcp any host 192.168.1.50 eq www
!
class-map protect
  description Protect web server from attacks
  match access-list 140
!
policy-map interface_policy
  class protect
    set connection embryonic-conn-max 100 per-client-max 25
!
service-policy interface_policy interface outside
```

Case Study: Intermittent Access to Web Server



Case Study: Intermittent Access to Web Server



Additional Security: ASA IPS-Module

Cisco IPS Manager Express 6.1 - Demo Mode

File View Tools Help

Home Configuration Event Monitoring Reports Help

Configuration > Corp-IPS > Policies > Signature Definitions > sig0 > Attack

Corp-IPS SFO-Sensor NY-Sensor Branch-ASA-IPS SJ-ASA-IPS Refresh

IPS Policies

- Signature Definitions
 - sig0
 - Active Signatures
 - Adware/Spyware
 - Attack
 - DDoS
 - DoS
 - Email
 - IOS IPS
 - Instant Messaging
 - L2/L3/L4 Protocol
 - Network Services
 - OS
 - Other Services
 - P2P
 - Reconnaissance
 - Releases
 - Viruses/Worms/Trojans
 - Web Server
 - All Signatures
- Event Action Rules
- rules0
- Anomaly Detections
- ad0

Sensor Setup

Interfaces

Policies

Sensor Management

Sensor Monitoring

Edit Actions Enable Disable Restore Default Show Events MySDN Edit Add Delete Clone Export Video Help

Select: All-Attack Filter: Sig ID Filter Clear Signature Wizard

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions	Type	Engine	Retired
						Alert and Log Deny Other			
1000/0	IP options-Bad Option ...	☒	Inform...	75	18	Alert	Default	Atomic IP	No
1003/0	IP options-Provide s,c...	☐	Inform...	100	25	Alert	Default	Atomic IP	Yes
1005/0	IP options-SATNET ID	☐	Inform...	100	25	Alert	Default	Atomic IP	Yes
1006/0	IP options-Strict Sourc...	☒	High	100	100	Alert	Default	Atomic IP	No
1007/0	IPv6 over IPv4	☐	Inform...	100	25	Alert	Default	Atomic IP	No
1101/0	Unknown IP Protocol	☒	Inform...	75	18	Alert	Default	Atomic IP	No
1104/0	IP Localhost Source S...	☒	High	100	100	Alert	Default	Atomic IP	No
1107/0	RFC 1918 Addresses ...	☐	Inform...	100	25	Alert	Default	Atomic IP	No
1108/0	IP Packet with Proto 11	☒	High	100	100	Alert	Default	Atomic IP	No
1200/0	IP Fragmentation Buff...	☒	Inform...	100	25	Alert	Default	Normalizer	No
1201/0	IP Fragment Overlap	☐	Inform...	100	25	Alert	Default	Normalizer	No
1202/0	IP Fragment Overrun ...	☒	High	100	100	Alert	Default	Normalizer	No
1203/0	IP Fragment Overwrit...	☒	High	100	100	Alert	Default	Normalizer	No
1204/0	IP Fragment Missing I...	☒	Inform...	100	25	Alert	Default	Normalizer	No
1205/0	IP Fragment Too Man...	☒	Inform...	100	25	Alert	Default	Normalizer	No
1206/0	IP Fragment Too Small	☒	Low	100	50	Alert	Default	Normalizer	No
1207/0	IP Fragment Too Man...	☒	Inform...	100	25	Alert	Default	Normalizer	No
1208/0	IP Fragment Incomple...	☒	Inform...	100	25	Alert	Default	Normalizer	No
1225/0	Fragment Flags Invalid	☐	High	100	100	Alert	Default	Normalizer	No
1250/0	Packet Bad Length	☒	Medium	100	75	Alert	Default	Normalizer	No
1300/0	TCP Segment Overwrite	☒	High	100	100	Alert	Default	Normalizer	No
1301/0	TCP Session Inactivi...	☒	Inform...	100	25	Alert	Default	Normalizer	No
1302/0	TCP Session Establish...	☒	Inform...	100	25	Alert	Default	Normalizer	No

Total Signatures: 2745 Enabled Signatures: 1161 Signatures in this category: 2527 Enabled in this category: 1069

MySDN (Embedded)

Description:

Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks. The first field of each option in the list consists of an eight bit code field that is broken into three subfields: COPY (Bit 0): Specifies to routers if the option information should be included in fragment headers. CLASS (Bits 1-2): Specifies 1 of 2 valid option classes: Network Control, Debugging NUMBER (Bits 3-7): Specifies one of

Explanation Related Threats

Apply Reset Advanced...

Total EPS:

Conclusion



ASA Advanced Firewall Summary

- Make yourself familiar with ASA Firewall portfolio and bundles
- Use Advanced Firewall-Features and Functions to optimize your Security-Policy
- Learn how to utilize additional ASA Security-Elements like Intrusion-Prevention and SSL-VPN

Online Learning Modules on CCO

- Great way to learn about new features on the ASA
- Located on CCO (no Login Required !)
- From <http://www.cisco.com/go/asa> select:
[Support] -> Training Resources
 - >Online Learning Modules
 - >Examples:
Active/Standby Failover for ASA5500
Modular Policy Framework on ASA 5500
and more

