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 5580-40

ASA 5580-20

ASA 5550

ASA 5540

ASA 5520

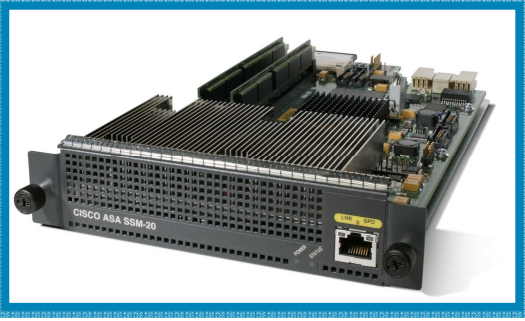
ASA 5510

ASA 5505

Teleworker | Branch Office | Internet Edge | Campus | Data Center

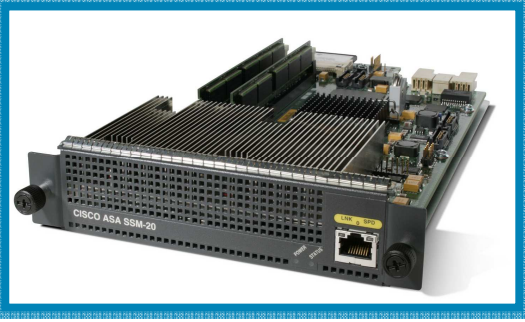
Wide-Range of Cisco ASA 5500 Series Security Service Modules (SSMs)

IPS Security Services Module (AIP-SSM)



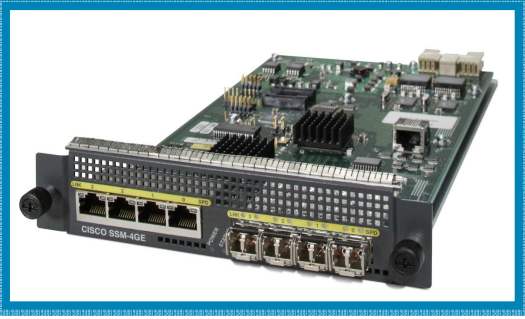
- Provides **full-featured IPS and IDS services** for protection of critical network assets
- Available in 3 models: SSM-10, SSM-20, SSM-40
- Delivers up to 650 Mbps of IPS throughput

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

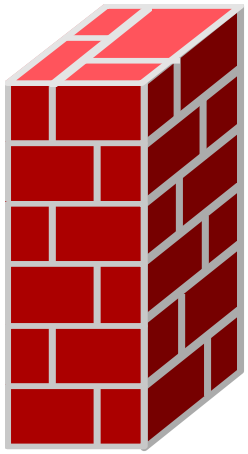
High Availability

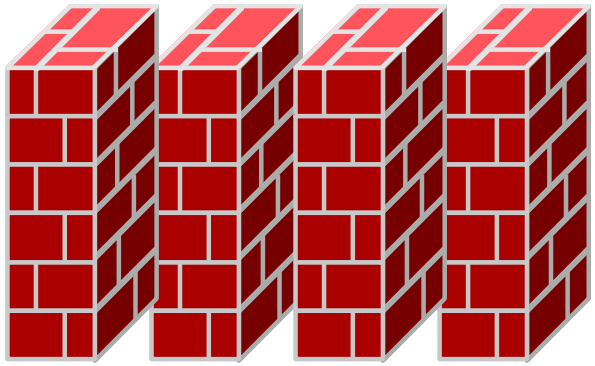
Different people, different opinions ...

- „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)

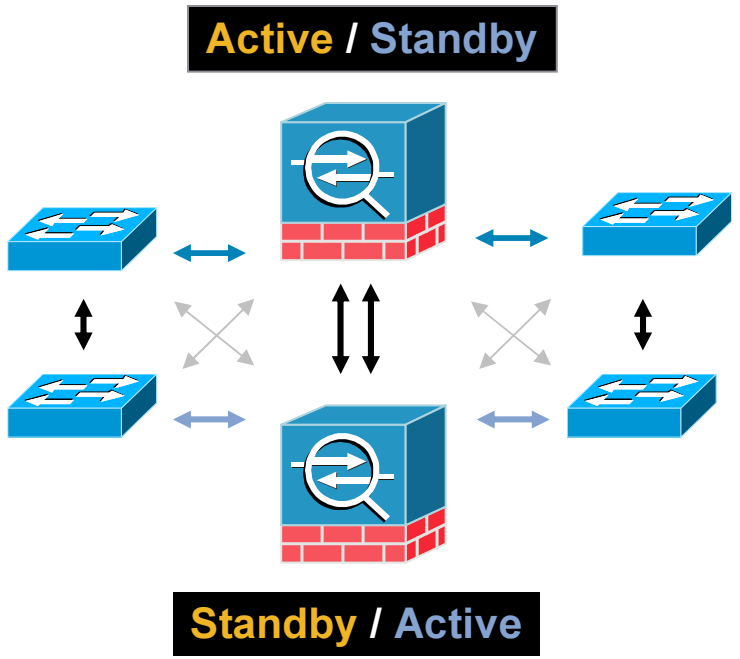




- Virtualization is a licensed feature
- Within the ASA a Virtual-Firewall-Instance is called a “Context”

Redundant Chassis

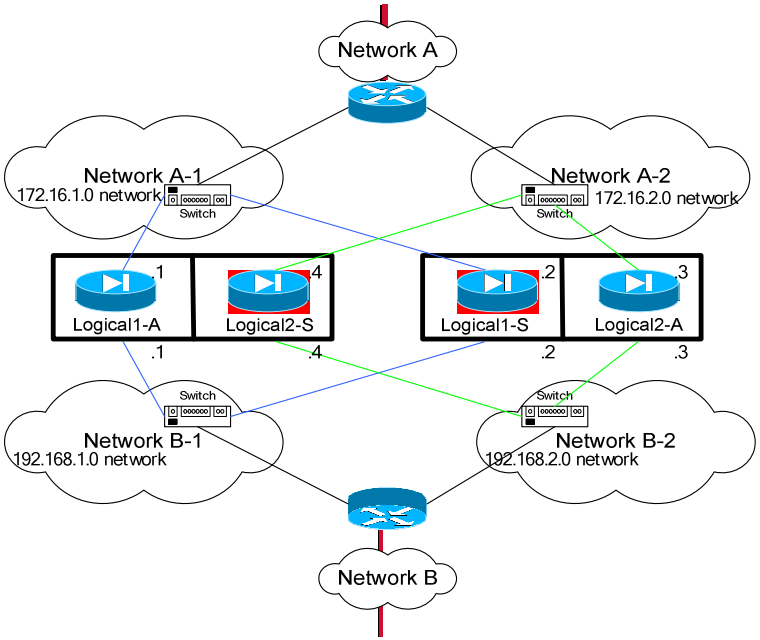
- 2x Identical chassis
- Identical SW-Releases
- Identical Service-Modules
- Dedicated Sync-Interfaces for „Config“ & „Session-State“ recommended
- „State“-Interface speed should follow „Data-Interface“ speeds*
- Cross-Over cable between ASA not recommended
- From 5505 to 5580 (Plus license on smaller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

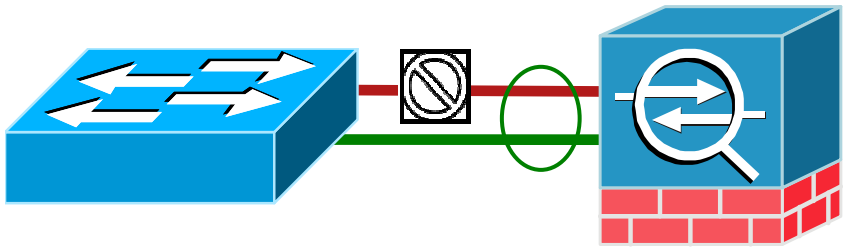
- Single Chassis Option
- Logical Interface represents physical interface-pair
- All configuration refers to Logical-Interface

  Nameif
  Security-Level
  IP-Address

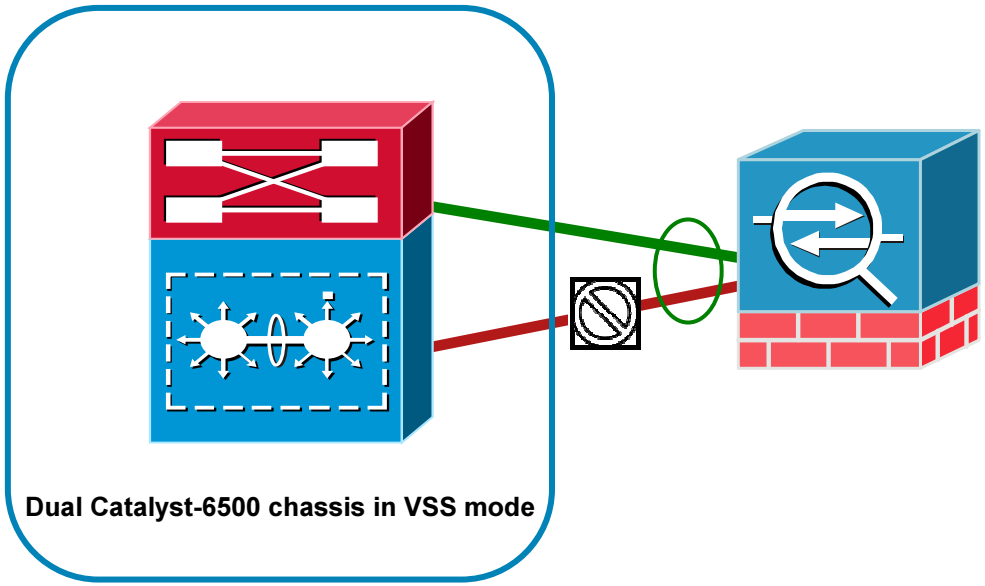
- Failover is less than 500ms
- Passes traffic when member interface is enabled
- Active interface can be moved between „pairs“
- Maximum 8 interface pairs

*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

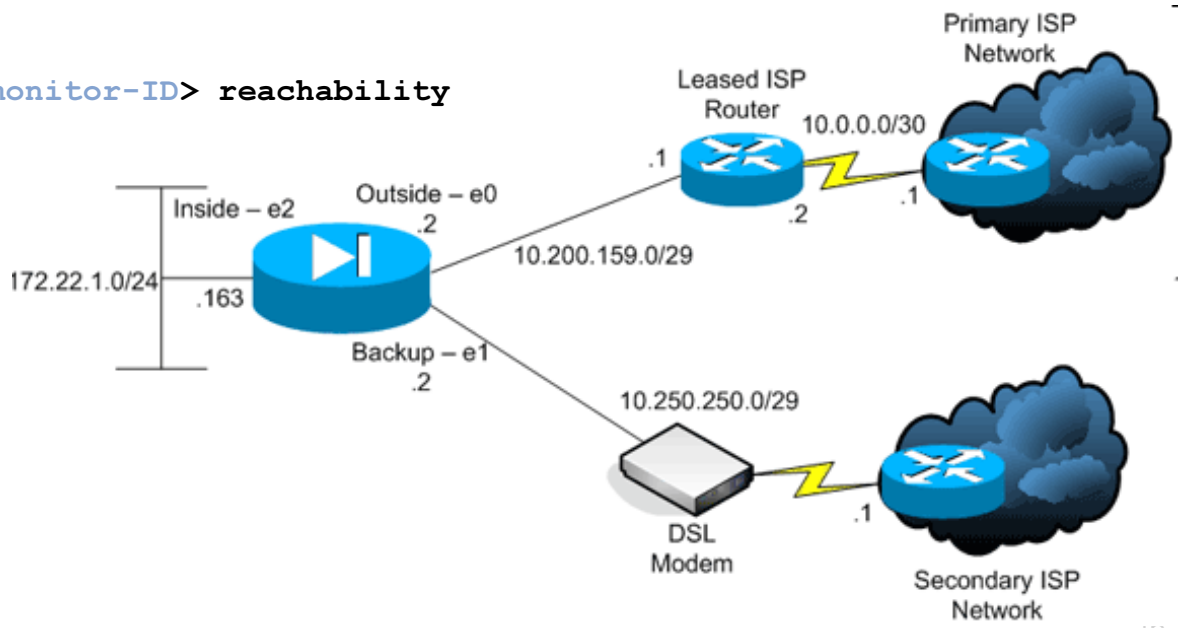
```
route outside 0.0.0.0 0.0.0.0 10.200.159.1 1 track <track-ID>
route backup  0.0.0.0 0.0.0.0 10.250.250.1 254
```

- 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

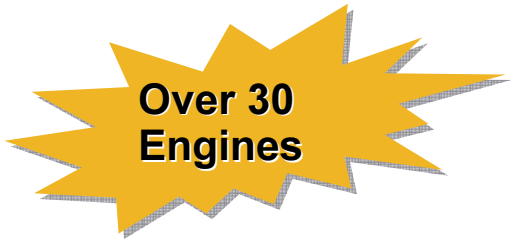
- Application and protocol-aware inspection services provide strong application-layer security and detailed policy controls
- Perform conformance checking, state tracking, security checks, NAT/PAT, dynamic port allocation, and offer a wide range of controls for businesses to set application-layer policies

Media/Voice over IP

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

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

Database/OS Services

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

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

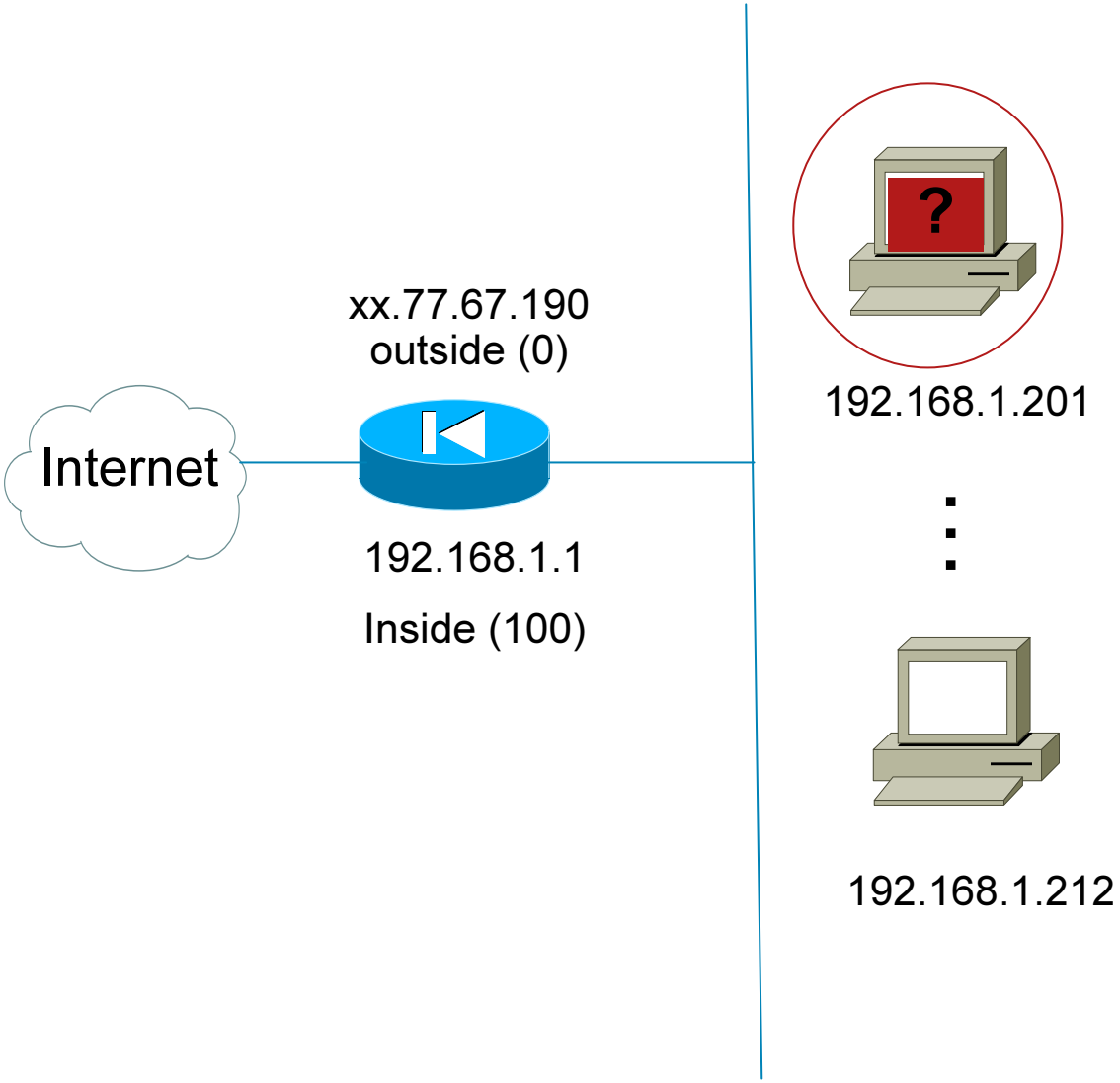
Case Study: Block GoToMyPC Application

- Problem:

After implementing filtering, we noticed host 192.168.1.201 talking via tcp/80 to Go2myPC.com

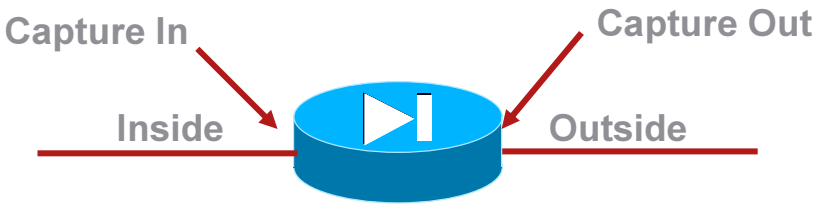
- Goal:

Using HTTP inspection engine to implement a policy that blocks users from using that service, while allowing access to tcp/80 for allowed traffic

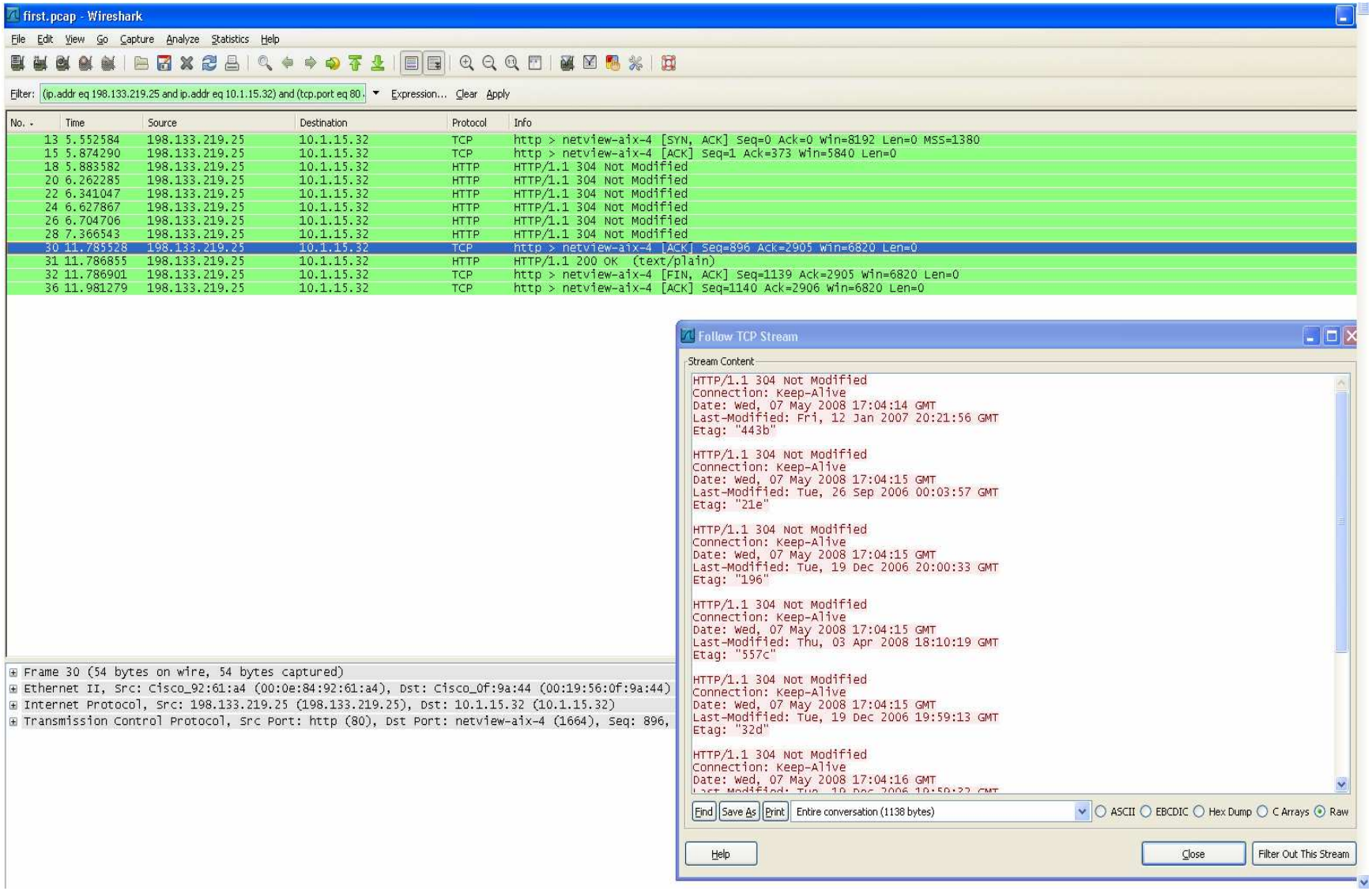


ASDM-Tool: Packet Capture

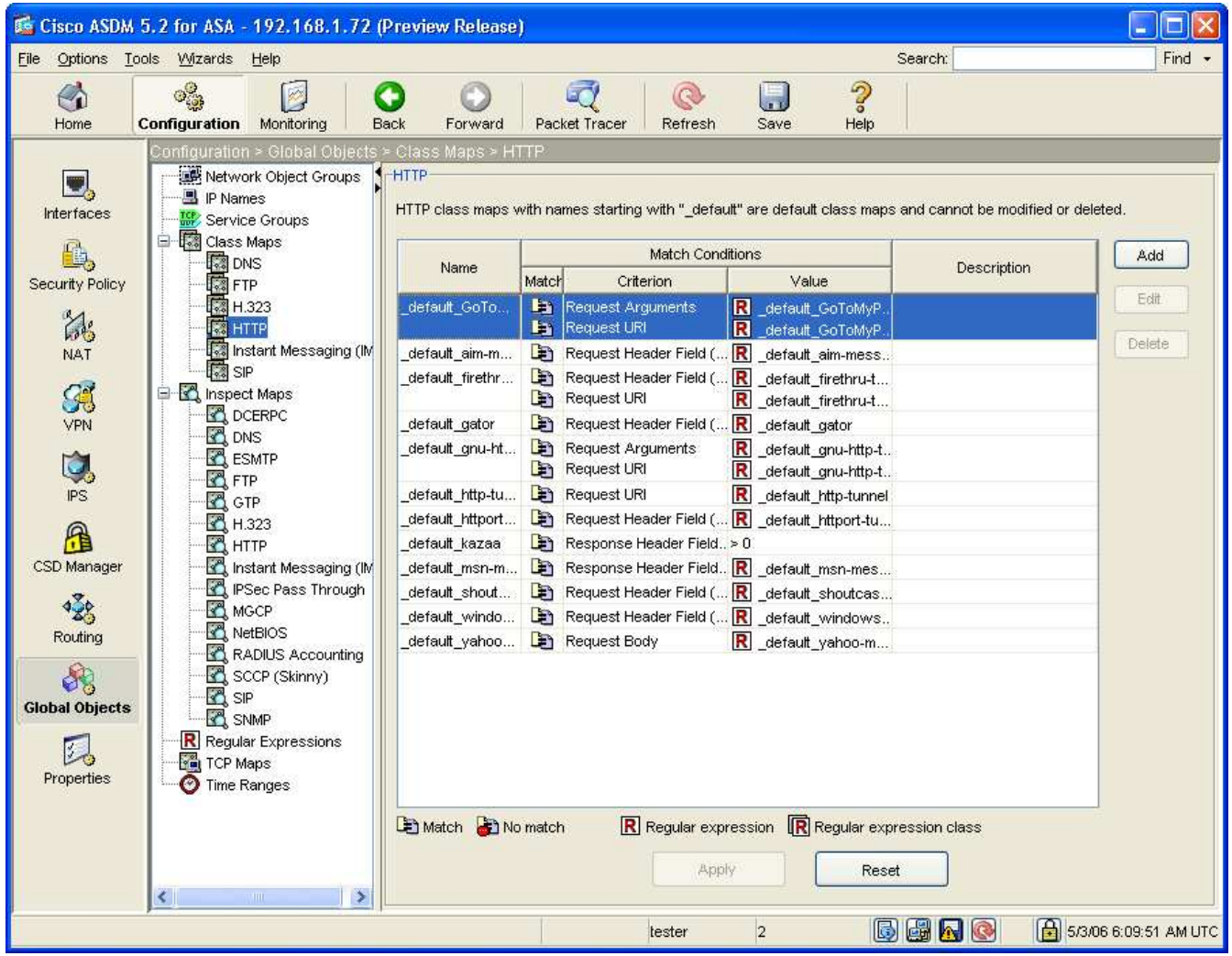
- Traffic can be captured both before and after it passes through the firewall; one capture on the inside interface, one capture on the outside interface
- Capture buffer saved in RAM (default size 512KB)
- Default is to stop capturing when buffer is full
- Default packet length is 1518 bytes
- Copy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



Capture viewed in Wireshark

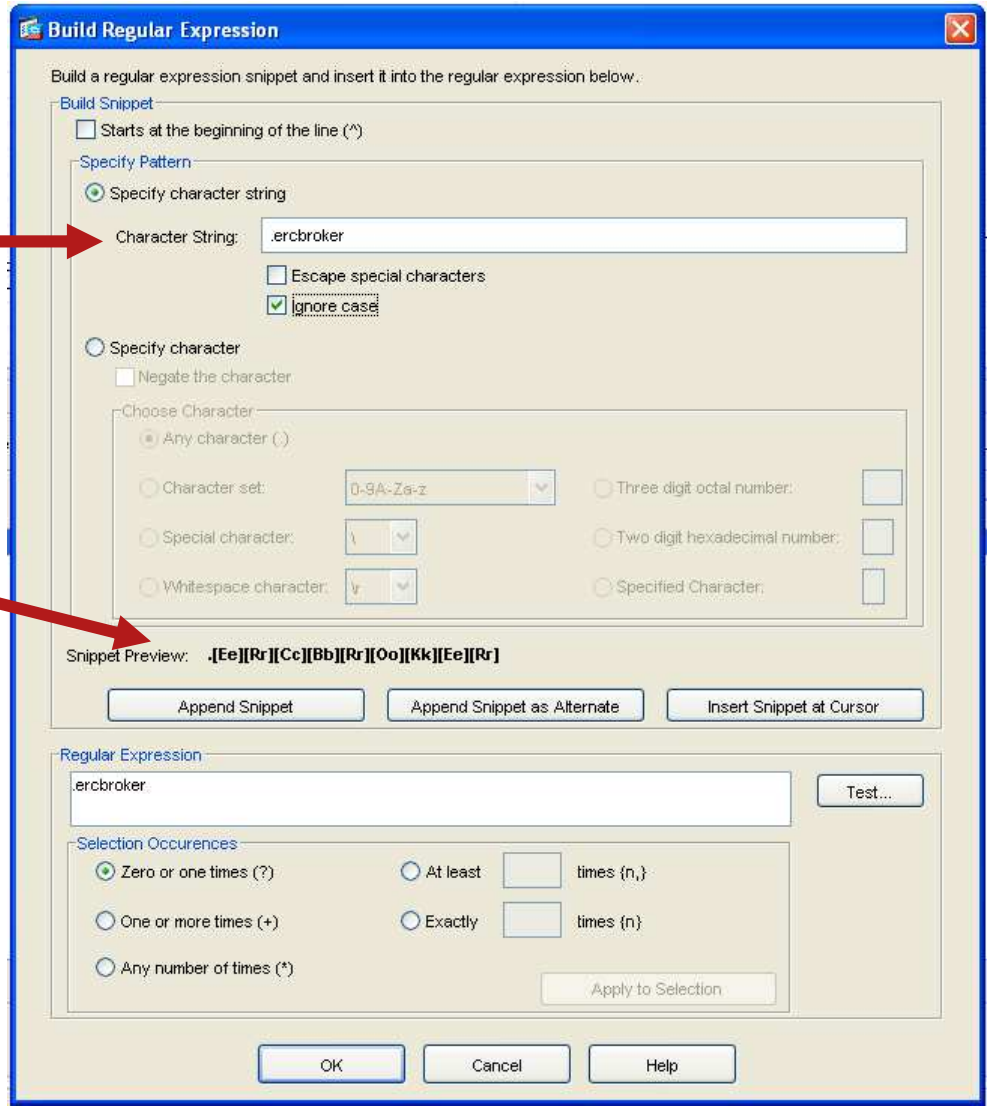


ASDM-Tool: HTTP Inspection

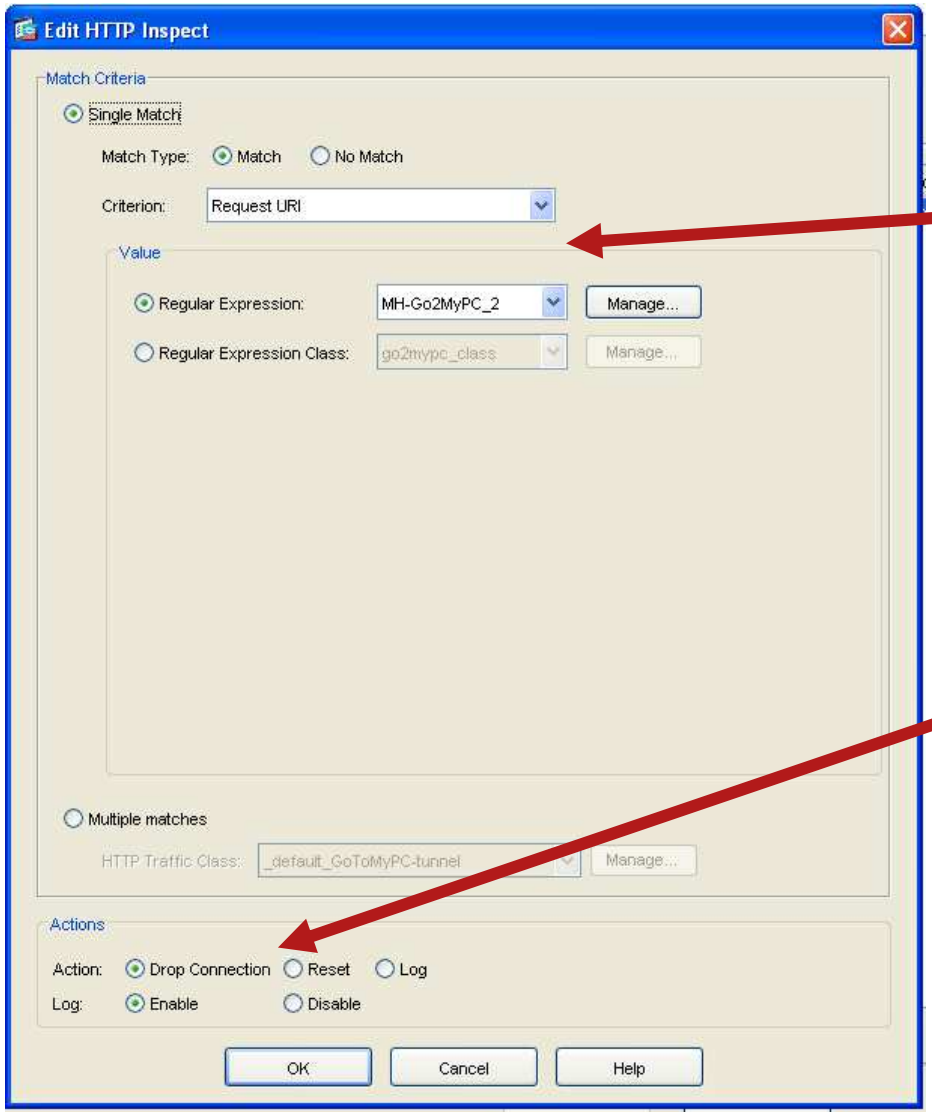


ASDM-Tool: Regex Build Wizard

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

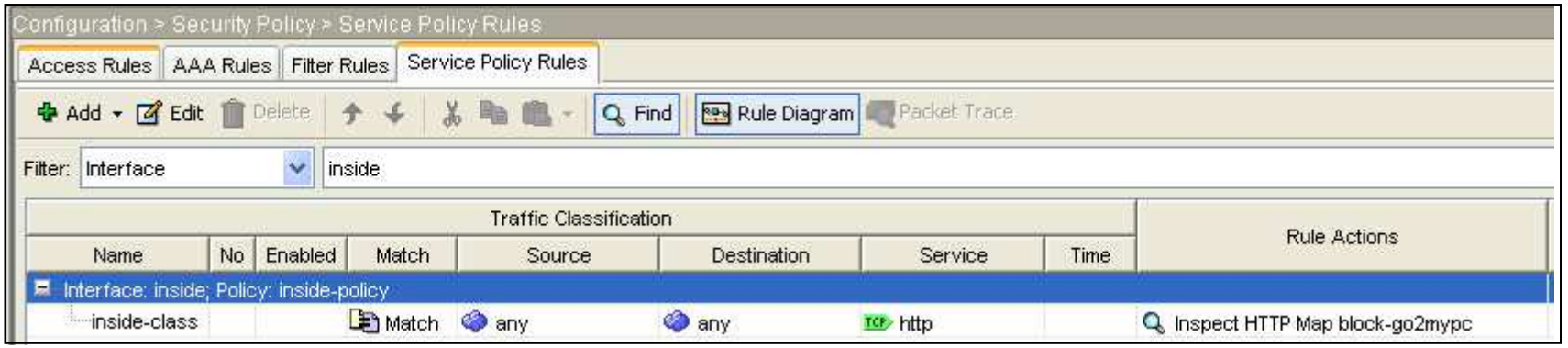


Final HTTP Inspect



- 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



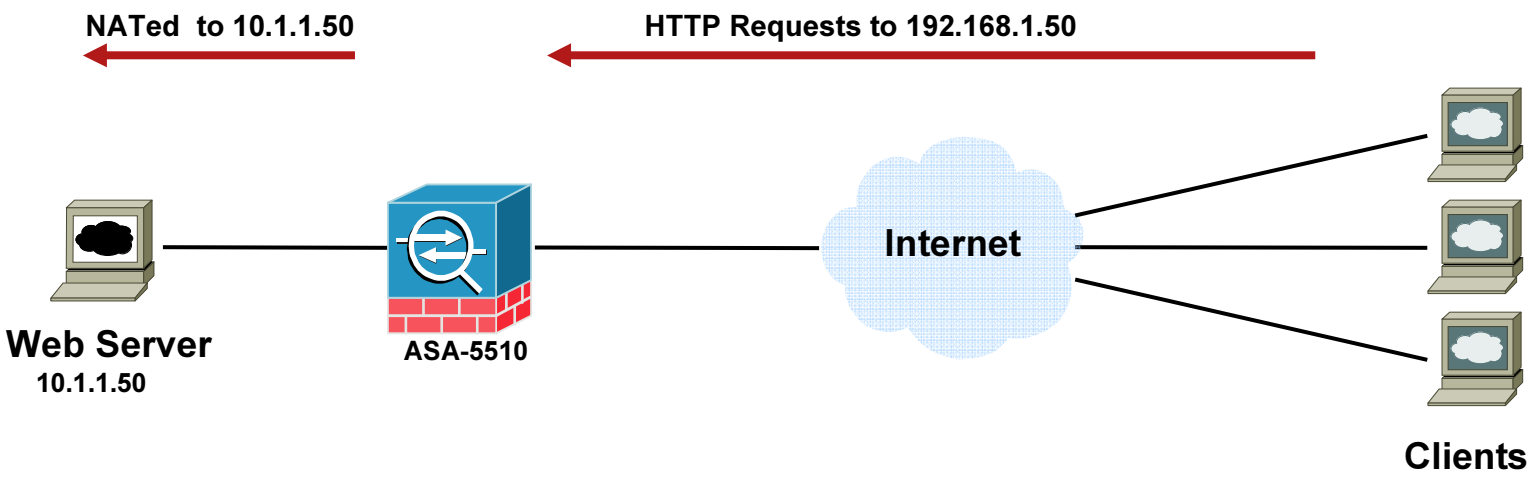
- In this example, note that the service policy is only inspecting tcp/80. All other traffic is not bound to this particular policy
- We could have also selected more granular source and destination L3 addresses, if necessary

Connection Management

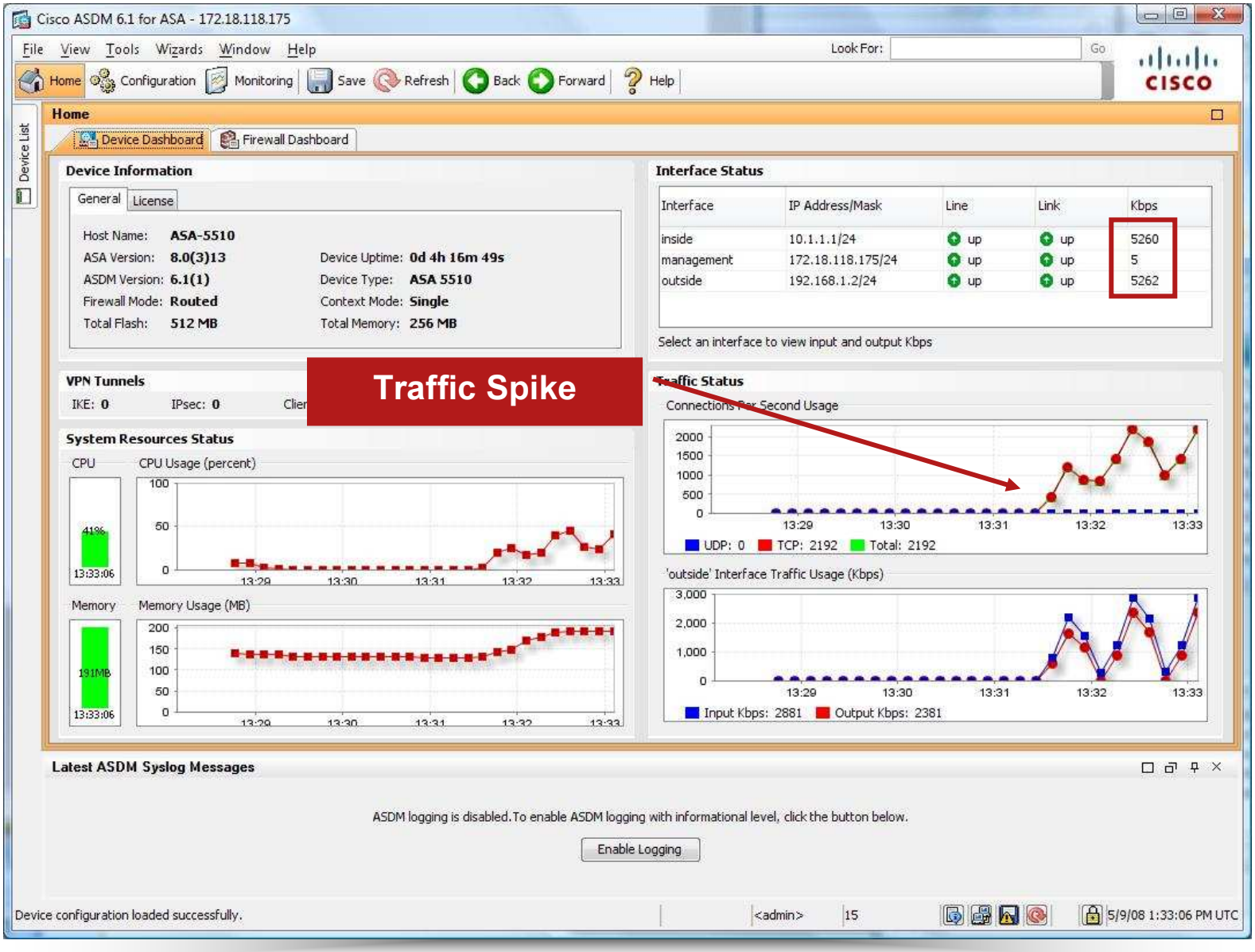
Case Study: Intermittent Access to Web Server

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

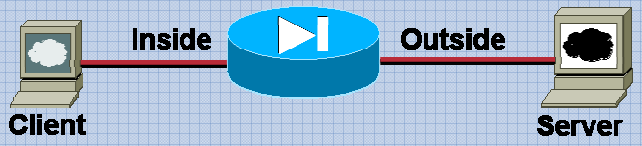
```
ASA# show conn detail
2 in use, 64511 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, 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

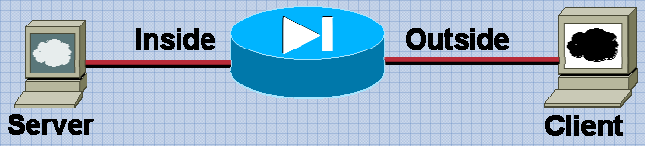
Outbound Connection

TCP Flags		FW Flags
SYN	→	saA
SYN+ACK	←	A
ACK	→	U
Inbound Data	←	UI
Outbound Data	→	UIO
FIN	→	Uf
FIN+ACK	←	UfFR
ACK	→	UfFRr



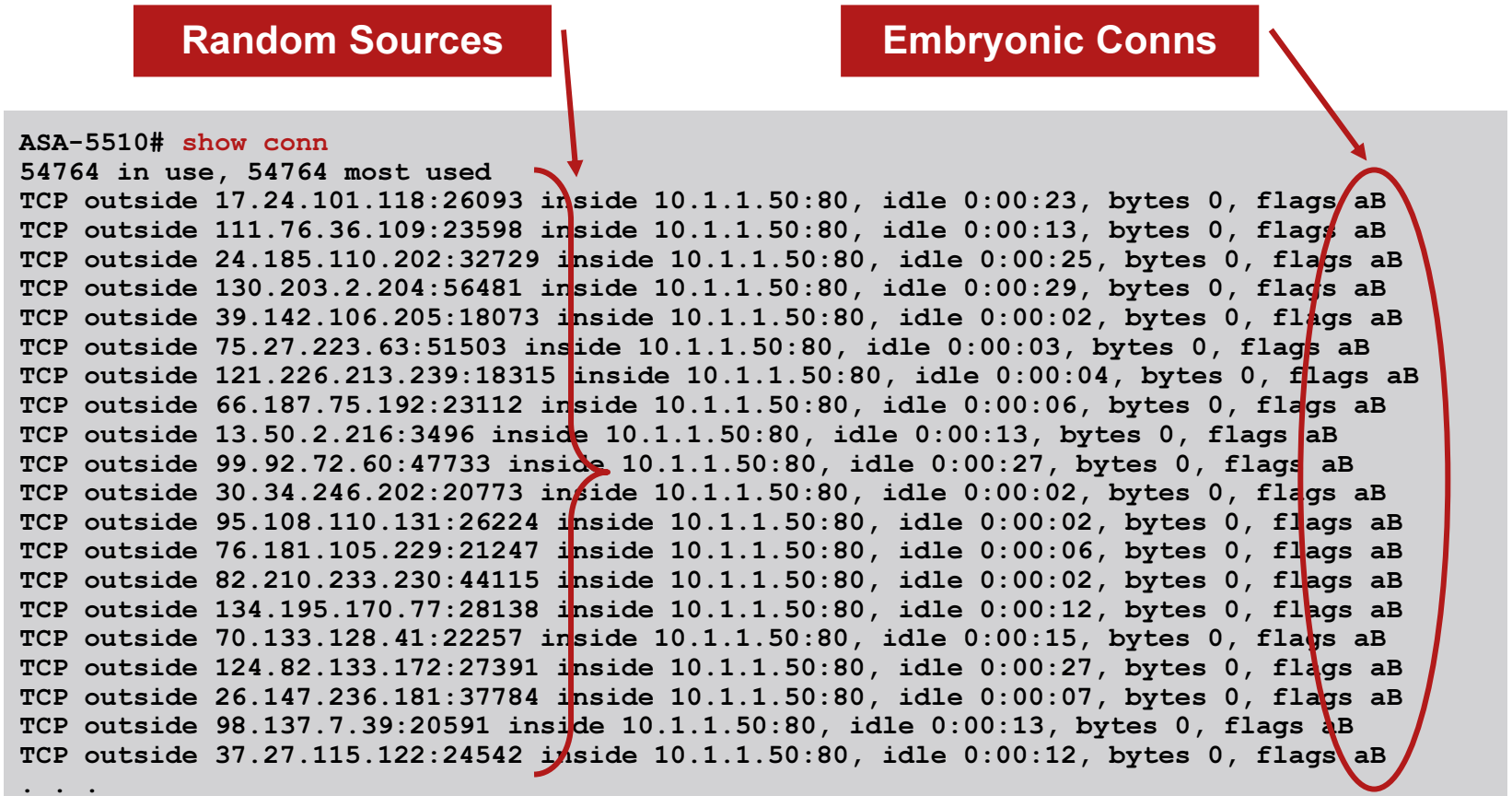
Inbound Connection

TCP Flags		FW Flags
SYN	←	SaAB
SYN+ACK	→	aB
ACK	←	UB
Inbound Data	←	UIB
Outbound Data	→	UIOB
FIN	←	UBF
FIN+ACK	→	UBfFr
ACK	←	UBfFRr

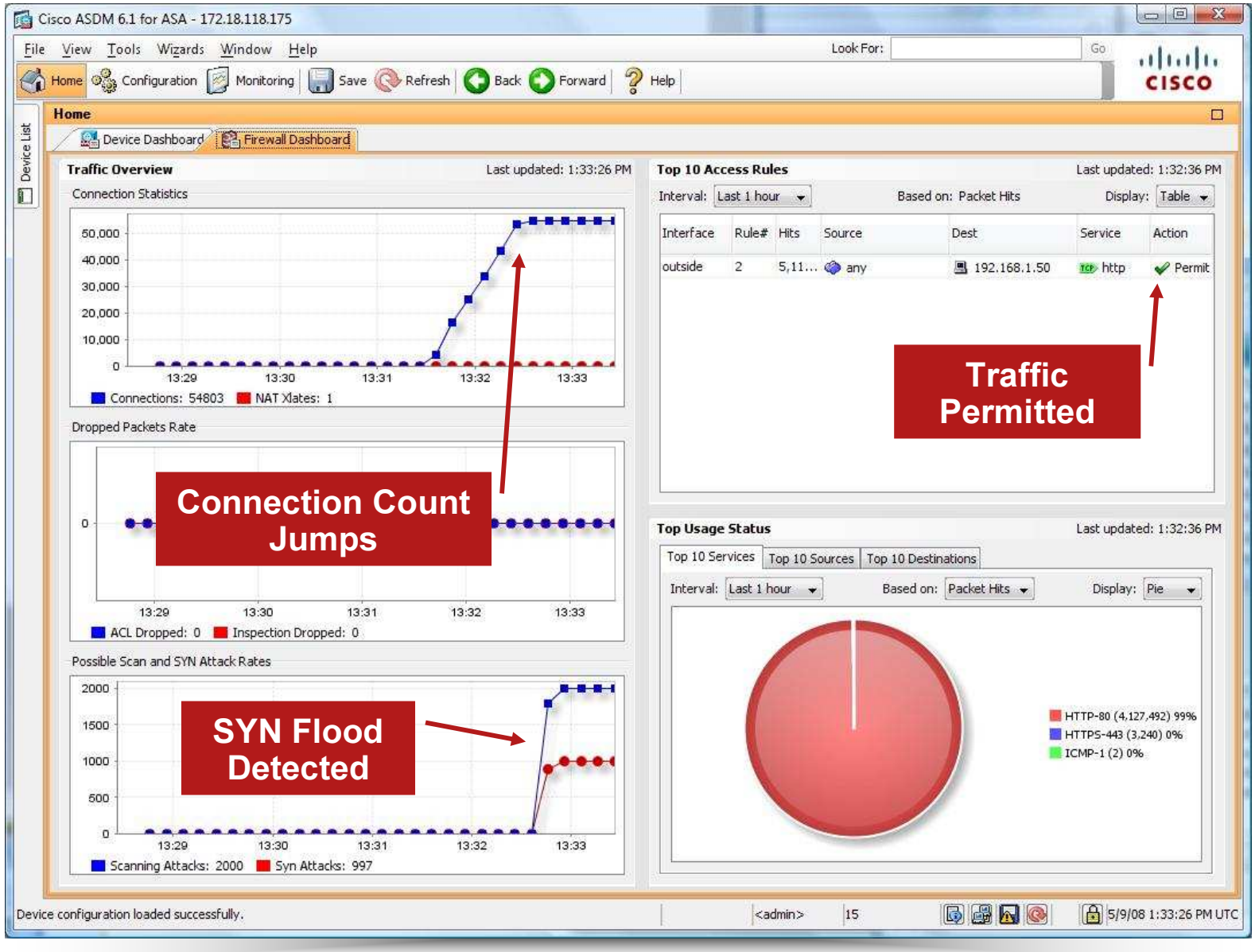


Case Study: Intermittent Access to Web Server

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



Case Study: Intermittent Access to Web Server

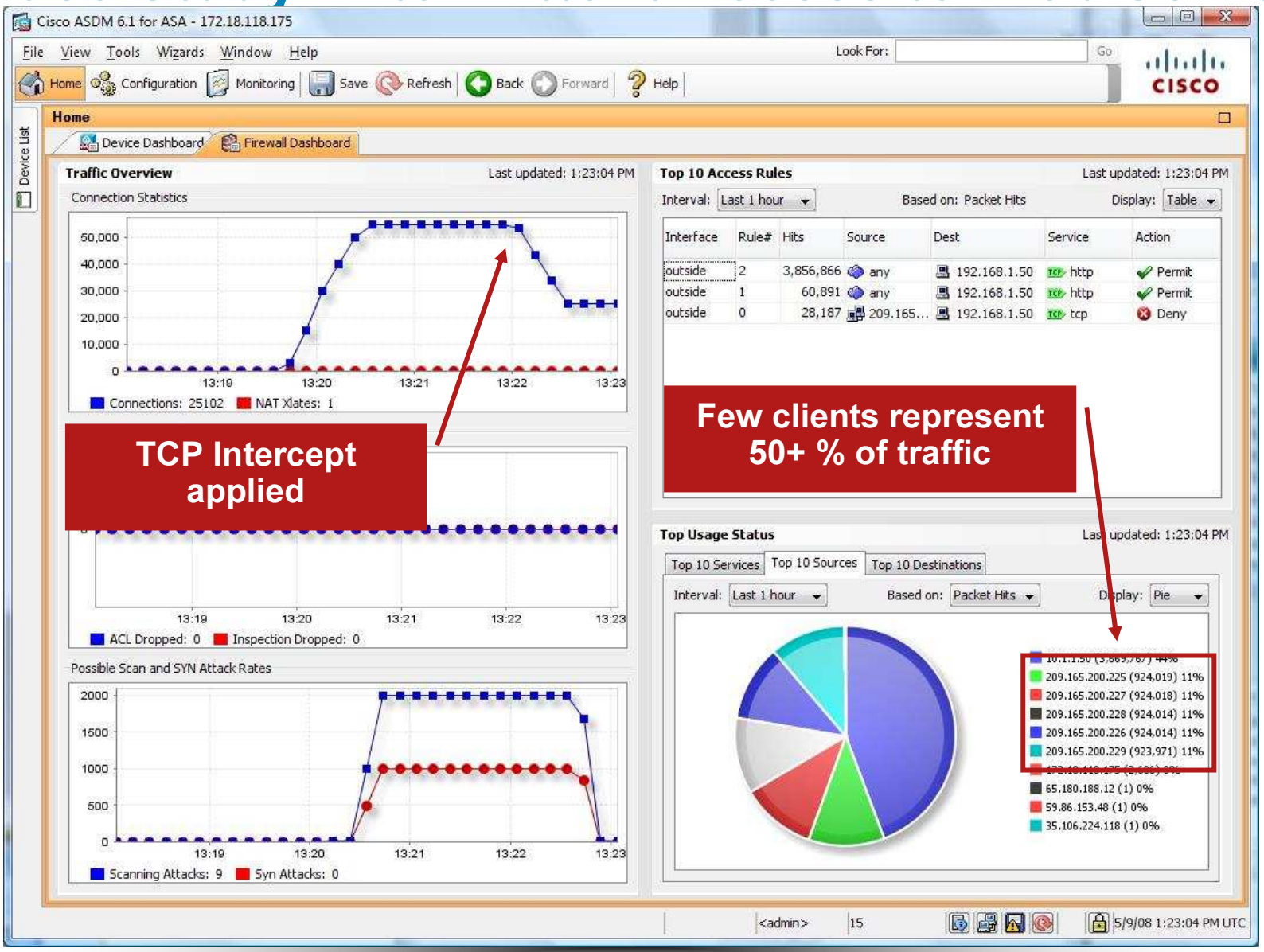


Case Study: Intermittent Access to Web Server

- 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

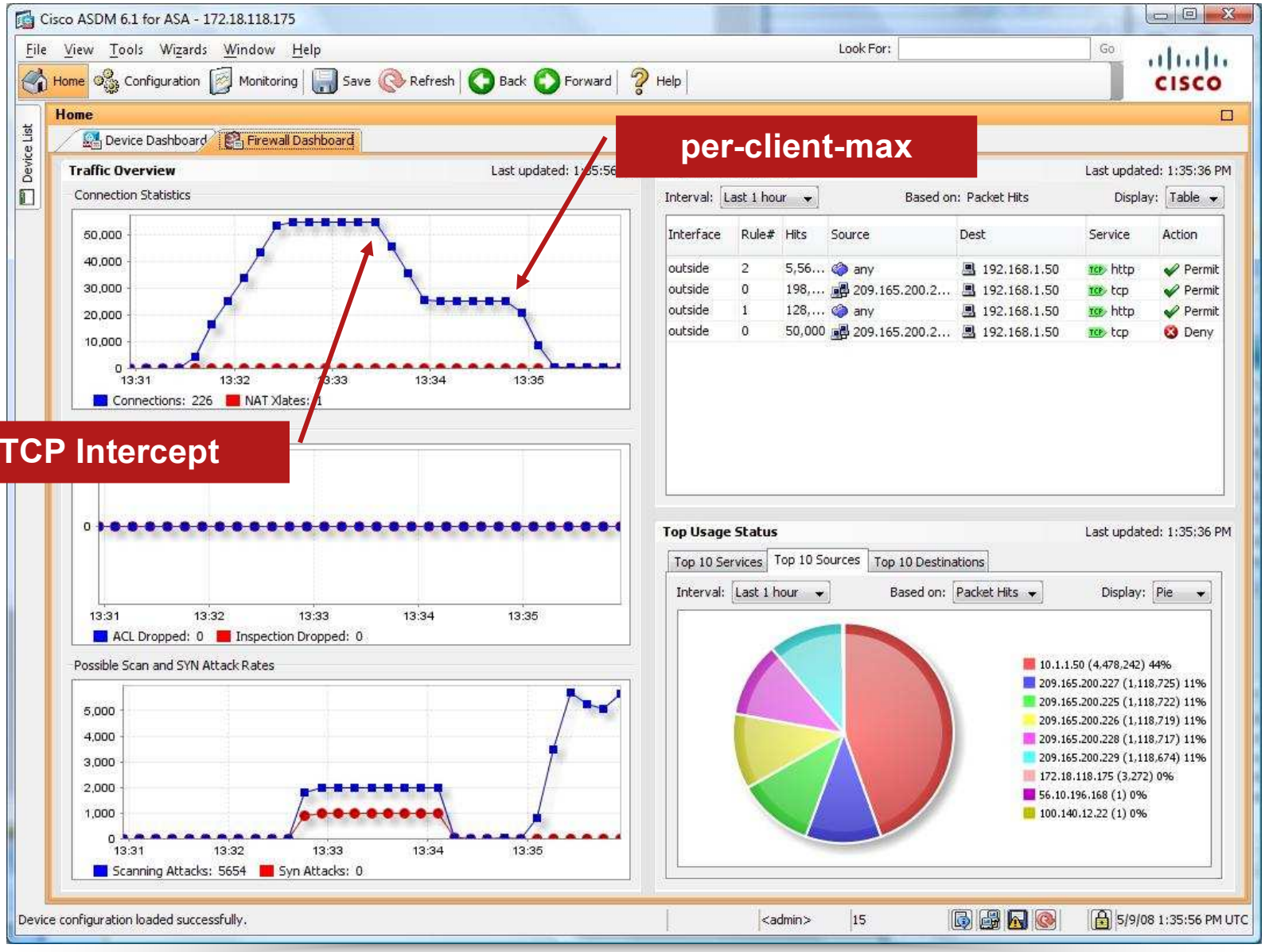


Case Study: Intermittent Access to Web Server

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

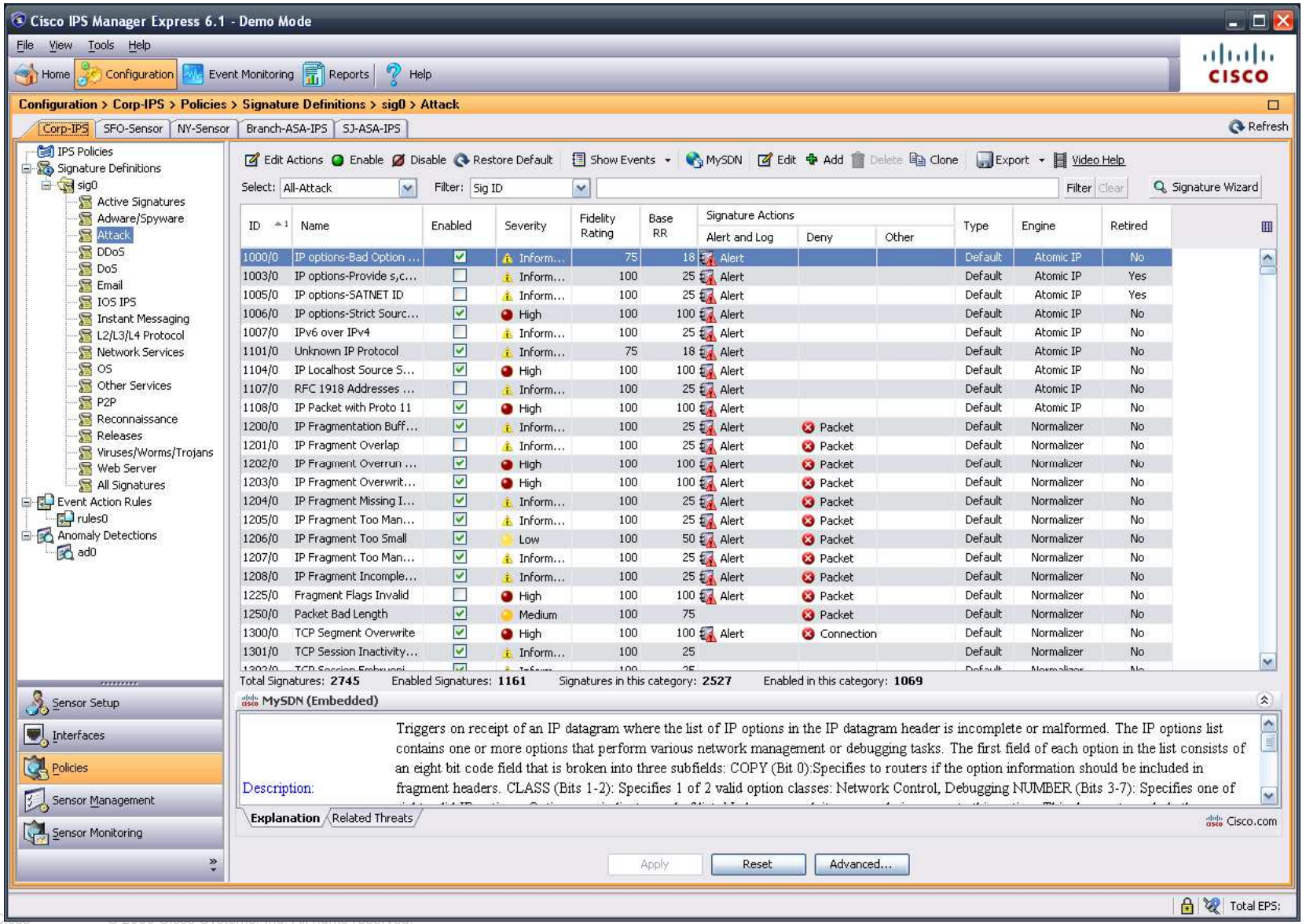
```
access-list 140 extended permit tcp any host 192.168.1.50 eq www
!
class-map protect
 description Protect web server from attacks
 match access-list 140
!
policy-map interface_policy
 class protect
  set connection embryonic-conn-max 100 per-client-max 25
!
service-policy interface_policy interface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

Case Study: Intermittent Access to Web Server



Case Study: Intermittent Access to Web Server

Additional Security: ASA IPS-Module



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