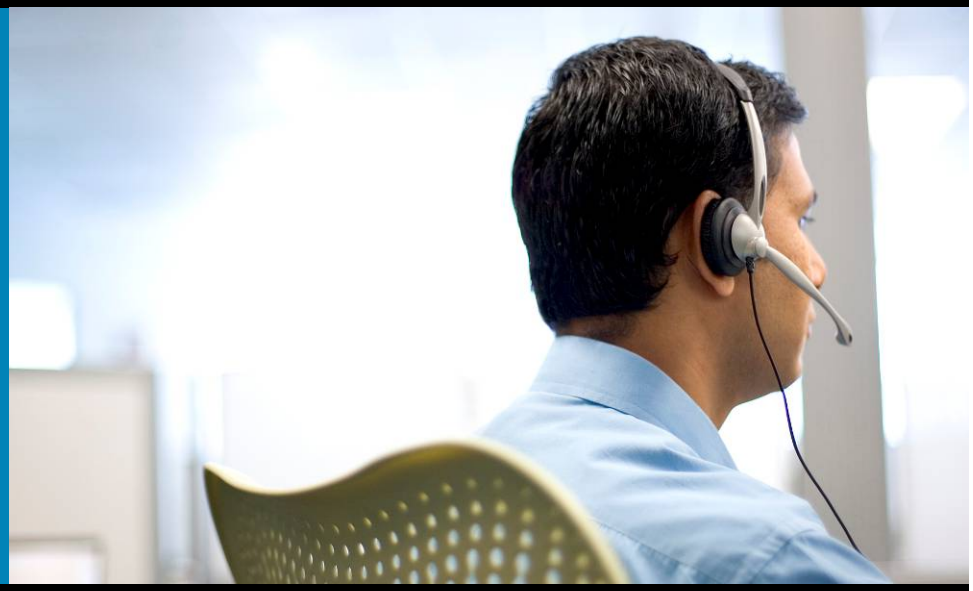
CS-MARS



Erik Lenten

Technical Marketing Engineer

Objectives

- Give an overview of CS-MARS product
- Explain how to deploy CS-MARS
- Explain the usage of NetFlow for CS-MARS

Security Operations/Reactions Today

Always Too Late

Network Operations

Action Steps:
1. Alert
2. Investigate
3. Mitigate

Security Operations

10K Win, 100s UNIX

Router/Switch

VPN

Authentication Servers

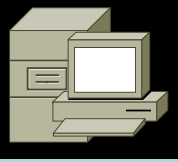
Collect Network Diagram Read and Analyze Tons of Data Repeat

Firewall

IDS/IPS

Anti-Virus

Vulnerability Scanners



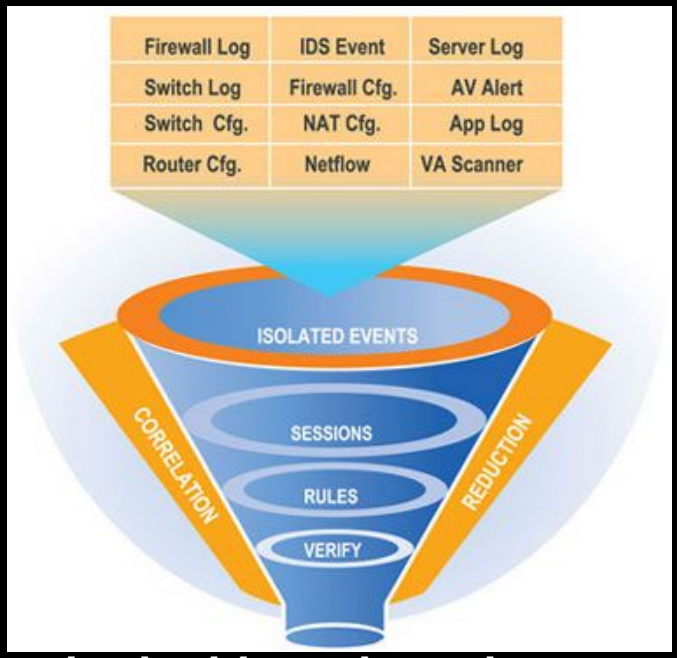
Security Knowledge Base

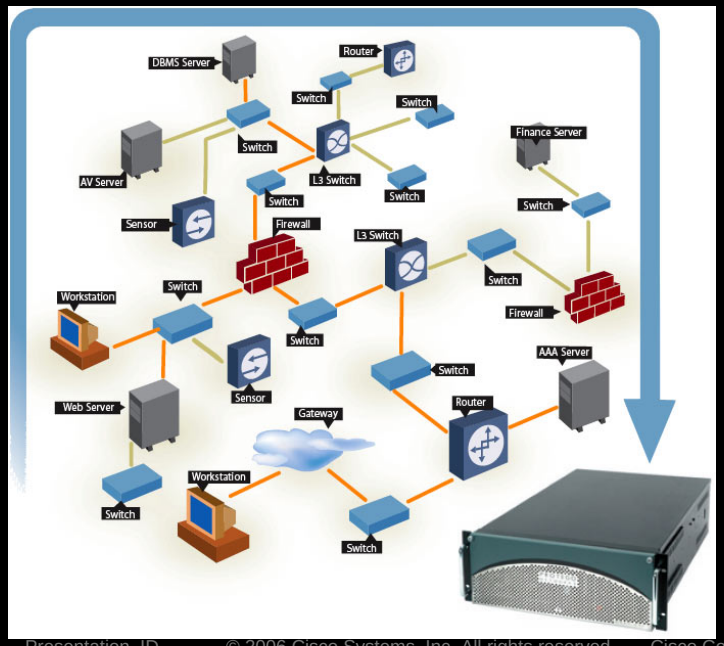
Mitigation, Analysis, and Response System (MARS) *Next Generation SIM/STM*

- Leverage YOUR existing investment to build "pervasive security"
- Correlate data from across the Enterprise

  NIDS, Firewalls, Routers, Switches, CSA

  Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs, Multi-Vendor
- Rapidly locate and mitigate attacks





- Key Features

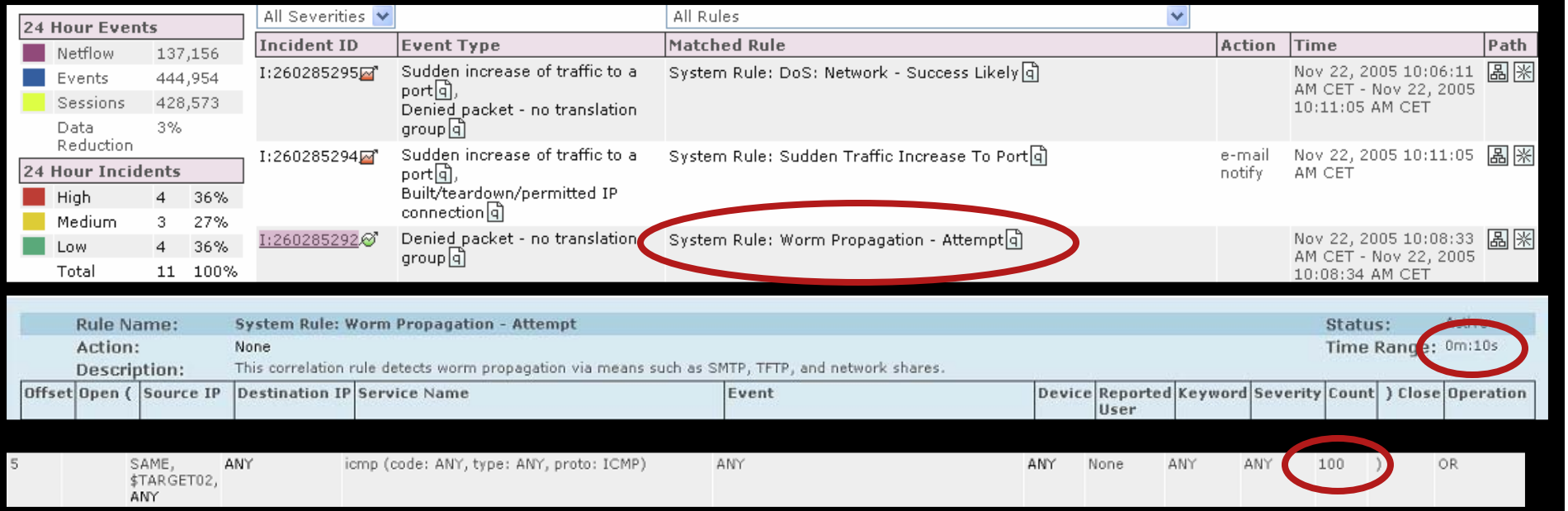
  Determines security *incidents* based on device *messages*, *events*, and "*sessions*"

  Incidents are topologically aware for visualization and replay

  Mitigation on L2 ports and L3 chokepoints

  Efficiently scales for real-time use across the Enterprise

Firewall Example



24 Hour Events	
Netflow	137,156
Events	444,954
Sessions	428,573
Data Reduction	3%

24 Hour Incidents		
High	4	36%
Medium	3	27%
Low	4	36%
Total	11	100%

All Severities | All Rules

Incident ID	Event Type	Matched Rule	Action	Time	Path
I:260285295	Sudden increase of traffic to a port, Denied packet - no translation group	System Rule: DoS: Network - Success Likely		Nov 22, 2005 10:06:11 AM CET - Nov 22, 2005 10:11:05 AM CET	
I:260285294	Sudden increase of traffic to a port, Built/teardown/permitted IP connection	System Rule: Sudden Traffic Increase To Port	e-mail notify	Nov 22, 2005 10:11:05 AM CET	
I:260285292	Denied packet - no translation group	System Rule: Worm Propagation - Attempt		Nov 22, 2005 10:08:33 AM CET - Nov 22, 2005 10:08:34 AM CET	

Rule Name: System Rule: Worm Propagation - Attempt
Status:
Action: None
Time Range: 0m:10s
Description: This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares.

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
5		SAME, $TARGET02, ANY	ANY	icmp (code: ANY, type: ANY, proto: ICMP)	ANY	ANY	None	ANY	ANY	100	)	OR

Denied packet - no translation group	10.1.1.246	0	10.1.61.1
Denied packet - no translation group	10.1.1.246	0	10.1.61.2
Denied packet - no translation group	10.1.1.246	0	10.1.61.3
Denied packet - no translation group	10.1.1.246	0	10.1.61.4

- 100 ICMP messages from the same source within ten seconds must mean something is wrong
- Have IDS/IPS functionality with just FW logs

CS-MARS: “Command and Control”

PROTEGO NETWORKS

SUMMARY | INCIDENTS | QUERY / REPORTS | RULES | MANAGEMENT | ADMIN | HELP

Dashboard | Network Status | My Reports (Trending)

SUMMARY | Version: 2.5 — Login: Administrator, Administrator (pnadmin) :: Logout :: Sep 8, 2004 12:50:43 PM PDT :: Activate

Page Refresh Rate

15 minutes

24 Hour Events

Netflow	38,112	
Events	669,661	
Sessions	384,514	
Data Reduction	42%	

24 Hour Incidents

High	185	25%
Medium	102	14%
Low	440	60%
Total	727	100%

All False Positives

To be confirmed	376,003	55%
System determined	300,620	44%
Logged	37	0%
Dropped	0	0%
Total	676,660	100%
User confirmed	2,051	

To-do List

No Escalated Incidents

My Reports

Activity: All Sessions - Top Destination Ports by Bytes (Normal)

Activity: All Sessions - Top Destinations by Bytes (Normal)

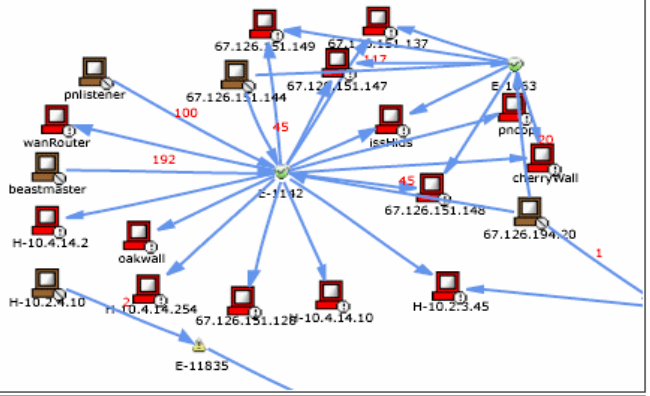
Activity: Denies - Top Destination Ports (Trend)

Recent Incidents All Severities

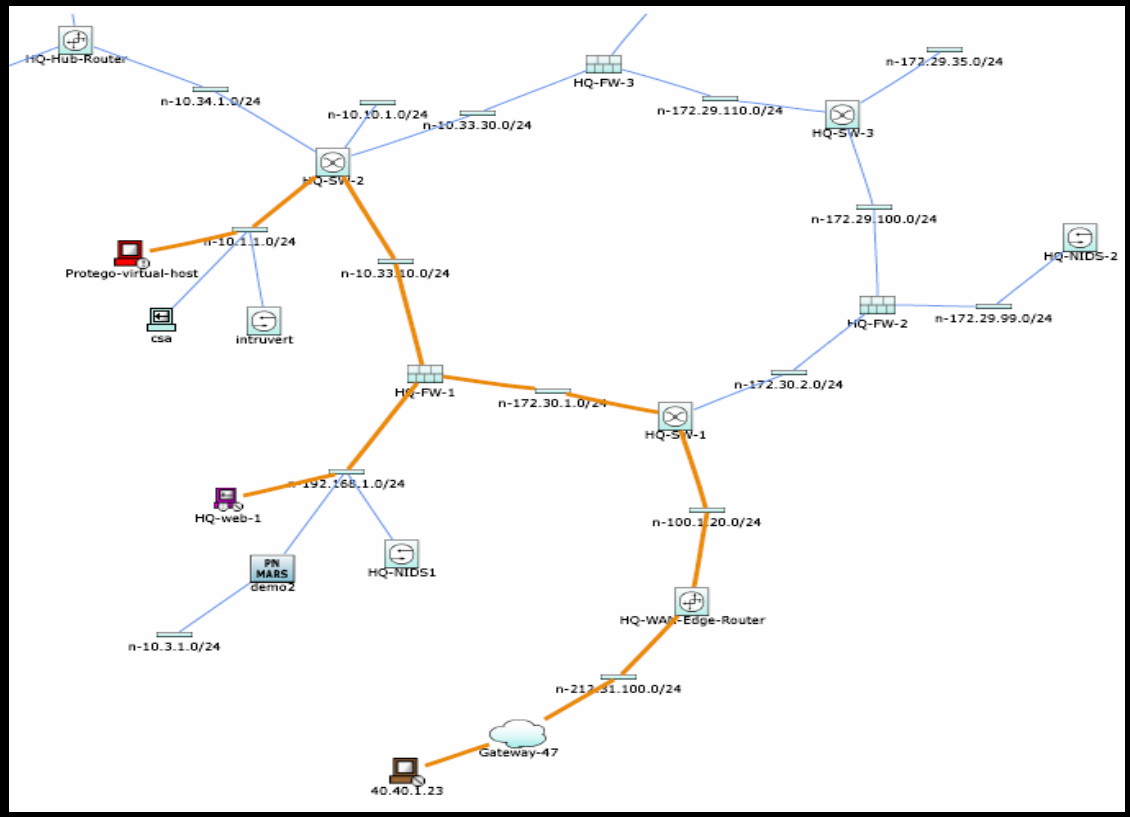
Incident ID	Event Type	Matched Rule	Action	Time	Path
I:426539035	Deny packet due to security policy	System Rule: Network Errors - Likely Routing Related		Sep 8, 2004 12:40:37 PM PDT - Sep 8, 2004 12:50:15 PM PDT	
I:426539033	Deny packet due to security policy, Built/teardown/permitted IP connection	System Rule: Worm Propagation - Attempt		Sep 8, 2004 12:37:52 PM PDT - Sep 8, 2004 12:47:41 PM PDT	
I:426539031	Deny packet due to security policy	System Rule: Network Errors - Likely Routing Related		Sep 8, 2004 12:30:22 PM PDT - Sep 8, 2004 12:40:04 PM PDT	
I:426539028	Deny packet due to security policy, Deny connection - no xlate, Built/teardown/permitted IP connection	System Rule: Worm Propagation - Attempt		Sep 8, 2004 12:28:00 PM PDT - Sep 8, 2004 12:37:11 PM PDT	
I:426539030	Deny packet due to security policy, Deny connection - no xlate, Built/teardown/permitted IP connection	TEST		Sep 8, 2004 12:32:52 PM PDT - Sep 8, 2004 12:32:56 PM PDT	

HotSpot Graph — Full Topo Graph | Large Graph | Help

Attack Diagram — Large Graph | Help



CS-MARS "Connect the Dots"



SureVector™ Analysis

Visible and accurate attack path

Drill-down, full incident and raw event details

Pinpoint the true sources of anomalous and attack behavior

More complete and accurate story

CS-MARS “Leveraged Mitigation”

- **Use control capabilities within your infrastructure**
  - **Layer 2/3 attack path is clearly visible**
  - **Mitigation enforcement devices are identified**
  - **Exact mitigation command is provided**

Enforcement Device: **switch_server**, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch-IOS 12.2	Protego Networks MARS 1.0 on pnvalis		N/A		

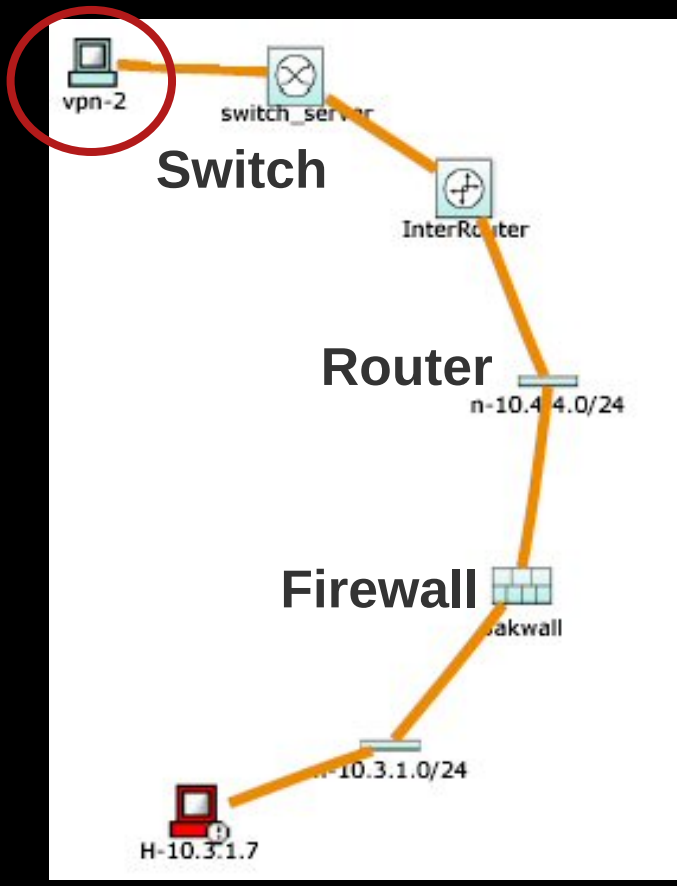
Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time

Recommended Policy/Command

```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```

Push Cancel



CS-MARS
“Compliance Reports”

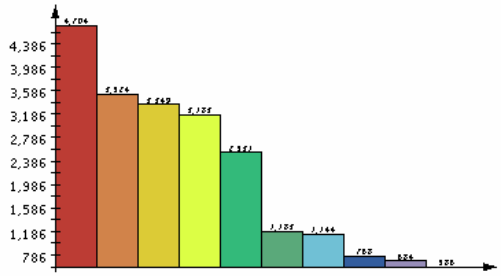
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

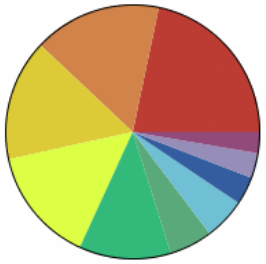
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

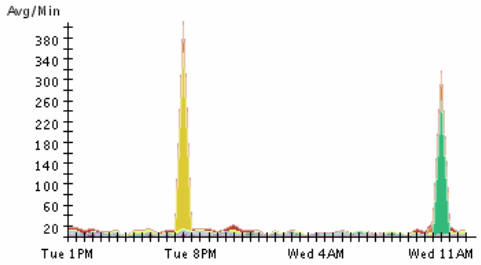
Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

Keywords: [None]







Rank		Count (# of sessions)	Raw Destination Port
	1	4704	445
	2	3524	80
	3	3349	26686
	4	3183	135
	5	2531	47683
	6	1183	1026
	7	1144	0
	8	768	139
	9	684	9898

Full Spectrum Product Line

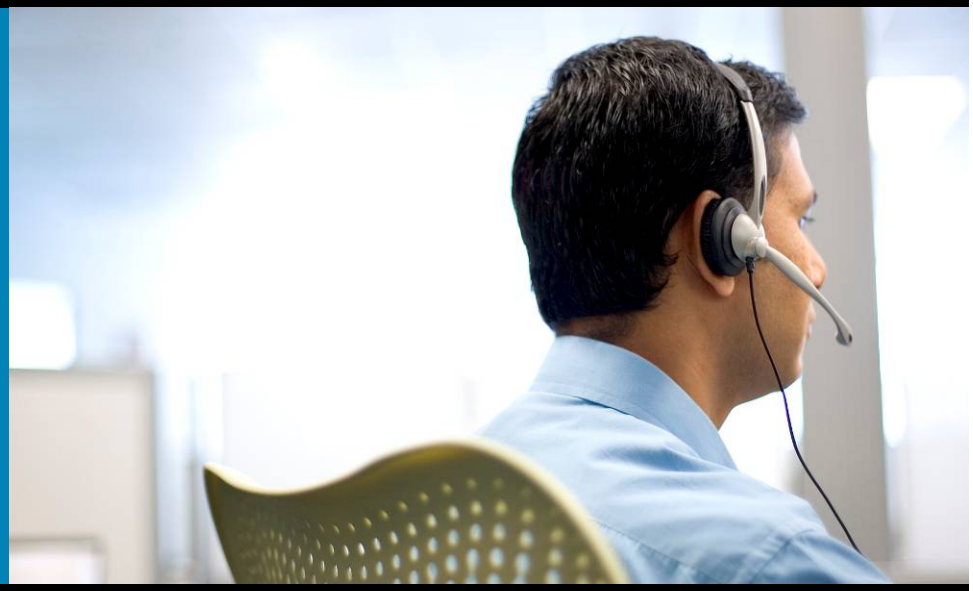
CS-MARS Model	20R	20	50	100e	100	200	Global Controller
Events/Sec	50	500	1,000	3,000	5,000	10,000	N/A
NetFlow Flows/Sec	1,500	15,000	25,000	75,000	150,000	300,000	N/A
RAID Storage	120GB	120GB	120GB	750GB	750GB	1TB	1TB
Rack Size	1 RU	1 RU	1 RU	3 RU	3 RU	4 RU	4 RU




- Fast installation
- Raid 1+0
- Oracle Embedded - No DBA Needed

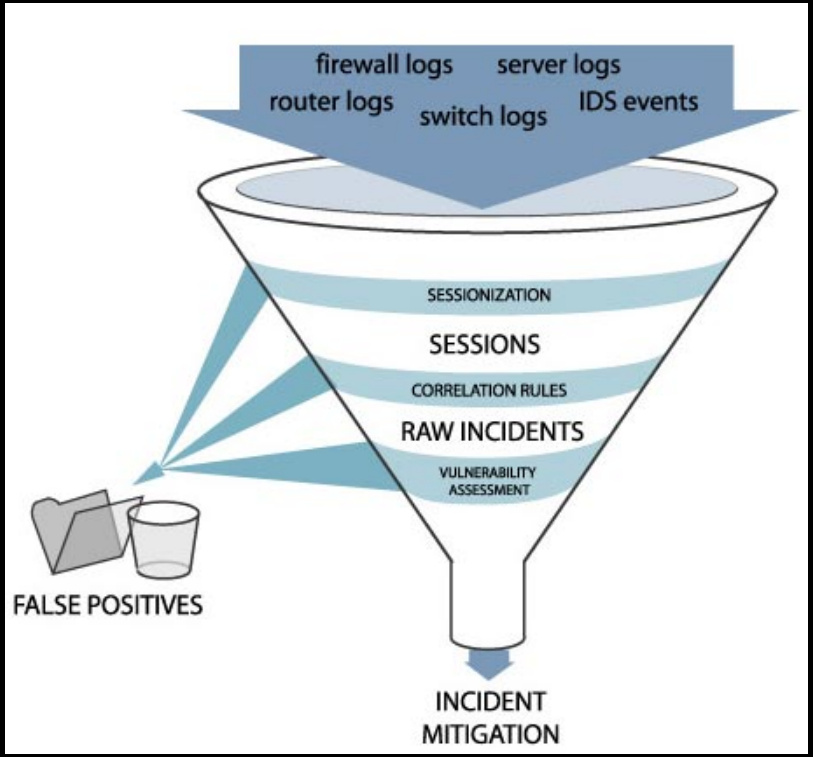
- Agent-less Event Collection
- Layer 2/3 Network Topology and Mitigation
  - NetFlow
  - Drill down to MAC addresses

Deploying CS-MARS



Life of an Incident

1. Events come into the appliance from network devices
2. Events are parsed
3. Normalized
4. Sessionized/NAT correlation
5. Run against rule engine
   - Drop rule matched first
   - All rules are checked
6. False-positive analysis
7. Vulnerability Assessments against suspected hosts



Interpreting a Syslog Message

Message ID

Source IP Address

Protocol

```
%FWSM-6-302014: Teardown TCP connection 219025563
faddr 144.254.71.150/53 gaddr 10.61.1.76/43611
laddr 10.1.70.60/43611 duration 0:00:05 bytes 18 (FIN Timeout)
```

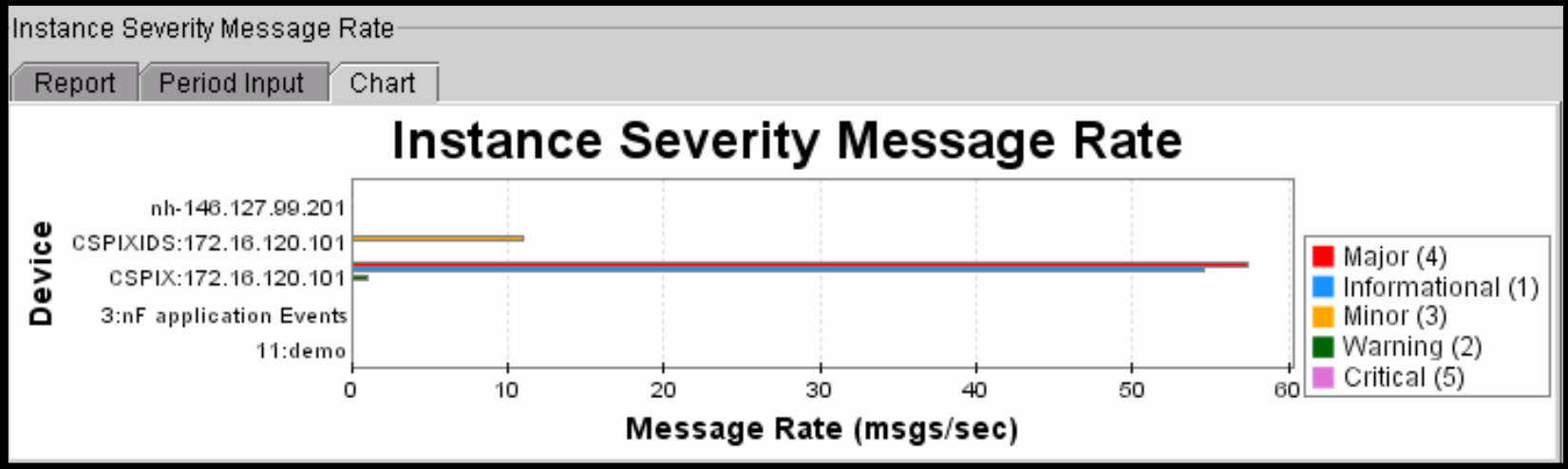
Local Destination IP

Global Destination IP

Bytes and Duration

EPS Best Practices

- Enable all events, after a couple of days run a system status reports to see data rate and disk space usage, etc.
- Disable messages that are of no interest on the device not on the security event monitoring solution



Normalization

- Security monitoring environment is multi-vendor
- Events from different devices and vendors have different formats
- Need to compare similar—normalized—events from multiple vendors “apples-to-apples”
- How do you like them apples ☺

Session Data—Requires Awareness of Topology, NAT, PAT, and Device Configurations

1. Host A **port scans** target X
2. Host A **buffer overflow attacks** X

   Where X is behind NAT device and

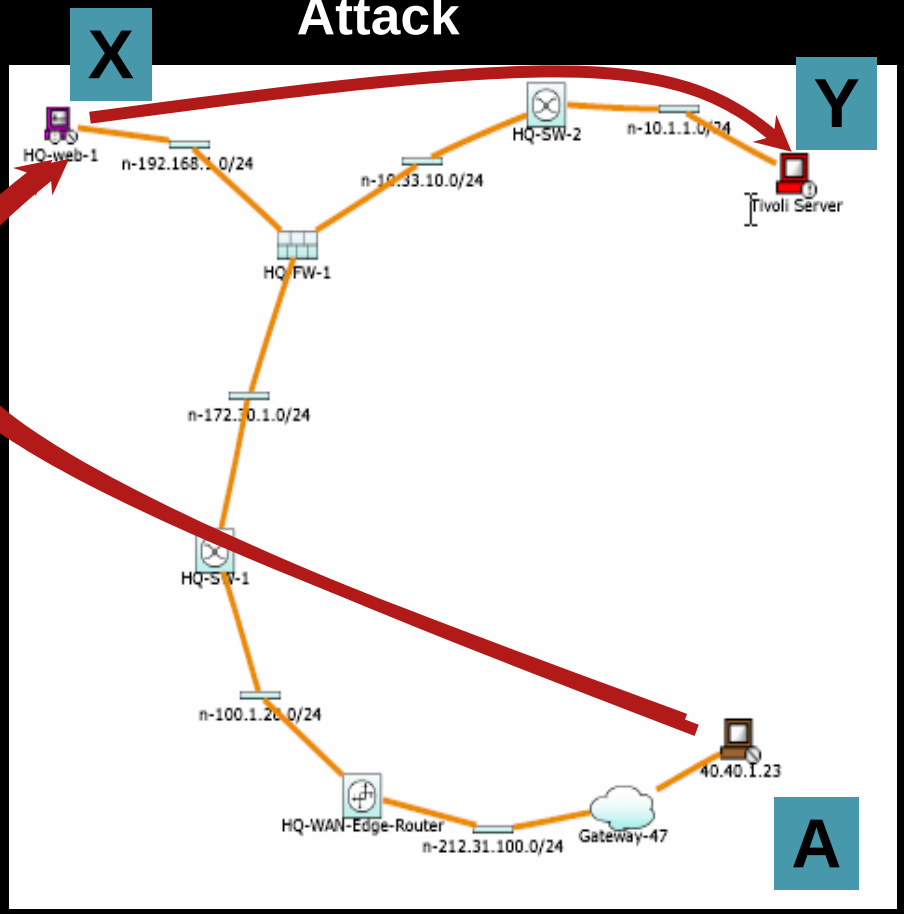
   Where X is **vulnerable** to attack

3. Target X executes **password attack** on Target Y located downstream from NAT Device

Port Scan

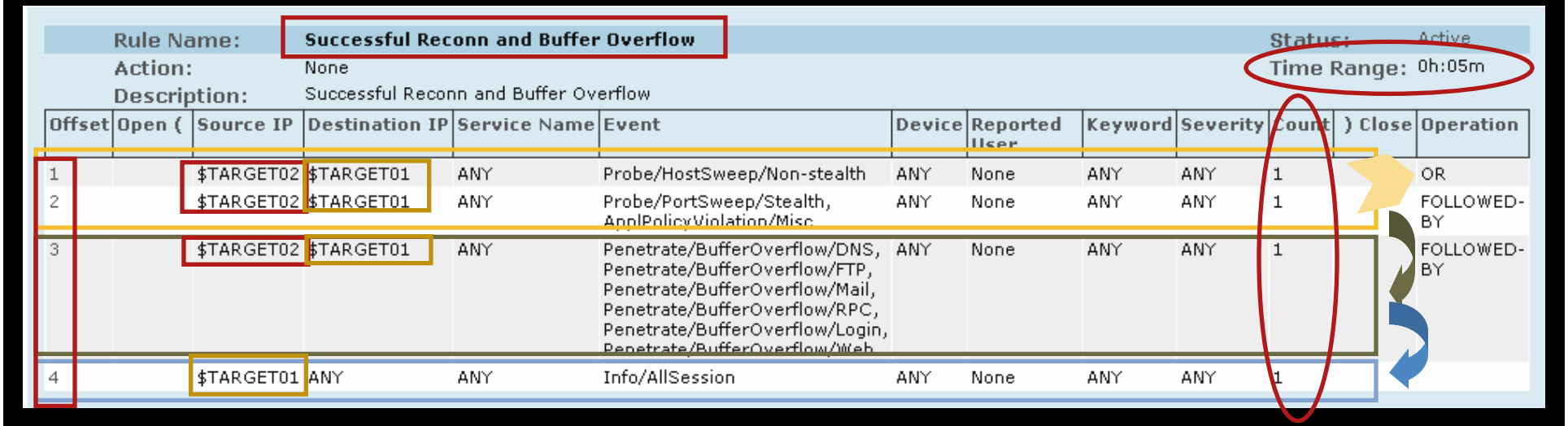
Buffer Overflow

Password Attack



Rules: Definition

Variables and Operators allow Context Sensitive Correlation



Rule Name: **Successful Reconn and Buffer Overflow**

Status: Active

Action: None

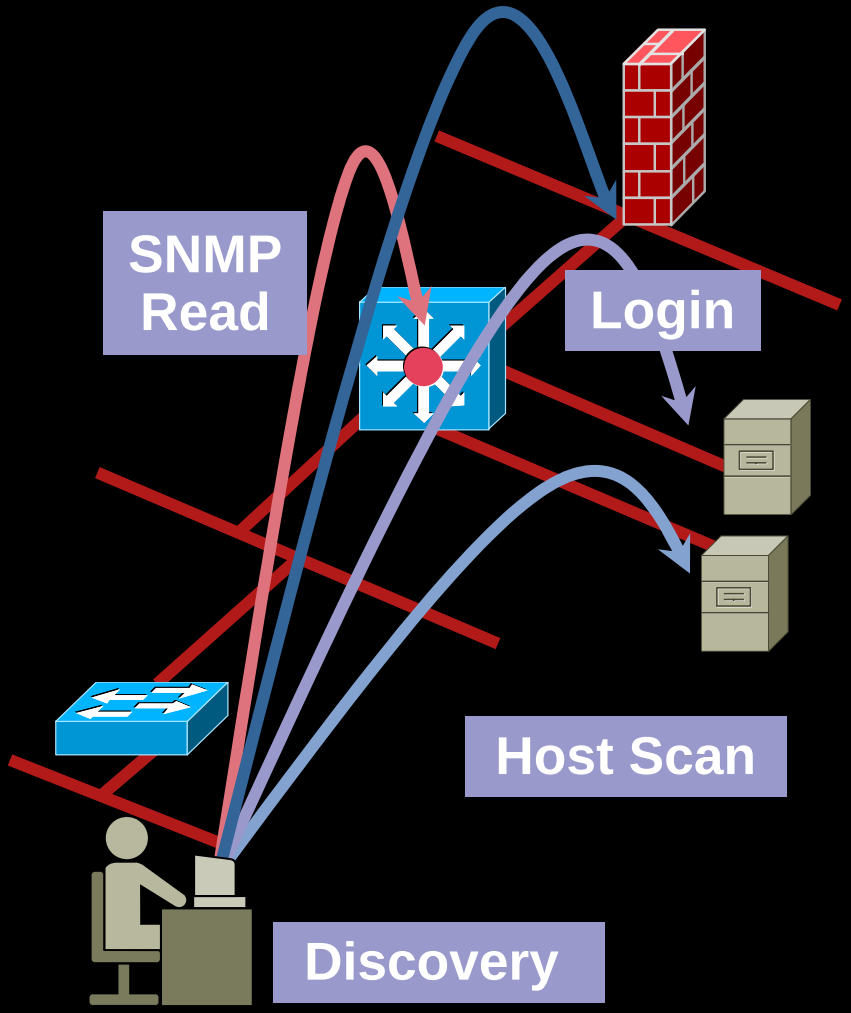
Time Range: 0h:05m

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/Non-stealth	ANY	None	ANY	ANY	1		OR
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/Stealth, ApplPolicyViolation/Misc	ANY	None	ANY	ANY	1		FOLLOWED-BY
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/Login, Penetrate/BufferOverflow/Web	ANY	None	ANY	ANY	1		FOLLOWED-BY
4		$TARGET01	ANY	ANY	Info/AllSession	ANY	None	ANY	ANY	1		

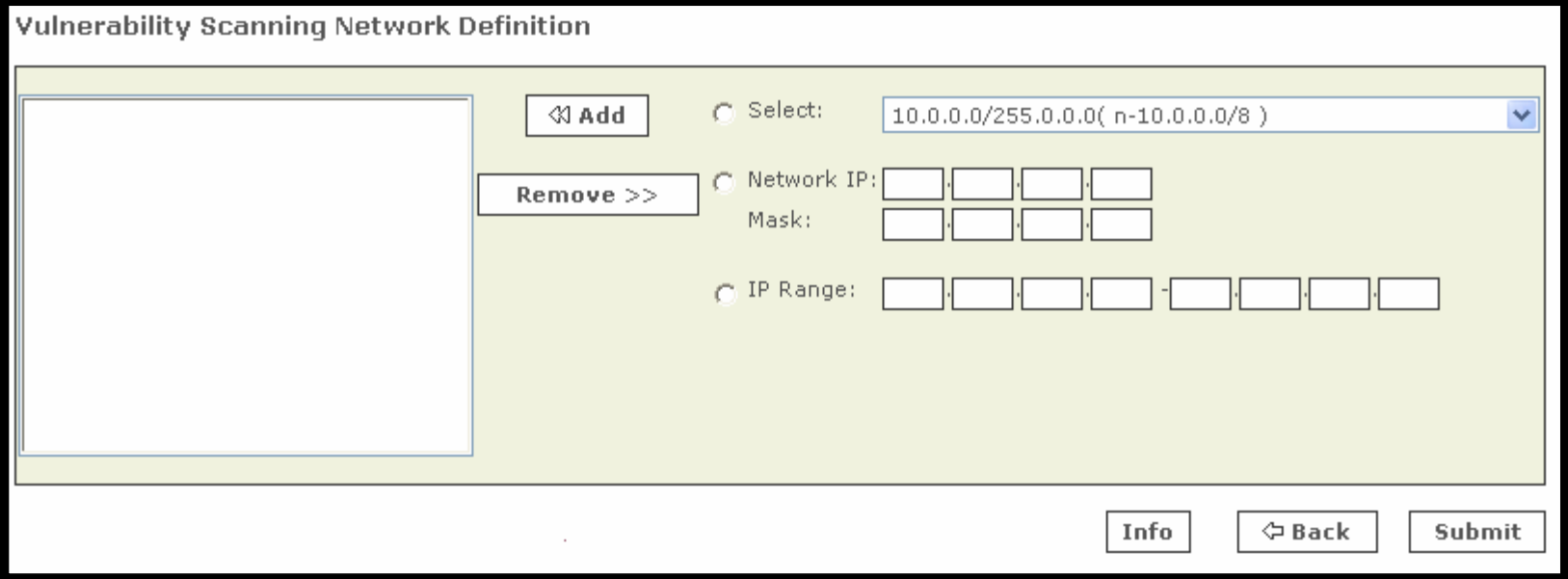
MARS and Vulnerability Assessment

- **Goal:**
  - **Reduce false positives**
- **How:**
  - **Manual definition of applications on hosts**
  - **Build in Nessus**
  - **Integration with VA tools**

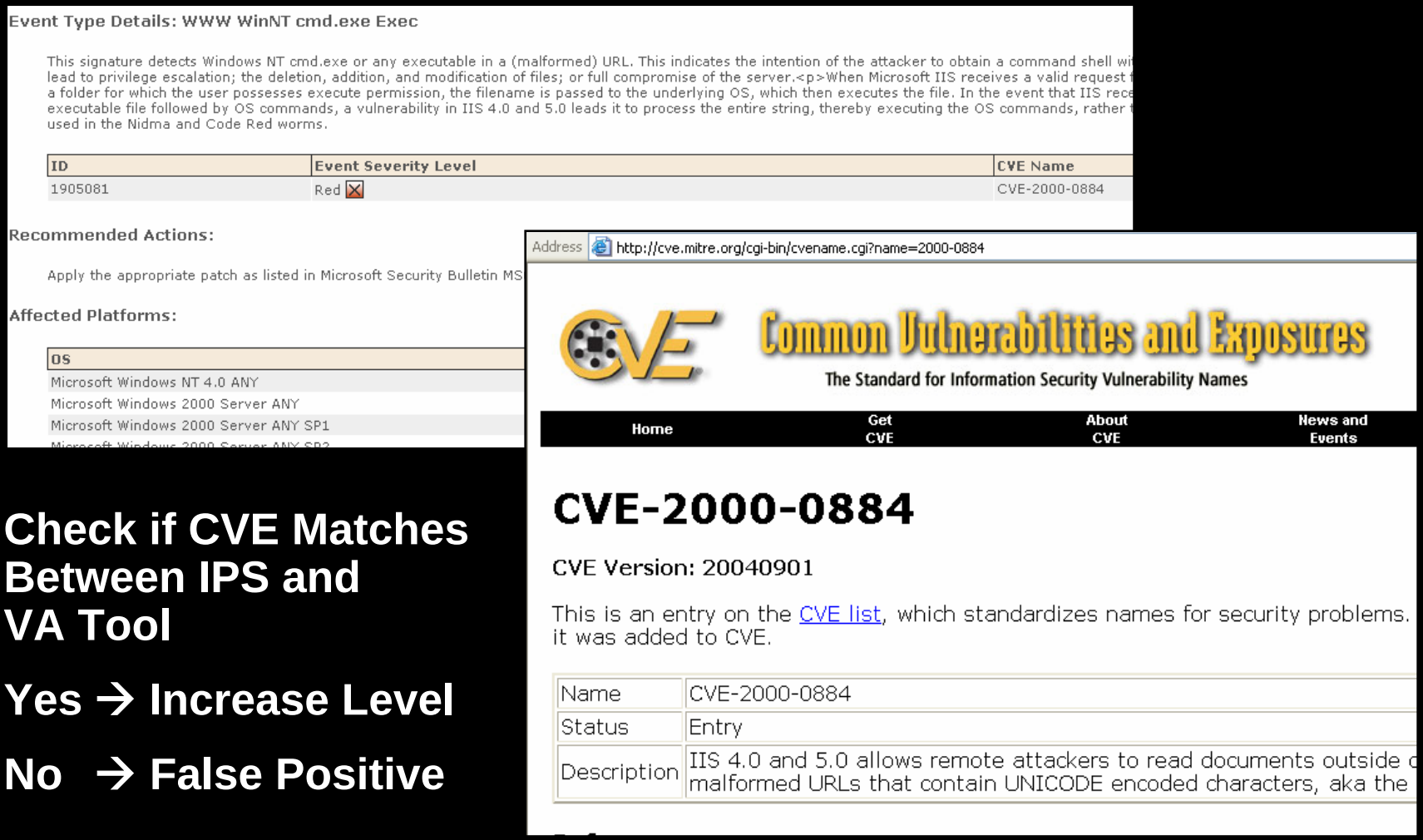


Build in VA Scanner

- MARS is able to check a victim IP address to see if an attack would be vulnerable
- Make sure your network design supports this, is MARS able to talk to the victim?



Integration with VA tools



Event Type Details: WWW WinNT cmd.exe Exec

This signature detects Windows NT cmd.exe or any executable in a (malformed) URL. This indicates the intention of the attacker to obtain a command shell wi
lead to privilege escalation; the deletion, addition, and modification of files; or full compromise of the server.<p>When Microsoft IIS receives a valid request
a folder for which the user possesses execute permission, the filename is passed to the underlying OS, which then executes the file. In the event that IIS rece
executable file followed by OS commands, a vulnerability in IIS 4.0 and 5.0 leads it to process the entire string, thereby executing the OS commands, rather
used in the Nidma and Code Red worms.

ID	Event Severity Level	CVE Name
1905081	Red	CVE-2000-0884

Recommended Actions:

Apply the appropriate patch as listed in Microsoft Security Bulletin MS

Affected Platforms:

OS
Microsoft Windows NT 4.0 ANY
Microsoft Windows 2000 Server ANY
Microsoft Windows 2000 Server ANY SP1

Address http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0884

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Home | Get CVE | About CVE | News and Events

CVE-2000-0884

CVE Version: 20040901

This is an entry on the CVE list, which standardizes names for security problems.
it was added to CVE.

Name	CVE-2000-0884
Status	Entry
Description	IIS 4.0 and 5.0 allows remote attackers to read documents outside c malformed URLs that contain UNICODE encoded characters, aka the

Check if CVE Matches Between IPS and VA Tool

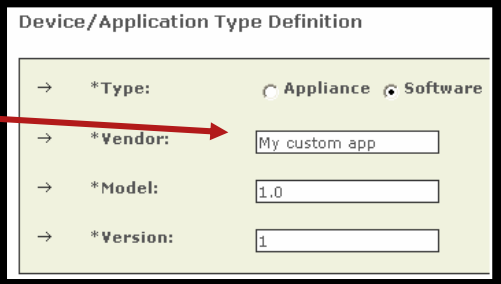
Yes → Increase Level

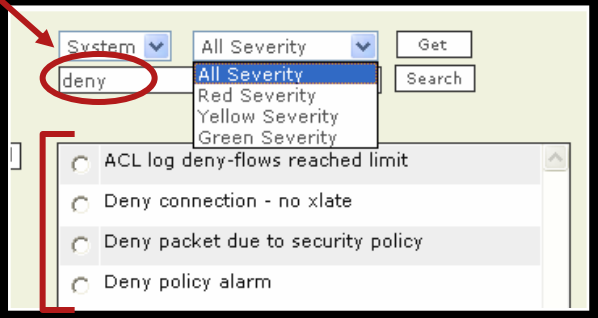
No → False Positive

Custom Parser

It Is Possible to Create a Custom Parser for Any Device Sending Syslog or SNMP Traps

1. Create a new device/ application type
2. Create an event type for the new device/application
3. Define the patterns associated to the event type
4. Add this new device/application into CS-MARS

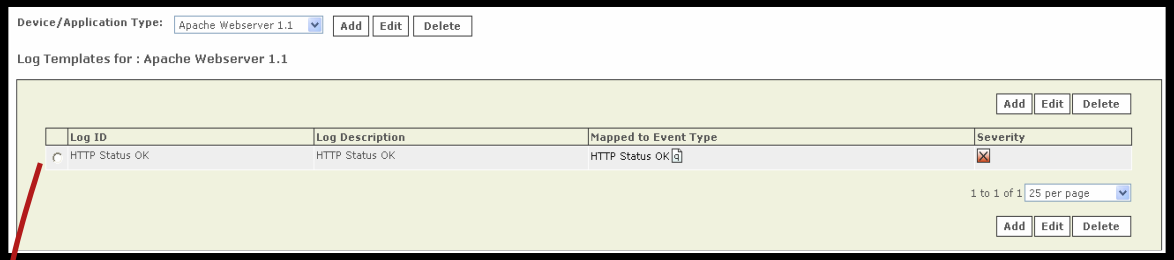




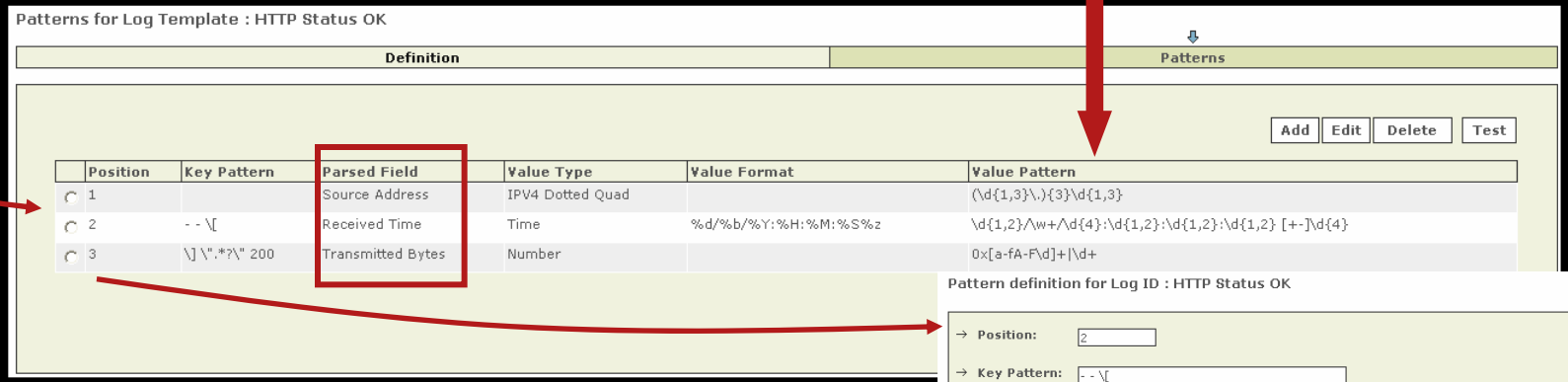
Note: If You Re-Use Events Already in the Database, the Predefined Reports and Rules Will Work Also for the Newly Defined Device

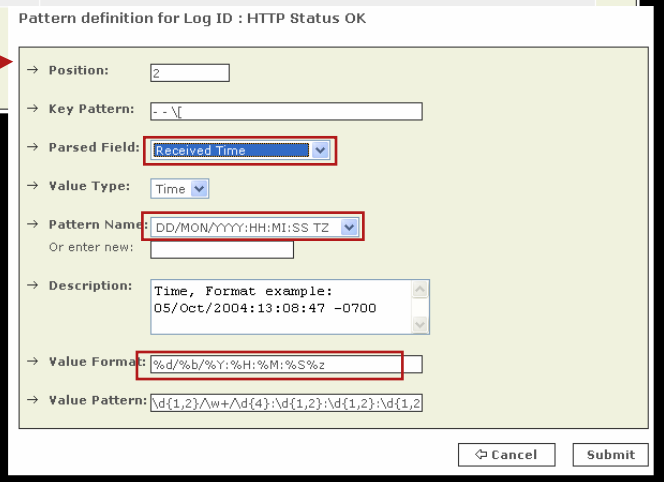
Custom Parser—Example

```
155.98.65.40 - - [21/Nov/2004:21:08:47 -0800] "GET /~user/ HTTP/1.0" 200
                1633 "-" "Lynx/2.8.2rel.1 libwww-FM/2.14"
```



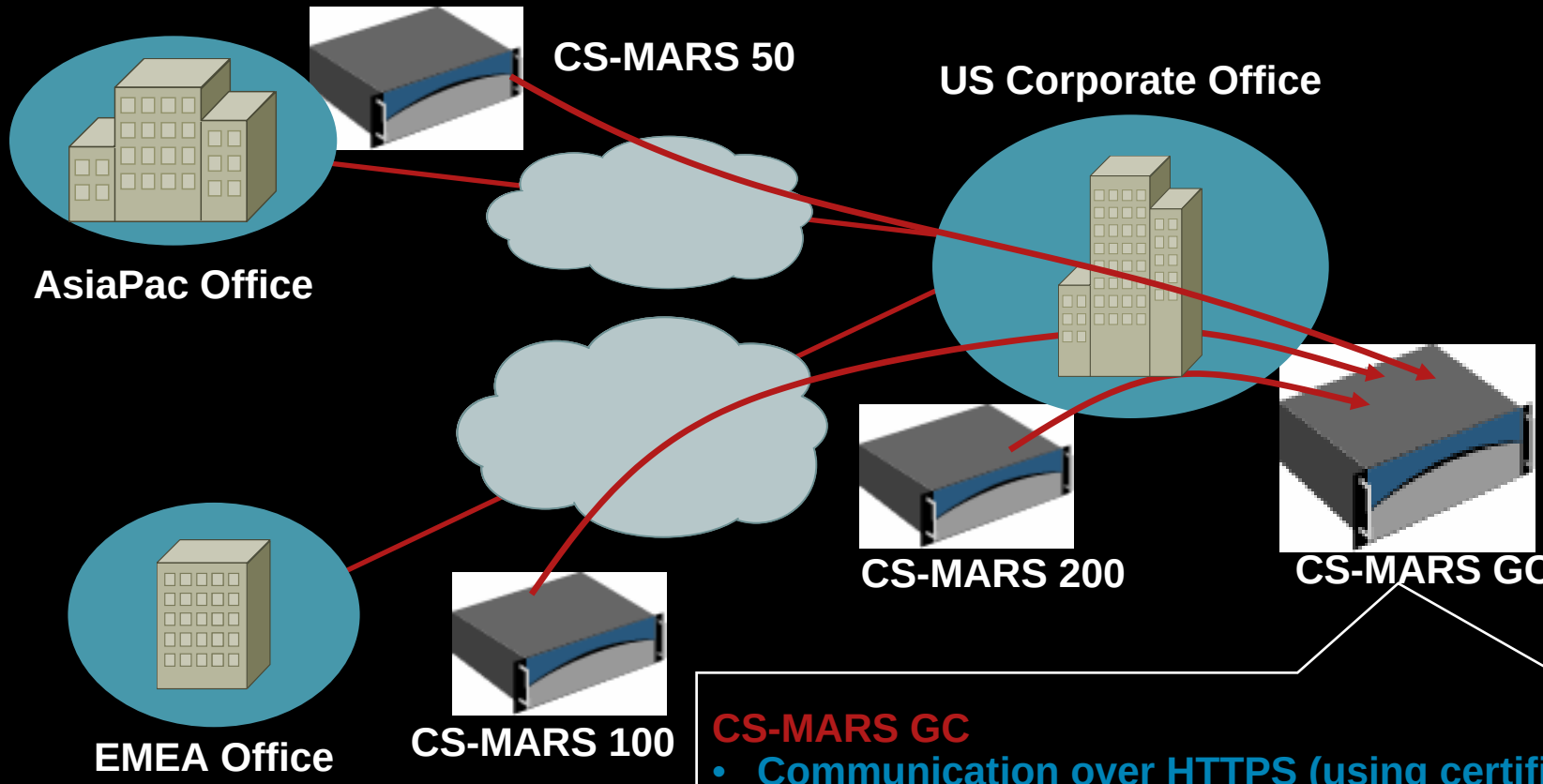
Precompiled Regular Expressions for known Parameters





- Define the fields you want to extract:
  - Source IP
  - Received time
  - Transmitted bytes

CS-MARS
Global Controller Deployment



CS-MARS GC

- Communication over HTTPS (using certificates)
- Only incidents from global rules are rolled up

- GC can distribute updates, rules, report templates, access rules, and queries across LC

CS-MARS and NetFlow

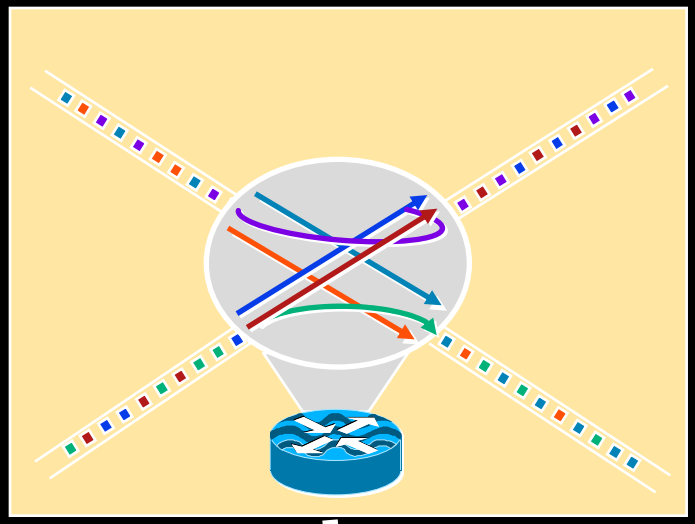
What People Find in NetFlow Data

- Who are my top N talkers? Which percentage?
- How many users are on the network at any given time? When will upgrades effect the least number of users?
- How long do my users surf?
- Where: which Internet sites do they use?
- Are users staying with in an acceptable usage policy?
- DOS attack detections!
- I have been attacked, which other machines could be having an issue?

What is a NetFlow Flow?

7 Keys define a flow

Source Address
Destination Address
Source Port
Destination Port
Layer 3 Protocol Type
TOS byte (DSCP)
Input Logical Interface (ifIndex)



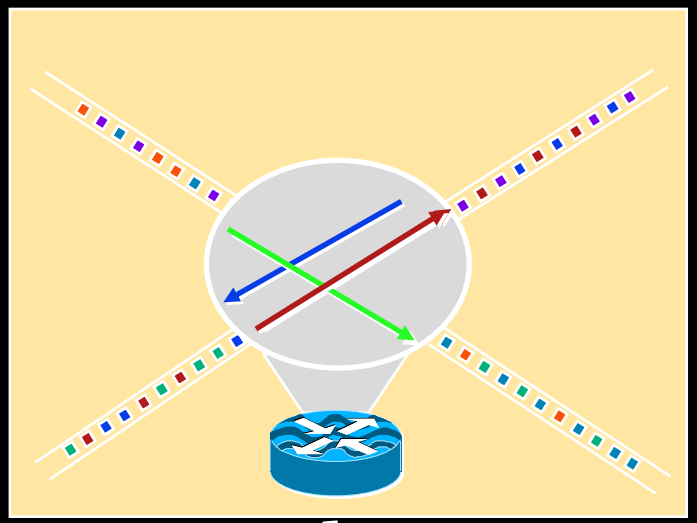
Exported Data

A flow is unidirectional

How does it work?

NetFlow Cache

7 identifiers	Other data
⋮	⋮

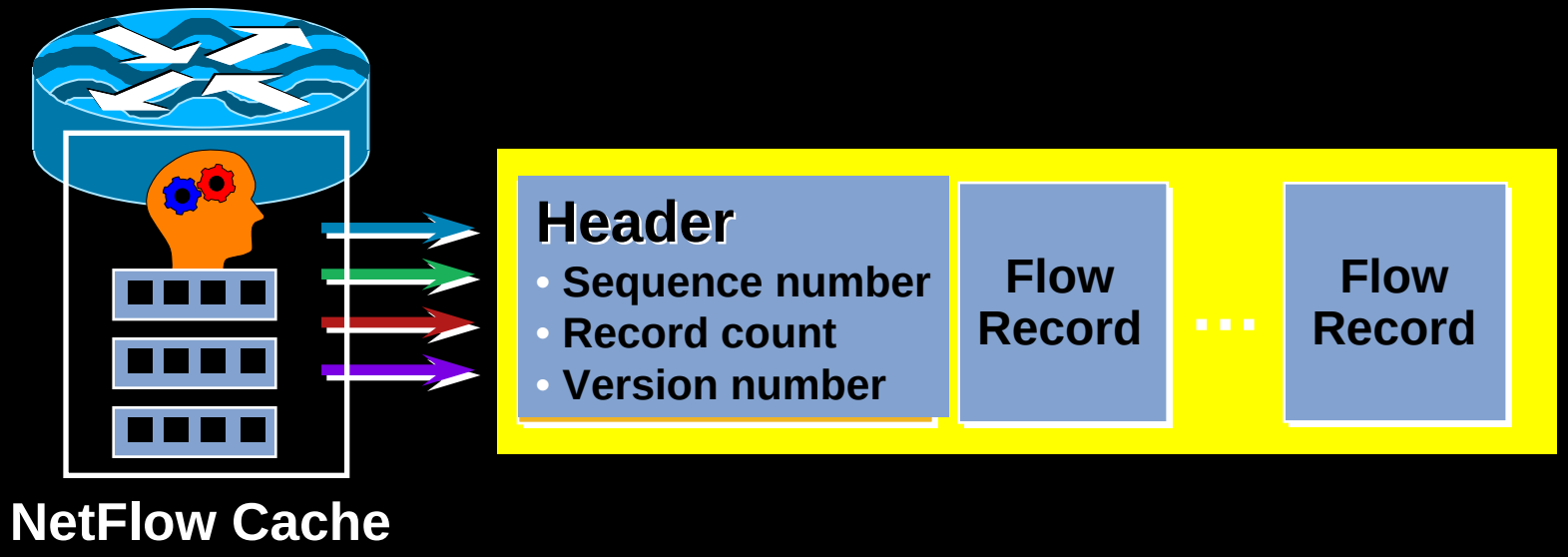


Exported Data

Versions

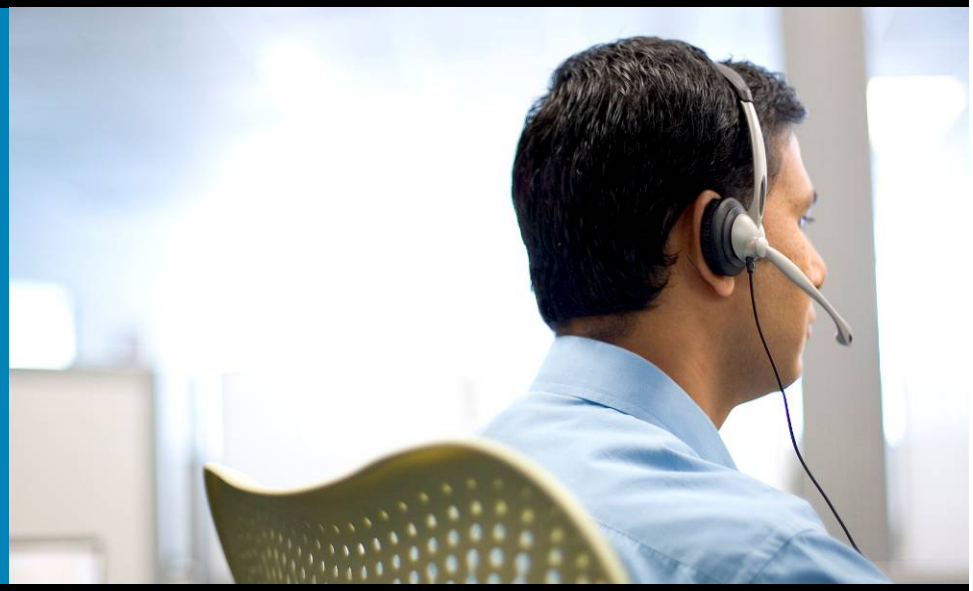
- Version 1, the initial one
- Version 5, the enhanced version 1
- Version 7, on the switches
- Version 8, the Router Based Aggregation
- Version 9, the new flexible and extensible version

Data Export



- Expired flows are grouped together into “NetFlow Export” UDP datagrams for export to a collector
- UDP is used for speed and simplicity

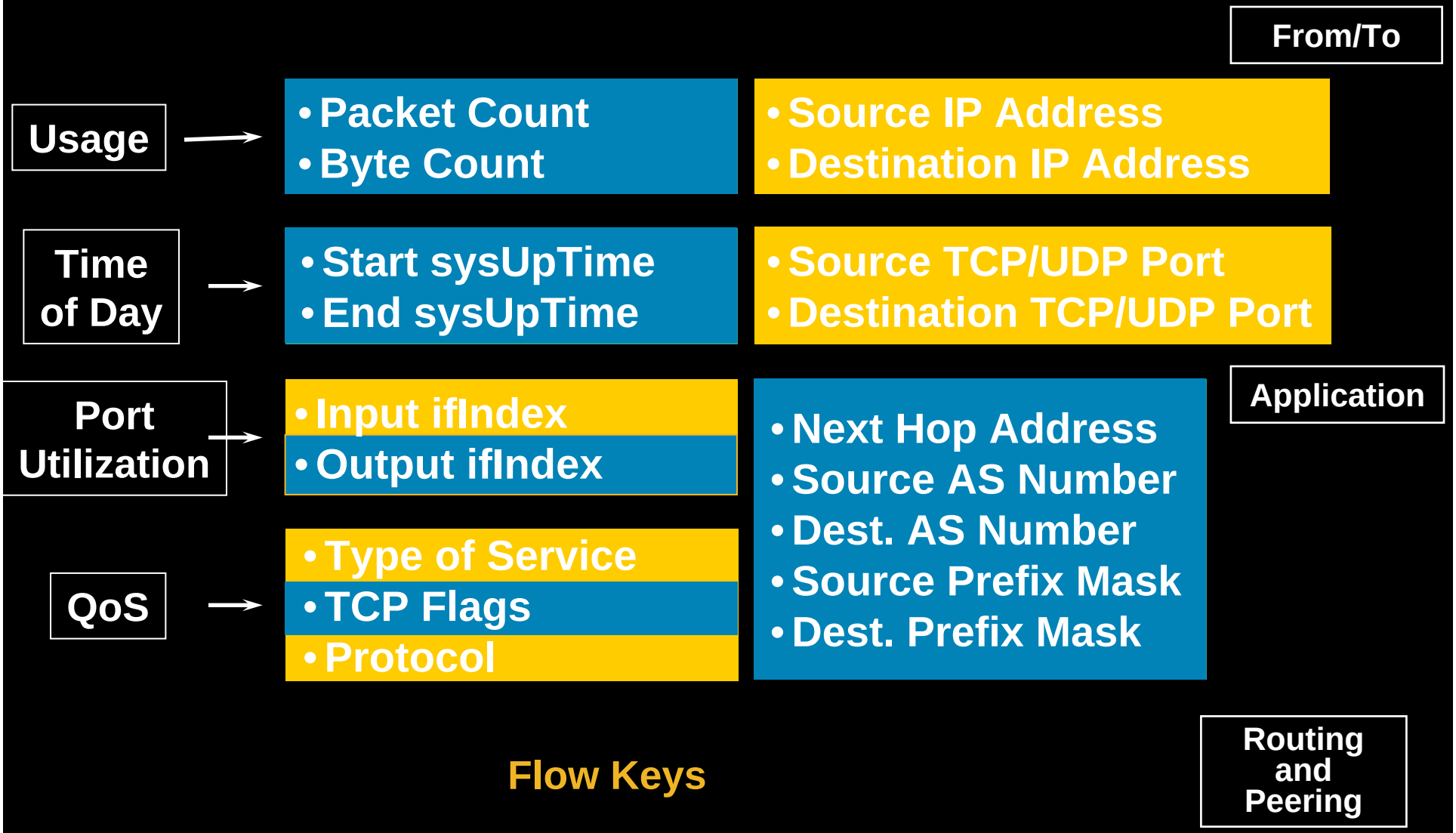
NetFlow on the Router Version 5



Version 5

- Supported on router starting from 11.1 CA and 12.0
- The most deployed version
- The most complete version in terms of exported data types
- Supported by CS-MARS! (together with version 7)

Version 5 Flow Format



NetFlow Cache Example

1. Create and update flows in NetFlow cache

Srclf	SrclPadd	Dstlf	DstlPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Expiration

- Inactive timer expired (15 sec is default)
- Active timer expired (30 min (1800 sec) is default)
- NetFlow cache is full (oldest flows are expired)
- RST or FIN TCP Flag

Srclf	SrclPadd	Dstlf	DstlPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

No

Yes

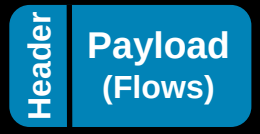
3. Aggregation

4. Export version

Non-Aggregated Flows—Export Version 5 or 9

5. Transport protocol

Export Packet



e.g. Protocol-Port Aggregation Scheme Becomes

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

Aggregated Flows—Export Version 8 or 9

Version 5 Configuration

```
router (config-if)#ip route-cache flow
router (config)#ip flow-export destination 172.17.246.225 9996
router (config)#ip flow-export version 5 <peer-as | origin-as>

Optional configuration
router (config)#ip flow-export source loopback 0
router (config)#ip flow-cache entries <1024-524288>
router (config)#ip flow-cache timeout …
```

NetFlow on Sub-Interface

- “ip route-cache flow” enables NetFlow on the main interface and all the sub-interfaces
- Allow to enable NetFlow on selected sub-interfaces

```
Router(config-if)# ip flow ingress
```

- “ip flow ingress” introduced in 12.2(14)S, 12.2(15)T, 12.0(22)S, for the 7200, 7400 and 7500

  http://www.cisco.com/go/fn

- “ip route-cache flow” should not be used anymore

NetFlow Performance

- Enabling NetFlow version 5 AND exporting increases the cpu utilization by around 15 % (with a max of 20 % depending on the platform)
- NetFlow is done in hardware on the Cat6500 supervisor
- http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/ntfo_wp.htm

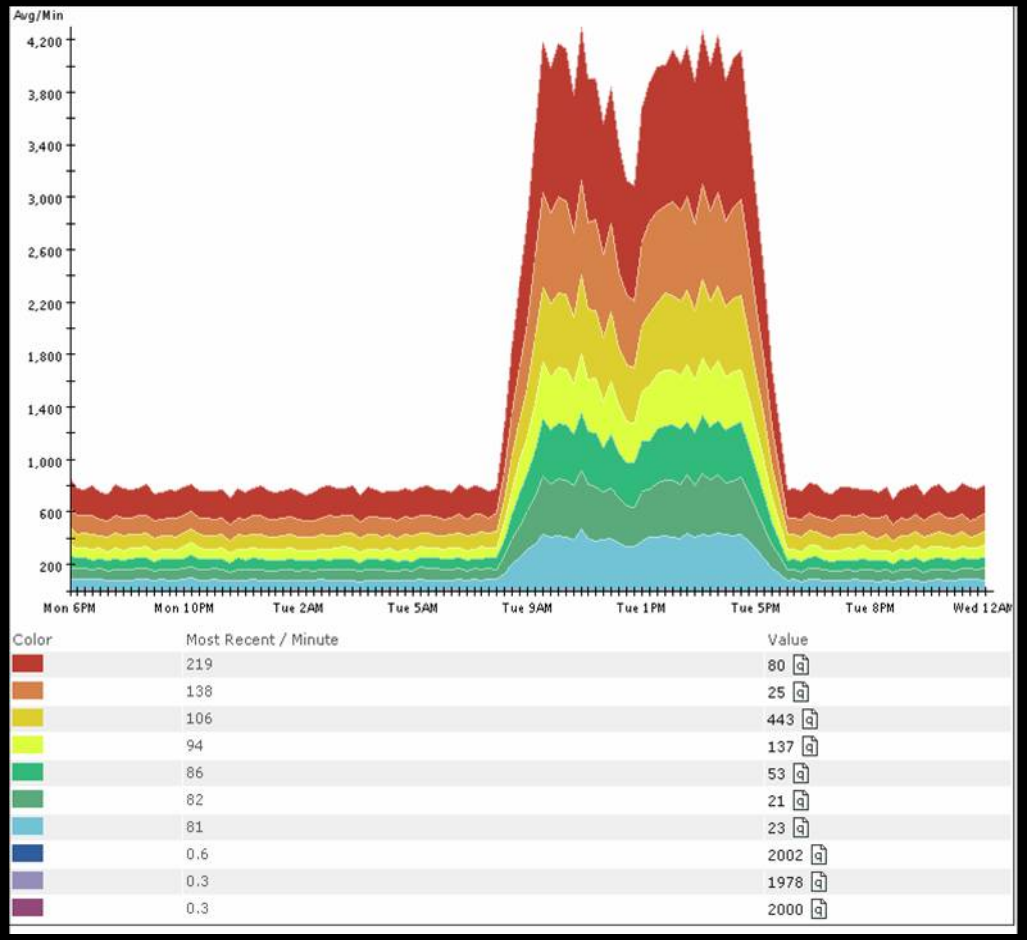
Design a network with NetFlow

- NetFlow traffic is 1 to 1,5% of actual traffic that is being accounted. (difficult to be precise)
- NetFlow is UDP, so no guarantees, use dedicated interfaces if available
- NetFlow over WAN, probably not…
- Use NetFlow Collector if application support this
  - 3 layer architecture (router, NFC, application)

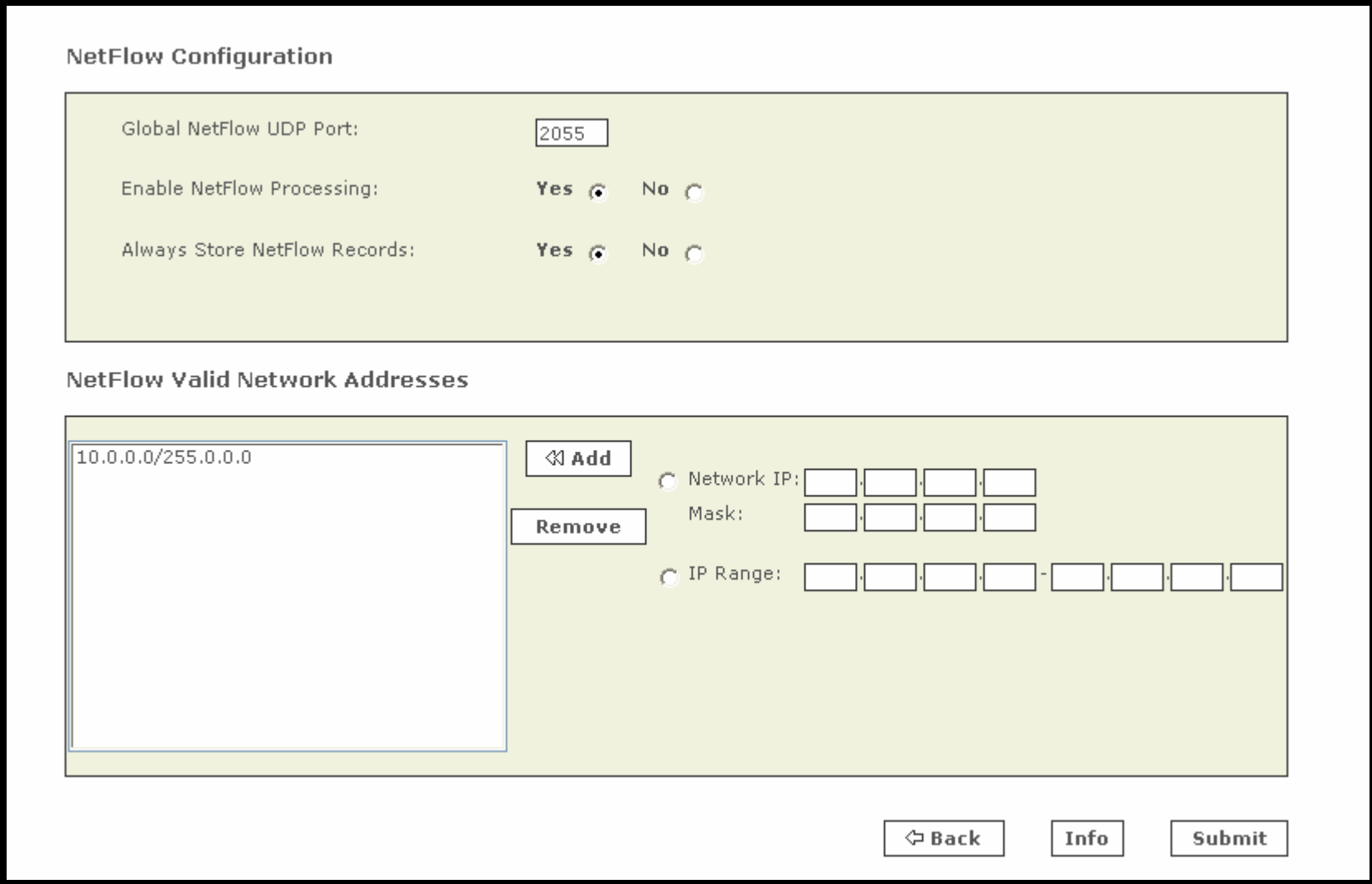
CS MARS - Netflow

What does CS-MARS use Netflow data for?

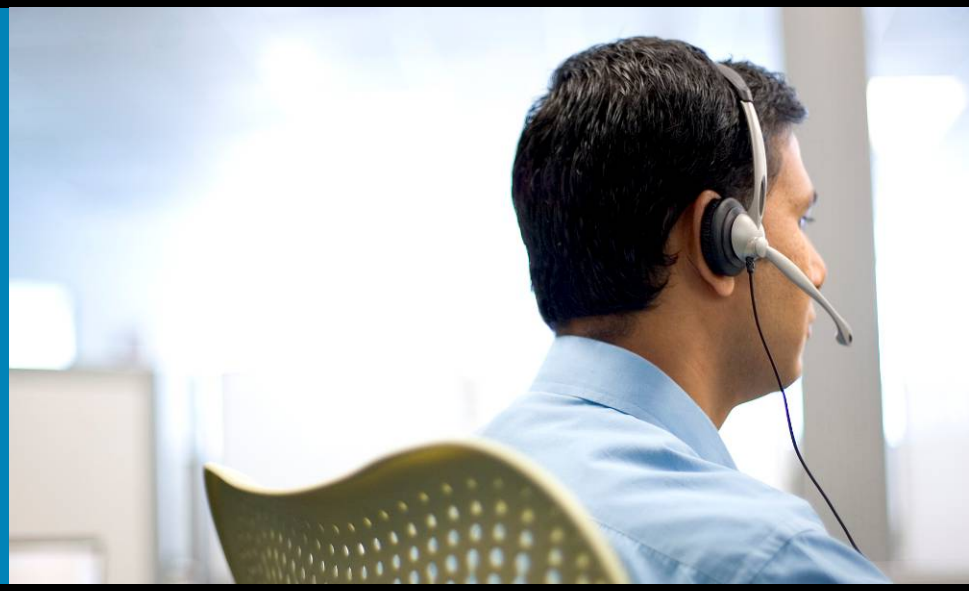
- Profile the network usage,
- Detect statistically significant anomalous behavior (from computed baseline) and
- Correlate anomalous behavior to attacks and other events reported by Network IDS systems.
- The NetFlow data and Firewall traffic logs are treated uniformly since they both represent traffic in an enterprise network.



How do you configure MARS for NetFlow

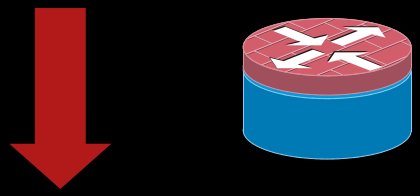


Cisco is about integration



Distributed Threat Mitigation

- ISR have limited memory and cannot run the full set of signatures



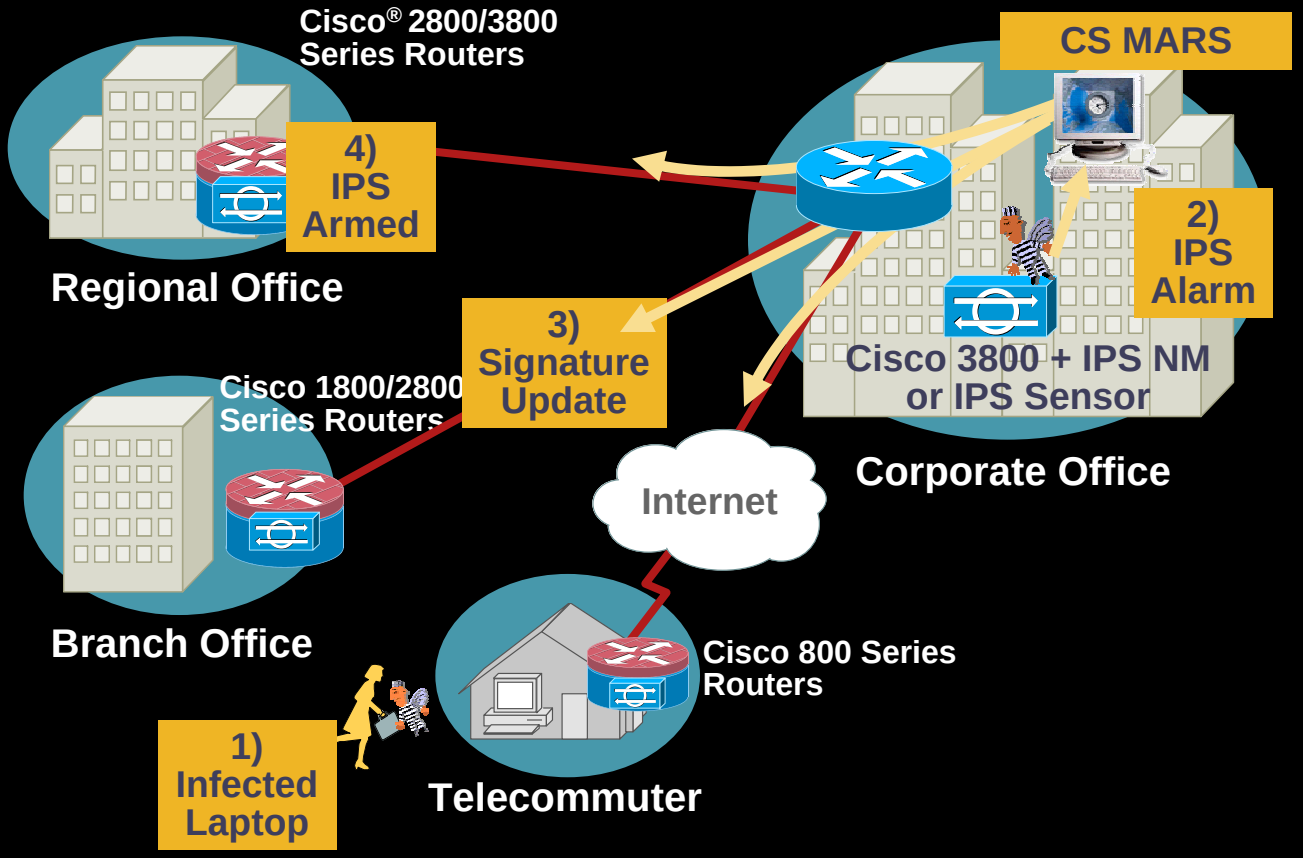
```
Default sdf file varies with
the router memory
     –128MB.sdf
     –256MB.sdf
```

- Need to know which signatures need to be enabled and which is not important

```
Rtr(config)# ip ips signature 2000 disable
Rtr(config)# copy <url> ips-sdf
```

- CS-MARS has the required visibility to make this decision and access right

Distributed Threat Mitigation Architecture



1. Infected Telecommuter Connects to the Corporate Network
2. Virus Sets off IPS Alarm at Corporate Office
3. CS-MARS Distributes Signatures to All Security Routers
4. Armed Routers Protect All Remote Sites

For more details refer to the following white paper:

http://www.cisco.com/en/US/products/ps6241/products_configuration_example09186a008067a2b0.shtml