# Network Admission Control

**Glen Stacey**

**System Engineer**

**Atlantic Canada Team**

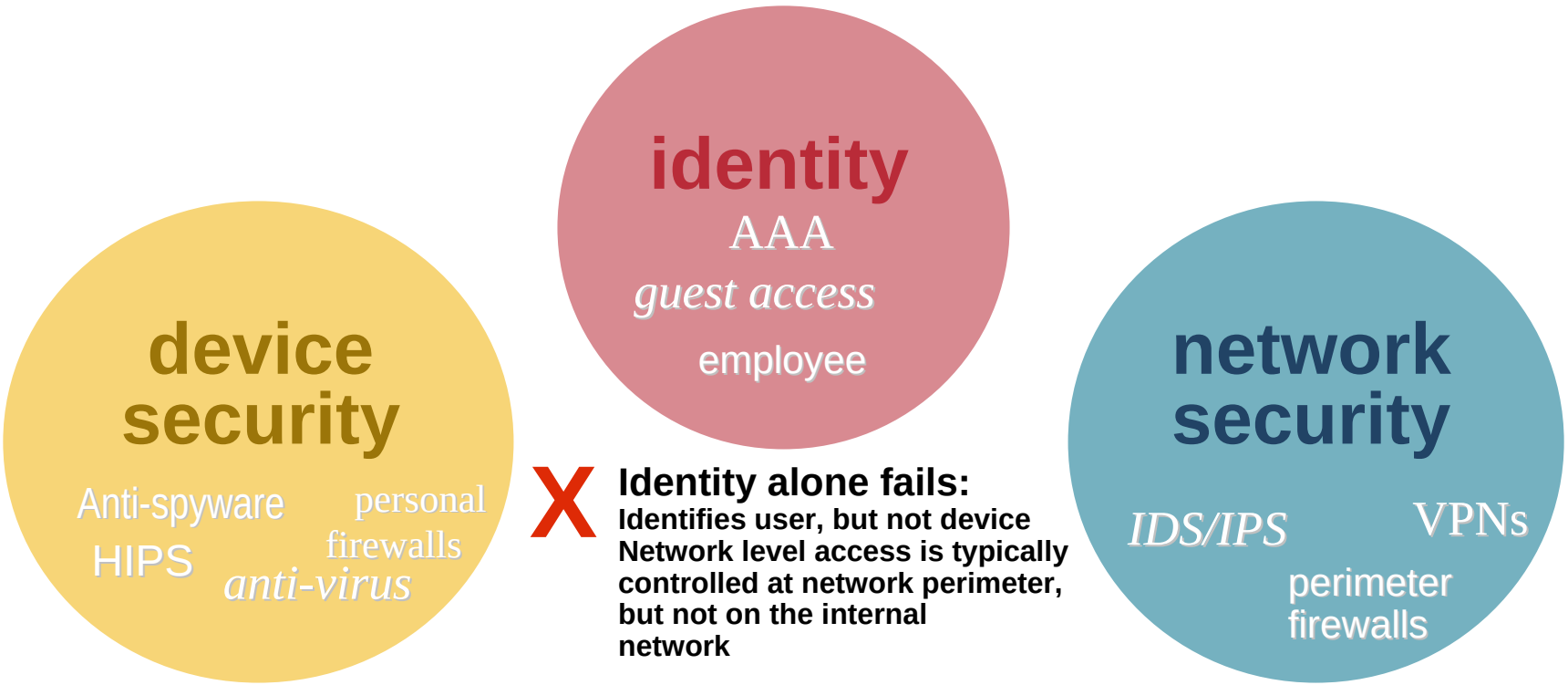
# Business Demands Require Strong Access Control

- Information security threats and endpoint vulnerabilities are growing faster than ever
- Disappearing security boundaries expose internal infrastructure and assets
- Stricter corporate-defined policies and government and regulatory compliance requirements impact many organizations
- Ensuring policy compliance for all endpoint devices seeking network access is critical to information security and business success

"***Security policy enforcement and malware defenses at the traditional network perimeter are no longer sufficient to protect the information and systems connected to the internal network***."

**- Phil Schacter, Burton Group**
**Mar 22, 2006**

# New Solution Is Needed



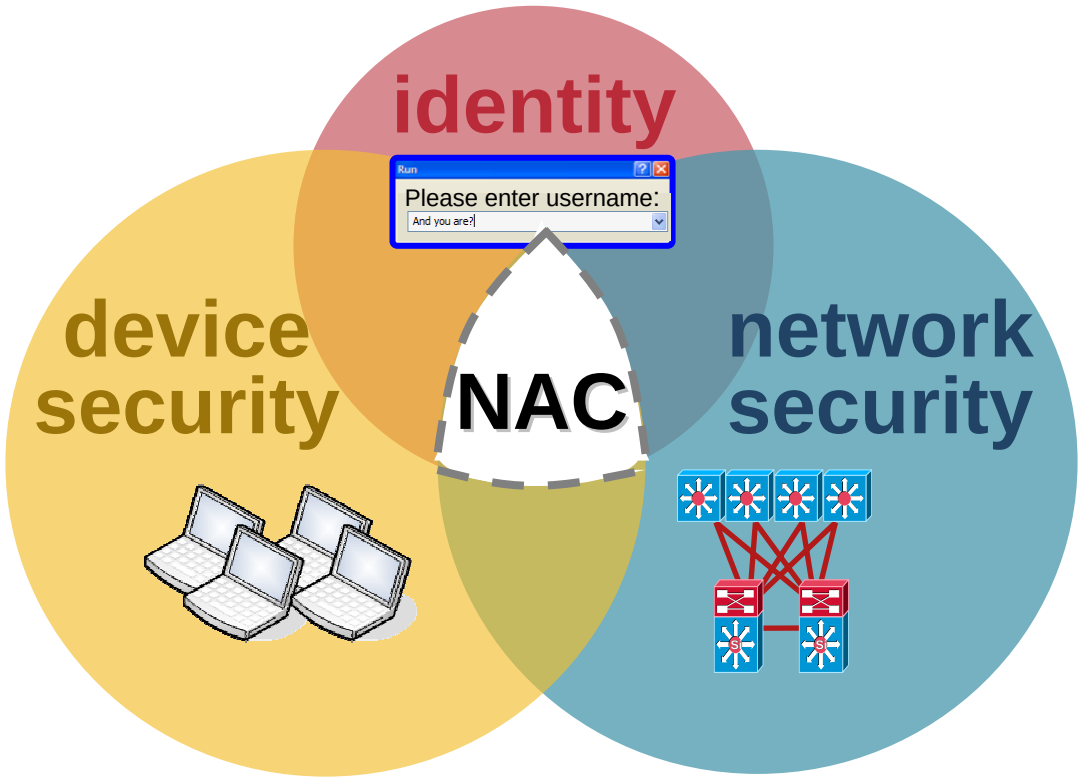

**X Identity alone fails:**
**Identifies user, but not device**
**Network level access is typically controlled at network perimeter, but not on the internal network**

**X Endpoint security alone fails:**
**Most corporate assets have AV, but infections persist!**
**Host based apps are easily manipulated (even unintentionally)**
**Lag time between new viruses and anti-virus patch upgrade cycle**
**Non-corporate assets often do not meet security requirements**

**X Network security alone fails:**
**Firewalls cannot block legitimate ports**
**VPNs cannot block legitimate users**
**Detection often occurs after-the-fact**
**Difficult to implement access control if users are on the internal network**

# What Is Network Admission Control?

**Network Admission Control (NAC) is a solution that uses the network infrastructure to ensure all devices seeking network access comply with an organization's security policy**



# Why Use The Network for Admission Control?

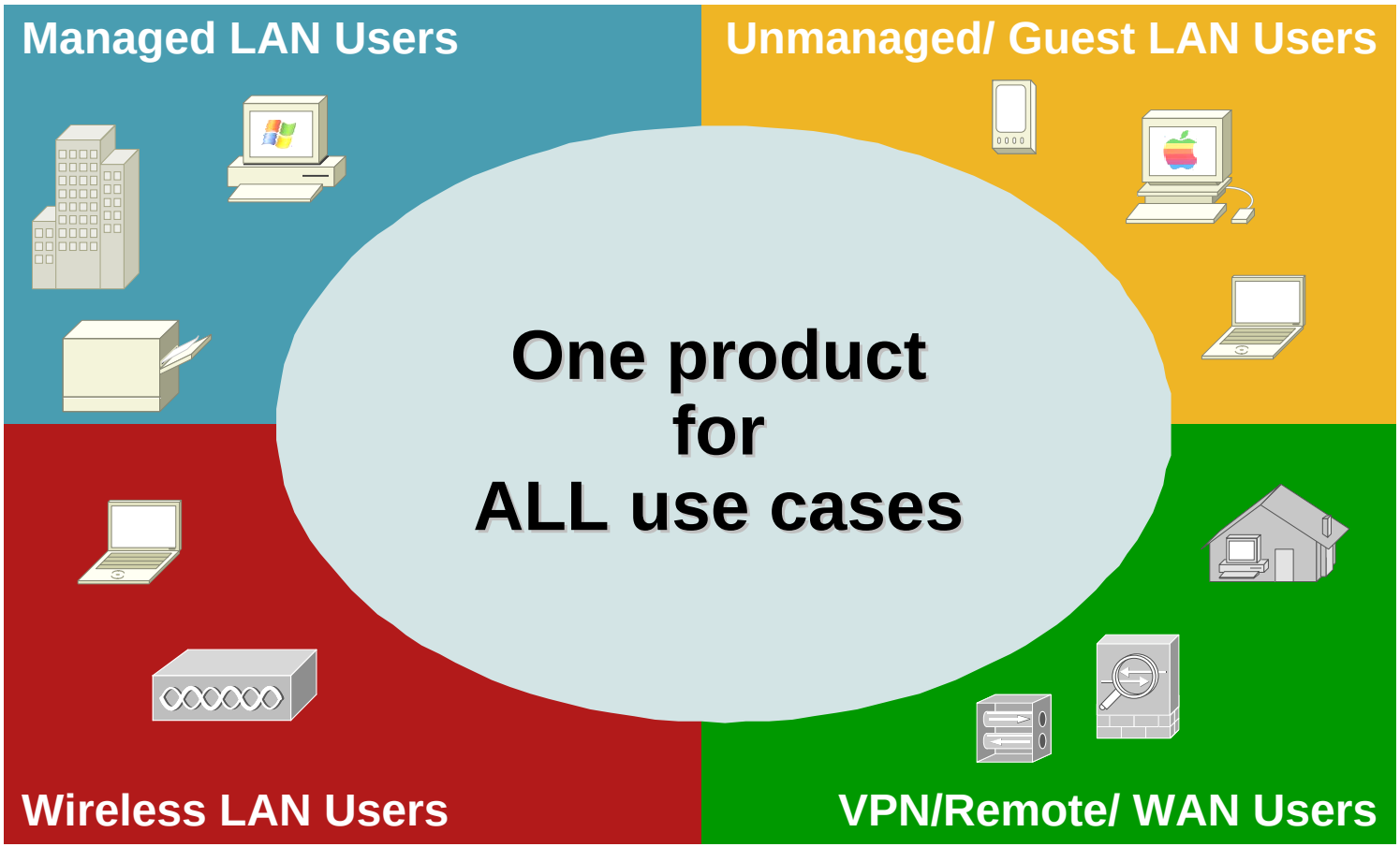
- Every bit of data you are concerned about touches the network
- Every device you are concerned about is attached to the network
- Broadest possible security solution covering the largest number of networked devices can be deployed
- Provides a consistent secure policy to all parts of the network with the smallest IT footprint possible

# Four Key Capabilities of NAC

| | SECURELY IDENTIFY DEVICE & USER | ENFORCE CONSISTENT POLICY | QUARANTINE AND REMEDIATE | CONFIGURE AND MANAGE |
|---|---|---|---|---|
| **WHAT IT MEANS** | **Uniquely identifies users and devices, and creates associations between the two** | **Ubiquitously assesses and enforces a policy across the entire network** | **Acts on posture assessment results, isolates device, and brings it into compliance** | **Easily creates comprehensive, granular policies that map quickly to user groups and roles** |
| **WHY IT IS IMPORTANT** | Associating users with devices enables granular enforcement in policies by role or group | Enforcement at the network level provides a solid foundation for holistic security | Quarantine critical to halt damage due to non-compliance; remediation addresses root cause problems | Policies that are easy to create and maintain lead to better system operations and adherence |

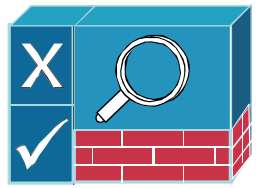
**A robust NAC solution must have all four capabilities.**

# The Cisco NAC Appliance Advantage



# Cisco NAC Appliance (Cisco Clean Access) Components

- Network Admission Control Server
- Serves as an in-band or out-of-band device for network access control



- Network Admission Control Manager

  Centralizes management for administrators, support personnel, and operators

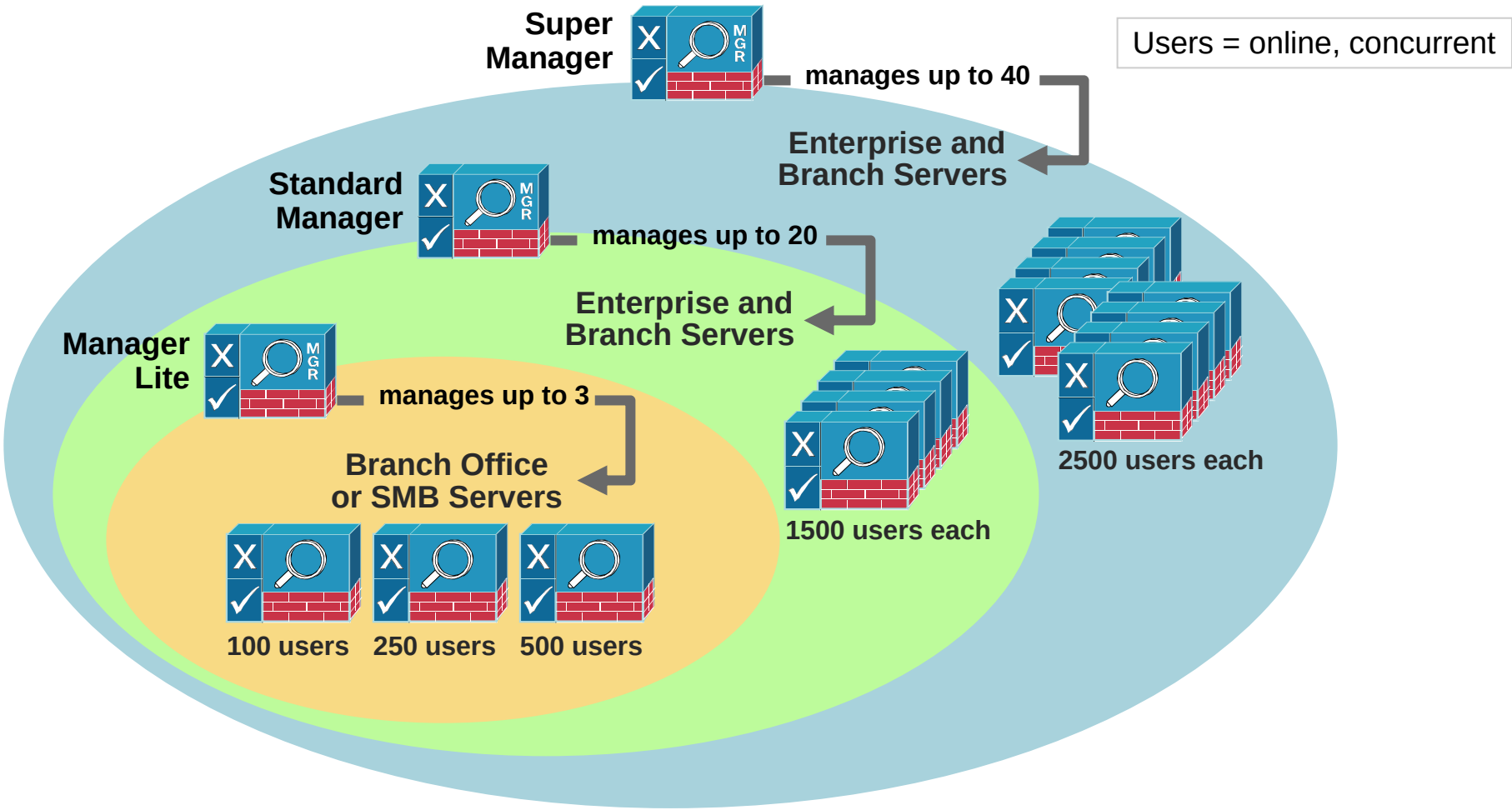

- Network Admission Control Agent

  Optional lightweight client for device-based registry scans in unmanaged environments

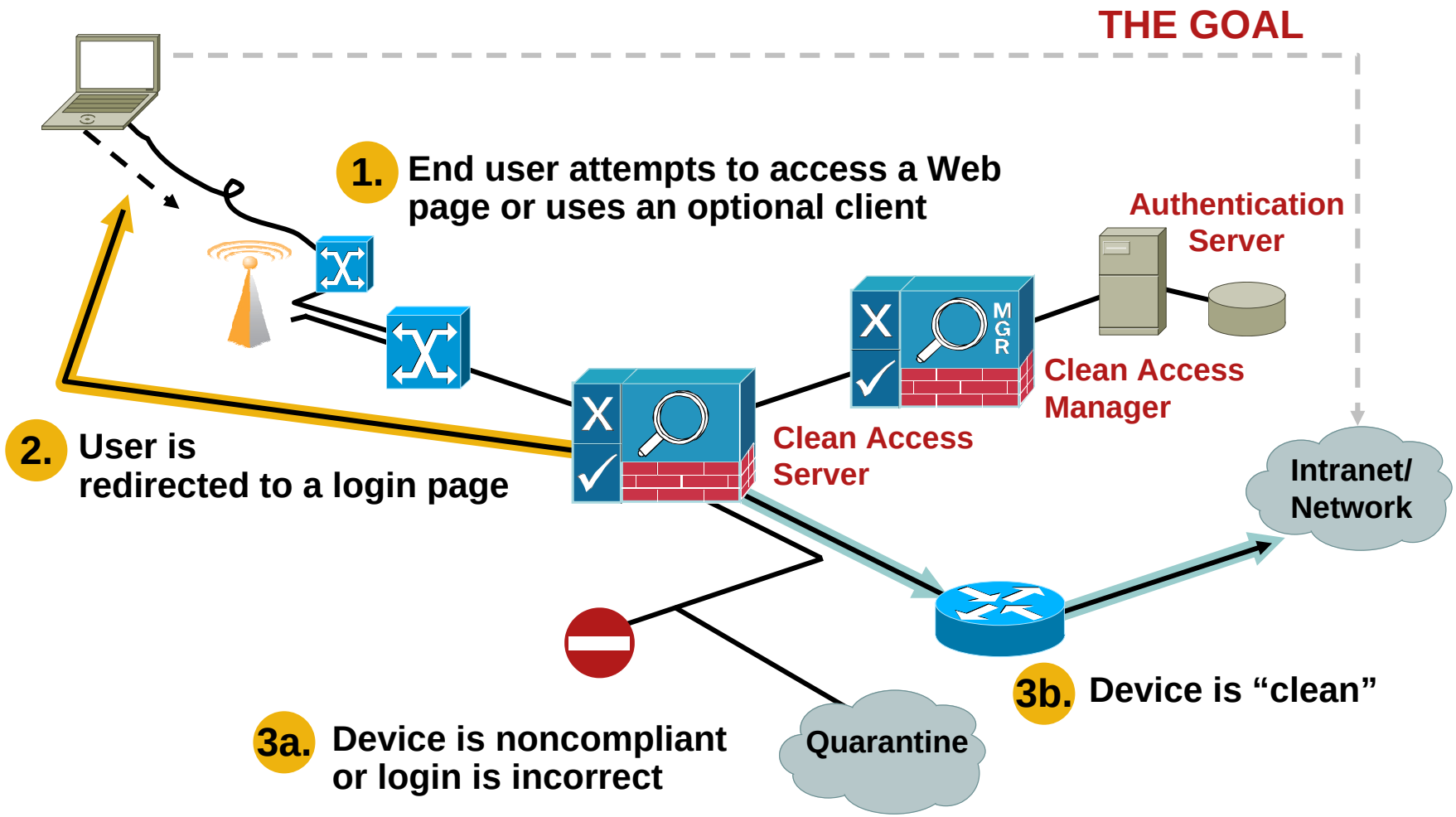

- Rule-set Updates

  Scheduled automatic updates for anti-virus, critical hot-fixes and other applications

# NAC Appliance Overview: Solution Sizing



# Cisco NAC Appliance: Product User Flow Overview

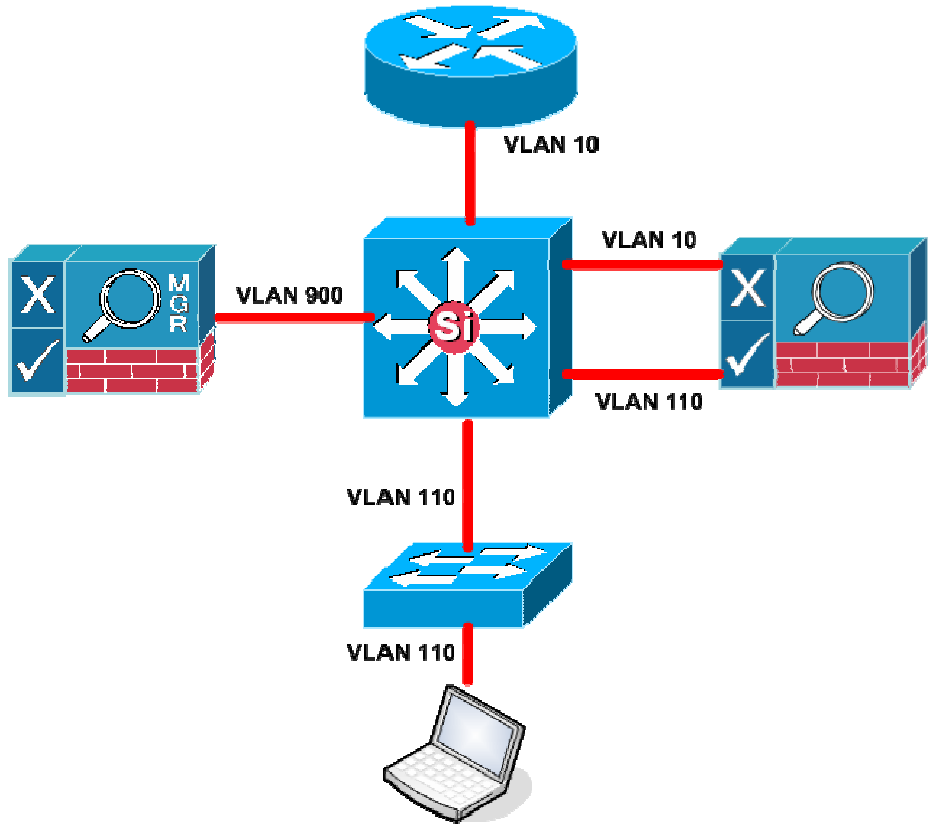


# NAC: In Band & Out of Band

- NAC Servers have two traffic flow deployment models
  - In Band
  - Out of Band
- Any NAC Server can be configured for either method, but a NAC Server can only be one at a time
- Selection is based on whether the customer wants to remove the NAC Server from the data path
- NAC Server is ALWAYS inline during Posture Assessment

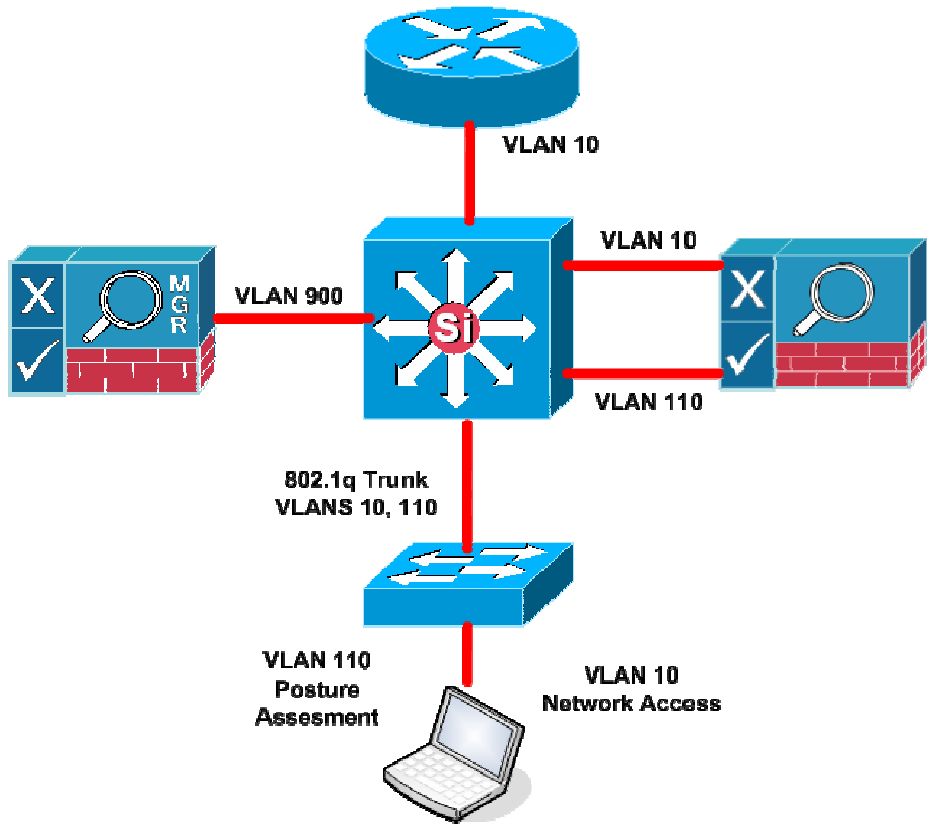
# NAC: In Band

- Easiest deployment option
- Server is Inline ( in the data path ) before and after posture assessment
- Supports any switch, any hub, any AP
- Role Based Access Control Guest, Contractor, Employee
- ACL Filtering and Bandwidth Throttling



# NAC: Out of Band

- Multi-Gig Throughput deployment option
- Server is Inline for Posture Assessment Only
- Supports most common Cisco Switches **
- Port VLAN Based and Role Based Access Control
- ACL Filtering and Bandwidth Throttling for Posture Assessment Only



# Cisco NAC Appliance: Sampling of Pre-Configured Checks

Critical Windows Updates

**Windows XP, Windows 2000, Windows 98, Windows ME**

Anti-Virus Updates

Anti-Spyware Updates

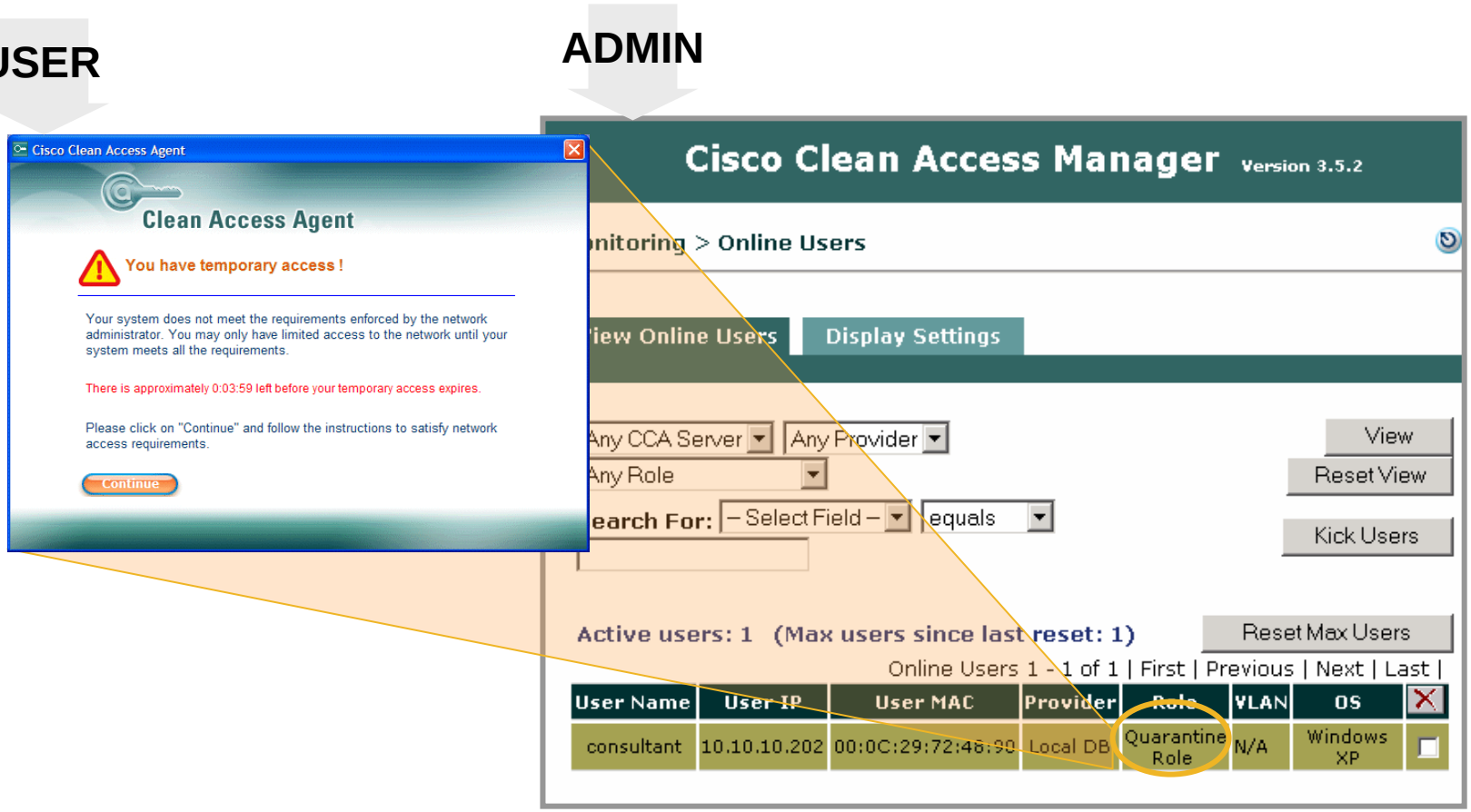
Other 3rd Party Checks

**Customers can easily add customized checks**

# Cisco NAC Appliance:
# Admin Control with Real-Time Information

**USER**

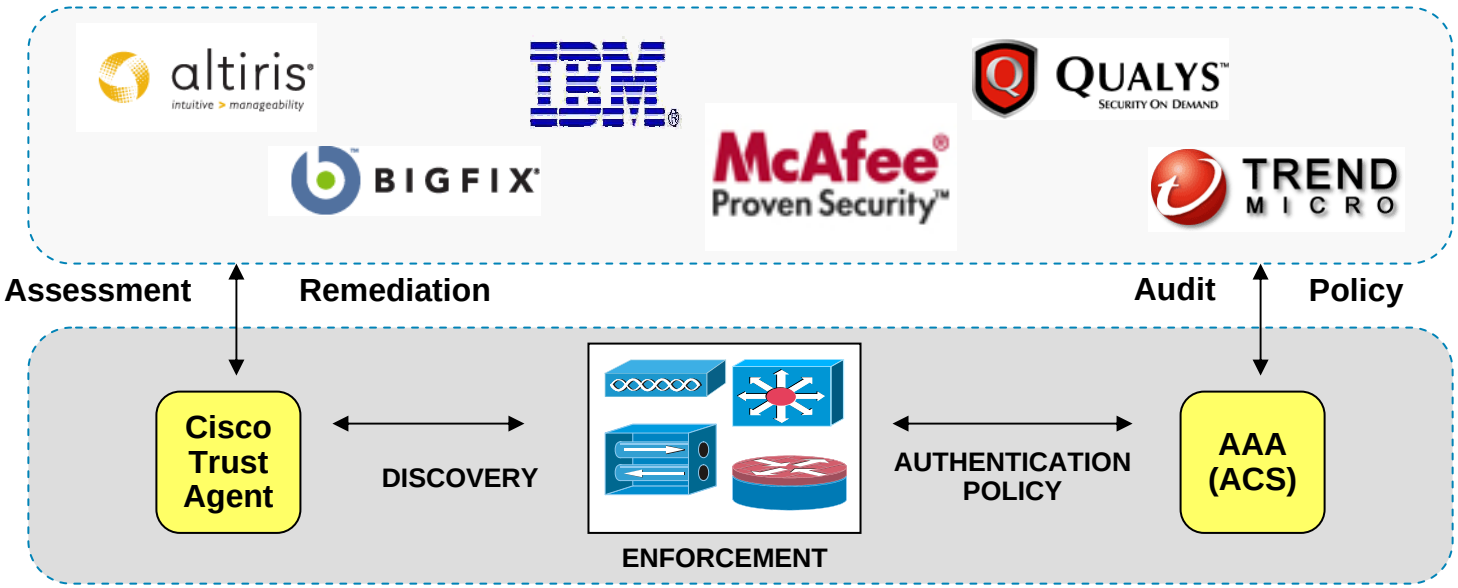
**ADMIN**




**Logs can be viewed locally or sent via Syslog to an off-box collection engine for custom reports**

# Cisco NAC Partner Program

- The NAC Partner Program is a third-party-technology integration program
- Over 70 industry leading security and management program participants with 25 certified, shipping solutions.
- Specific APIs are available for product integration in areas of assessment, remediation, and monitoring/reporting of an integrated NAC solution
- Useful for NAC customers with existing or planned investments in these partners' products
- For a complete partner list, see: www.cisco.com/go/nac/program



# Cisco NAC Advantages

- Comprehensive span of control
  - Routers, switches, VPN, wireless, plus complex deployments, including IP telephony
- Controls managed, unmanaged, and guest endpoint devices
  - Effective solution to integrate device posture and user identity
- Device posture security decisions made at the network, not on the endpoint device
  - Ability to prevent spoofed device as “compliant” and rock-solid policy enforcement
- Enjoys widest use of any technology
  - Largest deployed NAC solution to date
  - Including the most robust partner program
- Grow as your NAC solution as your network expands with Appliance *and* Framework components

# Cisco NAC Benefits

- Secure both managed or unmanaged assets
  - Consistent security standards applied for all assets
  - Broad integration with multi-vendor security products
- Ensure policy compliance
  - Security policy compliance enforcement at the network level
  - Addresses issues of disappearing security boundaries and unauthorized access
  - Assists in achieving regulatory compliance
- Proactive protection against viruses and worms
  - Controls and reduces large-scale infrastructure disruptions
  - Reduces OpEx and maintains higher employee productivity
- Integration with additional Cisco Self-Defending Network components
  - Such as integration with the Cisco Security Agent

# Monitor, Analyze and Respond with CS-MARS

**Glen Stacey**

**System Engineer**

**Atlantic Canada Team**

# Cisco Self-Defending Network

## A systems approach leveraging the Network Platform

### Integrated

Enabling every element to be a point of defense and policy enforcement

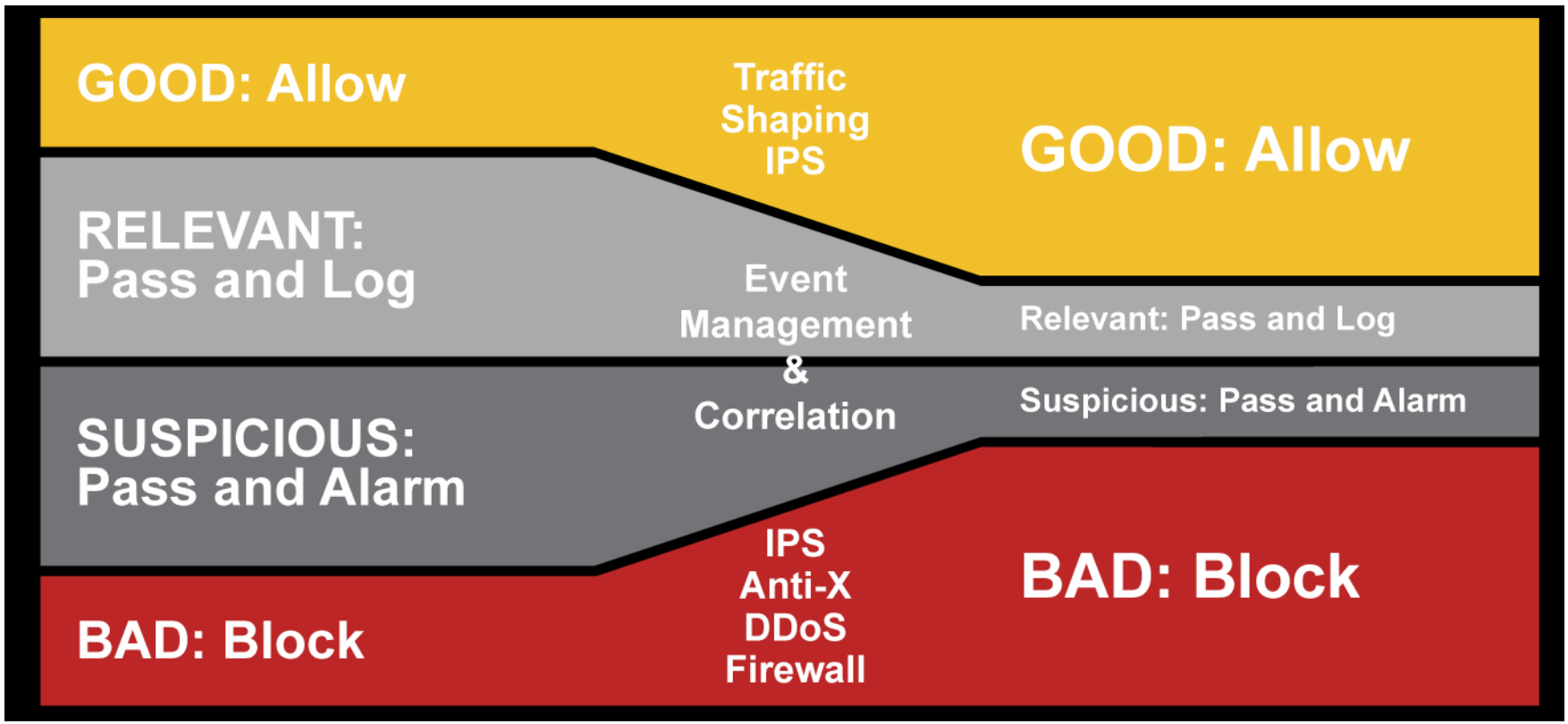
### Collaborative

Collaboration among the services and devices throughout the network to thwart attacks

### Adaptive

Proactive security technologies that automatically prevent threats

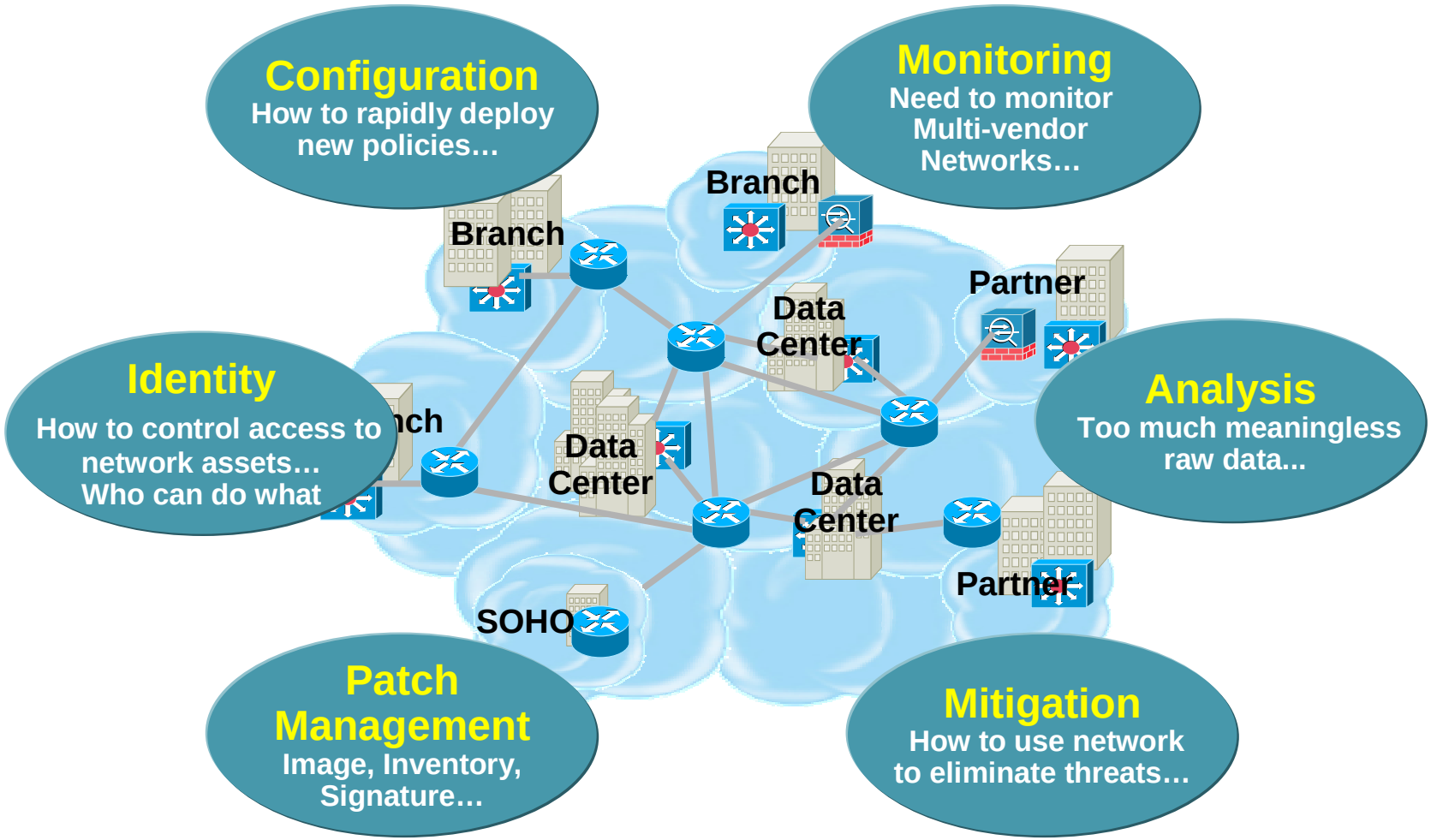
# Reducing the Gray Area




**Highly Manual**

**Automation Enablement**

# Critical Enterprise Security Practices

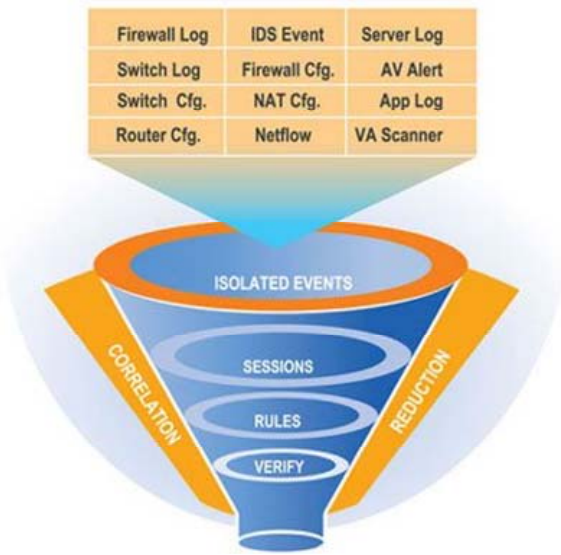


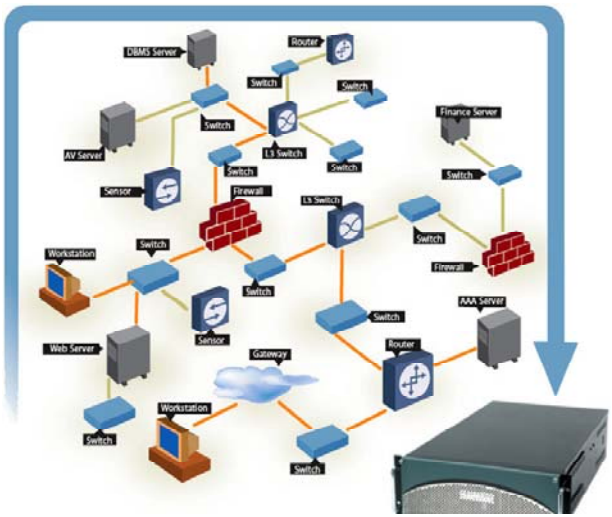
# Cisco Security – MARS
# Monitoring, Analysis and Response System

- **Command and control of 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**

# Cisco Security - MARS Feature Overview

**Key features**

- Collect, aggregate & correlate from heterogeneous devices in a single appliance
  - SDEE, Syslog, Host logs, Firewall logs …. From Cisco, Non-Cisco and Custom devices
  - No software agents required
- Network behavioural Analysis (NBA)
  - Netflow and Traffic Flow analysis provides enhanced threat detection precision
- Topological Awareness
  - Device Configuration (+NAT, +Routing) knowledge critical to global decision making
  - Attack-path views for detailed investigation and troubleshooting
- Centralized dashboard for Unified Security Operations
- Mitigation Capabilities
  - Layer 2 / Layer 3 Mitigation Suggestions (port disable, shun commands, ACLs etc.)
- Policy-Management Linkages

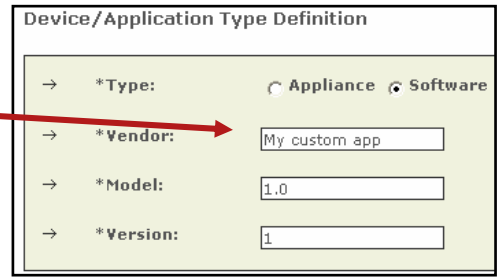
# Netflow as an input can assist with…

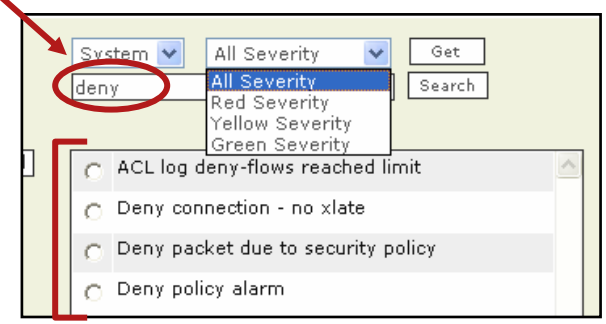
- Who are my top N talkers? Which percentage?
- How many users are on the network at any given time? When will upgrades effect the least number of users?
- How long do my users surf?
- Where: which Internet sites do they use?
- Are users staying with in an acceptable usage policy?
- DOS attack detections!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

# Custom Parser

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

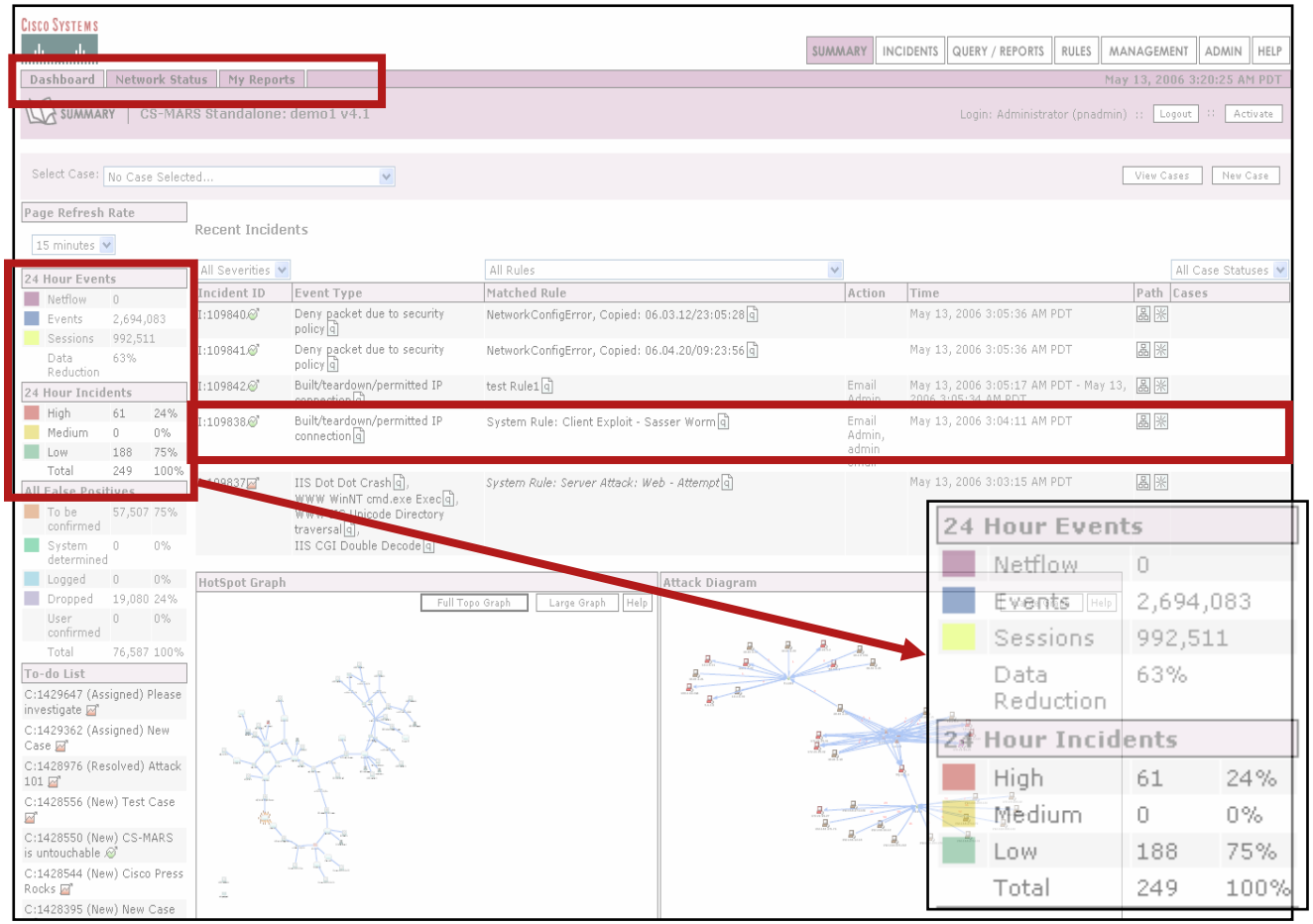
1. Create a new device/ application type
2. Create an event type for the new device/application
3. Define the patterns associated to the event type
4. Add this new device/application into CS-MARS




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

# Command and Control: Critical Data Reduction




**Incident Dashboard**
- **Aggregate**
- **Correlate**
- **Summarize**

**2,694,083 Events**

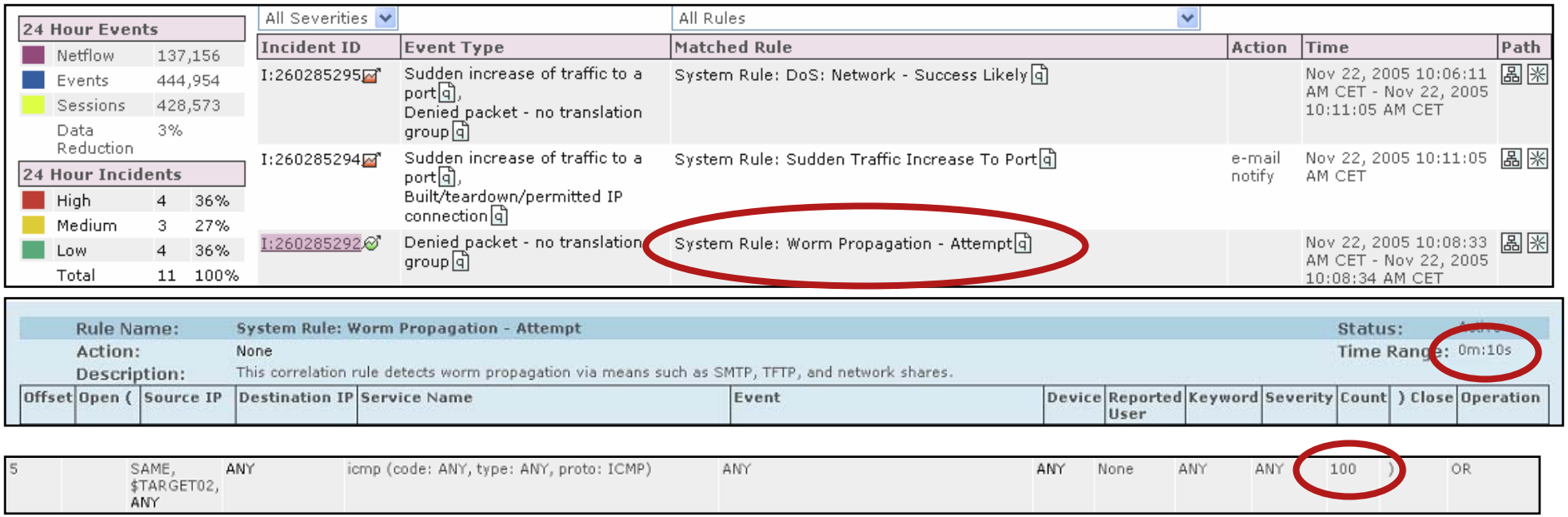
**992,511 Sessions**

**249 Incidents**

**61 High Severity Incidents**

**I Need to Clean My Network and Investigate Further**

# Command and Control Dashboard 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 | |

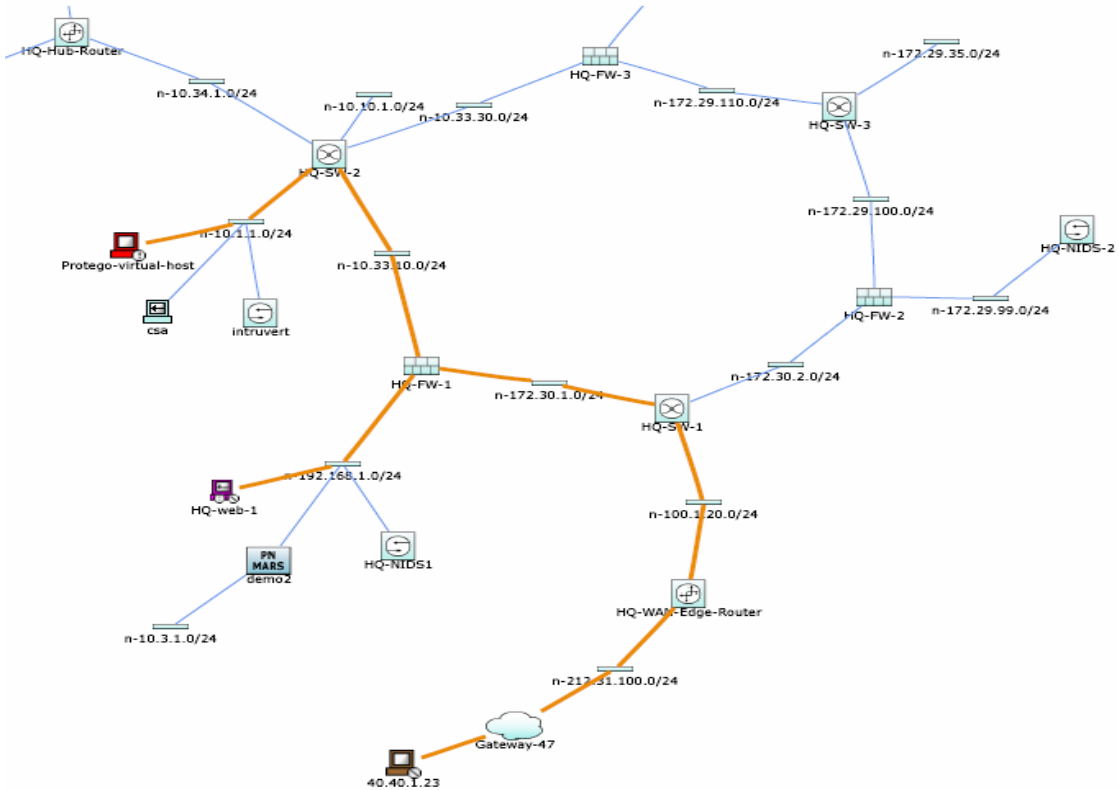
Rule Name: System Rule: Worm Propagation - Attempt
Status:
Action: None
Time Range: 0m:10s
Description: This correlation rule detects worm propagation via means such as SMTP, TFTP, and network shares.

| 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 functionality with just FW logs

# Attack Topology Awareness




## SureVector Analysis

**Visible and accurate attack path**

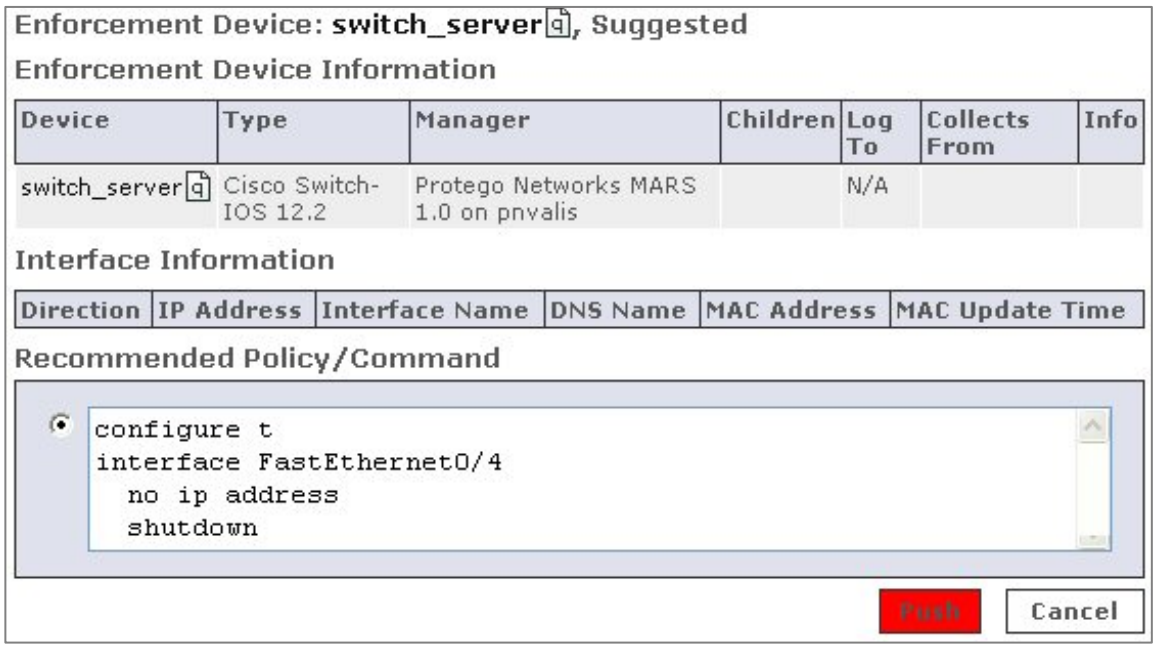
**Drill-down, full incident and raw event details**

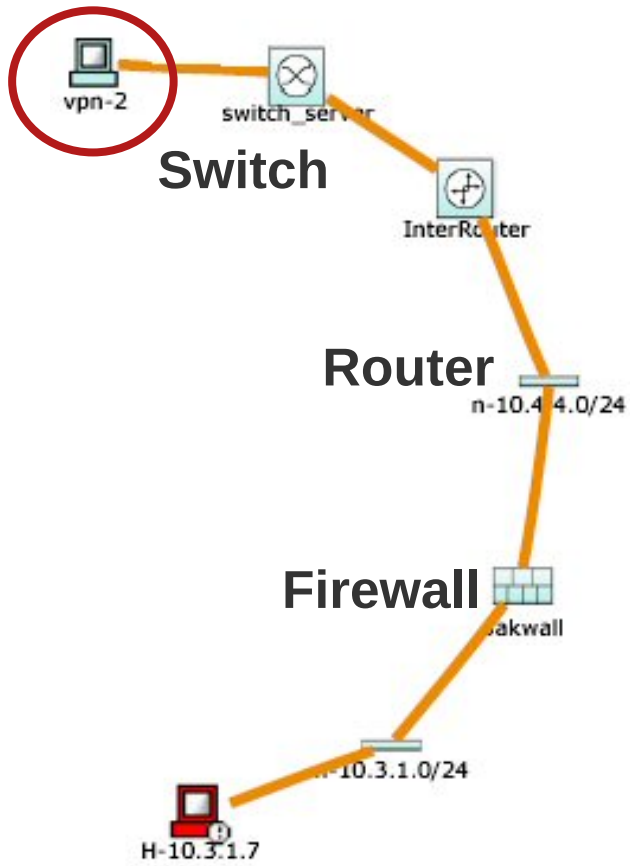
**Pinpoint the true sources of anomalous and attack behavior**

**More complete and accurate story**

# Command and Control: Attack 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**



# Reporting

# Compliance Reports

## Popular Reports With Customization and Distribution Options
## Queries Saved as Rules or Reports—Intuitive Framework

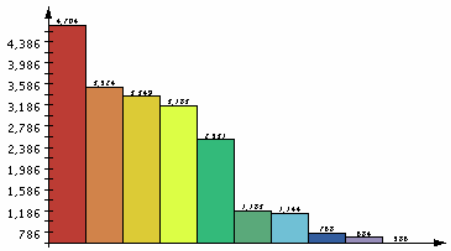
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

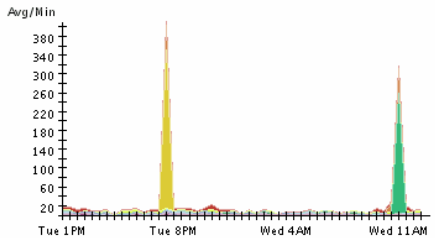
| Name | Schedule | Format | Recipients | Query | Description | Status | Submitted | Time Range |
|---|---|---|---|---|---|---|---|---|
| Activity: Denies - Top Destination Ports | *Every hour* | *Normal* | None | *Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports 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 |

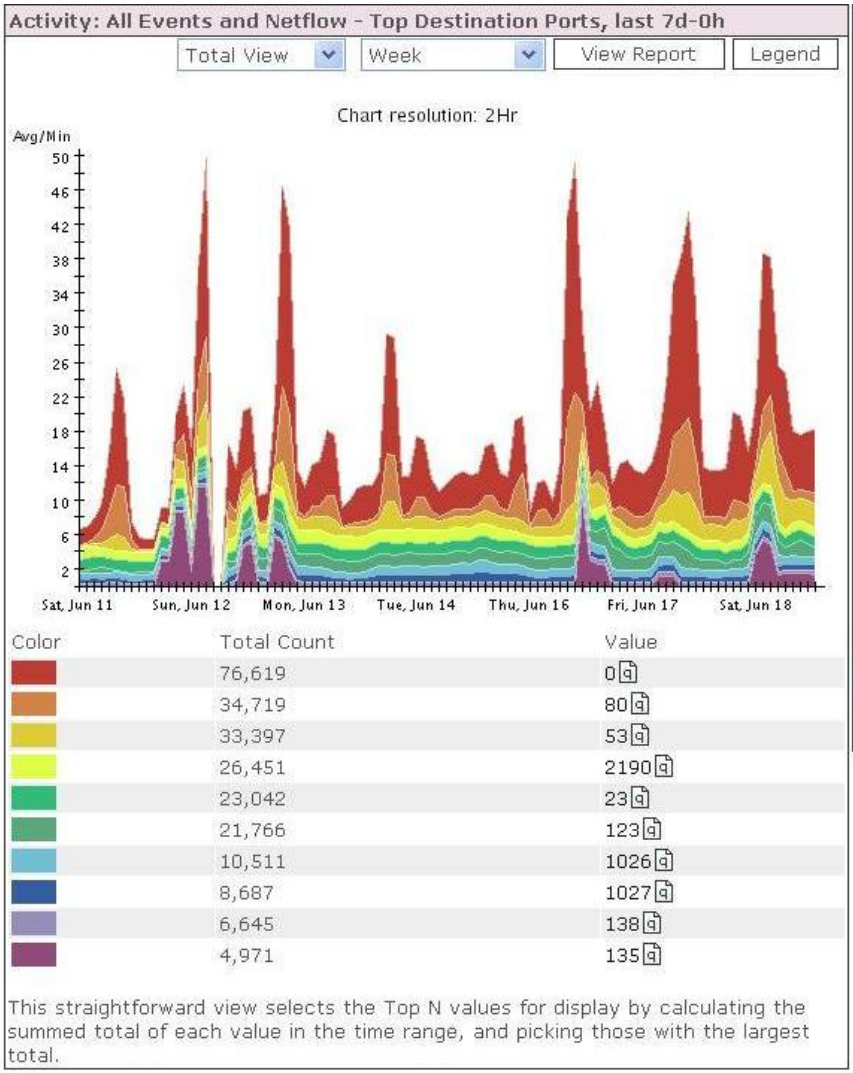
Keywords: [None]

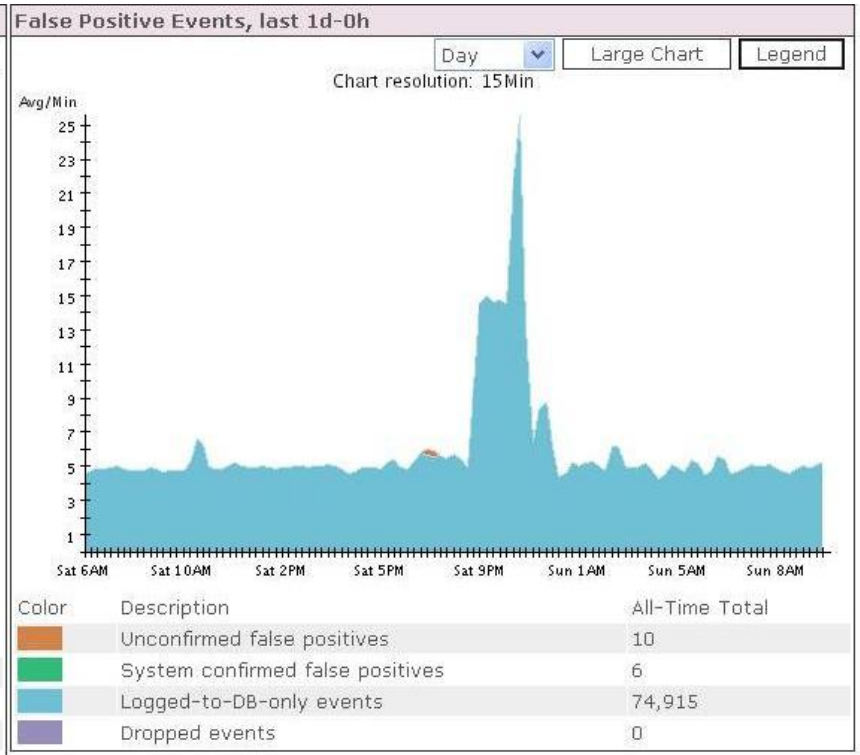



| Rank | | Count (# of sessions) | Raw Destination Port |
|---|---|---|---|
| | 1 | 4704 | 445 |
| | 2 | 3524 | 80 |
| | 3 | 3349 | 26686 |
| | 4 | 3183 | 135 |
| | 5 | 2531 | 47683 |
| | 6 | 1183 | 1026 |
| | 7 | 1144 | 0 |
| | 8 | 768 | 139 |
| | 9 | 684 | 9898 |

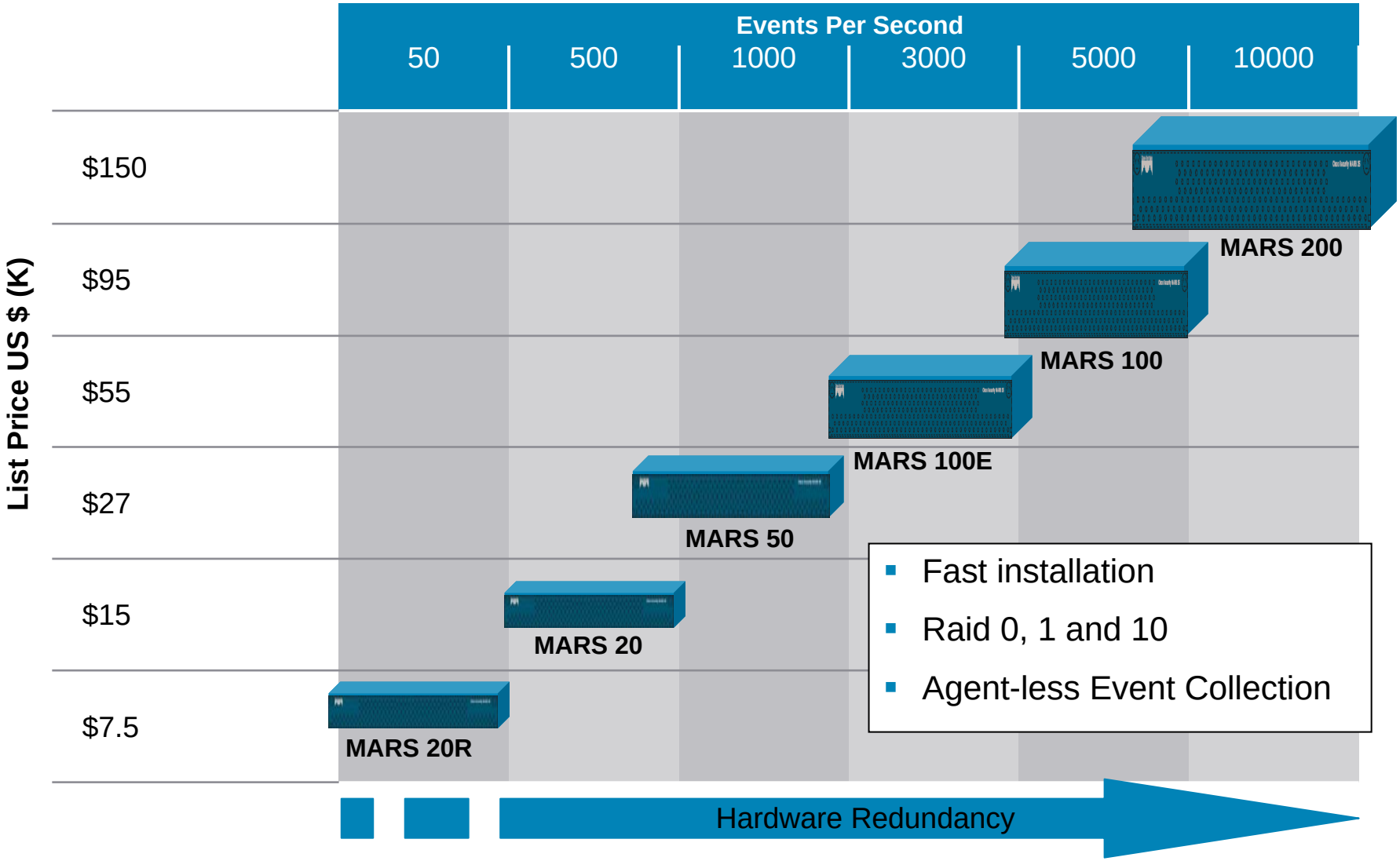
# Network Traffic Investigation



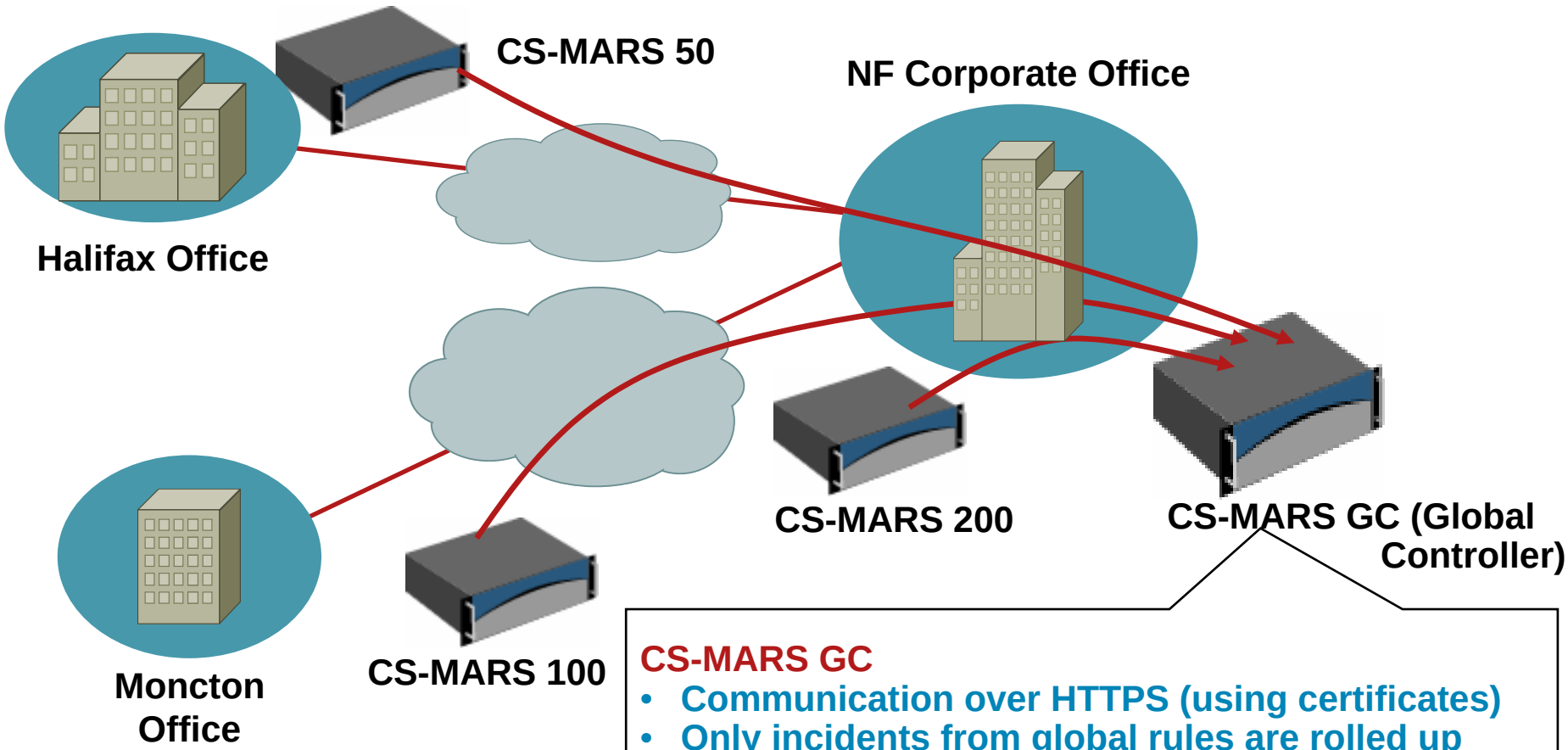



# CS-MARS Appliances

# CS-MARS Appliance Overview



# CS-MARS 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 Summary

**Better**

Integrated Network Intelligence

Isolate attacker by MAC, switch port

Stop attacks in progress

Visualize attack path

Security hardened OS and System

Purpose-built redundant design

**Faster**

Pipelined in-memory event analysis

Patent pending algorithms

10,000 EPS with full correlation (3-10x competition)

Scalable, distributed event analysis architecture with CS-MARS Global Controller

**Less expensive**

Appliance packaging

No hidden software/customization costs

Simple licensing – no software agents