Intelligent Information Network
Understanding and Deploying Network Admission Control

Michal Remper, CCIE#8151
Systems Engineer
mremper@cisco.com
Agenda

- Introduction
- NAC Framework
- NAC Architecture and Solution Overview
  - Landscape, components, policy considerations
- NAC Framework solutions
- Platforms and software components
- Conclusion
The Need for Admission Control

• Viruses, worms, spyware continue to plague organizations
  
  #1 cause of financial loss to enterprises

• Users are occasionally authenticated, BUT devices are not

• Non compliant & unmanaged devices pose an unacceptable risk
  
  Often source of infection
  
  Rogue assets untracked, invisible

• Device compliance as important as user authentication

*2005 FBI/CSI Report

“Endpoint systems are vulnerable and represent the most likely point of infection from which a virus or worm can spread rapidly and cause serious disruption and economic damage.”

– Burton Group
The Lingering Effect of Non-Compliant Endpoints
Example - “Blaster”

- Fast spreading – 128,000 systems infected in 1st 3 hours
- Worms linger on – need to put out ‘brush fires’
- CERT data on Blaster – 2+ weeks of damage
NAC Benefits

Dramatically Improves Security
• Ensures endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy
• Proactively protects against worms, viruses, spyware, and malware
• Focuses operations on prevention, not reaction

Extends Existing Investments
• Broad integration with multi-vendor antivirus, security, and management software
• Enhances investment in network infrastructure and vendor software

Increases Enterprise Resilience
• Comprehensive admission control across all access methods (LAN, WAN, Wireless, VPN, etc.)
• Prevents non-compliant and rogue endpoints from impacting network availability
• Reduces OpEx related to identifying and repairing non-compliant, rogue, and infected systems
Network Admission Control

What is it? NAC Controls access of all devices (managed, unmanaged, rogue)

What does Cisco offer?

Cisco Clean Access

1. Clean Access Agent
2. Discovery
3. Authentication Policy
4. Enforcement

The best turnkey appliance product
Address immediate pain-points with CCA

NAC Framework

1. Cisco Trust Agent
2. Discovery
3. Authentication Policy
4. Enforcement

The best technological approach for Enterprise
Begin Long-Term Enterprise Solution with integrated product and services

NAC Convergence = Future Proof
NAC FRAMEWORK PROTOCOLS
EAP (Extensible Authentication Protocol)

- Extensible Authentication Protocol (EAP)
- RFC 2284 http://www.ietf.org/rfc/rfc2284.txt
- RFC 3748 (Obsoletes 2284) http://www.ietf.org/rfc/rfc3748.txt
- An authentication framework which supports multiple authentication methods.
- EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.
- Extensions to EAP for NAC:
  - **EAP-TLV**: Carry posture credentials, adding posture AVPs, posture notifications
  - **Status Query**: New EAP method for securely querying the status of a peer without a full credential validation, L3 and L2 IP only
  - **EAPoUDP**: Use of EAP over IP for L3 transport
EoU (EAP over UDP)
NAC Posture Validation Flow
EAP-FAST Protocol

• Description

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS based RFC3748 compliant EAP method.

The tunnel establishment relies on a Protected Access Credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through AAA server.

PAC is a unique shared credential used to mutually authenticate client and server

PAC is associated with a specific user-ID and an Authority ID

PAC removes the need for PKI (digital certificates)
EAP-FAST Authentication Overview (802.1x)

1. Start EAP Authentication
   - Ask client for identity

2. Access Request with EAP-ID
   - Access Request with EAP-ID

Phase 1: Secure Tunnel (via TLS & PAC)

Phase 2: Client-side Authentication
- Perform sequence defined by EAP-FAST
  - EAP success
  - RADIUS Access Accept

Client derives PAC
- PAC Provisioning
- Protected DATA Transfer

Supplicant

RADIUS server

EAPoL-Start
- EAP-Request/Identity
- EAP-Response/Identity (EAP-ID)
HCAP (Host Credential Authorization Protocol)

- HTTP(S) communication between ACS and PV server
- HTTP(S) session between ACS and vendor servers to forward credentials from the ACS EAP-session with the client
- ACS forwards client credentials to one or more vendor servers
- ACS receives posture token response and optional notification messages from each vendor server
GAME (Generic Authorization Message Exchange)

- HTTP(S) session between ACS and vendor audit server extending Security Assertion Markup Language (SAML)
- ACS triggers posture validation of NAHs by the vendor audit server; polls periodically for audit decision
- Audit server responds with a posture state upon completion of the audit
NAC & Standards

- Cisco’s plan is to start NAC standardization process in 2006
- EAP-FAST and EAPoUDP currently published as informational Internet Drafts.
- Network Endpoint Assessment BOF was held at IETF Spring ’06 meeting. Co-chairs Cisco & Juniper
- Some refinement is occurring based on this meeting
- Initial scope targeted at subset of protocols between client and AAA server.
- Mailing list nea@ietf.org
NAC Data Types & Credentials

Attribute/Value pairs are packaged in EAP; 1KB limit per application

<table>
<thead>
<tr>
<th>OctetArray</th>
<th>Integer32</th>
<th>Unsigned32</th>
<th>String (UTF-8)</th>
<th>IPv4Addr</th>
<th>IPv6Addr</th>
<th>Time (4 octets)</th>
<th>Version (4 x 2-octet sets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>=, !=</td>
<td>=, &lt;, &gt;, !=, &gt;, &lt;=</td>
<td>=, &lt;, &gt;, !=, &gt;, &lt;=</td>
<td>=, !=, contains, starts with, regex</td>
<td>wildcards &amp; mask</td>
<td>wildcards &amp; mask</td>
<td>=, &lt;, &gt;, !=, &gt;, &lt;=</td>
<td>=, &lt;, &gt;, !=, &gt;, &lt;=</td>
</tr>
</tbody>
</table>

Namespace: <Vendor>:<Application-Type>:<Attribute>

<table>
<thead>
<tr>
<th>Application:</th>
<th>CTA</th>
<th>CTA</th>
<th>CSA</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor:</td>
<td>Cisco</td>
<td>Cisco</td>
<td>Cisco</td>
<td>Various</td>
</tr>
<tr>
<td>App-Type:</td>
<td>PA</td>
<td>Host</td>
<td>HIP</td>
<td>AV, PFW, etc.</td>
</tr>
</tbody>
</table>
NAC FRAMEWORK
ARCHITECTURE OVERVIEW
Network Admission Control Framework

• Cisco-led, Multi-partner Program
  Limits damage from non compliant devices, viruses, worms, & spyware
  Coalition of market leading vendors

• Restricts and Controls Network Access
  Endpoint interrogated for policy compliance
  Network determines appropriate admission enforcement for endpoint
  Comprehensive span of control covers all access methods and all endpoints

• A Cisco Self-Defending Network Initiative
  Dramatically improves network’s ability to identify, prevent, and adapt to threats
NAC Framework Architecture

Subject (Managed or Unmanaged host)

Enforcement

LAN

WAN

Remote

Decision & Remediation

ACS

Directory Server

Posture Validation Server(s)

Audit Server

Patch Server

Reporting Server
NAC Admission Flow

1. Traffic triggers challenge
2. Credentials
3. Credentials
4a. Identity
4b. Posture
4c. Audit
5. Compliant?
6. Authorization
7. Enforcement
8. Notification
9. Status

Cisco Trust Agent (CTA)
Network Access Devices (NADs)
Cisco Secure ACS
Policy Server Decision Points & Audit

Directory Server
Policy Vendor Server (PVS)
Audit Server (AS)

EAP
RADIUS
GAME: HTTPS
LDAP, OTP
HCAP

Key: Optional
Mandatory

© 2005 Cisco Systems, Inc. All rights reserved.
NAC Posture States

- **Healthy** - Host is compliant; no restrictions on network access.

- **Checkup** – Host is within policy but an update is available. Used to proactively remediate a host to the Healthy state.

- **Transition** – Host posturing is in process; give interim access pending full posture validation. Applicable during host boot when all services may not be running or audit results are not yet available.

- **Quarantine** – Host is out of compliance; restrict network access to a quarantine network for remediation. The host is not an active threat but is vulnerable to a known attack or infection.

- **Infected** – Host is an active threat to other endpoint devices; network access should be severely restricted or totally denied all network access.

- **Unknown** - Host posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined. May also
NAC Compliance: QUARANTINE to HEALTHY

Host Attempting Network Access

Network Access Devices (NADs)

Cisco Secure ACS

Policy Server Decision Points

1. Update AV
2. Revalidation / Status-Query
3. Credentials
4. EAP
5a. Identity
5b. Posture
6. Authentication Pass
7. Authorization: HEALTHY
8. Enforcement (VLAN, ACL, URL redirect)
9. Notification
10. Healthy! Cisco Trust Agent (CTA)

Directory Server

Anti-Virus Policy Server

Compliant

DATs valid

Authorization:

Healthy!
NAC Agentless Host (NAH)

1. Traffic triggers challenge
2. No CTA
3a. Audit
3c. Audit
4. Compliant?
5. Authorization: QUARANTINE
6. Enforcement (VLAN, ACL, URL redirect)
7. QUARANTINE!

Note: NAH in 802.1x currently unsupported!
NAC Logical Roles

Subject
- Offers ID & state
- Assist remediation
- Managed & unmanaged

Policy Enforcement Point
- Visibility & assessment trigger
- Authorization control

Policy Decision Point
- AAA function
- Remediation services
- Ties to many existing (and new) services/tools
- Audits ‘Agentless’ systems (non-responsive)
NAC Logical Components

NAC1
- Many Vendors
- Open License Program
- NT, XP, 2000, 2003
- RedHat Linux
- Cisco CTA Porting
- TA OEM & Authoring

NAC2
- EAPoUDP
- EAPo802.1x
- Switches (2900, 3500, 3700, 4000, 6500)
- Wireless AP & WLSM
- ASA, PIX
- SSL Devices

NAC2.x
- Initial vendors integrated
- NR Audit Server API
- Open License Program

Vendor Server
- Cisco Secure ACS

Host
- Security App
- Plug-ins

Network Access Device
- Non-responsive Audit Server
- AAA Server

EAPoUDP
RADIUS
HCAP
GAME
Strong NAC Partner Program

ANTI VIRUS

REMEDIATION

AUDIT

CLIENT SECURITY
NAC FRAMEWORK COMPONENTS OVERVIEW
Overview of NAC Components

• Posture Agent (Cisco Trust Agent)
• Network Access Device (NAD)
• Cisco Secure ACS
Cisco Trust Agent 2.0 (Posture Agent)

- Supported on Windows 2000, XP, 2003 and Red Hat Linux
- Supports 2 transport layers
  - EAPoUDP - layer 3
  - EAPo802.1x - layer 2 (Windows only)
- Includes OEM 802.1x supplicant from Meetinghouse Data Communications
  - Wired functionality only
  - Can be replaced by a retail version from either Funk or MDC for full feature support
- Gathers OS information including patch and hotfixes
- Support browser auto-launch
- Includes Customer Scripting Interface
- Backward compatible with CTA 1.0 posture plugins from NAC Program Participants
Network Access Device (Policy Enforcement Point)

- Policy enforcement point for NAC Framework. Policies defined in ACS are enforced by NAD.
- Includes NAC support for Layer 2, Layer 3, Wireless, VPN
- Initiates EAP through client discovery
- Support for NAC assessment Methods
  - NAC L3 IP (router, VPN)
  - NAC L2 IP (switch)
  - NAC L2 802.1x (switch, wireless)
Access Control Server (ACS) v4.0
(Policy Creation and Decision Point)

- NAC policy and enforcement decision are made here.
- Integration point for external policy servers, remediation servers, audit servers, reporting servers
- EAP-FAST, HCAP, GAME protocol support for NAC.
- Network Access Profiles
  Services: Groups, Protocols, Attributes
  Authentication: Protocols, Directories
  Compliance: Posture & Audit Policies
  Authorization: Groups, RACs, ACLs
- Template Configuration
- Configuration Cloning
POSTURE ASSESSMENT METHODS
**Posture Assessment Methods**

- **Posture assessment methods**
  - **NAC L3 IP**: at a layer 3 hop via IP, such as the perimeter, WAN, or distribution layer
  - **NAC L2 IP**: at a layer 2 switch port via IP, independent 802.1x
  - **NAC L2 802.1x**: via 802.1x at an L2 connection point (switch port or wireless AP)

- **Methods to perform a posture assessment**
  - *In-band*: obtain application state via CTA (an agent), and assess it in the policy system
  - *Out-of-band*: dynamic assessment (audit) of endpoint, mainly for ‘Agentless’ endpoints
  - *Exceptions*: create static exception handling for known assets (MAC, IP, port)

- **Agentless assessment useful for dynamic asset identification & risk**
  - Called **NAC Agentless Host**, “non-responsive audit”, or out-of-band assessment
  - Most Agentless technologies require IP connectivity to endpoint (scanning, login, or web download), others tie into inventory database systems
NAC L3 IP
Assess Posture (Only) at the Perimeter & Distribution Layers

• Deployed as a “chokepoint” at L3 perimeter points (like a firewall)
  - WAN edge: interoffice, extranet
  - Interior segmentation: non-production/lab networks, inter-department, distribution layer, data center access
  - Remote Access – IPsec and dial-in remote access aggregation ingress

• Posture assessment triggered and performed at L3
  - Triggers on IP packets from new sources
  - Control traffic via EAPoUDP

• Enforcement via ACLs (L3/4 controls) & URL redirection (provides NRH feedback)
• May be used in parallel to any user & device validation (e.g. IPsec, auth-proxy)
L3 Over-the-Wire Communications

Current AV Client-Server communication
Network as Pass-through

Client
- IPC
- PP
- DLL

Cisco Trust Agent

EAP Status Query

EAP-TLV/Posture +Posture-Notification

PEAP/EAP-FAST

EAPoUDP

Host

NAD

Third Party Policy Server

HCAP

ACS Server

Network as Pass-through

Cisco.com
1. IP packet triggers *Intercept ACL* on NAD
   Default ACL determines initial & interim network access
2. NAD triggers posture validation with CTA (*EAPoUDP*)
3. CTA sends posture credentials to NAD (*EAPoUDP*)
4. NAD sends posture credentials to AAA (*EAPoRADIUS*)
5. AAA can proxy portions of posture authentication to vendor server (*HCAP*)
6. AAA validates posture, determines authorization rights (*Healthy, Checkup, Quarantine*)
7. AAA sends authorization policy to NAD (*ACLs, URL redirection*)
   Notification may be sent to applications on host also
8. Host IP access granted (*or denied, restricted, URL redirected*)
1. Inactive Endpoint – Confirm inactive endpoint has not changed
   Called “L3 EAP Status Query”: New EAP method between CTA and NADs (not ACS)
   Router periodically polls to make sure:
   1) CTA is still there
   2) It’s the same validated device
   3) Posture hasn’t changed
   Authentication based on keyed MAC (Uses keys derived in EAP-Posture (PEAP))

2. Reassess Active Endpoint – Confirm continued compliance
   CTA indicates posture change by not responding to Status Query, triggers revalidation
**NAC L3 IP: NAC Agentless Host**

**Vulnerability Assessment-Based Example**

1. NAD attempts in-band NAC and gets no response from endpoint
2. NAD passes IP address of endpoint (from packet header) to Audit Server
3. NAD allows endpoint policy-defined controlled access to network
   - For example, to allow the Audit server to interact with the endpoint
   - Enforcement is done via ACLs
4. Audit Server assesses endpoint (e.g. vuln assessment tool scans endpoint)
5. Result provides best-effort device type (PC, printer) & risk assessment
6. Audit results then map to authorization policy in AAA
7. Resultant access policy then transferred to NAD (ACLs & URL redirection)
NAC L2 IP
Assess Posture (Only) at the Access-Layer

- Deployed at first connection into network at the access layer
  LAN – access layer connections directly in the switching infrastructure
- Posture assessment triggered and performed at L3 on a L2 switch port
  Triggers at layer 3 via DHCP & ARP requests from new sources
  Occurs after VLAN assignment before general IP access is granted for each source
  Control traffic via EAPoUDP
- Enforcement via ACLs (L3/4 controls) & URL redirection (provides NRH feedback)
  There are different ACL technologies (Port ACLs, VLAN ACLs, Policy-Based ACLs)
- Can be performed after 802.1x user & device validation (totally independent)
  Microsoft 802.1x supplicant use-case (until it supports NAC)
NAC L2 IP: System Flow
CTA-Capable Endpoints

1. DHCP or ARP request triggers NAD
2. NAD triggers posture validation with CTA (EAPoUDP)
3. CTA sends posture credentials to NAD (EAPoUDP)
4. NAD sends posture credentials to AAA (EAPoRADIUS)
5. AAA can proxy portions of posture authentication to vendor server (HCAP)
6. AAA validates posture, determines authorization rights (Healthy, Checkup, Quarantine)
7. AAA sends authorization policy to NAD (ACLs, URL redirection)
   Notification may be sent to applications on host also
8. Host IP access granted (or denied, restricted, URL redirected)
NAC L2 IP: NAC Agentless Host
Vulnerability Assessment-Based Example

- NAD attempts in-band NAC and gets no response from endpoint
- NAD passes IP address of endpoint (via DHCP snooping or ARP) to Audit Server
- NAD allows endpoint policy-defined controlled access to network
  For example, to allow the Audit server to interact with the endpoint
  Enforcement is done via ACLs
- Audit Server assesses endpoint (e.g. vuln assessment tool scans endpoint)
- Result provides best-effort device type (PC, printer) & risk assessment
- Audit results then map to authorization policy in AAA
- Resultant access policy then transferred to NAD (ACLs & URL redirection)
NAC-L2-802.1x: Overview

- Identity and/or posture authorization: switches only
- Leverages existing 802.1x (EAP) L2 session to perform posture assessment and enforcement
  - EAP-FAST required for posture authorization
  - MSCHAPv2, EAP-TLS, and EAP-GTC
- Enforcement via dynamic VLANs
  - 6500 also supports Policy Based ACLs
NAC L2 802.1x
Assess Identity & Posture in Homogeneous, Managed Access Layer

- Deployed at first connection into network at the access layer
  - LAN – access layer connections directly in the switching infrastructure
  - Wireless – mobile devices within the office
- Posture assessment triggered and performed at L2 in 802.1x
  - Endpoints must have 802.1x supplicant in addition to CTA for in-band assessment
  - Triggers on layer 2 connection via 802.1x protocol
  - Control traffic via EAPo802.1x, no L3 IP access given during in-band assessment
- Enforcement via VLANs (L2 controls)
- Used in conjunction with user and or device authentication in 802.1x
NAC L2 802.1x: System Flow
CTA-Capable Endpoints with NAC-Capable 802.1x Supplicants

1. 802.1x connection setup between Network Access Device (NAD) and endpoint
2. NAD requests credentials from endpoint (EAPo802.1x)
   This may include user, device, and/or posture
3. CTA, via NAC-capable supplicant, sends credentials to NAD (EAPo802.1x)
4. NAD sends credentials to AAA (EAPoRADIUS)
5. AAA can proxy portions of posture authentication to vendor server (HCAP)
   User/device credentials sent to authentication databases (LDAP, Active Directory, etc)
6. AAA validates credentials, determines authorization rights
   E.g. visitors given GUEST access, unhealthy devices given QUARANTINE access
7. AAA sends authorization policy to NAD (VLAN assignment)
   Notification may be sent to applications on host also
8. Host assigned VLAN, may then gain IP access (or denied, restricted)
NAC L2 802.1x: NAC Agentless Host
Assess Identity & Posture in Heterogeneous, Partially Managed Access Layer

- Dynamically handles devices incapable of NAC via Audit Server
  Device granted controlled access to network (e.g. Audit or Quarantine VLAN)
  Switch learns IP address (DHCP snooping or ARP), passes to Audit Server
  Audit Server assesses endpoint (e.g. vuln assessment tool scans device on access)
  Audit result provides best-effort device type (PC, printer) & risk assessment
  Differentiated access enforced by VLAN segmentation at layer 2
- Will not be available in all NAC L2 802.1x-capable platforms
## NAC Assessment Method Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>NAC-L2-802.1x</th>
<th>NAC-L2-IP</th>
<th>NAC-L3-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger mechanism</td>
<td>Data Link Up</td>
<td>DHCP or ARP</td>
<td>Forwarded Packet</td>
</tr>
<tr>
<td>Machine Identity</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Identity</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posture</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>VLAN assignment</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL-Redirection</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Downloadable ACLs</td>
<td>6500-only (PBACLS)</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Posture Status Queries</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Reauthentication/Revalidation</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Device</td>
<td>Switch or AP</td>
<td>Switch</td>
<td>Router</td>
</tr>
<tr>
<td>EAP over</td>
<td>802.1x</td>
<td>UDP</td>
<td>UDP</td>
</tr>
</tbody>
</table>
CONFIGURATION DETAILS
NAC-L2/L3-IP: IOS Required Configuration

```plaintext
aaa new-model
aaa authentication eou default group radius
aaa authorization auth-proxy default group radius
aaa session-id common

radius-server host 10.100.100.100 auth-port 1645 acct-port 1646
radius-server key cisco123
radius-server vsa send authentication
ip radius source-interface FastEthernet0/0

ip admission name NAC-L2-IP eapoudp
ip admission name NAC-L2-IP-Bypass eapoudp bypass
ip admission name NAC-L3-IP eapoudp list EoU-ACL

ip access-list extended EoU-ACL
deny udp any any eq domain
deny tcp any host 10.100.100.101 eq www
permit ip any any

ip access-list extended Interface-ACL
permit udp any any eq 21862
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit tcp any host 10.100.100.101 eq www
```
NAC-L2/L3-IP: IOS Required Configuration

eou timeout hold-period 60 #Delay re-EAP after EAP failure
eou timeout revalidation 60 #Timeout to re-check all credentials
eou timeout status-query 60 #ACS can override, enforces policy changes
ip auth-proxy inactivity-timer 60 #How often check for status changes
#Equivalent to EoU revalidation timer

eou allow clientless #Permit agentless hosts, used for auditing

ip http server #IOS web server required for URL redirection
ip http authentication aaa #Enable auth-proxy
ip http secure-server #SSL

eou logging
logging 10.100.100.150
NAC-L2/L3-IP: IOS Interface Configuration

Routers

<table>
<thead>
<tr>
<th>Interface FastEthernet0/0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address 10.7.7.1 255.255.255.0</td>
</tr>
<tr>
<td>ip access-group Interface-ACL in</td>
</tr>
<tr>
<td>ip admission NAC-L3-IP</td>
</tr>
</tbody>
</table>

Switches

<table>
<thead>
<tr>
<th>ip device tracking</th>
<th>#Build IP device table from ARP requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface GigabitEthernet1/0/1</td>
<td></td>
</tr>
<tr>
<td>switchport</td>
<td></td>
</tr>
<tr>
<td>switchport mode access</td>
<td></td>
</tr>
<tr>
<td>switchport access vlan 7</td>
<td></td>
</tr>
<tr>
<td>ip access-group Interface-ACL in</td>
<td></td>
</tr>
<tr>
<td>ip admission NAC-L2-IP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ip dhcp snooping vlan 7</th>
<th>#Need ACL or DHCP Snooping/DAI to trigger NAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping vlan 7</td>
<td>#Enable DHCP snooping on VLAN 1000</td>
</tr>
</tbody>
</table>
#exception based method, DEVICE-TYPE (CDP IP PHONE), MAC or IP
identity profile eapoudp
  device authorize ip-address 10.7.7.100 policy No-NAC #static NAC bypass by IP address
  device authorize mac-address 0010.a4c4.dfb4 #statically permit this MAC to bypass NAC
  or use ACS for MAC or IP whitelisting

identity profile No-NAC
  access-group No-NAC-ACL
  redirect url http://10.100.100.101/update #optional - redirect

#Statically permit access
ip access-list extended No-NAC-ACL
  permit ip any any
NAC-L2/L3-IP: Centralized NAH with ACS

CTA 2.0
DHCP (.100)

VLAN 7
10.7.7.0 /24
int VLAN7=.1

NADs

ACSv4.0
.100

10.100.100.0/24
VLAN100

Vendor Server
.101

eou allow ip-station-id          #Sends IP address instead of MAC address (default)

#Alternate method
eou allow clientless            #Sends clientless request to ACS

#interface ACL only permits basic L3/L4 services; Switches support MACs as well
ip access-list extended Interface-ACL
  permit udp any any eq 21862   #permit EAPoUDP
  permit udp any eq bootpc any eq bootps #permit DHCP

interface ethernet0
ip access-group Interface-ACL in
NAC-L2/L3-IP: CatOS Required Configuration

```
set radius server 10.100.100.100 primary
set radius key cisco123

set interface sc0 100 10.100.100.1 255.255.255.0 #Required – use only sc0 for NAC

set security acl ip nac-l2-ip permit arp #PBACL definition
set security acl ip nac-l2-ip permit arp-inspection any any #Required for CatOS
set security acl ip nac-l2-ip permit dhcp-snooping
set security acl ip nac-l2-ip permit eapoudp

set security acl ip nac-l2-ip permit ip group Healthy_hosts any #PBACLs
set security acl ip nac-l2-ip deny ip group Infected_hosts any #sec:pg=Infected_hosts
set security acl ip nac-l2-ip permit ip group Exception_hosts any
set security acl ip nac-l2-ip permit ip group Clientless_hosts host 10.100.100.101
set security acl map nac-l2-ip 7 #Apply to VLAN 7
```
NAC-L2/L3-IP: CatOS Configuration
continued…

Required Configuration (CatOS)

set eou enable
set eou allow clientless enable #Allow clientless access via ACS
set port eou 3/1 enable #Enable eou on port!
set vlan 7 3/1

Optional Configuration (CatOS)

set eou authorize ip 1.1.1.1 policy NAC #Static IP exception, wildcard too
set eou authorize mac 0000.0000.0001 policy NAC #Static MAC exception, wildcard too
NAC-L2-802.1x Configuration

**IOS**

```
aaa authentication dot1x default group radius
aaa authorization network default group radius

radius-server host 10.100.100.100 auth-port 1645 acct-port 1646
radius-server key cisco123

dot1x system-auth-control

interface GigabitEthernet1/0/1
  dot1x port-control auto
  dot1x timeout reauth-period server
  dot1x reauthentication
```

**CatOS**

```
set radius server 10.100.100.100 auth-port 1812 primary
set radius key cisco123

set dot1x system-auth-control enable

set port dot1x 3/1 port-control auto
set port dot1x 3/1 re-authentication enable
```
NAC Enforcement Features/Tradeoffs

- NAC L3 IP—EAPoUDP for posture only (Routers and VPN)
- NAC L2 IP—EAPoUDP for posture only (L2 switchports)
- NAC L2 802.1x—EAP over 802.1x (L2 switchports)

<table>
<thead>
<tr>
<th>Feature</th>
<th>NAC L2 802.1x</th>
<th>NAC L2 IP</th>
<th>NAC L3 IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Mechanism</td>
<td>Data Link Up</td>
<td>DHCP or ARP</td>
<td>Forwarded Packet</td>
</tr>
<tr>
<td>Machine Identity</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Identity</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VLAN Assignment</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL-Redirection</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Downloadable ACLs</td>
<td>6500-only (PBACLs)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Posture Status Queries</td>
<td>ASQ (CSA)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>802.1x Posture Change</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## NAC Exceptions and Whitelisting

<table>
<thead>
<tr>
<th>Component</th>
<th>NAC L2 802.1x</th>
<th>NAC L2 IP</th>
<th>NAC L3 IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAD (distributed)</td>
<td>MAC-Auth-Bypass (6500 only, identity + posture)</td>
<td>Device Type, IP, or MAC; Intercept ACL (IP/MAC)</td>
<td>Device Type, IP, or MAC; Intercept ACL (IP)</td>
</tr>
<tr>
<td>ACS whitelist</td>
<td>MAC-Auth-Bypass (above)</td>
<td>MAC\IP wildcards (posture only)</td>
<td>MAC\IP wildcards (posture only)</td>
</tr>
<tr>
<td>(centralized)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit (centralized)</td>
<td>Active network scan, remote login, browser object, hardware/software inventory</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Audit Server: Network Scanning Method

No CTA
DHCP (.100)

VLAN 7
10.7.7.0 /24
int VLAN7=.254

NADs

ACSv4.0
.100
10.100.100.0/24
VLAN100

Audit Server
.140

Token state depends on policy set on AS and result of scan. URL redirection may be used to AS

Attempt Network Access

EAPoUDP Hello/Req
EAPoUDP Hello/Req
EAPoUDP Hello/Req
EAPoUDP Hello/Req

Timeout! Access request session ID-1, IP 10.7.7.100

ACS Enters Transition State ID-1
Scan in-progress ID-1

Timeout! Update Session ID-1

Assign HEALTHY RAC

Audit Request ID-1
Audit Response: In-progress

Audit request ID-1 IP = 10.7.7.100
Audit Request ID-1
Audit Response HEALTHY

EAPoRADIUS
GAME

IP Connectivity Established

CTA not resident or accessible. Make certain ACLs permit scan!
Audit Server: URL Redirection-Applet Method

CTA not resident or accessible. Make certain ACLs permit HTTP!

No CTA
DHCP (.100)

VLAN 7
10.7.7.0 /24
int VLAN7=.254

NADs

ACSv4.0
10.100.100.0/24
VLAN100

Audit Server
1.140

Token state depends on policy set on Audit Server and result of scan. URL redirection required to AS.
WIRELESS LAN
NAC Framework
WLAN Deployment

Distributed WLAN Solution

- Hosts Attempting Network Access
- Network Access Device
- Cisco Aironet Autonomous IOS-based AP
- Dynamic VLAN Assignment
- Select a WDS Device: Cat6k w/WLSM or Cisco Aironet AP
- Cisco Secure ACS
- RADIUS
- HCAP

Centralized WLAN Solution

- Hosts Attempting Network Access
- Network Access Device
- Cisco Aironet Lightweight AP
- Cisco WLAN Controller
- Dynamic VLAN Assignment
- Cisco Secure ACS
- RADIUS
- HCAP

Cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.
NAC Wireless LAN—Network Access

  - NAC for WLAN enforces device security policy compliance at the access point when WLAN clients attempt to access the network
  - Access points implement NAC policy via VLAN assignment
- NAC support in Cisco Integrated Wireless Network
  - Distributed WLAN solution via Cisco IOS® Software upgrade
    - Cisco Aironet (Cisco IOS Software-based) access point in stand-alone or wireless domain services (WDS) mode—NAC framework and NAC appliance
    - Cisco Catalyst 6500 Series WLSM as WDS device—NAC framework only
  - Centralized WLAN solution
    - Cisco Aironet lightweight access points connected to Cisco WLAN Controller—NAC framework and NAC appliance
NAC Wireless LAN—Clients

- WLAN client devices require an IEEE 802.1X supplicant that supports NAC
  
  Cisco®-supplied supplicant is for Ethernet adapter only, not WLAN adapter

- Meetinghouse and Funk will provide both wired and wireless L2 NAC supplicants

- NAC support in Cisco-compatible version 4
  
  Cisco-compatible client devices (laptops, PDA, tablets, etc.)

  Embedded into wireless client silicon chipset

  Intel lead collaborator
NAC FRAMEWORK
AVAILABILITY
## NAC Schedule

<table>
<thead>
<tr>
<th></th>
<th>NAC1</th>
<th>NAC2</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Devices</strong></td>
<td>IOS Routers (17xx – 75xx), VPN 3000</td>
<td>Switches (29xx-65xx), Wireless (WLC, WLSM)</td>
<td>PIX, ASA, 6500 Svc Modules</td>
</tr>
<tr>
<td><strong>Cisco Trust Agent Support</strong></td>
<td>Windows NT, XP, 2000, 2003</td>
<td>Red Hat Linux</td>
<td>Vendor OEM/ Author, Solaris, MACOS, HPUX, AIX</td>
</tr>
<tr>
<td><strong>Integration</strong></td>
<td>Vendor Program</td>
<td>Many Vendors Integrated</td>
<td>Standards</td>
</tr>
<tr>
<td><strong>Device Communications</strong></td>
<td>Layer 3 EAPoUDP</td>
<td>Layer 2 EAPo802.1x</td>
<td>HTTP/SSL</td>
</tr>
<tr>
<td><strong>Non-Responsive Endpoints</strong></td>
<td>Exception List Single Policy</td>
<td>Initial Differentiated Policy for Agentless Hosts</td>
<td>Broad Agentless Host Handling</td>
</tr>
<tr>
<td><strong>Quarantine Method</strong></td>
<td>Layer 3 ACLs, URL Redirect</td>
<td>VLANs, Port/VLAN ACLs</td>
<td>Tag &amp; template, QoS</td>
</tr>
</tbody>
</table>

© 2005 Cisco Systems, Inc. All rights reserved.
NAC Framework Solutions: Remediation

- Example solution built with IBM Tivoli
- Network admission decisions are determined by policies on Cisco Secure ACS and managed by Tivoli Security Compliance Manager
NAC Framework Solutions: Audit

- Example Solution built with Qualys
- Traffic from hosts without CTA is blocked and redirected in audit segment. Audit scanner engine evaluates host and transmits information back to the policy server for Admission decision

Diagram:
- Host without CTA
- Network Access Device
- QualysGuard Scanning Engine
- Cisco Secure ACS

Steps:
1. Network Access Device
2. Cisco Secure ACS
3. QualysGuard Scanning Engine
4. QualysGuard Scanning Engine
5. Cisco Secure ACS
6. Network Access Device
NAC Framework Solutions: Audit & Remediation

- Example solution built with Altiris
NAP/NAC Deployment Scenarios

**Network AAA** – authorizes network access based on user auth, machine auth and posture validation

**Posture AAA** – Validates posture of the host

---

**Vista Client**

- 3rd Party System Health Agents (SHAs)
- Quarantine Agent (QA)
- EAP Host
- EAPoUDP
- 802.1x
- EAP FAST

- Components part of Vista O/S

---

Cisco developed EAPoUDP and EAP FAST modules distributed by Microsoft via Windows Update/WSUS

---

Health Certs allow hosts to move/reconnect without requiring full posture validation but cannot be revoked, so validity period must be commensurate with how often you expect policy to change

---

Network AAA – authorizes network access based on user auth, machine auth and posture validation

---

Posture AAA – Validates posture of the host

---

EAPoUDP

---

RADIUS

---

HCAP

---

Cisco ACS & Microsoft ISA or combined from single vendor

---

3rd Party Posture Validation Logic Plugs into Posture AAA via System Health Validator (SHV) API

---

In Band

---

Out of Band

---

Separate or Combined

---

Health Certificate Server

---

Network AAA

---

Posture AAA

---

EAP FAST

---

802.1x or UDP

---

RADIUS

---

Posture Validated & Health Cert issued

---

Health Certificate Server

---

RADIUS
Platforms and Components
# NAC Router Platform Support

- **NAC L3 IP shipped June 2004**
  - T-train images with Security
  - The same image that includes firewall, NIPS, and crypto
- **NAC Agentless host assessment expected in NAC2.1**
- **Mirage support expected in NAC2.1**
  - 16, 24, 48 port NM
  - 2800, 3700, 3800 switch platforms
  - NAC L2 802.1x & NAC L2 IP

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 18xx, 28xx, 38xx</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 72xx, 75xx</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 37xx</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 3640, 3660-ENT Series</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 2600XM, 2691</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 1701, 1711, 1712, 1721, 1751, 1751-V, 1760</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 83x</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 74xx, 73xx, 71xx (S-train)</td>
<td>TBD</td>
</tr>
<tr>
<td>Cisco 5xxx</td>
<td>TBD</td>
</tr>
<tr>
<td>Cisco 4500</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 3660-CO Series</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 3620</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 2600 non-XM Models</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 1750, 1720, 1710</td>
<td>No</td>
</tr>
</tbody>
</table>
VPN Concentrators

- Models 3005-3080
- Release v4.7 supports NAC L3 IP
- VPN Client does not include CTA
- Works with IPsec and L2TP/IPSec remote access sessions. NAC processing starts after an IPsec session is established
  Communication with CTA is within IPsec SAs
  NAC does not apply to PPTP, L2TP or LAN-to-LAN sessions
- Local exception lists also include OS type
- NAC Agentless Host assessment is not supported yet; timeline is TBD
### Catalyst Switch NAC2 Framework Support

**Progressive Functional Tiers**

<table>
<thead>
<tr>
<th>Platform, Supervisor</th>
<th>OS</th>
<th>NAC L2 802.1x</th>
<th>NAC L2 IP</th>
<th>NAC L3 IP</th>
<th>NAC Agentless Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>6500—Sup32, 720</td>
<td>Native IOS</td>
<td>Future</td>
<td>Yes</td>
<td>Future</td>
<td>NAC L2 IP</td>
</tr>
<tr>
<td>6500—Sup2</td>
<td>Native IOS</td>
<td>Future</td>
<td>Yes</td>
<td>No</td>
<td>NAC L2 IP</td>
</tr>
<tr>
<td>6500—Sup32, 720</td>
<td>Hybrid</td>
<td>Yes</td>
<td>Yes</td>
<td>Future</td>
<td>NAC L2 IP</td>
</tr>
<tr>
<td>6500—Sup2</td>
<td>Hybrid</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>NAC L2 IP</td>
</tr>
<tr>
<td>6500—Sup2, 32, 720</td>
<td>CATOS</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>NAC L2 IP</td>
</tr>
<tr>
<td>4500 Series— SupII+, II+TS, IV, V, V-10GE</td>
<td>IOS</td>
<td>Yes</td>
<td>Yes</td>
<td>Future</td>
<td>NAC L2 IP</td>
</tr>
<tr>
<td>4900</td>
<td>IOS</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3550,3560, 3750</td>
<td>IOS</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2950,2940, 2955, 2960, 2970</td>
<td>IOS</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6500—Sup1A</td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>5000</td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4000 Sup I, II, III (IOS)</td>
<td>CATOS</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>3500XL, 2900XM, 1900</td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
New Features

Network Access Profiles
Services: Groups, Protocols, Attributes
Authentication: Protocols, Directories
Compliance: Posture & Audit Policies
Authorization: Groups, RACs, ACLs

ACS determines authorization rights
Least privileges of all authentication results
(Healthy + Checkup = Checkup)

Audit Services
Whitelisting by MAC & IP addresses

Software only release
Appliance update in v4.1
Cisco Trust Agent 2.0

- Supported on Windows 2000, XP, 2003 and Red Hat Linux
- Supports 2 transport layers
  - EAPoUDP - layer 3
  - EAPo802.1x - layer 2 (Windows only)
- Includes OEM 802.1x supplicant from Meetinghouse Data Communications
  - Wired functionality only
  - Can be replaced by a retail version from either Funk or MDC for full feature support
- Gathers OS information including patch and hotfixes
- Support browser auto-launch
- Includes Customer Scripting Interface
- Backward compatible with CTA 1.0 posture plugins from NAC Program Participants
Cisco Trust Agent (CTA) 2.0 Features

- Free
- Wired only supplicant (on Windows platforms only)
- EAP-FAST only with MSCHAPv2, EAP-TLS, and EAP-GTC
- Initiates EAPoL-Start on posture plugin state change
- DHCP release/renews
Cisco Trust Agent 2.1  
(Posture Agent)

• This release extends NAC support for EAPoUDP on MAC OS X  
• OS X 10.3 & 10.4 on PPC, OS X 10.4 on Intel-based  
• Configurable size for posture plug-in buffers  
  Posture plugins and host posture plugins can now return information longer than 1024 bytes to ACS.  
  Configured through ctad.ini file  
• Asynchronous status query  
  CTA bridges the gap for legacy plugins (non-802.1x) to comply to 802.1x  
  CTA can actively query plugin for any application status change  
• Packaging simplification for Windows  
  New unified Microsoft installer (MSI) for both verbose and silent install.  
• MAC Address information  
  MAC address included as part of posture  
• Non-blocking plugin queries  
  Asynchronous querying of plugins  
  CTA will not be blocked to wait for response from earlier queries.
CTA 2.1
802.1x Supplicant Enhancements

802.1x Supplicant (Lite) Enhancements:

• Machine Authentication Only
  Option to exclude user authentication and perform machine authentication only

• Configurable external identity
  Configurable identity string in external identity in EAP-FAST

• Machine authentication using machine password option
  Along with Certificate and Machine PAC, option to use machine password
802.1x Supplicant Strategy is Important

• Customers interested in NAC with 802.1x must use compatible supplicant
• No existing supplicants support NAC today (including Microsoft)
  NAC requires new supplicant features (e.g. EAP chaining, EAP-TLV…)

• Cisco will ship an OEMed NAC-only “lite” supplicant embedded in CTA
  Benefits: available when NAC phase 2 ships, no charge
  Considerations: only works in NAC & IBNS wired envmnts, no central mgmt tool
• Cisco is working with primary supplicant providers (Meetinghouse & Funk) for support in their commercial releases
  Benefits: available shortly after phase 2, broad feature support, centralized mgmt
  Considerations: requires investment in supplicant technology on hosts
• Cisco is working with OS vendors to expand supplicants to support NAC features
• NAC features as part of the CCX specifications in v4
## CTA and Supplicant Comparisons

<table>
<thead>
<tr>
<th>Feature</th>
<th>CTA 2.0</th>
<th>Meetinghouse Aegis</th>
<th>Funk Odyssey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail Cost</td>
<td>Free</td>
<td>**</td>
<td>**</td>
</tr>
<tr>
<td>NAC-L2/L3-IP</td>
<td>✓</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>NAC L2 802.1x Wired</td>
<td>✓ (Windows)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NAC L2 802.1x Wireless</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PEAP-GTC</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EAP-FAST*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Others</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Supported OSes</td>
<td>Windows 2000, XP, 2003; RedHat Ent Linux (no supplicant)</td>
<td>Expected on Windows NT4, 2000, XP, 2003; RedHat Ent Linux **</td>
<td>Expected on Windows NT4, 2000, XP, 2003; RedHat Ent Linux **</td>
</tr>
</tbody>
</table>

* Must use EAP-FAST for NAC L2 802.1x with identity + posture compliance

** Meetinghouse and Funk information given without any guarantee expressed or implied. For specific pricing and platform support information, please contact each vendor directly
Cisco Security Agent (CSA)

- CSA is an optional NAC component
- CSA v4.5 and later includes CTA v1.0
  CTA 2.0 bundling expected in 5.0. However, can load any version for install through CSA.
- HIPS technology is recommended to protect the integrity files of all host security applications, including CTA!
- CSA policies can lockdown the host based on the posture received from a NAC authorization
  e.g. CSA can disable all host applications except patch management and anti-virus upon NAC Quarantine response
CTA posture dynamically modifies CSA Protection

CTA System Token used by CSA as a state modifier for policy

- Important protection for non-compliant NAC endpoints in the time before remediation
- Important protection for non-compliant endpoints when NAC is run in monitor mode
NAC Monitoring and Reporting with CS-MARS

- CS-MARS provides a centralized monitoring and reporting point for NAC-related events from ACS, NADs, and third party security servers.
- PN Log Agent forwards Syslog information for NAC from ACS to CS-MARS
- Pinpoints where NAC events are occurring in the network, provides detailed logging information regarding events, and detailed NAC-related reports.
NAC Monitoring and Reporting with CS-MARS

- Default NAC reports include:

- Custom reports can be created as well.
### NAC Incident investigation example

**Rule Name**: System Rule: Security Posture: Infected - Single Host  
**Description**: This rule detects a particular host's reporting INFECTED security posture status for an excessive period of time. This implies that the host is having trouble getting cleaned.

<table>
<thead>
<tr>
<th>Offset</th>
<th>Event Type</th>
<th>Device</th>
<th>Reported User</th>
<th>Severity</th>
<th>Count</th>
<th>Close</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host Posture Validated - Infected</td>
<td>ANONYMOUS</td>
<td>None</td>
<td>ANONYMOUS</td>
<td>ANY</td>
<td>5</td>
<td>Close Operation</td>
</tr>
</tbody>
</table>

**Incident ID**: 1712323913

**Event Type Details**: Host Posture Validated - Infected

**Device Event Type Information**

- Device: ANONYMOUS
- Event: Host Posture Validated - Infected
- Severity: ANONYMOUS
- Count: 5

**Event/Session/Incident ID**

- Event Type: Host Posture Validated - Infected
- Source IP: 192.168.116.68
- Destination IP: 192.168.116.69
- Protocol: TCP
- Time: 13:48:20
- Raw Message:

```plaintext
```

**L2 Enforcement Device Information**

- Device: 192.168.116.62
- Type: Cisco 12.2
- Manager: NA
- Children: NA
- Log To: NA
- Collects From: NA

**Interface Information**

- Direction: Inbound
- Interface Name: VLAN60
- NAC Address: 192.168.116.62
- NAC Update Time: 04/10/2006 11:50:11 PM

**Recommended L2 Policy/Command**

```
configure t
interface GigabitEthernet0/0
shutdown
```
Security Information Management (SIMS) Support

- Cisco’s SIMS tools provide NAC monitoring & reporting support
  - Cisco Secure Mitigation and Response System (MARS)
  - CiscoWorks Security Information Management Solution (CW SIMS)

  Collect and interprets IOS syslog and ACS events
  Real-time monitoring dashboard
    - Summary and detailed drill-down views
  NAC reporting
    - Compliance reports by network device, group, user
    - Enforcement actions
    - Rejected hosts and host remediation time
    - Application posture

- Third-party SIMS
  - Many third party vendors are supporting NAC
  - Information is public, integration encouraged
  - Formal validation program in progress
Conclusion
NAC Advantages

- Appliance *and* Framework solutions
- Comprehensive span of control
  - Routers, Switches, VPNs, wireless, plus complex deployments, including IP Telephony
- 100% host and device compliance
  - No need to install multiple servers
- Controls managed, unmanaged, and guest endpoint devices
  - Only solution to integrate device posture and user identity
- Device health decisions made at the network, not on the endpoint device
  - Limits ability to misrepresent device as “healthy” to the network
- Enjoys widest use of any technology
  - Including the most robust partner program
- NAC Appliance interoperable with NAC Framework
  - Future integration will provide smooth transition to architecture-based approach
Q and A