Network Admission Control and VMware ACE

Réza Malekzadeh
Manager, Product Marketing
Cisco Systems, Inc.
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 and unmanaged devices pose an unacceptable risk
  - Often source of infection
  - Rogue assets untracked, invisible
- Device compliance as important as user authentication

“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
Why Use The Network?

- Every bit of data you are concerned about touches the network
- Every device you are concerned about is attached to the network
- Gives you the ability to deploy the **broadest possible security solution** covering the **largest number of networked devices**
- Also leverages existing infrastructure, security, and management deployments, so it has the **smallest IT footprint** possible
NAC Controls Access of All Devices

1. **Clean Access Agent**
   - DISCOVERY
   - AUTHENTICATION
   - ENFORCEMENT
   - REMEDIATION
   - Best turnkey appliance product for all verticals
   - Address immediate pain-points with CCA

2. **NAC Framework**
   - DISCOVERY
   - AUTHENTICATION
   - ENFORCEMENT
   - REMEDIATION (VENDOR)
   - AAA (ACS)
   - Best technological approach for enterprise
   - Begin long-term enterprise solution with integrated product and services

3. **NAC convergence = future proof**
Leverage the network to intelligently enforce access privileges based on endpoint security posture.

**NAC Characteristics:**

- **Ubiquitous Solution For All Connection Methods**
- **Validates All Hosts**
- **Leverages Existing Network and Security and Mgmt SW**
- **Applications Gather and Assess Credentials, Remediation Services**
- **Network Provides Visibility, Forces Authentication, Isolation Services**
NAC Logical Components

- **Network Access Device**
  - EAPoUDP
  - EAPo802.1x

- **RADIUS**
  - Non-responsive audit server
  - AAA server

- **Vendor server**

- **GAME**

- **Many vendors**
  - Open License Program

- **NT, XP, 2000, 2003**

- **Cisco secure ACS**

- **Switches (2900, 3500, 3700, 4000, 6500)**
  -Wireless AP and WLSM

- **NR audit server API**
  - Initial vendors integrated

- **RedHat Linux**

- **Shipping**

- **NAC2**
  - Many vendors
  - Open License Program

- **Security App**
  - Vendor server

- **Plug-ins**

- **CTA**
Posture Assessment Methods

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

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 of endpoint, mainly for ‘agentless’ endpoints
- Exceptions: create static exception handling for known assets (MAC, IP, port)
Strong NAC Partner Program

**ANTI VIRUS**
- McAfee
- CA
- SOPHOS
- AhnLab
- NORTON
- F-SECURE
- 金山在线
- Panda

**REMEDIATION**
- altiris
- BigFix
- HP
- IBM
- iPass
- LANDesk
- PATCHLINK

**AUDIT**
- altiris
- McAfee
- QUALYS
- symantec

**CLIENT SECURITY**
- CAYMAS
- CREDANT
- CONSENTRY
- FIBERLINK
- I-PSWAT
- infoexpress
- TRIGEO
- Tenebril
- WEBSENSE
New PC Management Challenge

- Mixed business / personal applications and data
- Unsecured and intermittently-connected desktops and laptops used by remote and guest workers
- Mixed full-time / partner / contractor population
VMware Technology Overview

- **Traditional x86 PC Architecture**
  - OS and applications bound to hardware
  - Each PC runs single operating system

- **With VMware Technology**
  - Hardware-independent virtual machines
  - Standard environment can be provisioned anywhere
  - Strong fault and security isolation
  - Full environment encapsulated in files
Assured computing environments allow the same physical machine to participate safely in the enterprise environment.
Product Overview

- **VMware ACE Manager (Administrator’s PC)**
  - Used by security administrators to create assured computing environments that can be packaged and provisioned to any PC
- **VMware ACE (End-user’s PC)**
  - An application installed by end users to run a pre-configured, secured and sandboxed PC endpoint on their physical PC
Combining NAC and ACE
NAC Framework Solutions: ACE
Deployment Scenarios

Subject

LAN

WAN

Remote

Enforcement

Decision and Remediation

ACSv4.0

Directory

ACE manager

Other vendor servers

Remediation server

Subject

Decision and Remediation

Other vendor servers

Remediation server

LAN

WAN

Remote
ACE and NAC Setup

Native OS for NAC L2 802.1x
VMware images for NAC L2/L3 IP
CTA 2.0+
others...
vmedium

Clients
DHCP-assigned

Cisco ACS

VMware ACE manager

ACE environment 1
ACE environment 2
ACE environment 3
Etc.
Secured Endpoint

Telecommuters, offshore workers, or contractors use their host PC to run their personal applications with their own networking.

Simple interface optimized for end users.

Windows 2000 Host
Secured Endpoint

Telecommuters, offshore workers, or contractors use their host PC to run their personal applications with their own networking.

Simple interface optimized for end users.

Windows 2000 Host
Secured Endpoint

Telecommuters, offshore workers, or contractors use their host PC to run their personal applications with their own networking.

Windows 2000 Host

Pre-configured set of available devices

Simple interface optimized for end users

Standard Cisco VPN and corporate security software is installed inside ACE

Pre-configured and rules-based network access

Pre-configured applications and data

Authenticate against AD, password or script
Secured Endpoint

Telecommuters, offshore workers, or contractors use their host PC to run their personal applications with their own networking.

- Pre-configured set of available devices
- Simple interface optimized for end users
- Entire ACE can be encrypted and copy protected
- Entire ACE can be set to expire

- Standard Cisco VPN and corporate security software is installed inside ACE
- Pre-configured and rules-based network access
- Pre-configured applications and data
- Authenticate against AD, password or script
Tamper Resistant

Seamless encryption creates a tamper-resistant environment

- Protect data, configuration and VRM attributes
  - Protect configuration and policies against tampering by user
  - Protect against data theft
- Leverage existing authentication mechanisms
  - Password, active directory, script
‘Secure Sandbox’
A “secure sandbox” on unmanaged and unsecured PCs upon network connection to a NAC infrastructure

- Data security: Virtual machine isolation protects against host compromise
- Network security: Bi-directional firewall allows only Cisco VPN traffic in and out of virtual machine
- Network isolation: Lack of host VPN channel keeps corporate network isolated
- Operating system inside virtual machine can be locked down
Grant or Deny Device Access

Control device availability and access

- Grant or deny access to:
  - Printers
  - USB devices
  - CD/DVD players/writers
  - Serial and parallel devices
  - SCSI devices
Grant or Deny Device Access

Control device availability and access

- Grant or deny access to:
  - Printers
  - USB devices
  - CD/DVD players/writers
  - Serial and parallel devices
  - SCSI devices
ACE Lifecycle Management

Control VMware ACE life-cycle and therefore network access with expiration and copy protection.

- Expire VMware ACE at a future date or pre-configured number of days after installation
- Bind VMware ACE to each PC to prevent unauthorized copying or moving
- Control VMware ACE activity through pre-set policies
Summary of Benefits

- Ensuring NAC compliance without impacting PCs’ current configuration settings
- Ideal for users with non-corporate owned PCs requiring network access
- Provision users with only the right OS level and applications they need for compliance with network policies