

Network Access Control

Jesse Crim, MSIA CISSP

What is NAC?

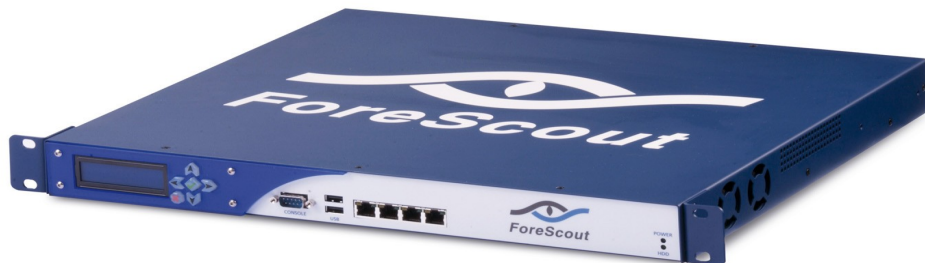
Network Access Control is a concept that deals with defining access controls based on user authentication, end-point security assessment, and network environmental information.

NAC is different because it is focused on the user and defines security policy (at least partially) based on the user's identity.

The term “user-focused” is what differentiates NAC from many other forms of access control, such as firewall.

“authenticating users, evaluating the security of end-point systems, and applying access controls focused on the user and their security status.”

Sophos NAC Advanced
Control unauthorized,
guest and non-compliant
computers →



Network Access Control

Three critical questions before deploying NAC:

- 1) What is my access control policy?
- 2) What access methods (LAN, Wireless, VPN) am I trying to protect?
- 3) How will this integrate with my existing infrastructure?

After you answer these questions, then begin your testing...

- Servers (policy definition points)
- Laptops / Desktops (End-points)
- Switches, Access points, VPN servers (policy enforcement points)

What NAC CAN DO:

A full-featured network access control solution should let you perform the following functions:

- Control who can get onto your LAN and limit what resources they can reach;
- Limit the reach of less-trusted or less-known users, such as contractors, technicians, remote users, or offshore workers;
- Segment users to meet compliance requirements;
- Restrict who can access sensitive financial or customer records;

What NAC CANNOT DO:

NAC won't help you with the following tasks:

- Protect information that leaves the premises via e-mail, laptop theft, printouts, or USB storage devices;
- Defend against social engineering;
- Block known malware from entering over the WAN connection;
- Prevent users with authorized access from using data inappropriately

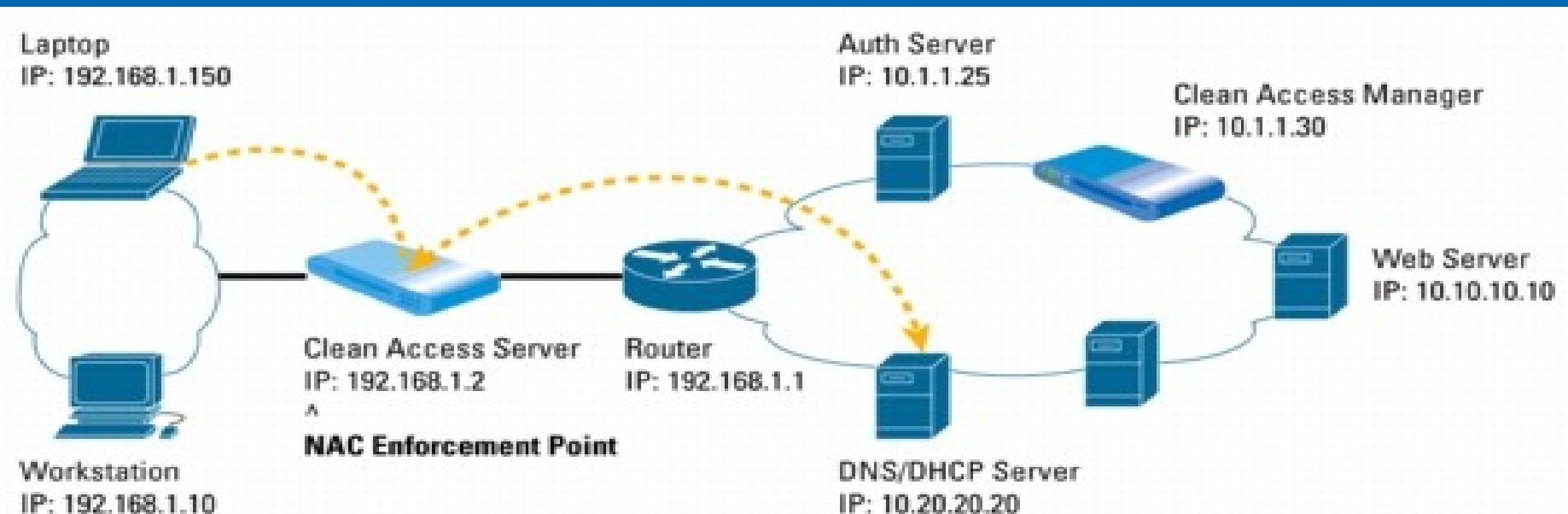
Reference:

<http://www.networkworld.com/columnists/2007/081307guardians.html?page=1>

NAC Fundamentals

How it is installed on the Network:

- Access Manager provides centralized management features
- Clean Access Server provides the distributed enforcement capabilities
- Authentication is through Active Directory, LDAP, RADIUS, 802.1X



In-Band

PROS:

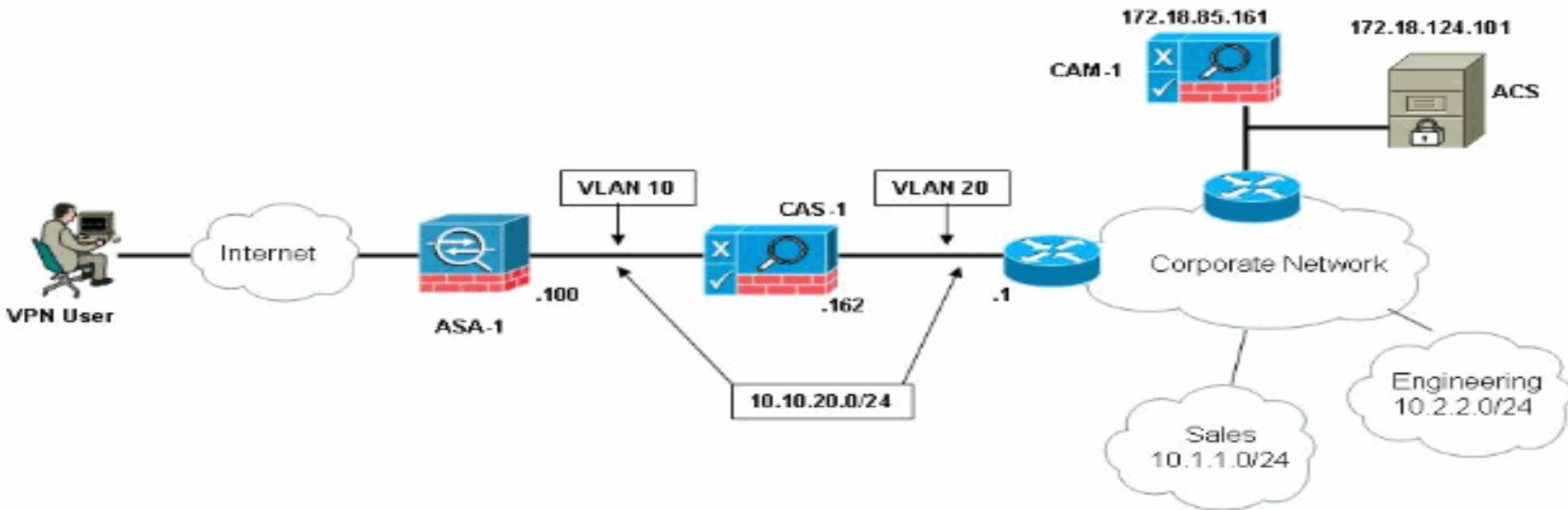
- Agnostic to switch/router platform
- Appropriate for wired and wireless
- Full network access control
- Bandwidth management control

CONS:

- In-line dependency
- No switch-port-level control

In-line means that the Clean Access Server is always inline with user traffic-before, during, and after authentication, posture assessment, and remediation.

The greater the feature set, the greater the control you'll have.



Out-of-Band

PROS:

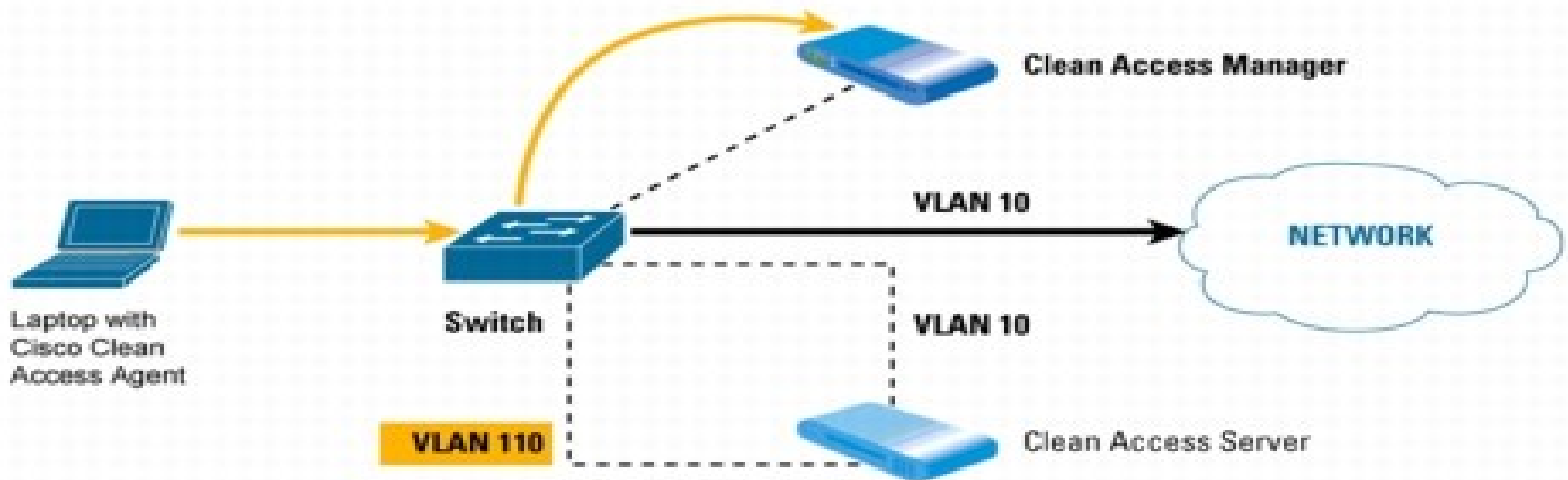
- Inline-only for quarantined traffic
- Full access control in quarantine
- Smooth switch control via SNMP
- Port- or role-based VLAN Assignment

CONS:

- Switch platform and version dependencies
- Most appropriate for wired scenerios

Out-of-band is what I like to call "edge enforcement", more like 802.1X.

Edge is preferred for big enterprise deployments. It scales, it handles the load and it doesn't depend on a single point to do enforcement.



NAC: Client Side

Cisco Clean Access Agent ✕



Clean Access Agent

Please enter your user name and password:

User Name :

Password :

Remember Me


Please select your authentication provider:

NAC: Client Side




NAC: Client Side

Cisco Clean Access Agent



Clean Access Agent

 Please download and install the required windows updates before accessing the network.

Required Software (0:59:47 left)

Name : Windows Update

Update: Change to download and installation

Description : Students are required to update their Operating System with the latest Patches to enhance performance and fix vulnerabilities. Click Update and the Auto Update agent will download / install the updates in the background. Process can take 2-30 Minutes! You can also visit

Cisco Clean Access Agent

Windows auto update launch is successful.

Network Access Control Benefits

- Higher availability of PC
 - Improve performance of students PC's
 - Increased network speeds
 - Reduction of one end user's PC infecting other PCs on the same network
 - Awareness and education on security through remediation of problems
-
- Technical Staff knows the status of students PC's
 - Quicker response to student problems
 - Quicker response to DMCA violations
 - Identify and isolate PC's attacking the network from the residence halls.

NAC PANEL:

Eric Weakland

Michael Nicolaides

Michael Miller

Jesse Crim