

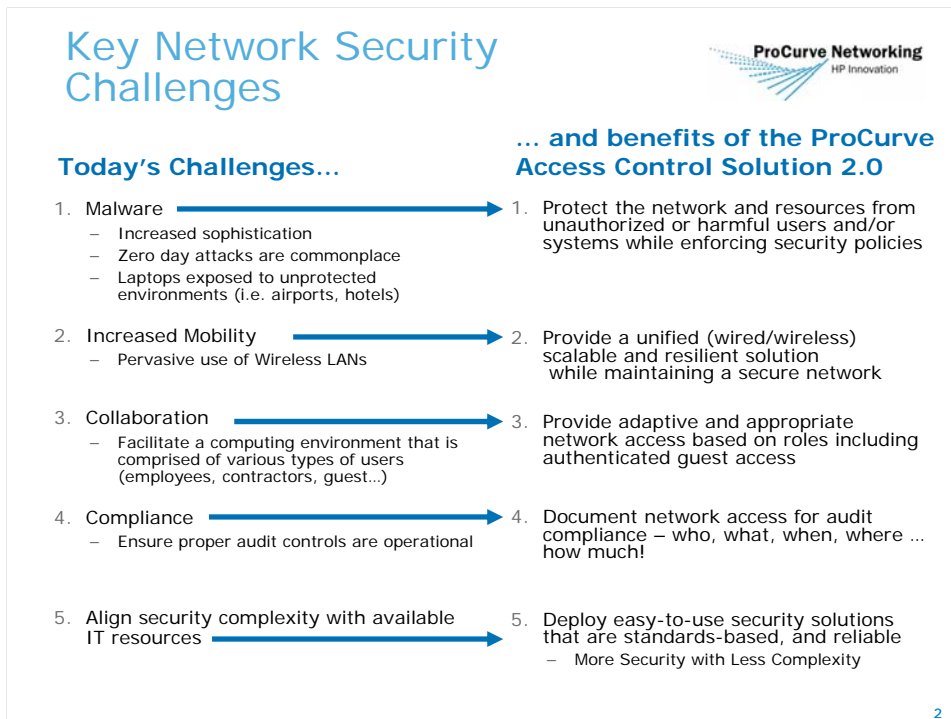


ProCurve Network Access Control Solutions

Technical Consultant: Oleg Ivanov
Sales Specialist: Harley Waterson
Inside Sales: Paul Pierre
October, 2007

© 2007 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice.





Here we examine five of today's challenging areas that is directly being addressed by ProCurve Access Control Solution 2.0. These are the key motivators to ProCurve Access Control Solution 2.0. As we progress you will see how ProCurve Access Control Solution 2.0 is flexible, rich in control and provides easy centralized management.

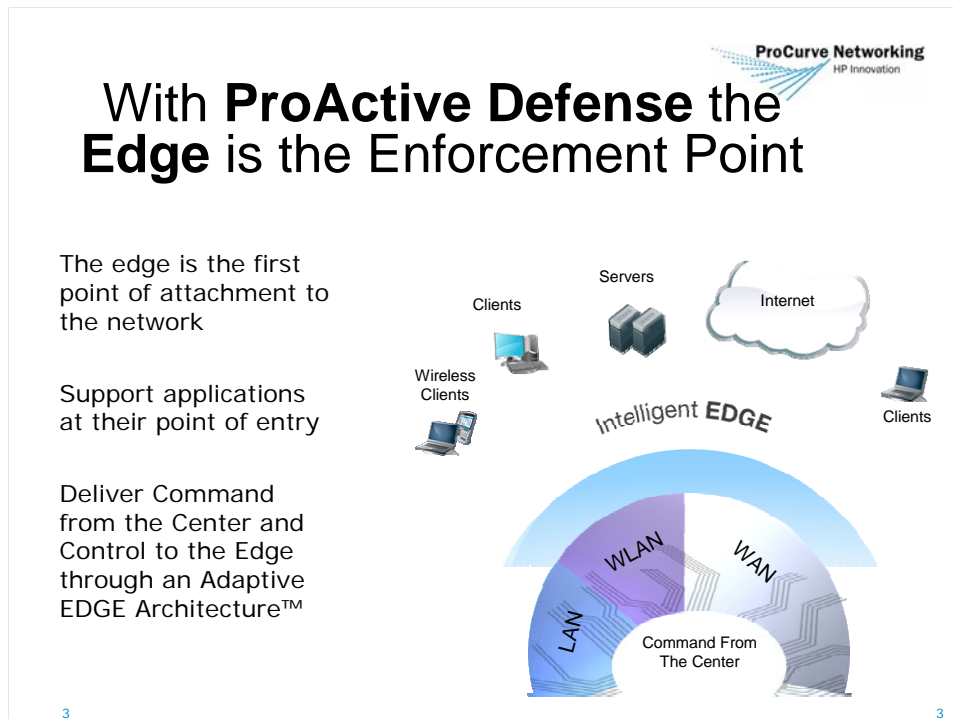
Beginning with Malware; we all hear about the various incidents that plague the Internet from time to time, freezing business operations at the expense of millions of dollars. With increased sophistication, viruses, worms, network fraud, and a host of other annoyances continue to present a stiff challenge for the IT organization. ProCurve Network Access Control Solution 2.0 provides the benefit of protecting network resources from unauthorized or harmful users and enforces security policies ensuring users have access to what they need while protecting resources that need not be accessed.

Increased Mobility; the pervasive use of wireless networks presents a unique challenge for organizations looking to provide appropriate access for mobile users. In addition to time of day and the role user plays within an organization, today's network must take into consideration from where the user may be accessing the network. ProCurve Access Control Solution 2.0 provides the benefit of ensuring a unified method of implementing access control regardless of whether the user is wired or wireless.

Collaboration reiterates how today's organizations operate, where the dynamic nature of business operations must exist across multiple user types without compromising the protection of network users and resources. ProCurve Access Control Solution 2.0 provides adaptive and appropriate network access based on location, time, and user role. The flexibility available in this solution ensures appropriate access with policy enforcement whether guest, contractor, organizational member or employee alike.

Challenge four reflects previous networking events that raise the awareness and have brought new measures of compliance into organizations. The enforcement of network policies is now necessary to protect the organization from mistreatment. Policies of compliance extend to meet the needs of regulatory agencies enabling businesses and organizations alike to operate with integrity. Today's ProCurve Access Control Solution 2.0 contributes to this compliance by providing reports that deliver information with regard to network access and integrity.

Challenge five prompts the conscious need to answer the organization's request for network access control with a solution that takes into consideration the organizations available workforce. ProCurve products are reliable, standards-based products and ProCurve Access Control Solution 2.0 is no exception. The solution is designed from ground up with familiar industry standards, yet it's unique implementation as outlined by the ProActive Defense Architecture ensures efficient use of resources by utilizing automation and command from the center.



This slide demonstrates how we integrate proactive controls, which are access controls, with defense controls, which are threat management controls. The enforcement of these controls is done at the edge of the network. The slide also demonstrates the importance of network management applications as the console for the automated process of protecting, detecting, and responding security issues.

In all cases, we use a Policy Controlled Intelligent Edge as the enforcement point for security policy. We want to do this as close to the end-user or source of attack as possible.

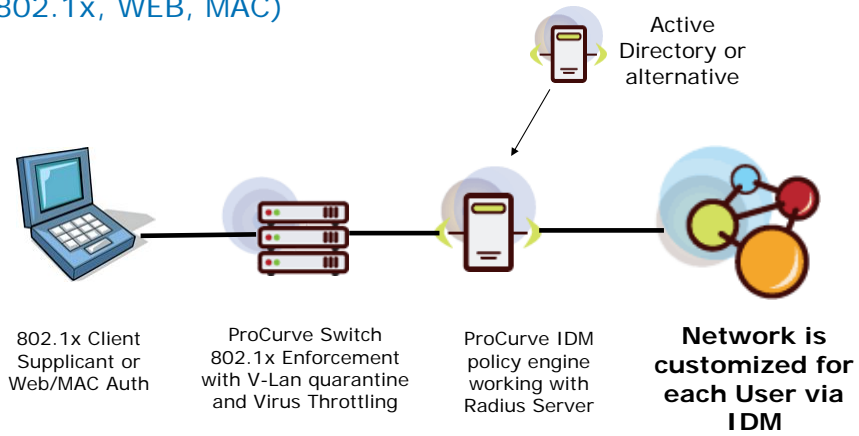
When we talk about the word “ProActive” with regard to the ProActive Defense Architecture we are talking about the dynamic configuration of the edge based upon access control. This is a fundamental tenant of the Adaptive Edge Architecture. Today, Access Control must be ‘comprehensive’ because we cannot guarantee a homogenous environment of endpoints connected to the network. Some will be managed, some will not. There will be guests, contractors, etc... The edge must supplement the access controls for un-trusted and uncontrolled endpoints accessing the network.

The word “Defense” in ProActive Defense is the implementation of embedded threat management in all edge devices; LAN, WAN, WLAN. The vision is to have capabilities like Virus Throttle at every edge point. Today it is in the switches only. The LAN, WAN, WLAN devices form a trusted infrastructure by being trustworthy themselves. They are solid, reliable and secure. Capable of forming the trusted infrastructure through authentication (e.g. device-to-device 802.1X) and eventually encryption.

Having both “ProActive” and “Defense” technologies integrated has the benefits of combining multiple approaches to address the blended threat – which is more the risk today – not a point attack anymore

- Having access to more data within the integrated system provides a greater opportunity to convert that intelligence into actionable items.

Access Control Example: (802.1x, WEB, MAC)



Identity Driven Manager 2.2

ProCurve Networking
HP Innovation

Dynamically apply security, access and performance settings based on user, location, and time and now client integrity status

Allows easy creation and management of user policy groups for optimizing network performance and increasing user productivity and overall efficiency (appropriate access)

Management policies set network parameters (think of them as “knobs”) to provide desired network functionality

Set these =>



VLAN



Bandwidth
Limit



QoS



ACLs



Based on these =>

User
ID

Device
ID

Time

Location

Client
Integrity
Status



Student Guide: 12-

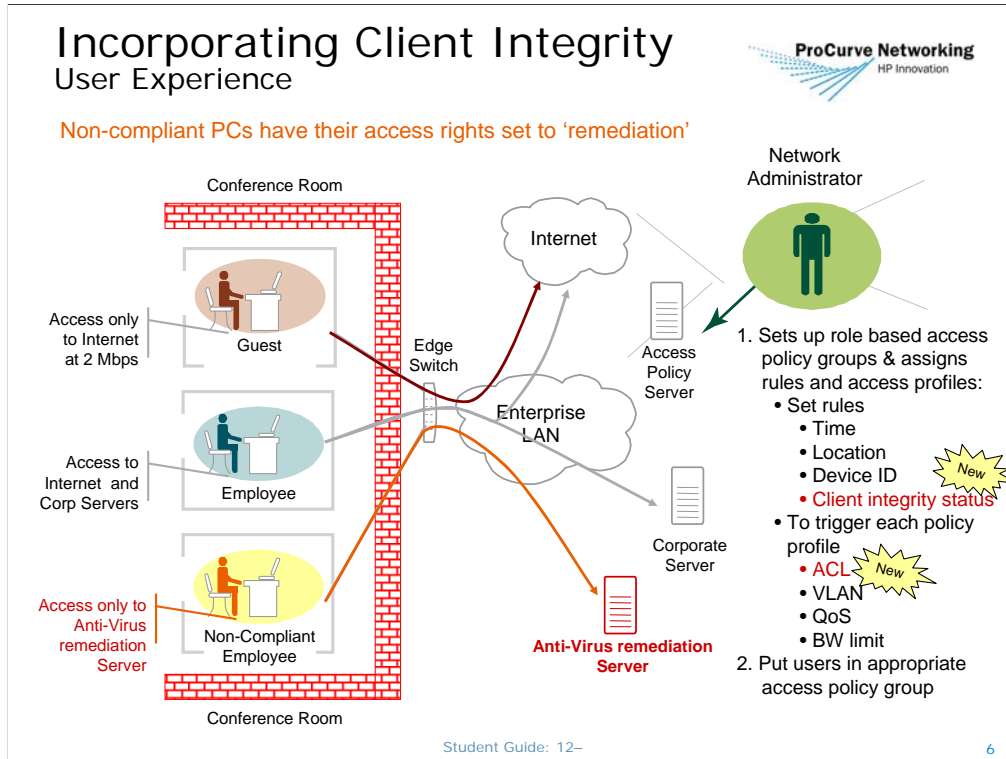
5

Go to slide view to see animation and previous vs. new features of IDM.

Two key new features in IDM 2.0 are user-based ACLs and Client Integrity Status.

- **ACLs:** ACLs in IDM 2.0 are dynamically written on the switch that a user connects to based on any or all of five criteria – user ID, device ID, time, location, and now client integrity status. Access Controls Lists are filters on users enforced at the port or AP that allows or denies access to protocols, destination IP addresses, or destination TCP/UDP ports. The addresses (TCP/UDP or IP) may also be specified in ranges as well as individual addresses.
- **Client Integrity Status:** New in this release IDM can now integrate with 3rd party client integrity checking software (such as Sygate, Zonelabs, etc.) to make certain that users don't have sub-standard security settings. IDM receives an indicator from client system's security agents (3rd parties) of the state of health of that client. These 3rd party clients will do the integrity checking and will report it to IDM in the standard RADIUS data stream. When IDM sees the client status indicator, it can send a 'dirty' client to a remediation VLAN or server.

Each user can be placed in an access policy group (APG) by the administrator. When a user is authenticated, IDM looks at the rules for the user's access policy group. The rules are based on device ID, time, location and client integrity status. When a rule match is found then an associated 'Access Profile' is invoked that sets a policy on the user's port that can include VLANs, bandwidth limitations, QoS and now ACLs.



Go to slide view to see the animation

This slide shows how client integrity checking works in then context of normal IDM operation as described below:

1. The network administrator decides the groups into which users are classified, most likely based on the user's role in the company
2. Each access policy group (APG) has a set of rules that establish time, location, device ID, and client integrity status states that a user can satisfy at login. When the rule is matched by login criteria then the access profile is executed.
3. When a rule match is found then an associated 'Access Profile' is invoked that sets a policy on the user's port that can include ACL's, VLANs, QoS and Bandwidth limitations.

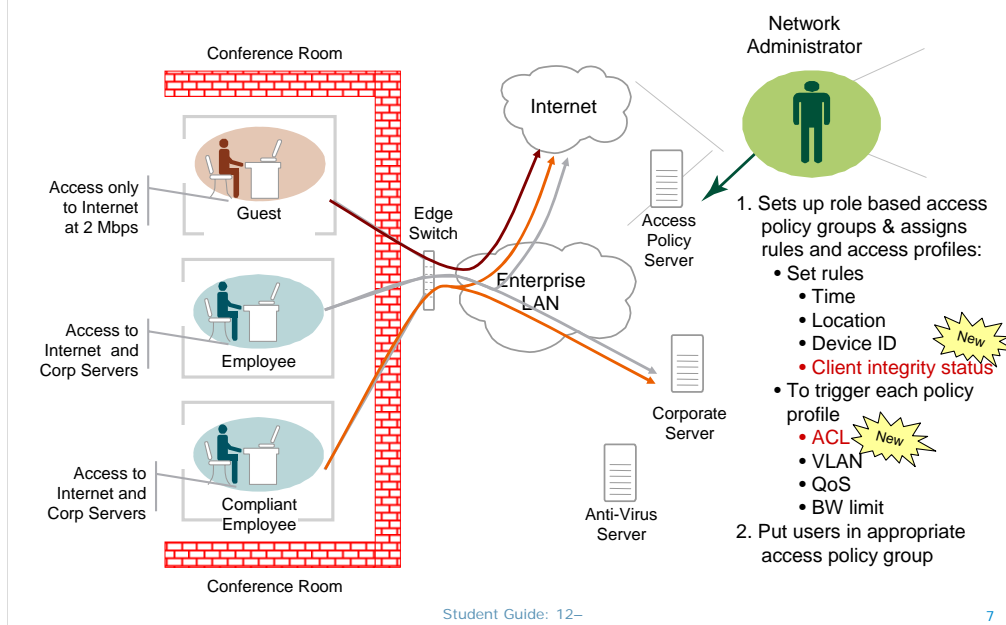
ACL's and client integrity are new.

Guests and employees get access to their appropriate resources provided their client status is OK.

In the example, you can see that the non-compliant employee is sent to a remediation server (either with an ACL or VLAN policy) to get their client back to an acceptable status. When clean then they get access again to the normal employee resources.

Identity Driven Manager The On-Demand Network User Experience

ProCurve Networking
HP Innovation



Go to slide view to see the animation

This slide shows how client integrity checking works in then context of normal IDM operation as described below:

1. The network administrator decides the groups into which users are classified, most likely based on the user's role in the company
2. Each access policy group (APG) has a set of rules that establish time, location, device ID, and client integrity status states that a user can satisfy at login. When the rule is matched by login criteria then the access profile is executed.
3. When a rule match is found then an associated 'Access Profile' is invoked that sets a policy on the user's port that can include ACL's, VLANs, QoS and Bandwidth limitations.

ACL's and client integrity are new.

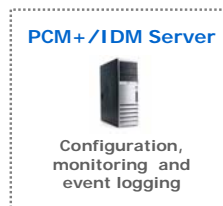
Guests and employees get access to their appropriate resources provided their client status is OK.

In the example, you can see that the non-compliant employee is sent to a remediation server (either with an ACL or VLAN policy) to get their client back to an acceptable status. When clean then they get access again to the normal employee resources.

IDM components



- IDM Server
 - Integrated with PCM+ Management Server
 - User interface is accessed using Identity tab on Network Management Home page
 - Used to perform configuration tasks and deployment of configuration to the IDM Agent
 - Is not an active participant during user authentication
- IDM Agent
 - Resides on each RADIUS server
 - Works directly with RADIUS server during authentication process
 - Setting ACLs, VLAN assignment, and QoS and bandwidth (rate limit) settings
 - Runs independent of the IDM Management Server
 - Configurations are deployed to the IDM Agent by the PCM+ administrator



Student Guide: 12-7

8

Let's now look a little closer at the IDM Product...

IDM is a *windows-based* program that is comprised of two separate components: An **IDM Server** and an **IDM Agent**.

The **IDM 2.0 Server** is integrated with **HP ProCurve Manager Plus** version 2.1. All **Configuration** tasks for both PCM Plus and IDM are handled on the management server within the **Integrated Graphical User Interface**.

This integration provides Network Administrators a **Single Pane of Glass** for overall network management - which now includes both network **Device Management** and network **User Management**.

IDM configuration includes setting when and where users can log into the network as well as what VLAN placement, QoS and Bandwidth settings will be done at the time of authentication.

Keep in mind – when talking about Network Security – final user authentication takes place at the RADIUS server. For this reason, IDM configuration information needs to be readily available to all RADIUS servers in the environment – **twenty-four by seven!**

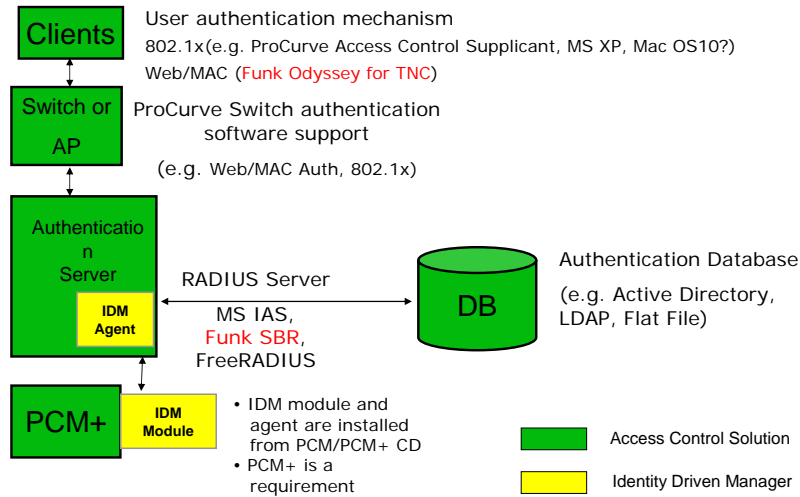
This brings us to the second component in IDM – known as the **IDM Agent**. The **IDM Agent** is installed on each RADIUS Server in the network. Every time configuration changes are made on the IDM server – the changes must be pushed-down, or deployed, to each IDM agent in the environment.

It is very important to note that the IDM Server and the IDM Agent run completely independent of one another.

The IDM management server provides the **mechanism** for performing IDM Configuration using a Graphical User Interface – or Client - and it is not until the configuration is **deployed** to the IDM Agent that the configuration changes will take effect.

This is an important concept when talking about high availability. If the IDM Server happens to be down – the IDM Agent that resides on the RADIUS server will always be up and running - delivering the appropriate **Access Rights** to the users logging into the network.

What components do I need?



9

Minimum Processor: 2.0 GHz Intel Pentium III or equivalent

Recommended Processor: 3.0 GHz Intel Pentium III or equivalent

Minimum Memory: 512 MB

Recommended Memory: 1 GB

Disk Space: 5-10 GB free hard disk space

Operating System(s):


MS Windows 2000

MS Windows XP Professional


MS Windows XP

MS Windows 2003

ProCurve Access Control Solution




ProCurve Manager Plus (PCM+) 2.2 with Identity Driven Manager (IDM) 2.2



- User Authentication
 - 802.1x, MAC, WEB
- VLAN Assignment
 - Dynamically place users into VLANS
- Rate Limiting
 - Rate limiting for selected users
- QoS
 - Dynamically enforce QoS based on User ID
- Locations
 - Define locations based on groups of ports/switches

ProCurve Network Access Controller 800



- Enforces network security compliance
- Endpoint integrity (EI) validation
- Network Access Control
- Network access reporting
- Built in RADIUS Server
- Supporting thousands of users

10

The ProCurve Access Control Solution 2.0 provides comprehensive access control with significant usage flexibility. ProCurve is enhancing the Access Control Solution with the introduction of ProCurve Manager Plus (PCM+) 2.2, Identity Driven Management (IDM) version 2.2 and the new ProCurve Network Access Controller 800 appliance. Also known as the ProCurve NAC 800. (Available in Q3 2007)

ProCurve Manager Plus and IDM versions 2.2 are enhanced software versions that provide central management of the new Network Access Controller 800 and add Endpoint Integrity to Access Policy Groups (APGs). IDM has also been enhanced to include simplified setup of the network access environment, and a new automated Active Directory synchronization feature.

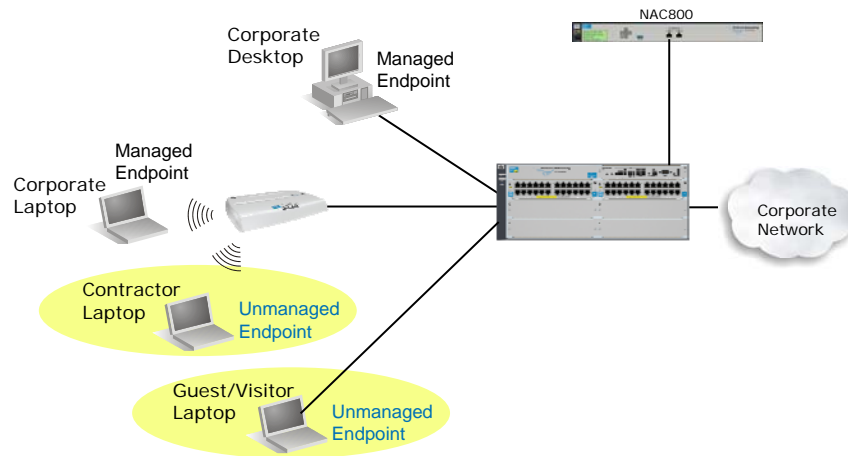
The ProCurve NAC 800 is designed to perform initial and ongoing Endpoint Integrity (EI) assessment of endpoints. Assessment is accomplished by running selected “tests” on endpoints to ensure they meet the defined goals of the corporate compliance policy. Supported endpoints, testing methods, and the types of tests that can be performed on endpoints will all be covered later in this presentation. We will also look at some of the reports which can be generated by the ProCurve NAC 800 to demonstrate confirmation of an organization’s compliance policy.

The ProCurve NAC 800 Agent License packages are procured to cover the customers endpoint population that will be measured against compliance policies. Licenses and their management will be covered later.

Managed and Unmanaged Endpoints



- Enforces security compliance on managed and unmanaged user stations



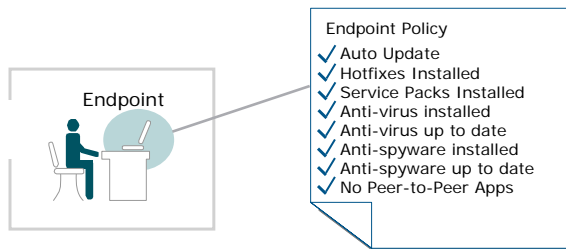
11

This slide expands the previous slide to include unmanaged endpoints. The unmanaged endpoint is not under direct control of the organization's network and presents the challenge of providing access to uncontrolled users while maintaining corporate compliance.

Endpoint Policy



- Defines a set of endpoint tests ensuring endpoint integrity
 - Assess operating systems to verify updates are enabled and that hotfixes and service packs are installed
 - Assess software to ensure Anti-virus, spyware, and other security applications are present and up-to-date
 - Check for potentially dangerous applications such as file sharing, peer-to-peer (P2P), or spyware
 - Detect the presence of worms, Trojans, and viruses



12

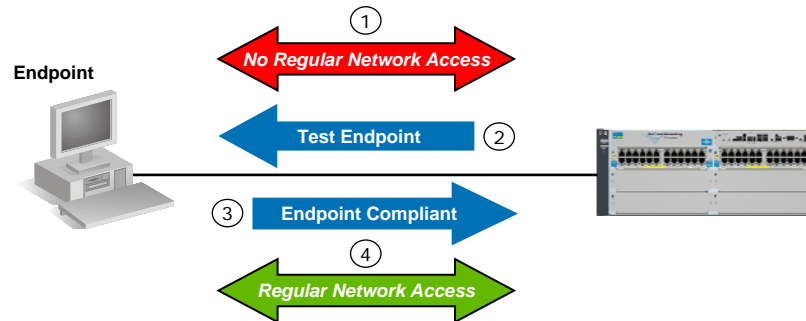
An Endpoint Policy is a collection of tests used to evaluate the integrity of an endpoint device attempting to access the network.

Tests can evaluate operating systems to ensure service packs and hotfixes exist according to policy. They can also assess the endpoints software to ensure Anti-virus, spyware and other security applications exist as required. Tests can also check for potentially dangerous applications such as peer-to-peer or spyware applications as well as checking for the presence of worms, Trojans, and viruses.

Pre-Connect NAC



- Testing an endpoint device to ensure compliance prior to the endpoint being granted regular access on the network



13

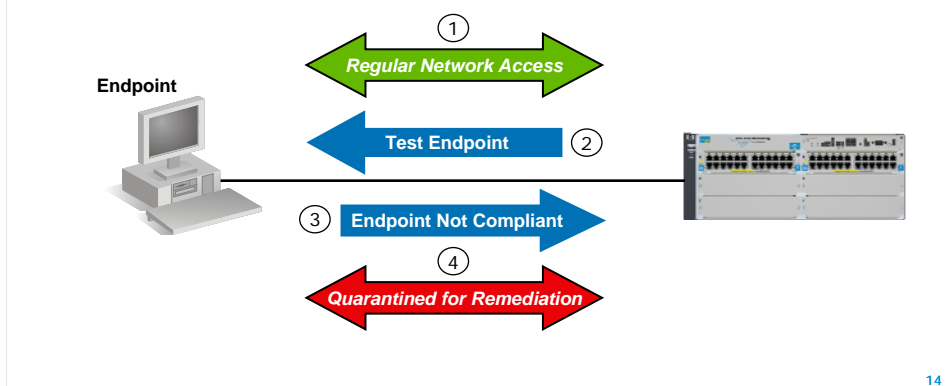
Pre-connect NAC refers to network access control where the testing of the device to ensure compliance with network access policies is done prior to the device being granted regular access on the network.

A similar term used in the industry is “preadmission”.

Post-Connect NAC



- Network access control where the endpoint device is periodically tested after network access has been granted
 - Upon determination of endpoint non-compliance the endpoint device is quarantined for remediation




Although NAC is about controlling access to the organizations network, control should not stop after pre-connect checks. Even a healthy endpoint with a known and trusted user has the potential to cause consequences once on the network. This drives the need for a more complete NAC solution that provides Post-Connect NAC validation and monitoring. Post-connect NAC is network access control where validation and monitoring of the endpoint continues after access to the organizations network has been granted.

A similar term used in the industry is “post-admission”.

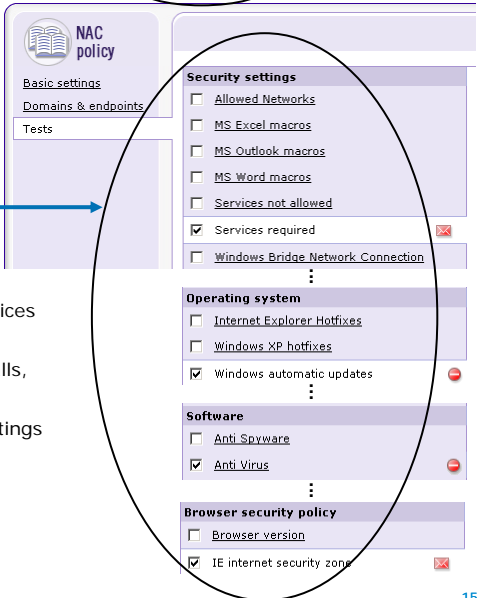
Note, in order to support business functions, a network cannot simply deny access; remediation mechanisms should also be included in NAC to facilitate the repair and rehabilitation of endpoints.

Endpoint Integrity Policies and Tests



- Policy Name home > nac policies > nac policy (lab01)

- Four test categories and associated tests:
- [Security Settings](#) - Allowed and prohibited programs and services
- [Operating System](#) - OS versions, services packs, hotfixes
- [Software](#) - Antivirus, Spyware, Firewalls, peer-to-peer
- [Browser Security Policy](#) - Security settings for browsers and applications



The ProCurve NAC 800 provides a comprehensive set of endpoint tests including tests for Antivirus software, spyware, firewalls, peer-to-peer, allowed and prohibited programs and services, OS versions, services packs, hotfixes, and security settings for browsers and applications.

New tests are continually being developed to address changes in software and new virus definitions. With a ProCurve NAC Endpoint Integrity Agent 1-yr Maintenance license in place, these new tests are automatically updated.

Endpoint Integrity Tests



- **Operating systems**
- Service Packs
- Rogue WAP Connection
- Windows 2000 hotfixes
- Windows Server 2003 SP1 hotfixes
- Windows Server 2003 hotfixes
- Windows XP SP2 hotfixes
- Windows XP hotfixes
- Windows automatic updates
- **Browser security policy**
- IE internet security zone
- IE local intranet security zone
- IE restricted site security zone
- IE trusted site security zone
- IE version
- **Security settings**
- MS Excel macros
- MS Outlook macros
- MS Word macros
- Services not allowed
- Services required
- Windows Bridge Network Connection
- Windows security policy
- Windows startup registry entries allowed
- **Personal firewalls**
- AOL Security Edition
- Black ICE Firewall
- Computer Associates EZ Firewall
- Internet Connection Firewall (Pre XP SP2)
- McAfee Personal Firewall
- Panda Internet Security
- F-Secure Personal Firewall
- Norton Personal Firewall / Internet Security
- Sygate Personal Firewall
- Symantec Client Firewall
- Tiny Personal Firewall
- Trend Micro Personal Firewall
- ZoneAlarm Personal Firewall
- Senforce Advanced Firewall
- Windows Firewall
- **MS Office version check**
- Microsoft Office XP
- Microsoft Office 2003
- Microsoft Office 2000
- **prohibited Software**
- Administrator defined
- **Required software**
- Administrator defined
- **P2P and instant messaging**
- Altnet
- AOL instant messenger
- BitTorrent
- Chainsaw
- Chatbot
- DICE
- dIRC
- Gator
- Hotline Connect Client
- IceChat IRC client
- ICQ Pro
- IRCXpro
- Kazaa
- Kazaa Lite K++
- leafChat
- Metasquarer
- mIRC
- Morpheus
- MyNapster
- MyWay
- NetIRC
- NexIRC
- Not Only Two
- P2PNet.net
- PerfectNav
- savIRC
- Trillian
- Turbo IRC
- Visual IRC
- XFire
- Yahoo! Messenger

Endpoint Integrity Checks



- | | | |
|--|---|---|
| <ul style="list-style-type: none"> • Anti-virus • NOD32 AntiVirus • AVG AntiVirus Free Ed • Computer Associates eTrust AntiVirus • Computer Associates eTrust EZ AntiVirus • F-Secure AntiVirus • Kaspersky AntiVirus for FileServers • Kaspersky AntiVirus for Workstations • McAfee VirusScan • McAfee Managed VirusScan • McAfee Enterprise VirusScan • McAfee Internet Security Suite 8.0 • Norton Internet Security • Trend Micro AntiVirus • Trend Micro OfficeScan Corporate Edition • Sophos AntiVirus • Panda Internet Security • Symantec Corporate AntiVirus | <ul style="list-style-type: none"> • Anti-spyware • Ad-Aware SE Personal • Ad-Aware Plus • Ad-Aware Professional • CounterSpy • McAfee AntiSpyware • Pest Patrol • Spyware Eliminator • Webroot Spy Sweeper • Windows Defender | <ul style="list-style-type: none"> • Spyware, Worms, viruses, and Trojans • W32.HLLW.Lovgate • W32.Hiton • W32.IRCBot.C • W32.Kifer • W32.Klez.H • W32.Klez.gen • W32.Korgo.G • W32.Mimail.Q • W32.Mimail.S • W32.Mimail.T • W32.Mydoom.A • W32.Mydoom.AX-1 • W32.Mydoom.AX • W32.Mydoom.B • W32.Mydoom.M • W32.Mydoom.O • W32.Mydoom.Worm • W32.Netsky.B • W32.Netsky.C • W32.Netsky.D • W32.Netsky.K • W32.Netsky.P • W32.Rusty@m • W32.Sasser.B • W32.Sasser.E • W32.Sasser.Worm • W32.Sircam.Worm • W32.Sober.O • W32.Sober.Z • W32.Welchia.Worm • W32.Zotob.E |
|--|---|---|

NAC800 Deployment Methods

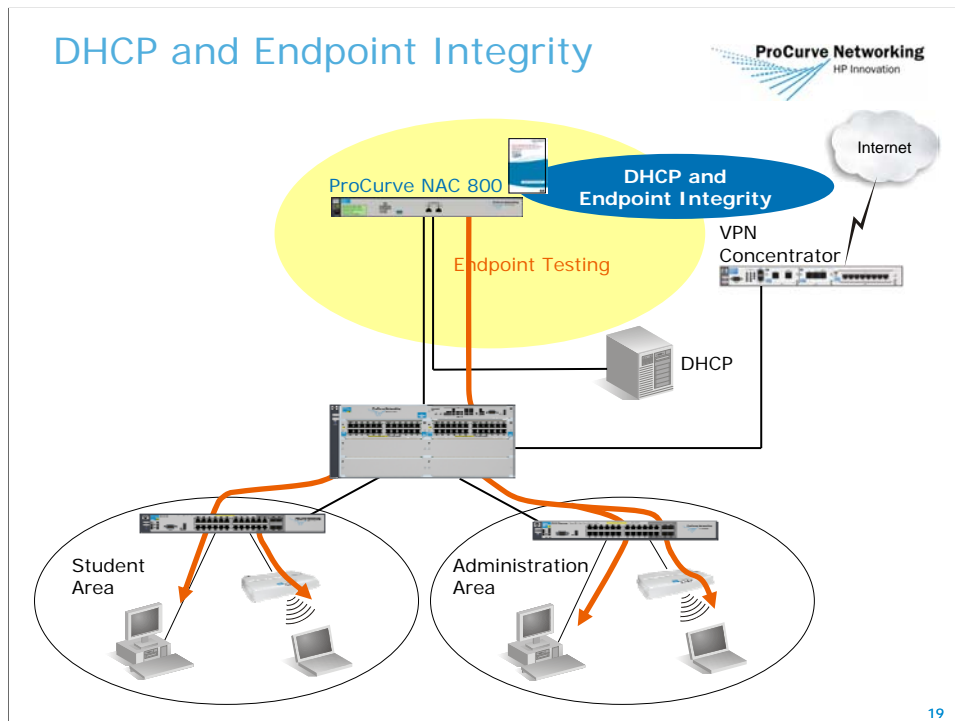


- DHCP Deployment
 - Physically connected between DHCP and the Network controlling IP DHCP request/response communication
- RADIUS/IDM Deployment
 - Deployed in combination with RADIUS and IDM. Constantly monitors authentication request/response communication between client and server.
- In-Line Deployment
 - Physically connected between VPN/RAS concentrator and the rest of the network. Used to enforce security policies on remote user.

18

As always, ProCurve provides an Industry leading warranty for the ProCurve NAC 800 including One-year next-business-day advance replacement which is available in most countries.

DHCP and Endpoint Integrity



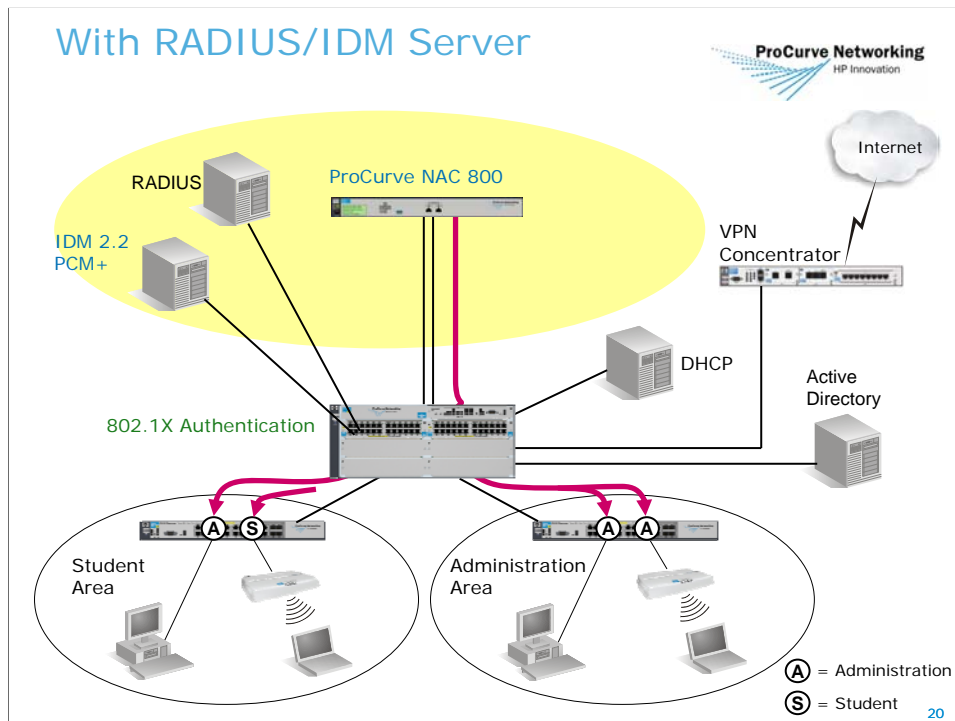
For environments without 802.1X, the NAC 800 offers implementations based on DHCP. In these solutions, the NAC 800 operates as DHCP server or monitors DHCP traffic to ensure non-compliant or untested endpoints are properly assigned to quarantine VLANs.

In the example, the NAC 800 is installed between edge devices and the DHCP server. When an endpoint connects, the NAC 800 acts as DHCP server, providing the client with an IP address that places it on a quarantine subnet for testing. If the endpoint passes testing, the NAC 800 releases its IP address and then allows it to receive an IP address from the production DHCP server.

To ensure the quarantine subnet is isolated from the production network, the administrator can use the NAC 800 to configure static routes on the endpoint or can configure Access Control Lists (ACLs) on routers that restrict the subnet's traffic.

In the static route solution, the NAC 800 provides endpoints with DHCP settings that include no default gateway and a netmask of 255.255.255.255. The routes are configured in the NAC 800's accessible "services and endpoints" list interface. The routes allow the endpoint access only to specific networks, IP addresses, and Web sites. The quarantine subnets can be subsets of existing DHCP scopes or separate networks multi-netted on routers.

In the router ACL solution, the NAC 800 provides DHCP settings that place endpoints in a quarantined network. A network router must act gateway for the quarantine subnet and must be configured with appropriate ACLs.



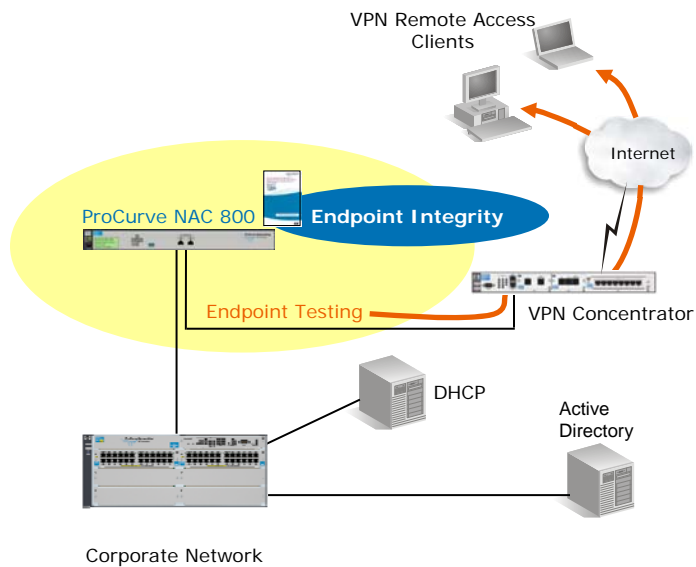
If the network does not require Endpoint Integrity testing, the NAC 800 can act as a standalone RADIUS server with IDM RADIUS Agent. In this solution, the customer can use PCM+/IDM to control access without installing RADIUS on a production server. This helps to avoid overloading servers or complicating their configurations, while still providing the functionality to provide Endpoint Integrity testing when desired.

PCM+/IDM provides the interface for configuration of all elements of the Access Control Solution. Administrators can use the new Security Access Wizard to configure the 802.1X switch infrastructure and the NAC 800 RADIUS server, which will serve as authentication server for the edge devices.

The NAC 800 also will act as authentication server for clients. In this role, the NAC 800 can access authentication information from Active Directory, OpenLDAP, or eDirectory servers.

All clients will be subject to Access Policies defined in IDM.

Inline and Endpoint Integrity



21

In Inline mode, the NAC 800 is placed between the endpoints and the production network and does not use DHCP to place them in quarantine VLANs. Instead, the NAC 800 blocks all network access for endpoints that fail testing, including access to remediation servers. In this way, the NAC 800 acts as an Endpoint Integrity firewall.

This solution is well suited to VPNs, as shown. However, this solution assumes the VPN Concentrator provides DHCP services. If VPN clients must communicate with DHCP servers on the production network, the administrator can configure the NAC 800 for DHCP mode.

Generic Testing Methods



- Methods by which an endpoint can be accessed for the purposes of testing
 - **Agent-based Permanent** – Agent software is installed on each endpoint and is always available for testing
 - **Agent-based Transient** – An agent is downloaded temporarily to the endpoint as required
 - **Agentless** – Uses native applications to provide agent functions

22

In the industry there are three access methods for testing you should be familiar with.

Agent-based Permanent - requires software to be installed on each endpoint and once installed and running it is always available for the endpoint to be tested.

Agent-based Transient – requires an agent to be temporarily downloaded to the endpoint while it is being tested.

Agentless is just that. It uses native applications to provide agent functions that are then used for testing.

ProCurve NAC 800 Testing Methods



Testing Methods Comparison:

Generic Testing Methods	ProCurve Named Method	Trade-offs	
		Plus (+)	Minus (-)
Agent-based Permanent	NAC Agent	<ul style="list-style-type: none"> Always available for retesting Automatic Agent updates 	<ul style="list-style-type: none"> Install and upgrade to maintain Requires one-time interaction from end-users
Agentless	File and Print Sharing Ports	<ul style="list-style-type: none"> No install or download Easiest of the three test methods to deploy 	<ul style="list-style-type: none"> Requires RPC Service to be available to ProCurve NAC 800 server Requires file and print sharing to be enabled If the device is not on a domain, the user must specify local credentials
Agent-based Transient	ActiveX	<ul style="list-style-type: none"> No installation or upgrade to maintain Only Internet Explorer application access required through personal firewall. No open ports necessary 	<ul style="list-style-type: none"> No retesting of device once browser is closed Not supported by non-Windows operating systems Browser security settings must allow ActiveX control operation of signed and safe controls

23



Shown are the differences between each of the three testing methods along with trade-offs, shown as plusses and minuses, associated with each method.

The Agent-based method requires a one time interaction by users to install the agent before accessing the network. Once installed, the agent is always available for retesting and it is automatically updated with product updates.

The Agentless method does not require the installation or download of software, however Remote Procedure Call Service must be available to the ProCurve NAC 800 server (ports 139 or 445) and both file and print sharing must be enabled. Also, if the device is not on a domain the user must specify local administrator credentials.

The ActiveX method does not require any installation or upgrade to maintain. However, browser security settings must allow ActiveX control operation.

ProCurve Access Control Solution 2.0 Implementation Options

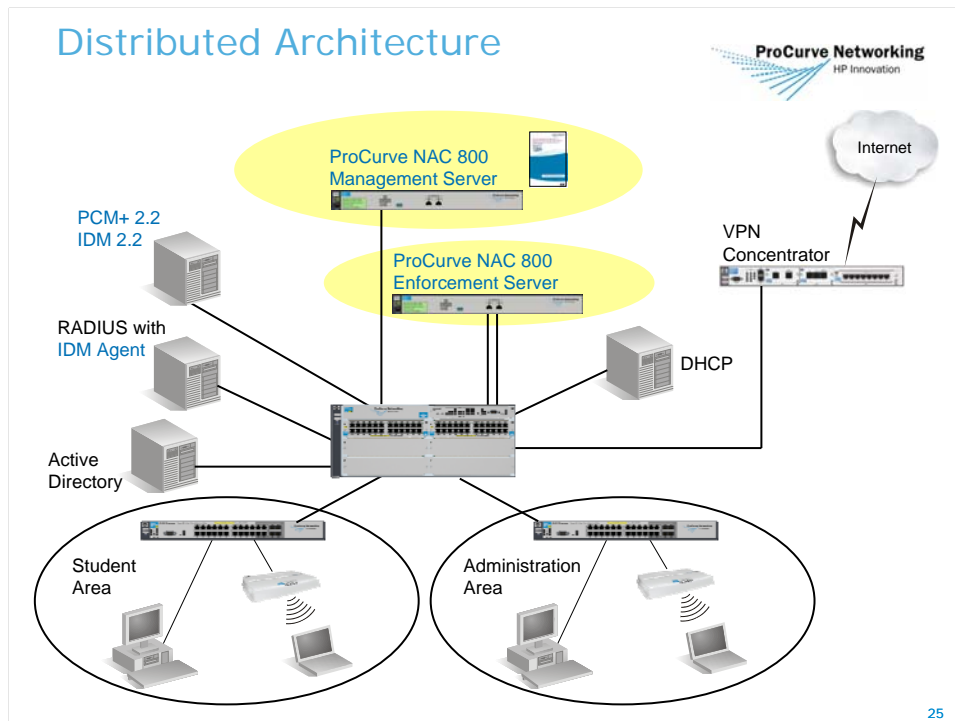


PCM+2.2 IDM 2.2 + ProCurve Network Access Controller 800 + ProCurve NAC Endpoint Integrity License

- Server Installation Options:
 - Combination Server
 - Multiple Server
- Testing Method Options
 - NAC Agent
 - Active X
 - Agentless

24

The ProCurve NAC 800 provides Combination Server and Multiple Server installation options. We will now take a look at each of these installation options to recognize their features



All previous diagrams reflect the Combination Server installation. Here we introduce a Multiple Server installation comprised of two ProCurve NAC 800s. One ProCurve NAC 800 provides the Management Server function while the other is an Enforcement Server.

The screenshot displays the ProCurve Network Agent interface. At the top, it says "Endpoint Screens" and "ProCurve Networking HP Innovation". A red 'X' icon indicates a failure: "Your computer needs immediate attention". Below this, a message states: "Test results from 3/9/07 1:51 pm show that your computer is not compliant with required network security policies. Your computer will only have limited access to the network until the following 6 issues are resolved:". A scrollable list of issues follows:

1. The required anti-spyware software was not found. Supported anti-spyware software: Webroot Spy Sweeper.
2. Automatic Updates must be configured to enabled, download automatically and notify before installing. For Windows 2000, install Service Pack 4, then enable Automatic Updates by selecting: Control Panel->Automatic Updates. For Windows XP: select Control Panel->System->Automatic Updates tab.
3. The hotfixes installed are not current. Run Windows Update to install the most recent service packs and hotfixes. The missing hotfixes are: 922760, 925454. You may need to run Windows Update multiple times to install all the hotfixes. Some of the hotfixes listed may be contained in a cumulative patch.
4. The following software is not allowed: present at registry key:

At the bottom of the list is a "PRINTABLE VERSION" button. Below the list, there is a help section: "Need help? Have questions or concerns? Contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55." and a "Diagnostics" link. At the very bottom is a "RETEST NOW" button.

On the right side of the screenshot, a smaller window titled "NAC Agent" is shown. It contains the message: "Your computer is not compliant with YourCompany's security policy. Click the button below for more details." and a "VIEW DETAILS" button.

26

As we chose to have a popup screen in our example, this is what the user on a failed endpoint would see on their screen. They would first see the popup on the right and once they click on "view details" their web browser will open and they will see a message similar to the one on the left that shows them what tests they have failed and hints on how to remediate there system. Once they believe they have fixed any/all issue's they can click on the retest now button to see if they are now in compliance.

IDM 2.2 and ProCurve Network Access Controller 800 Summary



		RADIUS				
		802.1X	Web Auth	Mac Auth	DHCP	Inline
Authentication	User	✓	✓			
	Client	✓	✓	✓		
	Location	✓	✓	✓		
	Time	✓	✓	✓		
	Posture	✓		✓	✓	✓
Authorization	QoS	✓	✓	✓		
	Rate Limit	✓	✓	✓		
	ACL	✓	✓	✓		
	VLAN	✓	✓	✓		
	IP Address				✓	
	IP Filter					✓
Accounting		✓	✓	✓	Limited	Limited

27

Aligned with standards based Authentication, Authorization, and Accounting this slide provides a snapshot of the combined features and capabilities of the new ProCurve Access Control Solution 2.0.

In the area of authentication, “Posture” is a new ability to validate an endpoint integrity. As we progress, this and all new features listed on the previous slides will be further explored.

ProCurve NAC EI Agent License and EI Maintenance



At initial purchase:

- ProCurve NAC EI Agent includes:
 - Software Agent License
 - Enables Endpoint Integrity testing using ProCurve NAC 800 hardware
 - ProCurve NAC 1-yr Maintenance License
 - Provides 1-yr live content updates to endpoint integrity checks:
 - OS patches
 - Virus signatures
 - AV software versions
 - AV virus definitions
- Additional 1-yr Maintenance Licenses purchased separately

ProCurve NAC EI Agent Licenses and 1-yr Maintenance



- 100 endpoints
- 250 endpoints
- 1000 endpoints
- 5000 endpoints

ProCurve NAC EI Agent 1-yr Maintenance



- 100 endpoints
- 250 endpoints
- 1000 endpoints
- 5000 endpoints

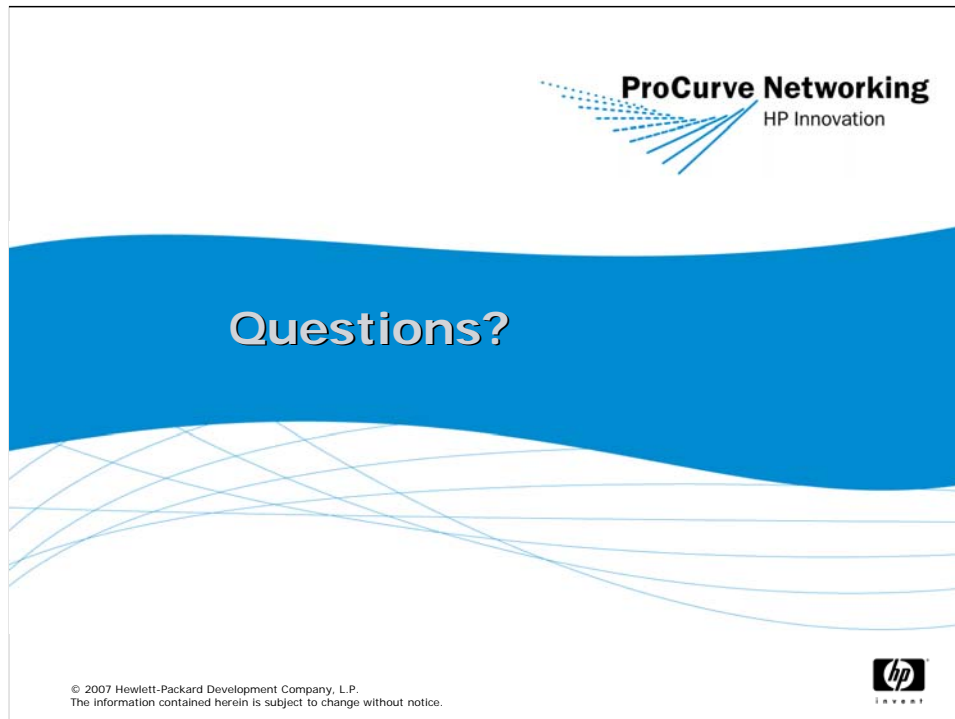
28

The initial purchase of ProCurve NAC 800 Agent licensing includes:

ProCurve NAC Endpoint Integrity (EI) Agent License to enable endpoint testing of endpoints.

ProCurve NAC 1-yr Maintenance License to enable live test updates and operating system patches for one year. This comes in quantities that support the number of Agent Licenses purchased.

Additional 1-yr maintenance licenses can be purchased. Multiple license part numbers exist to support 100, 250, 1000, or 5000 endpoints. Any mix of part numbers can be used to match the original product purchase.



We will now look at an example installation and configuration of ProCurve Access Control solution 2.0.



Thank you for your interest in learning about the ProCurve Network Access Control Solution 2.0