

Integrating ProCurve IDM and Windows NAP



Contents

| 1. Introduction | 3 |
|---|----|
| 2. Prerequisites | 3 |
| 3. Network and Active Directory tree diagrams | 3 |
| 4. Microsoft NAP architecture | 3 |
| 5. Configuration procedure | 4 |
| 5.1 Add the NPS Server role on your Windows 2008 Server | 4 |
| 5.2 Install the IDM Agent | 4 |
| 5.3 Configure an NPS policy | 5 |
| 5.4 Finish configuring NPS | 8 |
| 5.5 Define an IDM policy | 10 |

| 6. Configuring the Vista client | 11 |
|---|----|
| 6.1 Configure the Vista client | 12 |
| 6.2 Show authentication in the Vista client | 14 |
| 7. Reference documents | 15 |

1. Introduction

This application note illustrates how to integrate a ProCurve network and ProCurve Manager and Identity Driven Manager (PCM and IDM) with Windows Server 2008. It focuses on Windows Network Access Protection (NAP), the policy enforcement platform built into Microsoft Windows Vista and Windows Server 2008.

2. Prerequisites

This procedure assumes you have an already configured Windows Server 2008 installed, along with PCM/IDM, and connected to a ProCurve Switch 5400zl.

3. Network and Active Directory tree diagrams

Figure 1 details the hardware configuration referenced in this section.



ProCurve Switch 5400zl

Figure 1. Setup for integrating PCM/IDM and Windows NAP

4. Microsoft NAP architecture

With Windows Server 2008, Microsoft introduced Network Access Protection (NAP). This client-server architecture has three layers, as in the Trusted Network Connect (TNC) model. (Figure 2 shows TNC components in black, NAP in red.)



Figure 2. TNC and NAP

- Integrity Measurement Layer: This corresponds to the different tests that can be enforced on the endpoint and validated by the server; for example, antivirus test, Windows update test, and so forth. It contains, on the client side, the System Health Agents (SHAs) that collect health information. A built-in Windows SHA is available for Windows Vista and Windows XP SP3. Their counterparts on the server are the System Health Validators, which validate the health state provided by SHAs.
- Integrity Evaluation Layer: This corresponds to the security policy, the result of a set of tests done by the SHAs and SHVs. The NAP Agent coordinates and exchanges information between the SHA and Enforcement Client. The NAP Agent is available on Windows 2008, Vista, and XP SP3, and does continuous monitoring for ongoing policy enforcement. On the server side, the Administration Server coordinates and exchanges information between SHVs and the NAP Policy Server (NPS).
- Network Access Layer: This layer contains on the client side the NAP Enforcement Client (EC)—one for each connection mechanism (IPSec, DHCP, VPN, TS Gateway, 802.1X)—and handles access requests based on connection type. Its counterpart on the server is the NAP Enforcement Server. The NPS Service (RADIUS) receives information from the Enforcement Server, authenticates user identity and extracts system health information, and evaluates the validated health state for policy conformance. The NAP Enforcement Server enforces specific access capabilities specified by the NPS.

These different elements uses several types of messages to communicate:

- Statement of Health (SoH): Defines the state of the monitored component. Created by SHA and passed to NAP Agent.
- System SoH (SSoH): Complete set of SoHs from all SHAs. Packaged by Agent and sent by Enforcement Client to NPS through the Enforcement Server.
- SoH Response (SoHR): Can be healthy/unhealthy Response based on SoH claim.
- System SoHR (SSoHR): Complete set of SoHRs from all SHVs. Packaged by Administration Server for evaluation by NPS.

5. Configuration procedure

This section illustrates an example configuration procedure.

5.1 Add the NPS Server role on your Windows 2008 Server

To add the NPS Server role on your Windows 2008 Server:

- 1. Click Start, and then click Server Manager.
- 2. Under Roles Summary, click Add Roles, and then click Next.
- 3. Select the Network Policy and Access Services check box, and then click Next twice.
- 4. Select the Network Policy Server check box, click Next, and then click Install.

5.2 Install the IDM Agent

Install the IDM Agent from http://server-ip:8040. This operation must be performed on the client.

5.3 Configure an NPS policy

To configure an NPS policy:

1. From the Start Menu | Administrative Tools, open Network Policy Server.



- 2. In the Getting Started window, click on Configure NAP to launch the NAP Configuration Wizard.
- Choose a network connection method. In this case, the method is IEEE 802.1X Wired. Assign a name to this method (or simply leave the default name).



4. Configure the RADIUS clients (that is, the 802.1X authenticating switches). This is similar to IAS configuration on Windows 2003: you specify the IP address of the equipment and the shared secret.

| Configure NAP | × |
|---|-----------------------|
| Specify 802.1X Authenticating Switches | |
| RADIUS clients are network access servers, such as authenticating switches. RADIUS client computers. To specify a RADIUS client, click Add. RADIUS clients: | clients are not |
| 5400 3500 | Add Edit Remove |
| S400 Properties X Name and Address Friendly name: Friendly name: X Address (IP or DNS): 10.1.10.1 Verify Verify Shared Secret Verify and the same shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret: Confirm shared secret: Image: Confirm shared secret image: Confirm shared secr | |
| OK Cancel | |

5. On the next screen you can configure users and/or machine groups. In this example, user configuration is done in Identity Driven Manager. So you can skip this step.

6. On the next screen you configure an authentication method. This step is also similar to Windows 2003/IAS configuration: You select the NPS Server Certificate (if it is not already there), and the EAP type (Secure Password or Smart card or certificate).

| Configure NAP | x |
|---|---|
| Configure an Authentication Method | |
| Protected Extensible Authentication Protocol (PEAP) is the authentication method used with wireless access points and authenticating switches. To configure PEAP, you must select a server certificate on the NPS server and you must configure an authentication type. | |
| NPS Server Certificate To select a server certificate issued by your organization trusted root certification authority (CA) or a public CA that is trusted by client computers, click Choose. To view the selected certificate, click View. | |
| WIN-0PS0JN0FGI6.PCU01.edu (Valid until 2/24/2009 3:45:09 PM) | |
| View Choose | |
| EAP types: Select EAP types to use with PEAP. The authentication type determines the kind of credentials that NPS can accept from client computers and users (either user name and password or a cettificate). Secure Password (PEAP-MS-CHAP v2). This authentication type permits users to type password-based credentials during authentication. Smart Card or other certificate (EAP-TLS). This authentication type requires certificates on smart cards or in the client computer certificate store. For this authentication type you must deploy your own trusted root CA. | |
| | |
| Previous Next Finish Cancel | |

- 7. The next screen gives you the opportunity to configure VLANs using RADIUS attributes: an organization VLAN for users who have passed the endpoint integrity tests, and a restricted network VLAN. Since IDM will allocate the VLANs within the Access Profiles, you don't need to configure them under NPS. So skip this step.
- 8. Then you define the NAP Health Policy—that is, the set of tests that will be checked on the clients. In this example, the only available SHV is the built-in Windows Security Health Validator.

| Configure NAP X |
|---|
| Define NAP Health Policy |
| The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy. |
| Name Vindows Security Health Validator |
| Enable auto-remediation of client computers |
| If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers. |
| If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated. |
| Network access restrictions for NAP-ineligible client computers: |
| O Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only. |
| C Allow full network access to NAP-ineligible client computers. |
| Previous Next Finish Cancel |

On this screen you also decide whether to enable auto-remediation on NAP-capable client computers (leave it unchecked for purposes of this example), and whether non-NAP-capable clients will be allowed or denied access to the network.

9. Finally you see a summary of the different Health, Connection Request and Network Policies that have been defined:

| Configure NAP | | | | | x |
|---|---|---|---------------------------------------|-----------------------------|--------|
| | Completing N/ Client Configu | AP Enforcer ration | nent Polic | y and RAD | DIUS |
| You have succe • To view the co • To change the | safully created the followin infiguration details in your configuration, click Previo | g policies and com default browser, cli ous | lgured the follow ok Configuration | ing RADIUS clier Details | ta. |
| To save the co | onliguration and close this | wizard, click Finish | | | |
| NAP 802.1X (W NAP 802.1X (W | 19: red) 2 Compliant red) 2 Noncompliant | | | | |
| Connection R NAP 802.1X (W | equest Policy: red) 2 | | | | |
| Network: Polic NAP 802.1X (M NAP 802.1X (M NAP 802.1X (M | dea; red) 2 Compliant red) 2 Noncompliant red) 2 Non NAP-Capable | | | | |
| | | | | | |
| | | | | | |
| Configuration De | taks | | | | |
| | | | | | |
| | | Previous | Net | Finish | Cancel |
| | | 100 | 9 | Ge a | 1071 |

5.4 Finish configuring NPS

Once the policy has been created, you still have a few steps to complete in NPS:

1. Go to RADIUS Clients and Servers | RADIUS Clients, edit the clients, and configure them as NAP-Capable.



- 2. Go to Policies | Health Policies. You have two Policies: NAC 802.1X (Wired) Compliant and NAC 802.1X (Wired) Noncompliant. Edit both and check the conditions for the SHV. Specify the Client SHV checks as:
 - o Client passes all SHV checks for the Compliant policy.
 - \circ $\,$ Client fails one or more SHV checks for the NonCompliant policy.

| Server | | _ [] X |
|--|--|--------|
| File Action View Help | | |
| 🗇 🏟 🖄 📅 📓 📅 | | |
| ADJUS Clents and Servers ADJUS Clents and Servers ADJUS Clents RADJUS Clents | Health policies are used with Network Access Protection (NAP) and allow you to designate the configuration required NAP-capable client computers to access the network. | d for |
| E Policies | Policy Name | |
| Connection Request Polici | NAP 802.1X (Wired) Compliant | |
| Network Policies | NAP 802 1X (Wired) Noncompliant | |
| Health Policies | | |
| Network Access Protection | | |
| Te Accounting | | |
| | | |

| NAP 802.1X (Wired) Noncompliant Properties | × |
|---|---|
| Settings | |
| Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies. | |
| Policy game: | |
| NAP 802.1X (Wired) Noncompliant | |
| Client SHV checks: | |
| Client fails one or more SHV checks | 1 |
| SH <u>V</u> s used in this health policy: | |
| Name | |
| Windows Security Health Validator | 1 |
| | NAP 802.1X. (Wired) Noncompliant Properties Settings Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies. Policy game: NAP 802.1X (Wired) Noncompliant Client SHV checks: Client fails one or more SHV checks SHVs used in this health policy: Name Windows Security Health Validator |

- 3. In Network Access Protection, edit the Windows Security Health Validator. On the Settings tab, click on Configure. You obtain, for Windows Vista and Windows XP, the list of tests that the Windows SHV performs on the endpoints:
 - **For Windows Vista**: Firewall, Antivirus protection, Spyware protection, Automatic Updating, Security Updates Protection
 - For Windows XP (SP3): Same except no Spyware protection

For this example, uncheck everything except the Firewall test, so the SHAs will only check if a firewall is enabled on the client.

| 😌 Network Policy Server | | |
|---|--|---|
| File Action View Help | | |
| 🗢 🔿 🞽 📊 | | |
| ♦ NPS (Local) ■ ■ RADIUS Clients and Servers ■ RADIUS Clients ■ RADIUS Clients ■ Remote RADIUS Server G | System Health V SHVs and then | /alidators allow you to specify the settings required on NAP-capable client computers. add one or more to a health policy. |
| Policies | Name | Status |
| Connection Request Polici | Windows Security He | alth Validator Configured |
| Network Access Protection | | Windows Security Health Validator Properties |
| Remediation Server Group | | Settings |
| No. Counting | | To open and configure the system health validator program, click Configure. Configure |
| | | Error code resolution |
| | Windows Security I Status - Configured | Select how to resolve the following error codes that may be returned for this system health validator and its associated system health agent when a client requests network access. |
| | Error Code Configu SHV unable to contac | SHV unable to contact required services Noncompliant |
| | SHA unable to contac SHA not responding to | SHA unable to contact required services Noncompliant |
| | SHV not responding: Vendor specific error c | SHA not responding to NAP Client Noncompliant |
| | | SHV not responding Noncompliant |
| | | Vendor specific error code received Noncompliant |
| | | OK Cancel Apply |

5.5 Define an IDM policy

This example illustrates defining a simple IDM policy, with two groups of users: Marketing and Finance.

Identity Management Configuration:

- Locations: none
- Times: none
- Network Resources:
- Marketing Intranet: tcp 81 on 10.1.10.10
- Finance Intranet: tcp 82 on 10.1.10.10

Access Profiles:

| Access Profile | VLAN | QoS | Bandwidth | Network Resources |
|----------------|------|----------------|----------------|--|
| Marketing | 20 | Don't override | Don't override | Deny Finance Intranet Permit any |
| Finance | 30 | Don't override | Don't override | Deny Marketing Intranet Permit any |
| NonCompliant | 40 | Don't override | Don't override | Deny Marketing Intranet Deny Finance Intranet Permit any |

Access Policy Groups:

Finance and Marketing groups have been synchronized with Active Directory.

Finance: user jane

| Location | Time | System | WLAN | Endpoint Integrity | Access Profile |
|----------|------|--------|------|--------------------|----------------|
| ANY | ANY | ANY | ANY | PASS | Finance |
| ANY | ANY | ANY | ANY | FAIL | NonCompliant |

Marketing: user john

| Location | Time | System | WLAN | Endpoint Integrity | Access Profile |
|----------|------|--------|------|--------------------|----------------|
| ANY | ANY | ANY | ANY | PASS | Marketing |
| ANY | ANY | ANY | ANY | FAIL | NonCompliant |

6. Configuring the Vista client

The configuration of a Vista client is quite similar to the configuration of an XP client. With Vista, however, there are some additional considerations:

• In order to enable authentication to a port-authenticator (and obtain the Authentication tab on the client), the Wired AutoConfig service must be started. (Under Windows XP, it was the Wireless Zero Config service, for both wired and wireless.)

| Windows Search | Provides co | Started | Automatic | Local Syste |
|--------------------|--------------|---------|--------------|---------------|
| 端 Windows Time | Maintains d | Started | Automatic | Local Service |
| 🔍 Windows Update | Enables the | Started | Automatic (D | Local Syste |
| 🔍 WinHTTP Web Pr | WinHTTP i | Started | Manual | Local Service |
| 🎎 Wired AutoConfig | This service | Started | Automatic | Local Syste |
| 🖓 WLAN AutoConfig | This service | | Manual | Local Syste = |

For the Endpoint Integrity tests, the Network Access Protection Agent service must be also be started.

| 🔅 Multimedia Class | Enables rela | Started | Automatic | Local Syste |
|--------------------|--------------|---------|-----------|---------------|
| Ret.Tcp Port Shari | Provides abi | | Disabled | Local Service |
| Retlogon | Maintains a | Started | Automatic | Local Syste |
| Network Access P | Enables Net | Started | Automatic | Network S |
| A Network Connecti | Manages o | Started | Manual | Local Syste |

Before configuring the Vista client, check that these two services are started on the client machine. You can define a Group Policy on the domain to automatically start these services on each computer. For more information on how to configure it, please refer to the *NAP_802.1X_StepByStep.doc* document, available from Microsoft.

6.1 Configure the Vista client

To access the Network Connections under Vista:

- 1. From the Start Menu go to Network.
- 2. In Network, choose Network and Sharing Center:

| F asks Fiew computers and devices Connect to a network Set up a connection or network Manage network connections | Network and Sharing |) Center | View full map |
|---|--|---|---------------|
| Diagnose and repair | (This comp | Duter) | Internet |
| | Junidentified network | (Public network) | Customize |
| | | | |
| | Access | Limited Connectivity | |
| | Connection | Limited Connectivity Local Area Connection | View status |
| | Access Connection Sharing and Discovery | Limited Connectivity Local Area Connection | View status |
| | Access Connection Connection Sharing and Discovery Network discovery | Limited Connectivity Local Area Connection | View status |
| | Access Connection B Sharing and Discovery Network discovery File sharing | Limited Connectivity Local Area Connection • Off • Off | View status |
| | Access Connection Sharing and Discovery Network discovery File sharing Public folder sharing | Limited Connectivity Local Area Connection | View status |
| | Access Connection Sharing and Discovery Network discovery File sharing Public folder sharing Printer sharing | Limited Connectivity Local Area Connection | View status |

- 3. From there, click on Manage Network Connections. You obtain the list of your connections.
- 4. Right-click on your LAN connection and choose Properties, then choose the Network tab.
- 5. On the Network tab, disable IPv6:



6. On the Authentication tab, enable IEEE 802.1X and choose Protected EAP as the network authentication method:

| 📮 Local Area Connec | tion Prop | erties | | × |
|--|-------------------------------------|---|------------------|-----|
| Networking Authenti | cation | | | |
| Select this option t this Ethemet adap I Enable IEEE 8 Choose a network | to provide a ter. 02.1X authe | uthenticated entication tion method | d network access | for |
| Protected EAP (P | 'EAP) | • | Settings | |
| Cache user inf to this network | ormation for | subsequen | t connections | |

7. Click on Settings to configure the PEAP properties. Put a check mark in the Validate server certificate box, choose the server certificate from your certification authority, and select EAP-MSCHAPv2 as the authentication method.

Then click Configure.

| Protected EAP Properties | | | | |
|--|--|--|--|--|
| When connecting: | | | | |
| Connect to these servers: | | | | |
| Trusted Root Certification Authorities: | | | | |
| Class 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority ✓ PCU01-WIN-0PS0JN0FGI6-CA Thawte Server CA Thawte Timestamping CA | | | | |
| Do not prompt user to authorize new servers or trusted certification authorities. | | | | |
| Select Authentication Method: | | | | |
| Secured password (EAP-MSCHAP v2) Configure | | | | |
| ✓ Enable Fast Reconnect ✓ Enable Quarantine checks ✓ Disconnect if server does not present cryptobinding TLV | | | | |
| OK Cancel | | | | |

8. In the EAP MSCHAPv2 Properties box, select Automatically use my Windows logon name and password, and click OK.



9. In the Protected EAP Properties window, select Enable Fast Reconnect and Enable Quarantine Checks. Click on OK twice.

6.2 Show authentication in the Vista client

To show an authentication from the Vista Client:

- 1. Start a Windows 2008 Server image.
- 2. Plug the Vista client into a port authenticator and log on as john/hp. (Log off your Vista session and log on again if you were logged as another user). You should obtain the following message:

| This computer meets the requireme You have full network access. | ents of this network × |
|--|------------------------|
| | |
| Network Access Protection | |
| Network Connections Folder | |

3. If you click on this message, or if you right-click on the icon and choose Network Access Protection, you obtain more details:



7. Reference documents

This concludes the procedure for integrating ProCurve IDM and Windows NAP.

For further information about how to configure ProCurve switches and ProCurve IDM to support security, please refer to the following links:

- For the *ProCurve Identity Driven Manager User's Guide* for Software Release 2.3: <u>http://cdn.procurve.com/training/Manuals/IDM_UG-59908851-0508.pdf</u>
- For other PCM+ and IDM manuals: <u>http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm</u> http://www.hp.com/rnd/support/manuals/IDM.htm
- For user manuals for ProCurve 3500yl-5400zl-8212zl switches: http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm
- For ProCurve Switch 2610 series manuals: <u>http://www.hp.com/rnd/support/manuals/2610.htm</u>

For further information, please visit www.procurve.eu



© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, and Active Directory are U.S. registered trademarks of Microsoft Corporation.

4AA2-1625EEE, July 2008