# ProCurve Network Access Control
for HP Thin Clients and CCI

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>The Components</td>
<td>2</td>
</tr>
<tr>
<td>HP PC Client Computing Solutions</td>
<td>2</td>
</tr>
<tr>
<td>Network Access Control</td>
<td>3</td>
</tr>
<tr>
<td>ProCurve Networking Access Control</td>
<td>3</td>
</tr>
<tr>
<td>ProCurve NAC 800 Solution</td>
<td>4</td>
</tr>
<tr>
<td>Implementation Prerequisites</td>
<td>4</td>
</tr>
<tr>
<td>The Implementation</td>
<td>5</td>
</tr>
<tr>
<td>NAC Installation</td>
<td>5</td>
</tr>
<tr>
<td>Connecting to the Network</td>
<td>5</td>
</tr>
<tr>
<td>Initial Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Configuring Policy Settings</td>
<td>9</td>
</tr>
<tr>
<td>Testing Methods</td>
<td>9</td>
</tr>
<tr>
<td>Quarantine and Remediation</td>
<td>9</td>
</tr>
<tr>
<td>Thin Client Policy</td>
<td>10</td>
</tr>
<tr>
<td>Blade PC Policy</td>
<td>13</td>
</tr>
<tr>
<td>End-Point Configuration</td>
<td>17</td>
</tr>
<tr>
<td>Thin Client Firewall Exceptions</td>
<td>17</td>
</tr>
<tr>
<td>Policy Enforcement</td>
<td>23</td>
</tr>
<tr>
<td>Thin Client Policy Enforcement</td>
<td>23</td>
</tr>
<tr>
<td>Blade PC Policy Enforcement</td>
<td>27</td>
</tr>
<tr>
<td>For more information</td>
<td>32</td>
</tr>
<tr>
<td>HP Links:</td>
<td>32</td>
</tr>
<tr>
<td>General NAC Links</td>
<td>32</td>
</tr>
</tbody>
</table>
Introduction

This white paper provides a reference implementation of layered security policy enforcement created by integrating HP thin clients and Consolidated Client Infrastructure (CCI) blade PCs with the HP Procurve Network Admission Control (NAC) solution. The combination of HP thin clients and Consolidated Client Infrastructure (CCI) blade PCs provides a very robust, secure, and cost-effective computing solution that can be applied to any network. Like any other networked component, it is important to examine security issues associated with their operation. This paper addresses the use of network policy enforcement services with HP thin clients and blade PCs linked to the HP ProCurve Network Access Control (NAC) appliance, NAC800, to ensure PC client devices on the network are properly configured; otherwise these clients can be quarantined or remediated. Overviews of NAC, as well as their usage models and known working implementations, are provided.

The Components

HP PC Client Computing Solutions

HP PC client computing solutions consist of two major components: thin clients and blade PCs. A thin client is a computing device without a hard drive that provides display and input/output for applications running on remotely located servers or blade PCs. A basic thin client consists of a processor, flash memory for storing the embedded operating system, local RAM, a network adapter, and standard input/output for the display and other select peripherals. HP thin clients have no moving parts, offering higher reliability than a PC, lower ownership costs, enhanced security, and extended product life. These small, robust devices consume significantly less energy than a desktop PC, put out less heat into your office spaces, are made with much less material than a desktop, and are practically silent.

HP offers thin clients based on three operating systems: Windows XPe, Debian Linux, and Windows CE. Each operating system provides protection for the OS image housed within the flash device while creating a partition on that flash device to act as a virtual hard drive. Only an account with administrator privileges can make changes to the base image to add applications or operating system patches. With the Windows XPe operating system, HP also includes a Sygate firewall on the base image that locks down all ports except those necessary for typical Microsoft Remote Desktop Protocol (RDP) and Citrix-level connections and general Web browsing. The Sygate settings must be edited to unlock any additional ports on the thin client.

Consolidated Client Infrastructure (CCI) is the enterprise/data center computing architecture through which blade PCs can be allocated to end-users connecting on thin clients. The blade PCs are stored and managed in a centralized location, and are accessed through HP Remote Graphics Software (RGS) or RDP. A remote user can present credentials to the HP Session Allocation Management (SAM) service and be connected to a computing session on a blade PC with access to network resources such as applications and data. Unlike Terminal Services-, Citrix-, or VDI-hosted computing sessions, CCI compute sessions typically match up a connected user onto a blade PC that is not shared, which provides a stable computing experience that does not change as additional users are added to the array of PC blades.

Although CCI blade PCs are housed in the data center for security, they are full-blooded PC systems running the latest operating systems. As such, it is assumed in this paper that images for blades are configured with a firewall and virus scanning software as a security baseline. For the usage models presented here, the blades were configured to use the native Windows XP firewall, as well as anti-malware software.
Network Access Control

Advancements in computer networking have significantly changed the way people and organizations communicate and access information. Networks have become critical resources in many organizations, providing real-time communications and access, through both the Internet and enterprise intranets, to unprecedented levels of information. In addition, much of the data available on internal business networks needs to be protected, either to follow data privacy regulations or to protect valuable information assets. As such, the need to provide reliable and secure network access has become a key challenge facing today’s Information Technology (IT) organizations.

As organizations take advantage of the benefits of making information available, they also need to consider the security implications. They must protect valuable proprietary information. They also might be responsible for complying with government regulations related to data privacy. This leads to two business objectives that many IT organizations are striving to maximize: data availability and data security. While addressing each of these objectives individually can be straightforward, the methods used to address one often conflict with the other. Therefore, it is important for organizations to address these objectives together.

To meet these needs adequately requires a layered security approach, often defined as Defense in Depth. NAC is one component of such an approach, and should not be considered in isolation. The high level role of NAC is to protect the network and its resources from harmful users and devices or systems. It does this by restricting network access based on certain criteria and business policies. The policies may be quite simple, such as allowing access to a set of known users or devices while denying all others. Or, in order to model more intricate business policies, the policies may be much more complex.

NAC works together with other network security layers such as firewalls, Intrusion Detection and Prevention Systems (IDPS), endpoint security, and so forth to build a defensive posture in your environment. NAC should be used to minimize the risk associated with unauthorized, infected, or improperly configured devices trying to connect to your network.

In its most basic form, NAC allows a network administrator to restrict network access to authorized users and/or devices. However, many organizations have the need to provide, or can benefit from providing, different levels of access depending on the role of the user. For example, employees have access to internal network resources and the Internet while guest users are only provided access to the external Internet.

There is also a need for protection from malicious software, which is accomplished by evaluating the security posture of devices connecting to the network. The security posture required is defined by organizational policies and is based on checking for things such as operating system versions and patches, security software (antivirus, anti-spam, firewalls, etc.), security settings on common software, and other required or prohibited software.

There are many aspects to a complete network security implementation. This white paper addresses use cases of Network Access Control (NAC) as applied to HP thin clients and blade PCs to control their access to a production network and the information available on that network. It also describes the access control solution provided by ProCurve networking by HP.

ProCurve Networking Access Control

The ProCurve Access Control Solution is based on the ProCurve Adaptive EDGE Architecture and its “command from the center” approach to management. It begins with ProCurve network devices that push intelligence to the edge of the network, where users and devices connect. The ProCurve Identity Driven Manager (IDM) product is a network access policy server that dynamically adapts network ports to the needs of the user and device(s). The ProCurve Network Access Controller 800 enables a simplified authentication service deployment, along with endpoint integrity policy verification. Together, these products create a comprehensive access control solution that fortifies network security.

This solution implements the ProCurve Network Access Controller 800.
ProCurve NAC 800 Solution

The ProCurve NAC 800 is designed with multiple enforcement modes to accommodate the needs of enterprise networks. All enforcement methods use pre-authorization checks for security policy in order to protect the network from harmful systems. The following enforcement modes can be used together to provide complete access control coverage across the network:

- **802.1X Enforcement**: Utilizing the 802.1X capabilities in ProCurve network devices, this is the most efficient and effective enforcement method and is recommended for environments with devices supporting 802.1X authentication. Users and devices are authenticated using RADIUS. Endpoints are isolated so they can be tested for security policies. Then, they are either allowed to join the network, or are put in a remediation network so the user can resolve the security settings that have caused the isolation.

- **In-line Enforcement**: In this mode, the ProCurve NAC 800 is placed in-line with network traffic and actively filters new connections until they are tested for compliance with the security policies. This is an effective solution for testing endpoints that connect remotely through a VPN concentrator.

- **DHCP Enforcement**: The ProCurve NAC 800 integrates with the enterprise DHCP server to isolate and test endpoints. As endpoints request a network address, they are isolated by their network address so they can be tested for compliance with security policies. If they comply, they are provided with a new network address and allowed to participate on the network. If they fail, they are placed into a remediation network so the user can resolve the security settings that have caused the isolation. This method is useful for environments where 802.1X authentication is not available because it is not supported by the network infrastructure.

Each mode provides benefits, and poses drawbacks, to the security of certain networks. The inline mode has a greater ability to restrict devices, since the appliance physically sits between the clean and unclean networks; however, this mode can tend to be hard to scale up to larger deployments. The DHCP model is well-suited for existing infrastructures of any size, but care and consideration must be given to the current network’s threat model for this model to be effective. Lastly, IEEE 802.1X provides a robust authentication scheme that integrates well, but it requires extra infrastructure (such as RADIUS services and 802.1X supplicants).

The remainder of this white paper provides a working example to demonstrate the use of the ProCurve NAC appliance in DHCP mode. In particular, we concentrate on the nuances in configuring HP blade PCs and thin client hardware as they relate to a NAC implementation.

Implementation Prerequisites

For the purpose of this white paper, we assume a basic network infrastructure is already in place. The reference implementation consists of HP BladeSystem bc1500, bc2000, and bc2500 Blade PCs running Windows XP. HP Compaq t5720 Thin Clients (t5720) running Windows XPe are used as access devices.

The network topology for this reference implementation consists of a flat Class-C network setup with topology: 172.16.1.xxx/24, see Table 1 below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Operating System</th>
<th>Host Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS, DHCP, Active Directory Servers</td>
<td>Windows 2003Server</td>
<td>ccidc.ccidomain.net</td>
<td>172.16.1.250</td>
</tr>
<tr>
<td>Thin Client (t5720)</td>
<td>Windows XPe</td>
<td>t5720.ccidomain.net</td>
<td>172.16.1.1 – 172.16.1.10</td>
</tr>
<tr>
<td>Blade PC (bc1500, bc2000 &amp; bc2500)</td>
<td>Windows XP, Vista</td>
<td>bc2000.ccidomain.net</td>
<td>172.16.1.11 – 172.16.1.19</td>
</tr>
</tbody>
</table>

Table 1 -- Procurve NAC Reference Solution -- Network Topology
The Implementation

NAC Installation

This section covers use of a ProCurve NAC 800 appliance to ensure that thin clients and blade PCs meet configuration policy prior to receiving a valid IP address on the production network. We use the NAC800 switch in DHCP mode and set up a quarantine DHCP area via the Web-based administration console.

Connecting to the Network

In order to install the ProCurve NAC 800 into the network, do the following:

1. Disconnect the DHCP server (this may be the domain controller, as well) from the production network.
2. Connect RJ45 Port 1 of the NAC 800 directly into the production network.
3. Connect DHCP server to RJ45 Port 2 on the NAC 800.

Note that the ProCurve NAC 800 appliance has an internal switch, so a crossover cable is unnecessary.

The NAC 800 should now be inline with the switch and the domain controller. This allows the interception of DHCP requests to enforce testing before an IP address is issued to the end-point devices.

Initial Configuration

The ProCurve NAC 800 can be used as a Combination, Management, or Enforcement server. For the purpose of this reference implementation, we are defining the ProCurve NAC 800 as a Combination Server. This is the default server type configured on a new ProCurve NAC 800. A Combination server provides the combined functions of both Management and Enforcement Servers. Using the LCD and Front Panel buttons, configure the following settings:

- Server Type: Combination Server
- IP Address – Port1: 172.16.1.101
- Subnet Mask: 255.255.255.0
- Gateway: 172.16.1.150

Now the NAC should be ready to be configured via the Web Console as shown in the following illustration. This is the main interface that we use from now on to configure the NAC appliance.
1. Using the domain controller, go to https://172.16.1.101 in Internet Explorer to view the Web console.

2. Click **OK** when the Security Alert appears.

3. Accept the license agreement.
4. Enter management server settings:
   o Root Password: procurve [Type a root configuration “password.”]
   o Re-enter Password: procurve [Type the root configuration “password” again.]
   o Region: Enter a region for your location.
   o Time Zone: Enter a time zone for your location.
   o NTP Servers: Type 172.16.1.250.
   o Host Name: Type nac800.ccidomain.net.
   o DNS IP Address: Type 172.16.1.250.

5. Create an administrator account:
   o User ID: admin
   o Password: password01 [Type a Web administration “password.”]
   o Re-enter Password: password01 [Type a Web administration “password” again.]

6. Click Finish. The home menu of the Web Console is now displayed.
7. Click **System Configuration**.

8. Click **Quarantining**.

9. For the purposes of this paper, we are demonstrating DHCP quarantining methods. Select the **DHCP** button.

10. Select **Add Quarantine Area**.

11. Type the following information in the appropriate fields:
   - Quarantined Subnet: 10.88.10.0/24
   - DHCP IP Range: 10.88.10.100 to 10.88.10.150
   - Gateway: 10.88.10.1
   - Domain: ccidomain.net
   - Non-quarantined subnets: 172.16.1.0/24
   - DHCP Quarantine Option: Router Access Control Lists (ACLs)

12. Click **OK** twice.
Configuring Policy Settings

As we are focusing on the integration of NAC into a CCI and thin client network, we are exploring only the network policy enforcement settings that are pertinent to thin clients and blade PCs. This is by no means all the features of the ProCurve NAC Solution. Likewise, in a production environment, you may wish to validate many more Windows configuration components than are discussed in this reference white paper.

Testing Methods

The NAC 800 has three ways to test policy on new devices: the NAC agent, an ActiveX agent, and agentless methods. The NAC agent is a permanent service that is installed onto the device to check policy periodically and report to the NAC 800 switch. The ActiveX agent tests new devices by being downloaded through a Web browser per testing session. Finally, the agentless method uses administrative credentials to run remote method invocation, so no local agent needs to be installed.

In order to select which testing mode to use:

From the home screen of the NAC Web console (https://172.16.1.102), select **System Configuration**.

![System Configuration](image)

Quarantine and Remediation

On the network switch used in this example, we have configured two separate subnets to provide a quarantine area for devices found to be out of compliance. In our examples above, we are using one VLAN (VLAN 1) for network configuration. We configured a second IP address for VLAN 1 of 10.88.10.1 with a 24-bit subnet mask (class C). This second IP address range allows for a remediated client to communicate with the ProCurve NAC 800 appliance while they are in a quarantined state. The ProCurve NAC 800 responds to DHCP requests for clients with an address in the 10.88.10.x range until the device has passed all testing.
Thin Client Policy
First, since we are just evaluating the NAC appliance, we must ensure that the appliance does not quarantine machines from the network, but merely warns that it would have been quarantined.

1. From the home screen of the NAC Web console (https://172.16.1.102), select System Configuration.

2. Click Cluster #1.

3. Set the Access Mode to be Allow all.

4. Select OK.

Now, we can set up our policy that pertains specifically to thin clients.
5. On the Domain Controller, open Internet Explorer and go to https://172.16.1.102/ (the Web console).

6. Log on to the Web console to access the home screen.

7. From the navigation menu on the left, select **NAC policies**.

8. Select **Add a NAC policy**.
9. Under Basic Settings, in the Policy Name text box, enter Thin Client Policy.
10. Set the NAC Policy Group to Default.
11. Set the Operation Mode to Enabled.
12. Set the Retest Frequency to retest every 2 minutes.
13. Select Never quarantine inactive endpoints.

14. Select Tests from the left navigation bar. On the Tests page, you can select the tests for this particular policy.

15. Enable and select the Services Required test. This test requires devices to have the specified services running.
16. In the Test Properties text box, enter EWFStatusSvc, which is the name of a service that is related to the thin client write filter.

17. Under Test failure actions check Quarantine Access and select Immediately.

18. Locate the Personal Firewalls test, and enable and select it. This test enforces a required firewall.

19. Under Test Properties, clear all check boxes except for Sygate Personal Firewall, which is the standard firewall installed on HP thin clients.

20. Under Test failure actions, select Quarantine Access and Immediately.

21. Select OK at the top of the window.

Blade PC Policy
First, since we are just evaluating the NAC appliance, we must ensure that the appliance does not quarantine machines from the network, but merely warns that it would have been quarantined.

1. From the home screen of the NAC Web console (https://172.16.1.102), select System Configuration.
2. Click **Cluster #1**.

3. Set the **Access Mode** to be **Allow all**.

4. Select **OK**.

   Now, we can set up our policy that pertains specifically to blade PCs.


6. Login to the Web console to access the home screen.
7. From the navigation menu on the left, select **NAC policies**.

8. Select **Add a NAC policy**.
9. Under **Basic Settings**, in the **Policy Name** text box, enter **Blade Policy**.
10. Set the **NAC Policy Group** to **Default**.
11. Set the **Operation Mode** to **Enabled**.
12. Set the **Retest Frequency** to retest every 2 minutes.
13. Select **Never quarantine inactive endpoints**.
14. Select **Tests** from the left navigation bar. The **Tests** page is where tests are put in place for this particular policy.

15. Find the **Services Required** test, enable and select it. This test ensures that any device under this policy has the specified services running.

16. In the **Test Properties** text box, enter *daesvc*, which is the name of a service that is related to the SAM server.

17. Under **Test failure actions** check **Quarantine Access** and select **Immediately**.

18. Find the **Personal Firewalls** test, enable and select it. This test enforces a required firewall.
19. Under **Test Properties**, clear all checkboxes except for **Windows Firewall**.
20. Under **Test failure actions**, check **Quarantine Access** and select **Immediately**.
21. Select **OK** at the top of the window.

**End-Point Configuration**

**Thin Client Firewall Exceptions**

The HP t5720 XPe-based thin client is configured by default with the Sygate firewall actively blocking all ports except those required for basic Web browsing and RDP connections. The t5720 thin clients used in this reference white paper also had firewall port exceptions added for RGS, which accelerates graphics in a manner superior to RDP.

In order to properly communicate with the NAC 800 and allow scans to the t5720, the Sygate firewall must be modified as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>IP Address</th>
<th>Remote Ports</th>
<th>Local Ports</th>
<th>Incoming/Outgoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow NAC UDP</td>
<td>172.16.1.101</td>
<td>137, 1500</td>
<td>Both</td>
<td></td>
</tr>
<tr>
<td>Allow NAC TCP In</td>
<td>172.16.1.101</td>
<td>139, 1500</td>
<td>Incoming</td>
<td></td>
</tr>
<tr>
<td>Allow NAC TCP Out</td>
<td>172.16.1.101</td>
<td>89</td>
<td>Outgoing</td>
<td></td>
</tr>
</tbody>
</table>

1. Reboot the t5720 and log on using an account with administrator privileges. This ensures that the thin client is in a known, clean OS state.
2. In the **System Tray**, right-click the **Sygate** icon.
3. Select **Advanced Rules**.
4. Read the warning notification and click **OK**.
5. In the **Advanced Rules** window, click **Add**.
6. On the **General** tab, type **Allow NAC UDP** in the **Rule Description** field.
7. Select **Allow this traffic**.
8. On the **Hosts** tab, select **IP Addresses**, and then type the IP address of the NAC800 (172.16.1.101) in the field.

![Advanced Rule Settings](image)

9. On the **Ports and Protocols** tab in the **Protocol** list, select **UDP**.
10. Type 137, 1500 in the **Local** field.

![Advanced Rule Settings](image)

11. In the **Traffic Direction** list, select **Both**.
12. Click **OK**.
13. In the **Advanced Rules** window, click **Add**.
14. In the **Advanced Rule Settings** window on the **General** tab, type **Allow NAC TCP In** in the **Rule Description** field.
15. Select **Allow this traffic**.

16. In the **Hosts** tab, select **IP Addresses** and then type the IP address of the NAC800 (172.16.1.101) in the field.
17. In the **Ports and Protocols**, select **TCP** in the **Protocol** field.
18. Type 139, 1500 in the **Local** field.

![Advanced Rule Settings](image)

19. Select **Incoming** in the **Traffic Direction** field.
20. Click **OK**.
21. In the **Advanced Rules** window, click **Add**.
22. In the **Advanced Rule Settings** window, on the **General** tab, type **Allow NAC TCP Out** in the **Rule Description** field.
23. Select **Allow this traffic**.

![Advanced Rule Settings](image)
24. On the **Hosts** tab, select **IP Addresses** and type the IP address of the NAC800 (172.16.1.101) in the field.

25. On the **Ports and Protocols** tab, select **TCP** in the **Protocol** field.

26. Type 89 in the **Remote** field,

27. Select **Outgoing** in the **Traffic Direction** field.
28. Click **OK**.
Policy Enforcement

Now that the ProCurve NAC appliance is fully integrated into the network and configured with policy tests, we can now demonstrate policy enforcement in action.

<table>
<thead>
<tr>
<th>Generic Testing Methods</th>
<th>ProCurve Name Method</th>
<th>Trade-offs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Plus (+)</td>
</tr>
<tr>
<td>Agent-based</td>
<td>NAC Agent</td>
<td>• Always available for retesting</td>
</tr>
<tr>
<td>Permanent</td>
<td></td>
<td>• Automatic Agent updates</td>
</tr>
<tr>
<td>Agentless</td>
<td>Agentless</td>
<td>• No install or download</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Easiest of the three test methods to deploy</td>
</tr>
<tr>
<td>Agent-based</td>
<td>ActiveX</td>
<td>• No installation or upgrade to maintain</td>
</tr>
<tr>
<td>Transient</td>
<td></td>
<td>• Only Internet Explorer application access is allowed through the personal firewall. No open ports are necessary</td>
</tr>
</tbody>
</table>

Table 2 – ProCurve NAC 800 DHCP Enforcement Methods

Thin Client Policy Enforcement

1. Turn on the thin client.
2. Ensure that the firewall and write filters are running.
4. Click **Begin Testing** to start the policy test.

5. Upon your first connection to the NAC 800 appliance in transient agent-based mode (as described in **Policy Enforcement**), you are prompted to accept an ActiveX control. Depending on your version of Web client (Internet Explorer 6.0 is used in this reference document) and security setting in that Web browser, you may have to right-click on the notification bar to accept installation of the ActiveX control, as shown here.

   **NOTE:** This can be avoided by pre-installing a dedicated NAC agent or by validating compliance in Agentless mode using an RPC connection to the client being tested.
Once the ActiveX control is loaded, the testing can begin for the thin client.

6. Confirm this by opening a command prompt and typing `ipconfig`. The result should show that the thin client IP address is 172.16.1.x.

7. Close the browser.

8. Right-click **My Computer**.
9. Click **Manage**.

10. Click **Services and Applications**.

11. Click **Services**.

12. Disable **EWF Status Service** by right-clicking on the entry and selecting **Stop**.

13. Retest the machine.
Now, since the required service is off, the thin client is out of policy, so it is placed in the quarantine subnet.

14. Confirm this by opening a command prompt and typing `ipconfig`. The result should show that the thin client IP address is now 10.88.10.x.

15. Restart **EWF Status Service**.

16. Retest the thin client to verify that the thin client meets policy again and is admitted to the network.

17. Confirm this by opening a command prompt and typing `ipconfig`. The result should show that the thin client IP address is again 172.16.1.x.

**Blade PC Policy Enforcement**

1. Turn on the blade PC.

2. Ensure that the firewall and write filters are running.
3. Go to [https://172.16.1.102:89](https://172.16.1.102:89) on your browser.

4. Upon your first connection to the NAC 800 appliance in transient agent-based mode (as described in Policy Enforcement), you are prompted to accept an ActiveX control. Depending on your version of Web client (Internet Explorer 6.0, for this reference document) and security setting in that Web browser, you may have to right-click on the notification bar to accept installation of the ActiveX control as shown here.

   NOTE: This can be avoided by pre-installing a dedicated NAC agent or by validating compliance in Agentless mode using an RPC connection to the client being tested.
5. Start the policy test by clicking **Begin Testing**.

![Image of a computer screen showing a web page with a message that the user has full access to the network.]

At this point, the blade PC should be in policy and therefore should be allowed to access the network.

![Image of a command prompt showing the IP configuration details, including the thin client IP address of 172.16.1.x.]

6. Confirm this by opening a command line up and typing `ipconfig`. It should show that the thin client IP address is 172.16.1.x.

7. Close the browser.
8. Right-click **My Computer**.
9. Select **Manage**.
10. Select **Services and Applications**.
11. Select **Services**.

12. Next, right-click on **HP SAM registration Service** and select **Properties**. Click **Stop** to end this DAESVC service.
13. Retest the machine.

Now, since the required service is off, the blade PC is out of policy, so it is placed in the quarantine subnet.

14. Confirm this by running ipconfig on the command line to ensure the thin client IP address is 10.88.10.x.

15. Restart the DAESVC Service.

16. Retest the machine.

17. Repeat steps 5 and 6 to verify that the blade PC meets policy again and is admitted to the network.
For more information

For more information about the HP thin clients or any other HP product, contact your HP Authorized Reseller or visit these online locations to learn more about HP products, services, and support:

HP Links:

- HP desktop, blade PC or thin client information: www.hp.com/desktops
- HP Procurve NAC 800 Appliance: http://www.hp.com/rnd/support/manuals/NAC800.htm
- HP workstations information: www.hp.com/workstations
- HP security: www.hp.com/go/security
- HP notebook information: www.hp.com/notebooks
- HP notebooks options information: www.hp.com/notebooks/options
- HP desktop options information: www.hp.com/desktops/options
- HP Services: www.hp.com/go/services
- HP support: www.hp.com/go/support
- HP Care Pack: www.hp.com/hps/carepack
- “How to buy”: www.hp.com/buy/howtobuy

ProCurve NAC Links

- ProCurve Network Access Control
- ProCurve NAC 800 Overview
  http://www.hp.com/rnd/products/Appliance/ProCurve_Network_Access_Controller_800/overview.htm
- ProCurve Network Immunity Manager 1.0
  http://www.hp.com/rnd/products/management/ProCurve_Network_Immunity_Manager_1.0/overview.htm
- ProCurve Identity Driven Manager (IDM) 2.2

© 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.

Linux is a U.S. registered trademark of Linus Torvalds. Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

466209-001, January 2008