ProCurve Network Access Control for HP Thin Clients and CCI

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 an/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.

Component	Operating System	Host Name	IP Address
DNS, DHCP, Active Directory Servers	Windows 2003Server	ccidc.ccidomain.net	172.16.1.250
Thin Client (t5720)	Windows XPe	t5720.ccidomain.net	172.16.1.1 – 172.16.1.10
Blade PC (bc1500, bc2000 & bc2500)	Windows XP, Vista	bc2000.ccidomain.net	172.16.1.11 – 172.16.1.19

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 1of 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.

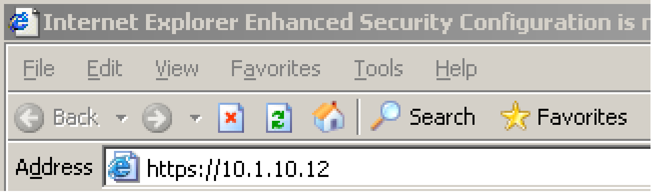
The NAC 800 should now be inline with the switch and the domain controller. This allows the interception of DHCP requests to enforce testing before an IP address is issued to the end-point devices.

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:

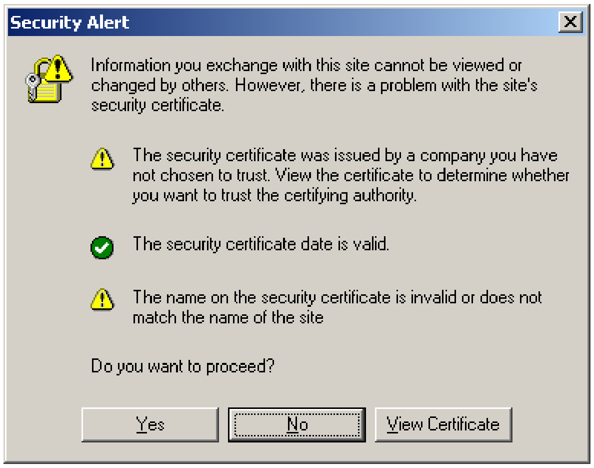
- Server Type: Combination Server
- IP Address – Port1: 172.16.1.101
- Subnet Mask: 255.255.255.0
- Gateway: 172.16.1.150

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.



https://10.1.10.12

1. Using the domain controller, go to https://172.16.1.101 in Internet Explorer to view the Web console.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

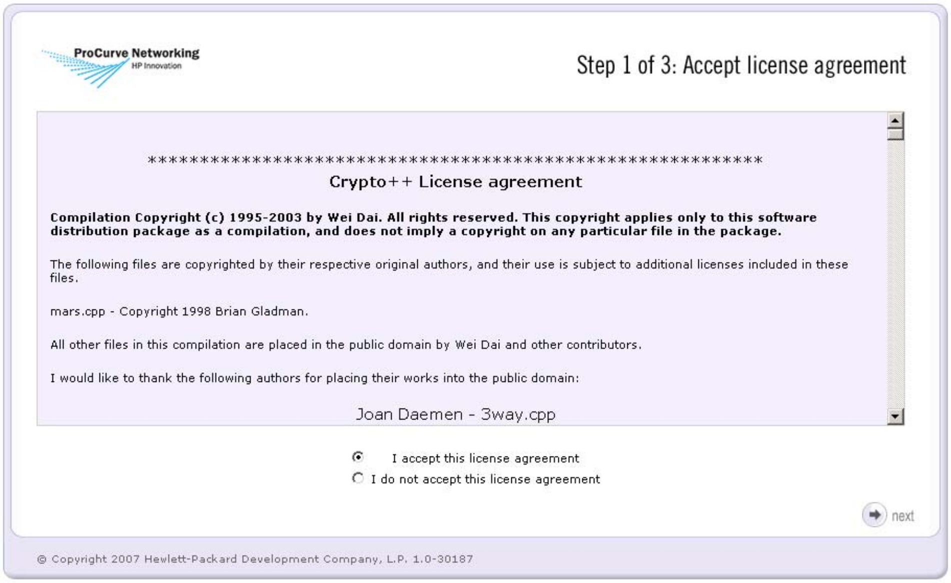
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

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



Step 1 of 3: Accept license agreement

****

Crypto++ License agreement

Compilation Copyright (c) 1995-2003 by Wei Dai. All rights reserved. This copyright applies only to this software distribution package as a compilation, and does not imply a copyright on any particular file in the package.

The following files are copyrighted by their respective original authors, and their use is subject to additional licenses included in these files.

mars.cpp - Copyright 1998 Brian Gladman.

All other files in this compilation are placed in the public domain by Wei Dai and other contributors.

I would like to thank the following authors for placing their works into the public domain:

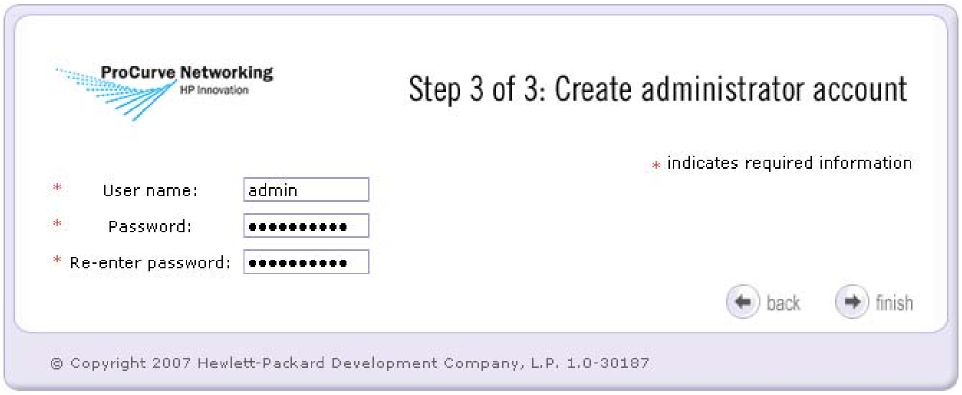
Joan Daemen - 3way.cpp

● I accept this license agreement
○ I do not accept this license agreement

© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30187

3. Accept the license agreement.

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



Step 3 of 3: Create administrator account

* indicates required information

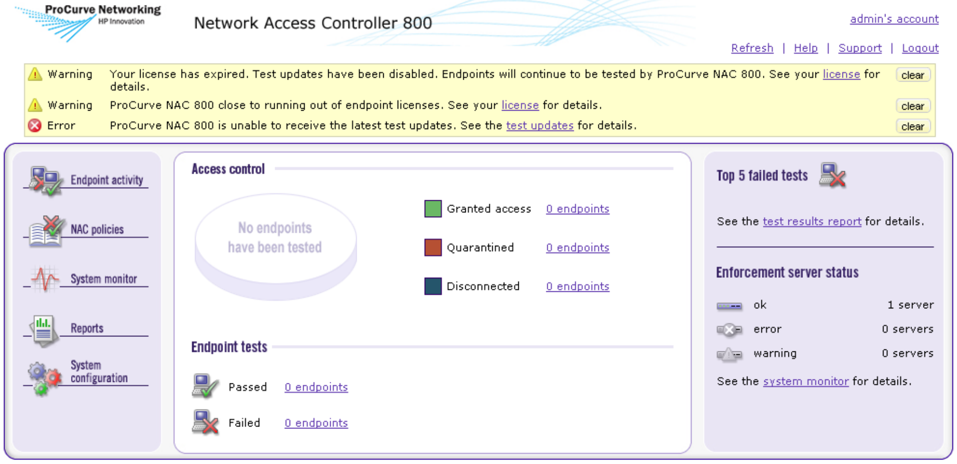
* User name: admin

* Password: ●●●●●●●●●●●

* Re-enter password: ●●●●●●●●●●●

© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30187

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



Warning Your license has expired. Test updates have been disabled. Endpoints will continue to be tested by ProCurve NAC 800. See your license for details.

Warning ProCurve NAC 800 close to running out of endpoint licenses. See your license for details.

Error ProCurve NAC 800 is unable to receive the latest test updates. See the test updates for details.

Access control

🟩	Granted access	0 endpoints
🟥	Quarantined	0 endpoints
■	Disconnected	0 endpoints

Endpoint tests

Passed	0 endpoints
Failed	0 endpoints

Top 5 failed tests

See the test results report for details.

Enforcement server status

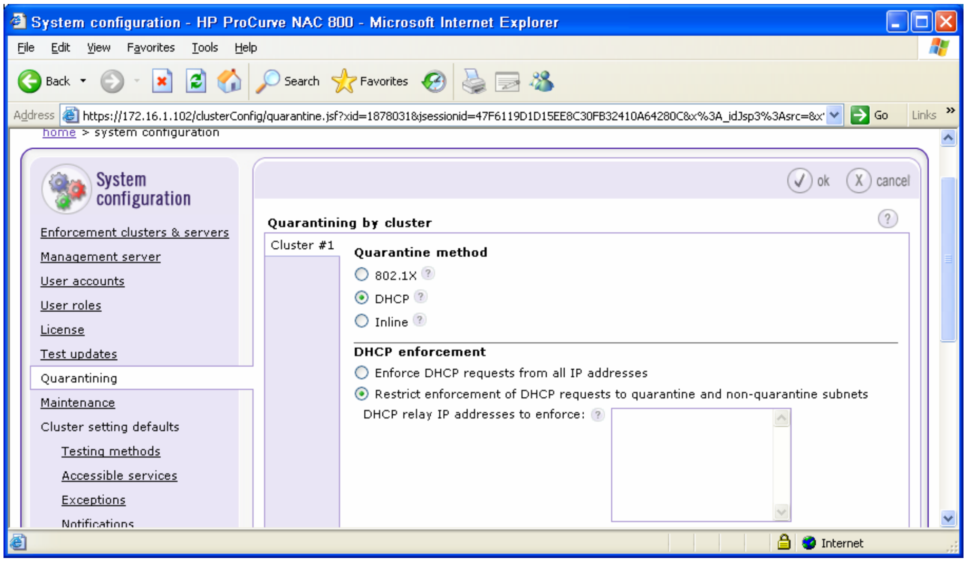
ok	1 server
error	0 servers
warning	0 servers

See the system monitor for details.

Figure 1 – NAC 800 Web Console Home Page

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

7. Click **System Configuration**.



System configuration - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/clusterConfig/quarantine.jsf?xid=1878031&jsessionid=47F6119D1D15EE8C30FB32410A64280C&x%3A_idJsp3%3Asrc=&x'
Go Links
home > system configuration
System configuration
Enforcement clusters & servers
Management server
User accounts
User roles
License
Test updates
Quarantining
Maintenance
Cluster setting defaults
Testing methods
Accessible services
Exceptions
Notifications
ok
cancel
Internet

Quarantining by cluster

Cluster #1

Quarantine method

○ 802.1X

● DHCP

○ Inline

DHCP enforcement

○ Enforce DHCP requests from all IP addresses

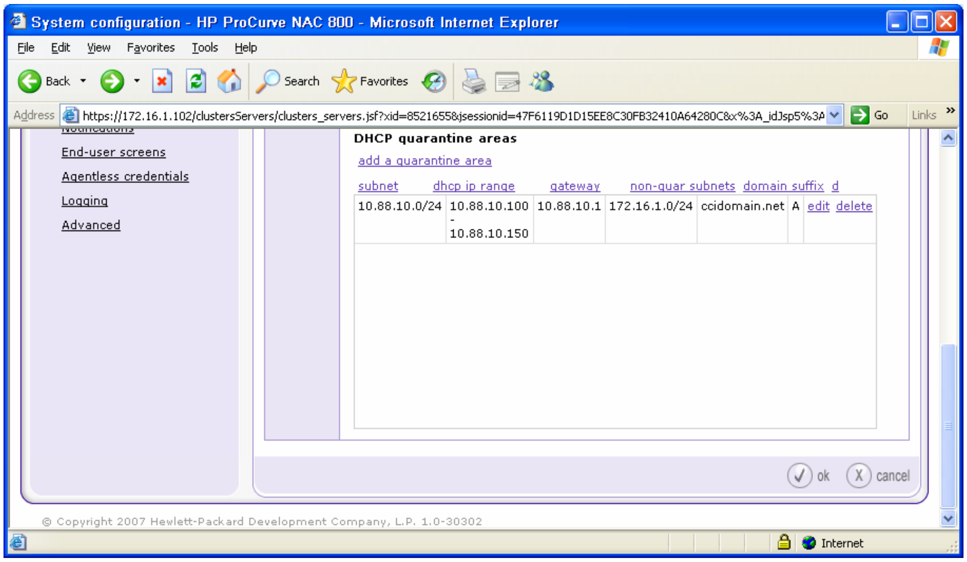
● Restrict enforcement of DHCP requests to quarantine and non-quarantine subnets

DHCP relay IP addresses to enforce:

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**.



System configuration - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/clustersServers/clusters_servers.jsf?xid=8521655&jsessionid=47F6119D1D15EE8C30FB32410A64280C&x%3A_idJsp5%3A
Go Links
End-user screens
Agentless credentials
Logging
Advanced
ok
cancel
© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30302
Internet

DHCP quarantine areas

add a quarantine area

subnet	dhcp ip range	gateway	non-quar subnets	domain suffix	d	
10.88.10.0/24	10.88.10.100 - 10.88.10.150	10.88.10.1	172.16.1.0/24	ccidomain.net	A	edit delete

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

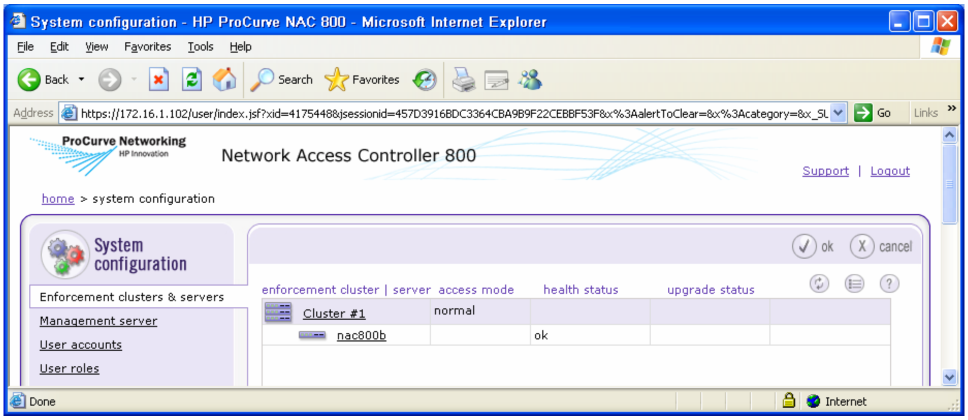
As we are focusing on the integration of NAC into a CCI and thin client *network*, we are exploring only the network policy enforcement settings that are pertinent to thin clients and blade PCs. This is by no means all the features of the ProCurve NAC Solution. Likewise, in a production environment, 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**.



https://172.16.1.102/user/index.jsf?xid=4175448&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3AalertToClear=&x%3Acategory=&x_SL

enforcement cluster | server	access mode	health status	upgrade status
Cluster #1	normal		
nac800b		ok	

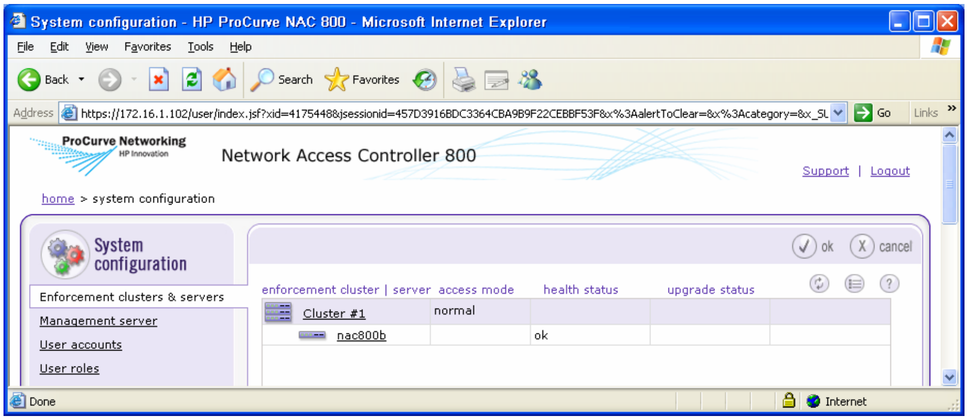
Quarantine and Remediation

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**.


System configuration - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address Go Links
ProCurve Networking
HP Innovation
Done
Internet

Address: https://172.16.1.102/user/index.jsf?xid=4175448&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3AalertToClear=&x%3Acategory=&x_SL

Network Access Controller 800

Support | Logout

home > system configuration

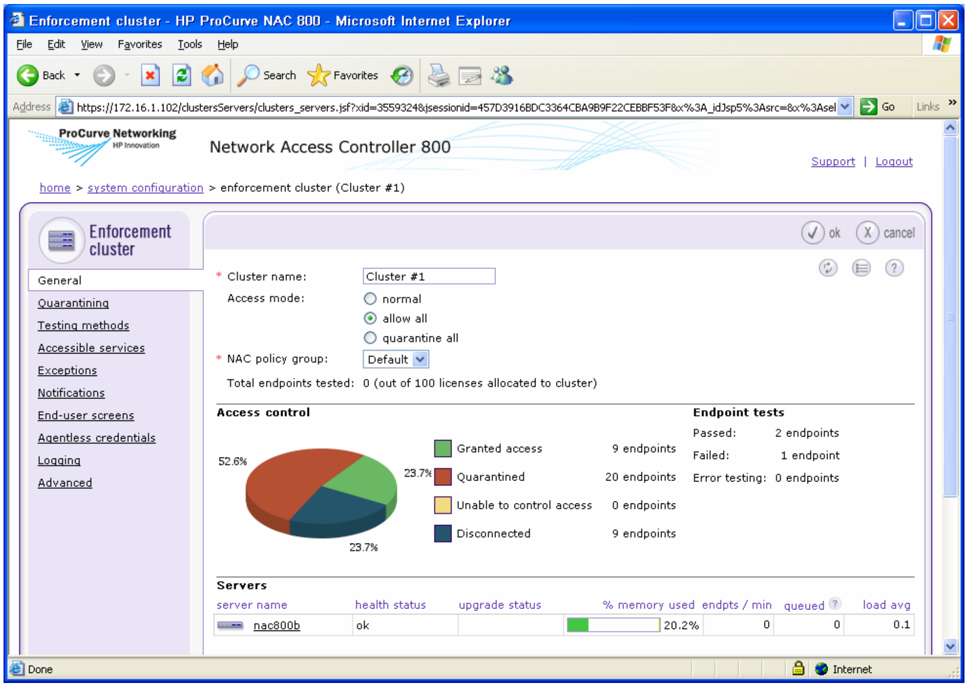
System configuration

- Enforcement clusters & servers
- Management server
- User accounts
- User roles

ok cancel

enforcement cluster | server	access mode	health status	upgrade status
Cluster #1	normal		
nac800b		ok	

2. Click **Cluster #1**.


Enforcement cluster - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address Go Links
ProCurve Networking
HP Innovation
52.6%
23.7%
23.7%
Done
Internet

Address: https://172.16.1.102/clustersServers/clusters_servers.jsf?xid=3559324&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3A_idJsp5%3Asrc=&x%3Asel

Network Access Controller 800

Support | Logout

home > system configuration > enforcement cluster (Cluster #1)

Enforcement cluster

- General
- Quarantining
- Testing methods
- Accessible services
- Exceptions
- Notifications
- End-user screens
- Agentless credentials
- Logging
- Advanced

ok cancel

* Cluster name: Cluster #1

Access mode: ○ normal ● allow all ○ quarantine all

* NAC policy group: Default

Total endpoints tested: 0 (out of 100 licenses allocated to cluster)

Access control

🟩	Granted access	9 endpoints
🟥	Quarantined	20 endpoints
🟨	Unable to control access	0 endpoints
🟦	Disconnected	9 endpoints

Endpoint tests

Passed:	2 endpoints
Failed:	1 endpoint
Error testing:	0 endpoints

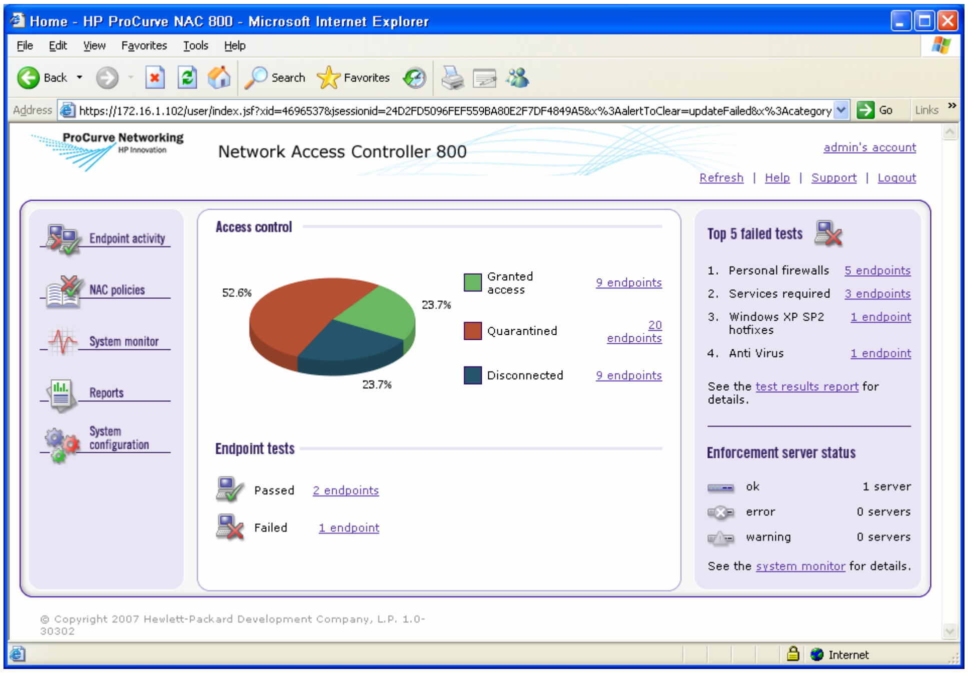
Servers

server name	health status	upgrade status	% memory used	endpts / min	queued	load avg
nac800b	ok		20.2%	0	0	0.1

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).


Home - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/user/index.jsf?xid=469653&jsessionid=24D2FD5096FEF559BA80E2F7DF4849A5&x%3AalertToClear=updateFailed&x%3Acategory
Go Links
ProCurve Networking
HP Innovation
Network Access Controller 800
admin's account
Refresh | Help | Support | Logout
Endpoint activity
NAC policies
System monitor
Reports
System configuration
52.6%
23.7%
23.7%
Internet

Access control

🟩 Granted access	9 endpoints
🟥 Quarantined	20 endpoints
🟦 Disconnected	9 endpoints

Endpoint tests

Passed	2 endpoints
Failed	1 endpoint

Top 5 failed tests

1.	Personal firewalls	5 endpoints
2.	Services required	3 endpoints
3.	Windows XP SP2 hotfixes	1 endpoint
4.	Anti Virus	1 endpoint

See the test results report for details.

Enforcement server status

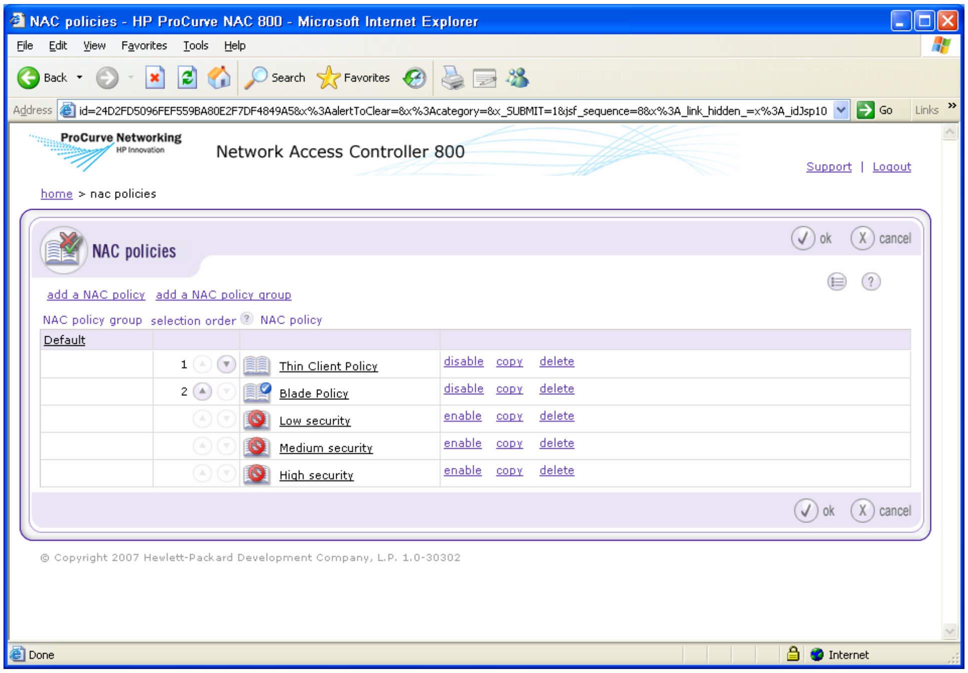
ok	1 server
error	0 servers
warning	0 servers

See the system monitor for details.

© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30302

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

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


NAC policies - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address id=24D2FD5096FEF559BA80E2F7DF4849A5&x%3AalertToClear=&x%3Acategory=&x_SUBMIT=1&jsf_sequence=8&x%3A_link_hidden_=x%3A_idJsp10
Go Links
ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > nac policies
ok cancel
Done
Internet

NAC policies

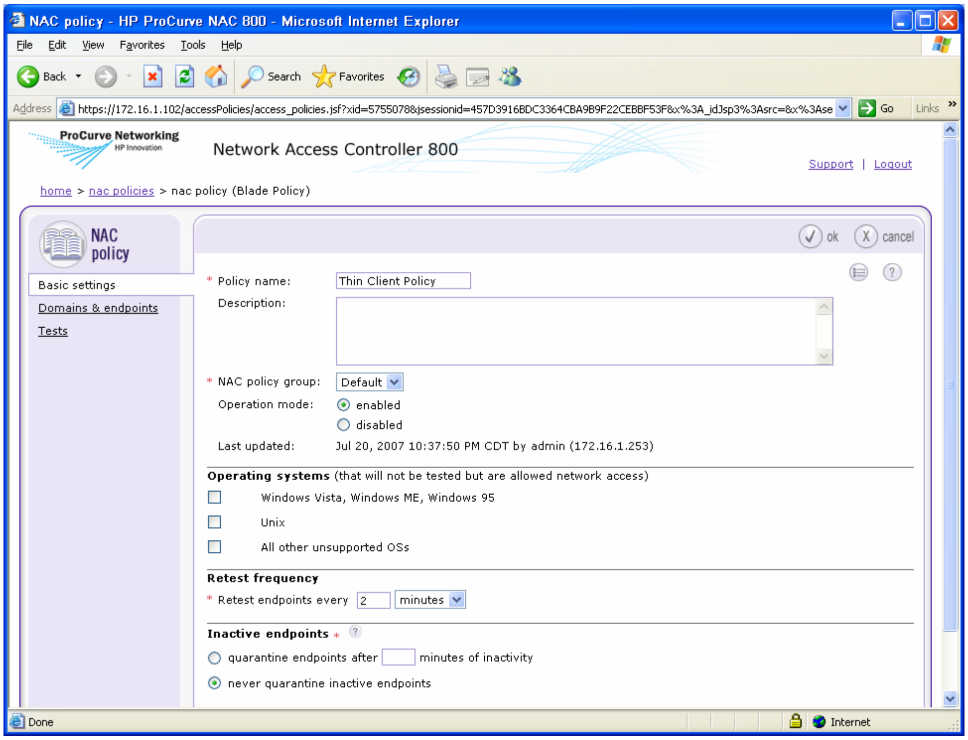
add a NAC policy add a NAC policy group

NAC policy group	selection order	NAC policy	
Default			
	1	Thin Client Policy	disable copy delete
	2	Blade Policy	disable copy delete
		Low security	enable copy delete
		Medium security	enable copy delete
		High security	enable copy delete

© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30302

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**.


NAC policy - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/accessPolicies/access_policies.jsf?xid=5755078&jsessionid=457D3916BDC3364CBA9BF22CEBBF53F8&x%3A_idJsp3%3Asrc=&x%3Ase
Go Links
ProCurve Networking HP Innovation
Network Access Controller 800
Support | Logout

home > nac policies > nac policy (Blade Policy)

NAC policy
Basic settings
Domains & endpoints
Tests
ok cancel

* Policy name: Thin Client Policy

Description:

* NAC policy group: Default

Operation mode: ● enabled ○ disabled

Last updated: Jul 20, 2007 10:37:50 PM CDT by admin (172.16.1.253)

Operating systems (that will not be tested but are allowed network access)

□ Windows Vista, Windows ME, Windows 95

□ Unix

□ All other unsupported OSs

Retest frequency

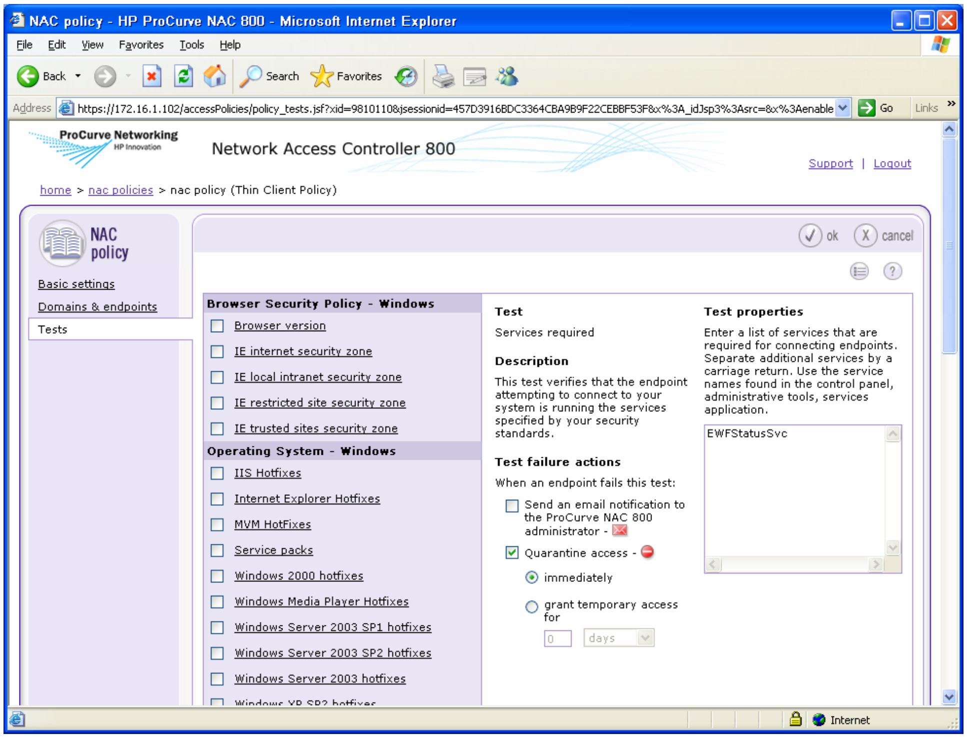
* Retest endpoints every 2 minutes

Inactive endpoints *

○ quarantine endpoints after minutes of inactivity

● 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.


NAC policy - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/accessPolicies/policy_tests.jsf?xid=981011&jsessionid=457D3916BDC3364CBA9BF22CEBBF53F8&x%3A_idJsp3%3Asrc=&x%3Aenable
Go Links
ProCurve Networking HP Innovation
Network Access Controller 800
Support | Logout

home > nac policies > nac policy (Thin Client Policy)

NAC policy
Basic settings
Domains & endpoints
Tests
ok cancel

Browser Security Policy - Windows

□ Browser version

□ IE internet security zone

□ IE local intranet security zone

□ IE restricted site security zone

□ IE trusted sites security zone

Operating System - Windows

□ IIS Hotfixes

□ Internet Explorer Hotfixes

□ MVM HotFixes

□ Service packs

□ Windows 2000 hotfixes

□ Windows Media Player Hotfixes

□ Windows Server 2003 SP1 hotfixes

□ Windows Server 2003 SP2 hotfixes

□ Windows Server 2003 hotfixes

□ Windows XP SP2 hotfixes

Test

Services required

Description

This test verifies that the endpoint attempting to connect to your system is running the services specified by your security standards.

Test failure actions

When an endpoint fails this test:

□ Send an email notification to the ProCurve NAC 800 administrator -

☑ Quarantine access -

● immediately

○ grant temporary access for 0 days

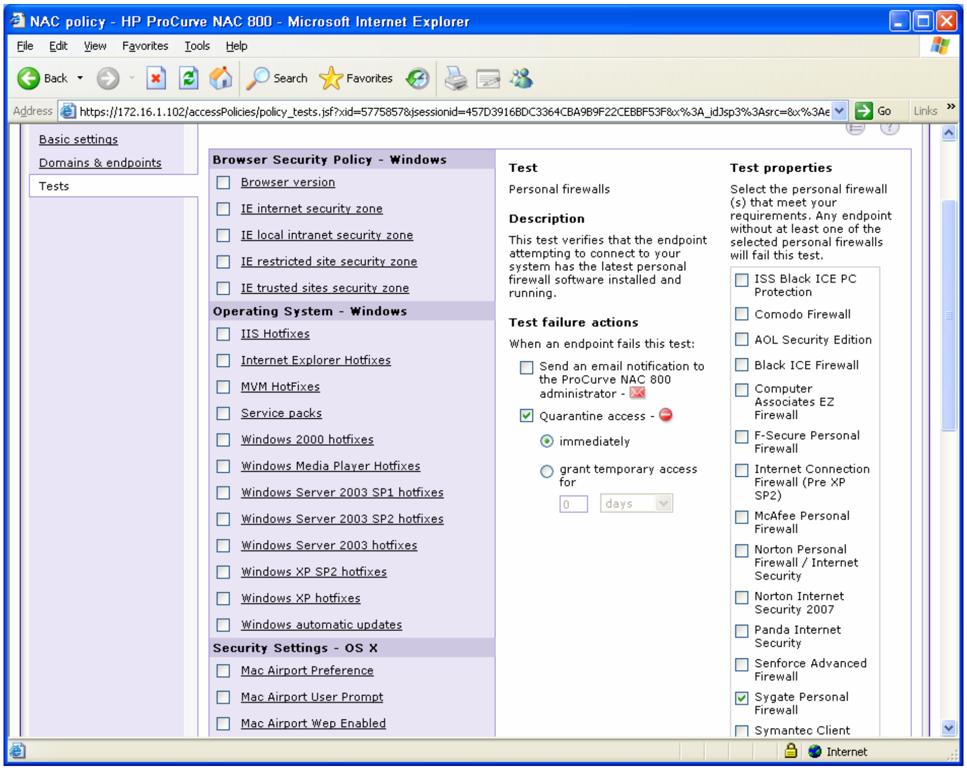
Test properties

Enter a list of services that are required for connecting endpoints. Separate additional services by a carriage return. Use the service names found in the control panel, administrative tools, services application.

EWFStatusSvc

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**.


NAC policy - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/accessPolicies/policy_tests.jsf?xid=5775857&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3A_idJsp3%3Asrc=&x%3Ae
Go Links
Internet

Basic settings
Domains & endpoints
Tests

Browser Security Policy - Windows
- □ Browser version
- □ IE internet security zone
- □ IE local intranet security zone
- □ IE restricted site security zone
- □ IE trusted sites security zone

Operating System - Windows
- □ IIS Hotfixes
- □ Internet Explorer Hotfixes
- □ MVM HotFixes
- □ Service packs
- □ Windows 2000 hotfixes
- □ Windows Media Player Hotfixes
- □ Windows Server 2003 SP1 hotfixes
- □ Windows Server 2003 SP2 hotfixes
- □ Windows Server 2003 hotfixes
- □ Windows XP SP2 hotfixes
- □ Windows XP hotfixes
- □ Windows automatic updates

Security Settings - OS X
- □ Mac Airport Preference
- □ Mac Airport User Prompt
- □ Mac Airport Wep Enabled

Test

Personal firewalls

Description

This test verifies that the endpoint attempting to connect to your system has the latest personal firewall software installed and running.

Test failure actions

When an endpoint fails this test:

- □ Send an email notification to the ProCurve NAC 800 administrator -
- ☑ Quarantine access -
  - ● immediately
  - ○ grant temporary access for 0 days

Test properties

Select the personal firewall (s) that meet your requirements. Any endpoint without at least one of the selected personal firewalls will fail this test.

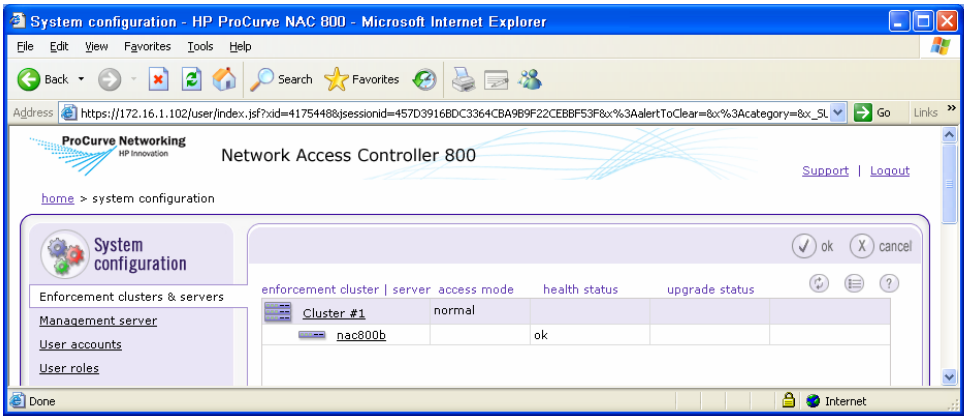
- □ ISS Black ICE PC Protection
- □ Comodo Firewall
- □ AOL Security Edition
- □ Black ICE Firewall
- □ Computer Associates EZ Firewall
- □ F-Secure Personal Firewall
- □ Internet Connection Firewall (Pre XP SP2)
- □ McAfee Personal Firewall
- □ Norton Personal Firewall / Internet Security
- □ Norton Internet Security 2007
- □ Panda Internet Security
- □ Senforce Advanced Firewall
- ☑ Sygate Personal Firewall
- □ Symantec Client

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**.


System configuration - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/user/index.jsf?xid=417544&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3AalertToClear=&x%3Acategory=&x_SL
Go Links
ProCurve Networking
HP Innovation
Support | Logout
ok
cancel
Done
Internet

Network Access Controller 800

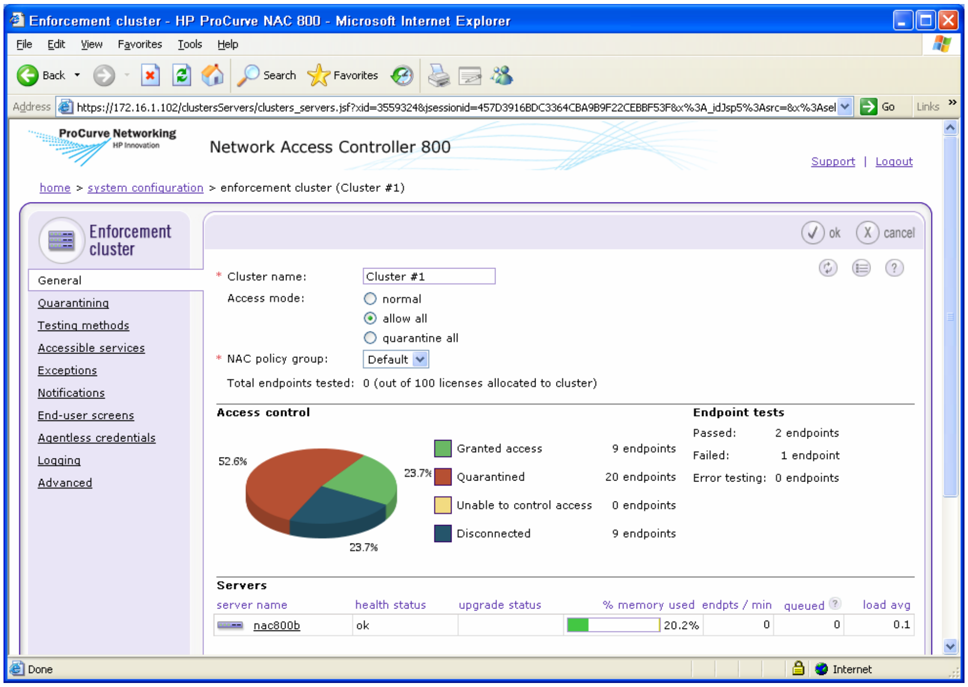
home > system configuration

System configuration

Enforcement clusters & servers
Management server
User accounts
User roles

enforcement cluster | server	access mode	health status	upgrade status
Cluster #1	normal		
nac800b		ok	

2. Click **Cluster #1**.


Enforcement cluster - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/clustersServers/clusters_servers.jsf?xid=3559324&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3A_idJsp5%3Asrc=&x%3Asel
Go Links
ProCurve Networking HP Innovation
Network Access Controller 800
Support | Logout
ok cancel
Done
Internet

home > system configuration > enforcement cluster (Cluster #1)

Enforcement cluster

General
Quarantining
Testing methods
Accessible services
Exceptions
Notifications
End-user screens
Agentless credentials
Logging
Advanced

* Cluster name: Cluster #1

Access mode: ○ normal ● allow all ○ quarantine all

* NAC policy group: Default

Total endpoints tested: 0 (out of 100 licenses allocated to cluster)

Access control

🟩	Granted access	9 endpoints
🟥	Quarantined	20 endpoints
🟨	Unable to control access	0 endpoints
■	Disconnected	9 endpoints

Endpoint tests

Passed:	2 endpoints
Failed:	1 endpoint
Error testing:	0 endpoints

Servers

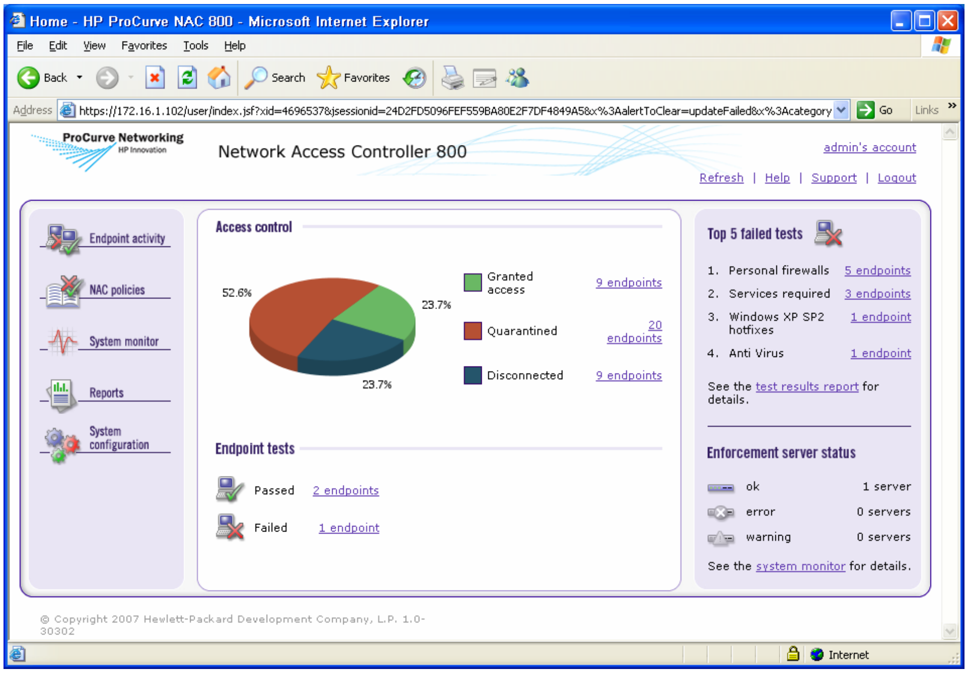
server name	health status	upgrade status	% memory used	endpts / min	queued	load avg
nac800b	ok		20.2%	0	0	0.1

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.

5. On the Domain Controller, open the Web console at https://172.16.1.102/ in your Web browser.


Home - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/user/index.jsf?xid=4696537&jsessionid=24D2FD5096FEF559BA80E2F7DF4849A5&x%3AalertToClear=updateFailed&x%3Acategory
Go Links
ProCurve Networking HP Innovation
Network Access Controller 800
admin's account
Refresh | Help | Support | Logout
Endpoint activity
NAC policies
System monitor
Reports
System configuration
Internet

Access control

🟩	Granted access	9 endpoints
🟥	Quarantined	20 endpoints
■	Disconnected	9 endpoints

Endpoint tests

Passed	2 endpoints
Failed	1 endpoint

Top 5 failed tests

1.	Personal firewalls	5 endpoints
2.	Services required	3 endpoints
3.	Windows XP SP2 hotfixes	1 endpoint
4.	Anti Virus	1 endpoint

See the test results report for details.

Enforcement server status

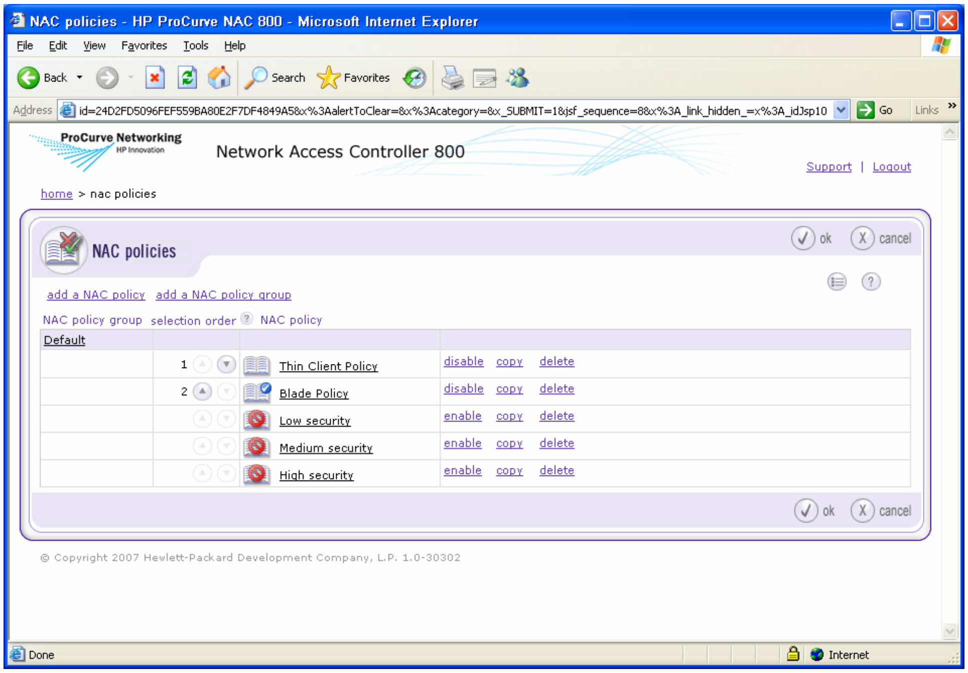
ok	1 server
error	0 servers
warning	0 servers

See the system monitor for details.

© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30302

6. Login to the Web console to access the home screen.

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


NAC policies - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address id=24D2FD5096FEF559BA80E2F7DF4849A58x%3AalertToClear=&x%3Acategory=&x_SUBMIT=1&jsf_sequence=8&x%3A_link_hidden_=x%3A_idJsp10
Go Links
ProCurve Networking
HP Innovation
Done
Internet

Network Access Controller 800

Support | Logout

home > nac policies

NAC policies

ok cancel

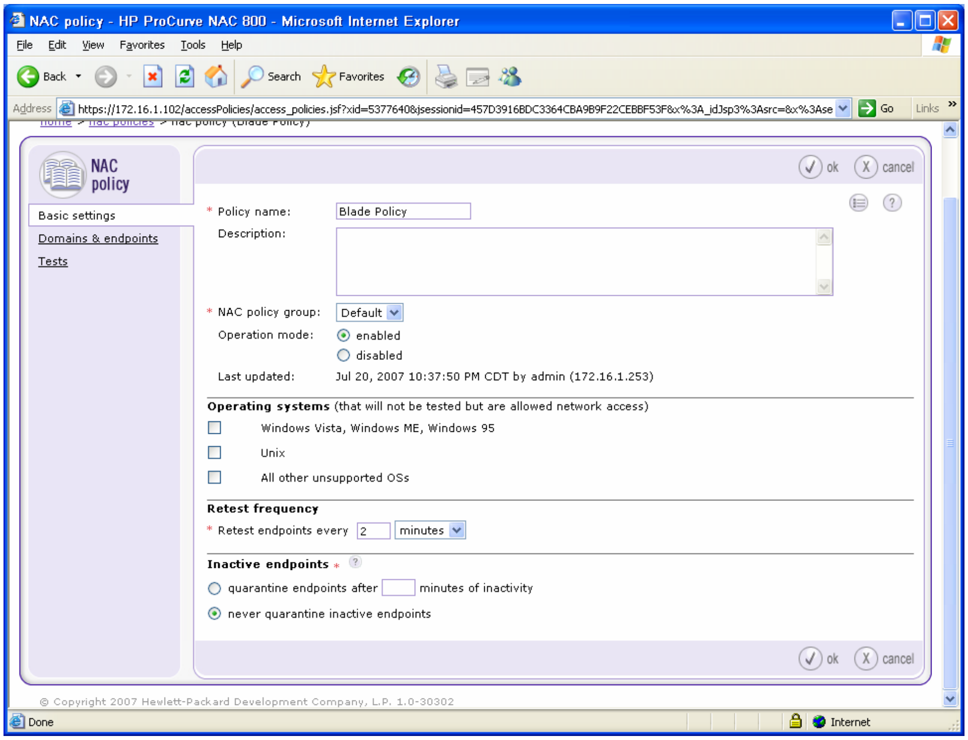
add a NAC policy add a NAC policy group

NAC policy group	selection order	NAC policy	
Default			
	1	Thin Client Policy	disable copy delete
	2	Blade Policy	disable copy delete
		Low security	enable copy delete
		Medium security	enable copy delete
		High security	enable copy delete

ok cancel

© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30302

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**.


NAC policy - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/accessPolicies/access_policies.jsf?xid=5377640&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3A_idJsp3%3Asrc=&x%3Ase
Go Links
Done
Internet

home > nac policies > nac policy (Blade Policy)

NAC policy

Basic settings
Domains & endpoints
Tests

ok cancel

* Policy name: Blade Policy

Description:

* NAC policy group: Default

Operation mode: ● enabled ○ disabled

Last updated: Jul 20, 2007 10:37:50 PM CDT by admin (172.16.1.253)

Operating systems (that will not be tested but are allowed network access)

□ Windows Vista, Windows ME, Windows 95

□ Unix

□ All other unsupported OSs

Retest frequency

* Retest endpoints every 2 minutes

Inactive endpoints *

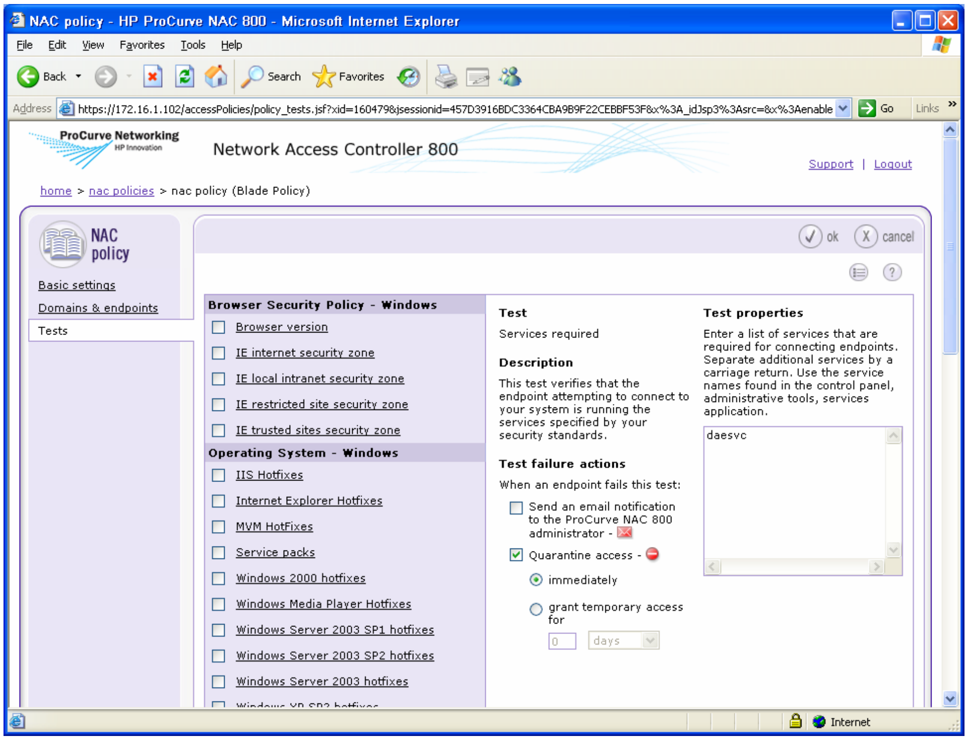
○ quarantine endpoints after minutes of inactivity

● never quarantine inactive endpoints

ok cancel

© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30302

14. Select **Tests** from the left navigation bar. The **Tests** page is where tests are put in place for this particular policy.


NAC policy - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/accessPolicies/policy_tests.jsf?xid=160479&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3A_idJsp3%3Asrc=&x%3Aenable
Go Links
ProCurve Networking HP Innovation
Network Access Controller 800
Support | Logout
home > nac policies > nac policy (Blade Policy)
NAC policy
Basic settings
Domains & endpoints
Tests
ok cancel
Internet

Browser Security Policy - Windows

- □ Browser version
- □ IE internet security zone
- □ IE local intranet security zone
- □ IE restricted site security zone
- □ IE trusted sites security zone

Operating System - Windows

- □ IIS Hotfixes
- □ Internet Explorer Hotfixes
- □ MVM HotFixes
- □ Service packs
- □ Windows 2000 hotfixes
- □ Windows Media Player Hotfixes
- □ Windows Server 2003 SP1 hotfixes
- □ Windows Server 2003 SP2 hotfixes
- □ Windows Server 2003 hotfixes
- □ Windows XP SP2 hotfixes

Test

Services required

Description

This test verifies that the endpoint attempting to connect to your system is running the services specified by your security standards.

Test failure actions

When an endpoint fails this test:

□ Send an email notification to the ProCurve NAC 800 administrator

☑ Quarantine access -

● immediately

○ grant temporary access for 0 days

Test properties

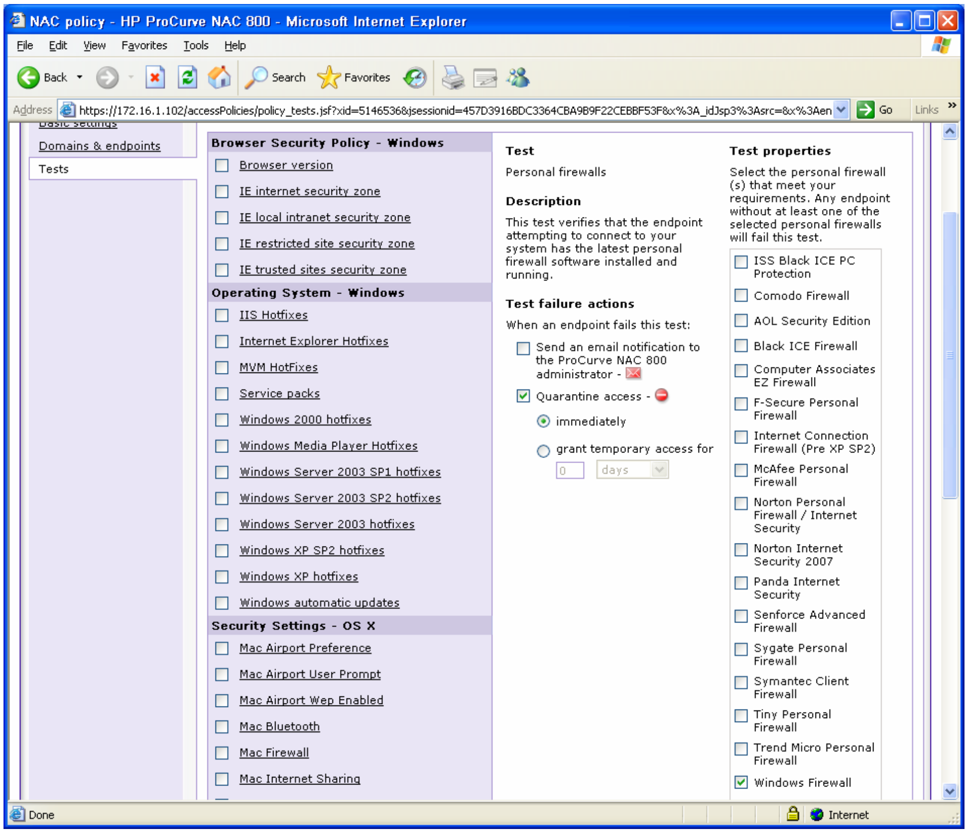
Enter a list of services that are required for connecting endpoints. Separate additional services by a carriage return. Use the service names found in the control panel, administrative tools, services application.

daesvc

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**.


NAC policy - HP ProCurve NAC 800 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.16.1.102/accessPolicies/policy_tests.jsf?xid=5146536&jsessionid=457D3916BDC3364CBA9B9F22CEBBF53F&x%3A_idJsp3%3Asrc=&x%3Aen
Go Links
Basic settings
Domains & endpoints
Tests
Done
Internet

Browser Security Policy - Windows

- □ Browser version
- □ IE internet security zone
- □ IE local intranet security zone
- □ IE restricted site security zone
- □ IE trusted sites security zone

Operating System - Windows

- □ IIS Hotfixes
- □ Internet Explorer Hotfixes
- □ MVM HotFixes
- □ Service packs
- □ Windows 2000 hotfixes
- □ Windows Media Player Hotfixes
- □ Windows Server 2003 SP1 hotfixes
- □ Windows Server 2003 SP2 hotfixes
- □ Windows Server 2003 hotfixes
- □ Windows XP SP2 hotfixes
- □ Windows XP hotfixes
- □ Windows automatic updates

Security Settings - OS X

- □ Mac Airport Preference
- □ Mac Airport User Prompt
- □ Mac Airport Wep Enabled
- □ Mac Bluetooth
- □ Mac Firewall
- □ Mac Internet Sharing

Test

Personal firewalls

Description

This test verifies that the endpoint attempting to connect to your system has the latest personal firewall software installed and running.

Test failure actions

When an endpoint fails this test:

□ Send an email notification to the ProCurve NAC 800 administrator

☑ Quarantine access -

● immediately

○ grant temporary access for 0 days

Test properties

Select the personal firewall (s) that meet your requirements. Any endpoint without at least one of the selected personal firewalls will fail this test.

- □ ISS Black ICE PC Protection
- □ Comodo Firewall
- □ AOL Security Edition
- □ Black ICE Firewall
- □ Computer Associates EZ Firewall
- □ F-Secure Personal Firewall
- □ Internet Connection Firewall (Pre XP SP2)
- □ McAfee Personal Firewall
- □ Norton Personal Firewall / Internet Security
- □ Norton Internet Security 2007
- □ Panda Internet Security
- □ Senforce Advanced Firewall
- □ Sygate Personal Firewall
- □ Symantec Client Firewall
- □ Tiny Personal Firewall
- □ Trend Micro Personal Firewall
- ☑ Windows Firewall

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

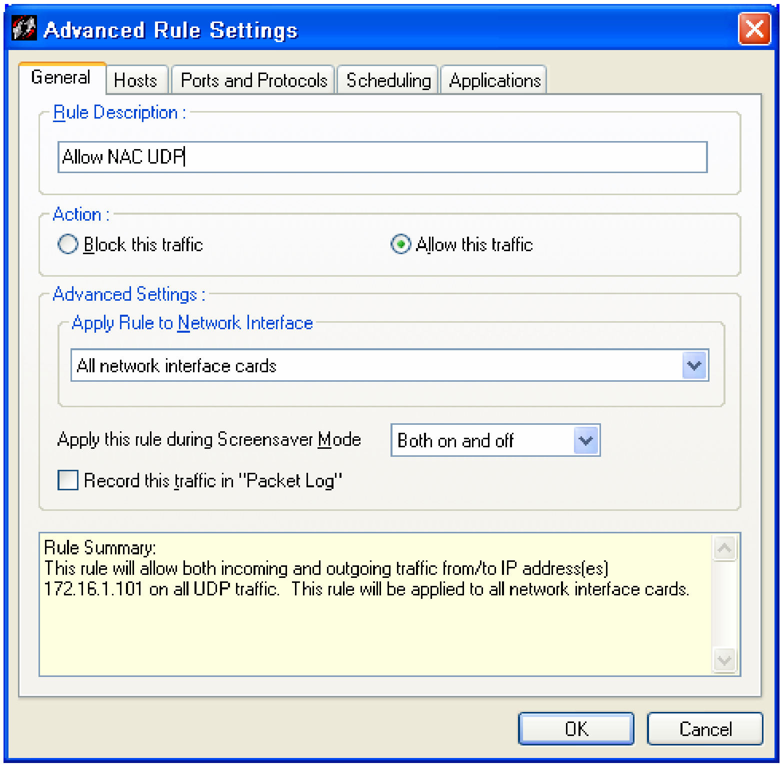
Thin Client Firewall Exceptions

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:

Description	IP Address	Remote Ports	Local Ports	Incoming/Outgoing
Allow NAC UDP	172.16.1.101		137, 1500	Both
Allow NAC TCP In	172.16.1.101		139, 1500	Incoming
Allow NAC TCP Out	172.16.1.101	89		Outgoing

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**.



Rule Description : Allow NAC UDP

Action : ○ Block this traffic ● Allow this traffic

Advanced Settings :

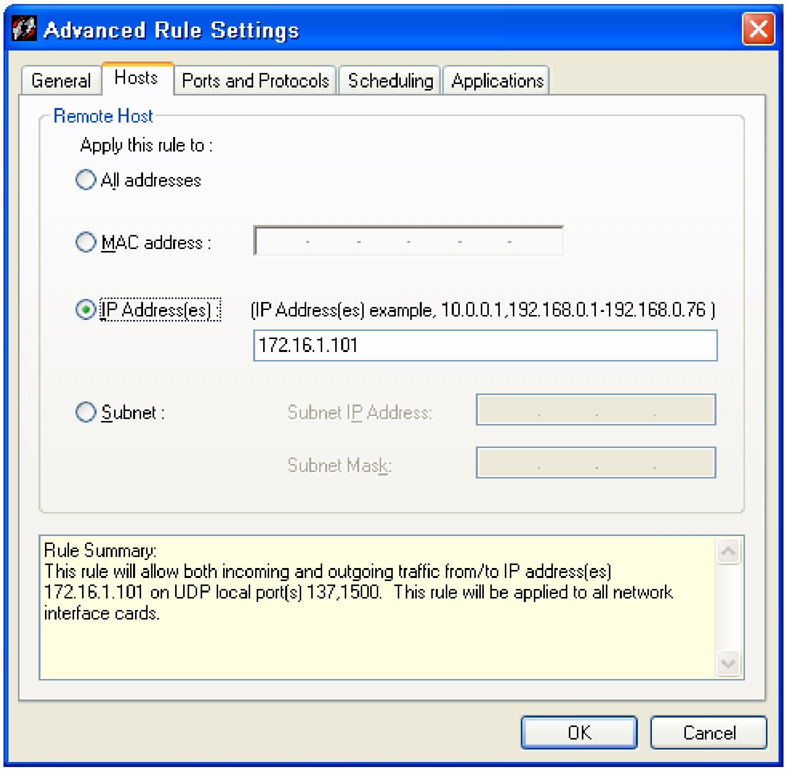
Apply Rule to Network Interface: All network interface cards

Apply this rule during Screensaver Mode: Both on and off

☐ Record this traffic in "Packet Log"

Rule Summary:
This rule will allow both incoming and outgoing traffic from/to IP address(es) 172.16.1.101 on all UDP traffic. This rule will be applied to all network interface cards.

8. On the **Hosts** tab, select **IP Addresses**, and then type the IP address of the NAC800 (`172.16.1.101`) in the field.



Apply this rule to :

○ All addresses

○ MAC address :

● IP Address(es) : (IP Address(es) example, 10.0.0.1,192.168.0.1-192.168.0.76)

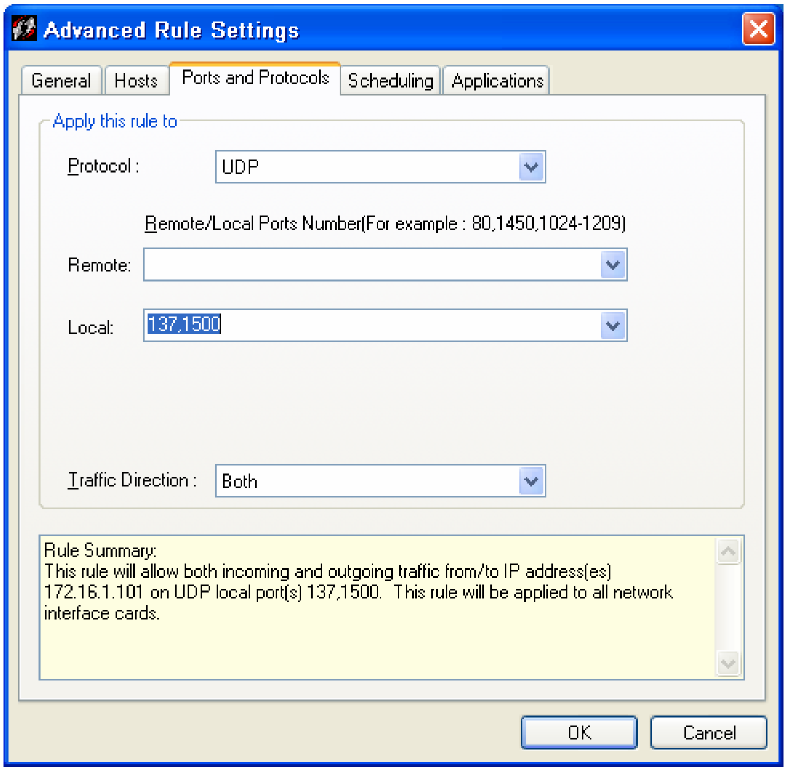
172.16.1.101

○ Subnet : Subnet IP Address: Subnet Mask:

Rule Summary:
This rule will allow both incoming and outgoing traffic from/to IP address(es) 172.16.1.101 on UDP local port(s) 137,1500. This rule will be applied to all network interface cards.

9. On the **Ports and Protocols** tab in the **Protocol** list, select **UDP**.

10. Type `137, 1500` in the **Local** field.



Protocol : UDP

Remote/Local Ports Number(For example : 80,1450,1024-1209)

Remote:

Local: 137,1500

Traffic Direction : Both

Rule Summary:
This rule will allow both incoming and outgoing traffic from/to IP address(es) 172.16.1.101 on UDP local port(s) 137,1500. This rule will be applied to all network interface cards.

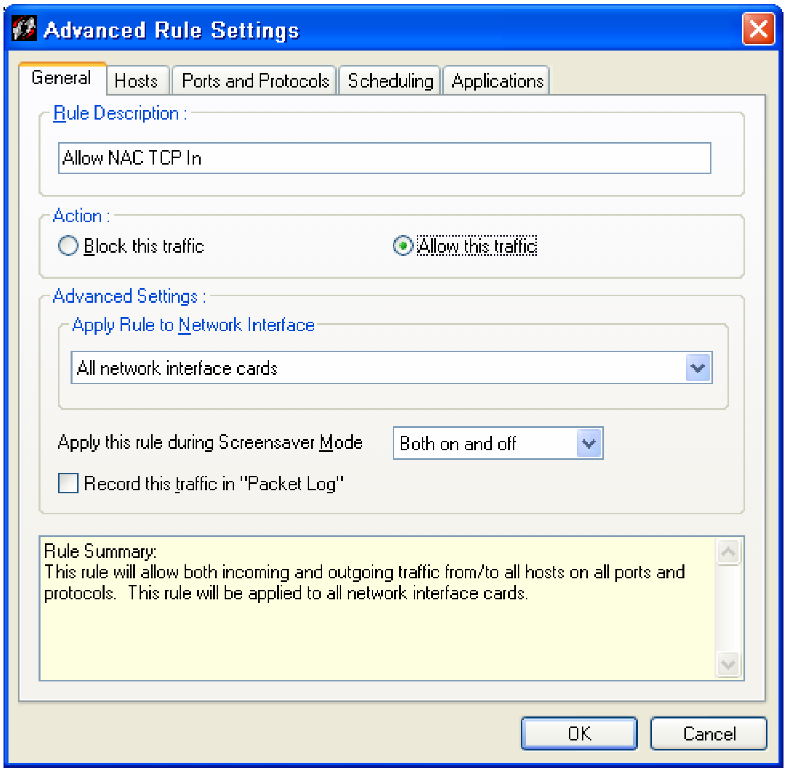
11. In the **Traffic Direction** list, select **Both**.

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**.



Rule Description : Allow NAC TCP In

Action : ○ Block this traffic ● Allow this traffic

Advanced Settings :

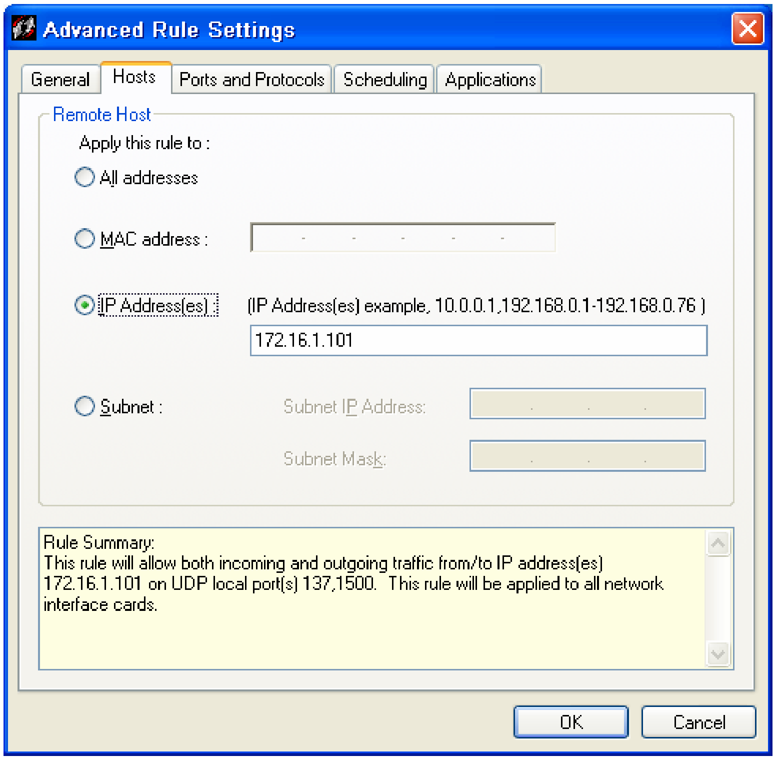
Apply Rule to Network Interface: All network interface cards

Apply this rule during Screensaver Mode: Both on and off

□ Record this traffic in "Packet Log"

Rule Summary:
This rule will allow both incoming and outgoing traffic from/to all hosts on all ports and protocols. This rule will be applied to all network interface cards.

16. In the **Hosts** tab, select **IP Addresses** and then type the IP address of the NAC800 (`172.16.1.101`) in the field.



Remote Host

Apply this rule to :

○ All addresses

○ MAC address :

● IP Address(es) : (IP Address(es) example, 10.0.0.1,192.168.0.1-192.168.0.76)

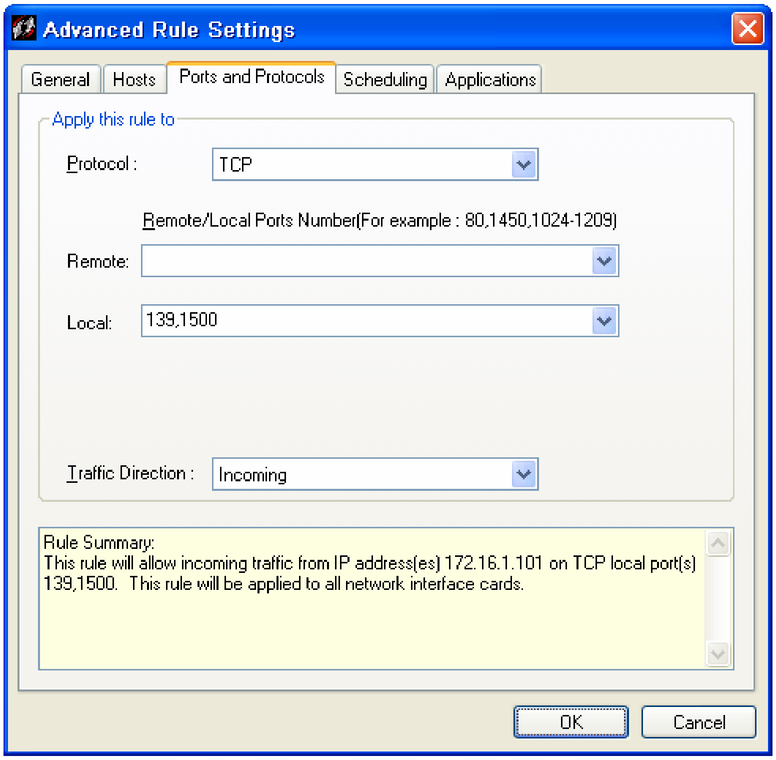
172.16.1.101

○ Subnet : Subnet IP Address: Subnet Mask:

Rule Summary:
This rule will allow both incoming and outgoing traffic from/to IP address(es) 172.16.1.101 on UDP local port(s) 137,1500. This rule will be applied to all network interface cards.

17. In the **Ports and Protocols,** select **TCP** in the **Protocol** field.

18. Type `139, 1500` in the **Local** field.



Protocol : TCP

Remote/Local Ports Number(For example : 80,1450,1024-1209)

Remote:

Local: 139,1500

Traffic Direction : Incoming

Rule Summary:
This rule will allow incoming traffic from IP address(es) 172.16.1.101 on TCP local port(s) 139,1500. This rule will be applied to all network interface cards.

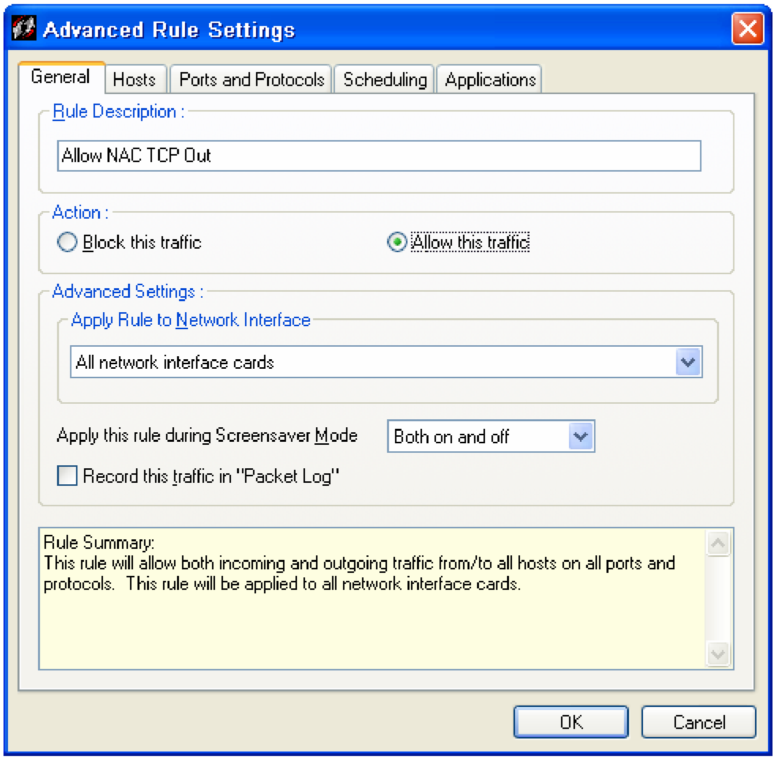
19. Select **Incoming** in the **Traffic Direction** field.

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**.



Rule Description : Allow NAC TCP Out

○ Block this traffic ● Allow this traffic

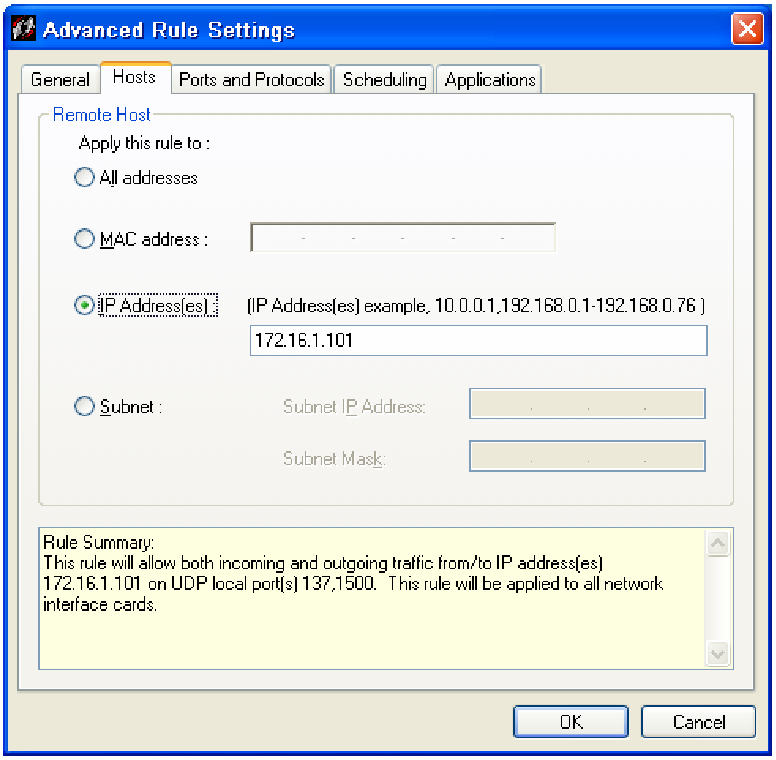
All network interface cards

Apply this rule during Screensaver Mode: Both on and off

□ Record this traffic in "Packet Log"

Rule Summary:
This rule will allow both incoming and outgoing traffic from/to all hosts on all ports and protocols. This rule will be applied to all network interface cards.

24. On the **Hosts** tab, select **IP Addresses** and type the IP address of the NAC800 (`172.16.1.101`) in the field.



Remote Host

Apply this rule to :

○ All addresses

○ MAC address :

● IP Address(es) : (IP Address(es) example, 10.0.0.1,192.168.0.1-192.168.0.76)

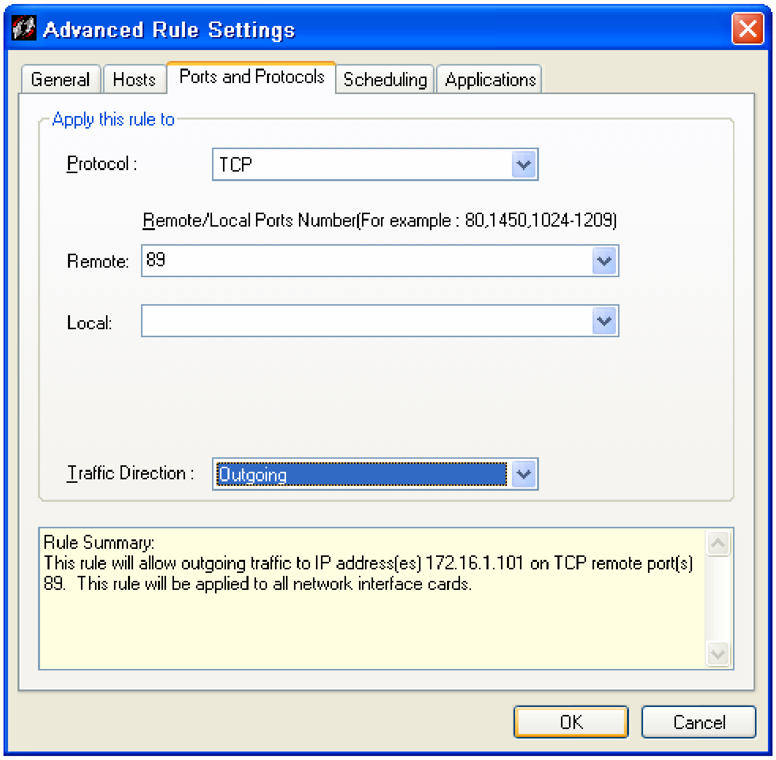
172.16.1.101

○ Subnet : Subnet IP Address: Subnet Mask:

Rule Summary:
This rule will allow both incoming and outgoing traffic from/to IP address(es) 172.16.1.101 on UDP local port(s) 137,1500. This rule will be applied to all network interface cards.

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

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



Apply this rule to

Protocol : TCP

Remote/Local Ports Number(For example : 80,1450,1024-1209)

Remote: 89

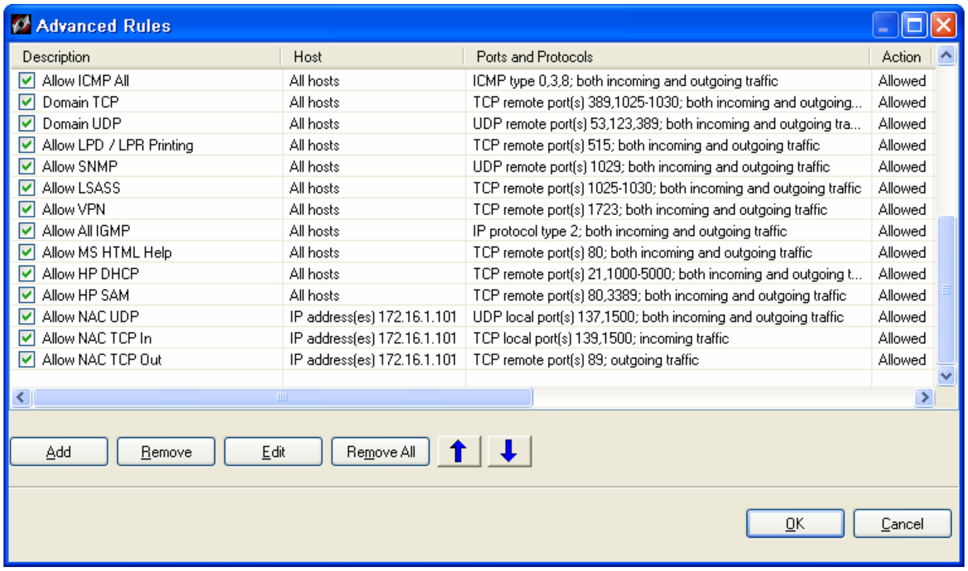
Local:

Traffic Direction : Outgoing

Rule Summary:
This rule will allow outgoing traffic to IP address(es) 172.16.1.101 on TCP remote port(s) 89. This rule will be applied to all network interface cards.

27. Select **Outgoing** in the **Traffic Direction** field.

28. Click **OK**.



Description	Host	Ports and Protocols	Action
☑ Allow ICMP All	All hosts	ICMP type 0,3,8; both incoming and outgoing traffic	Allowed
☑ Domain TCP	All hosts	TCP remote port(s) 389,1025-1030; both incoming and outgoing...	Allowed
☑ Domain UDP	All hosts	UDP remote port(s) 53,123,389; both incoming and outgoing tra...	Allowed
☑ Allow LPD / LPR Printing	All hosts	TCP remote port(s) 515; both incoming and outgoing traffic	Allowed
☑ Allow SNMP	All hosts	UDP remote port(s) 1029; both incoming and outgoing traffic	Allowed
☑ Allow LSASS	All hosts	TCP remote port(s) 1025-1030; both incoming and outgoing traffic	Allowed
☑ Allow VPN	All hosts	TCP remote port(s) 1723; both incoming and outgoing traffic	Allowed
☑ Allow All IGMP	All hosts	IP protocol type 2; both incoming and outgoing traffic	Allowed
☑ Allow MS HTML Help	All hosts	TCP remote port(s) 80; both incoming and outgoing traffic	Allowed
☑ Allow HP DHCP	All hosts	TCP remote port(s) 21,1000-5000; both incoming and outgoing t...	Allowed
☑ Allow HP SAM	All hosts	TCP remote port(s) 80,3389; both incoming and outgoing traffic	Allowed
☑ Allow NAC UDP	IP address(es) 172.16.1.101	UDP local port(s) 137,1500; both incoming and outgoing traffic	Allowed
☑ Allow NAC TCP In	IP address(es) 172.16.1.101	TCP local port(s) 139,1500; incoming traffic	Allowed
☑ Allow NAC TCP Out	IP address(es) 172.16.1.101	TCP remote port(s) 89; outgoing traffic	Allowed

Policy Enforcement

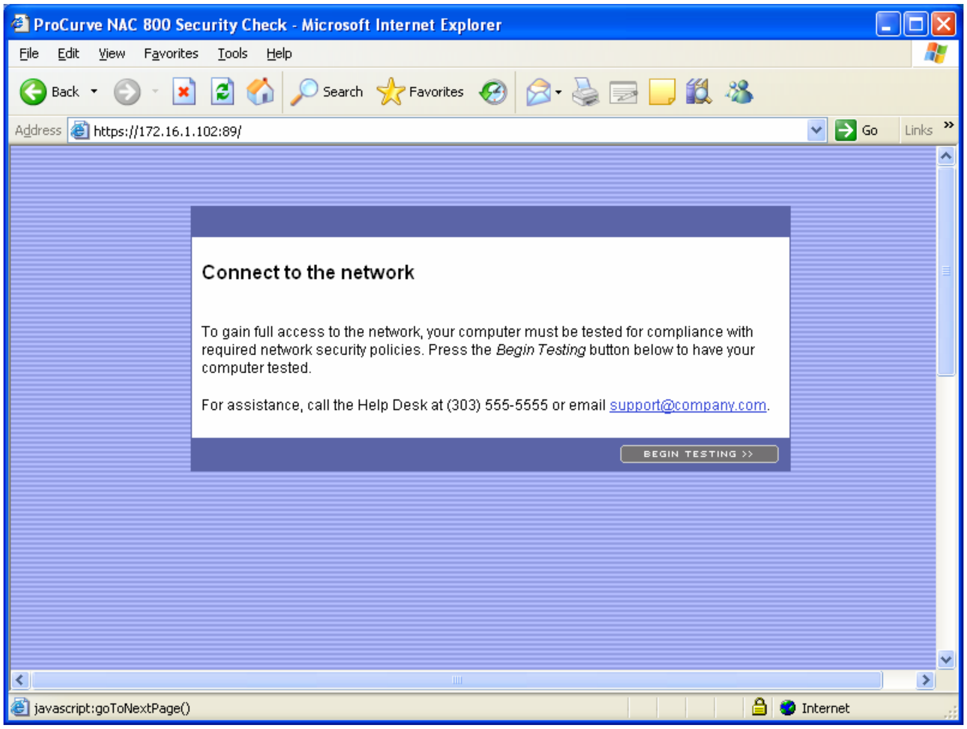
Now that the ProCurve NAC appliance is fully integrated into the network and configured with policy tests, we can now demonstrate policy enforcement in action.

Generic Testing Methods	ProCurve Named Method	Trade-offs	
		Plus (+)	Minus (-)
Agent-based Permanent	NAC Agent	• Always available for retesting • Automatic Agent updates	• Install and upgrade to maintain • Requires one-time interaction from end-users
Agentless	Agentless	• No install or download • Easiest of the three test methods to deploy	• Requires RPC Service to be available to the 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	• No installation or upgrade to maintain • Only Internet Explorer application access is allowed through the personal firewall. No open ports are necessary	• 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

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.
3. Go to https://172.16.1.101:89 on your browser.


ProCurve NAC 800 Security Check - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Go
Links

Address: https://172.16.1.102:89/

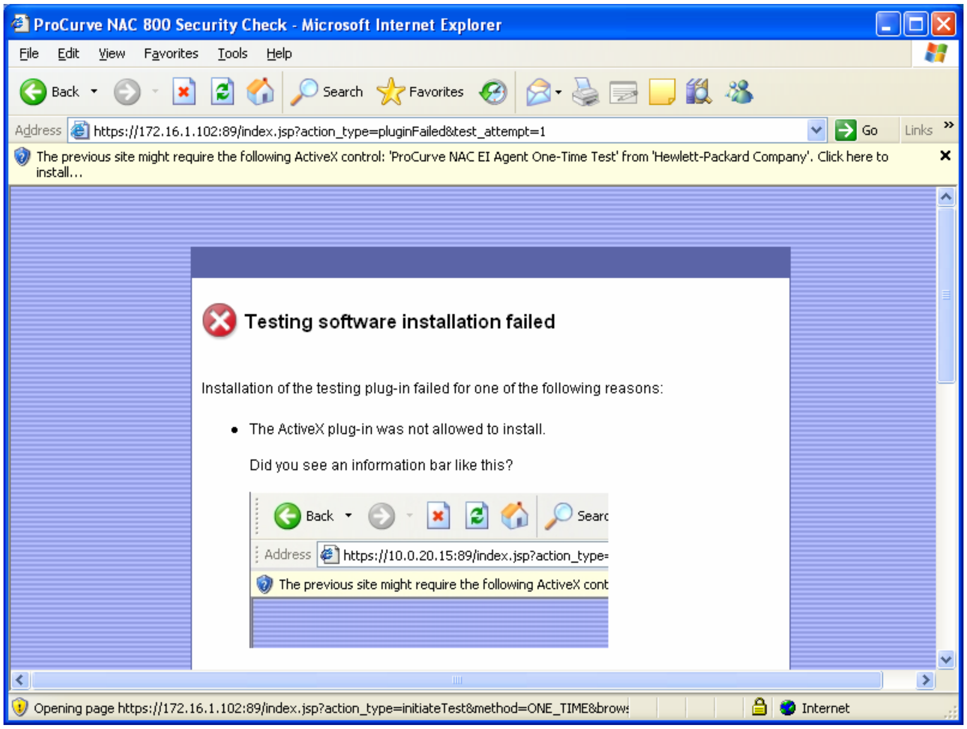
Connect to the network

To gain full access to the network, your computer must be tested for compliance with required network security policies. Press the *Begin Testing* button below to have your computer tested.

For assistance, call the Help Desk at (303) 555-5555 or email support@company.com.

javascript:goToNextPage()

4. Click **Begin Testing** to start the policy test.


ProCurve NAC 800 Security Check - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links

https://172.16.1.102:89/index.jsp?action_type=pluginFailed&test_attempt=1

The previous site might require the following ActiveX control: 'ProCurve NAC EI Agent One-Time Test' from 'Hewlett-Packard Company'. Click here to install...

Testing software installation failed

Installation of the testing plug-in failed for one of the following reasons:

- The ActiveX plug-in was not allowed to install.

Did you see an information bar like this?

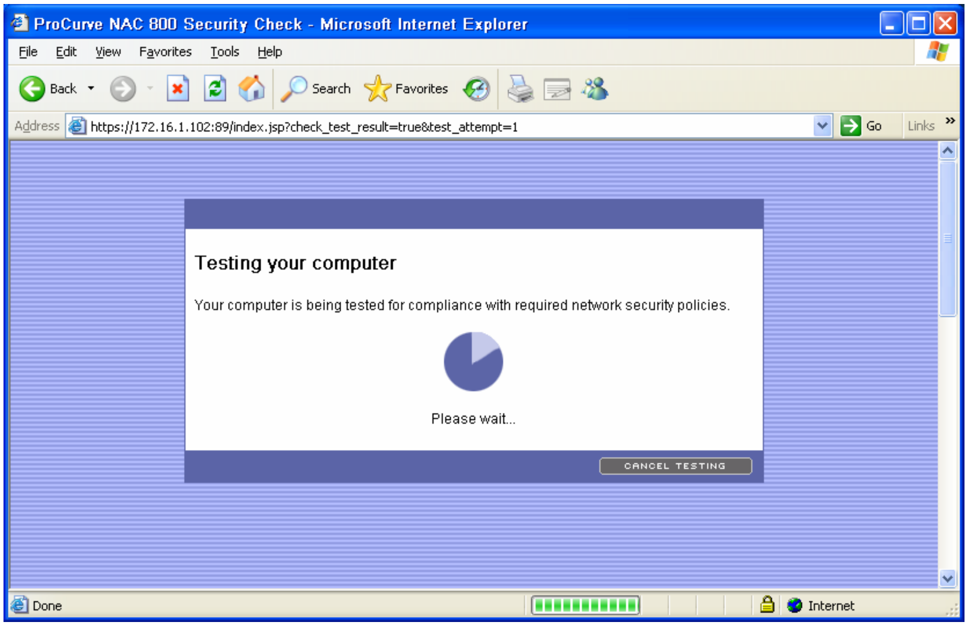
https://10.0.20.15:89/index.jsp?action_type=

The previous site might require the following ActiveX cont

Opening page https://172.16.1.102:89/index.jsp?action_type=initiateTest&method=ONE_TIME&brows

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.


ProCurve NAC 800 Security Check - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links

https://172.16.1.102:89/index.jsp?check_test_result=true&test_attempt=1

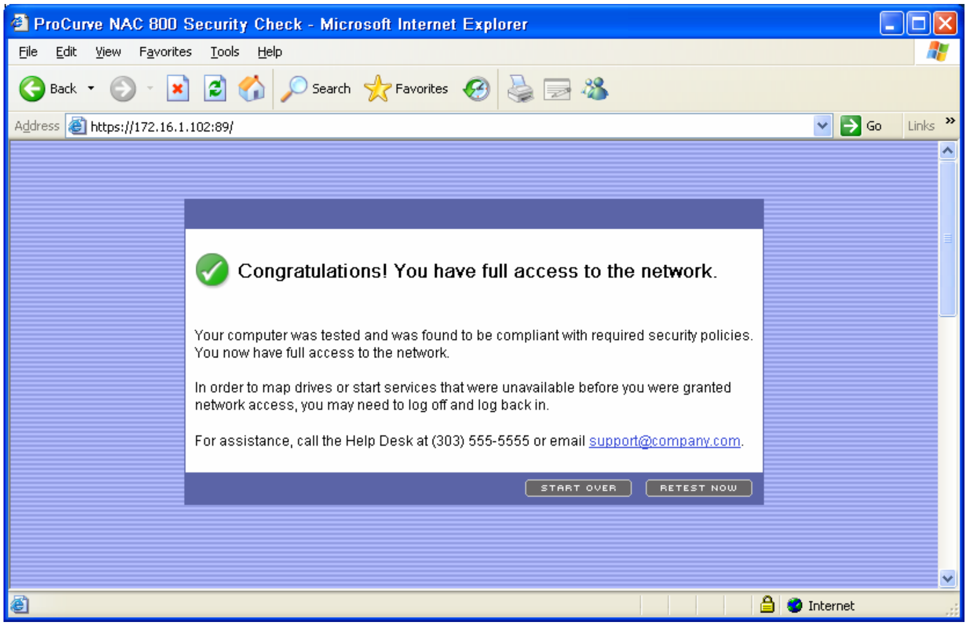
Testing your computer

Your computer is being tested for compliance with required network security policies.

Please wait...

CANCEL TESTING
Done
Internet

Once the ActiveX control is loaded, the testing can begin for the thin client.


ProCurve NAC 800 Security Check - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://172.16.1.102:89/
Go
Links
Internet

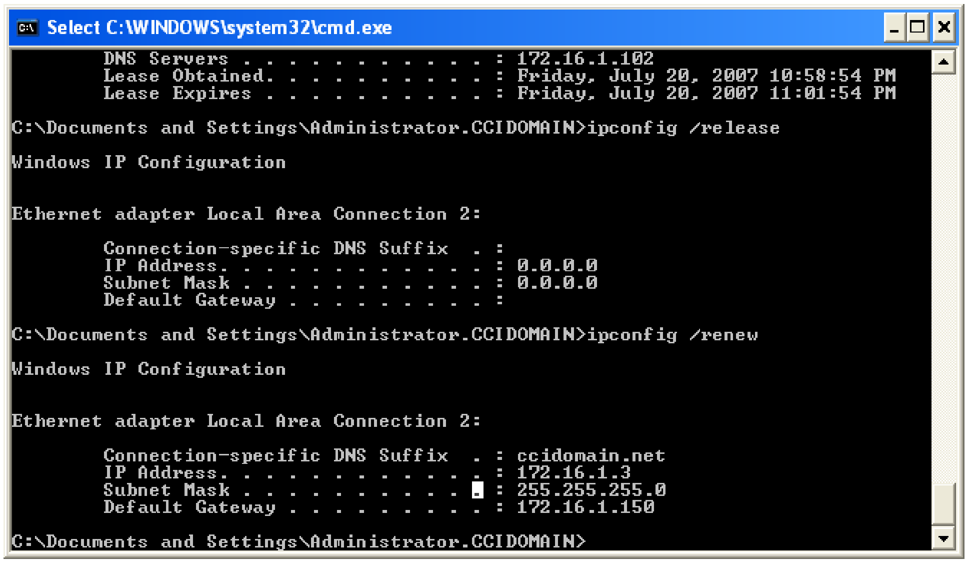
Congratulations! You have full access to the network.

Your computer was tested and was found to be compliant with required security policies. You now have full access to the network.

In order to map drives or start services that were unavailable before you were granted network access, you may need to log off and log back in.

For assistance, call the Help Desk at (303) 555-5555 or email support@company.com.

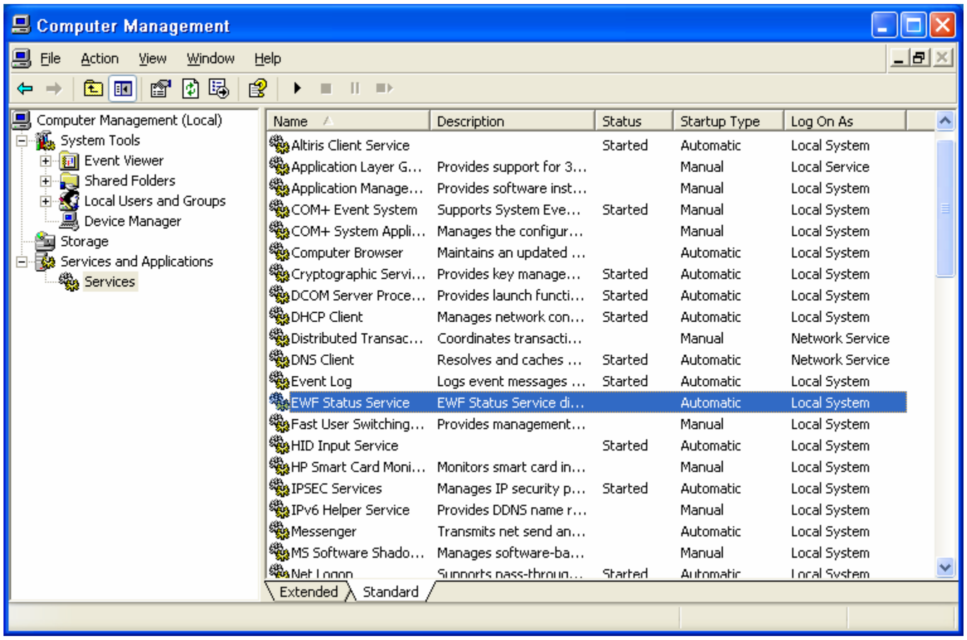
At this point, the thin client should be within policy and should therefore be allowed to access the network.



```
        DNS Servers . . . . . . . . . . . : 172.16.1.102
        Lease Obtained. . . . . . . . . . : Friday, July 20, 2007 10:58:54 PM
        Lease Expires . . . . . . . . . . : Friday, July 20, 2007 11:01:54 PM

C:\Documents and Settings\Administrator.CCIDOMAIN>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator.CCIDOMAIN>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : ccidomain.net
        IP Address. . . . . . . . . . . . : 172.16.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.1.150

C:\Documents and Settings\Administrator.CCIDOMAIN>
```

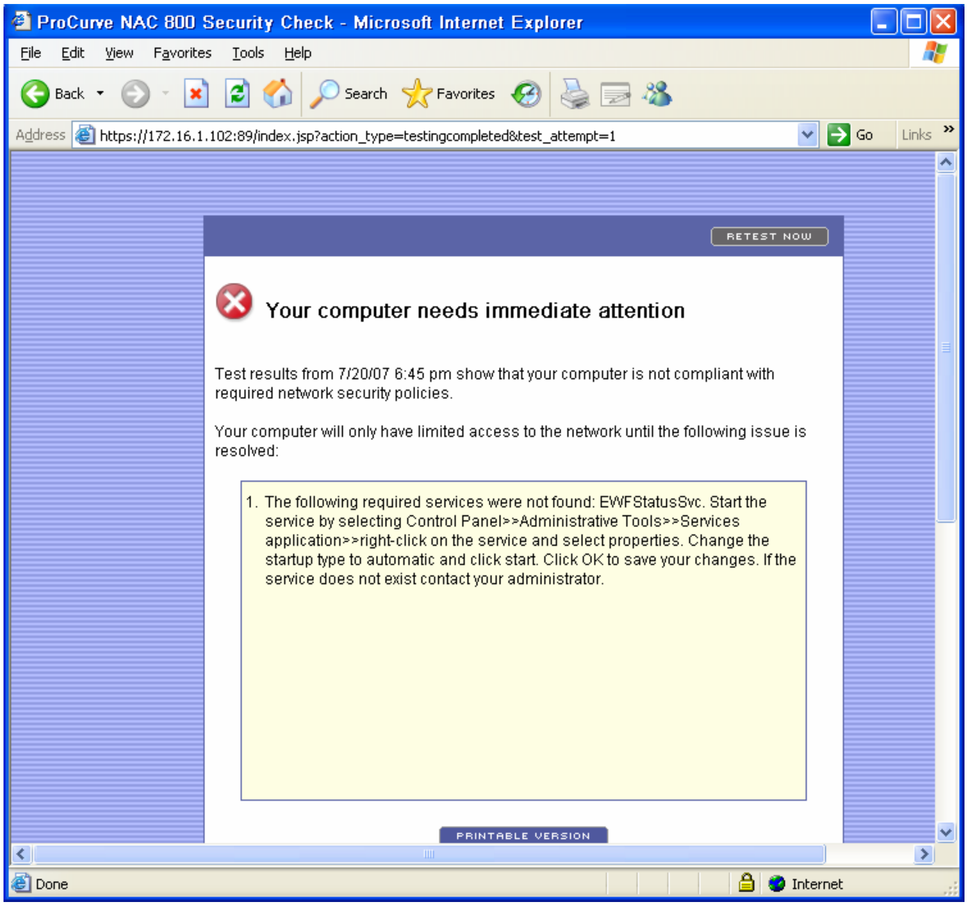
6. Confirm this by opening a command prompt and typing `ipconfig`. The result should show that the thin client IP address is 172.16.1.x.
7. Close the browser.
8. Right-click **My Computer**.

9. Click **Manage**.
10. Click **Services and Applications**.
11. Click **Services**.



Name	Description	Status	Startup Type	Log On As
Altiris Client Service		Started	Automatic	Local System
Application Layer G…	Provides support for 3…		Manual	Local Service
Application Manage…	Provides software inst…		Manual	Local System
COM+ Event System	Supports System Eve…	Started	Manual	Local System
COM+ System Appli…	Manages the configur…		Manual	Local System
Computer Browser	Maintains an updated …		Automatic	Local System
Cryptographic Servi…	Provides key manage…	Started	Automatic	Local System
DCOM Server Proce…	Provides launch functi…	Started	Automatic	Local System
DHCP Client	Manages network con…	Started	Automatic	Local System
Distributed Transac…	Coordinates transacti…		Manual	Network Service
DNS Client	Resolves and caches …	Started	Automatic	Network Service
Event Log	Logs event messages …	Started	Automatic	Local System
EWF Status Service	EWF Status Service di…		Automatic	Local System
Fast User Switching…	Provides management…		Manual	Local System
HID Input Service		Started	Automatic	Local System
HP Smart Card Moni…	Monitors smart card in…		Manual	Local System
IPSEC Services	Manages IP security p…	Started	Automatic	Local System
IPv6 Helper Service	Provides DDNS name r…		Manual	Local System
Messenger	Transmits net send an…		Automatic	Local System
MS Software Shado…	Manages software-ba…		Manual	Local System
Net Logon	Supports pass-throu…	Started	Automatic	Local System

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


ProCurve NAC 800 Security Check - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
RETEST NOW
PRINTABLE VERSION
Done
Internet

https://172.16.1.102:89/index.jsp?action_type=testingcompleted&test_attempt=1

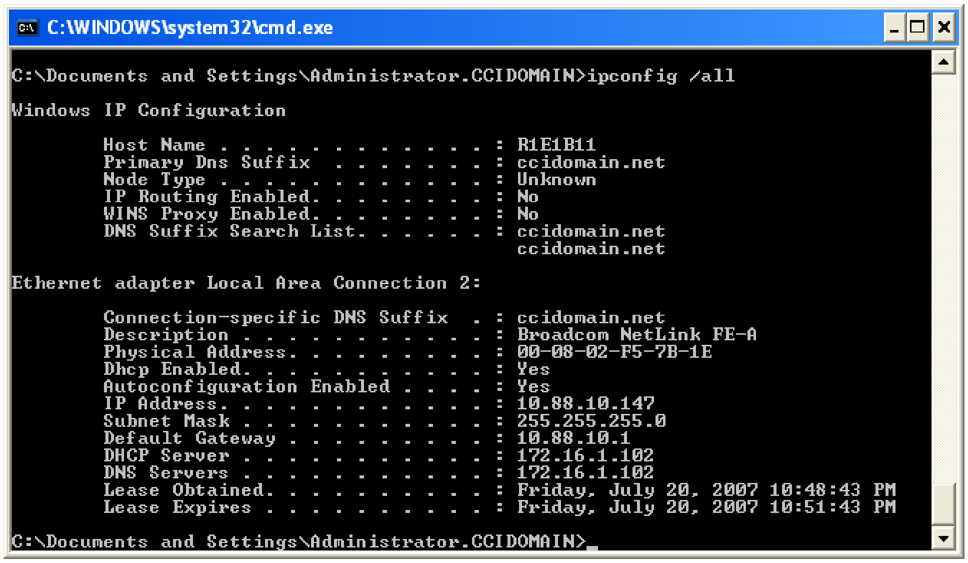
Your computer needs immediate attention

Test results from 7/20/07 6:45 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 issue is resolved:

1. The following required services were not found: EWFStatusSvc. Start the service by selecting Control Panel>>Administrative Tools>>Services application>>right-click on the service and select properties. Change the startup type to automatic and click start. Click OK to save your changes. If the service does not exist contact your administrator.

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

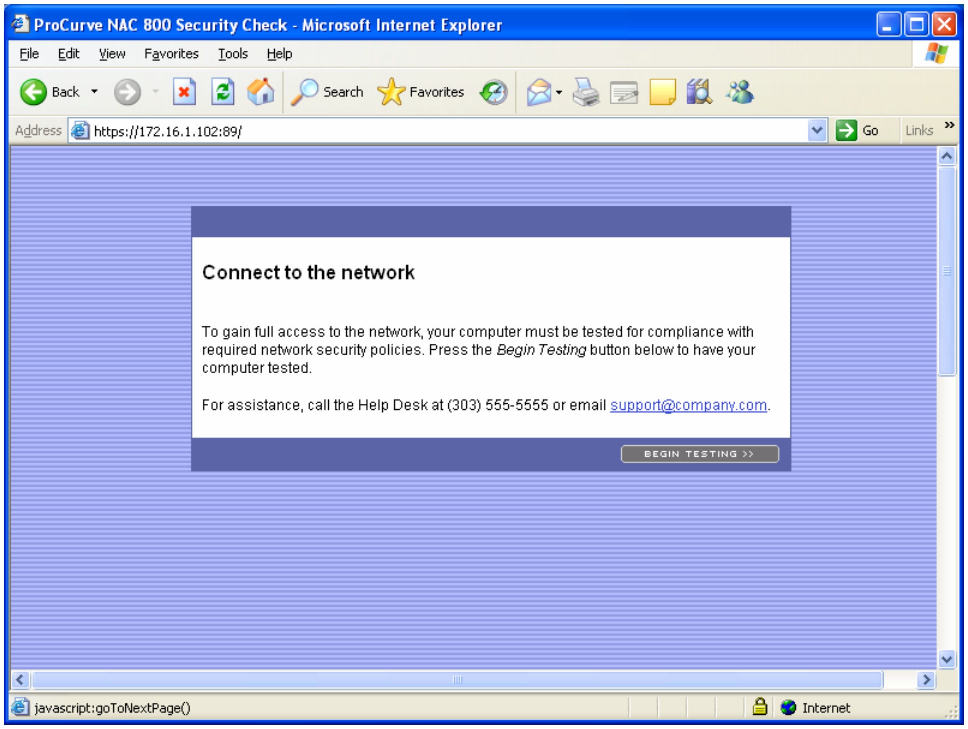


```
C:\Documents and Settings\Administrator.CCIDOMAIN>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : R1E1B11
        Primary Dns Suffix  . . . . . . . : ccidomain.net
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : ccidomain.net
                                            ccidomain.net

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : ccidomain.net
        Description . . . . . . . . . . . : Broadcom NetLink FE-A
        Physical Address. . . . . . . . . : 00-08-02-F5-7B-1E
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.88.10.147
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.88.10.1
        DHCP Server . . . . . . . . . . . : 172.16.1.102
        DNS Servers . . . . . . . . . . . : 172.16.1.102
        Lease Obtained. . . . . . . . . . : Friday, July 20, 2007 10:48:43 PM
        Lease Expires . . . . . . . . . . : Friday, July 20, 2007 10:51:43 PM

C:\Documents and Settings\Administrator.CCIDOMAIN>_
```

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.

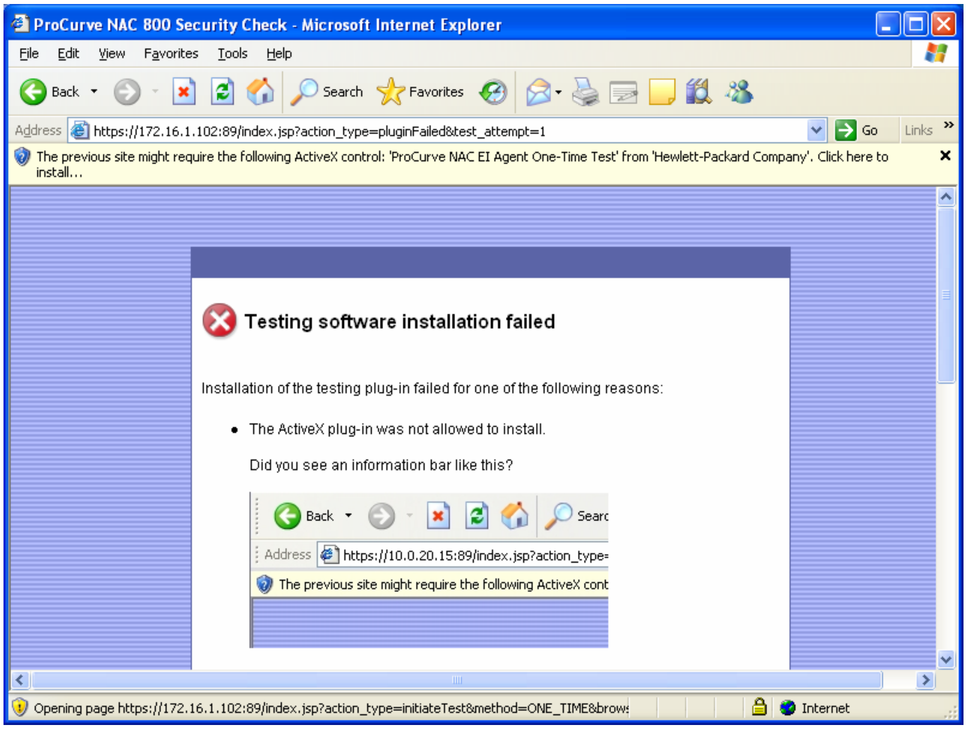


Connect to the network

To gain full access to the network, your computer must be tested for compliance with required network security policies. Press the *Begin Testing* button below to have your computer tested.

For assistance, call the Help Desk at (303) 555-5555 or email support@company.com.

3. Go to https://172.16.1.102:89 on your browser.



ProCurve NAC 800 Security Check - Microsoft Internet Explorer

Address https://172.16.1.102:89/index.jsp?action_type=pluginFailed&test_attempt=1

The previous site might require the following ActiveX control: 'ProCurve NAC EI Agent One-Time Test' from 'Hewlett-Packard Company'. Click here to install...

Testing software installation failed

Installation of the testing plug-in failed for one of the following reasons:

- The ActiveX plug-in was not allowed to install.

  Did you see an information bar like this?

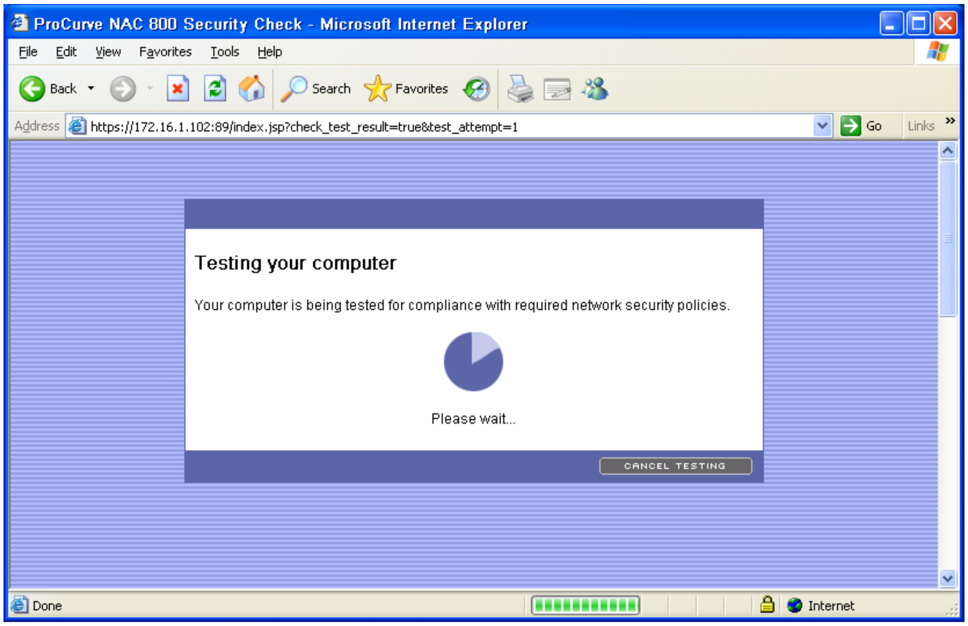
  Address https://10.0.20.15:89/index.jsp?action_type=

  The previous site might require the following ActiveX cont

Opening page https://172.16.1.102:89/index.jsp?action_type=initiateTest&method=ONE_TIME&brows

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.



ProCurve NAC 800 Security Check - Microsoft Internet Explorer

Address https://172.16.1.102:89/index.jsp?check_test_result=true&test_attempt=1

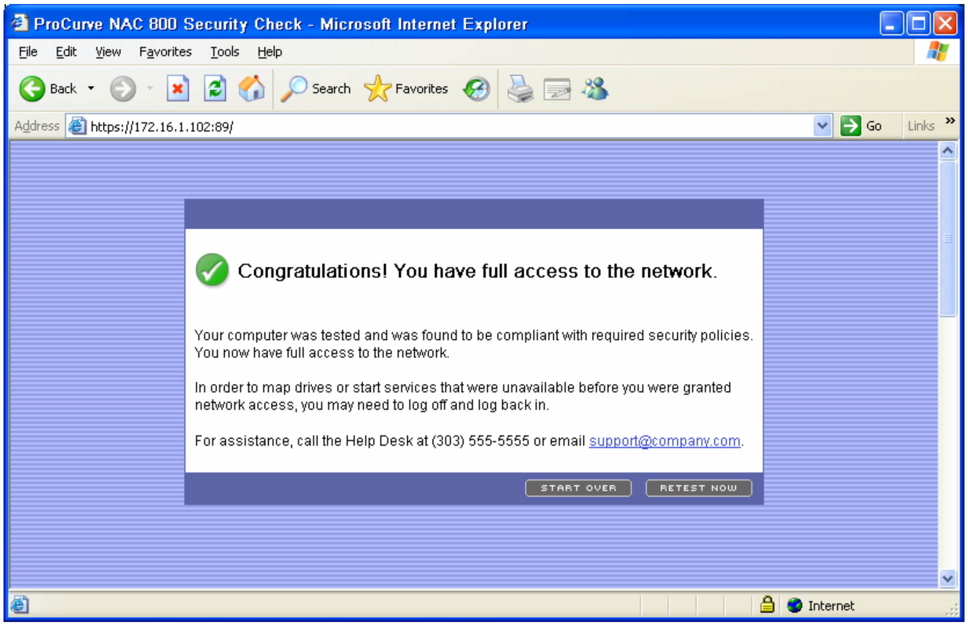
Testing your computer

Your computer is being tested for compliance with required network security policies.

Please wait...

Done

5. Start the policy test by clicking **Begin Testing**.


ProCurve NAC 800 Security Check - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address https://172.16.1.102:89/
Go
Links
START OVER
RETEST NOW
Internet

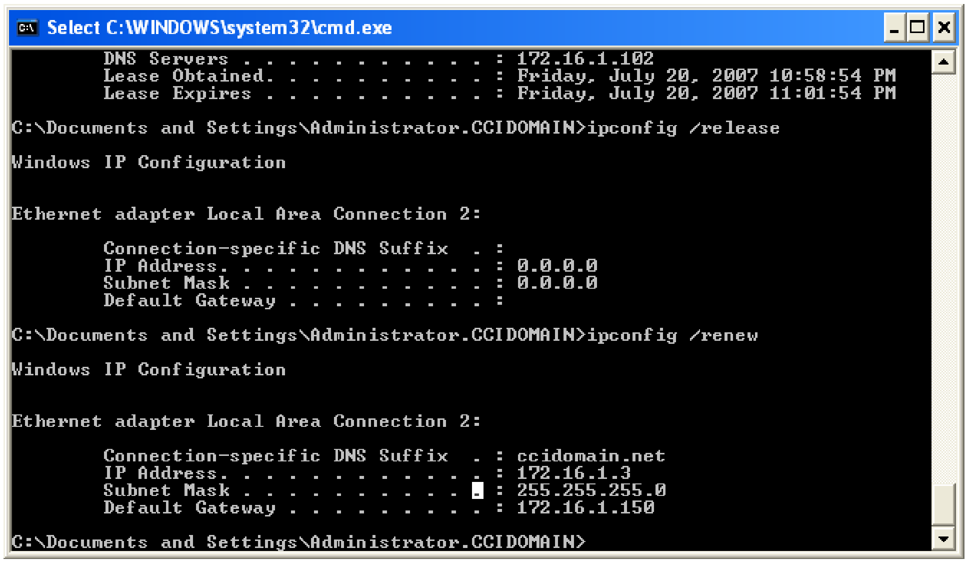
Congratulations! You have full access to the network.

Your computer was tested and was found to be compliant with required security policies. You now have full access to the network.

In order to map drives or start services that were unavailable before you were granted network access, you may need to log off and log back in.

For assistance, call the Help Desk at (303) 555-5555 or email support@company.com.

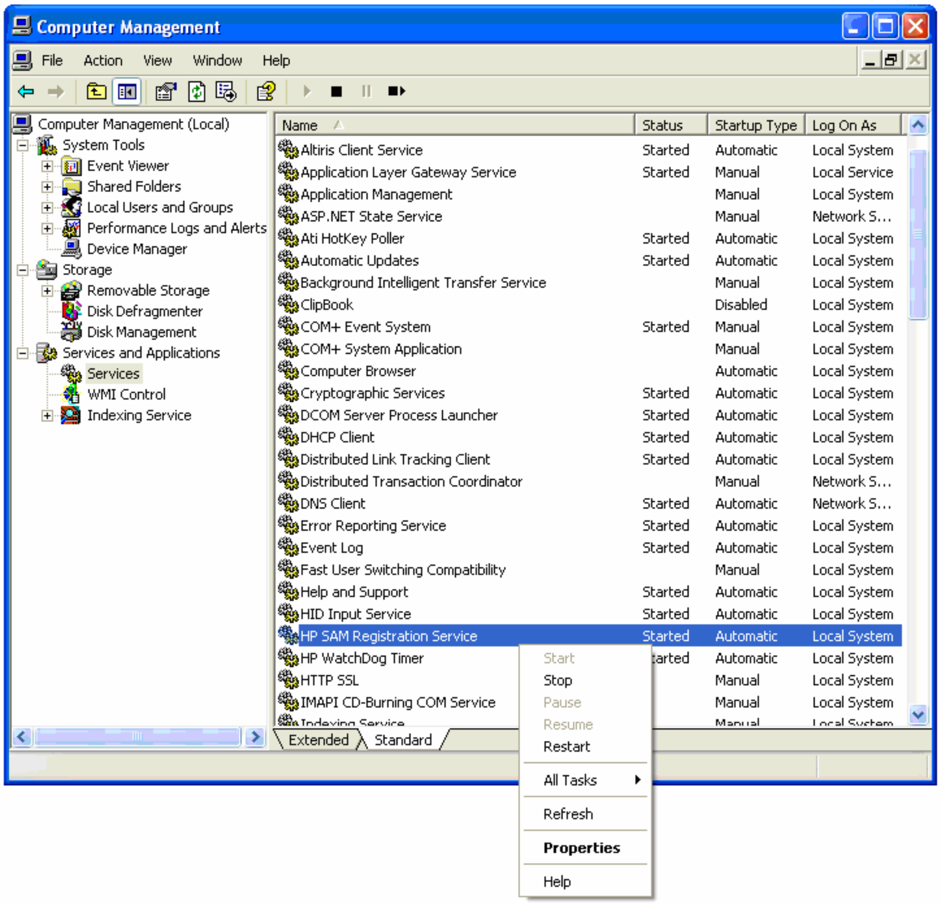
At this point, the blade PC should be in policy and therefore should be allowed to access the network.



```
        DNS Servers . . . . . . . . . . . : 172.16.1.102
        Lease Obtained. . . . . . . . . . : Friday, July 20, 2007 10:58:54 PM
        Lease Expires . . . . . . . . . . : Friday, July 20, 2007 11:01:54 PM

C:\Documents and Settings\Administrator.CCIDOMAIN>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator.CCIDOMAIN>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : ccidomain.net
        IP Address. . . . . . . . . . . . : 172.16.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.1.150

C:\Documents and Settings\Administrator.CCIDOMAIN>
```

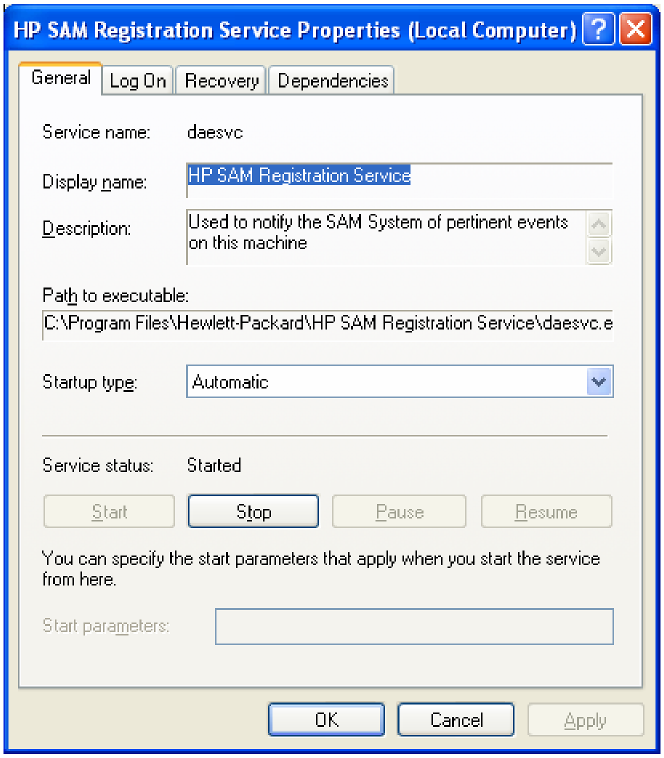
6. Confirm this by opening a command line up and typing `ipconfig`. It should show that the thin client IP address is 172.16.1.x.
7. Close the browser.

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



Name	Status	Startup Type	Log On As
Altiris Client Service	Started	Automatic	Local System
Application Layer Gateway Service	Started	Manual	Local Service
Application Management		Manual	Local System
ASP.NET State Service		Manual	Network S...
Ati HotKey Poller	Started	Automatic	Local System
Automatic Updates	Started	Automatic	Local System
Background Intelligent Transfer Service		Manual	Local System
ClipBook		Disabled	Local System
COM+ Event System	Started	Manual	Local System
COM+ System Application		Manual	Local System
Computer Browser		Automatic	Local System
Cryptographic Services	Started	Automatic	Local System
DCOM Server Process Launcher	Started	Automatic	Local System
DHCP Client	Started	Automatic	Local System
Distributed Link Tracking Client	Started	Automatic	Local System
Distributed Transaction Coordinator		Manual	Network S...
DNS Client	Started	Automatic	Network S...
Error Reporting Service	Started	Automatic	Local System
Event Log	Started	Automatic	Local System
Fast User Switching Compatibility		Manual	Local System
Help and Support	Started	Automatic	Local System
HID Input Service	Started	Automatic	Local System
HP SAM Registration Service	Started	Automatic	Local System
HP WatchDog Timer	arted	Automatic	Local System
HTTP SSL		Manual	Local System
IMAPI CD-Burning COM Service		Manual	Local System
Indexing Service		Manual	Local System

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



Service name: daesvc

Display name: HP SAM Registration Service

Description: Used to notify the SAM System of pertinent events on this machine

Path to executable:
C:\Program Files\Hewlett-Packard\HP SAM Registration Service\daesvc.e

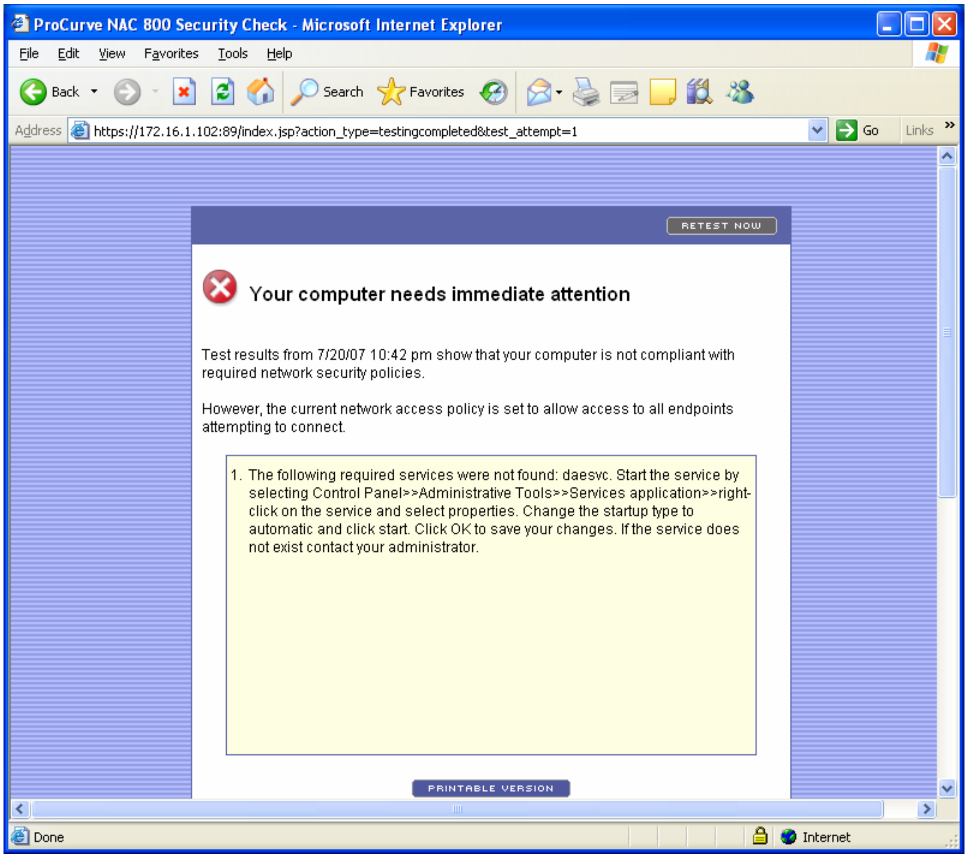
Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

13. Retest the machine.


ProCurve NAC 800 Security Check - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://172.16.1.102:89/index.jsp?action_type=testingcompleted&test_attempt=1
Go
Links
RETEST NOW
PRINTABLE VERSION
Done
Internet

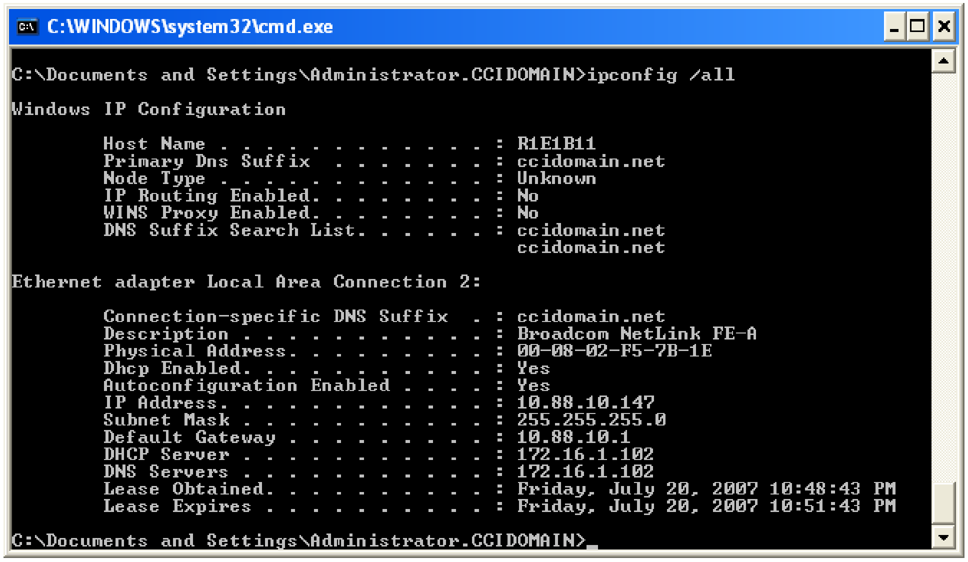
Your computer needs immediate attention

Test results from 7/20/07 10:42 pm show that your computer is not compliant with required network security policies.

However, the current network access policy is set to allow access to all endpoints attempting to connect.

1. The following required services were not found: daesvc. Start the service by selecting Control Panel>>Administrative Tools>>Services application>>right-click on the service and select properties. Change the startup type to automatic and click start. Click OK to save your changes. If the service does not exist contact your administrator.

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



```
C:\Documents and Settings\Administrator.CCIDOMAIN>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : R1E1B11
        Primary Dns Suffix  . . . . . . . : ccidomain.net
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : ccidomain.net
                                            ccidomain.net

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : ccidomain.net
        Description . . . . . . . . . . . : Broadcom NetLink FE-A
        Physical Address. . . . . . . . . : 00-08-02-F5-7B-1E
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.88.10.147
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.88.10.1
        DHCP Server . . . . . . . . . . . : 172.16.1.102
        DNS Servers . . . . . . . . . . . : 172.16.1.102
        Lease Obtained. . . . . . . . . . : Friday, July 20, 2007 10:48:43 PM
        Lease Expires . . . . . . . . . . : Friday, July 20, 2007 10:51:43 PM

C:\Documents and Settings\Administrator.CCIDOMAIN>_
```

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
  http://www.hp.com/rnd/products/security/index.htm
- 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
  http://www.hp.com/rnd/products/management/idm/overview.htm

466209-001, January 2008