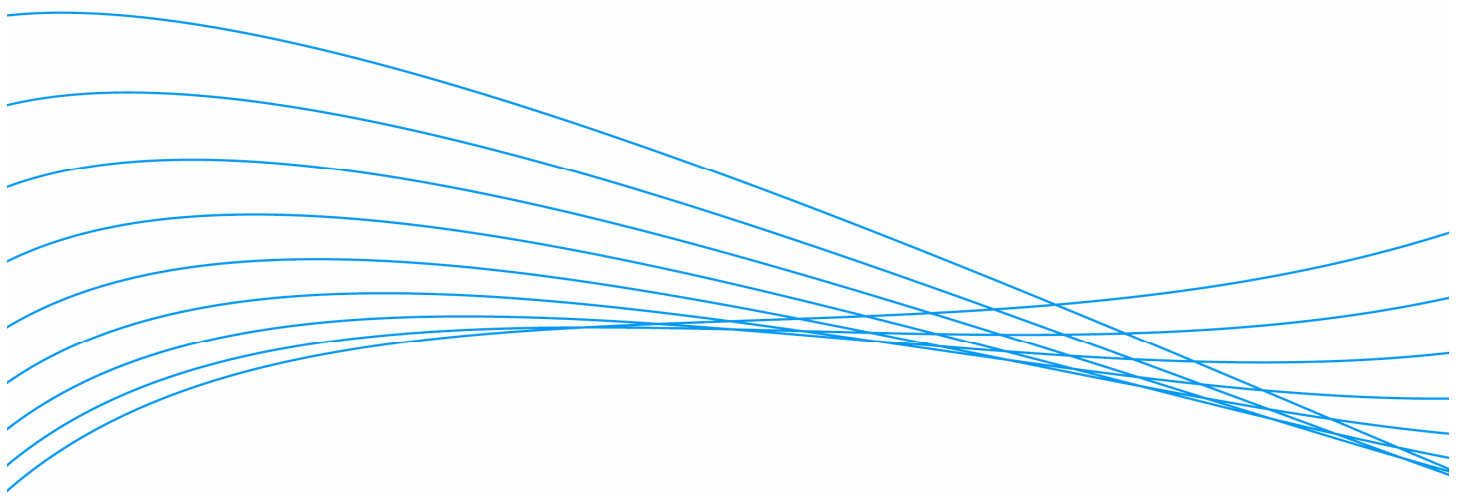


Access Control Solution



Introduction	2
Background	2
Related Trends	2
Network Threats	3
Network Access Control.....	3
Primary Objectives of NAC.....	3
The AAA Security Framework	4
ProCurve Networking’s Access Control Solution.....	4
How It Works	5
Architecture	5
ProCurve Secure Network Infrastructure.....	5
ProCurve Identity Driven Manager (IDM)	6
ProCurve Network Access Controller 800	7
Endpoint Integrity Tests.....	7
RADIUS Authentication	7
Multiple Deployment Modes	7
Benefits of the ProCurve Access Control Solution	8
Business Benefits	8
IT Manager Benefits	8
Summary.....	8

Introduction

Technology in today's world is changing at an ever-increasing rate. 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 with others, 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 due to 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.

People today are accustomed to being "connected" — having quick and easy access to the information they need (or want) at any time. In addition to accessing publicly available information, more and more company-sensitive information is being made available on company intranets. Having the ability to access information anytime, anywhere enables people to be more efficient and productive. Being connected also means being available to others and having access to others who also are connected. The proliferation of e-mail, instant messaging, and Internet telephony allows for communication to happen whenever and wherever people are "connected."

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 which 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.

There are many aspects to a complete network security implementation. This white paper addresses the concept of Network Access Control (NAC), which provides organizations the ability to control access to networks and the information available on those networks. It also describes the access control solution provided by ProCurve networking by HP. ProCurve Networking is dedicated to providing networking solutions that enable organizations to increase productivity, fortify security, and reduce complexity.

Background

Related Trends

Security is certainly not a new concept for IT organizations in the business world. However, the need to control access to corporate networks has evolved significantly over the past decade. This need can be linked to several trends in the networking industry and business processes.

Wireless networking – Prior to wireless networking, many enterprises relied on physical access to enforce network security; they knew where the network connections existed and maintained physical security to them as necessary. However, the boundaries of wireless networking cannot be seen and can easily extend beyond the protected boundaries of an organization. Network and security experts quickly identified the need to control access to wireless connections. In turn, they realized that wired networks held many of the same security concerns and therefore, required a solution for controlling all network access.

Mobile workforce – With the use of laptop computers exceeding that of desktop computers, employees are connecting into the enterprise network from many different locations both inside and outside the enterprise. As employees with laptops move between shared offices or from office to meeting room, different users and devices are connecting to the network via the same physical network connection. When systems were connected to one network port and did not move, security could be statically applied to that network port. However, now that one port must support many different users and devices over time, it must be able to enable access and security levels appropriate for each of those users (e.g., R&D, marketing and finance) and their devices (e.g., laptops, PDAs and VoIP phones).

In addition, mobile devices connecting to networks outside the protected enterprise pose an elevated threat to becoming infected by viruses or other malware. Threats are unknowingly transferred into the enterprise by the user when their device is returned to the office connection.

Shared network access – Increasingly, networks are being shared by users with different roles. For example, many organizations work with contractors, partners and suppliers on a regular basis. This often requires providing some level of network access to these external workers, while maintaining security for internal data and assets. Also, guest access to the Internet, either as a benefit or a service, has become almost expected from visitors to sites.

Malicious software – The increasing number of attacks, along with the rising costs resulting from such attacks, has emphasized the need to protect the network and its resources from harmful devices.

Government regulations – Many organizations today are required to comply with a growing number of government regulations, such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPPA). These regulations often require organizations to set and enforce policy around network security and data privacy.

Network Threats

Network attacks continue to threaten network assets. According to the 2006 CSI/FBI Computer Security Survey of U.S. corporations, government agencies, financial institutions, medical institutions and universities, the majority of organizations experienced computer security incidents during the previous year. In addition, these attacks are becoming more sophisticated and dangerous. Initial network attacks began with individuals attempting to demonstrate their ability to outsmart new technology. Today's attacks are often highly organized schemes, sometimes assisted by insiders, and increasingly, are designed for financial gain.

Traditional network security efforts primarily have targeted the perimeter of networks to protect from external threats. Therefore, there are some very good solutions built upon firewalls, VPN devices, IDS/IPS systems and UTMs to address these threats. However, there is an increasing need to protect against threats from *inside* the corporate network. These internal threats stem primarily from malicious users or harmful devices, and are the primary focus of network access control.

Network Access Control

Securing the network and, in turn, the resources on the network, has become one of the most important tasks facing IT organizations today. NAC has quickly become one of the most important aspects of network security. However, it is also one of the least well-defined terms in network security. Network access control can simply mean "the process of controlling access to computer networks and network resources." This broad definition, combined with a heightened awareness of the need to address network security, has led to the NAC being used to market many fairly diverse network security products and solutions. This also has led to confusion about exactly what a NAC solution provides.

The goal of NAC is to protect the network and its resources from harmful users and systems. It does this by restricting network access based on certain criteria and business policies. The policies may be quite simple, such as allowing a set of known users or devices, and denying all others. Or, in order to model more intricate business policies, they may be much more complex. In general, most NAC solutions are designed to accomplish one or more of the following objectives:

Primary Objectives of NAC

Restricting user access – In its most basic form, this is the need 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.

Protection from malicious software – This is the need to evaluate 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.

Regulatory compliance documentation – As more government regulations are defined, organizations need to have plans in place to enforce network data privacy. In addition, they will need documentation about the policies and how they are enforced.

The AAA Security Framework

The framework of authentication, authorization, and accounting (AAA) has been used for quite some time to describe the layers of controlling access to computer resources. A complete NAC solution will include aspects of each one of these layers.

Authentication: Authentication is the process of identifying a user (or device) requesting access and verifying their credentials. Credentials can range from a simple username/password pair to a strong two-factor authentication scheme. The authentication process evaluates the passed credentials with those stored in an authentication database.

Authorization: Authorization is the matching of an authenticated user with appropriate network access rights. These access rights may be as simple as allowing or denying access to the network. However, it is also possible to provide a much richer set of network access rights that define a number of network resources to which the user is allowed to access.

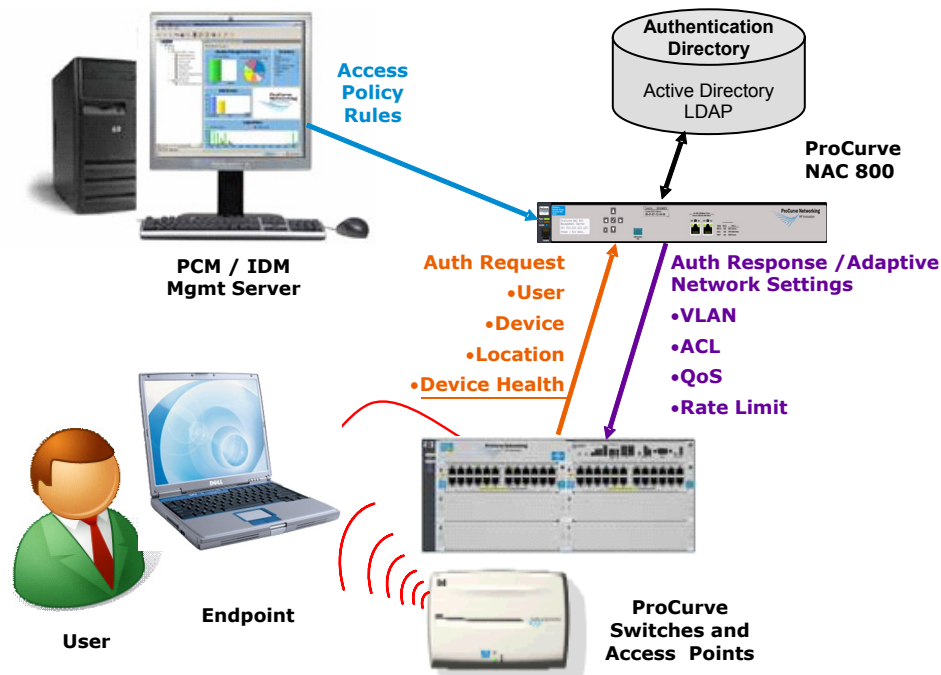
Accounting: Accounting is the process of documenting network access. This often includes a complete list of all authentication requests and the resulting authorization. This allows for a rich set of data, which can be used for documenting network security policy and enforcement, as well as for investigating potential network breaches.

ProCurve Networking's Access Control Solution

The ProCurve Access Control Solution is based on the ProCurve Adaptive EDGE Architecture and the ProCurve "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. ProCurve's Identity Driven Manager (IDM) product is a network access policy server which dynamically adapts network ports to the needs of the user and the device(s) that connect. 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 which fortifies network security.

How It Works

Architecture



ProCurve Secure Network Infrastructure

ProCurve network devices (switches and access points) provide a range of security technologies to meet the diverse needs of enterprise networks. These technologies are used consistently across both wired and wireless network devices to provide a unified security and access control solution across the enterprise network. Specific features related to access control include:

Flexible Port Security: The most effective way to control network access is to authenticate users and devices prior to letting them on the network. ProCurve devices enable this capability using standard 802.1X authentication. In addition, many ProCurve devices support two alternate authentication methods: a captive portal web-authentication (Web-auth), and MAC-based authentication (MAC-auth), which also enable pre-authentication enforcement. These multiple authentication modes provide effective enforcement for network access control along with flexibility to meet the mixed needs of enterprise networks.

Multiple Authentication Types per Port: ProCurve devices can be configured to support multiple authentication types on a port simultaneously. This allows for the same port to automatically authenticate an employee's PC, which is configured to use 802.1X at one time, and later, authenticate a guest who has not configured 802.1X on his or her PC by using the captive-portal functionality of Web-auth. This provides simplified access for regular network users, while still providing the flexibility to authenticate guests without requiring client software.

Multiple Authentications per Port: In addition, some ProCurve devices provide the ability to authenticate multiple sessions on a single port, enabling multiple downstream devices to connect securely to a single secured port. This is especially important when computers are connected to a VoIP phone and the computer and phone share the same network port.

Adaptive Network Configuration: In addition to allowing users and devices to authenticate, ProCurve network devices support the ability to authorize varying levels of network access. These network devices respond to settings defined in ProCurve Identity Driven Manager to customize network access based on business policy. These settings are user-based and can define resources on the network to which the user is allowed or denied access, based on VLAN or specific access control lists. Access also can enforce network performance settings. Such

customization makes it possible to prioritize VoIP devices in order to maximize call quality and eliminate drops, or to throttle guest user traffic so that it does not impact performance negatively.

ProCurve Identity Driven Manager (IDM)

IDM helps companies maximize network security and improve productivity by enabling automatic configuration of the network edge through security and management policies defined on a centrally administered server. The IDM solution makes this possible by allowing network administrators to dynamically apply security and performance settings to network infrastructure devices based on user, device, location, time and other variables. The result is a unified management infrastructure and a more secure, mobile and converged network.

IDM is a plug-in module to the ProCurve Manager Plus platform. It provides the centralized policy management interface for defining network access rights and monitoring network access. It integrates with standard RADIUS authentication services and user directories (LDAP and Active Directory) to authenticate users and/or devices connecting to the network and then adds a rich set of authorization capabilities on top of the basic authentication.

IDM utilizes the ProCurve command from the center capability to dynamically automate the configuration of edge ports and provide unique – and appropriate – network access for each network connection. Pushing control to the edge of the network allows security and performance settings to be enforced as close to the endpoint as possible, where it is most effective.

IDM provides facilities to simplify and organize network access policies. Although it is possible to identify unique access rights for every user, it is not realistic nor does it probably match with business policies. Generally, there are relatively few unique communities within an organization that require a unique network access policy.

IDM defines communities of users who share common network access privileges. Typically, these communities are defined by department, such as marketing, or by role, such as purchasing. Each community has a unique set of rules, based on business policy, which indicate the level of network access users will get when they connect.

These rules are based on common business concepts. IDM can provide unique access based on the following information:

- Who is the user?
- With what community(s) is the user associated?
- Is the user's device (PC, laptop, PDA, etc.) running the appropriate software required by the business?
- Where is the user (switch/port)?
- What time is it?

In turn, IDM identifies the appropriate level of network access rights:

- Resources are made available/denied to that community(s)
- Performance attributes are assigned to that community(s)

Some have argued that intelligence at the edge of the network poses unmanageable complexity for an IT organization to handle. They contend it is conceptually easier to implement and manage intelligence at the core in a couple of switches versus the edge, where there are potentially thousands of ports and even more users.

However, if the configuration and desired behavior of that intelligence is automated, and the complexity remains behind the scenes, network management becomes simpler and the user experience is enhanced.

This approach is significantly different from the traditional strategy, where a particular switch and particular port were configured to act a particular way. This new methodology enables any switch and any port to act uniquely for each individual. It provides the user with the same network functionality, resources and view no matter where or how they connect.

In general, this is the essence of an intelligent, adaptive network and in particular, IDM. The network no longer behaves uniformly; instead, it adapts appropriately to the needs of each user.

ProCurve Network Access Controller 800

The ProCurve Network Access Controller 800 (ProCurve NAC 800) enables the ProCurve Access Control Solution to evaluate the integrity of endpoints before they are allowed to access the enterprise network. In addition, it provides a RADIUS authentication capability that integrates with the ProCurve command from the center management platform.

Endpoint Integrity Tests

The primary role of the ProCurve NAC 800 is to evaluate the health of endpoints as they connect onto the network. Verifying the health of endpoints before they connect to the network allows infected or otherwise harmful systems to be denied access or isolated so they cannot attack other network systems, therefore reducing costly network and system downtime. In addition, endpoints are tested while they remain connected to the network, providing an ongoing post-authentication health check.

Endpoint integrity tests are used to determine the overall security posture of an endpoint. When evaluating an endpoint, it is important to not only determine the current health of the system, but also, to evaluate the endpoint's ability to remain healthy. The ProCurve NAC 800 provides a comprehensive set of tests to evaluate the current health of a system as well as the appropriate configuration to protect itself from attacks by others. These tests include checks for:

- **Operating system:** services packs, hotfixes, auto-update settings
- **Security software:** antivirus, spyware, firewalls, peer-to-peer applications, allowed and prohibited programs and services
- **Security settings:** for browsers and applications
- **Required and prohibited software:** *customizable by the administrator*
- **Malicious software:** checks for some common spyware, worms, viruses and Trojans

RADIUS Authentication

The ProCurve NAC 800 appliance also provides RADIUS-based authentication services to enable secure network access. RADIUS is a standards-based authentication service that is the basis for almost all NAC solutions which use network infrastructure for enforcement. This authentication service can be used with IDM to provide the adaptive network access rights to network devices.

Multiple Deployment Modes

The ProCurve NAC 800 is designed with multiple enforcement modes in order to accommodate the needs of enterprise networks. All enforcement methods utilize pre-authorization checks for security policy in order to protect the network from harmful systems. These 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 security settings which 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 to comply with the security policies. This is an effective solution for testing endpoints which connect remotely through a VPN concentrator.

DHCP Enforcement: The ProCurve NAC 800 integrates with the enterprise DHCP server to isolate endpoints as they request a network address. Endpoints are isolated by their network address so they can be tested for 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 security settings which 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.

Benefits of the ProCurve Access Control Solution

In today's world, businesses strive to maximize network productivity and reliability while enforcing network security. They must make information easily available to those who need it, but also, create security policies that will keep information from those who should not have access to it. Also, many businesses are now required to document their security policies and show how they are being enforced. Finally, this all must be accomplished without making a forklift-upgrade to the existing network infrastructure. The ProCurve access control solution helps IT organizations meet these needs.

Business Benefits

Business Needs	ProCurve Access Control Solution
Increase Network Productivity	Controls network access, providing appropriate access (based on policy) only to authenticated users and devices
Maximum Network Reliability	Isolates infected or harmful systems before they are allowed to connect to the network and infect others
Regulatory Compliance Assistance	Provides reporting of network access security policies, along with detailed logs of all network access provided and denied
Investment Protection	Leverages built-in ProCurve switch technology to enforce authenticated network access and provide secure access to authorized resources

IT Manager Benefits

IT Needs	ProCurve Access Control Solution
Secure the network from unauthorized users and devices	Provides easy-to-use policy-based network access controls which integrate with standard RADIUS authentication services and user authentication directories
Endpoint Integrity Verification	Enables pre-authorization testing of endpoints before they are allowed to enter the enterprise network, along with post-authorization testing to ensure they remain safe
Network threat and usage information	Logs and reports on all network accesses, including time on the network, network data sent/received, security posture results, network access privileges provided, and failed login attempts

Summary

The ProCurve Access Control solution is the proactive element of the ProCurve ProActive Defense security strategy to build a trusted network infrastructure. Together with the ProCurve Network Immunity Solution, which includes the ProCurve Network Immunity Manager, the ProCurve Access Control solution fortifies security at the edge of the network where users connect. ProCurve access control provides the initial layer of network security by authenticating users and devices before they are allowed onto the network. It continues to verify the health and security posture of devices while they are connected.

The ProCurve Access Control Solution provides significant value by:

- Increasing network productivity
- Maximizing network availability
- Maximizing the current investment in ProCurve switches
- Securing access to data based on user and business policy
- Providing a unified access control solution for LAN, WLAN, and remote access users

ProCurve provides an access control solution which can be easily deployed and managed using the ProCurve command from the center management. It also offers comprehensive access control capabilities.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2007 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.

Itanium is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

5982-9129EN, 04/2007