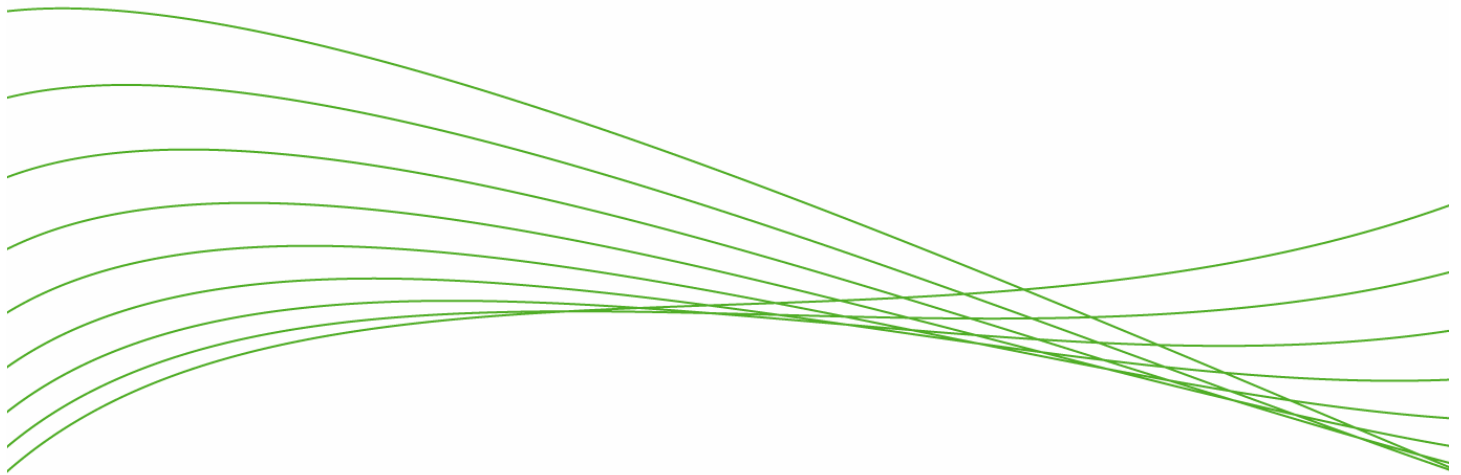


ACLs in ProCurve IDM 2.0: Making User-Based Security More Usable



Overview	2
“Traditional” ACLs	2
IDM ACLs Expand on the Traditional.....	2
User-Based ACLs.....	2
Resource-Based Configuration.....	3
IDM ACLs Combined With VLAN-Based ACLs.....	4
Summary.....	4
For More Information.....	5

Overview

Access control lists (ACLs) hold promise for helping network administrators to realize the fulfillment of the Adaptive EDGE Architecture™ promise, yet administering ACLs can be complex, cumbersome and prone to error. ProCurve Identity Driven Manager (IDM) 2.0 adds ACLs to the list of settings that network administrators can use to control access to their networks, but with a twist: IDM ACLs are user-based, rather than VLAN-based, meaning they are applied individually to users while they are connected to the network. Additionally, IDM simplifies the process of configuring ACLs using the concept of *resources* rather than more detailed items such as IP addresses, access control entries (ACEs), classless Internet domain routing (CIDR) notation, or specific ports and port ranges.

The ACLs implemented in IDM 2.0 make it possible to secure and manage network resources more safely, precisely and simply than ever before.

"Traditional" ACLs

ACLs are mechanisms for defining network security that limit and control access between users and network resources using "filter" rules. ACLs are made up of individual rules that apply to incoming packets. When a packet arrives at a switch, ACLs trigger a filtering process on that packet that matches it with pre-defined rules. The packet is either allowed (continues on through the switch) or denied (prevented from further travel through the network).

Historically, ACLs have acted on things such as the source and destination IP address, source destination port and protocol type. ACLs are set up to evaluate rules in order. Typically, the most granular or precise rules are defined (and thus processed) first.

IDM ACLs Expand on the Traditional

IDM ACLs are implemented using a feature of ProCurve switches called RADIUS-assigned ACLs. IDM ACLs are unique in that they are applied to individual users as they connect to the network and are removed when the user is no longer connected. Another characteristic of IDM ACLs is that they offer a simpler, resource-based configuration of access control rules.

Typical VLAN-based ACLs apply filters to traffic as it passes from one subnet to another. Most often, these VLAN-based ACLs are defined to control traffic at the subnet-to-subnet level. IDM ACLs are more specific, applying rules to traffic from individual users.

Using IDM ACLs, network administrators can assign access rights for users and groups directly to the network resources to which they require access. For instance, finance employees can be allowed access to specific finance resources, while everybody else is denied access. Contractors can be prohibited from using the Web entirely. Employees can be allowed to access only the specific servers from which they require data. Coupled with endpoint integrity products, IDM ACLs can quarantine users who attempt to access the network using a virus-infected device, restricting them from using any system except the remediation server.

User-Based ACLs

User-based ACLs in IDM 2.0 enable network administrators to quickly and precisely assign access rights to individuals – automatically, at the moment of access to the network – wherever and whenever they log in. The IDM ACLs become active when the user authenticates, and they are removed when the user is no longer connected to the network.

ProCurve has made these IDM ACLs easy to manage by allowing the specification of ACL rights at the group level, so they apply to all users in the group.

Users are placed within an Access Policy Group that best matches their network access characteristics. At a company, these Access Policy Groups might include Employee, Contractor and Guest, or Finance, Marketing, R&D and Guest. At a school or university, they might include Faculty, Student, Administrator and Guest.

As with IDM 1.0, each Access Policy Group in IDM 2.0 has a set of policy rules, which define the Access Profile that is used to give connecting users access to the network. Inputs to these policy rules are the same as before, including Location, Time and System. Each rule references an Access Profile, which defines the access rights for the user.

With IDM 2.0, the Access Profile includes the VLAN, QoS and rate limits for the user, as before. Additionally, IDM 2.0 adds a new attribute: IDM ACLs. The IDM ACLs allow the administrator to include the network resources to which a user is allowed, or denied, access.

For example, a school IDM Access Policy Group called Faculty would be defined with a rule that references the appropriate Access Profile for faculty members. That Access Profile would include the resources to which faculty members would be included (e.g., a server containing student grades and tests). All faculty members who belong to that group would have the appropriate faculty ACLs applied to them when they log in to the network.

User-based ACLs can even be used to lessen the need for VLANs. One of the main purposes of VLANs was to segregate users so that subnet-based (i.e., VLAN-based) ACLs could be applied to subnets. With user-based ACLs, much of the value of VLANs goes away because users are either allowed or denied access to network resources individually, at the edge of the network where they connect.

User-based ACLs are active only while the user is connected; they go away when the user disconnects from the network by logging out or disconnecting. One thing to note is that the ACL is applied independently of whether a packet is routed or not — in contrast to VLAN-based ACLs, which are applied only to routed packets. By evaluating all packets, user-based ACLs offer a greater degree of security at the edge of the network.

Resource-Based Configuration

Resource-based configuration takes the configuration of ACLs to a higher, more intuitive level.

Understanding and remembering the syntax of VLAN-based ACLs is both difficult and prone to error. In addition, the people responsible for the network often tend to think in terms of resources rather than ACEs, IP addresses, CIDR notation, or specific ports and port ranges. In IDM 2.0, you specify access to specific resources in the network. Resources can include a subnet, a server, a service, a protocol (e.g., TCP, UDP, ICMP), a port (e.g., HTTP, Telnet, DHCP) or a combination of these.

As a result, IDM 2.0 attempts to raise the fundamental definition of ACLs to a higher level: When network administrators configure IDM ACLs they define resources, and they configure specific access rights regarding those resources, either allowing access or denying access to the individual resources.

Network resource details are a combination of one or more of the following:

- Protocol (IP, TCP, UDP)
- Destination addresses (hosts or subnets)
- Application port (HTTP, Telnet, etc.)

Network administrators must still take a little time to define the specific resources they wish to deal with, such as Web access (e.g., ports 80 and 443), finance servers or protocols such as ICMP. But once defined, the access rights are configured within an IDM Access Profile using a GUI-based wizard that makes it easy for administrators to define the appropriate access rights to those resources and create the user-based ACLs that are dynamically applied.

As an example, access rights for a team of contractors might be the following:

- Allow DHCP
- Deny Internet access
- Allow access to contractor database
- Deny everything else

As is clear in this example, by working at the resource level, the administrator can deal with concepts and entities that are familiar and intuitive, which saves time and greatly simplifies the configuration process.

IDM ACLs Combined With VLAN-Based ACLs

The two types of ACLs – the new IDM ACLs and the existing VLAN-based ACLs – are by no means mutually exclusive. In fact, ProCurve has designed its IDM ACLs to ensure the greatest level of security in networks where both types of ACLs exist.

When both user-based ACLs and VLAN-based ACLs are configured on the switch, both will be enforced in IDM 2.0 in the most secure manner. That is, if there is a “deny” that matches either the user-based ACL or the VLAN-based ACL, the corresponding packet will be denied.

Many typical VLAN-based ACLs are used in a defensive manner, to protect resources from unwarranted access. In IDM 2.0, the denial of these VLAN-based ACLs will always be honored. This process of automatically denying a packet that matches “deny” for either the IDM or VLAN-based ACL ensures that an individual’s IDM ACL is unable to override the more general and often more secure VLAN-based ACLs.

Summary

The ACLs in IDM 2.0 enable the network to adapt to each individual user by applying ACLs on his or her behalf, no matter when or where the network connection is made. Because IDM ACLs are applied at the edge, at the point of access to the network, they can keep people and their devices from getting access to protected areas, devices and protocols in the network. In this way, IDM ACLs enhance network security while also simplifying network administration and strengthening network administrators’ ability to control their networks.

IDM ACLs represent the most striking example to date of the Adaptive EDGE Architecture promise of control to the edge with command from the center.

For More Information

To learn more about ProCurve Networking solutions, contact your local ProCurve sales representative or visit the company's Web site at www.procurve.com.

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

www.procurve.com



© 2005 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.

4AA0-2249ENW, 10/2005