

Interopyet What is Network Policy Enforcement? My Rodney Thayer

by Rodney Thayer

Policy enforcement is an old term that is now being used to describe a variety of technical solutions. This paper defines the term "Policy Enforcement" in the context where we want to control access to a network. Note that "policy enforcement" could mean other things not having anything to do with networking.

Why use this? Because you can control access to your network in the event of a problem. If a new virus starts to propagate across your network, or if a user brings a laptop computer into the network from the outside that has inappropriate software, or if a machine is simply not running the latest software updates, you can control it. No longer do you have to simply allow any random machine to connect to the network. This can significantly improve the defense of the network.

Definition

"Network Policy Enforcement" is the application of some sort of network access control mechanism to control access to a network. The criteria for whether an end system is allowed to access the network are specified in a set of rules or parameters known as a "policy".

The process of policy enforcement consists of three steps:

- 1. Examine the system's "posture" to determine if it is compliant with the policy.
- 2. Using a Policy Enforcement Point, make a decision regarding which parts of the network, if any, that the device should be allowed to access.
- 3. Allow the device to access the network as decided. Note the access might be limited to remediation correcting some policy violation.

What's a "Policy"?

A policy is either a set of usage rules, a set of parameters to be used by a specific authorized user, or a set of system criteria that is used to precisely define the rules that must be complied with before the system is allowed to access the network. In principle these are contained in some sort of "policy description language". In reality, more simple schemes are used. Some examples of policy information are:

- RADIUS attribute/value pairs specifying what VLAN to connect a user to
- LDAP-stored data specifying what Anti-Virus update level a system must be using
- Vendor-proprietary rules about what files must or must not be present
- Rules about programs that may or may not be executing on the system (like music file sharing)
- Firewall-like rules defining what network traffic is allowed, like allowing port 80 (HTTP for web access) but not 25 (SMTP to act as your own email server.)

Examples of Network Policy

Here are some examples of things you might consider to be "policy":

- A bank teller can only connect their computer to the bank network during business hours while the bank is
- An end user can only connect to the network if they are running the corporate-specified anti-virus product, and they are running the latest virus definition update
- A laptop must be running a personal firewall to connect to the corporate network (because it was mobile and was recently used on the road in an Internet Café)
- All users in the Sales department connect only to the Sales VLAN
- Guest users who have non-compliant but not malicious systems are allowed limited guest access only for access to the public internet.

Network Policy Devices

How are these policies enforced? There are three major categories of mechanisms:

1. use of in-line devices, called "policy enforcement points", that actually sit in-line with the network traffic from the systems to be controlled. If the policy of a given system is not found to be compliant, the system

- is not allowed to access the network at all, or is only allowed to access some sort of remediation infrastructure. This requires an in-line device.
- use of VLAN's via switches or wireless access points to control which VLAN a system is connected to based on the system's policy compliance. This requires an 802.1X-aware switch, or AP and 802.1Xaware client systems.
- 3. web portals that act as 'captive portals', redirecting all network traffic to the portal while the policy compliance determination is done. This requires a web browser.

Policy Infrastructure

In addition to the actual policy enforcement device, the network infrastructure has to provide support services to implement this. Some sort of back-end authentication mechanism must be used if username/passwords are to be used to control access. A security event management mechanism must be in place so the policy enforcement devices can report when there are non-compliance events and for network management. Some sort of centralized policy store may be used to control policy distribution, such as an LDAP server, or policy data embedded in RADIUS data, or Active Directory.