ROBERT HASKINS

ISPadmin: policy enforcement

Robert Haskins has been a UNIX system administrator since graduating from the University of Maine with a B.A. in computer science. Robert is employed by Shentel, a fast-growing network services provider based in Edinburg, Virginia. He is lead author of *Slamming Spam: A Guide for System Administrators* (Addison-Wesley, 2005).

rhaskins@usenix.org

IN THIS EDITION OF ISPADMIN, I TAKE a look at the policy enforcement area. This is a critical area for service providers who need to provide existing or new services to their customers in a low-cost, accurate, but quickly provisioned fashion. As a direct result of policy enforcement systems, the provider can more accurately track its customer's services while at the same time reducing its cost to acquire and retain subscribers. Although policy enforcement is directly related to Remote Authentication Dial In User Sevices (RADIUS), it really is a combination of everything a service provider does: provide service, authenticate users, bill subscribers, and more.

Policy Enforcement Background

Policy enforcement is the ability to apply access control to services across a network in a consistent, sane manner. It is related to the ideas of authentication and authorization, which are both critical to all service provider operations. After all, if you are allowing anyone to access your services, you probably aren't making much money! To be specific, authentication is the act of proving without a shadow of a doubt "who the user is," and authorization is "what services that user is allowed to access."

For example, an Apache .htaccess/.htpasswd file combination can be thought of as a simple policy enforcement system. This is because it controls who is allowed to access what resources on an Apache Web server. In a similar fashion, a UNIX passwd file controls who has access to the system, but it is more difficult to specify what services that user is allowed to access on the system in question. On traditional UNIX systems, policy enforcement is usually accomplished by a combination of additional access files beyond the passwd file.

In a hosted Web service provider environment, the group file can be used to control access to uploaded Web server files. In a similar fashion, fields in the passwd file can control access to what that user can do on the host. For example, the SHELL field in the passwd file might be set to /etc/nologin in the case of a host running a POP3 server. This would effectively disable interactive logins for the POP3 user but allow access to that user's mailbox. Of course, these mechanisms lie outside of any network-based controls on the host, such as iptables firewall or TCP wrapper.

If you are familiar with the traditional ISP dial-up network, you might be aware that the RADIUS protocol is often used to authenticate and authorize users (as well as account for them). The RADIUS protocol has excellent policy control abilities, enabling equipment manufacturers to define their own features and control mechanisms by virtue of the Vendor-Specific attribute in the RADIUS dictionary. (For a background on RADIUS, please see the April 2001 ISPadmin column titled "RADIUS" as well as [1].)

A Short History and Policy Enforcement Vendors

Historically, policy enforcement systems (like many parts of service provider operations) were developed in-house. RADIUS-only policy enforcement engines continue to form the basis of many ISPs' operations. However, if the provider wants features such as subscriber self-provisioning and/or next-generation services (video, voice, gaming, etc.) then plain vanilla RADIUS-based solutions won't work.

On the traditional telephone company side (i.e., non–IP-based network policy control), companies such as Lucent and Nortel have been the big players. Of course, a telephone company's proprietary switch must have the associated company's proprietary policy control engine to control it, because telephone systems usually lack open standards for provisioning and controlling their services. However, with the advent of IP networks and associated openness for provisioning services, the policy management arena has blossomed. Companies that have products in this market include Broadhop [2], Bridgewater Systems [3], and Tazz Networks [4].

What Are Policy Enforcement Systems?

Policy enforcement engines control access to services on a provider's network. These systems can take many forms and can be quite specialized in the case of traditional telephone networks. An example of a simple policy enforcement engine would be RADIUS. In fact, policy enforcement engines in the IP world are often built around service-provider-grade RADIUS systems. However, modern IP-based policy enforcement engines handle much more functionality than just RADIUS. Some of the additional services provided by enforcement engines include the following:

- DHCP services
- Subscriber self-provisioning/upgrading
- Subscriber/customer support
- Billing system interface for accounting detail
- Plan/package management

These services will be examined in some detail in the next sections.

DHCP SERVICES

DHCP services don't have to be integrated into the policy engine, but the provider gets a higher degree of control if they are. For example, if the provider wants to offer a service that uses a device that doesn't support RADIUS (e.g., some game consoles or VoIP handsets), then assigning an IP address via DHCP and the associated MAC address is often the only way that this can be done. Without policy control of the DHCP server, integration is much harder at best, or impossible in the worst case.

SUBSCRIBER PROVISIONING AND SUPPORT

One big reason for implementing policy control is to reduce subscriber signup and support costs. This can be accomplished by implementing systems that allow a subscriber to sign up as a new customer, add or change services, view his or her bill, and perform other functions, all without incurring the cost of a phone call to the support center. This is accomplished by simply integrating the provider's support and signup Web site into the policy enforcement system (if one already exists).

Allowing customers to add services also increases the likelihood that impulse purchases will occur. For example, if the subscriber knows that merely pressing the "turbo" button will increase DSL speed from 0.5M b/s to 3 Mb/s for 60 minutes to download a large file six times as fast, it is much more probable that the subscriber will buy the service. The easier it is for a customer to buy a product, the more likely it is that the customer will buy it.

BILLING SYSTEM INTEGRATION

Integration into the service provider's billing system is the key to successful deployment of policy-based systems. Often, the service plans offered by the provider are in the billing system and must be transferred to the policy enforcement engine easily and quickly. Alternatively, the policy control engine must give the provider the ability to create and manage the billing plan and associated services if no direct integration with the billing system is warranted.

In addition to plans, RADIUS accounting records must be transferred to the provider's billing system so that customers can be billed. Sometimes, rating can be done on the accounting records prior to sending billing detail to the billing system for updating customer records.

Of course, newly provisioned customers must be sent to the provider's billing platform. Any new or changed customer data (resulting from signups or service changes) must be transferred to the billing system as well, so that the master billing database is kept up-to-date. In IP-based policy engines, this can be done much more easily than was possible in the past by utilizing a standard XML interface.

Policy Enforcement and Equipment

End-user access devices such as a dial-in remote access server (RAS), BRAS (DSL access equipment), and wireless access points must interact with the policy enforcement engine. These devices actually enforce the policy served by the policy engine. Often, the policy enforcement software must be programmed to support the device even though the policy engine acts just like a "normal" RADIUS server. This is a result of the tight integration between the RADIUS server and other components of the policy control engine.

There are a number of devices that can be used as a gateway device to enforce policy where no such device exists (e.g., RAS or BRAS). Cisco has implemented its Service Selection Gateway (SSG) software in its current IOS releases. Of course, the Cisco hardware platform must support the SSG capability [5]. Other gateway device manufacturers include Nomadix [6] and Colubris [7]. Another lower-cost option would be a "roll your own" solution using mini-ITX or Soekris hardware (see the October 2005

ISPadmin column for background). Although the "do it yourself" price is right, it does take some work to set up your own device to act as a gateway/policy enforcement device.

Conclusion

In this edition of ISPadmin, I've looked at what the policy enforcement engine is and how it fits into the service provider environment. Policy enforcement is critical to any service provider wanting to reduce its operating cost while improving the level of service to the customer. Enforcement engines are implemented as commercial software packages, owing to their specific application in service provider environments. Policy enforcement ties together many of the disparate services utilized by a service provider, including RADIUS, DHCP, billing, provisioning, and customer signup. Gateway devices such as Nomadix, Colubris, and Cisco's SSG IOS version are often used to implement policy on end-user connections.

REFERENCES

[1] RADIUS-related RFC listing: http://www.freeradius.org/rfc/.

[2] Broadhop home: http://www.broadhop.com/.

[3] Bridgewater Systems home: http://bridgewatersystems.com/.

[4] Tazz Networks home: http://www.tazznetworks.com/.

[5] Cisco 6400 policy enforcement device: http://www.cisco.com/en/US/products/hw/routers/ps314/products_data_sheet091-86a008007ce99.html.

[6] Nomadix AG 3000 home: http://www.nomadix.com/products/platforms/ag3000.

[7] Colubris Multi Service Controller: http://www.colubris.com/global-wireless-network-management/multiservice-controllers.asp.

Background on policy management engines: http://www.lightreading.com/document.asp?doc_id=77367.