CHAPTER 1

Security Overview

This chapter provides an overview of the following security features used with the Cisco Nexus 1000V.

User Accounts

Access to the Cisco Nexus 1000V is accomplished by setting up user accounts that define the specific actions permitted by each user. You can create up to 256 user accounts. For each user account, you define a role, user name, password, and expiration date. For information about configuring and managing user accounts, see Chapter 2, “Managing User Accounts.”

Authentication, Authorization, and Accounting (AAA)

AAA, called Triple A, is an architectural framework for configuring a set of three independent, consistent, and modular security functions.

- Authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods and then applying that list to various interfaces.
- Authorization—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual capabilities and restrictions.

- Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services that users are accessing, as well as the amount of network resources that they are consuming.

Note You can configure authentication outside of AAA. However, you must configure AAA if you want to use RADIUS or TACACS+, or if you want to configure a backup authentication method.

For information about configuring AAA, see Chapter 3, "Configuring AAA."

RADIUS Security Protocol

AAA establishes communication between your network access server and your RADIUS security server.

RADIUS is a distributed client/server system implemented through AAA that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

For information about configuring RADIUS, see Chapter 4, "Configuring RADIUS."

TACACS+ Security Protocol

AAA establishes communication between your network access server and your TACACS+ security server.

TACACS+ is a security application implemented through AAA that provides a centralized validation of users who are attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon that usually runs on a UNIX or Windows NT workstation. TACACS+ provides separate and modular authentication, authorization, and accounting facilities.

For information about configuring TACACS+, see Chapter 5, "Configuring TACACS+."

SSH

You can use the Secure Shell (SSH) server to enable an SSH client to make a secure, encrypted connection to a device. SSH uses strong encryption for authentication. The SSH server can interoperate with publicly and commercially available SSH clients.

The SSH client works with publicly and commercially available SSH servers.

For information, see the "Configuring SSH" section on page 6-1.

Telnet

You can use the Telnet protocol to set up TCP/IP connections to a host. Telnet allows a person at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address. For information, see the "Configuring Telnet" section on page 7-1.

Access Control Lists (ACLs)

An ACL is an ordered set of rules for filtering traffic. When the device determines that an ACL applies to a packet, it tests the packet against the rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies a default rule. The device processes packets that are permitted and drops packets that are denied.

ACLs protect networks and specific hosts from unnecessary or unwanted traffic. For example, ACLsare used to disallow HTTP traffic from a high-security network to the Internet. ACLs also allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

For more information, see the following:

- Chapter 8, "Configuring an IP ACL."
- Chapter 9, "Configuring a MAC ACL."

Port Security

Port security lets you configure Layer 2 interfaces permitting inbound traffic from a restricted set of MAC addresses called secure MAC addresses. In addition, traffic from these MAC addresses is not allowed on another interface within the same VLAN. The number of MAC addresses that can be secured is configurable per interface.

For more information, see Chapter 10, "Configuring Port Security."