Implementing Identity Management

An important aspect of trust and identity being established in a network involves the ability to authenticate users and devices to a central, trusted repository. Cisco devices will use the TACACS+ plus or RADIUS protocol to authenticate users back to an authentication, authorization, and accounting (AAA) server. A number of AAA servers are on the market, including the Cisco Secure Access Control Server (ACS). The Cisco Secure ACS can be installed on a Microsoft Windows server and provides a central location for network devices to request authentication and authorization and to perform accounting.

AAA is the process of performing authentication, authorization, and accounting for users who require network resources. AAA is a framework in which additional protocols are needed for communication between AAA servers and AAA clients. Those additional protocols include TACACS+ and RADIUS. A brief discussion of each follows.

Cisco Secure ACS for Windows Overview

Cisco Secure ACS for Windows is a centralized identity networking solution that simplifies the management of users across all Cisco devices and security management applications. Cisco Secure ACS provides enforcement of policy for administrators and users who access a network. With reporting capabilities, ACS provides records for use in billing and network audits.

Cisco Secure ACS enables you to manage administrators of devices such as Cisco IOS routers, virtual private networks (VPNs), firewalls, dialup and digital subscriber line (DSL) connections, cable access solutions, storage, content, VoIP, Cisco wireless solutions, and Cisco Catalyst switches using IEEE 802.1x access control. Cisco Secure ACS is also an important component of Cisco Admission Control (NAC).
CHAPTER 2
Trust and Identity

Authentication, Authorization, and Accounting

Authentication is the process of confirming the identity of a person or device that requests access to the network or for network resources. Authorization is the process of ensuring that authenticated users are allowed to perform the request based on policy. Accounting is the process of recording the activity of users or devices that have accessed the network.

TACACS+ and RADIUS

TACACS itself is an Internet Engineering Task Force (IETF) standard. TACACS+ is a Cisco proprietary extension to that standard and is TCP based and uses port 49. TACACS+ encrypts the entire body of the message that is sent between the network access server (NAS), which is the server that performs the authentication (in our case, Cisco Secure ACS), and the TACACS+ daemon that runs on the client device (IOS router, VPN concentrator, Adaptive Security Appliance [ASA], and so on). TACACS+ supports the use of Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and MS-CHAP, and also provides command authorization capabilities.

RADIUS is a protocol that was developed by Livingston Enterprises. RADIUS is now an IETF standard that can be found in RFC 2865. RADIUS is User Datagram Protocol (UDP) based and uses ports 1645 and 1646 in most implementations, although those ports are not assigned to the RADIUS protocol. RADIUS is assigned ports 1812 and 1813, and newer implementations will use these ports. Two ports are used because authentication and authorization are done together on port 1812 or 1645 depending on implementation, and accounting is done separately using port 1813 or 1645 depending on implementation.

Either TACACS+ or RADIUS is required for a Cisco IOS device to communicate AAA information between the Cisco Secure ACS server and itself. Your decision to use one over the other may include the type of device that you will be using for authentication; for example, non-Cisco equipment would not use TACACS+. Another reason for choosing one over the other might be the type of feature that you are implementing; for example, if you’re going to do command authorization, you need to use TACACS+; if you want to do downloadable IP access control lists (ACL), UDP is RADIUS.
Configuring TACACS+ and RADIUS

To enable the Cisco IOS device to communicate with the Cisco Secure ACS using TACACS+, follow these steps:

1. Globally enable AAA.
2. Specify AAA lists and methods.
3. Specify AAA server hosts' addresses.
4. Specify encryption keys used to encrypt data between the NAS and the AAA server.

The following configuration example first shows AAA being enabled on the SNRS router. It then shows an authentication method list for logins to the router using TACACS+. When users log in to the router, they will be authenticated with a username and password that is stored on the TACACS+ server. The TACACS+ server in this case is the Cisco Secure ACS server. Then in the configuration, authorization is configured using the `aaa authorization` and `exec` command. With this command, it instructs the router to check with the TACACS+ server and verify whether the user is allowed exact privileges. With the `aaa accounting` and `exec` command, accounting messages will be sent to the TACACS+ server, both when the session starts and when the session stops. The last two configuration lines define the protocol being used to communicate with the Cisco Secure ACS server as TACACS+. They also define the secret key that is used to encrypt the messages between the router and the AAA server:

```
SNRS_ROUTER(config)#aaa new-model
SNRS_ROUTER (config)#aaa authentication login default group tacacs+
SNRS_ROUTER (config)#aaa authorization exec default group tacacs+
SNRS_ROUTER (config)#aaa accounting exec default start-stop group tacacs+
SNRS_ROUTER (config)#tacacs-server key secretkey
SNRS_ROUTER (config)#tacacs-server host 172.26.10.1 ref
```

This is just a simple configuration example, but there is much more to be understood with AAA configurations. For a detailed discussion about AAA and the Cisco Secure ACS, refer to *Cisco Secure Access Control Security AAA Administrative Services*, by Brandon Carroll (Cisco Press).
To enable the Cisco IOS device to communicate with the Cisco Secure ACS using RADIUS, follow these steps:

1. Globally enable AAA.
2. Specify AAA lists and methods.
3. Specify AAA server hosts’ addresses.
4. Specify encryption keys used to encrypt data between the NAS and the AAA server.

The following configuration example is similar to the TACACS example shown previously. The difference with this example is that rather than using TACACS, we are using the RADIUS protocol for communication between the router and the AAA server:

```
SNRS_ROUTER(config)##aa new-model
SNRS_ROUTER (config)##aaa authentication login default group tacacs+
SNRS_ROUTER (config)##aaa authorization exec default group tacacs+
SNRS_ROUTER (config)##aaa accounting exec default start-stop group tacacs+
SNRS_ROUTER (config)##radius-server key secretkey
SNRS_ROUTER (config)##radius-server host 172.26.10.1 ref
```

You can find a number of configuration examples at the following site:


**Working in Cisco Secure ACS**

Cisco Secure ACS is an AAA server. In the preceding section, you enabled the IOS devices to communicate with the AAA server. In this section, you will enable the AAA server (in this case, Cisco Secure ACS) to communicate to the IOS device.
Just about any administration tasks can be performed in the Cisco Secure ACS web interface. You access the web interface by browsing to `http://<server address>:2002`. From the web interface, you can easily modify and view the Cisco Secure ACS configuration. Figure 2-1 shows the layout of the HTML interface.