Securing User Services Overview

First Published: June 5, 2009
Last Updated: June 5, 2009

The Securing User Services Overview document covers the topics of identifying users through the authentication, authorization, and accounting (AAA) protocol, controlling user access to remote devices and using security server information to track services on Cisco IOS networking devices.

Finding Feature Information

Your software release may not support all the features documented in this overveiw module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

AutoSecure

The AutoSecure feature simplifies the security configuration of a router and hardens the router configuration by disabling common IP services that can be exploited for network attacks and enable IP services and features that can aid in the defense of a network when under attack.

AutoSecure secures both the management and forwarding planes in the following ways:

- Securing the management plane is accomplished by turning off certain global and interface services that can be potentially exploited for security attacks and turning on global services that help mitigate the threat of attacks. Secure access and secure logging are also configured for the router.
- Securing the forwarding plane is accomplished by enabling Cisco Express Forwarding (CEF) or distributed CEF (dCEF) on the router whenever possible. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Thus, routers configured for CEF perform better under SYN attacks than routers using the traditional cache.

Authentication, Authorization, and Accounting

Cisco's authentication, authorization, and accounting (AAA) paradigm is an architectural framework for configuring a set of three independent security functions in a consistent, modular manner. AAA provides a primary method for authenticating users (for example, a username/password database stored on a TACACS+ server) and then specify backup methods (for example, a locally stored username/password database).The backup method is used if the primary method's database cannot be accessed by the networking device. To configure AAA, refer to the Authentication, Authorization, and Accounting chapters. You can configure up to four sequential backup methods.

Note If backup methods are not configured, access is denied to the device if the username/password database cannot be accessed for any reason.

The following sections discuss the AAA security functions in greater detail:

Authentication

Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. AAA authentication is configured by defining a named list of authentication methods and then applying that list to various interfaces.

Authorization

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, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (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

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 users are accessing, as well as the amount of network resources they are consuming.

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

Authentication Proxy

The Cisco IOS Firewall Authentication Proxy feature is used by network administrators to apply dynamic, per-user authentication and authorization security policies, which authenticates users in addition to industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks because users can be identified and authorized on the basis of their per-user policy.

Once the authentication proxy feature is implemented, users can log into the network or access the Internet through HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

Authentication proxy is compatible with other Cisco IOS security features such as Network Address Translation (NAT), Context-Based Access Control (CBAC), IP security (IPsec) encryption, and Cisco Secure VPN Client (VPN client) software.

802.1x Authentication Services

802.1x Authentication Services feature is used to configure local 802.1x port-based authentication and Virtual Private Network (VPN) access on Cisco integrated services routers (ISRs) through the IEEE 802.1X protocol framework. IEEE 802.1x authentication prevents unauthorized devices (supplicants) from gaining access to the network.

Cisco ISRs can combine the functions of a router, a switch, and an access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built-in switch ports or a plug-in module with switch ports.

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a port before making available any services offered by the device or the network.

Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Network Admission Control

The Cisco Network Admission Control (NAC) feature addresses the increased threat and impact of worms and viruses have on business networks. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.

NAC enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be made on the basis of information about the endpoint device, such as its current antivirus state, which includes information such as version of antivirus software, virus definitions, and version of scan engine.

NAC allows noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network. The key component of NAC is the Cisco Trust Agent (CTA), which resides on an endpoint system and communicates with Cisco routers on the network. The CTA collects security state information, such as what antivirus software is being used, and communicates this information to Cisco routers. The information is then relayed to a Cisco Secure Access Control Server (ACS) where access control decisions are made. The ACS directs the Cisco router to perform enforcement against the endpoint.

Security Server Protocols

AAA security protocols are used on a router or network access server administers its security functions. AAA is the means through which communication is established between the network access server and Cisco supported RADIUS and TACACS+ security server protocols.

If the database on a security server is used to store login username/password pairs, the router or access server must be configured to support the applicable protocol; in addition, because most supported security protocols must be administered through the AAA security services, AAA must be enabled.

The following sections discuss the RADIUS and TACACS+ security server protocols in greater detail:

- RADIUS, page 5
- TACACS+, page 5

RADIUS

The RADIUS distributed client/server system is implemented through the AAA protocol. RADIUS 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.

TACACS+

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

The protocol was designed to scale as networks grow and to adapt to new security technology. The underlying architecture of the TACACS+ protocol complements the independent AAA architecture.

RADIUS and TACACS+ Attributes

There are various vendor interpretations of the RADIUS and TACACS+ RFCs. Although different vendors can be in compliance with any RFC does not guarantee interoperability. Interoperability is guaranteed only if standard RFCs are used for the RADIUS and TACACS+ protocols.

When nonstandard RADIUS and TACACS+ RFCs are used, attributes must be developed and implemented by vendors so that their respective devices can interoperate with each other.

The following sections discuss the RADIUS and TACACS+ attributes in greater detail:

- RADIUS Attributes, page 5
- TACACS+ Attributes, page 5

RADIUS Attributes

RADIUS attributes are used to define specific AAA elements in a user profile, which is stored on the RADIUS daemon.

TACACS+ Attributes

TACACS+ attribute-value pairs are used to define specific AAA elements in a user profile, which is stored on the TACACS+ daemon.

Secure Shell

The Secure Shell (SSH) feature is an application and a protocol that provides a secure replacement to a suite of UNIX r-commands such as rsh, rlogin and rcp. (Cisco IOS supports rlogin.) The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2.

Cisco IOS Login Enhancements

The Cisco IOS Login Enhancements (Login Block) feature allows users to enhance the security of a router by configuring options to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected.

The login block and login delay options introduced by this feature can be configured for Telnet or SSH virtual connections. By enabling this feature, you can slow down "dictionary attacks" by enforcing a "quiet period" if multiple failed connection attempts are detected, thereby protecting the routing device from a type of denial-of-service attack.

Cisco IOS Resilient Configuration

The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash).

Image Verification

Image Verification feature allows users to automatically verify the integrity of Cisco IOS images. Thus, users can be sure that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

IP Source Tracker

The IP Source Tracker feature allows information to be gathered about the traffic to a host that is suspected of being under attack. This feature also allows you to easily trace an attack to its entry point into the network.

Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

Security with Passwords, Privileges, and Login Usernames for CLI Sessions on Networking Devices

There are conditions where networking devices are installed on the network with no security options configured, or a networking device is installed and help is needed to understand how baseline of security is implemented on the Cisco IOS CLI operating system session running on the networking device.

In this document, the following basic security topics are discussed:

- Different levels of authorization for CLI sessions can be differentiated to control access to commands that can modify the status of the networking device versus commands that are used to monitor the device
- Passwords can be assigned to CLI sessions
- Users can be required to log in to a networking device with a username
- Privilege levels of commands can be changed to create new authorization levels for CLI sessions

Kerberos

The Kerberos feature is a secret-key network authentication protocol implemented through AAA that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources and is based on the concept of a trusted third-party that performs secure verification of users and services. It is primarily used to verify that users and the network services they use are really who and what they claim to be. To accomplish this verification, a trusted Kerberos server issues tickets that have a limited lifespan, are stored in a user's credential cache, and can be used in place of the standard username-and-password authentication mechanism.

Lawful Intercept

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies to provide the ability to intercept Voice over IP (VoIP) or data traffic going through the edge routers. The Lawful Intercept (LI) architecture includes the Cisco Service Independent Intercept architecture and PacketCable Lawful Intercept architecture.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.