AAA Support for Cisco TrustSec

Last Updated: July 11, 2011

Cisco TrustSec (CTS) is a system that provides security for CTS-enabled network devices at each routing hop. In this system, each network device works to authenticate and authorize its neighbor devices and next applies some level of security (group tagging, role-based access control lists (ACLs), encryption, and so on) to traffic between the devices.

The AAA Support for CTS feature involves using Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering. Secure RADIUS uses automatic Protected Access Credential (PAC) provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling (EAP-FAST) to establish a Transport Layer Security (TLS) tunnel in which client credentials are verified.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for AAA Support for Cisco TrustSec

- The network topology requires a minimum of two switches, both of which must be enabled and configured with the CTS Network Device Admission Control (NDAC). NDAC provides AAA services that prohibit rogue devices on the network. Devices such as Ethernet switches in the data center are authenticated by neighboring infrastructure devices to establish trust before these devices are allowed to connect to the trusted network.
- The Cisco Secure Access Control Server (ACS) Express Appliance server is required for authentication. AAA server enhancements are required to support the entire CTS solution.
- Configuring AAA support for CTS on a single device does not affect the operation of the individual device, and the support is dormant until the complete CTS solution is connected and configured.
- The devices must be 802.1x enabled. The IEEE 802.1x standard allows or denies network access based on the security state of the device.

Information About AAA Support for Cisco TrustSec

Secure RADIUS

The RADIUS protocol requires a secret to be shared between a client and a server. Shared secrets are used to verify that RADIUS messages are sent by a RADIUS enabled device that is configured with the same shared secret. Shared secrets also verify that the RADIUS message has not been modified in transit (message integrity). The message integrity is checked by including the Message Authenticator attribute in the RADIUS messages. This attribute is a Hash-based Message Authentication Code-Message Digest 5 (HMAC-MD5) of the entire radius message using the shared secret as the key. The shared secret is also used to encrypt some RADIUS attributes, such as User-Password and Tunnel-Password.

EAP-FAST

EAP-FAST is a publicly accessible IEEE 802.1X extensible authentication protocol type that is used to support customers who cannot enforce a strong password policy. EAP-FAST is used for the following reasons:

- Digital certificates are not required.
- A variety of database types for usernames and passwords are supported.
- Password expiration and change are supported.
- EAP-FAST is flexible, easy to deploy and manage.

Note Lightweight Directory Access Protocol (LDAP) users cannot be automatically PAC provisioned and must be manually provisioned.

EAP-FAST comprises three basic phases:

- Phase 0 (optional): the PAC is initially distributed to the client.
- Phase 1: using the PAC, a secure tunnel is established.
- Phase 2: the client is authenticated via the secure tunnel.

The initial Phase 0 or auto-provisioning (also called in-band provisioning) component of EAP-FAST permits the secure distribution of the user PAC to each client. With some other authentication protocols, it is necessary to establish a network connection or manually install a file in order to distribute credentials to the user. Phase 0 in EAP-FAST permits a user PAC to be distributed to the client during an encrypted session after the user's credentials are authenticated. This user authentication uses a challenge-handshake protocol to authenticate the client and to validate the server response. This authentication mechanism guards against potential interception and reforwarding of provisioning requests for the purpose of intercepting a user PAC.

Note Phase 0 is optional in EAP-FAST. PAC files may also be manually generated at the PAC server and distributed manually to client devices (this process is called manual or out-of-band provisioning). Because auto provisioning uses Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2), it may be necessary to use manual provisioning if you use a non-Microsoft-format database such as LDAP, which does not support MSCHAPv2 credentials.

The end result of Phase 0 is PAC distribution, not client authentication. After successful PAC distribution, the server issues an authentication failure to the access point and the user is disassociated from the network. Then the client reinitiates an EAP-FAST authentication with the network using the newly provisioned PAC and the user's credentials.

After the optional Phase 0, the actual EAP-FAST authentication starts with Phase 1. In the Phase 1 EAP-FAST authentication transaction, a secure tunnel is established between the user and the EAP-FAST-capable RADIUS server using the user's PAC credential with TLS protocol.

During the initial authentication request, the server sends its Authority ID (A-ID). The client selects the correct PAC from its storage by correlating the provided A-ID with its saved PACs and its respective PAC-Info fields.

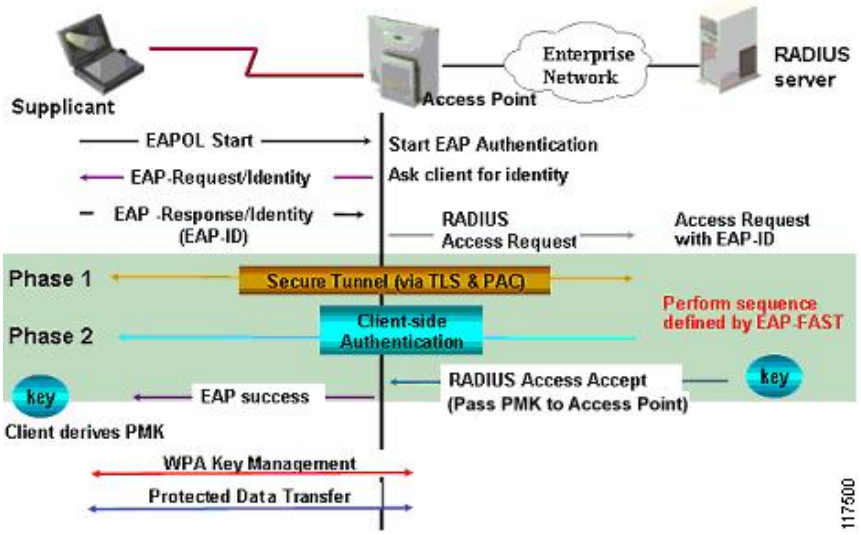
Note The client sends only the PAC-Opaque field to the server, not the PAC key. The server decrypts the PAC-Opaque field using its master key. As the server and client now share the PAC key, the PAC key is used to create the unique TLS tunnel for this client's authentication.

After the TLS tunnel is established using the PAC, user authentication credentials are passed securely using the Extensible Authentication Protocol-Generic Token Card (EAP-GTC) protocol within the encrypted tunnel to the RADIUS server (Phase 2).

Note The client response is cryptographically bound to the EAP authentication success message. This prevents a Man-In-The-Middle (MITM) attack in which the attacker (client) attempts to provide a false response to the server in order to obtain the session key.

After the successful Phase 2 authentication of the client to the EAP-FAST server, a RADIUS Access-Accept message is passed to the access point (along with the master session key). An EAP success message is generated at the access point (as with other EAP authentication protocols). Upon receipt of the EAP-success packet, the client derives the session key using a complimentary algorithm used at the server to generate the session key passed to the access point. This key permits the client and access point to establish a unique session key using the defined encryption mechanism (Wi-Fi Protected Access (WPA) authentication key management, Cisco Centralized Key Management (CCKM), or standard 802.11 Wired Equivalent Privacy (WEP) keying.

The figure below shows an overview of EAP-FAST authentication.



PAC

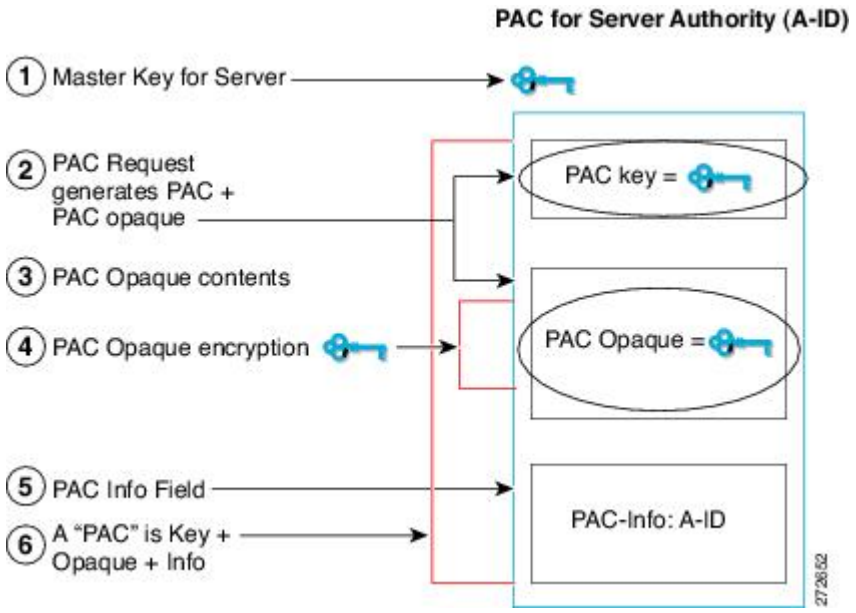
The PAC is a unique shared credential used to mutually authenticate client and server. It is associated with a specific client username and a server A-ID. A PAC removes the need for Public Key Infrastructure (PKI) and digital certificates.

Creating a PAC consists of the following steps:

1. Server A-ID maintains a local key (master key) that is only known by the server.
2. When a client identity (I-ID) requests a PAC from the server, the server generates a randomly unique PAC key and PAC-Opaque field for this client.
3. The PAC-Opaque field contains the randomly generated PAC key along with other information such as user identity (I-ID) and key lifetime.
4. PAC Key, I-ID, and Lifetime in the PAC-Opaque field are encrypted with the master key.
5. A PAC-Info field that contains the A-ID is created.
6. The PAC is distributed or imported to the client automatically or manually.

Note The server does not maintain the PAC or the PAC key, enabling the EAP-FAST server to be stateless.

The figure below describes the PAC's construction. A PAC consists of the PAC-Opaque, PAC Key and PAC-Info fields. The PAC-Info field contains the A-ID.



PAC Provisioning

In Secure RADIUS, the PAC key is provisioned into each device during authentication to derive the shared secret. Since the RADIUS ACS does not store the PAC key for each device, the clients must also send an additional radius attribute containing the PAC-Opaque field, which is a variable length field that is sent to the server when the TLS tunnel is being established. The PAC-Opaque field can only be interpreted by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque field may include the PAC key and the PAC's peer identity.

The PAC-Opaque field format and contents are specific to the PAC server on which it is issued. The RADIUS server obtains the PAC Key from the PAC-Opaque field and derives the shared secret the same way clients do. Secure RADIUS only modifies the way shared secret is derived and not its usage.

EAP-FAST offers two options to provision a client with a PAC:

- Automatic PAC provisioning (EAP-FAST Phase 0 or in-band PAC provisioning)
- Manual (out-of-band) PAC provisioning

Manual PAC provisioning generates the PAC file locally on the ACS server. With manual provisioning, the user credentials are supplied to the server to generate the PAC file for that user. This PAC must then be manually installed on the client device.

How to Provide AAA Support for Cisco TrustSec

- Configuring Secure RADIUS Automatic PAC Provisioning, page 6

Configuring Secure RADIUS Automatic PAC Provisioning

In seed devices, also known as core switches, the PAC-Opaque field has to be provisioned so that all radius exchanges can use the PAC-Opaque field to make the server it communicates with capable of automatic PAC provisioning. All nonseed devices obtain the PAC-Opaque field during the authentication phase of a link initialization.

A PAC-Opaque field is a variable length field that is sent to the server during the TLS tunnel establishment phase. The PAC-Opaque field can only be interpreted by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque field may include the PAC Key and the PAC's peer identity. The PAC-Opaque field format and contents are specific to the issuing PAC server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** *ip-address* **auth-port** *port* **acct-port** port {**pac** | **key** *encryption-key*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server host** *ip-address* **auth-port** *port* **acct-port** port {**pac** | **key** *encryption-key*} **Example:** `Router(config)#radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac`	Configures automatic PAC provisioning to be triggered. **Note** The **pac** keyword is mutually exclusive with the shared secret **key**keyword which already exists.

Note Automatic PAC Provisioning can also be triggered by Secure RADIUS when the server has no PAC or when an Access-Reject message is received from the Autonomous System (AS) says "PAC Expired".

Configuration Examples for Providing AAA Support for Cisco TrustSec

Secure RADIUS Automatic PAC Provisioning Example

The following example configures automatic PAC provisioning on a router:

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

Additional References

Related Documents

Related Topic	Document Title
EAP Flexible Authentication via Secured Tunnel (EAP-FAST) authentication protocol deployment in wireless networks	EAP-FAST Deployment Guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for AAA Support for Cisco TrustSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1 Feature Information for AAA Support for Cisco TrustSec

Feature Name	Releases	Feature Information
AAA Support for CiscoTrusted Sec	12.2(33)SXI	The IOS AAA support for Cisco TrustSec feature involves using secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering. Secure RADIUS uses automatic PAC provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with EAP-FAST to establish a TLS tunnel in which client credentials are verified. In release12.2(33)SXI, this feature was introduced on Cisco IOS software. The following command was modified: **radius-server host**