Source Interface Selection for Outgoing Traffic with Certificate Authority

The Source Interface Selection for Outgoing Traffic with Certificate Authority feature allows you to specify that the address of an interface be used as the source address for all outgoing TCP connections associated with that trustpoint when a designated trustpoint has been configured.

Information About Source Interface Selection for Outgoing Traffic with Certificate Authority

Certificates That Identify an Entity

Certificates can be used to identify an entity. A trusted server, known as the certification authority (CA), issues the certificate to the entity after determining the identity of the entity. A router that is running Cisco IOS XE software obtains its certificate by making a network connection to the CA. Using the Simple Certificate Enrollment Protocol (SCEP), the router transmits its certificate request to the CA and receives the granted certificate. The router obtains the certificate of the CA in the same manner using SCEP. When validating a certificate from a remote device, the router may again contact the CA or a Lightweight Directory Access Protocol (LDAP) or HTTP server to determine whether the certificate of the remote device has been revoked. (This process is known as checking the certificate revocation list [CRL].)

Note Depending on your Cisco IOS release, LDAP is supported.

In some configurations, the router may make the outgoing TCP connection using an interface that does not have a valid or routable IP address. The user must specify that the address of a different interface be used as the source IP address for the outgoing connection. Cable modems are a specific example of this requirement because the outgoing cable interface (the RF interface) usually does not have a routable address. However, the user interface (usually FastEthernet) does have a valid IP address.

Source Interface for Outgoing TCP Connections Associated with a Trustpoint

The **crypto pki trustpoint** command is used to specify a trustpoint. The **source interface**command is used along with the **crypto pki trustpoint**command to specify the address of the interface that is to be used as the source address for all outgoing TCP connections associated with that trustpoint.

Note If the interface address is not specified using the **source interface**command, the address of the outgoing interface is used.

How to Configure Source Interface Selection for Outgoing Traffic with Certificate Authority

Configuring the Interface for All Outgoing TCP Connections Associated with a Trustpoint

Perform this task to configure the interface that you want to use as the source address for all outgoing TCP connections associated with a trustpoint.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **source interface** *interface-address*
6. **interface** *type slot / port*
7. **description** *string*
8. **ip address** *ip-address mask*
9. **interface** *type slot / port*
10. **description** *string*
11. **ip address** *ip-address mask*
12. **crypto map** *map-name*

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	**crypto pki trustpoint** *name* **Example:** `Router (config)# crypto pki trustpoint ms-ca`	Declares the Certificate Authority (CA) that your router should use and enters ca-trustpoint configuration mode.
Step 4	**enrollment url** *url* **Example:** `Router (ca-trustpoint)# enrollment url http://yourname:80/certsrv/mscep/mscep.dll`	Specifies the enrollment parameters of your CA.
Step 5	**source interface** *interface-address* **Example:** `Router (ca-trustpoint)# interface fastethernet1/0`	Interface to be used as the source address for all outgoing TCP connections associated with that trustpoint.
Step 6	**interface** *type slot / port* **Example:** `Router (ca-trustpoint)# interface fastethernet1/0`	Configures an interface type and enters interface configuration mode.
Step 7	**description** *string* **Example:** `Router (config-if)# description inside interface`	Adds a description to an interface configuration.
Step 8	**ip address** *ip-address mask* **Example:** `Router (config-if)# ip address 10.1.1.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 9	**interface** *type slot / port* **Example:** `Router (config-if)# interface fastethernet1/0`	Configures an interface type.

	Command or Action	Purpose
Step 10	**description** *string* **Example:** `Router (config-if)# description outside interface 10.1.1.205 255.255.255.0`	Adds a description to an interface configuration.
Step 11	**ip address** *ip-address mask* **Example:** `Router (config-if)# ip address 10.2.2.205 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 12	**crypto map** *map-name* **Example:** `Router (config-if)# crypto map mymap`	Applies a previously defined crypto map set to an interface.

Troubleshooting Tips

Ensure that the interface specified in the command has a valid address. Attempt to ping the router using the address of the specified interface from another device (possibly the HTTP or LDAP server that is serving the CRL). You can do the same thing by using a traceroute to the router from the external device.

You can also test connectivity between the router and the CA or LDAP server by using Cisco IOS XE command-line interface (CLI). Enter the **ping ip**command and respond to the prompts. If you answer “yes” to the “Extended commands [n]:” prompt, you will be able to specify the source address or interface.

In addition, you can use Cisco IOS XE CLI to input a traceroute command. If you enter the **traceroute ip** command (in EXEC mode), you will be prompted for the destination and source address. You should specify the CA or LDAP server as the destination and the address of the interface that you specified in the “source interface” as the source address.

Configuration Examples for Source Interface Selection for Outgoing Traffic with Certificate Authority

Source Interface Selection for Outgoing Traffic with Certificate Authority Example

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. FastEthernet 1 is the “outside” interface that connects to the Internet Service Provider (ISP). FastEthernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office, the router must send its IP datagrams out interface FastEthernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, the CA does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto pki trustpoint ms-ca
 enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
 source interface fastethernet0
!
interface fastethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface fastethernet 1
 description outside interface
 ip address 10.2.2.205 255.255.255.0
 crypto map main-office
```

Additional References

The following sections provide references related to the Source Interface Selection for Outgoing Traffic with Certificate Authority feature.

Related Documents

Related Topic	Document Title
Configuring IPSec and certification authority	Security for VPNs with IPsec
IPSec and certification authority commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature.	-

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	-

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Source Interface Selection for Outgoing Traffic with Certificate Authority

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 Source Interface Selection for Outgoing Traffic with Certificate Authority

Feature Name	Releases	Feature Information
Source Interface Selection for Outgoing Traffic with Certificate Authority.	Cisco IOS XE Release 2.1	This feature allows you to specify that the address of an interface be used as the source address for all outgoing TCP connections associated with that trustpoint when a designated trustpoint has been configured. The following command was introduced: **source interface**.

Glossary

authenticate--Toprove the identity of an entity using the certificate of an identity and a secret that the identity poses (usually the private key corresponding to the public key in the certificate).

CA --Certificate Authority. A CA is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

CA authentication --The user manually approves a certificate from a root CA. Usually a fingerprint of the certificate is presented to the user, and the user is asked to accept the certificate based on the fingerprint. The certificate of a root CA is signed by itself (self-signed) so that it cannot be automatically authenticated using the normal certificate verification process.

CRL --certificate revocation list. A CRL is a data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire.

enrollment --A router receives its certificate via the enrollment process. The router generates a request for a certificate in a specific format (known as PKCS #10). The request is transmitted to a CA, which grants the request and generates a certificate encoded in the same format as the request. The router receives the granted certificate and stores it in an internal database for use during normal operations.

certificate --A data structure defined in International Organization for Standardization (ISO) standard X.509 to associate an entity (machine or human) with the public key of that entity. The certificate contains specific fields, including the name of the entity. The certificate is normally issued by a CA on behalf of the entity. In this case the router will act as its own CA. Common fields within a certificate include the distinguished name (DN) of the entity, the DN of the authority issuing the certificate, and the public key of the entity.

LDAP --Lightweight Directory Access Protocol. A LDAP is a protocol that provides access for management and browser applications that provide read-and-write interactive access to the X.500 directory.