



Source Interface Selection for Outgoing Traffic with Certificate Authority

First Published: March 17, 2003
Last Updated: March 31, 2011

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

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 for Source Interface Selection for Outgoing Traffic with Certificate Authority”](#) section on page 7.

Use Cisco Feature Navigator to find information about platform support and Cisco 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

- [Information About Source Interface Selection for Outgoing Traffic with Certificate Authority, page 2](#)
- [How to Configure Source Interface Selection for Outgoing Traffic with Certificate Authority, page 2](#)
- [Configuration Examples for Source Interface Selection for Outgoing Traffic with Certificate Authority, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 8](#)



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

Information About Source Interface Selection for Outgoing Traffic with Certificate Authority

To configure the Source Interface Selection for Outgoing Traffic with Certificate Authority feature, you must understand the following concepts:

- [Certificates That Identify an Entity, page 2](#)
- [Source Interface for Outgoing TCP Connections Associated with a Trustpoint, page 2](#)

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 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].)

In some configurations, the router may make the outgoing TCP connection using an interface that does not have a valid or IP address that can be routed. 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 an IP address that can be routed. However, the user interface (usually Ethernet) does have a valid IP address.

Source Interface for Outgoing TCP Connections Associated with a Trustpoint

The **crypto ca trustpoint** command is used to specify a trustpoint. The **source interface** command is used along with the **crypto ca 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

This section includes the following procedure:

- [Configuring the Interface for All Outgoing TCP Connections Associated with a Trustpoint, page 3](#)

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 ca 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. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ca trustpoint <i>name</i> Example: Router (config)# crypto ca trustpoint ms-ca	Declares the Certificate Authority (CA) that your router should use and enters ca-trustpoint configuration mode.
Step 4	enrollment url <i>url</i> Example: Router (ca-trustpoint)# enrollment url http://yourname:80/certsrv/mscep/mscep.dll	Specifies the enrollment parameters of your CA.

	Command or Action	Purpose
Step 5	source interface <i>interface-address</i> Example: Router (ca-trustpoint)# interface ethernet 0	Interface to be used as the source address for all outgoing TCP connections associated with that trustpoint.
Step 6	interface <i>type slot/port</i> Example: Router (ca-trustpoint)# interface ethernet 1	Configures an interface type and enters interface configuration mode.
Step 7	description <i>string</i> Example: Router (config-if)# description inside interface	Adds a description to an interface configuration.
Step 8	ip address <i>ip-address mask</i> 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 <i>type slot/port</i> Example: Router (config-if)# interface ethernet1/0	Configures an interface type.
Step 10	description <i>string</i> 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 <i>ip-address mask</i> 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 <i>map-name</i> 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 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 can specify the source address or interface.

In addition, you can use Cisco IOS CLI to input a **traceroute** command. If you enter the **traceroute ip** command (in EXEC mode), you are 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

This section includes the following example:

- [Source Interface Selection for Outgoing Traffic with Certificate Authority Example, page 5](#)

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. Ethernet 1 is the “outside” interface that connects to the Internet Service Provider (ISP). Ethernet 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 Ethernet 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 ca trustpoint ms-ca
  enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
  source interface ethernet0
!
interface ethernet 0
  description inside interface
  ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
  description outside interface
  ip address 10.2.2.205 255.255.255.0
  crypto map main-office
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
Configuring IPSec and certification authority	<i>Security for VPNs with IPsec</i>
IPSec and certification authority commands	<i>Cisco IOS Security Command Reference</i>

MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 Source Interface Selection for Outgoing Traffic with Certificate Authority

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 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.

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	12.2(15)T	<p>This feature allows the IP address of an interface to be specified and used as the source address for all outgoing TCP connections associated with that trustpoint when a designated trustpoint has been configured.</p> <p>This feature was introduced in Cisco IOS Release 12.2(15)T.</p> <p>The following command was introduced or modified: source interface.</p>

Glossary

authenticate—To prove 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 through 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 acts 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

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

© 2007–2011 Cisco Systems, Inc. All rights reserved.