SSL VPN - IPv6 Support

The SSL VPN - IPv6 Support feature implements support for IPv6 transport over IPv4 SSL VPN session between a client, such as Cisco AnyConnect Mobility Client, and SSL VPN.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 SSL VPN - IPv6 Support

- The **ipv6 unicast-routing** command must be enabled globally.

Note This feature is supported on the Cisco CSR 1000V Series Cloud Services Router only.

Information About SSL VPN - IPv6 Support

IPv6 for SSL VPN

The SSL VPN - IPv6 Support feature implements an dual stack IPv6 over IPv4 session between a client, such as Cisco AnyConnect Mobility Client, and SSL VPN. An IPv6 session is activated on SSL VPN when the following commands in the SSL authorization policy:

- **ipv6 dns**
- **ipv6 pool**
- **ipv6 prefix**
- **ipv6 route**

1. When Cisco AnyConnect Mobility Client sends a connection request for a session, SSL VPN checks whether the request pertains to a new session or a session reconnect or rekey. If the request pertains to an existing session and an IPv6 address is already associated and allocated to the session, the allocated IPv6 address is used. If there is no associated IPv6 address, the value of the framed address RADIUS attribute is sent to the client or an IPv6 address is assigned from the IPv6 pool.

Note When SSL VPN receives a connection request from a client, an IPv6 session is triggered when the client sends the **X-CSTP-Full-IPv6-Capability: true** message as a part of the connection request. This prevents from sending unsupported IPv6 attributes to the client.

2. After an IPv6 address is allocated, the IPv6 session hash is added to the IPv6 hash table. The session hash is created based on the IPv6 address of the tunnel and looked up via the address and the VRF. If the hash is not inserted to the table, the session is disabled and an IPv4 session is established.
3. The static routes are added to the virtual access interface for the tunnel IP addresses. The IPv6 routes are added first followed by the IPv4 routes. If IPv6 route addition fails, the IPv6 session is disabled. If both IPv6 and IPv4 route additions fail, the session is aborted.
4. A response containing the IPv4 attributes and the IPv6 tunnel address, prefix length, split tunnel IPv6 routes, IPv6 DNS servers (primary and secondary) are pushed to the client, from the gateway indicating that the session is up.
5. On receiving the response, the client creates an adaptor and assigns an IP address to the adaptor. All IPv6 packets are sent to the adaptor. The client adds and encrypts an 8-byte CSTP header and an SSL header, transporting the IPv6 packet to the gateway.
6. The gateway receives the IPv6 packet, decrypts, and sends the packet to SSL VPN. SSL VPN check the packet for control packet or data packet. If the packet is a data packet, the CSTP header is removed and the raw IPv6 packet is forwarded to the IPv6 queue to route it the virtual access interface.

   On Cisco CSR 1000V Series Cloud Services Router, the session is looked up based on the IPv6 address and the VRF to find the appropriate session from the session IPv6 hash table.

Supported RADIUS Attributes

The following RADIUS attribute-value pairs are available for IPv6 support on SSL VPN:

Table 1: Supported RADIUS Attributes

RADIUS Attribute	Description
cryptovpn-ssl:prefix-len	Sets the IPv6 prefix length for the session.
cryptovpn-ssl:ipv6-dns-servers-addr	Specifies the primary and secondary IPv6 DNS servers.
cryptovpn-ssl:route-set	Specifies the IPv6 access list to be pushed to the client.
cryptovpn-ssl:ipv6-addr-pool	Specifies the IPv6 tunnel address pool.
cryptovpn-ssl:ipv6_addr	Specifies the framed IPv6 address to be pushed to the client.

How to Configure SSL VPN - IPv6 Support

Configuring the SSL Authorization Policy

Perform this task to configure the SSL authorization policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ssl authorization policy** *policy-name*
4. **banner** *banner-text*
5. **client profile** *profile-name*
6. **def-domain** *domain-name*
7. Do one of the following:
   - **dns** *primary-server* [*secondary-server*]
   - **ipv6 dns** *primary-server* [*secondary-server*]
8. **dpd-interval** {**client** | **server**} *interval*
9. **homepage** *homepage-text*
10. **include-local-lan**
11. **ipv6 prefix** *prefix*
12. **keepalive** *seconds*
13. **module** *module-name*
14. **msie-proxy exception** *exception-name*
15. **msie-proxy option** {**auto** | **bypass** | **none**}

16. **msie-proxy server** {*ip-address* | *dns-name*}
17. **mtu** *bytes*
18. **netmask** *mask*
19. Do one of the following:
    - **pool** *name*
    - **ipv6 pool** *name*
20. **rekey time** *seconds*
21. Do one of the following:
    - **route set access-list** *acl-name*
    - **ipv6 route set access-list** *access-list-name*
22. **smartcard-removal-disconnect**
23. **split-dns** *string*
24. **timeout** {**disconnect** *seconds* | **idle** *seconds* | **session** *seconds*}
25. **wins** *primary-server* [*secondary-server*]
26. **end**
27. **show crypto ssl authorization policy** [*policy-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ssl authorization policy** *policy-name* **Example:** `Device(config)# crypto ssl authorization policy policy1`	Specifies the SSL authorization policy and enters SSL authorization policy configuration mode.
Step 4	**banner** *banner-text* **Example:** `Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel. NOTE: DO NOT dial emergency response numbers (e.g. 911,112) from software telephony clients. Your exact location and the appropriate emergency response agency may not be easily identified.`	Specifies the banner. The banner is displayed on successful tunnel set up.
Step 5	**client profile** *profile-name* **Example:** `Device(config-crypto-ssl-auth-policy)# client profile profile1`	Specifies the client profile. The profile must already be specified using the **crypto ssl profile** command.

	Command or Action	Purpose
Step 6	**def-domain** *domain-name* **Example:** `Device(config-crypto-ssl-auth-policy)# def-domain example.com`	Specifies the default domain. This parameter specifies the default domain that the client can use.

Step 7	Do one of the following:
	• **dns** *primary-server* [*secondary-server*]
	• **ipv6 dns** *primary-server* [*secondary-server*]
	Example:
	`Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100`
	Example:
	`Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2`
		Specifies an IPv4-or IPv6-based address for the primary and secondary Domain Name Service (DNS) servers.
		• *primary-server*—IP address of the primary DNS server.
		• *secondary-server*—(Optional) IP address of the secondary DNS server.

Step 8	**dpd-interval** {**client** | **server**} *interval* **Example:** `Device(config-crypto-ssl-auth-policy)# dpd-interval client 1000`	Configures Dead Peer Detection (DPD).globally for the client or server. • **client**—DPD for the client mode. The default value is 300 (five minutes). • **server**—DPD for the server mode. The default value is 300. • *interval*—Interval, in seconds. The range is from 5 to 3600.
Step 9	**homepage** *homepage-text* **Example:** `Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com`	Specifies the SSL VPN home page URL.
Step 10	**include-local-lan** **Example:** `Device(config-crypto-ssl-auth-policy)# include-local-lan`	Permits the remote user to access resources on a local LAN, such as a network printer.
Step 11	**ipv6 prefix** *prefix* **Example:** `Device(config-crypto-ssl-auth-policy)# ipv6 prefix 64`	Defines the IPv6 prefix for IPv6 addresses. • *prefix*—Prefix length. The range is from 1 to 128.
Step 12	**keepalive** *seconds* **Example:** `Device(config-crypto-ssl-auth-policy)# keepalive 500`	Enables setting the minimum, maximum, and default values for keepalive, in seconds.

	Command or Action	Purpose
Step 13	**module** *module-name* **Example:** `Device(config-crypto-ssl-auth-policy)# module gina`	Enables the server gateway to download the appropriate module for VPN to connect to a specific group. • **dart**—Downloads the AnyConnect Diagnostic and Reporting Tool (DART) module. • **gina**—Downloads the Start Before Logon (SBL) module.
Step 14	**msie-proxy exception** *exception-name* **Example:** `Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2`	The DNS name or the IP address specified in the *exception-name* argument that must not be sent via the proxy.
Step 15	**msie-proxy option** {**auto** | **bypass** | **none**} **Example:** `Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass`	Specifies the proxy settings for the Microsoft Internet Explorer browser. The proxy settings are required to specify an internal proxy server and to route the browser traffic through the proxy server when connecting to the corporate network. • **auto**—Browser is configured to auto detect proxy server settings. • **bypass**—Local addresses bypass the proxy server. • **none**—Browser is configured to not use the proxy server.
Step 16	**msie-proxy server** {*ip-address* | *dns-name*} **Example:** `Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2`	The IP address or the DNS name, optionally followed by the port number, of the proxy server. **Note** This command is required if the **msie-proxy option bypass** command is specified.
Step 17	**mtu** *bytes* **Example:** `Device(config-crypto-ssl-auth-policy)# mtu 1000`	(Optional) Enables setting the minimum, maximum, and default MTU value. **Note** The value specified in this command overrides the default MTU specified in Cisco AnyConnect Secure client configuration. If not specified, the value specified Cisco AnyConnect Secure client configuration is the MTU value. If the calculated MTU is less than the MTU specified in this command, this command is ignored.
Step 18	**netmask** *mask* **Example:** `Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0`	Specifies the netmask of the subnet from which the IP address is assigned to the client. • *mask*—Subnet mask address.

	Command or Action	Purpose

Step 19	Do one of the following:
	• **pool** *name*
	• **ipv6 pool** *name*
	Example:
	`Device(config-crypto-ssl-auth-policy)# pool abc`
	Example:
	`Device(config-crypto-ssl-auth-policy)# ipv6 pool ipv6pool`
		Defines a local IPv4 or IPv6 address pool for assigning IP addresses to the remote access client.
		• *name*—Name of the local IP address pool.
		Note The local IP address pool must already be defined using the **ip local pool** command.

Step 20	**rekey time** *seconds* **Example:** `Device(config-crypto-ssl-auth-policy)# rekey time 1110`	Specifies the rekey interval, in seconds. The default value is 3600.

Step 21	Do one of the following:
	• **route set access-list** *acl-name*
	• **ipv6 route set access-list** *access-list-name*
	Example:
	`Device(config-crypto-ssl-auth-policy)# route set access-list acl1`
	Example:
	`Device(config-crypto-ssl-auth-policy)# ipv6 route set access-list acl1`
		Establishes IPv4 or IPv6 routes via the access list that must be secured through tunnels.
		• *acl-name*—Access list name.

Step 22	**smartcard-removal-disconnect** **Example:** `Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect`	Enables smartcard removal disconnect and specifies that the client should terminate the session when the smart card is removed.
Step 23	**split-dns** *string* **Example:** `Device(config-crypto-ssl-auth-policy)# split-dns example.com example.net`	Allows you to specify up to ten split domain names, which the client should use for private networks.
Step 24	**timeout** {**disconnect** *seconds* | **idle** *seconds* | **session** *seconds*} **Example:** `Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000`	Specifies the timeout, in seconds. • **disconnect** *seconds*—Specifies the retry duration, in seconds, for Cisco AnyConnect client to reconnect to the server gateway. The default value is 0. • **idle** *seconds*—Specifies the idle timeout, in seconds. The default value is 1800 (30 minutes). • **session** *seconds*—Specifies the session timeout, in seconds. The default value is 43200 (12 hours).

	Command or Action	Purpose
Step 25	**wins** *primary-server* [*secondary-server*] **Example:** `Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115`	Specifies the internal Windows Internet Naming Service (WINS) server addresses. • *primary-server*—IP address of the primary WINS server. • *secondary-server*—(Optional) IP address of the secondary WINS server.
Step 26	**end** **Example:** `Device(config-crypto-ssl-auth-policy)# end`	Exits SSL authorization policy configuration mode and returns to privileged EXEC mode.
Step 27	**show crypto ssl authorization policy** [*policy-name*] **Example:** `Device(config-crypto-ssl-auth-policy)# show crypto ssl authorization policy`	(Optional) Displays the SSL authorization policy.

Verifying SSL Authorization Policy Configuration

Perform this task to verify the SSL authorization policy configuration.

SUMMARY STEPS

1. **enable**
2. **show crypto ssl authorization policy** [*name*]
3. **show crypto ssl stats** [**profile** *profile-name*] [**tunnel**] [**detail**]

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show crypto ssl authorization policy** [*name*]

Example:

```
Device# show crypto ssl authorization policy

SSL Auth Policy: pol1
 V6 Parameter:
   Address Pool: none
   Prefix: none
   Route ACL : ipv6acl
   DNS  :
```

```
    2001:DB8:1::1
    2001:DB8:2::2
 V4 Parameter:
   Address Pool: none
   Netmask: none
   Route ACL : none
   DNS  : none
   WINS : none
 Banner                  : none
 Home Page               : none
 Idle timeout            : 1800
 Disconnect Timeout      : 0
 Session Timeout         : 43200
 Keepalive Interval      : 30
 Client DPD Interval     : 300
 Gateway DPD Interval    : 300
 Rekey
   Interval: 3600
   Method  : none
 Split DNS: none
 Default domain          : none
 Proxy Settings
     Server: none
     Option: NULL
     Exception(s): none
 Anyconnect Profile Name :
 Module                  : none
 MAX MTU                 : 1406
 Smart Card
 Removal Disconnect      : NO
 Include Local LAN       : NO
 Disable Always On       : NO


SSL Auth Policy: sslauth
 V6 Parameter:
   Address Pool: sslvpn6
   Prefix: 120
   Route ACL : none
   DNS  : none
 V4 Parameter:
   Address Pool: sslvpn
   Netmask: 255.255.255.0
   Route ACL : sslvpn
   DNS  : none
   WINS : none
 Banner                  : none
 Home Page               : none
 Idle timeout            : 1800
 Disconnect Timeout      : 0
 Session Timeout         : 1000
 Keepalive Interval      : 30
 Client DPD Interval     : 300
 Gateway DPD Interval    : 300
 Rekey
   Interval: 3600
   Method  : none
 Split DNS: none
 Default domain          : none
 Proxy Settings
     Server: none
     Option: NULL
     Exception(s): none
 Anyconnect Profile Name :
```

```
Module                  : none
MAX MTU                 : 1406
Smart Card
Removal Disconnect      : NO
Include Local LAN       : NO
Disable Always On       : NO
```

Displays the SSL authorization policy.

Step 3 **show crypto ssl stats** [**profile** *profile-name*] [**tunnel**] [**detail**]

Example:

```
Device# show crypto ssl stats

SSLVPN Global statistics:
    Active connections       : 0          AAA pending reqs         : 0
    Peak connections         : 1          Peak time                : 1w6d
    Authentication failures  : 21
    VPN session timeout      : 1          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Login Denined            : 0
    Connect succeed          : 1          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
    IP Addr Alloc Failed     : 0          VA creation failed       : 0
    Route Insertion Failed   : 0
    IPV6 Addr Alloc Failed   : 0
    IPV6 Route Insert Failed : 0
    IPV6 Hash Insert Failed  : 0
    IPV6 STC Alloc Failed    : 0
    in  CSTP control         : 5          out CSTP control         : 3
    in  CSTP data            : 21         out CSTP data            : 8
```

Displays SSL VPN statistics.

Configuration Examples for SSL VPN - IPv6 Support

Example: Configuring SSL Authorization Policy

The following example shows how to configure an SSL authorization policy.

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile profile1
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
Device(config-crypto-ssl-auth-policy)# include-local-lan
Device(config-crypto-ssl-auth-policy)# keepalive 500
Device(config-crypto-ssl-auth-policy)# module gina
Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass
Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy)# mtu 1000
Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0
```

```
Device(config-crypto-ssl-auth-policy)# pool abc
Device(config-crypto-ssl-auth-policy)# rekey interval 1110
Device(config-crypto-ssl-auth-policy)# route set access-list acl1
Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy)# split-dns abc1
Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000
Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy)# end
```

The following example shows how to enable IPv6 support for SSL VPN.

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile profile1
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
Device(config-crypto-ssl-auth-policy)# include-local-lan
Device(config-crypto-ssl-auth-policy)# ipv6 prefix 64
Device(config-crypto-ssl-auth-policy)# ipv6 route set access-list acl1
Device(config-crypto-ssl-auth-policy)# keepalive 500
Device(config-crypto-ssl-auth-policy)# module gina
Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass
Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy)# mtu 1000
Device(config-crypto-ssl-auth-policy)# ipv6 pool ipv6pool
Device(config-crypto-ssl-auth-policy)# rekey interval 1110
Device(config-crypto-ssl-auth-policy)# route set access-list acl1
Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy)# split-dns abc1
Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000
Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy)# end
```

Example: Configuring SSL VPN with Local Authorization for IPv6 Session

Example: Configuring SSL VPN with Local Authorization on Cisco CSR 1000V Series Cloud Services Router

The following example shows how to configure IPv6 support for SSL VPN on Cisco CSR 1000V Series Cloud Services Router.

```
aaa new-model
!
aaa authentication login local-group-author-list local
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
enrollment url http://192.168.3.1:80
revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ssl proposal proposal1
```

```
 protection rsa-aes256-sha1
!
crypto ssl authorization policy author-policy1
 ipv6 prefix 64
 ipv6 pool v6-pool
 ipv6 dns  2001:DB8:1::11 2001:DB8:1::12
 ipv6 route set access-list subnet-acl v6-acl
!
crypto ssl policy policy1
 ssl proposal proposal1
 pki trustpoint trustpoint1 sign
 ip address local 121.0.0.92 port 443
!
crypto ssl profile profile1
 match policy policy1
 aaa authentication user-pass list local-group-author-list
 aaa authorization group user-pass list local-group-author-list author-policy1
 authentication remote user-credentials
!
interface Ethernet0/0
 ip address 121.0.0.92 255.255.255.0
 ipv6 address 2001:DB8:1::1/32
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
permit ipv6 host 2001:DB8:1::20 any
permit ipv6 host 2001:DB8:1::30 any
```

Additional References for SSL VPN - IPv6 Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z
Recommended cryptographic algorithms	Next Generation Encryption

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 SSL VPN - IPv6 Support

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 2: Feature Information for SSL VPN - IPv6 Support

Feature Name	Release	Feature Information
SSL VPN - IPv6 Support	Cisco IOS XE Release 3.15S	The SSL VPN - IPv6 Support feature implements support for IPv6 transport over IPv4 SSL VPN session between a client, such as Cisco AnyConnect Mobility Client, and SSL VPN. In Cisco IOS XE Release 3.15S, this feature was introduced on Cisco CSR 1000V Series Cloud Services Router. The following commands were introduced or modified: **ipv6 dns**, **ipv6 pool**, **ipv6 prefix**, **ipv6 route set**, **show crypto ssl authorization policy**, **show crypto ssl stats**.