SSL Host Peering Service Configuration Mode Commands

SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections. To configure secure socket layer (SSL) encryption peering services on a WAAS device, use the **crypto ssl services host-service peering** global configuration command. To delete a parameter use the **no** form of the command.

crypto ssl services host-service peering

no crypto ssl services host-service peering

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the **crypto ssl services host-service** command to configure SSL peering service parameters. The **crypto ssl services host-service** command initiates SSL host peering service configuration mode, as indicated by the following prompt:

```
WAE(config-ssl-peering)#
```

Within SSL host peering service configuration mode, you can use SSL host peering service configuration commands. To return to global configuration mode, enter **exit** at the SSL host peering service configuration mode prompt.

Examples

The following example shows how to enter SSL host peering service configuration mode:

```
WAE(config)# crypto ssl services host-service peering
WAE(config-ssl-peering)# exit
WAE(config)#
```

Related Commands

(config-ssl-peering) cipher-list

(config-ssl-peering) peer-cert-verify

(config-ssl-peering) version

(config-ssl-peering) cipher-list

To configure secure socket layer (SSL) encryption cipher lists on a WAAS device, use the **cipher-list** command. To delete a cipher list use the **no** form of the command.

cipher-list *cipher-list-name*

no cipher-list *cipher-list-name*

Syntax Description

cipher-list-name	Name of the cipher list you want to create or edit. The cipher list name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

SSL host peering service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

A cipher list is customer list of cipher suites that you assign to an SSL connection. (See the SSL Cipher List Configuration Mode Commands chapter for more information.)

Examples

The following example shows how to enter SSL host peering service configuration mode, and then create or edit a cipher list called myciphers. If the cipher list is already established on the WAAS device, the **cipher-list** command edits it. If the cipher list does not exist, the **cipher-list** command creates it:

```
WAE(config)# crypto ssl services management-service
WAE(config-ssl-peering)# cipher-list myciphers
```

Related Commands

(config) crypto ssl

(config-ssl-peering) peer-cert-verify

To enable verification of peer certificates, use the **peer-cert-verify** command.

peer-cert-verify [**revocation-check none**]

Syntax Description

revocation-check none	(optional) Specifies a revocation check null method that returns revocation success.

Defaults

No default behavior or values.

Command Modes

SSL host peering service configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections.

If peer certificate verification is enabled, WAAS devices that use self-signed certificates will not be able to establish peering connections to each other and, thus, not be able to accelerate SSL traffic.

To disable OCSP certificate revocation checking, set the revocation check value to none.

Examples

The following example shows how to enter SSL host peering service configuration mode, and then set the revocation check method to none:

```
WAE(config)# crypto ssl services host-service peering
WAE(config-ssl-peering)# peer-cert-verify revocation-check none
```

Related Commands

(config) crypto ssl

(config-ssl-peering) version

To specify the type of SSL protocol to use for management services, use the **version** command.

version {**all** | **ssl3** | **tls1**}

Syntax Description

version {**all** | **ssl3** | **tls1**}	Specifies SSL3 for the SSL version 3 protocol, TLS1 for the Transport Layer Security version 1 protocol, or All to use both SSL3 and TLS1 SSL protocols.

Defaults

No default behavior or values.

Command Modes

SSL host peering service configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to enter SSL host peering service configuration mode, and then set the protocol to SSL version 3:

```
WAE(config)# crypto ssl services host-service peering
WAE(config-ssl-peering)# version SSL3
```

Related Commands

(config) crypto ssl