Cisco Wide Area Application Services Software Version 4.1.3: SSL Application Acceleration Q&A

Cisco® Wide Area Application Services (WAAS) Software Version 4.1.3 adds support for SSL optimization. The SSL application optimizer provides the full benefits of Cisco WAAS data redundancy elimination (DRE), Lempel-Ziv (LZ) compression techniques, and transport flow optimization (TFO) for secure, web-based (HTTPS) services and other applications that use SSL as the underlying security protocol.

SSL provides data encryption, server authentication, message integrity, and optionally, client authentication. SSL uses X.509 certificates for authentication. Each certificate is signed either by a third-party certificate authority (CA; such as VeriSign), or by an internal enterprise authority, or enterprise CA. The clients and servers must trust these authorities to accept each other's signed certificates. This document answers SSL application optimization-related questions for Cisco WAAS 4.1.3.

Performance

Q. What benefit does Cisco WAAS 4.1.3 provide over previous versions for HTTPS web-based applications?

A. Previous Cisco WAAS versions provided only TFO for secure applications running over HTTPS/SSL. The encryption applied to secure the data traveling between the client and the server limits the ability of Cisco WAAS to apply the added benefit of DRE and persistent LZ data compression. The new Cisco WAAS 4.1.3 SSL application optimizer now adds the capability to decrypt and encrypt SSL traffic between the client and server so that the decrypted clear-text data can be optimized using Cisco WAAS DRE and persistent LZ techniques, providing significant bandwidth savings for subsequent retransmissions. The Cisco WAAS SSL application optimizer can provide immediate improvements for secure web-based enterprise applications such as SAP, Oracle, Siebel, SharePoint, and Microsoft Outlook Web Access running over HTTPS. The Cisco WAAS optimizations are transparent and automatic and do not require any configuration changes to either the client or server environment. The Cisco WAAS SSL solution fully preserves the existing enterprise security architecture.

Q. How does Cisco WAAS 4.1.3 accelerate secure web-based applications?

A. Cisco WAAS 4.1.3 accelerates SSL web-based applications by using the new Cisco SSL application optimizer. By adding the capability to encrypt and decrypt SSL traffic, the Cisco WAAS SSL application optimizer can now provide the full benefits of Cisco WAAS DRE, persistent LZ data compression, and TFO to SSL traffic between the client and server.

Q. What changes to the SSL web-based application are required to work with Cisco WAAS 4.1.3 SSL application optimizer?

A. The Cisco WAAS 4.1.3 SSL application optimizer does not require any changes to the web client or server applications and is fully transparent in operation.

Q. Does the Cisco WAAS 4.1.3 SSL application optimizer handle all versions of SSL?

A. The Cisco WAAS SSL application optimizer handles both SSL Version 3 (SSLv3) and Transport Layer Security (TLS) Version 1 (TLSv1) protocols. It will bypass requests that use SSLv2 and TLSv1.1 and v1.2

Q. What is the maximum number of SSL accelerated services that can be configured on a core Cisco Wide Area Application Engine (WAE)?

A. Currently Cisco WAAS 4.1.3 supports a maximum of 128 aggregated SSL accelerated services. Each SSL accelerated services requires a separate SSL certificate. Using wildcard certificates, each aggregated service can potentially support an unlimited number of back-end SSL services that run on a single port (for instance, 443). Additionally, if needed, each service can use up to 32 different ports using a single aggregated service.

Q. What is the maximum number of CA certificates that can be configured on a core Cisco Wide Area Application Engine (WAE)?

A. Currently Cisco WAAS 4.1.3 supports a maximum of 256 CA certificates that can be imported into the CA certificate store on the Cisco WAE device. This includes the well-known CA certificates as well.

Configuration

Q. Which Cisco WAAS devices do I need to enable the Cisco WAAS SSL application optimizer in Cisco WAAS 4.1.3? What type of license is required to enable the SSL application optimizer?

A. The Cisco WAAS SSL application optimizer must be enabled on both core and edge Cisco WAAS devices, either from the Cisco WAAS Central Manager or the individual device's command-line interface (CLI), to apply full optimization for web-based applications using HTTPS. The SSL application optimizer requires that the Enterprise license be enabled on the Cisco WAAS device before the SSL application optimizer can be enabled.

Q. What are the minimum configuration steps required to enable an SSL accelerated service in Cisco WAAS 4.1.3?

A. To accelerate any HTTPS application using the Cisco WAAS SSL application optimizer, the following are the minimum configuration steps required. This procedure assumes that the Enterprise license has been enabled on both the edge and core Cisco WAAS devices.

Step 1. Open and initialize the Cisco WAAS Central Manager secure store.

Step 2. Register the edge and core Cisco WAAS devices with the Cisco WAAS Central Manager.

Step 3. Check that the SSL application optimizer is enabled on both the edge and core Cisco WAE devices.

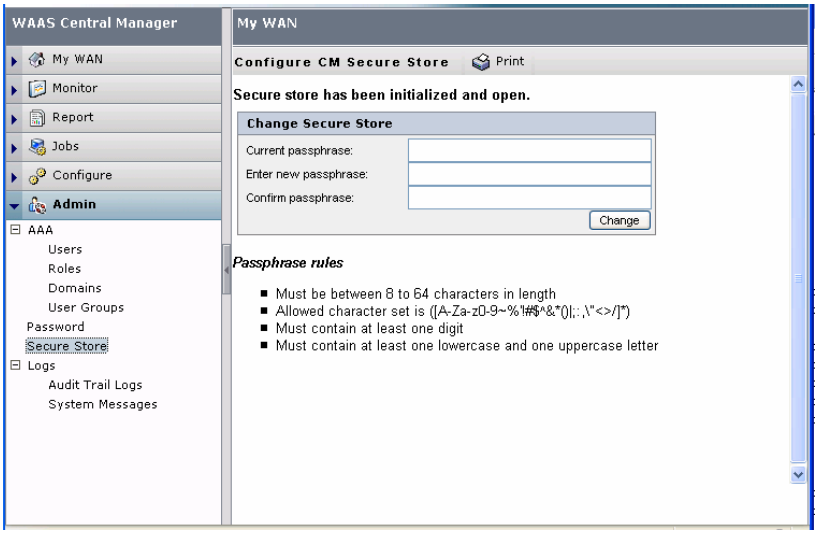
Step 4. Configure and enable an SSL accelerated service on the core Cisco WAE device.

Q. What is the secure store used for in the Cisco WAAS Central Manager?

A. The Cisco WAAS Central Manager's secure store is used to securely store all imported and generated SSL certificates and private keys associated with SSL host or accelerated services. Before it can be used for the first time, the secure store on the Cisco WAAS Central Manager must be initialized. To initialize and open the Cisco WAAS Central Manager secure store, from the Cisco WAAS Central Manager GUI, go to the WAAS Central Manager homepage. On the homepage, from the navigation pane, choose **Admin > Secure Store** and enter the passphrase to initialize and open the Cisco WAAS Central Manager secure store for the first time. To reopen the Cisco WAAS Central Manager secure store each time after the Cisco WAAS Central Manager is rebooted, enter the same passphrase that was entered the first time the secure store was initialized.

Figure 1 shows the Cisco WAAS Central Manager secure store in the open state.

Figure 1. Cisco WAAS Central Manager Secure Store



To initialize the secure store, use the **cms secure-store** CLI command:

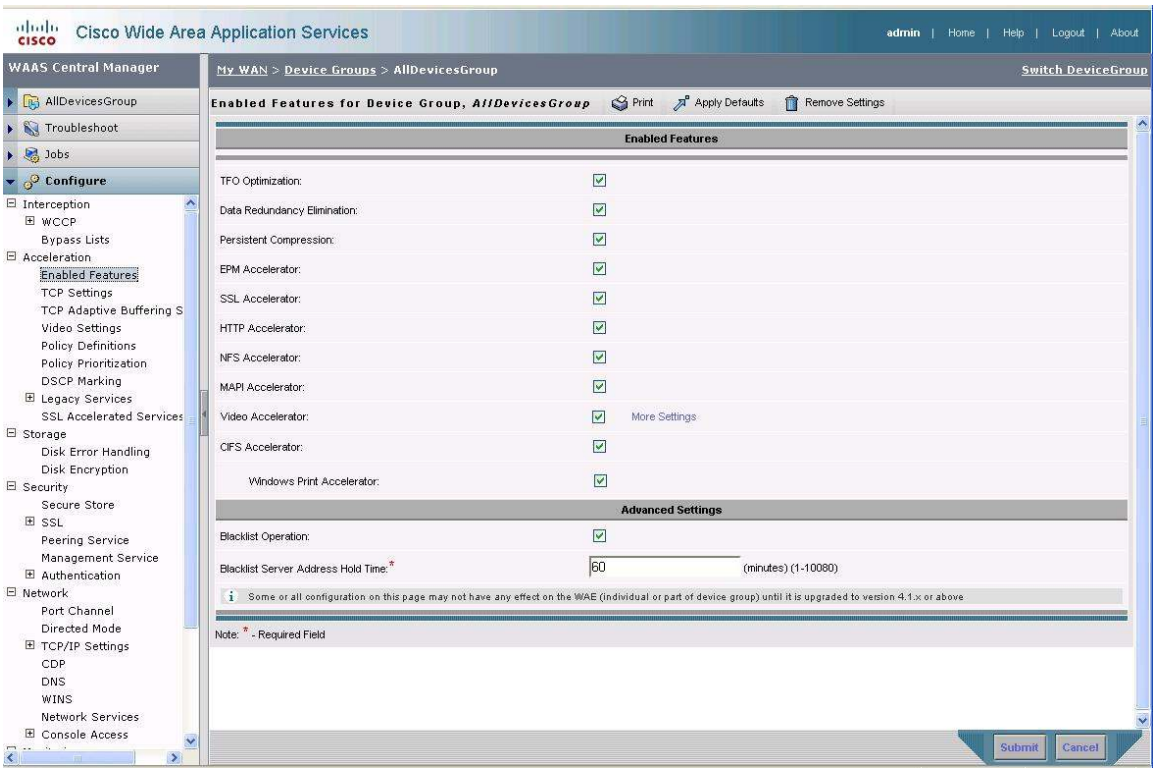
```
cm#cms secure-store [init|open|change]
To verify the status of the secure store, use this command:
cm#show cms secure-store
```

Q. How do I enable the SSL application optimizer on the Cisco WAE devices?

A. The SSL application optimizer is enabled by default on all Cisco WAE devices running Cisco WAAS Software Version 4.1.3 and later. The Cisco WAAS SSL application optimizer can be enabled on a Cisco WAAS device either from the Cisco WAAS Central Manager or by using the Cisco WAAS device CLI configuration if it is in the disabled state.

To enable the Cisco WAAS SSL accelerator, from the Cisco WAAS Central Manager GUI, select the WAE from choose **My WAN > Devices** and select the Cisco WAE. For the selected Cisco WAE device, from the navigation pane, choose **Configure > Acceleration > Enabled Features > SSL Accelerator**, select the check box to enable the device, and then click Submit. Figure 2 shows how to enable the SSL accelerator service on a Cisco WAE appliance through the Cisco WAAS Central Manager GUI.

Figure 2. Enabling the SSL Application Optimizer from the Cisco WAAS Central Manager



To enable the SSL application optimizer from the Cisco WAAS WAE device CLI, enter this command:

```
wae(config)# accelerator ssl enable
```

Q. Which SSL versions and cipher lists are supported by the Cisco WAAS SSL accelerated service?

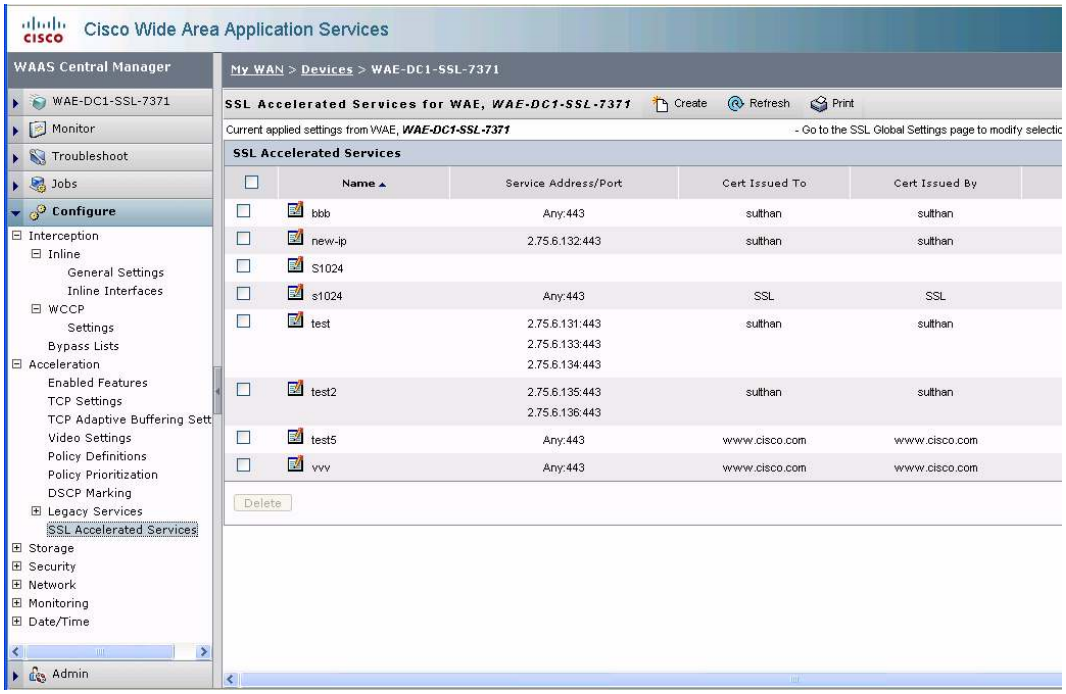
A. Cisco WAAS SSL accelerated service supports both SSLv3 and TLSv1 by default. A cipher list is a set of cipher suites that is assigned to the SSL acceleration configuration. A cipher suite is an SSL encryption method that includes the key exchange algorithm, encryption algorithm, and secure hash algorithm. The SSL accelerated service supports the following list of cipher suites:

```
dhe-rsa-with-aes-256-cbc-sha
rsa-with-aes-256-cbc-sha
dhe-rsa-with-aes-128-cbc-sha
rsa-with-aes-128-cbc-sha
dhe-rsa-with-3des-ede-cbc-sha
rsa-with-3des-ede-cbc-sha
rsa-with-rc4-128-sha
rsa-with-rc4-128-md5
dhe-rsa-with-des-cbc-sha
rsa-export1024-with-rc4-56-sha
rsa-export1024-with-des-cbc-sha
dhe-rsa-export-with-des40-cbc-sha
rsa-export-with-des40-cbc-sha
rsa-export-with-rc4-40-md5
```

Q. How do I configure an SSL accelerated service on the core Cisco WAE from the Cisco WAAS Central Manager?

A. To configure a Cisco WAAS SSL accelerated service on a core Cisco WAAS WAE device using the Cisco WAAS Central Manager GUI, choose **My WAN > Managed Devices** and select the core Cisco WAE. In the navigation pane for the selected core Cisco WAAS device, choose **Configure > Acceleration > SSL Accelerated Services** and then click the Create button. Figure 3 shows how to create a new SSL accelerated service on the core Cisco WAE using the Cisco WAAS Central Manager GUI.

Figure 3. Cisco WAAS SSL Accelerated Service Configuration



To configure a Cisco WAAS SSL accelerated service, follow these steps:

Step 1. Click the **Create** button and add a new service.

Step 2. Add a server hostname or server IP address and TCP port number for this service.

Step 3. Add a new certificate and private key for this service and generate a self-signed certificate or use a preexisting certificate key pair.

Step 4. Enable the service.

Q. What is a CA? How do I import a new CA certificate into the Cisco WAAS WAE device?

A. A certificate authority, or CA, is a trusted third party that issues certificates used to verify a site's identity. Cisco WAAS Software ships with a list of many well-known CA certificates, which can be configured by the admin user. The Cisco WAAS SSL acceleration feature also allows you to import your own CA certificate into the CA store. Refer to the product documentation for more details about how to configure the well-known CA certificates or import a new CA certificate.

Q. What is Online Certificate Status Protocol? How does Cisco WAAS use this protocol for certificate verification?

A. Online Certificate Status Protocol (OCSP) is an Internet protocol used to obtain the revocation status of an X.509 digital certificate (SSL certificate). OCSP servers are referred to as OCSP responders. The Cisco WAAS SSL application optimizer supports OCSP certificate verification for server and client devices. Refer to the product documentation for more details about OCSP revocation check and the options available in Cisco WAAS.

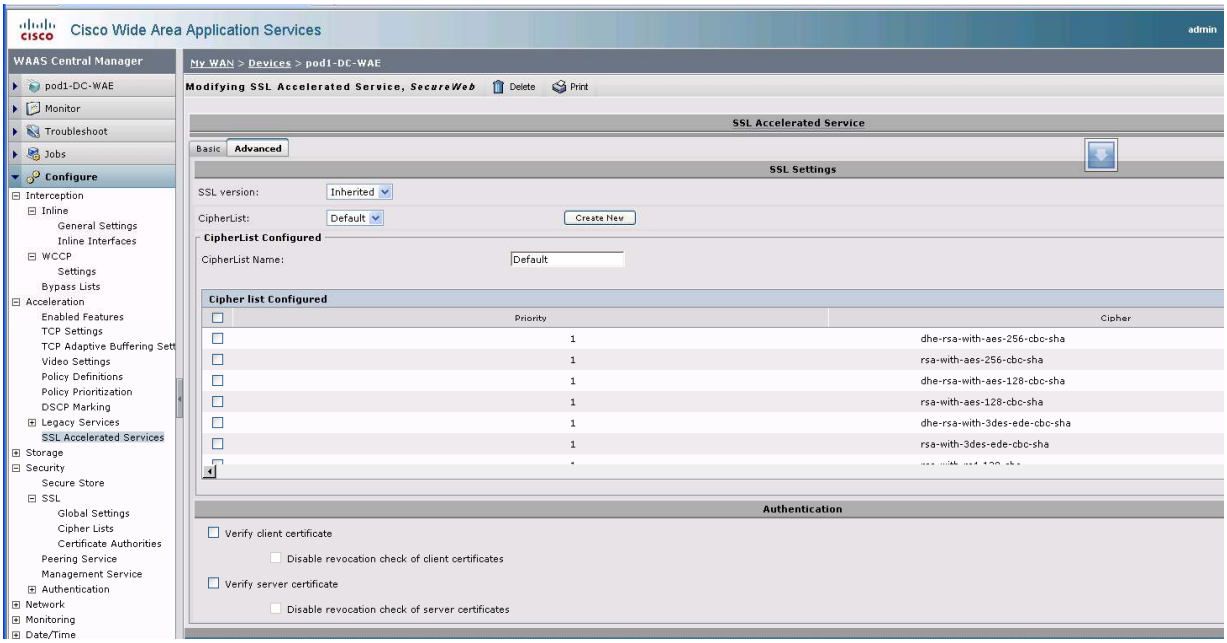
Q. How do I configure certificate verification for a certificate?

A. When running over an SSL protected session, the client and server can authenticate each other by verifying the certificate presented to them by the other party. In the case where the back-end SSL server is configured to perform client certificate verification, the server can delegate the certificate verification part to a Cisco WAAS core device.

To enable certificate verification on the core Cisco WAAS device, from the Cisco WAAS Central Manager GUI, choose **My WAN > Managed Devices** and select the core Cisco WAAS device. In the navigation pane for the selected core Cisco WAAS device, choose **Configure > Acceleration > SSL Accelerated Services** and then click the **Edit** button for a previously configured SSL accelerated service. Within the SSL accelerated service configuration settings, click **Advanced Settings.** Figure 4 shows how to enable client certificate verification and server certificate verification.

Certificate verification enables OCSP revocation check by default. To turn off OCSP revocation check and perform only certificate verification, select the box next to **Disable revocation check.**

Figure 4. Cisco WAAS SSL Accelerated Service Configuration Advanced Properties for Certificate Verification



Q. How do I configure SSL global settings?

A. SSL global settings are the default settings applicable to all SSL services running on the Cisco WAAS device. The global settings page allows you to set three parameters:

- **SSL version:** The SSL version default settings include both SSLv3 and TLSv1 protocols. If for any particular reason the SSL version needs to be restricted to a certain protocol, modify this parameter globally.

- **Cipher lists:** Cisco WAAS includes a list of 16 cipher suites by default. If the SSL negotiation needs to be restricted to a limited subset of these cipher suites, configure a new cipher list and apply it to the SSL services.
- **Revocation check:** The default value for OCSP revocation check is disabled, which means OCSP revocation check will not be performed. If OCSP revocation check should be enabled, change the default to **ocsp-url** or **ocsp-cert-url.**

  The **ocsp-url** configuration requires you to additionally configure an OCSP responder URL, which will be used to perform OCSP revocation checks.

  The **ocsp-cert-url** configuration means that the OCSP revocation check will be performed against an OCSP revocation check URL embedded in the certificate that is being checked. If the certificate does not contain an OCSP responder URL, then the OCSP revocation check process will fall back to the globally configured OCSP URL.

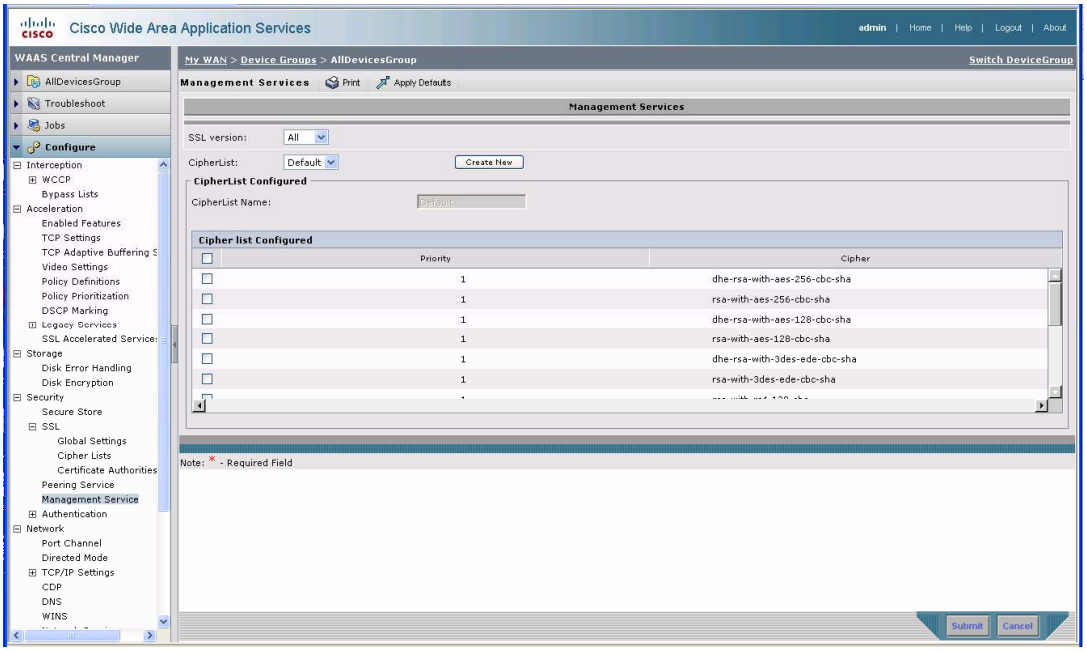
Q. How do I configure the optional SSL management service?

A. The secure communication channel between the Cisco WAAS devices and the Cisco WAAS Central Manager is called the SSL management service. The Cisco WAAS devices and the Cisco WAAS Central Manager use this SSL management service to send configuration updates and exchange certificates and keys. The SSL management service uses the SSL global settings as its defaults. However, these settings can be overridden by configuring the SSL management service on a Cisco WAE device. To make configuration changes to the SSL management services for a Cisco WAAS device, from the Cisco WAAS Central Manager GUI choose **My WAN > Managed Devices** and select the Cisco WAAS device. In the navigation pane for the selected Cisco WAAS device, choose **Configure > Security > SSL > Management Services**. The SSL Management Services configuration settings allow changes to the default SSL version and default cipher list configuration.

Note: SSL management service configuration changes on the Cisco WAAS Central Manager GUI should be made with proper care. A mismatched version or a mismatched cipher list configuration between the Cisco WAAS Central Manager and Cisco WAAS WAE will stop the secure channel communication between them.

Figure 5 shows how to modify the SSL management service.

Figure 5. Cisco WAAS SSL Management Services Configuration Settings Page

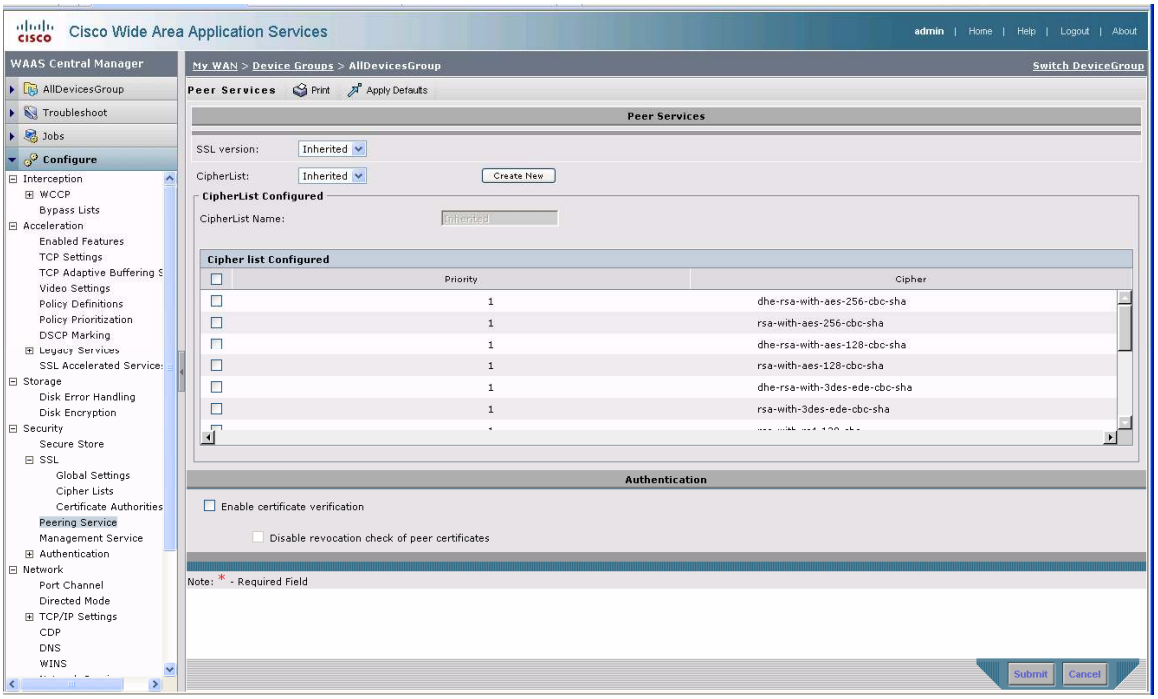


Q. How do I configure the optional SSL peering service?

A. The secure communication between the core and edge Cisco WAAS devices is called the SSL peering service. The SSL peering service is used to send the temporary session keys from the core Cisco WAAS device to the edge Cisco WAAS device. The SSL peer service uses the SSL global settings as its defaults. However, these settings can be overridden by configuring the SSL management service on a Cisco WAAS device. To modify the SSL peering service for a Cisco WAE, from the Cisco WAAS Central Manager GUI choose **My WAN > Managed Devices** and select the Cisco WAE device. In the navigation pane for the selected Cisco WAE device, choose **Configure > Security > SSL > Peering Service**. The SSL Peer Services configuration settings allow changes to the default SSL version and default cipher list configuration. The SSL Peer Services configuration page also allows you to import a CA signed certificate and private key to be used for the SSL peering session. It also allows you to enable certification verification for the peering session. Figure 6 shows how to modify the SSL peering service.

Note: Be sure to make SSL peering service configuration changes properly. A mismatched version or a mismatched cipher list configuration between the branch Cisco WAE and the data center Cisco WAE will prevent the peering session between the branch and the data center Cisco WAE devices from starting and will result in a connection failure.

Figure 6. Cisco WAAS SSL Peer Services Configuration Settings Page



Q. How do I back up and restore private keys and certificates on the Cisco WAAS Central Manager?

A. The Cisco WAAS Central Manager provides an option to back up the private keys and certificates stored in its secure store to enable recovery in case of failure. To back up and restore keys and certificates, enter the CLI command cms database backup from the Cisco WAAS Central Manager. The Cisco WAAS Central Manager backs up all the contents of the cms secure-store with this backup command. Private keys and certificates are stored in the cms secure-store file. To restore the backed up data, use the cms database restore CLI command.

Q. What optimization policy is applied to traffic that is handled by an SSL accelerated service?

A. When an SSL accelerated service is created and put into service on the data center Cisco WAE, the following policy actions take place automatically:

- The server IP address and port number are used to generate a dynamic classifier.
- This dynamic classifier is attached to the application policy called SSL.
- The optimization action for this dynamic classifier is set to DRE, LZ, and TFO.

For the purpose of SSL statistics collection, the application policy named SSL must be defined on the Cisco WAAS Central Manager Policy Definition page by the administrator.

The dynamic classifier attached to SSL policy can be checked using the following command on the Cisco WAE CLI:

```
show policy-engine application dynamic

Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 1  Max In Use: 3  Allocations: 76

Dynamic Match Type/Count Information:
  None                    0
  Clean-Up                0
  Host->Host              0
  Host->Local             0
  Local->Host             0
  Local->Any              0
  Any->Host               1
  Any->Local              0
  Any->Any                0

Individual Dynamic Match Information:
  Number:     1   Type: Any->Host (6)  User Id: SSL (4)
    Src: ANY:ANY  Dst: 2.8.3.20:443
    Map Name: basic
    Flags: SSL
    Seconds: 0  Remaining: - NA -  DM Index: 32765
    Hits: 21  Flows: - NA -  Cookie: 0x00000000
```

Q. How does SSL acceleration work for secure web applications running over SSL if the client web browser uses HTTPS proxy to connect to the secure web application?

A. When the client web browser is set for HTTP or HTTPS proxy and the user requests a connection using https://<sitename>, the HTTP protocol uses its CONNECT method for SSL tunnel establishment. The following conditions must be met for SSL acceleration to take place:

- The initial HTTPS proxy request in this case should be handled by the HTTP application optimizer.
- An SSL accelerated service should be configured and enabled for the SSL server for which SSL acceleration is required.
- Upon receipt of the HTTP CONNECT method in the HTTP data payload, the HTTP application optimizer will hand off the SSL connection to the Cisco WAAS SSL application optimizer for acceleration.

Q. What happens to HTTPS traffic when the Cisco WAAS SSL application optimizer is not enabled on the Cisco WAAS device in both the data center and the branch?

A. Cisco WAAS SSL application optimization works only if it is enabled on both the branch and the data center Cisco WAAS device. If the Cisco WAAS SSL application optimizer is not enabled on both ends, Cisco WAAS will optimize HTTPS traffic using the default HTTPS application policy settings. The default HTTPS application policy settings are TFO only.

Troubleshooting

Q. How can I check the status of the Cisco WAAS SSL application optimizer and verify that it is enabled and running?

A. To verify that the Cisco WAAS SSL application optimizer is configured and running properly, enter the CLI command **show accelerator ssl.**

```
WAE# show accelerator ssl

Accelerator     Licensed        Config State    Operational State
-----------     --------        ------------    -----------------
ssl             Yes             Enabled         Running

SSL:
   Policy Engine Config Item            Value
   -------------------------            -----
   State                                Registered
   Default Action                       Use Policy
   Connection Limit                     1500
   Effective Limit                      1490
   Keepalive timeout                    5.0 seconds

WAE#
```

The operational state should be **Running** and the configuration state should be **Enabled**. If the operational state is **Shutdown** and the configuration state is **Enabled**, there likely is a licensing problem.

Q. How can I verify that SSL acceleration is working, and in case of an error, which logs do I check for errors?

A. To verify that SSL acceleration is working for SSL connections, enter the CLI command **show statistics connection.**

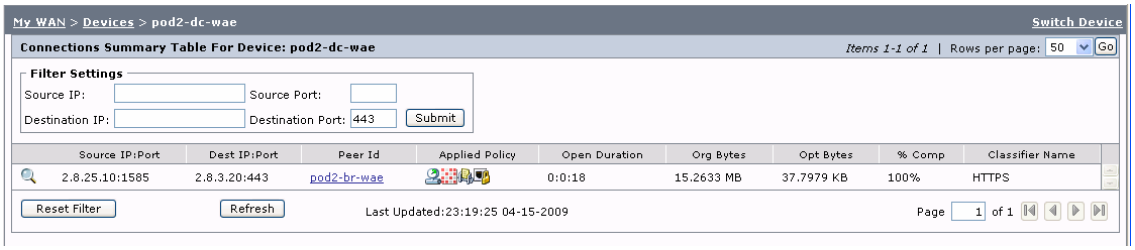
The SSL accelerated connections will be reported as TSDL in the CLI output as shown here.

```
WAE# show statistics connection

Current Active Optimized Flows:                     1
   Current Active Optimized TCP Plus Flows:         1
   Current Active Optimized TCP Only Flows:         0
   Current Active Optimized TCP Preposition Flows:  0
Current Active Auto-Discovery Flows:                0
Current Active Pass-Through Flows:                  3
Historical Flows:                                   100


D:DRE,L:LZ,T:TCP Optimization,
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID  Source IP:Port        Dest IP:Port          PeerID             Accel

436     2.8.15.10:2776        2.8.3.20:443          00:14:5e:85:41:8b  TSDL
```

WAE#

The SSL accelerated connections on the Cisco WAAS Central Manager will display a lock icon in the applied policy as shown in Figure 7.

Figure 7. Connection Summary Table in WAAS Central Manager showing an SSL accelerated connection



An HTTPS connection should be accelerated if it matches the SSL accelerated service policy criteria. If there is an SSL application optimizer error, the error logs can be found in the directory /local1/errorlog. The SSL error log files in the errorlog directory are:

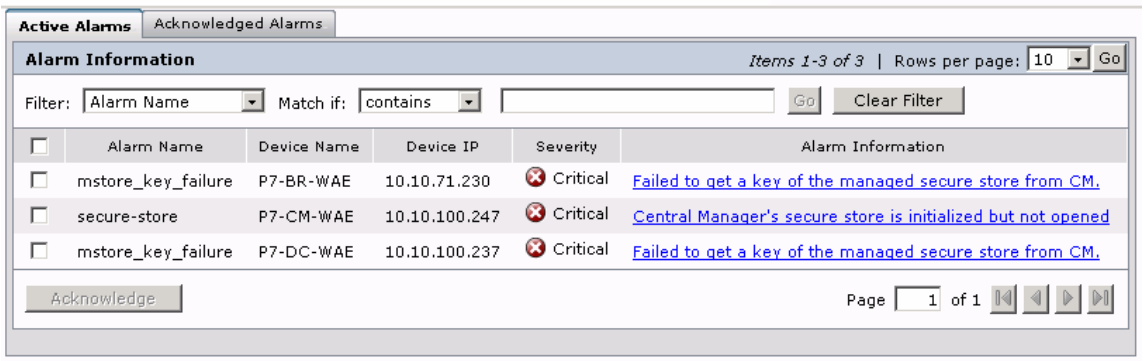
- sslao-errorlog.0
- sslao-errorlog.current

Q. What should I do if I see the alarm message "Central Manager's secure store is initialized but not open" in the Cisco WAAS Central Manager GUI?

A. As a best practice, the Cisco WAAS Central Manager secure store should always be open. Typically this message appears after the Cisco WAAS Central Manager has recovered from a reboot and its secure store has not been opened by the administrator yet. The secure store is used to store the SSL server private keys and the encryption keys used to encrypt the secure store on the data center Cisco WAE devices.

The Cisco WAAS Central Manager admin user should log into the Cisco WAAS Central Manager and open the secure store by entering the passphrase that was used to initialize and open the secure store earlier (Figure 8).

Figure 8. Cisco WAAS Central Manager showing secure store alarms



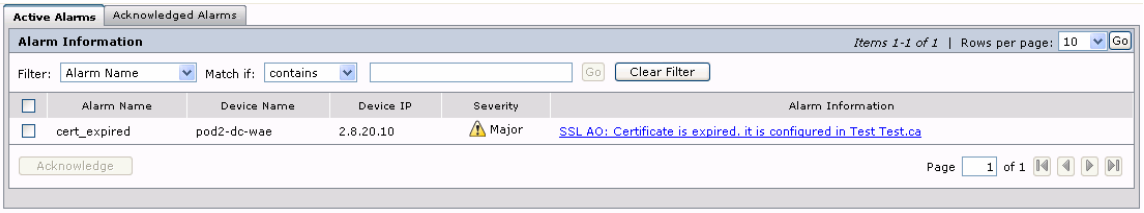
Q. What should I do if I see the alarm message "Failed to get a key of the managed store from CM" in the Cisco WAAS Central Manager GUI?

A. A Cisco WAAS WAE device never stores its secure store encryption key on the physical disk itself and instead obtains the secure store key from the Cisco WAAS Central Manager upon reboot. This message indicates that the Cisco WAE device has rebooted and is waiting to obtain its secure store encryption key from the Cisco WAAS Central Manager.

Q. What should I do if I see the alarm message "cert_expired" in the Cisco WAAS Central Manager GUI?

A. Cisco WAAS WAE devices will raise an alarm for expiring and expired certificates. When a "certificate expired" alarm appears in the Cisco WAAS Central Manager GUI, the expired certificate needs to be replaced with a valid certificate (Figure 9).

Figure 9. Expired certificate alarm seen in Cisco WAAS Central Manager



Q. What should be done if the admin user forgets the Cisco WAAS Central Manager secure store passphrase?

A. If the Cisco WAAS Central Manager admin user forgets the secure store passphrase, the Cisco WAAS Central Manager secure store needs to be reinitialized with a new passphrase. To reinitialize the Cisco WAAS Central Manager secure store, refer to the Cisco WAAS configuration guide.

Reinitializing the Cisco WAAS Central Manager secure store will also result in the loss of encryption keys for the Cisco WAAS WAE devices' secure stores. After the Cisco WAAS Central Manager secure store has been reinitialized and opened, follow the recovery process to reinitialize the secure store on the individual Cisco WAE devices.

Q. What command can be used to gather useful statistics about connections handled by an SSL accelerated service?

A. To obtain useful information about connections handled by an SSL accelerated service, enter the CLI command **show statistics accelerator ssl detail.** The command output provides useful information about SSL connection handling and is also helpful for troubleshooting failed connections. For example, certificate verification failures and OCSP revocation check failures are reported in this output.

```
pod2-dc-wae#show statistics accelerator ssl detail

SSL:

  Global Statistics
  -----------------
  Time Accelerator was started:                                  Thu Apr  9
17:15:11 2009
  Time Statistics were Last Reset/Cleared:                       Thu Apr  9
17:15:11 2009
  Total Handled Connections:                                     3237
  Total Optimized Connections:                                   3225
  Total Connections Handed-off with Compression Policies Unchanged:  4
  Total Dropped Connections:                                     0
  Current Active Connections:                                    0
  Current Pending Connections:                                   0
  Maximum Active Connections:                                    3
  Total LAN Bytes Read:                                          65676420
  Total Reads on LAN:                                            21282
  Total LAN Bytes Written:                                       1464397
```

```
Total Writes on LAN:                                          9715
Total WAN Bytes Read:                                         3482318
Total Reads on WAN:                                           147605
Total WAN Bytes Written:                                      18323151
Total Writes on WAN:                                          46117
Total LAN Handshake Bytes Read:                               24760
Total LAN Handshake Bytes Written:                            867977
Total WAN Handshake Bytes Read:                               1570536
Total WAN Handshake Bytes Written:                            8240330
Total Accelerator Bytes Read:                                 527825
Total Accelerator reads:                                      3250
Total Accelerator Bytes Written:                              582742697
Total Accelerator Writes:                                     38623
Total DRE Bytes Read:                                         8307536
Total DRE Reads:                                              26763
Total DRE Bytes Written:                                      1191634
Total DRE Writes:                                             27698
Total Failed Handshakes:                                      8
Pipe-through due to cipher mismatch:                          0
Pipe-through due to version mismatch:                         0
Pipe-through due to detection of non-SSL traffic:             4
Total SSLv3 Negotiated on LAN:                                3196
Total TLSv1 Negotiated on LAN:                                29
Total SSLv3 Negotiated on WAN:                                3196
Total TLSv1 Negotiated on WAN:                                29
Total SSLv3 Negotiated on Peer:                               0
Total TLSv1 Negotiated on Peer:                               3225
Total renegotiations requested by server:                     0
Total SSL renegotiations performed:                           0
[W2W-Srvr] Number of session hits:                            3214
[W2W-Srvr] Number of session misses:                          1
[W2W-Srvr] Number of sessions timedout:                       22
[W2W-Srvr] Number of sessions deleted because of cache full:  0
[W2W-Srvr] Number of bad sessions deleted:                    0
[W2W-Clnt] Number of session hits:                            0
[W2W-Clnt] Number of session misses:                          0
[W2W-Clnt] Number of sessions timedout:                       0
[W2W-Clnt] Number of sessions deleted because of cache full:  0
[W2W-Clnt] Number of bad sessions deleted:                    0
[C2S-Srvr] Number of session hits:                            22
[C2S-Srvr] Number of session misses:                          3201
[C2S-Srvr] Number of sessions timedout:                       2
[C2S-Srvr] Number of sessions deleted because of cache full:  0
[C2S-Srvr] Number of bad sessions deleted:                    14
[C2S-Clnt] Number of session hits:                            19
[C2S-Clnt] Number of session misses:                          3206
[C2S-Clnt] Number of sessions timedout:                       0
[C2S-Clnt] Number of sessions deleted because of cache full:  0
[C2S-Clnt] Number of bad sessions deleted:                    14
Total Successful Certificate Verifications:                   0
```

```
Total Failed Certificate Verifications:                          0
Failed certificate verifications due to invalid certificates:    0
Failed Certificate Verifications based on OCSP Check:            0
Failed Certificate Verifications (non OCSP):                     0
Total Failed Certificate Verifications due to Other Errors:      0
Total OCSP Connections Outstanding:                              0
Total OCSP Requests Processed:                                   0
Maximum Concurrent OCSP Requests:                                0
Total Successful OCSP Requests:                                  0
Total Successful OCSP Requests Returning OK Status:              0
Total Successful OCSP Requests with 'NONE' Revocation:           0
Total Successful OCSP Requests Returning REVOKED Status:         0
Total Successful OCSP Requests Returning UNKNOWN Status:         0
Total Failed OCSP Requests:                                      0
Total Failed OCSP Requests due to Other Errors:                  0
Total Failed OCSP Requests due to Connection Errors:             0
Total Failed OCSP Requests due to Connection Timeouts:           0
Total Failed OCSP Requests due to Insufficient Resources:        0
Total OCSP Bytes Read:                                           0
Total OCSP Write Bytes:                                          0
Flows dropped due to verification check:                         0
Flows dropped due to revocation check:                           0
Flows dropped due to other reasons:                              0


Policy Engine Statistics
------------------------
Session timeouts: 0,  Total timeouts: 0
Last keepalive received 01.6 Secs ago
Last registration occurred 5:21:52:44.6 Days:Hours:Mins:Secs ago
Hits:                    3237, Update Released:                    0
Active Connections:         0, Completed Connections:           3237
Drops:                      0
Rejected Connection Counts Due To: (Total: 0)
   Not Registered      :          0,  Keepalive Timeout   :          0
   No License          :          0,  Load Level          :          0
   Connection Limit    :          0,  Rate Limit          :          0
   Minimum TFO         :          0,  Resource Manager    :          0
   Global Config       :          0,  TFO Limit           :          0
   Server-Side         :          0,  DM Deny             :          0
   No DM Accept        :          0

Auto-Discovery Statistics
-------------------------
Connections queued for accept:        6472
Accept queue add failures:            0
AO discovery successful:              0
AO discovery failure:                 0

WAE#
```

Miscellaneous

Q. Do I need to purchase a separate license for SSL acceleration?

A. SSL acceleration is a feature of the Cisco WAAS Enterprise license that is purchased for each Cisco WAAS device. Existing Cisco WAAS Enterprise customers with Software Application Support plus Upgrades (SASU) support for the Cisco WAAS Enterprise license will get the SSL acceleration at no additional cost.

Q. Does Cisco WAAS accelerate Microsoft Outlook Web Access (OWA) in secure mode?

A. Yes, Cisco WAAS accelerates Microsoft OWA in secure mode using the Cisco WAAS SSL application optimizer and with full optimization (DRE, TFO, and LZ compression). The SSL application optimizer should be configured with an SSL accelerated service that matches the Microsoft OWA IP address and port if the secure mode of Microsoft OWA is used over port 443. For information about the Microsoft OWA architecture, please refer to http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/confeat/e2kowa.mspx.

Q. Does the SSL application optimizer accelerate encrypted Message Application Programming Interface traffic?

A. Microsoft uses native encryption for Microsoft Exchange Message Application Programming Interface (MAPI) communication with the Microsoft Outlook client. The Cisco WAAS SSL application optimizer does not accelerate MAPI traffic secured using native MAPI encryption.

Microsoft also supports using SSL for encryption of MAPI traffic: by sending a MAPI remote procedure call (RPC) over HTTPS. This feature is called Outlook Anywhere and is supported by Microsoft Outlook 2003 and 2007. The Cisco WAAS SSL application optimizer will provide full (DRE, and LZ, TFO) acceleration benefits for SSL encrypted MAPI traffic.

Enterprises can easily switch clients to HTTPS instead of native encryption for Microsoft Outlook through Group Policy Objects (GPOs) or the Microsoft Exchange 2007 autodiscover service.

Use of SSL encryption is recommended by Microsoft as a scalable encryption solution as SSL offload devices can be used to improve the performance of a Microsoft Exchange server farm. For information about how to configure Microsoft Office Outlook 2007 and 2003 clients for Outlook Anywhere, refer to the Microsoft documentation at http://technet.microsoft.com/en-us/library/aa996922.aspx.

Q. How does the Cisco WAAS Central Manager secure SSL private keys and certificates used for SSL accelerated services?

A. The Cisco WAAS Central Manager secure store is initialized with a user-supplied passphrase. Private keys and certificates are stored in this secure store in an encrypted format using this passphrase, which must be entered at the time that the private key or certificate is imported.

Q. How does the Cisco WAAS device secure SSL private keys and certificates used for SSL accelerated services?

A. The core Cisco WAAS device stores the private keys and certificates in a secure store on the disk. The secure store is encrypted using a key that is retrieved from the Cisco WAAS Central Manager and stored in memory only.

Q. What types of certificate and key formats does Cisco WAAS support?

A. Cisco WAAS supports both privacy-enhanced mail (PEM) and Public Key Cryptography Standards 12 (PKCS12) format certificates and keys. The certificates and private keys are encrypted using a passphrase and stored in an encrypted data store on the Cisco WAAS Central Manager and the core Cisco WAAS device. The certificate and keys are never pushed out to the branch edge Cisco WAAS devices.

Q. What types of SSL services do Cisco WAAS devices and the Cisco WAAS Central Manager use?

A. Cisco WAAS uses four types of SSL services:

- **SSL accelerated service:** This service is used to accelerate SSL connections on the core Cisco WAAS device.
- **SSL management service:** The Cisco WAAS Central Manager and Cisco WAAS core and edge devices use the SSL management service for management purposes.
- **SSL peering service:** This is the secure communication service between the Cisco WAAS core device and the edge device used for session key exchange or transfer.
- **SSL admin service:** This is the service running on the Cisco WAAS Central Manager used to access the Cisco WAAS Central Manager GUI.

Q. Does a Cisco WAAS SSL accelerated service support certificate chains?

A. Yes, certificate chains are supported by Cisco WAAS SSL accelerated service configuration. The certificate chain can be imported by either copying and pasting it in the PEM format or uploading a PKCS12 file with the entire certificate chain.

Q. What happens when a certificate has expired or is about to expire?

A. If a certificate associated with an SSL service or a CA certificate has expired or is expiring in the next 30 days, the Cisco WAAS device will generate an alarm. The device will, however, still continue to use that certificate.

Q. What happens to new and existing connections when the SSL certificate and private key associated with an SSL accelerated service are changed by importing a new key and certificate?

A. When a new certificate and key are imported in an Cisco WAAS SSL accelerated service, the existing connections continue using the old certificate and key until they close. New connections will use the newly imported certificate and keys.

Q. What application policy does the SSL application optimizer uses for reporting SSL accelerated connection statistics in the Cisco WAAS Central Manager generate?

A. The SSL application optimizer reports SSL accelerated connections under application type SSL. Cisco WAAS Software Version 4.1.3 added a new application policy called SSL, which is applied to the classifier HTTPS. The Cisco WAAS Central Manager statistics for SSL include both the SSL accelerated connections and those HTTPS connections optimized with TFO only by Cisco WAAS WAE devices. The default SSL application policy configuration in the Cisco WAAS WAE device CLI is shown here.

```
policy-engine application
   name SSL

   classifier HTTPS
      match dst port eq 443

   map basic
      name SSL classifier HTTPS action optimize DRE no compression none
```

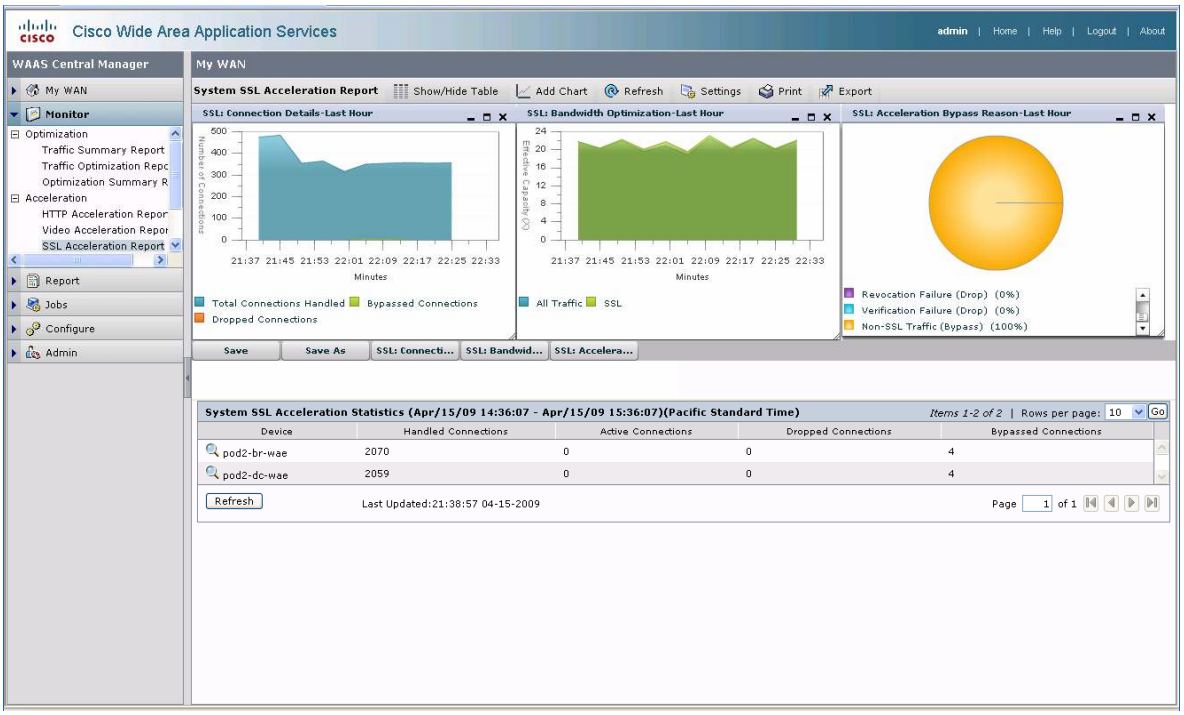
Q. What SSL reports does the Cisco WAAS Central Manager generate?

A. The Cisco WAAS Central Manager provides SSL acceleration reports including:

- SSL connection statistics
- SSL bandwidth optimization
- SSL acceleration bypass reason

Figure 10 shows an SSL acceleration report from the Cisco WAAS Central Manager.

Figure 10. Cisco WAAS SSL Acceleration Report from the Cisco WAAS Central Manager



Q. How does Cisco WAAS report SSL acceleration statistics?

A. The output of the command **show statistics application SSL** provides a consolidated report about SSL traffic handled by the Cisco WAAS device. This report includes both the SSL accelerated traffic and the SSL traffic that was optimized using the default policy with TFO only.

```
WAE# show statistics application SSL
Application                Inbound                 Outbound
                           ----------------------- -----------------------

SSL
  Opt TCP Plus:
     Bytes                                  2579                    24311
     Packets                                  27                       33
  Orig TCP Plus:
     Bytes                                 60654                     1855
     Packets                                  44                       28
  Opt Preposition:
     Bytes                                     0                        0
     Packets                                   0                        0
  Orig Preposition:
     Bytes                                     0                        0
     Packets                                   0                        0
  Opt TCP Only:
     Bytes                                     0                        0
     Packets                                   0                        0
  Orig TCP Only:
     Bytes                                     0                        0
     Packets                                   0                        0
  Internal Client:
```

```
   Bytes                                0                      0
   Packets                              0                      0
Internal Server:
   Bytes                                0                      0
   Packets                              0                      0
PT Client:
   Bytes                                                       0
   Packets                                                     0
PT Server:
   Bytes                                                       0
   Packets                                                     0

                    Active                 Completed
                    ---------------------- ----------------------
Opt TCP Plus                             0                      1
Preposition                              0                      0
Opt TCP Only                             0                      0
Internal Client                          0                      0
Internal Server                          0                      0
PT No Peer                               0                      0
PT Config                                0                      0
PT Intermediate                          0                      0
PT_Other                                 0                      0
```