Cisco WAAS-Fehlerbehebungsleitfaden für Version 4.1.3 und höher

Kapitel: Fehlerbehebung bei SSL AO

In diesem Artikel wird die Fehlerbehebung für SSL AO beschrieben.

Inh

Ha
An
Da
Vo
Op
Pro
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Ha
Fel
vW
Fel
Fel

Inhalt

SSL Accelerator - Übersicht

Der SSL Accelerator (ab Version 4.1.3 verfügbar) optimiert verschlüsselten SSL- (Secure Sockets Layer) und TLS-Datenverkehr (Transport Layer Security). Der SSL Accelerator bietet Datenverkehrsverschlüsselung und -entschlüsselung innerhalb von WAAS, um eine End-to-End-Optimierung des Datenverkehrs zu ermöglichen. Der SSL Accelerator bietet außerdem eine sichere Verwaltung der Verschlüsselungszertifikate und -schlüssel.

In einem WAAS-Netzwerk fungiert die WAE im Rechenzentrum als vertrauenswürdiger zwischengeschalteter Knoten für SSL-Anfragen des Clients. Der private Schlüssel und das Serverzertifikat werden auf der WAE des Rechenzentrums gespeichert. Die WAE im Rechenzentrum nimmt am SSL-Handshake teil, um den Sitzungsschlüssel abzuleiten, der sicher in-band an die WAE der Außenstelle verteilt wird. Dadurch kann die WAE der Außenstelle den Client-Datenverkehr entschlüsseln, optimieren, neu verschlüsseln und über das WAN an die WAE im Rechenzentrum senden. Die WAE im Rechenzentrum unterhält eine separate SSL-Sitzung mit dem Ursprungsserver.

Die folgenden Services sind für die SSL/TLS-Optimierung relevant:

- Accelerated Service - Eine Konfigurationseinheit, die Beschleunigungsmerkmale beschreibt, die für einen SSL-Server oder eine Gruppe von Servern angewendet werden. Gibt das Zertifikat und den privaten Schlüssel an, die bei der Positionierung als vertrauenswürdiger Vermittler, die zu verwendenden Verschlüsselungen, die zulässige SSL-Version und die Einstellungen für die Zertifikatsüberprüfung verwendet werden sollen.
- Peering Service - Eine Konfigurationseinheit, die die Beschleunigungsmerkmale für In-Band-SSL-Verbindungen zwischen den WAEs in Zweigstellen und im Rechenzentrum beschreibt. Dieser Service wird für die Übertragung von Sitzungsschlüsselinformationen vom Rechenzentrum an die WAEs der Außenstelle zur Optimierung von SSL-Verbindungen verwendet.
- Central Manager Admin Service - Wird nicht direkt vom SSL Accelerator verwendet, sondern von einem Administrator für das Konfigurationsmanagement von SSL Accelerated Services. Wird auch zum Hochladen von Zertifikaten und privaten Schlüsseln verwendet, die in SSL-beschleunigten Diensten verwendet werden.
- Central Manager Management Service - Wird nicht direkt vom SSL Accelerator verwendet, sondern für die Kommunikation zwischen Geräten der Anwendungsbeschleuniger und dem Central Manager. Dieser Service wird für das Konfigurationsmanagement, den sicheren Abruf von Speicherverschlüsselungsschlüsseln und Gerätestatusaktualisierungen verwendet.

Der sichere Store Central Manager ist für den Betrieb des SSL AO unerlässlich, da er sichere Verschlüsselungsschlüssel für alle WAEs speichert. Nach dem erneuten Laden jedes Central Managers muss der Administrator den sicheren Speicher erneut öffnen, indem er die Passphrase mit dem Befehl **cms secure-store open** bereitstellt. Bei jedem Neustart der WAE ruft eine WAE automatisch den Verschlüsselungsschlüssel für den sicheren Speicher von der zentralen Verwaltungsschnittstelle ab. Nach einem erneuten Laden ist daher keine Aktion auf der WAE erforderlich.

Wenn Clients eine HTTP-Proxy-Lösung verwenden, wird die erste Verbindung von der HTTP AO verarbeitet, die sie als SSL-Tunnel-Anforderung an Port 443 erkennt. Das HTTP AO sucht nach einem passenden SSL-beschleunigten Service, der auf der WAE des Rechenzentrums definiert ist. Wenn eine Übereinstimmung gefunden wird, übergibt es die Verbindung mit dem SSL AO. Der Datenverkehr, den das HTTP-AO für einen HTTPS-Proxy an das SSL-Betriebssystem übergibt,

wird jedoch als Teil der Webanwendungsstatistik und nicht in der SSL-Anwendung gemeldet. Wenn die HTTP-AO keine Übereinstimmung findet, wird die Verbindung entsprechend der Konfiguration der statischen HTTPS-Richtlinie (SSL) optimiert.

Die SSL AO kann selbstsignierte Zertifikate anstelle von Zertifizierungsstellen signierten Zertifikaten verwenden. Dies kann bei der Bereitstellung von Machbarkeitsnachweisen (Proof Concept Systems, POC) und bei der Behebung von SSL-Problemen hilfreich sein. Durch die Verwendung selbstsignierter Zertifikate können Sie schnell ein WAAS-System bereitstellen, ohne die Ursprungsserverzertifikate importieren zu müssen. Außerdem können Sie Zertifikate als potenzielle Quelle für Probleme beseitigen. Beim Erstellen eines SSL Accelerated Service können Sie im Central Manager ein selbstsigniertes Zertifikat konfigurieren. Wenn Sie jedoch ein selbstsigniertes Zertifikat verwenden, zeigt der Clientbrowser eine Sicherheitswarnung an, dass das Zertifikat nicht vertrauenswürdig ist (da es nicht von einer bekannten Zertifizierungsstelle signiert wird). Um diese Sicherheitswarnung zu vermeiden, installieren Sie das Zertifikat im Ordner Trusted Root Certification Authority im Client-Browser. (Klicken Sie in Internet Explorer in der Sicherheitswarnung auf **Zertifikat anzeigen**, und klicken Sie dann im Dialogfeld Zertifikat auf **Zertifikat installieren** und schließen Sie den Zertifikatimport-Assistenten ab.)

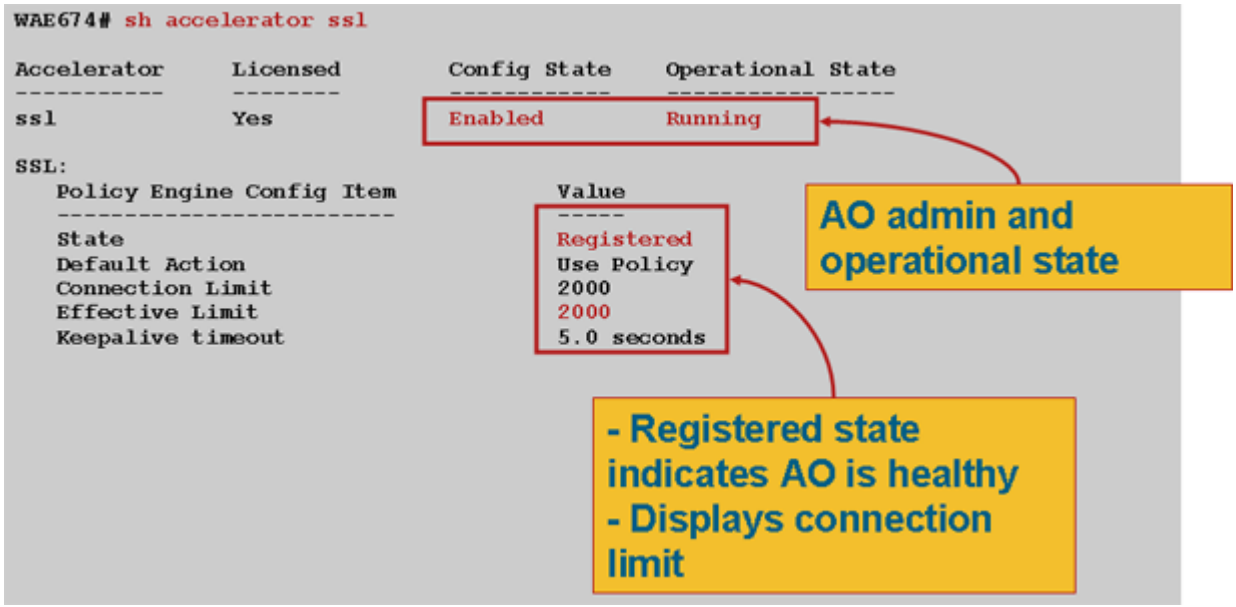
Die Konfiguration der SSL Management Services ist optional. Sie können die SSL-Version und die Verschlüsselungsliste für die Kommunikation in Central Manager in WAEs und in den Browser (für den Administratorzugriff) ändern. Wenn Sie Chiffren konfigurieren, die nicht von Ihrem Browser unterstützt werden, wird die Verbindung zum Central Manager unterbrochen. Verwenden Sie in diesem Fall den Konfigurationsbefehl **crypto SSL management-service** von der CLI, um die Einstellungen für den SSL-Management-Dienst wieder auf die Standardeinstellungen zurückzusetzen.

Fehlerbehebung bei SSL AO

Sie können die allgemeine AO-Konfiguration und den allgemeinen Status mit dem **Show Accelerator** überprüfen und **Lizenzbefehle anzeigen**, wie im Artikel Problembehandlung bei Anwendungsbeschleunigung beschrieben. Die Enterprise-Lizenz ist für den SSL Accelerator-Betrieb erforderlich.

Überprüfen Sie anschließend den für SSL AO spezifischen Status der WAEs für Rechenzentren und Zweigstellen, indem Sie den Befehl **show accelerator ssl** verwenden (siehe Abbildung 1). Sie möchten sehen, dass SSL AO aktiviert, ausgeführt und registriert ist und dass die Verbindungsbeschränkung angezeigt wird. Wenn der Config State (Konfigurationsstatus) aktiviert ist, der Operational State jedoch Shutdown lautet, weist dies auf ein Lizenzierungsproblem hin. Wenn der Betriebsstatus deaktiviert ist, kann dies daran liegen, dass die WAE die SSL-Schlüssel nicht vom sicheren Speicher der Central Manager abrufen kann, entweder weil der sichere Speicher nicht geöffnet ist oder der Central Manager nicht erreichbar ist. Überprüfen Sie mithilfe der Befehle **show cms info** und **ping**, ob der Central Manager erreichbar ist.

Abbildung 1: Überprüfen des Status von SSL Accelerator



Wenn Sie einen Betriebszustand der Gen Crypto Params sehen, warten Sie, bis der Status Running (Wird ausgeführt) lautet. Dies kann einige Minuten nach einem Neustart dauern. Wenn der Status "Keys from CM" (Schlüssel von CM abrufen) länger als einige Minuten angezeigt wird, kann dies darauf hinweisen, dass der CMS-Dienst auf der zentralen Verwaltungsschnittstelle nicht ausgeführt wird, dass keine Netzwerkverbindung zum zentralen Manager besteht, dass die WAAS-Versionen auf der WAE und Central Manager nicht kompatibel sind oder dass der sichere Speicher der zentralen Verwaltungsschnittstelle nicht geöffnet ist.

Sie können mithilfe des Befehls **show cms secure-store** wie folgt überprüfen, ob der sichere Speicher für die zentrale Verwaltungsschnittstelle initialisiert und geöffnet ist:

```
cm# show cms secure-store
secure-store is initialized and open.
```

Wenn der sichere Speicher nicht initialisiert oder geöffnet ist, werden kritische Alarme wie mstore_key_failure und secure-store angezeigt. Sie können den sicheren Speicher mit dem Befehl **cms secure-store open** oder über den Central Manager öffnen, indem Sie **Admin > Secure Store** auswählen.

Tipp: Dokumentieren Sie das Kennwort für den sicheren Speicher, um zu vermeiden, dass der sichere Speicher zurückgesetzt werden muss, wenn Sie das Kennwort vergessen haben.

Tritt ein Problem mit der Festplattenverschlüsselung auf einer WAE auf, kann dies auch den Betrieb der SSL-E/A-Verbindung verhindern. Mit dem Befehl **show disk details (Datenträgerdetails anzeigen**) können Sie überprüfen, ob die Festplattenverschlüsselung aktiviert ist, und überprüfen, ob die Partitionen CONTENT und SPOOL bereitgestellt wurden. Wenn diese Partitionen gemountet werden, zeigt dies an, dass die Verschlüsselungsschlüssel erfolgreich vom Central Manager abgerufen wurden und verschlüsselte Daten von den Festplatten geschrieben und gelesen werden können. Wenn der Befehl **show disk details (Datenträgerdetails anzeigen)** den Befehl "System initialisiert" anzeigt, bedeutet dies, dass die Verschlüsselungsschlüssel noch nicht vom zentralen Manager abgerufen wurden und die Festplatten noch nicht bereitgestellt wurden. Die WAE stellt in diesem Zustand keine Beschleunigungsdienste bereit. Wenn die WAE die Festplattenverschlüsselungsschlüssel nicht von der zentralen Verwaltungsschnittstelle abrufen kann, wird ein Alarm ausgelöst.

Sie können überprüfen, ob der SSL-beschleunigte Dienst konfiguriert ist und sein Status auf der WAE des Rechenzentrums "Enabled" (Aktiviert) lautet (wählen Sie in der zentralen Verwaltungsschnittstelle das Gerät aus, und wählen Sie dann **Configure > Acceleration > SSL**

Accelerated Services). Ein konfigurierter und aktivierter beschleunigter Dienst kann vom SSL Accelerator aus folgenden Gründen inaktiv werden:

- Das im beschleunigten Dienst konfigurierte Zertifikat wurde von der WAE gelöscht. Verwenden Sie den Befehl **show running-config**, um das im beschleunigten Dienst verwendete Zertifikat zu ermitteln. Verwenden Sie dann die Befehle **show crypto certificate** und **show crypto certificate-details**, um zu bestätigen, dass das Zertifikat ein sicherer Speicher ist. Wenn das Zertifikat fehlt, importieren Sie es erneut.
- Das Zertifikat für beschleunigte Services ist abgelaufen. Verwenden Sie die **Befehle zum Anzeigen von Kryptozertifikaten** und **Anzeigen von Zertifikatsdetails**, um das Ablaufdatum des Zertifikats zu überprüfen.
- Das beschleunigte Service-Zertifikat hat ein gültiges Datum, das in der Zukunft beginnt. Verwenden Sie die **Befehle zum Anzeigen von Kryptozertifikaten** und **Anzeigen von Zertifikatsdetails** und überprüfen Sie den Gültigkeitsbereich der Befehlsausgabe. Stellen Sie außerdem sicher, dass die Informationen zu WAE-Uhr und Zeitzone korrekt sind.

Sie können überprüfen, ob für SSL-Verbindungen die richtige Richtlinie angewendet wurde, d. h., sie verfügen über eine vollständige Optimierung mit SSL-Beschleunigung, wie in Abbildung 2 gezeigt. Wählen Sie in Central Manager (Zentraler Manager) das WAE-Gerät aus, und wählen Sie dann **Monitor > Optimization > Connections Statistics (Überwachung > Optimierung > Verbindungsstatistiken)**.

Abbildung 2: Überprüfen der richtigen Richtlinie für SSL-Verbindungen

Mit dem Befehl **show running-config** können Sie überprüfen, ob die HTTPS-Datenverkehrsrichtlinie ordnungsgemäß konfiguriert ist. Sie möchten **die DRE-Komprimierung für** die SSL-Anwendungsaktion **optimieren**, und Sie möchten die entsprechenden Übereinstimmungsbedingungen für den HTTPS-Klassifizierer wie folgt anzeigen:

```
WAE674# sh run | include HTTPS
   classifier HTTPS
      name SSL classifier HTTPS action optimize DRE no compression none              <---------
----

WAE674# sh run | begin HTTPS

...skipping
```

```
   classifier HTTPS
      match dst port eq 443                                                    <---------
----
   exit
```

Ein aktiver beschleunigter Dienst fügt dynamische Richtlinien ein, die dem Server-IP:Port, dem Servernamen:Port oder der Serverdomäne:Port entsprechen, der im beschleunigten Dienst konfiguriert ist. Diese Richtlinien können mithilfe des Befehls **show policy-engine application dynamic** überprüft werden. Das Feld "Dst" in jeder angezeigten Richtlinie gibt die Server-IP und den Port an, die mit dem beschleunigten Dienst übereinstimmen. Für die Platzhalterdomäne (z. B. Serverdomäne *.webex.com-Port 443) lautet das Feld "Dst" "Any:443". Bei der Servernamenkonfiguration wird eine Weiterleitungs-DNS-Suche durchgeführt, wenn der beschleunigte Dienst aktiviert wird, und alle in der DNS-Antwort zurückgegebenen IP-Adressen werden in die Richtlinien-Engine eingefügt. Dieser Befehl ist hilfreich, um Situationen zu erkennen, in denen ein beschleunigter Dienst als "inservice" (nicht in Betrieb) markiert ist, der beschleunigte Dienst jedoch aufgrund eines anderen Fehlers inaktiv wird. Beispielsweise sind alle beschleunigten Dienste vom Peering-Service abhängig, und wenn der Peering-Service aufgrund eines fehlenden/gelöschten Zertifikats inaktiv ist, wird ein beschleunigter Dienst auch als inaktiv markiert, obwohl er in der Ausgabe show running-config als "inservice" zu bezeichnen scheint. Sie können mithilfe des Befehls **show policy-engine application dynamic** überprüfen, ob die dynamische SSL-Richtlinie für die WAE im Rechenzentrum aktiv ist. Sie können den Peering-Dienststatus überprüfen, indem Sie den Befehl **show crypto ssl services host-service peering** verwenden.

Eine beschleunigte SSL AO-Servicekonfiguration kann vier Servereinträge enthalten:

- Statische IP (Server-IP) - verfügbar ab Version 4.1.3
- Catch All (server-ip any) - ab Version 4.1.7 verfügbar
- Hostname (Servername) - ab Version 4.2.1 verfügbar
- Wildcard-Domäne (Server-Domäne) - verfügbar ab Version 4.2.1

Sobald die Verbindung vom SSL AO empfangen wurde, entscheidet das Unternehmen, welcher beschleunigte Dienst für die Optimierung verwendet werden soll. Die statische IP-Konfiguration erhält die höchste Präferenz, gefolgt vom Servernamen, der Server-Domäne und der Server-IP-Adresse any. Wenn keiner der konfigurierten und aktivierten beschleunigten Dienste mit der Server-IP für die Verbindung übereinstimmt, wird die Verbindung zum generischen AO weitergeleitet. Das Cookie, das von SSL AO in die Policy Engine eingefügt wird, wird verwendet, um zu bestimmen, welcher beschleunigte Dienst und welcher Servereintrag für eine bestimmte Verbindung zugeordnet wird. Dieses Policy Engine Cookie ist eine 32-Bit-Nummer und nur für die SSL AO-Funktion von Bedeutung. Die höheren Bit werden verwendet, um verschiedene Servereingabetypen anzugeben, und die unteren Bits geben den beschleunigten Dienstindex wie folgt an:

Cookie-Werte der SSL Policy Engine

Cookie-Wert	Servereingabetyp	Kommentare
0x8*xxxxxxx*	Server-IP-Adresse	Konfiguration statischer IP-Adressen
0x4*xxxxxxx*	Server-Hostname	Die WAE im Rechenzentrum führt eine DNS-Vorwärtssuche für den Hostnamen durch und fügt die IP-Adressen hinzu, die in die dynamische Richtlinienkonfiguration zurückgegeben werden. Standardmäßig alle 10 Minuten aktualisiert.

0x2FFFFFFFFF	Server-Domänenname	Die WAE im Rechenzentrum führt eine umgekehrte DNS-Suche an der IP-Adresse des Ziel-Hosts durch, um festzustellen, ob sie mit der Domäne übereinstimmt. Bei einer Übereinstimmung wird der SSL-Datenverkehr beschleunigt, und wenn er nicht übereinstimmt, wird der Datenverkehr gemäß der statischen HTTPS-Richtlinie verarbeitet.
0x1*xxxxxxx*	Alle Server	Alle SSL-Verbindungen werden mithilfe dieser beschleunigten Servicekonfiguration beschleunigt.

Beispiel 1: Beschleunigter Service mit Server-IP-Konfiguration:

```
WAE(config)#crypto ssl services accelerated-service asvc-ip
WAE(config-ssl-accelerated)#description "Server IP acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-ip 171.70.150.5 port 443
WAE(config-ssl-accelerated)#inservice
```

Der entsprechende Policy Engine-Eintrag wird wie folgt hinzugefügt:

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
  Number:     1   Type: Any->Host (6)  User Id: SSL (4)           <----------------
    Src: ANY:ANY  Dst: 171.70.150.5:443                          <----------------
    Map Name: basic
    Flags: SSL
    Seconds: 0  Remaining: - NA -  DM Index: 32764
    Hits: 25  Flows: - NA -  Cookie: 0x80000001                  <----------------
```

Beispiel 2: Accelerated-Service mit Servernamenkonfiguration:

Diese Konfiguration ermöglicht eine einfache Bereitstellung für die Optimierung von SSL-Unternehmensanwendungen. Es ist an DNS-Konfigurationsänderungen anpassbar und reduziert IT-Verwaltungsaufgaben.

```
WAE(config)#crypto ssl services accelerated-service asvc-name
WAE(config-ssl-accelerated)#description "Server name acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-name www.google.com port 443
WAE(config-ssl-accelerated)#inservice
```

Der entsprechende Policy Engine-Eintrag wird wie folgt hinzugefügt:

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.104:443                           <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     2   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.147:443                           <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32763
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     3   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.103:443                           <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32764
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     4   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.99:443                            <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32765
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

Beispiel 3: Schnellerer Service mit Serverdomänenkonfiguration:

Mit dieser Konfiguration können WAAS-Geräte eine einheitliche Platzhalterdomäne konfigurieren, sodass keine IP-Adressen für alle Server benötigt werden. Die WAE im Rechenzentrum verwendet Reverse DNS (rDNS), um den zur konfigurierten Domäne gehörenden Datenverkehr abzugleichen. Durch die Konfiguration einer Platzhalterdomäne wird die Konfiguration mehrerer IP-Adressen vermieden, sodass die Lösung skalierbar und für die SaaS-Architektur geeignet ist.

```
WAE(config)#crypto ssl services accelerated-service asvc-domain
WAE(config-ssl-accelerated)#description "Server domain acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-name *.webex.com port 443
WAE(config-ssl-accelerated)#inservice
```

Der entsprechende Policy Engine-Eintrag wird wie folgt hinzugefügt:

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751
```

```
< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: ANY:443                                     <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x2FFFFFFF                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

Beispiel 4: Beschleunigter Service mit Server-IP-Konfiguration:

Diese Konfiguration bietet einen Mechanismus für den Abruf. Wenn ein beschleunigter Service mit **server-ip an einem beliebigen Port 443** aktiviert ist, können alle Verbindungen an Port 443 durch SSL AO optimiert werden. Diese Konfiguration kann während POCs verwendet werden, um den gesamten Datenverkehr an einem bestimmten Port zu optimieren.

```
WAE(config)#crypto ssl services accelerated-service asvc-ipany
WAE(config-ssl-accelerated)#description "Server ipany acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-ip any port 443
WAE(config-ssl-accelerated)#inservice
```

Der entsprechende Policy Engine-Eintrag wird wie folgt hinzugefügt:

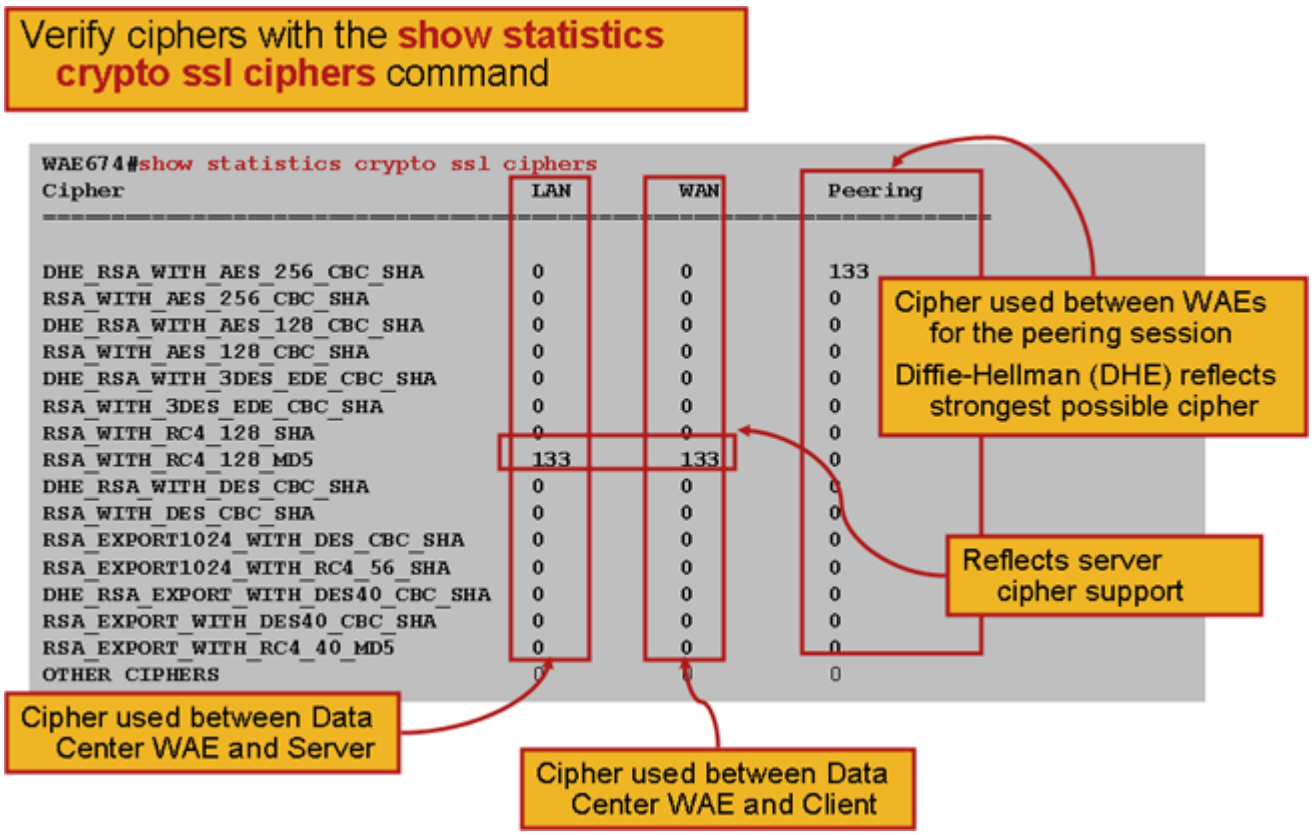
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: ANY:443                                     <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x10000004                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

Sie können die verwendeten Chiffren mit den Befehlen **show statistics crypto ssl ciphers** überprüfen (siehe Abbildung 3).

Abbildung 3: Überprüfen von Chiffren



Sie können überprüfen, ob diese Chiffren mit den auf dem Ursprungsserver konfigurierten Chiffren übereinstimmen. **Hinweis**: Chiffren, die DHE enthalten, werden von Microsoft IIS-Servern nicht unterstützt.

Auf einem Apache-Server können Sie die SSL-Version und die Verschlüsselungsdetails in der Datei httpd.conf überprüfen. Diese Felder können sich auch in einer separaten Datei (sslmod.conf) befinden, auf die von httpd.conf verwiesen wird. Suchen Sie die Felder SSLProtocol und SSLCipherSuite wie folgt:

```
SSLProtocol -all +TLSv1 +SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:+SHA1:+MD5:+HIGH:+MEDIUM
. . .
SSLCertificateFile /etc/httpd/ssl/server.crt
SSLCertificateKeyFile /etc/httpd/ssl/server.key
```

Um den Zertifikatsaussteller auf einem Apache-Server zu überprüfen, lesen Sie das Zertifikat mit dem Befehl openssl wie folgt:

```
> openssl x509 -in cert.pem -noout -issuer -issuer_hash
issuer= / C=US/ST=California/L=San
Jose/O=CISCO/CN=tools.cisco.com/emailAddress=webmaster@cisco.com be7cee67
```

Im Browser können Sie ein Zertifikat und dessen Details anzeigen, um die Zertifikatskette, die Version, den Verschlüsselungsschlüsseltyp, den gemeinsamen Namen des Emittenten (CN) und den Betreff/die Site-CN zu bestimmen. Klicken Sie in Internet Explorer auf das Schlosssymbol, klicken Sie auf **Zertifikat anzeigen**, und überprüfen Sie dann die Registerkarten Details und Zertifizierungspfad für diese Informationen.

Die meisten Browser verlangen, dass Clientzertifikate das PKCS12-Format und nicht das X509-

PEM-Format haben. Um das X509 PEM-Format in das PKCS12-Format zu exportieren, verwenden Sie den Befehl openssl wie folgt auf einem Apache-Server:

```
> openssl pkcs12 -export -in cert.pem -inkey key.pem -out cred.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Wenn die privaten Schlüssel verschlüsselt sind, ist die Passphrase für den Export erforderlich. Das Exportkennwort wird erneut verwendet, um Anmeldeinformationen an das WAAS-Gerät zu importieren.

Verwenden Sie den Befehl **show statistics accelerator ssl**, um die SSL-AO-Statistiken anzuzeigen.

```
WAE7326# show statistics accelerator ssl
SSL:

  Global Statistics
  -----------------
  Time Accelerator was started:                    Mon Nov 10     15:28:47 2008
  Time Statistics were Last Reset/Cleared:         Mon Nov 10    15:28:47 2008
  Total Handled Connections:                                        17                <-------
---------
  Total Optimized Connections:                                      17                <-------
---------
  Total Connections Handed-off with Compression Policies Unchanged:  0                <-------
---------
  Total Dropped Connections:                                        0                 <-------
---------
  Current Active Connections:                                       0
  Current Pending Connections:                                      0
  Maximum Active Connections:                                       3
  Total LAN Bytes Read:                                             25277124          <-------
---------
  Total Reads on LAN:                                               5798              <-------
---------
  Total LAN Bytes Written:                                          6398              <-------
---------
  Total Writes on LAN:                                              51                <-------
---------
  Total WAN Bytes Read:                                             43989             <-------
---------
  Total Reads on WAN:                                               2533              <-------
---------
  Total WAN Bytes Written:                                          10829055          <-------
---------
  Total Writes on WAN:                                              3072              <-------
---------
. . .
```

Fehlgeschlagene Sitzungen und Statistiken zur Zertifikatsverifizierung können zur Fehlerbehebung nützlich sein und können einfacher abgerufen werden, indem der folgende Filter auf dem Befehl **show statistics accelerator ssl** verwendet wird:

```
WAE# show statistics accelerator ssl | inc Failed
  Total Failed Handshakes:                                          47
```

```
  Total Failed Certificate Verifications:                          28
  Failed certificate verifications due to invalid certificates:    28
  Failed Certificate Verifications based on OCSP Check:            0
  Failed Certificate Verifications (non OCSP):                     28
  Total Failed Certificate Verifications due to Other Errors:      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
```

DNS-bezogene Statistiken können bei der Fehlerbehebung für die Konfiguration von Servernamen und Platzhalterdomänen hilfreich sein. Um diese Statistiken abzurufen, verwenden Sie den Befehl **show statistics accelerator ssl**:

```
WAE# show statistics accelerator ssl
 . . .
 Number of forward DNS lookups issued:                          18
 Number of forward DNS lookups failed:                          0
 Number of flows with matching host names:                      8
 Number of reverse DNS lookups issued:                          46
 Number of reverse DNS lookups failed:                          4
 Number of reverse DNS lookups cancelled:                       0
 Number of flows with matching domain names:                    40
 Number of flows with matching any IP rule:                     6
 . . .
 Pipe-through due to domain name mismatch:                      6
 . . .
```

Statistiken zu SSL-Weiterleitungen können für die Fehlerbehebung nützlich sein und mit dem folgenden Filter im Befehl **show statistics accelerator ssl** abgerufen werden:

```
WAE# show statistics accelerator ssl | inc renegotiation
  Total renegotiations requested by server:                       0
  Total SSL renegotiations attempted:                             0
  Total number of failed renegotiations:                          0
  Flows dropped due to renegotiation timeout:                     0
```

Verwenden Sie den Befehl **show statistics connection Optimized ssl**, um zu überprüfen, ob das WAAS-Gerät optimierte SSL-Verbindungen herstellt. Überprüfen Sie, ob in der Spalte Accel (Aktiv) für eine Verbindung "TDLS" angezeigt wird. "S" bedeutet, dass die SSL-AO wie folgt verwendet wurde:

```
WAE674# sh stat conn opt ssl
Current Active Optimized Flows:                       3
   Current Active Optimized TCP Plus Flows:           3
   Current Active Optimized TCP Only Flows:           0
   Current Active Optimized TCP Preposition Flows:    1
Current Active Auto-Discovery Flows:                  0
Current Active Pass-Through Flows:                    0
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  Local IP:Port         Remote IP:Port        PeerID             Accelerator
342     10.56.94.101:3406     10.10.100.100:443     0:1a:64:d3:2f:b8   TDLS                <---
```

```
--Look for "S"
```

Sie können Verbindungsstatistiken für geschlossene Verbindungen überprüfen, indem Sie den Befehl **show statistics connection closed ssl** verwenden.

Wenn die Verbindungen nicht optimiert werden, überprüfen Sie, ob WCCP/PBR korrekt konfiguriert und funktioniert, und suchen Sie nach asymmetrischem Routing.

Sie können die SSL-Verbindungsstatistik anzeigen, indem Sie den Befehl **show statistics connection Optimierte ssl detail** verwenden, in dem die dynamische Richtlinie angezeigt wird, die aus dem konfigurierten SSL-beschleunigten Dienst resultiert. **Hinweis**: Die konfigurierte Richtlinie ist nur die TFO-Optimierung, aber die vollständige Optimierung wird als Ergebnis des konfigurierten SSL-Service angewendet.

```
WAE674# sh stat connection optimized ssl detail
Connection Id:            1633
   Peer Id:                  00:14:5e:84:24:5f
   Connection Type:          EXTERNAL CLIENT
   Start Time:               Wed Jul 15 06:35:48 2009
   Source IP Address:        10.10.10.10
   Source Port Number:       2199
   Destination IP Address:   10.10.100.100
   Destination Port Number:  443
   Application Name:         SSL
   Classifier Name:          HTTPS
   Map Name:                 basic
   Directed Mode:            FALSE
   Preposition Flow:         FALSE
   Policy Details:
          Configured:        TCP_OPTIMIZE                                    <------TFO only
is configured
             Derived:        TCP_OPTIMIZE + DRE + LZ
                Peer:        TCP_OPTIMIZE
          Negotiated:        TCP_OPTIMIZE + DRE + LZ
             Applied:        TCP_OPTIMIZE + DRE + LZ                         <------Full
optimization applied
   Accelerator Details:
               Configured:   None
                  Derived:   None
                  Applied:   SSL                                            <------SSL
acceleration applied
                     Hist:   None

                                          Original            Optimized
                                 -------------------- --------------------
   Bytes Read:                                 1318                  584
   Bytes Written:                               208                 1950
. . .
```

Später in dieser Ausgabe werden erweiterte Details zur SSL-Sitzungsebene wie folgt angezeigt:

```
. . .
SSL : 1633

  Time Statistics were Last Reset/Cleared:                    Tue Jul 10 18:23:20 2009
  Total Bytes Read:                                           0         0
  Total Bytes Written:                                        0         0
  Memory address:                                             0x8117738
```

```
  LAN bytes read:                                          1318
  Number of reads on LAN fd:                               4
  LAN bytes written out:                                   208
  Number of writes on LAN fd:                              2
  WAN bytes read:                                          584
  Number of reads on WAN fd:                               23
  WAN bytes written out:                                   1950
  Number of writes on WAN fd:                              7
  LAN handshake bytes read:                                1318
  LAN handshake bytes written out:                         208
  WAN handshake bytes read:                                542
  WAN handshake bytes written out:                         1424
  AO bytes read:                                           0
  Number of reads on AO fd:                                0
  AO bytes written out:                                    0
  Number of writes on AO fd:                               0
  DRE bytes read:                                          10
  Number of reads on DRE fd:                               1
  DRE bytes written out:                                   10
  Number of writes on DRE fd:                              1
  Number of renegotiations requested by server:            0
  Number of SSL renegotiations performed:                  0
  Flow state:                                              0x00080000
  LAN work items:                                          1
  LAN conn state:                                          READ
  LAN SSL state:                                           SSLOK (0x3)
  WAN work items:                                          0
  WAN conn state:                                          READ
  WAN SSL state:                                           SSLOK (0x3)
  W2W work items:                                          1
  W2W conn state:                                          READ
  W2W SSL state:                                           SSLOK (0x3)
  AO  work items:                                          1
  AO  conn state:                                          READ
  DRE work items:                                          1
  DRE conn state:                                          READ
  Hostname in HTTP CONNECT:                                          <-----
Added in 4.1.5
  IP Address in HTTP CONNECT:                                        <-----
Added in 4.1.5
  TCP Port in HTTP CONNECT:                                          <-----
Added in 4.1.5
```

Fehlerbehebung bei HTTP AO-zu-SSL AO-Handoff-Verbindungen

Wenn ein Client einen Proxy durchlaufen muss, um einen HTTPS-Server zu erreichen, wird die Clientanforderung zuerst als HTTP CONNECT-Nachricht an den Proxy gesendet (wobei die tatsächliche HTTPS-Server-IP-Adresse in der CONNECT-Nachricht eingebettet ist). An diesem Punkt verarbeitet HTTP AO diese Verbindung auf den Peer-WAEs. Der Proxy erstellt einen Tunnel zwischen dem Client- und dem Server-Port und leitet nachfolgende Daten zwischen dem Client und dieser Server-IP-Adresse und diesem Server-Port weiter. Der Proxy antwortet mit der Meldung "200 OK" auf den Client zurück und übergibt die Verbindung mit dem SSL AO, da der Client beabsichtigt, über SSL mit dem Server zu kommunizieren. Der Client initiiert dann einen SSL-Handshake mit dem SSL-Server über die TCP-Verbindung (Tunnel), die vom Proxy

eingerichtet wurde.

Überprüfen Sie bei der Behebung von Problemen mit abgemeldeten Verbindungen die folgenden Punkte:

- Überprüfen Sie die Ausgabe des Befehls **show statistics accelerator http**, um zu bestätigen, dass eine Verbindung vom HTTP-AO behandelt wurde, und geben Sie sie dann an SSL AO weiter. Sehen Sie sich die Zähler Gesamtzahl der verarbeiteten Verbindungen und Gesamtzahl der an SSL übergebenen Verbindungen an. Überprüfen Sie bei Problemen Folgendes:
  - HTTP AO ist aktiviert und befindet sich im Ausführungszustand auf den Peer-WAEs.
  - Der SSL Accelerated-Service wird mit dem Port konfiguriert, der vom Client in der CONNECT-URL verwendet wird (oder implizit Port 443, wenn HTTPS verwendet wird). Oft unterscheidet sich der Proxyport vom CONNECT URL-Port, und dieser Proxyport sollte nicht im SSL-beschleunigten Dienst konfiguriert werden. Der Proxyport sollte jedoch in die Datenverkehrsklassifizierung aufgenommen werden, die der HTTP-AO zugeordnet ist.
- Überprüfen Sie die Ausgabe des Befehls **show statistics accelerator**, ob diese Verbindung von SSL AO behandelt und optimiert wurde. Schauen Sie sich die Zähler Gesamtzahl der verarbeiteten Verbindungen und Gesamtzahl optimierter Verbindungen an. Wenn die Statistikindikatoren nicht korrekt sind, führen Sie eine grundlegende SSL-Fehlerbehebung durch, wie im vorherigen Abschnitt beschrieben.
- Überprüfen Sie auf der WAE des Rechenzentrums, ob der Befehl **show statistics connection optimize detail** den Hostnamen, die IP-Adresse und den TCP-Port des SSL-Servers anzeigt. Wenn diese Felder nicht richtig eingestellt sind, überprüfen Sie Folgendes:
  - Überprüfen Sie, ob die Proxyeinstellungen für den Client-Browser korrekt sind.
  - Stellen Sie sicher, dass der DNS-Server auf der WAE des Rechenzentrums konfiguriert und erreichbar ist. Sie können einen DNS-Server auf der WAE mit dem Befehl **ip name-server** ***A.B.C.D*** konfigurieren.

Fehlerbehebung bei der Überprüfung von Serverzertifikaten

Bei der Überprüfung von Serverzertifikaten müssen Sie das richtige Zertifizierungsstellenzertifikat in die WAE des Rechenzentrums importieren.

Führen Sie die folgenden Schritte aus, um bei der Überprüfung von Serverzertifikaten Fehler zu beheben:

1. Überprüfen Sie das Serverzertifikat, und rufen Sie den Namen des Ausstellers ab. Der Name des Ausstellers im Serverzertifikat muss mit dem Betreffnamen im entsprechenden Zertifizierungsstellenzertifikat übereinstimmen. Wenn PEM-kodierte Zertifikate vorhanden sind, können Sie den folgenden **openssl-**Befehl auf einem Server verwenden, auf dem OpenSSL installiert ist:

```
> openssl x509 -in cert-file-name -noout -text
```

2. Stellen Sie sicher, dass die entsprechende Konfiguration des Crypto Pki auf der WAE des Rechenzentrums vorhanden ist. Verwenden Sie dazu den Befehl **show running-config**. Damit ein CA-Zertifikat von der WAE im Überprüfungsprozess verwendet werden kann, ist für jedes importierte CA-Zertifikat ein krypto-pki-Konfigurationselement erforderlich. Wenn z. B. ein

Zertifizierungsstellenzertifikat firma1.ca importiert wird, muss die folgende Konfiguration für die WAE im Rechenzentrum vorgenommen werden:

```
crypto pki ca company1
   ca-certificate company1.ca
   exit
```

Hinweis: Wenn ein Zertifizierungsstellenzertifikat mithilfe der GUI des Central Managers importiert wird, fügt der Central Manager automatisch die oben angegebene Konfiguration für die Crypto Pki-CA hinzu, um das importierte Zertifizierungsstellenzertifikat einzuschließen. Wenn das Zertifizierungsstellenzertifikat jedoch über die CLI importiert wird, müssen Sie die oben genannte Konfiguration manuell hinzufügen.

3. Wenn das zu überprüfende Zertifikat eine Zertifikatskette enthält, stellen Sie sicher, dass die Zertifikatskette kohärent ist und das Zertifikat des obersten Emittenten in die WAE importiert wird. Verwenden Sie den Befehl **openssl verify**, um das Zertifikat zuerst separat zu überprüfen.

4. Wenn die Überprüfung immer noch fehlschlägt, überprüfen Sie das Debug-Protokoll des SSL Accelerator. Verwenden Sie die folgenden Befehle, um die Debug-Protokollierung zu aktivieren:

```
wae# config
wae(config)# logging disk priority debug
wae(config)# logging disk enable
wae(config)# exit
wae# undebug all
wae# debug accelerator ssl verify
wae# debug tfo connection all
```

5. Initiieren Sie eine Testverbindung, und überprüfen Sie anschließend die /local/local1/errorlog/sslao-errorlog.current. Diese Datei sollte den Namen des Emittenten angeben, der im Serverzertifikat enthalten war. Stellen Sie sicher, dass der Name des Ausstellers genau mit dem Betreffnamen des Zertifizierungsstellenzertifikats übereinstimmt.

Wenn weitere interne Fehler in den Protokollen vorhanden sind, können zusätzliche Debugoptionen aktiviert werden.

6. Auch wenn der Name des Emittenten und die Betreffnamen übereinstimmen, ist das Zertifizierungsstellenzertifikat möglicherweise nicht das richtige. Wenn in solchen Fällen das Serverzertifikat von einer bekannten Zertifizierungsstelle ausgestellt wird, kann ein Browser verwendet werden, um direkt (ohne WAAS) den Server zu erreichen. Wenn der Browser die Verbindung herstellt, kann das Zertifikat überprüft werden, indem Sie auf das Sperrsymbol klicken, das unten rechts im Browserfenster oder in der Adressleiste des Browsers angezeigt wird. Die Zertifikatdetails können angeben, welches Zertifizierungsstellenzertifikat mit diesem Serverzertifikat übereinstimmt. Aktivieren Sie das Feld Seriennummer im Zertifizierungsstellenzertifikat. Diese Seriennummer muss mit der Seriennummer des Zertifikats übereinstimmen, das in die WAE des Rechenzentrums importiert wird.

7. Wenn Sie die Überprüfung auf OCSP-Widerruf aktiviert haben, deaktivieren Sie sie, und überprüfen Sie, ob die Zertifikatüberprüfung von sich aus funktioniert. Hilfe bei der Behebung von OCSP-Einstellungen finden Sie im Abschnitt "Troubleshooting OCSP Revocation Checks" (Fehlerbehebung bei OCSP-Revocation Checks).

Problembehandlung bei der Überprüfung von Client-Zertifikaten

Die Verifizierung des Client-Zertifikats kann auf dem Ursprungsserver und/oder der WAE im Rechenzentrum aktiviert werden. Wenn WAAS zum Beschleunigen des SSL-Datenverkehrs verwendet wird, ist das vom Ursprungsserver empfangene Clientzertifikat das Zertifikat, das in dem vom **Crypto SSL Services-**Befehl für die **globalen** Einstellungen des WAE-Befehls für das Rechenzentrum oder dem selbst signierten Zertifikat für das WAE-Gerät des Rechenzentrums angegebenen Zertifikat angegeben ist, wenn der Systemschlüssel nicht konfiguriert ist. Wenn die Überprüfung von Clientzertifikaten auf dem Ursprungsserver fehlschlägt, kann dies darauf zurückzuführen sein, dass das WAE-Maschinenzertifikat des Rechenzentrums auf dem Ursprungsserver nicht verifizierbar ist.

Wenn die Überprüfung von Client-Zertifikaten auf der WAE des Rechenzentrums nicht funktioniert, ist dies wahrscheinlich, weil das Zertifizierungsstellen-Zertifikat, das mit dem Client-Zertifikat übereinstimmt, nicht in die WAE des Rechenzentrums importiert wird. Anweisungen zum Überprüfen, ob das richtige CA-Zertifikat in die WAE importiert wurde, finden Sie im Abschnitt "Problembehandlung bei der Überprüfung von Serverzertifikaten".

Fehlerbehebung: Überprüfung des Peer-WAE-Zertifikats

Führen Sie die folgenden Schritte aus, um Probleme bei der Überprüfung von Peer-Zertifikaten zu beheben:

1. Überprüfen Sie, ob es sich bei dem zu überprüfenden Zertifikat um ein Zertifikat mit Zertifizierungsstellennummer handelt. Ein selbstsigniertes Zertifikat von einer WAE kann nicht von einer anderen WAE verifiziert werden. WAEs werden standardmäßig mit selbstsignierten Zertifikaten geladen. Ein selbstsigniertes Zertifikat muss mithilfe des Befehls **crypto ssl services global-settings machine-cert-key** konfiguriert werden.

2. Überprüfen Sie, ob das richtige Zertifizierungsstellenzertifikat auf das Gerät geladen wird, das das Zertifikat verifiziert. Wenn z. B. Peer-cert-verify auf der WAE des Rechenzentrums konfiguriert ist, muss das WAE-Zertifikat der Außenstelle mit CA-Signatur versehen und dasselbe signierende CA-Zertifikat in die WAE des Rechenzentrums importiert werden. Vergessen Sie nicht, eine Zertifizierungsstelle mit dem Befehl **crypto pki** zur Verwendung des importierten Zertifikats zu erstellen, wenn Sie das Zertifikat manuell über die CLI importieren. Beim Import über die GUI Central Manager erstellt der Central Manager automatisch eine passende Konfiguration für die Crypto Pki-CA.

3. Wenn die Überprüfung der Peer-WAE immer noch fehlschlägt, überprüfen Sie die Debug-Protokolle wie im Abschnitt "SSL AO Logging" beschrieben.

Fehlerbehebung bei der Prüfung der OCSP-Widerrufung

Wenn das System Schwierigkeiten hat, erfolgreiche SSL-Verbindungen herzustellen, bei denen die Überprüfung des Online Certificate Status Protocol (OCSP)-Widerrufs aktiviert ist, befolgen Sie die folgenden Schritte zur Fehlerbehebung:

1. Stellen Sie sicher, dass der OCSP-Responder-Service auf dem Responder-Server ausgeführt wird.
2. Stellen Sie eine gute Verbindung zwischen der WAE und dem Responder sicher. Verwenden Sie die Befehle **ping** und **telnet** (zum entsprechenden Port) von der WAE, um zu prüfen.
3. Bestätigen Sie, dass das zu validierende Zertifikat tatsächlich gültig ist. Das Ablaufdatum und die richtige URL der Antworten sind in der Regel Bereiche, in denen Probleme auftreten.
4. Überprüfen Sie, ob das Zertifikat für OCSP-Antworten in die WAE importiert wird. Antworten von einem OCSP-Responder werden ebenfalls signiert, und das

Zertifizierungsstellenzertifikat, das mit den OCSP-Antworten übereinstimmt, muss sich auf der WAE befinden.

5. Überprüfen Sie die Ausgabe des Befehls **show statistics accelerator ssl**, um nach OCSP-Statistiken zu suchen, und überprüfen Sie die Zähler für OCSP-Fehler.
6. Wenn die OCSP-HTTP-Verbindung einen HTTP-Proxy durchläuft, versuchen Sie, den Proxy zu deaktivieren, um festzustellen, ob er hilft. Wenn dies hilfreich ist, stellen Sie sicher, dass die Proxykonfiguration den Verbindungsfehler nicht verursacht. Wenn die Proxy-Konfiguration in Ordnung ist, kann es zu einer gewissen HTTP-Header-Besonderheit kommen, die möglicherweise zu einer Inkompatibilität mit dem Proxy führt. Erfassen Sie eine Paketverfolgung für weitere Untersuchungen.
7. Wenn alles andere fehlschlägt, müssen Sie möglicherweise eine Paketverfolgung der ausgehenden OCSP-Anforderung für das weitere Debuggen erfassen. Sie können die **tcpdump**- oder **tethereal-**Befehle verwenden, wie im Abschnitt "Erfassen und Analysieren von Paketen" im Artikel zur vorläufigen WAAS-Fehlerbehebung beschrieben.

Die vom WAE des Rechenzentrums verwendete URL zum Erreichen eines OCSP-Responders wird auf zwei Arten abgeleitet:

- Die statische OCSP-URL, die mit dem Konfigurationsbefehl **crypto pki global-settings** konfiguriert wurde.
- Die im zu überprüfenden Zertifikat angegebene OCSP-URL

Wenn die URL aus dem zu überprüfenden Zertifikat abgeleitet ist, muss unbedingt sichergestellt werden, dass die URL erreichbar ist. Aktivieren Sie die SSL Accelerator-OCSP-Debug-Protokolle, um die URL zu ermitteln, und überprüfen Sie dann die Verbindung zum Responder. Weitere Informationen zur Verwendung von Debug-Protokollen finden Sie im nächsten Abschnitt.

Fehlerbehebung DNS-Konfiguration

Wenn das System Probleme bei der Optimierung von SSL-Verbindungen mit Servernamen- und Serverdomänenkonfigurationen hat, befolgen Sie die folgenden Schritte zur Fehlerbehebung:

1. Stellen Sie sicher, dass der auf der WAE konfigurierte DNS-Server erreichbar ist und Namen auflösen kann. Verwenden Sie den folgenden Befehl, um den konfigurierten DNS-Server zu überprüfen:

```
WAE# sh running-config | include name-server
ip name-server 2.53.4.3

Try to perform DNS or reverse DNS lookup on the WAE using the following commands:

WAE# dnslookup www.cisco.com
The specified host/domain name is unknown !
```

Diese Antwort gibt an, dass der Name von den konfigurierten Namenservern nicht aufgelöst werden kann.

Versuchen Sie, einen Ping/Traceoute für die konfigurierten Nameserver durchzuführen, um deren Verfügbarkeit und die Round-Trip-Zeit zu überprüfen.

```
WAE# ping 2.53.4.3
```

```
PING 2.53.4.3 (2.53.4.3) 56(84) bytes of data.
--- 2.53.4.3 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4008ms


WAE# traceroute 2.53.4.3
traceroute to 2.53.4.3 (2.53.4.3), 30 hops max, 38 byte packets
1  2.53.4.33 (2.53.4.33)  0.604 ms  0.288 ms  0.405 ms
2  * * *
3  * * *
4  * * *
5  * * *
```

2. Wenn der DNS-Server erreichbar ist und Namen aufgelöst werden können und die SSL-Verbindungen immer noch nicht optimiert werden, stellen Sie sicher, dass der beschleunigte Dienst, der die angegebene Domäne oder den angegebenen Hostnamen konfiguriert, aktiv ist und es keine Alarme für den SSL AO gibt. Verwenden Sie die folgenden Befehle:

```
WAE#  show alarms
Critical Alarms:
----------------
      Alarm ID                Module/Submodule              Instance
 ---------------            --------------------          ---------------
 1 accl_svc_inactive         sslao/ASVC/asvc-host         accl_svc_inactive
 2 accl_svc_inactive         sslao/ASVC/asvc-domain       accl_svc_inactive

Major Alarms:
-------------
None

Minor Alarms:
-------------
None
```

Das Vorhandensein des Alarms "accl_svc_inactive" ist ein Hinweis darauf, dass die beschleunigte Servicekonfiguration eine gewisse Diskrepanz aufweist und es bei einem oder mehreren beschleunigten Diensten zu Überschneidungen bei der Konfiguration von Servereinträgen kommen kann. Überprüfen Sie die beschleunigte Servicekonfiguration, und stellen Sie sicher, dass die Konfiguration korrekt ist. Verwenden Sie den folgenden Befehl, um die Konfiguration zu überprüfen:

```
WAE# show crypto ssl accelerated service
Accelerated Service     Config State    Oper State      Cookie
-------------------     ------------    -----------     ------
asvc-ip                  ACTIVE          ACTIVE          0
asvc-host                ACTIVE          INACTIVE        1
asvc-domain              ACTIVE          INACTIVE        2
```

Verwenden Sie den folgenden Befehl, um Details zu einem bestimmten beschleunigten Dienst zu überprüfen:

```
WAE# show crypto ssl accelerated service asvc-host
 Name: asvc-host
   Config state: ACTIVE, Oper state: INACTIVE, Cookie: 0x3, Error vector: 0x0
   No server IP addresses are configured
   The following server host names are configured:
     lnxserv.shilpa.com port 443
```

```
        Host 'lnxserv.shilpa.com' resolves to following IPs:
        --none--
   No server domain names are configured
```

Ein Grund dafür, dass der Betriebsstatus des beschleunigten Services INACTIVE sein kann, ist ein DNS-Fehler. Wenn beispielsweise ein Server-Hostname in der beschleunigten Servicekonfiguration vorhanden ist und die WAE die Server-IP-Adresse nicht auflösen kann, kann die entsprechende dynamische Richtlinie nicht konfiguriert werden.

3. Wenn der Statistikindikator für "Pipe-through by non-matching domain name" (Durchleitung aufgrund des nicht übereinstimmenden Domänennamens) ansteigt, ist dies ein Hinweis darauf, dass die SSL-Verbindung für einen Server konfiguriert ist, der für die Optimierung konfiguriert ist. Überprüfen Sie die Policy Engine-Einträge mit dem folgenden Befehl:

```
WAE#sh policy-engine application dynamic
       Number:     1   Type: Any->Host (6)  User Id: SSL (4)
       Src: ANY:ANY  Dst: 2.53.4.2:443
       Map Name: basic
       Flags: TIME_LMT DENY
       Seconds: 10  Remaining: 5  DM Index: 32767
       Hits: 1  Flows: - NA -  Cookie: 0x2EEEEEEE
       DM Ref Index: - NA -  DM Ref Cnt: 0
```

Überprüfen Sie den Verbindungsstatus mit dem Befehl **show statistics connection**. Die erste Verbindung sollte einen Accelerator von TSGDL anzeigen, und die nachfolgenden Verbindungen sollten bis zur Lebensdauer des TIME_DENY-Richtlinieneintrags TDL sein.

4. Wenn sich der DNS-Server im Hinblick auf die WAE im Rechenzentrum im WAN befindet oder die umgekehrte DNS-Reaktionszeit zu lang ist, werden möglicherweise einige Verbindungen verworfen. Dies hängt vom Client-Timeout und der rDNS-Reaktionszeit ab. In diesem Fall erhöht sich der Zähler für "Number of reverse DNS lookups canceled" (Anzahl der abgebrochenen DNS-Lookups), und die Verbindung wird getrennt. Diese Situation ist ein Hinweis darauf, dass der DNS-Server nicht reagiert oder sehr langsam ist und/oder NSCD auf WAAS nicht funktioniert. Der NSCD-Status kann mit dem Befehl **show alarm (Alarme anzeigen)** überprüft werden. Die Wahrscheinlichkeit, dass dies geschieht, ist sehr gering, da in den meisten Bereitstellungen der DNS-Server sich im selben LAN wie die WAE des Rechenzentrums befinden wird.

Fehlerbehebung HTTP-zu-SSL-AO-Verkettung

HINWEIS: Die HTTP-zu-SSL-AO-Verkettung wurde in WAAS Version 4.3.1 eingeführt. Dieser Abschnitt gilt nicht für frühere WAAS-Versionen.

Durch die Verkettung kann ein AO während der Lebensdauer eines Datenflusses jederzeit eine weitere AO einfügen, und beide AOs können ihre AO-spezifische Optimierung unabhängig auf den Datenfluss anwenden. Die AO-Verkettung unterscheidet sich von der AO-Handoff-Funktion, die WAAS in Versionen vor 4.3.1 bereitstellt, da die erste AO-Verkettung den Fluss weiter optimiert.

Das SSL AO verarbeitet zwei Verbindungstypen:

- Byte-0 SSL: Das SSL AO empfängt die Verbindung zuerst und schließt den SSL-Handshake ab. Er analysiert den ursprünglichen Teil der Payload, um eine HTTP-Methode zu überprüfen. Wenn die Payload HTTP angibt, wird HTTP AO eingefügt. andernfalls wird die übliche TSDL-

Optimierung angewendet.
- Proxy CONNECT: Die HTTP-AO empfängt zuerst die Verbindung. Er identifiziert die CONNECT-Headermethode in der Client-Anfrage und fügt die SSL-AO ein, nachdem der Proxy dies mit einer 200 OK-Nachricht bestätigt hat.

Das SSL AO verwendet einen einfachen HTTP-Parser, der die folgenden HTTP-Methoden erkennt: GET, HEAD, POST, PUT, OPTIONEN, TRACE, COPY, LOCK, POLL, BCOPY, BMOVE, MKCOL, DELETE, SUCHE, LOCKIEREN, BDELETE, PROPFIND, BPROPFIND, PROPPATCH, SUBSCRIBE, BPROPPATCH, UNSUBSCRIBE, UMX__MS_ENCH ATTS. Sie können den Befehl **debug accelerator ssl parser** verwenden, um Probleme im Zusammenhang mit dem Parser zu debuggen. Sie können den Befehl **show stat accel ssl payload http/other** verwenden, um Statistiken des Datenverkehrs anzuzeigen, der anhand des Payload-Typs klassifiziert wurde.

Tipps zur Fehlerbehebung:

1. Stellen Sie sicher, dass die HTTPS-Funktion in der HTTP-AO-Konfiguration aktiviert ist, da diese der HTTP-AO gehört. Ausführliche Informationen finden Sie im Artikel Troubleshooting the HTTP AO (Fehlerbehebung bei HTTP-AO).
2. Überprüfen Sie den Verbindungsstatus mit dem Befehl **show stat connection** (**Verbindung anzeigen)**. Bei korrekter Optimierung sollte THSDL als Hinweis auf TCP-, HTTP-, SSL- und DRE-LZ-Optimierung angezeigt werden. Wenn eine dieser Optimierungen fehlt, müssen Sie weiter auf diesem Optimierer (SSL, HTTP usw.) debuggen. Wenn beispielsweise der Verbindungsstatus THDL anzeigt, bedeutet dies, dass die SSL-Optimierung nicht auf die Verbindung angewendet wurde. Einzelheiten zu Debugproblemen im Zusammenhang mit SSL AO folgen.
3. Stellen Sie sicher, dass SSL AO aktiviert ist und sich im aktuellen Zustand befindet (siehe Abschnitt "Problembehandlung bei SSL AO").
4. Vergewissern Sie sich, dass keine Alarme vorhanden sind, indem Sie den Befehl **show alarm** verwenden.
5. Wenn der SSL-Datenverkehr nicht optimiert wird, stellen Sie sicher, dass die Server-IP-Adresse, der Hostname oder der Domänenname und die Portnummer als Teil des beschleunigten Services hinzugefügt werden.
6. Vergewissern Sie sich, dass der beschleunigte Dienst im AKTIVEN Zustand ist, indem Sie den Befehl **show crypto ssl services accelerated-service *ASVC-name*** verwenden (siehe Abschnitt "Troubleshooting DNS Configuration").
7. Stellen Sie sicher, dass die Policy Engine über einen Eintrag für diesen Server und Port verfügt. Verwenden Sie dazu den Befehl **show policy-engine application dynamic**.
8. Wenn der Zielserver SSL auf einem nicht standardmäßigen Port verwendet (der Standardwert ist 443), stellen Sie sicher, dass dies in der Richtlinie-Engine-Konfiguration wiedergegeben wird. Der Central Manager verwendet diese Informationen, um SSL-Datenverkehrsdaten zu melden.
9. Stellen Sie sicher, dass der konfigurierte Hostname mithilfe des Befehls **show crypto ssl services accelerated-service *ASVC-name*** in eine gültige IP-Adresse aufgelöst wird. Wenn keine IP-Adresse gefunden wurde, überprüfen Sie, ob der Namenserver richtig konfiguriert ist. Überprüfen Sie auch die Ausgabe des Befehls **dnslookup *IP-Adresse***.

```
wae# sh run no-policy
. . .
```

```
crypto ssl services accelerated-service sslc
  version all
  server-cert-key test.p12
  server-ip 2.75.167.2 port 4433
  server-ip any port 443
  server-name mail.yahoo.com port 443
  server-name mail.google.com port 443
  inservice


wae# sh crypto ssl services accelerated-service sslc
Name: sslc
Config state: ACTIVE, Oper state: ACTIVE, Cookie: 0x0, Error vector: 0x0

   The following server IP addresses are configured:
     2.75.167.2 port 4433
     any port 443

   The following server host names are configured:
     mail.yahoo.com port 443
         Host 'mail.yahoo.com' resolves to following IPs:
         66.163.169.186

     mail.google.com port 443
         Host 'mail.google.com' resolves to following IPs:
         74.125.19.17
         74.125.19.18
         74.125.19.19
         74.125.19.83


wae# dnslookup mail.yahoo.com
Official hostname: login.lga1.b.yahoo.com
         address: 66.163.169.186
Aliases: mail.yahoo.com
Aliases: login.yahoo.com
Aliases: login-global.lgg1.b.yahoo.com

wae# dnslookup mail.google.com
Official hostname: googlemail.l.google.com
         address: 74.125.19.83
         address: 74.125.19.17
         address: 74.125.19.19
         address: 74.125.19.18
Aliases: mail.google.com
```

SSL-AO-Protokollierung

Die folgenden Protokolldateien sind zur Fehlerbehebung bei SSL AO-Problemen verfügbar:

- Transaktionsprotokolldateien: /local1/logs/tfo/working.log (und /local1/logs/tfo/tfo_log_*.txt)
- Debugging-Protokolldateien: /local1/errorlog/sslao-errorlog.current (und slao-errorlog.*)

Um das Debuggen zu vereinfachen, sollten Sie zunächst eine ACL einrichten, um Pakete auf einen Host zu beschränken.

```
WAE674(config)# ip access-list extended 150 permit tcp host 10.10.10.10 any
WAE674(config)# ip access-list extended 150 permit tcp any host 10.10.10.10
```

Um die Transaktionsprotokollierung zu aktivieren, verwenden Sie den Konfigurationsbefehl

transaction-logs wie folgt:

```
wae(config)# transaction-logs flow enable
wae(config)# transaction-logs flow access-list 150
```

Sie können das Ende einer Transaktionsprotokolldatei anzeigen, indem Sie den Befehl **type-tail** wie folgt verwenden:

```
wae# type-tail tfo_log_10.10.11.230_20090715_130000.txt
Wed Jul 15 14:35:48 2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :OT :START  :EXTERNAL
CLIENT :00.14.5e.84.24.5f :basic
 :SSL :HTTPS :F :(TFO) (DRE,LZ,TFO) (TFO) (DRE,LZ,TFO) (DRE,LZ,TFO) :<None> :(None) (None)
(SSL) :<None> :<None>  :0 :332
Wed Jul 15 14:36:06
2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :SODRE :END :165 :15978764 :63429 :10339 :0
Wed Jul 15 14:36:06 2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :OT :END :EXTERNAL
CLIENT :(SSL) :468 :16001952 :80805 :27824
```

Verwenden Sie die folgenden Befehle, um die Debug-Protokollierung für SSL AO einzurichten und zu aktivieren.

HINWEIS: Die Debug-Protokollierung ist CPU-intensiv und kann eine große Menge an Ausgabe generieren. Verwenden Sie sie sorgfältig und sparsam in einer Produktionsumgebung.

Sie können die detaillierte Protokollierung auf dem Datenträger wie folgt aktivieren:

```
WAE674(config)# logging disk enable
WAE674(config)# logging disk priority detail
```

Sie können die Debug-Protokollierung für Verbindungen in der ACL wie folgt aktivieren:

```
WAE674# debug connection access-list 150
```

Für das SSL AO-Debugging sind folgende Optionen verfügbar:

```
WAE674# debug accelerator ssl ?
 accelerated-svc   enable accelerated service debugs
 alarm             enable SSL AO alarm debugs
 all               enable all SSL accelerator debugs
 am                enable auth manager debugs
 am-generic-svc    enable am generic service debugs
 bio               enable bio layer debugs
 ca                enable cert auth module debugs
 ca-pool           enable cert auth pool debugs
 cipherlist        enable cipherlist debugs
 client-to-server  enable client-to-server datapath debugs
 dataserver        enable dataserver debugs
 flow-shutdown     enable flow shutdown debugs
 generic           enable generic debugs
 ocsp              enable ocsp debugs
 oom-manager       enable oom-manager debugs
 openssl-internal  enable opnessl internal debugs
 peering-svc       enable peering service debugs
 session-cache     enable session cache debugs
```

```
 shell             enable SSL shell debugs
 sm-alert          enable session manager alert debugs
 sm-generic        enable session manager generic debugs
 sm-io             enable session manager i/o debugs
 sm-pipethrough    enable sm pipethrough debugs
 synchronization   enable synchronization debugs
 verify            enable certificate verification debugs
 waas-to-waas      enable waas-to-waas datapath debugs
```

Sie können die Debug-Protokollierung für SSL-Verbindungen aktivieren und dann das Ende des Debug-Fehlerprotokolls wie folgt anzeigen:

```
WAE674# debug accelerator ssl all
WAE674# debug connection all
Enabling debug messages for all connections.
Are you sure you want to do this? (y/n) [n]y
WAE674# type-tail errorlog/sslao-errorlog.current follow
```

Fehlerbehebung bei Warnmeldungen zum Ablauf eines Zertifikats auf NME- und SRE-Modulen

Das SSL AO generiert Alarme, wenn das selbst signierte Computerzertifikat abgelaufen ist (oder innerhalb von 30 Tagen nach Ablauf liegt) und auf dem WAAS-Gerät kein benutzerdefiniertes globales Computerzertifikat konfiguriert ist. Die WAAS-Software generiert selbstsignierte Zertifikate mit einem Ablaufdatum von 5 Jahren ab dem ersten Start des WAAS-Geräts.

Die Uhr in allen WAAS-NME- und SRE-Modulen ist beim ersten Start auf den 1. Januar 2006 festgelegt, obwohl das NME- oder SRE-Modul jünger ist. Dadurch läuft das selbstsignierte Zertifikat am 1. Januar 2011 ab, und das Gerät generiert Alarme zum Ablauf des Zertifikats.

Wenn Sie das werkseitige Standardzertifikat nicht als globales Zertifikat verwenden und stattdessen ein benutzerdefiniertes Zertifikat für das SSL AO verwenden, tritt dieser unerwartete Ablauf nicht auf, und Sie können das benutzerdefinierte Zertifikat nach Ablauf des Zertifikats aktualisieren. Wenn Sie das NME- oder SME-Modul mit einem neuen Software-Image aktualisiert und die Uhr mit einem neueren Datum synchronisiert haben, tritt dieses Problem möglicherweise nicht auf.

Das Symptom des Ablauf eines Zertifikats ist eine der folgenden Alarme (hier in der Ausgabe des Befehls **show alarm**):

```
Major Alarms:
-------------
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 cert_near_expiration      sslao/SGS/gsetting           cert_near_expiration
```

oder

```
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 cert_expired              sslao/SGS/gsetting           cert_expired
```

Die GUI Central Manager meldet den folgenden Alarm: "Certificate__waas-self__.p12 ist nahezu

abgelaufen und wird in den globalen Einstellungen als "Machine cert" (Systemzertifizierung) konfiguriert."

Sie können eine der folgenden Lösungen verwenden, um dieses Problem zu beheben:

- Konfigurieren Sie ein anderes Zertifikat für globale Einstellungen:

```
SRE# crypto generate self-signed-cert waas-self.p12 rsa modulus 1024
SRE# config
SRE(config)# crypto ssl services global-settings machine-cert-key waas-self.p12
```

- Aktualisieren Sie das selbstsignierte werkseitige Zertifikat mit einem späteren Ablaufdatum. Für diese Lösung ist ein Skript erforderlich, das Sie über das Cisco TAC erhalten.

HINWEIS: Dieses Problem wird durch die Behebung des Problems mit dem in den WAAS-Softwareversionen 4.1.7b, 4.2.3c und 4.3.3 veröffentlichten Vorbehalt CSCte05426 behoben. Das Ablaufdatum der Zertifizierung wird in 2037 geändert.