WAAS - probleemoplossing bij de SSL AO

Hoofdstuk: Probleemoplossing voor SSL AO

Dit artikel beschrijft hoe u een probleem met de SSL AO kunt oplossen.

Inh

Ho
De
Vo
Op
To
Pro
Pro
Pro
Pro
Pro
Pro
Vid
Pro
Vo
WC
Ap
Pro
har
Pro
Pro
Pro
NA

Inhoud

SSL-versnellerkaart - Overzicht

De SSL-versneller (beschikbaar in 4.1.3 en hoger) optimaliseert het gecodeerde Secure Socket

Layer (SSL) en Transport Layer Security (TLS) verkeer. De SSL-versneller verstrekt verkeersencryptie en decryptie binnen WAAS om end-to-end verkeersoptimalisatie mogelijk te maken. De SSL-versneller biedt ook een veilig beheer van de coderingscertificaten en -toetsen.

In een WAAS netwerk, handelt het datacenter WAE als een vertrouwde intermediair knooppunt voor SSL-verzoeken door de client. De privé sleutel en het servercertificaat worden opgeslagen op het datacenter WAE. Het datacenter WAE neemt deel aan de SSL-handdruk om de sessiesleutel af te leiden, die het veilig in-band distribueert naar de aftakking WAE, waardoor de aftakking WAE clientverkeer kan decrypteren, optimaliseren, herversleutelen en doorsturen via WAN naar het datacenter WAE. Het datacenter WAE onderhoudt een afzonderlijke SSL-sessie met de oorspronkelijke server.

De volgende services zijn relevant voor SSL/TLS-optimalisatie:

- Accelerated Service - een configuratie-eenheid die versnellingskenmerken beschrijft die moeten worden toegepast op een SSL-server of een reeks servers. Specificeert de certificering en privé-toets die moeten worden gebruikt bij het poseren als een vertrouwde intermediair, te gebruiken ciphers, toegestane SSL-versie en instellingen voor verificatie van certificaten.
- Peerservice - een configuratie-eenheid die versnellingskenmerken beschrijft die moeten worden toegepast voor in-band SSL-verbindingen tussen een tak en een datacenter-WAE's. Deze service wordt gebruikt voor het overdragen van sessiekerninformatie van datacenter naar tak WAE's voor het optimaliseren van SSL-verbindingen.
- Central Manager Admin Service - Niet direct gebruikt door de SSL-versneller, maar te gebruiken door een beheerder voor het configuratiebeheer van SSL-versnelde services. Ook gebruikt om certificaten en privé toetsen te uploaden die in SSL versnelde services kunnen worden gebruikt.
- Central Manager Management Service - niet rechtstreeks gebruikt door de SSL-accelerator, maar gebruikt voor communicatie tussen applicatie-apparaten en de Central Manager. Deze service wordt gebruikt voor configuratiebeheer, veilig opslagencryptie-sleutelherstel en de updates van de apparaatstatus.

De Central Manager Secure Store is essentieel voor de SSL AO om te werken omdat het beveiligde encryptiesleutels voor alle WAE's opslaat. Na elke herlading van de Centrale Manager moet de beheerder de veilige winkel heropenen door het wachtwoord van de **veilige opslag** van het **cms open** bevel te voorzien. WAE haalt automatisch de beveiligde encryptie-toets van de Central Manager op wanneer de WAE-herstart wordt gestart, zodat er na een herlading geen actie in de WAE vereist is.

Als klanten een HTTP proxy-oplossing gebruiken, wordt de initiële verbinding verwerkt door de HTTP AO, die het herkent als een SSL-tunnelverzoek om poort 443. De HTTP AO zoekt een matching SSL-versnelde service die gedefinieerd is op het datacenter WAE en wanneer er een match is, maakt hij de verbinding met SSL AO af. Maar het verkeer dat HTTP AO afgeeft naar SSL AO voor een HTTPS-proxy wordt gemeld als onderdeel van de webtoepassingsstatistieken, niet in de SSL-toepassing. Als HTTP AO geen overeenkomst vindt, wordt de verbinding geoptimaliseerd zoals per statische HTTPS (SSL) beleidsconfiguratie.

SSL AO kan zelfgetekende certificaten in plaats van CA-ondertekende certificaten gebruiken, die kunnen helpen in het implementeren van bewijs van concept (POC) systemen en in het oplossen van SSL kwesties. Door zelfgetekende certificaten te gebruiken, kunt u snel een WAAS-systeem implementeren zonder de oorsprongserver-certificaten te hoeven importeren, en u kunt certificaten elimineren als een mogelijke bron van problemen. U kunt een zichzelf ondertekend certificaat in

de Centrale Manager configureren wanneer u een SSL Accelerated Service maakt. Wanneer u echter een zichzelf ondertekend certificaat gebruikt, zal de browser van de cliënt een veiligheidswaarschuwing tonen dat het certificaat onbetrouwbaar is (omdat het niet door een bekend CA wordt ondertekend). Om deze veiligheidswaarschuwing te vermijden, installeert u het certificaat in de winkel Trusted Root Certified Certified Autoriteiten op de browser van de client. (Klik in Internet Explorer op de beveiligingswaarschuwing op **Certificaat bekijken** en klik vervolgens in het dialoogvenster Certificaat op **Installeer** het **Certificaat** en vul de wizard Certificaat importeren in.)

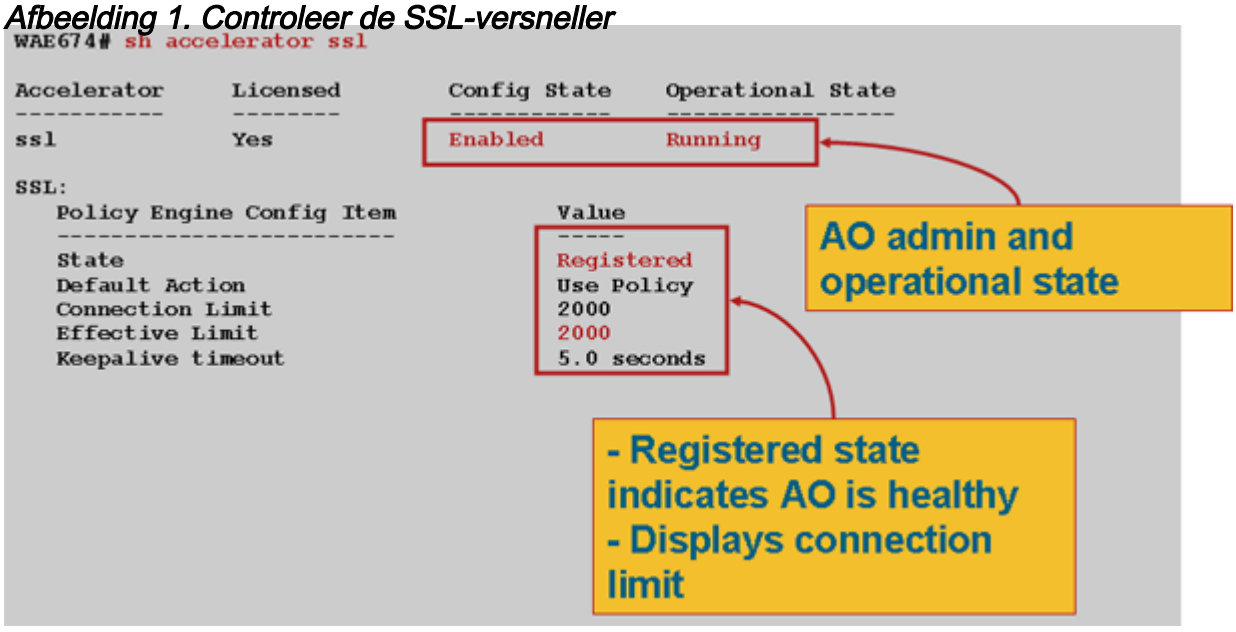
Het configureren van de SSL Management Services is optioneel en stelt u in staat de SSL versie en de algoritme lijst die voor Centrale Manager communicatie wordt gebruikt te veranderen naar WAE's en naar de browser (voor administratieve toegang). Als u ciphers vormt die niet door uw browser worden ondersteund, zult u de verbinding met de Central Manager verliezen. In dit geval, gebruik de **crypto SSL beheer-service** configuratieopdracht van de CLI om de SSL beheerservice instellingen terug te zetten naar de standaard.

Probleemoplossing voor SSL AO

U kunt de algemene AO-configuratie en -status controleren met de **show-versneller** en de **licentie-**opdrachten **weergeven**, zoals beschreven in het artikel Problemen oplossen bij Toepassingsversnelling. De Enterprise-licentie is vereist voor SSL-accelerator.

Controleer vervolgens de status die specifiek is voor SSL AO op zowel het datacenter als de tak WAE's door de opdracht **Show accelerator** ssl te gebruiken, zoals in afbeelding 1. U wilt zien dat SSL AO is ingeschakeld, actief en geregistreerd en dat de verbindingslimiet wordt weergegeven. Als de Config-staat is ingeschakeld maar de operationele staat is uitgeschakeld, duidt dit op een licentieprobleem. Als de Operationele Staat gehandicapt is, kan het zijn omdat WAE de SSL toetsen niet van de veilige opslag van de Centrale Manager kan terugkrijgen, of omdat de veilige opslag niet open is of de Centrale Manager onbereikbaar is. Gebruik de opdrachten **voor** het **weergeven van cms en** het **pingelen** om te bevestigen dat de functie Central Manager bereikbaar is.

Afbeelding 1. Controleer de SSL-versneller



Als u een operationele staat van generaal Crypto Params ziet, wacht dan tot de status draait. Dat kan een paar minuten duren na de herstart. Als u een staat van het ophalen van sleutels van CM meer dan een paar minuten ziet, kan dit erop wijzen dat de CMS-dienst op de Central Manager niet actief is, dat er geen netwerkconnectiviteit is voor de Central Manager, dat de WAAS-versies

op de WAE en de Central Manager niet compatibel zijn of dat de Central Manager Secure Store niet open is.

U kunt controleren of de veilige opslag van de Centrale Manager op de volgende manier wordt geïnitialiseerd en geopend door de opdracht **van de** showcms **Secure-Store** te gebruiken:

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

Als de veilige winkel niet wordt geïnitialiseerd of geopend, zult u kritieke alarmen zoals mstore_key_fail en safe zien. U kunt de beveiligde winkel openen met de **cms-beveiligde opslagopdracht** of via de Central Manager, **Admin > Secure Store**.

Tip: Document het veilige opslagwachtwoord om te voorkomen dat u de beveiligde winkel opnieuw moet instellen, indien u het wachtwoord vergeet.

Als er een probleem is met de diskencryptie op een WAE, kan dit ook verhinderen dat SSL AO werkt. Gebruik de opdracht Show disk details om te controleren of diskencryptie is ingeschakeld en controleer of de DELEN CONTENT en SPOOL zijn gemonteerd. Als deze partities worden gemonteerd, duidt dit erop dat de toetsen voor diskencryptie met succes zijn opgeroepen van de Central Manager en dat versleutelde gegevens kunnen worden geschreven en gelezen vanaf de disks. Als de opdracht **op** de **disk details tonen** "System is initializing" laat zien, dat aangeeft dat de encryptiesleutels nog niet zijn opgehaald uit de Central Manager en dat de disks nog niet zijn gemonteerd. WAE zal in deze staat geen versnellingsservices leveren. Als WAE de toetsen voor diskencryptie niet uit de Central Manager kan ophalen, zal het alarm opvoeren.

U kunt controleren of de SSL-versnelde service is geconfigureerd en de status "Ingeschakeld" is op de WAE van het datacenter (kies in Central Manager het apparaat en kies vervolgens **Configureren > Acceleration > SSL Accelerated Services**). Een geconfigureerde en enabled-versnelde service kan door de SSL-versneller inactief worden gemaakt als gevolg van de volgende voorwaarden:

- Het certificaat dat is ingesteld in de versnelde service is verwijderd uit de WAE. Gebruik de opdracht **show run-software-configuratie** om te bepalen het certificaat dat gebruikt wordt in de versnelde service, gebruik dan de **show crypto certificaten** en **show crypto certificaat-details** opdrachten om te bevestigen dat het certificaat een veilige winkel is. Indien het certificaat niet bestaat, moet u het certificaat opnieuw importeren.
- Het geaccelereerde servicecertificaat is verlopen. Gebruik de opdrachten **voor cryptografische certificaten** en **cryptografische** certificaten om de vervaldatum van het certificaat te controleren.
- Het versnelde servicecertificaat heeft een geldige datum die in de toekomst aanvangt. Gebruik de opdrachten **Encrypt** en **crypto**, **certificatie-details** tonen en controleer de geldigheidssectie van de opdrachtoutput. Zorg er ook voor dat de informatie over de WAE-kloktijd en de tijdzone nauwkeurig is.

U kunt verifiëren dat SSL-verbindingen het juiste beleid hebben toegepast, dat wil zeggen, zij hebben volledige optimalisatie met SSL versnelling, zoals in Afbeelding 2 wordt getoond. Kies in de Central Manager het WAE-apparaat en kies vervolgens **Monitor > Optimization > Connections Statistieken**.

Afbeelding 2. Controleer het juiste beleid voor SSL-verbindingen

Gebruik de opdracht **Show in werking stellen-fig** om te verifiëren dat het vervoersbeleid HTTPS correct wordt geconfigureerd. U wilt **DRE** op **een optimale manier** zien**, geen compressie** voor de SSL-toepassingsactie en u wilt de juiste matchvoorwaarden zien voor de HTTPS-classificator, als volgt:

```
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
```

Een actieve versnelde service voert dynamisch beleid in dat overeenkomt met de server-IP:poort, servernaam:poort of serverdomein:poort ingesteld in de versnelde service. Dit beleid kan worden geïnspecteerd met behulp van de **dynamische** opdracht **voor de** toepassing **van de showbeleidsmotor**. Het veld Dst in elk weergegeven beleid geeft de IP-server en poort aan die overeenkomen met de versnelde service. Voor het vervanging-domein (bijvoorbeeld server-domein *.webex.com poort 443) zal het Dst-veld 'Any:443' zijn. Voor de server-name-configuratie, wordt de DNS-raadpleging door-gestuurd wanneer de versnelde service wordt geactiveerd en alle IP-adressen die in de DNS-respons worden teruggegeven, worden in de beleidsmachine ingevoegd. Deze opdracht is handig om situaties te onderkennen waarin een versnelde service is gemarkeerd met "inservice", maar de versnelde service wordt inactief verklaard vanwege een andere fout. Bijvoorbeeld, alle versnelde diensten zijn afhankelijk van de peerservice en als de peerservice inactief is vanwege een ontbrekende/verwijderde certificaat, dan zal een versnelde service ook gemarkeerd worden als inactief alhoewel het "inservice" lijkt te zijn in de show-run-configuratieuitvoer. U kunt verifiëren dat het SSL dynamische beleid op het datacenter WAE actief is door de **show beleid-motor toepassing dynamisch** bevel te gebruiken. U kunt de peerservice-status controleren met behulp van de opdracht **host-service** van **showcrypto SSL-services**.

Een SSL AO-versnelde serviceconcentratie kan vier typen serveritems bevatten:

- Statische IP (server-ip) - beschikbaar in versie 4.1.3 en later
- Catch All (server-ip any) — beschikbaar in 4.1.7 en later

- Hostname (server-name) - beschikbaar in 4.2.1 en later
- Wildcard domein (server-domein) beschikbaar in 4.2.1 en later

Zodra de verbinding door SSL AO wordt ontvangen, beslist het welke versnelde service voor optimalisatie moet worden gebruikt. De statische IP configuratie krijgt de hoogste voorkeur, gevolgd door servernaam, serverdomein en dan de server ip elk. Als geen van de geconfigureerde en geactiveerd versnelde services overeenkomt met de server-IP voor de verbinding, wordt de verbinding naar de generieke AO geduwd. Het koekje dat door de SSL AO in de beleidsmotor wordt ingebracht wordt gebruikt om te bepalen welke versnelde dienst en welk type van serveringang voor een bepaalde verbinding wordt aangepast. Dit beleidsmachinekaart is een 32-bits getal en is alleen betekenisvol voor SSL AO. De hogere bits worden gebruikt om de verschillende typen servers in te sturen en de lagere bits geven de versnelde service index als volgt aan:

SSL Policy Engine Cookie-waarden

Koekwaarde	Type ingangssignaal voor servers	Opmerkingen
0x8*xxxxx*	IP-adres server	Statische IP-adresconfiguratie
0x4*xxxxx*	Hostnaam van de server	Data Center WAE voert een voorwaartse DNS raadpleging voor de hostname uit en het voegt de IP adressen toe die in de dynamische beleidsconfiguratie worden teruggegeven. Verfris elke 10 minuten standaard.
0x2FFF	Naam van serverdomein	Data Center WAE voert een omgekeerde DNS raadpleging op het IP-adres van de doelhost uit om te bepalen of deze met het domein overeenkomt. Als het met elkaar overeenkomt, wordt SSL-verkeer versneld en als het niet overeenkomt, wordt het verkeer verwerkt volgens het statische HTTPS-beleid.
0x1*xxxxx*	Alle servers	Alle SSL-verbindingen worden versneld met behulp van deze versnelde serviceconconfiguratie

Voorbeeld 1: Accelerated Service met server-ip configuratie:

```
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
```

De bijbehorende beleidsmotor wordt als volgt toegevoegd:

```
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                   <----------------
```

Voorbeeld 2: Accelerated Service met servernaamconfiguratie:

Deze configuratie maakt een eenvoudige implementatie mogelijk voor optimalisatie van de SSL-applicaties van ondernemingen. Het kan worden aangepast aan DNS-configuratiewijzigingen en vermindert IT-administratieve taken.

```
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
```

De bijbehorende beleidsmotor wordt als volgt toegevoegd:

```
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
```

Voorbeeld 3: Accelerated Service met server-domein configuratie:

Dankzij deze configuratie kunnen WAAS-apparaten één wildkaartdomein configureren, zodat het niet nodig is IP-adressen te kennen voor alle servers. Het datacenter WAE gebruikt omgekeerde DNS (rDNS) om verkeer dat tot het geconfigureerde domein behoort aan te passen. Door een jokerdomein te configureren voorkomt u het configureren van meerdere IP-adressen, wat de oplossing schaalbaar en toepasbaar maakt voor SaaS-architectuur.

```
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
```

De bijbehorende beleidsmotor wordt als volgt toegevoegd:

```
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
```

Voorbeeld 4: Accelerated Service met server-ip elke configuratie:

Deze configuratie biedt een catch-all mechanisme. Wanneer een versnelde service met **server-ip elke poort 443** actief wordt gemaakt, zorgt deze ervoor dat alle verbindingen op poort 443 geoptimaliseerd worden door SSL AO. Deze configuratie kan tijdens POC's worden gebruikt om al het verkeer op een bepaalde poort te optimaliseren.

```
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
```

De bijbehorende beleidsmotor wordt als volgt toegevoegd:

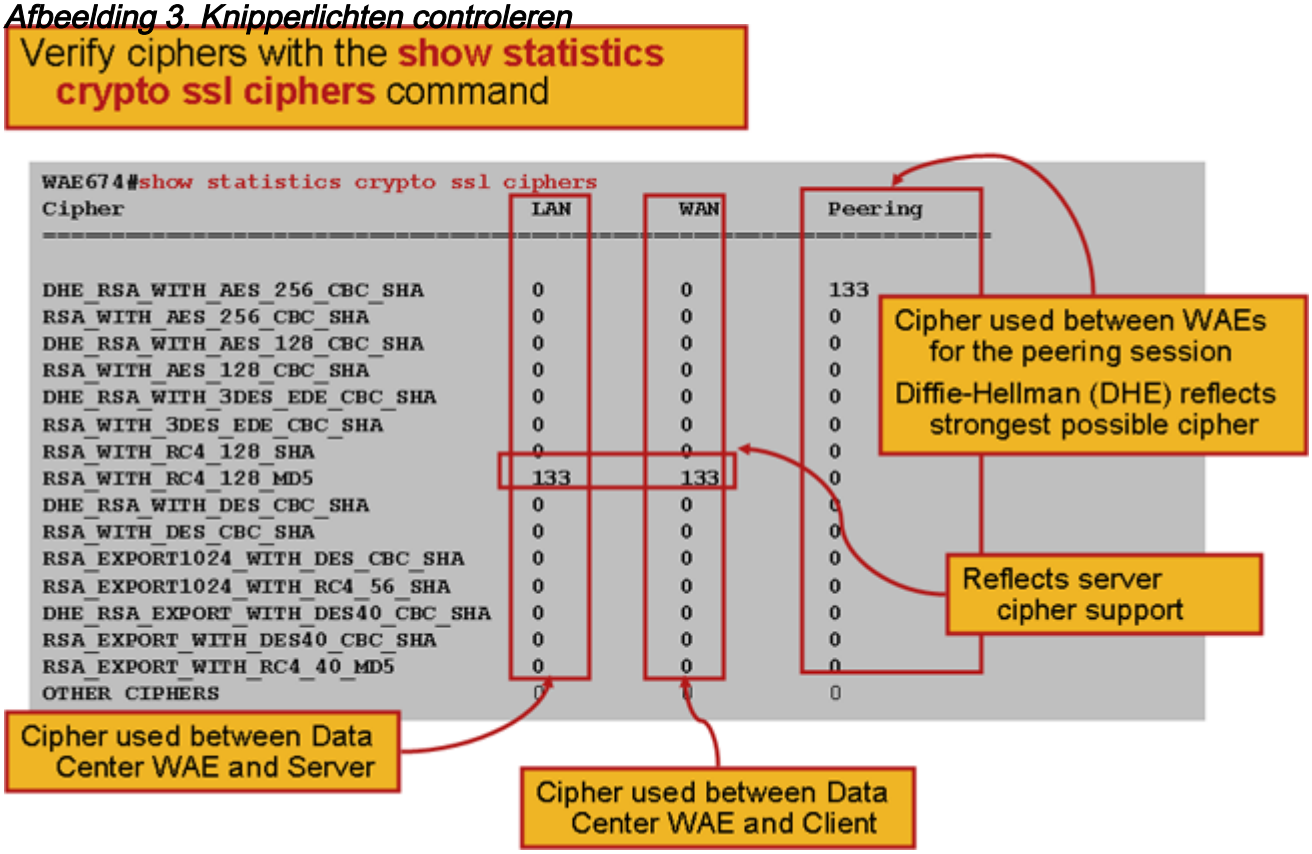
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

U kunt de ciphers die met de opdrachten **van** de **showstatistieken crypto SSL-ciphers** worden gebruikt, zoals in afbeelding 3 tonen.

Afbeelding 3. Knipperlichten controleren



U kunt controleren of deze ciphers overeenkomen met de cips die op de oorspronkelijke server zijn ingesteld. **Opmerking:** Knipperaars die DHE bevatten worden niet ondersteund door Microsoft IS-servers.

Op een Apache-server kunt u de SSL-versie en de algoritme in het httpd.conf-bestand controleren. Deze velden kunnen ook in een apart bestand (sslmod.conf) worden geplaatst dat afkomstig is van httpd.conf. Bekijk de velden van het SSLP-protocol en SLCipherSuite als volgt:

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

Om de uitgevende instelling van certificaten op een Apache-server te controleren, gebruikt u de opdracht openssl om het certificaat als volgt te lezen:

```
> 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
```

In de browser kunt u een certificaat en zijn details bekijken om de certificatieketen, versie, encryptie sleuteltype, uitgever gemeenschappelijke naam (CN) en onderwerp/site CN te bepalen. In Internet Explorer klikt u op het pictogram hangslot, klikt u op **Certificaat bekijken** en vervolgens kijkt u naar de tabbladen Details en certificeringspad voor deze informatie.

De meeste browsers schrijven voor dat de client certificaten in de PKCS12-indeling moeten zijn in plaats van de X509 PEM-indeling. Als u het X509 PEM-formaat wilt exporteren naar PKCS12-indeling, gebruikt u de opdracht openssl als volgt op een Apache-server:

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

Als de privé toetsen zijn versleuteld, moet het wachtwoord voor de export worden gebruikt. Het uitvoerwachtwoord wordt opnieuw gebruikt voor het importeren van aanmeldingsgegevens naar het WAAS-apparaat.

Gebruik de opdracht **show statistics accelerator sl** om de SSL AO statistieken te zien.

```
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              <-------
---------
. . .
```

Oplossingen en verificaties kunnen mislukt zijn en kunnen nuttig zijn voor het oplossen van problemen. Ze worden makkelijker opgeroepen door het volgende filter te gebruiken in de opdracht **Show statistics accelerator**:

```
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-gerelateerde statistieken kunnen nuttig zijn voor het configureren van servernaam en wilde domeinconfiguratie. Om deze statistieken terug te krijgen gebruikt de **show statistics versneller ssl** opdracht, als volgt:

```
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
 . . .
```

SSL rehandshake-gerelateerde statistieken kunnen nuttig zijn voor het oplossen van problemen en kunnen worden opgehaald met behulp van de volgende filter in de **show statistics accelerator ssl** opdracht:

```
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
```

Gebruik de **verbinding van showstatistieken geoptimaliseerde** opdracht van **ssl** om te controleren dat het WAAS apparaat geoptimaliseerde SSL verbindingen opstelt. Controleer dat "TDLS" in de kolom Accel voor een verbinding voorkomt. "S" geeft aan dat SSL AO als volgt is gebruikt:

```
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"
```

U kunt verbindingsstatistieken voor gesloten verbindingen controleren door de **verbinding van de showstatistieken te** gebruiken **gesloten SLV** opdracht.

Als de verbindingen niet worden geoptimaliseerd, controleer of WCCP/PBR correct is geconfigureerd en werkt en controleer op asymmetrische routing.

U kunt de SSL verbindingsstatistieken bekijken door de **van de showstatistiek verbinding geoptimaliseerde** opdracht **van het** detaildetail te gebruiken, waar u het dynamische beleid zult zien dat van de geconfigureerde SSL versnelde service voortvloeit. **Opmerking:** Het geconfigureerde beleid is uitsluitend TFO-optimalisatie, maar de volledige optimalisatie wordt toegepast als resultaat van de geconfigureerde SSL-service.

```
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
. . .
```

Later in deze uitvoer worden de uitgebreide SSL-sessieniveaus als volgt weergegeven:

```
. . .
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
```

Aansluitingen voor probleemoplossing HTTP AO op SSL AO Handoff

Als een client een proxy moet opgeven om een HTTPS server te bereiken, gaat het verzoek van de client eerst als een HTTP CONNECT-bericht naar de proxy (waarbij het IP-adres van de HTTPS-server is ingesloten in het CONNECT-bericht). Op dit punt behandelt de HTTP AO deze verbinding via peer WAE's. De proxy maakt een tunnel tussen de client- en serverpoort en geeft opeenvolgende gegevens tussen de client en dat server-IP-adres en -poort door. De proxy reageert terug naar de client met een bericht "200 OK" en maakt de verbinding met SSL AO af omdat de client voornemens is om met de server te praten via SSL. De client initieert vervolgens een SSL-handdruk met de SSL-server via de TCP-verbinding (tunnel) die door de proxy is ingesteld.

Controleer de volgende dingen bij het oplossen van problemen met uitgaande verbindingen:

- Controleer de output van de **show statistics accelerator http** opdracht om te bevestigen dat een verbinding door de HTTP AO werd verwerkt en vervolgens aan SSL AO werd overgedragen. Kijk naar de Total Handled Connections en Total Connections Handed-off naar SSL tellers. Bij problemen controleert u het volgende:
  - De HTTP AO is ingeschakeld en in de actieve toestand in de peer WAE's.
  - De SSL versnelde service wordt ingesteld met de poort die door de client wordt gebruikt in de CONNECT URL (of impliciete poort 443 als HTTPS wordt gebruikt). Vaak is de proxy poort anders dan de CONNECT URL poort en deze proxy poort dient niet te worden geconfigureerd in de SSL-versnelde service. De proxy-poort moet echter zijn opgenomen in de traffic classificatie die is gekoppeld aan de HTTP AO.
- Controleer de output van de **show statistics accelerator http** opdracht om te bevestigen dat deze verbinding werd verwerkt en geoptimaliseerd door SSL AO. Kijk naar de Total Handled Connections en Total Optimized Connections tellers. Als de statistische tellers niet correct zijn, voert u fundamentele SSL-probleemoplossing uit zoals in de vorige sectie wordt besproken.
- Op het datacenter WAE, verifieer dat de **show statistics verbinding geoptimaliseerde** detailopdracht uitvoer de hostname, IP adres en TCP poort toont van de eigenlijke SSL server. Als deze velden niet goed zijn ingesteld, controleert u het volgende:
  - Controleer dat de client browser proxy instellingen correct zijn.
  - Controleer dat de DNS-server op het WAE-datacenter is geconfigureerd en bereikbaar is. U kunt een DNS-server op WAE configureren met de opdracht **ip-**naamserver ***A.B.C.D***.

Verificatie van certificaat voor probleemoplossing

Voor de verificatie van het servercertificaat moet u het juiste CA-certificaat importeren naar de WAE van het datacenter.

U kunt de verificatie van het certificaat van probleemoplossing als volgt uitvoeren:

1. Controleer het servercertificaat en haal de naam van de emittent terug. Deze naam van de emittent in het servercertificaat moet overeenkomen met de naam van de onderwerp in het corresponderende CA-certificaat. Als u PEM gecodeerde certificaten hebt, kunt u de volgende **openssl** opdracht op een server gebruiken terwijl openssl is geïnstalleerd:

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

2. Verzeker dat de overeenkomende configuratie van de crypto-Pki op de WAE van het datacenter door **show in werking stellen-configuratie** opdracht te gebruiken. Voor een CA-certificaat dat door de WAE tijdens het verificatieproces moet worden gebruikt, is een crypto pki-configuratie vereist voor elk geïmporteerd CA-certificaat. Als bijvoorbeeld een CA-certificeringsbedrijf1.ca wordt geïmporteerd, moet de volgende configuratie worden uitgevoerd op de WAE van het datacenter:

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

Opmerking: Als een CA-certificaat wordt geïmporteerd met behulp van de Central Manager GUI, voegt de Central Manager automatisch de bovenstaande crypto pki-configuratie toe om het geïmporteerde CA-certificaat op te nemen. Als echter het CA-certificaat via de CLI wordt geïmporteerd, moet u de bovenstaande configuratie handmatig toevoegen.

3. Indien het te controleren certificaat een certificeringsketen bevat, moet de certificatenketen coherent zijn en moet het CA-certificaat van de hoogste emittent in de WAE worden ingevoerd. Gebruik de opdracht **openssl verify** om het certificaat eerst afzonderlijk te controleren.

4. Als de verificatie nog steeds mislukt, moet u het SSL-versneller onderzoeken om het logbestand te debug. Gebruik de volgende opdrachten om debug logging mogelijk te maken:

```
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. Start een testverbinding en controleer vervolgens het logbestand van /local/local1/errorlog/sslao-errorlog.current. In dit bestand moet de naam van de uitgevende instelling worden vermeld die in het servercertificaat is opgenomen. Zorg ervoor dat deze naam van de uitgevende instelling exact overeenkomt met de doelnaam van het CA-certificaat.

Als er andere interne fouten in de logbestanden staan, kan het handig zijn om de opties voor het debug van de bestanden extra toe te voegen.

6. Zelfs indien de naam van de uitgevende instelling en de naam van de doelgroep overeenkomen, is het CA-certificaat mogelijk niet de juiste. In dergelijke gevallen, als het servercertificaat door een bekende CA wordt verstrekt, kan een browser worden gebruikt om direct (zonder WAAS) de server te bereiken. Wanneer de browser de verbinding instelt, kan het certificaat worden onderzocht door te klikken op het pictogram Lock dat op de onderkant van het browser venster of in de adresbalk van de browser verschijnt. De certificeringsgegevens kunnen het juiste CA-certificaat aangeven dat bij dit servercertificaat hoort. Controleer het veld Serienummer in het CA-certificaat. Dit serienummer moet overeenkomen met het serienummer van het certificaat dat in het datacenter WAE wordt ingevoerd.

7. Als u OCSP-herroepingscontrole hebt ingeschakeld, schakelt u deze uit en controleert u op zichzelf de verificatie van het certificaat. Zie het gedeelte Problemen oplossen voor informatie over OCSP-instellingen voor probleemoplossing.

Clientverificatie voor probleemoplossing

Verificatie van het client-certificaat kan worden ingeschakeld op de oorspronkelijke server en/of op de WAE van het datacenter. Wanneer WAAS wordt gebruikt om SSL-verkeer te versnellen, is het client-certificaat dat wordt ontvangen door de oorspronkelijke server het certificaat dat is aangegeven in de machine-cert-key die is gespecificeerd in de opdracht **wereldwijd ingestelde** instellingen voor **crypto** services in het datacenter WAE of in het datacenter WAE machine met eigen handtekening, indien de machine-cert-toets niet is ingesteld. Als de verificatie van de client niet op de server van oorsprong kan gebeuren, kan dit het gevolg zijn van het feit dat het WAE machine-certificaat van het datacenter niet kan worden geverifieerd op de server van oorsprong.

Als de verificatie van de client van de WAE van het datacenter niet werkt, is dit waarschijnlijk omdat het CA-certificaat dat overeenkomt met het client-certificaat niet wordt geïmporteerd in de WAE van het datacenter. Zie het gedeelte "Problemen oplossen bij het controleren van het Server-certificaat" voor instructies hoe u controleert of het juiste CA-certificaat dat op WAE is geïmporteerd.

Verificatie van peer-WAE-certificaten voor probleemoplossing

Volg deze stappen om problemen met de verificatie van peer-certificaten op te lossen:

1. Controleer of het te controleren certificaat een door de CA ondertekend certificaat is. Een door een WAE zelf ondertekend certificaat kan niet door een andere WAE worden geverifieerd. WAE's worden standaard geladen met zelfondertekende certificaten. Een zelfgetekend certificaat moet worden ingesteld met de opdracht **crypto ssl services global-settings machine-cert-key**.

2. Controleer of het juiste CA-certificaat is geladen op het apparaat dat het certificaat controleert. Als peer-cert-verify bijvoorbeeld is geconfigureerd op de WAE van het datacenter, is het essentieel dat het WAE-certificaat van de aftakking CA-ondertekend is en dat het certificaat van dezelfde handtekening CA op de WAE van het datacenter wordt geïmporteerd. Vergeet niet een CA te creëren met de opdracht **crypto pki** om het geïmporteerde certificaat te gebruiken, indien u het certificaat handmatig via de CLI importeert. Indien geïmporteerd door de Central Manager GUI, creëert de Central Manager automatisch een corresponderende configuratie van crypto-pki.

3. Als de verificatie van de peer WAE nog steeds mislukt, controleert u de debug-logbestanden zoals beschreven in het gedeelte "SSL AO-vastlegging".

Controleer van OCSP-herroeping voor probleemoplossing

Als het systeem moeite heeft om succesvolle SSL-verbindingen te maken met de OCSP-herroeping (Online certificaatprotocol) en de OCSP-herroeping, volgt u deze stappen bij het oplossen van problemen:

1. Verzeker u ervan dat de OCSP responder-service op de responderserver wordt uitgevoerd.
2. Zorg voor goede connectiviteit tussen de WAE en de responder. Gebruik de opdrachten **ping** en **telnet** (naar de juiste poort) van de WAE om te controleren.
3. Bevestig dat het certificaat geldig is. De vervaldatum en de juiste URL zijn gebieden waar er problemen zijn.
4. Controleer dat het certificaat voor OCSP-responsen in de WAE is geïmporteerd. De antwoorden van een OCSP-responder worden ook ondertekend en het CA-certificaat dat de OCSP-responsen weergeeft, moet op de WAE staan.
5. Controleer de **show statistics accelerator sl** opdracht output om OCSP statistieken te

controleren en controleer de tellers overeenkomend met OCSP mislukkingen.

6. Als de OCSP HTTP verbinding door een HTTP proxy gaat, probeer dan de proxy uit te schakelen om te zien of deze helpt. Als het helpt, controleer dan of de proxy configuratie niet de connectie-storing veroorzaakt. Als de proxy-configuratie prima is, dan kan er een HTTP header-eigenheid zijn die iets oncompatibel met de proxy kan veroorzaken. Leg een pakketspoor vast voor verder onderzoek.
7. Als al het andere faalt, kunt u een pakketspoor van het uitgaande OCSP verzoek om verder het zuiveren moeten opnemen. U kunt de opdrachten **TCP-oplossing** of **thermische oplossing** gebruiken zoals beschreven in het gedeelte "Packets opnemen en analyseren" in het artikel Voorbereidende WAAS-probleemoplossing.

De URL die door het datacenter WAE wordt gebruikt om een OCSP-responder te bereiken, is op een van twee manieren afgeleid:

- De statische OCSP URL die door de configuratieopdracht van het **cryptografische pki** wordt geconfigureerd
- De OCSP URL die in het certificaat wordt gespecificeerd dat wordt gecontroleerd

Als de URL is afgeleid van het certificaat dat wordt gecontroleerd, is het essentieel om te verzekeren dat de URL bereikbaar is. Schakel de SSL-versneller OCSP-debug in om de URL te bepalen en vervolgens te controleren op connectiviteit in de responder. Zie de volgende sectie voor meer informatie over het gebruik van debug-logbestanden.

DNS-configuratie voor probleemoplossing

Als het systeem problemen heeft met het optimaliseren van SSL-verbindingen met servernaam en serverdomeinconfiguraties, volgt u deze stappen bij het oplossen van problemen:

1. Zorg ervoor dat de DNS-server op de WAE bereikbaar is en u de namen kunt oplossen. Gebruik de volgende opdracht om de geconfigureerde DNS-server te controleren:

```
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 !
```

Deze respons geeft aan dat de naam niet kan worden opgelost door de ingestelde naamservers.

Probeer pingelen/traceren voor de geconfigureerde naamservers om hun bereikbaarheid en de rondreistijd te controleren.

```
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. Als de DNS-server bereikbaar is en deze kan namen oplossen en de SSL-verbindingen worden niet geoptimaliseerd, zorg er dan voor dat de versnelde service bij het configureren van het gespecificeerde domein of de hostname actief is en dat er geen alarm zijn voor SSL AO. Gebruik de volgende opdrachten:

```
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
```

De aanwezigheid van het "accl_svc_inactive" alarm is een indicatie dat er enige discrepantie is in de versnelde serviceconfiguratie en dat er een of meer versnelde services zijn die overlappende configuratie hebben voor serveringangen. Controleer de configuratie van de versnelde service en controleer of de configuratie juist is. Gebruik de volgende opdracht om de configuratie te controleren:

```
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
```

U kunt als volgt informatie over een bepaalde versnelde service controleren:

```
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
```

Eén reden dat de operationele status van de versnelde service INACTIEF is, is een DNS-fout. Bijvoorbeeld, als er een server hostname in de versnelde dienstconfiguratie is en WAE het server-IP adres niet kan oplossen, dan kan de WAE niet het juiste dynamische beleid configureren.

3. Als de statistiek teller voor "Pipe-through" door een niet-matchende domeinnaam toeneemt, is dit een indicatie dat de SSL-verbinding voor een server is die voor optimalisatie is geconfigureerd.

Controleer de items voor de beleidsmotor met de volgende opdracht:

```
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
```

Controleer de verbindingsstatus met behulp van de opdracht **van de** verbinding **tonen statistieken**. De eerste verbinding zou een versneller van TSGDL en de daaropvolgende verbindingen moeten tonen, tot de levensduur van de TIME_DENY beleidsingang, zou TDL moeten zijn.

4. Als de DNS-server binnen WAN is met betrekking tot het datacenter WAE, of als de omgekeerde DNS-responstijd te lang is, kunnen sommige verbindingen worden verbroken. Dit hangt af van de client-timeout en de DNS-responstijd. In dit geval wordt de teller voor "Aantal omgekeerde DNS raadpleging geannuleerd" hoger en wordt de verbinding verbroken. Deze situatie geeft aan dat de DNS-server niet reageert of zeer langzaam en/of NSCD op WAAS niet werkt. De NSCD-status kan worden gecontroleerd met behulp van de opdracht **Taalalarmen**. De waarschijnlijkheid van dit gebeuren is zeer laag aangezien in de meeste implementaties de DNS-server naar verwachting op hetzelfde LAN zal staan als het datacenter WAE.

Problemen oplossen HTTP naar SSL AO-filtering

OPMERKING: HTTP naar SSL AO-routing is geïntroduceerd in WAAS versie 4.3.1. Deze sectie is niet van toepassing op eerdere WAAS-versies.

Ketsen stelt een AO in staat om op elk moment tijdens de levensduur van een stroom een andere AO in te voegen en beide AO's kunnen hun AO-specifieke optimalisatie onafhankelijk van de stroom toepassen. Een ketting is anders dan de AO handoff-functie die door WAAS is meegeleverd in pre-4.3.1 releases omdat AO-ketting van de eerste AO-functie de stroom blijft optimaliseren.

SSL AO verwerkt twee soorten verbindingen:

- Byte-0 SSL: SSL AO ontvangt eerst de verbinding en voltooit de SSL handdruk. Het ontleent het eerste deel van de lading om op een HTTP methode te controleren. Als de lading HTTP aangeeft, plaatst het de HTTP AO in; indien dit niet het geval is, past zij de reguliere TSDL-optimalisatie toe.
- Proxy-VERBINDING: HTTP AO ontvangt eerst de verbinding. Het identificeert de CONNECT header methode in het verzoek van de client en voegt SSL AO toe nadat de proxy bevestigt met een OK-bericht van 200.

SSL AO gebruikt een lichtgewicht HTTP-parser die de volgende HTTP-methoden detecteert: KRIJG, HOOFD, POST, PUT, OPTIES, TRACE, KOPIE, LOCK, POLL, BCOPY, BMOVE, MKCOL, VERWIJDEREN, ZOEKEN, ONLOCK, BDELETE, PROPFIND, PROPFIND, PROPPATCH, SUBSCRIBE, BPROPPATCH, UNSUBSCRIBE, EN X_ MS_ENMATUMATUMATUMATUMS TS. U kunt de opdracht **debug accelerator sl parser** gebruiken om problemen met betrekking tot de parser te debug. U kunt de **show** stat **ACL** lading **sl**

gebruiken **http/**andere opdracht om statistieken van verkeer te bekijken gerubriceerd op basis van het type lading.

Tips voor probleemoplossing:

1. Controleer of de HTTPS optie in de HTTP AO-configuratie is ingeschakeld omdat deze eigendom is van de HTTP AO. Zie het artikel Problemen oplossen in het HTTP artikel.
2. Controleer de verbindingsstaat met behulp van de opdracht **om** statverbinding **te tonen**. Indien correct geoptimaliseerd, zou het THSDL-indicatie voor TCP-, HTTP-, SSL- en DRE-LZ-optimalisatie moeten tonen. Als een van deze optimalisaties ontbreekt, debug verder op die optimizer (SSL, HTTP, enzovoort). Bijvoorbeeld, als de verbindingsstaat THDL toont, betekent het SSL optimalisatie werd niet toegepast op de verbinding. Details over problemen met debuggen gerelateerd aan SSL AO volgen.
3. Zorg ervoor dat SSL AO is ingeschakeld en in de actieve toestand is (zie het gedeelte "Problemen oplossen als SSL AO").
4. Zorg ervoor dat er geen alarmen zijn door de opdracht **tonen** te gebruiken.
5. Als het SSL-verkeer niet wordt geoptimaliseerd, zorg er dan voor dat het IP-adres van de server, de host-naam of het domeinnaam en het poortnummer als deel van de versnelde service wordt toegevoegd.
6. Controleer of de versnelde service in de actieve staat is met behulp van de opdracht ***ASVC-naam voor*** programmacryptografische **DSL-services** (zie het gedeelte "DNS-configuratie van probleemoplossing").
7. Zorg ervoor dat de beleidsmotor een ingang voor deze server en haven heeft door gebruik te maken van de **show beleid-motor applicatie dynamische** opdracht.
8. Als de doelserver SSL op een niet-standaardpoort gebruikt (de standaard is 443), zorg er dan voor dat dit in de configuratie van de beleidsmotor wordt weerspiegeld. De Central Manager is op deze informatie gebaseerd voor het rapporteren van SSL verkeersgegevens.
9. Zorg ervoor dat de geconfigureerde host-name oplost tot een geldig IP-adres door de **opdracht Show crypto SSL Services Accelerated-Service *ASVC-naam*** te gebruiken. Als er geen IP-adres is gevonden, controleert u of de naamserver correct is ingesteld. Controleer ook de uitvoer van de opdracht ***IP-adres bij het ontwerp***.

```
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-vastlegging

De volgende logbestanden zijn beschikbaar voor problemen met SSL AO:

- Bestanden van transactielogboek: /local1/logs/tfo/working.log (en/local1/logs/tfo/tfo_log_*.txt)
- Debug logbestanden: /local1/errorlog/sslao-errorlog.current (en sslao-errorlog.*)

Voor makkelijkere debugging moet u eerst een ACL instellen om pakketten te beperken tot één host.

```
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
```

Gebruik de configuratieopdracht **voor** transactielogingen als volgt:

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

U kunt het einde van een transactielogbestand als volgt weergeven door de opdracht **type-munt** te gebruiken:

```
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
```

Gebruik de volgende opdrachten om de vastlegging van het SSL AO-netwerk in te stellen en te activeren.

OPMERKING: Debug logging is CPU-intensief en kan een grote hoeveelheid output genereren. Gebruik het voorzichtig en spaarzaam in een productieomgeving.

U kunt als volgt gedetailleerd loggen op de schijf inschakelen:

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

U kunt debug logging voor verbindingen in ACL als volgt inschakelen:

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

De opties voor het zuiveren van SSL AO zijn als volgt:

```
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
```

U kunt debug van loggen voor SSL-verbindingen inschakelen en vervolgens het einde van het debug-logbestand als volgt weergeven:

```
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
```

Waarschuwingen voor probleemoplossing bij certificaataanvraag op NME en SRE-modules

Het SSL AO genereert alarmen wanneer het zelf-ondertekende machinecertificaat is verlopen (of binnen 30 dagen na afloop) en een aangepast mondiaal machinecertificaat is niet op het WAAS-apparaat ingesteld. De WAAS-software genereert fabriekscertificaten met een datumnotatie van 5 jaar vanaf de eerste start van het WAAS-apparaat.

De kloktijd in alle WAAS NME- en SRE-modules wordt ingesteld op 1 januari 2006 tijdens de eerste opstartfase, ook al is de NME- of SRE-module recent. Hierdoor verloopt het zelfgetekende certificaat op 1 januari 2011 en genereert het apparaat certificeringswaarschuwingen.

Als u het standaard fabriekscertificaat niet gebruikt als het wereldwijde certificaat en in plaats daarvan een aangepast certificaat gebruikt voor de SSL AO, dan ervaart u deze onverwachte beëindiging en kunt u het aangepaste certificaat bijwerken wanneer het verlopen is. Als u de NME of MKB-module met een nieuw softwarebeeld hebt bijgewerkt en de klok tot een recentere datum heeft gesynchroniseerd, kunt u dit probleem ook niet ervaren.

Het symptoom van certificaatverloopdatums is een van de volgende alarmen (weergegeven hier in de uitvoer van de opdracht **alarmen** tonen):

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

of

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

De Central Manager GUI meldt het volgende alarm: "certificaat__waas-self_.p12 is bijna verloopd en wordt in mondiale instellingen als machinecoördinaat geconfigureerd"

U kunt een van de volgende oplossingen gebruiken om dit probleem op te lossen:

- Configureer een ander certificaat voor mondiale instellingen:

```
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
```

- Update het zelf ondertekende fabriekscertificaat met een latere verloopdatum. Deze oplossing vereist een script dat u kunt verkrijgen door contact op te nemen met Cisco TAC.

OPMERKING: Deze kwestie wordt geregeld door de resolutie van voorbehouden CSCte05426, vrijgegeven in de WAAS-softwareversies 4.1.7b, 4.2.3c en 4.3.3. De certificeringsvervaldatum wordt gewijzigd in 2037.