WAAS - Dépannage de l'AO SSL

Chapitre : Dépannage de l'AO SSL

Cet article décrit comment dépanner l'AO SSL.

Contenu

Présentation de SSL Accelerator

L'accélérateur SSL (disponible en version 4.1.3 et ultérieure) optimise le trafic SSL (Secure Sockets Layer) chiffré et TLS (Transport Layer Security). L'accélérateur SSL assure le chiffrement et le déchiffrement du trafic au sein du WAAS pour permettre l'optimisation du trafic de bout en

bout. L'accélérateur SSL assure également la gestion sécurisée des clés et des certificats de cryptage.

Dans un réseau WAAS, le WAE du centre de données agit en tant que noeud intermédiaire de confiance pour les requêtes SSL du client. La clé privée et le certificat de serveur sont stockés sur le périphérique WAE du data center. Le périphérique WAE du data center participe à la connexion SSL pour dériver la clé de session, qu'il distribue en bande sécurisée au périphérique WAE de la succursale, ce qui permet au périphérique WAE de déchiffrer le trafic client, de l'optimiser, de le rechiffrer et de l'envoyer via le WAN au périphérique WAE du data center. Le périphérique WAE du data center gère une session SSL distincte avec le serveur d'origine.

Les services suivants sont pertinents pour l'optimisation SSL/TLS :

- Service accéléré : entité de configuration qui décrit les caractéristiques d'accélération à appliquer à un serveur SSL ou à un ensemble de serveurs. Spécifie le certificat et la clé privée à utiliser lors de la pose en tant qu'intermédiaire approuvé, les chiffrement à utiliser, la version SSL autorisée et les paramètres de vérification du certificat.
- Service d'appairage : entité de configuration qui décrit les caractéristiques d'accélération à appliquer pour les connexions SSL intrabande entre les WAE des filiales et des centres de données. Ce service est utilisé pour transférer les informations de clé de session du data center aux WAE de la succursale afin d'optimiser les connexions SSL.
- Service d'administration du gestionnaire central - Non utilisé directement par l'accélérateur SSL, mais à utiliser par un administrateur pour la gestion de la configuration des services accélérés SSL. Également utilisé pour télécharger des certificats et des clés privées à utiliser dans les services accélérés SSL.
- Service de gestion du gestionnaire central - Non utilisé directement par l'accélérateur SSL, mais utilisé pour la communication entre les périphériques d'accélérateur d'applications et le gestionnaire central. Ce service est utilisé pour la gestion de la configuration, la récupération sécurisée des clés de chiffrement du magasin et les mises à jour d'état des périphériques.

Le magasin sécurisé Central Manager est essentiel au fonctionnement de l'AO SSL car il stocke des clés de chiffrement sécurisées pour tous les WAE. Après chaque rechargement de Central Manager, l'administrateur doit rouvrir le magasin sécurisé en fournissant la phrase de passe avec la commande **cms secure-store open**. Un périphérique WAE récupère automatiquement sa clé de cryptage de magasin sécurisé à partir du Gestionnaire central chaque fois que le périphérique WAE redémarre. Aucune action n'est donc requise sur le périphérique WAE après un rechargement.

Si les clients utilisent une solution proxy HTTP, la connexion initiale est gérée par l'AO HTTP, qui la reconnaît comme une demande de tunnel SSL vers le port 443. L'AO HTTP recherche un service SSL accéléré correspondant défini sur le WAE du centre de données et, lorsqu'il trouve une correspondance, désactive la connexion à l'AO SSL. Cependant, le trafic que l'AO HTTP transmet à l'AO SSL pour un proxy HTTPS est signalé dans les statistiques de l'application Web, et non dans l'application SSL. Si l'AO HTTP ne trouve pas de correspondance, la connexion est optimisée conformément à la configuration de stratégie HTTPS (SSL) statique.

L'AO SSL peut utiliser des certificats auto-signés plutôt que des certificats signés CA, ce qui peut être utile pour déployer des systèmes de validation de principe (POC) et résoudre les problèmes SSL. En utilisant des certificats auto-signés, vous pouvez déployer rapidement un système WAAS sans avoir à importer les certificats du serveur d'origine, et vous pouvez éliminer les certificats comme source potentielle de problèmes. Vous pouvez configurer un certificat auto-signé dans le Gestionnaire central lors de la création d'un service SSL accéléré. Cependant, lorsque vous

utilisez un certificat auto-signé, le navigateur client affiche une alerte de sécurité indiquant que le certificat n'est pas fiable (car il n'est pas signé par une autorité de certification connue). Pour éviter cet avertissement de sécurité, installez le certificat dans le magasin Autorités de certification racines de confiance du navigateur client. (Dans Internet Explorer, dans l'avertissement de sécurité, cliquez sur **Afficher le certificat**, puis dans la boîte de dialogue Certificat, cliquez sur **Installer le certificat** et terminez l'Assistant Importation de certificat.)

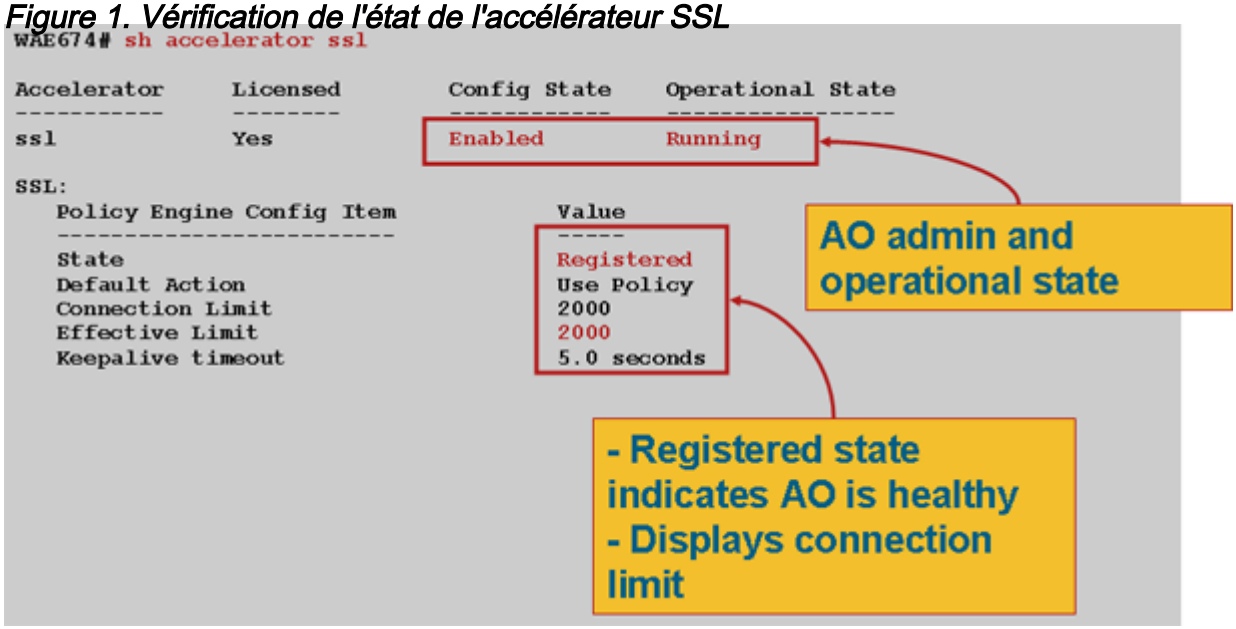
La configuration des services de gestion SSL est facultative et vous permet de modifier la version et la liste de chiffrement SSL utilisées pour les communications de Central Manager vers les WAE et le navigateur (pour l'accès administratif). Si vous configurez des chiffrement qui ne sont pas pris en charge par votre navigateur, vous perdrez la connexion au Gestionnaire central. Dans ce cas, utilisez la commande de configuration **crypto ssl management-service** de l'interface de ligne de commande pour rétablir les paramètres du service de gestion SSL par défaut.

Dépannage de l'AO SSL

Vous pouvez vérifier la configuration et l'état général de l'AO à l'aide des commandes **show accélérator** et **show license**, comme décrit dans l'article Dépannage de l'accélération des applications. La licence Enterprise est requise pour le fonctionnement de l'accélérateur SSL.

Ensuite, vérifiez l'état qui est spécifique à l'AO SSL sur les WAE du centre de données et de la succursale à l'aide de la commande **show accélérator ssl**, comme illustré à la Figure 1. Vous voulez voir que l'AO SSL est activée, en cours d'exécution et enregistrée et que la limite de connexion est affichée. Si l'état de configuration est Activé mais que l'état opérationnel est Arrêté, cela indique un problème de licence. Si l'état opérationnel est désactivé, c'est peut-être parce que le périphérique WAE ne peut pas récupérer les clés SSL du magasin sécurisé Central Manager, soit parce que le magasin sécurisé n'est pas ouvert, soit parce que le gestionnaire central est inaccessible. Utilisez les commandes **show cms info** et **ping** pour confirmer que le Gestionnaire central est accessible.

Figure 1. Vérification de l'état de l'accélérateur SSL



Si vous voyez un état opérationnel de Param Crypto Gen, attendez que l'état devienne En cours d'exécution, ce qui peut prendre quelques minutes après un redémarrage. Si vous voyez un état de récupération des clés de CM pendant plus de quelques minutes, cela peut indiquer que le service CMS sur le Gestionnaire central n'est pas en cours d'exécution, qu'il n'y a pas de connectivité réseau au Gestionnaire central, que les versions WAAS sur le WAE et le Gestionnaire central sont incompatibles ou que le magasin sécurisé du Gestionnaire central n'est

pas ouvert.

Vous pouvez vérifier que le magasin sécurisé du Gestionnaire central est initialisé et ouvert à l'aide de la commande **show cms secure-store** comme suit :

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

Si le magasin sécurisé n'est pas initialisé ou ouvert, des alarmes critiques telles que mstore_key_fail et secure-store s'affichent. Vous pouvez ouvrir le magasin sécurisé à l'aide de la commande **cms secure-store open** ou à partir du Gestionnaire central, choisissez **Admin > Secure Store**.

Astuce : Documentez le mot de passe du magasin sécurisé pour éviter d'avoir à réinitialiser le magasin sécurisé si vous oubliez le mot de passe.

En cas de problème de chiffrement de disque sur un périphérique WAE, cela peut également empêcher l'AO SSL de fonctionner. Utilisez la commande **show disk details** pour vérifier que le chiffrement de disque est activé et vérifier si les partitions CONTENT et SPOOL sont montées. Si ces partitions sont montées, cela indique que les clés de chiffrement de disque ont été récupérées avec succès à partir du Gestionnaire central et que les données chiffrées peuvent être écrites et lues à partir des disques. Si la commande **show disk details** affiche « Le système est en cours d'initialisation », qui indique que les clés de chiffrement n'ont pas encore été récupérées à partir du Gestionnaire central et que les disques n'ont pas encore été montés. Le périphérique WAE ne fournit pas de services d'accélération dans cet état. Si le périphérique WAE ne parvient pas à récupérer les clés de chiffrement de disque à partir du Gestionnaire central, il déclenche une alarme.

Vous pouvez vérifier que le service SSL accéléré est configuré et que son état est Activé sur le WAE du centre de données (dans le Gestionnaire central, choisissez le périphérique, puis choisissez **Configurer > Accélération > Services SSL accélérés**). Un service accéléré configuré et activé peut être rendu inactif par l'accélérateur SSL en raison des conditions suivantes :

- Le certificat configuré dans le service accéléré a été supprimé du WAE. Utilisez la commande **show running-config** pour déterminer le certificat utilisé dans le service accéléré, puis utilisez les commandes **show crypto certificate** et **show crypto certificate-details** pour confirmer que le certificat est présent dans le magasin sécurisé. Si le certificat est manquant, réimportez le certificat.
- Le certificat de service accéléré a expiré. Utilisez les commandes **show crypto certificate** et **show crypto certificate-details** pour vérifier la date d'expiration du certificat.
- Le certificat de service accéléré a une date valide commençant à l'avenir. Utilisez les commandes **show crypto certificate** et **show crypto certificate-details** et vérifiez la section de validité du résultat de la commande. Assurez-vous également que l'horloge WAE et les informations de fuseau horaire sont exactes.

Vous pouvez vérifier que les connexions SSL ont la politique correcte appliquée, c'est-à-dire qu'elles ont une optimisation complète avec l'accélération SSL, comme illustré à la Figure 2. Dans Central Manager, sélectionnez le périphérique WAE, puis sélectionnez **Monitor > Optimization > Connections Statistics**.

Figure 2. Vérification de la stratégie correcte sur les connexions SSL

Utilisez la commande **show running-config** pour vérifier que la stratégie de trafic HTTPS est correctement configurée. Vous voulez voir **optimiser DRE no compression none** pour l'action d'application SSL et vous voulez voir les conditions de correspondance appropriées listées pour le classifieur HTTPS, comme suit :

```
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
```

Un service accéléré actif insère des stratégies dynamiques correspondant au serveur IP:port, nom de serveur:port ou domaine de serveur:port configuré dans le service accéléré. Ces stratégies peuvent être inspectées à l'aide de la commande **show policy-engine application dynamic**. Le champ Dst de chaque stratégie affichée indique l'adresse IP et le port du serveur correspondant au service accéléré. Pour le domaine générique (par exemple, le domaine du serveur *.webex.com port 443), le champ Dst sera 'Any:443'. Pour la configuration du nom de serveur, la recherche DNS directe est effectuée lorsque le service accéléré est activé et que toutes les adresses IP retournées dans la réponse DNS sont insérées dans le moteur de stratégie. Cette commande est utile pour détecter les situations où un service accéléré est marqué « en service » mais où le service accéléré est rendu inactif en raison d'une autre erreur. Par exemple, tous les services accélérés dépendent du service d'appairage et si le service d'appairage est inactif en raison d'un certificat manquant/supprimé, alors un service accéléré sera également marqué comme inactif bien qu'il semble être en service dans la sortie show running-config. Vous pouvez vérifier que la stratégie dynamique SSL est active sur le périphérique WAE du centre de données à l'aide de la commande **show policy-engine application dynamic**. Vous pouvez vérifier l'état du service d'appairage à l'aide de la commande **show crypto ssl services host-service appairage**.

Une configuration de service SSL AO accélérée peut avoir quatre types d'entrées de serveur :

- Static IP (server-ip) : disponible dans les versions 4.1.3 et ultérieures
- Catch All (server-ip any) : disponible dans 4.1.7 et versions ultérieures

- Nom d'hôte (nom de serveur) : disponible dans la version 4.2.1 et ultérieure
- Domaine générique (domaine de serveur) : disponible dans la version 4.2.1 et ultérieure

Une fois la connexion reçue par l'AO SSL, il décide quel service accéléré doit être utilisé pour l'optimisation. La configuration IP statique reçoit la préférence la plus élevée, suivie du nom du serveur, du domaine du serveur, puis du serveur ip any. Si aucun des services accélérés configurés et activés ne correspond à l'adresse IP du serveur pour la connexion, la connexion est repoussée vers l'AO générique. Le cookie inséré dans le moteur de stratégie par l'AO SSL est utilisé pour déterminer quel service accéléré et quel type d'entrée de serveur correspond pour une connexion particulière. Ce cookie de moteur de stratégie est un nombre 32 bits et n'a de sens que pour l'AO SSL. Les bits les plus élevés sont utilisés pour indiquer différents types d'entrée de serveur et les bits les plus bas indiquent l'index de service accéléré, comme suit :

Valeurs des cookies du moteur de stratégie SSL

Valeur des cookies	Type d'entrée de serveur	Commentaires
0x8*xxxxxxx*	Adresse IP du serveur	Configuration des adresses IP statiques
0x4 *xxxxxxx*	Nom d'hôte du serveur	Le périphérique WAE du centre de données effectue une recherche DNS directe pour le nom d'hôte et ajoute les adresses IP qui sont retournées dans la configuration de stratégie dynamique. Actualisé toutes les 10 minutes par défaut.
0x2FFFFFF	Nom de domaine du serveur	Le périphérique WAE du centre de données effectue une recherche DNS inverse sur l'adresse IP de l'hôte de destination pour déterminer si elle correspond au domaine. S'il correspond, le trafic SSL est accéléré, et s'il ne correspond pas, le trafic est traité conformément à la politique HTTPS statique.
0x1 *xxxxxxx*	Serveur Any	Toutes les connexions SSL sont accélérées à l'aide de cette configuration de service accélérée

Exemple 1 : Service accéléré avec configuration IP serveur :

```
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
```

L'entrée correspondante du moteur de stratégie est ajoutée comme suit :

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

Exemple 2 : Service accéléré avec configuration du nom de serveur :

Cette configuration facilite le déploiement pour l'optimisation des applications SSL d'entreprise. Il est adaptable aux modifications de configuration DNS et réduit les tâches administratives informatiques.

```
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
```

L'entrée correspondante du moteur de stratégie est ajoutée comme suit :

```
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
```

Exemple 3 : Service accéléré avec configuration du domaine de serveur :

Cette configuration permet aux périphériques WAAS de configurer un seul domaine générique qui évite de connaître les adresses IP de tous les serveurs. Le WAE du data center utilise le DNS inverse (rDNS) pour correspondre au trafic appartenant au domaine configuré. La configuration d'un domaine générique évite de configurer plusieurs adresses IP, ce qui rend la solution évolutive et applicable à l'architecture SaaS.

```
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
```

L'entrée correspondante du moteur de stratégie est ajoutée comme suit :

```
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
```

Exemple 4 : Accélération du service avec la commande server-ip any Configuration :

Cette configuration fournit un mécanisme de capture-all. Lorsqu'un service accéléré avec **server-ip any port 443** est rendu actif, il permet d'optimiser toutes les connexions sur le port 443 par l'AO SSL. Cette configuration peut être utilisée pendant les POC pour optimiser tout le trafic sur un port particulier.

```
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
```

L'entrée correspondante du moteur de stratégie est ajoutée comme suit :

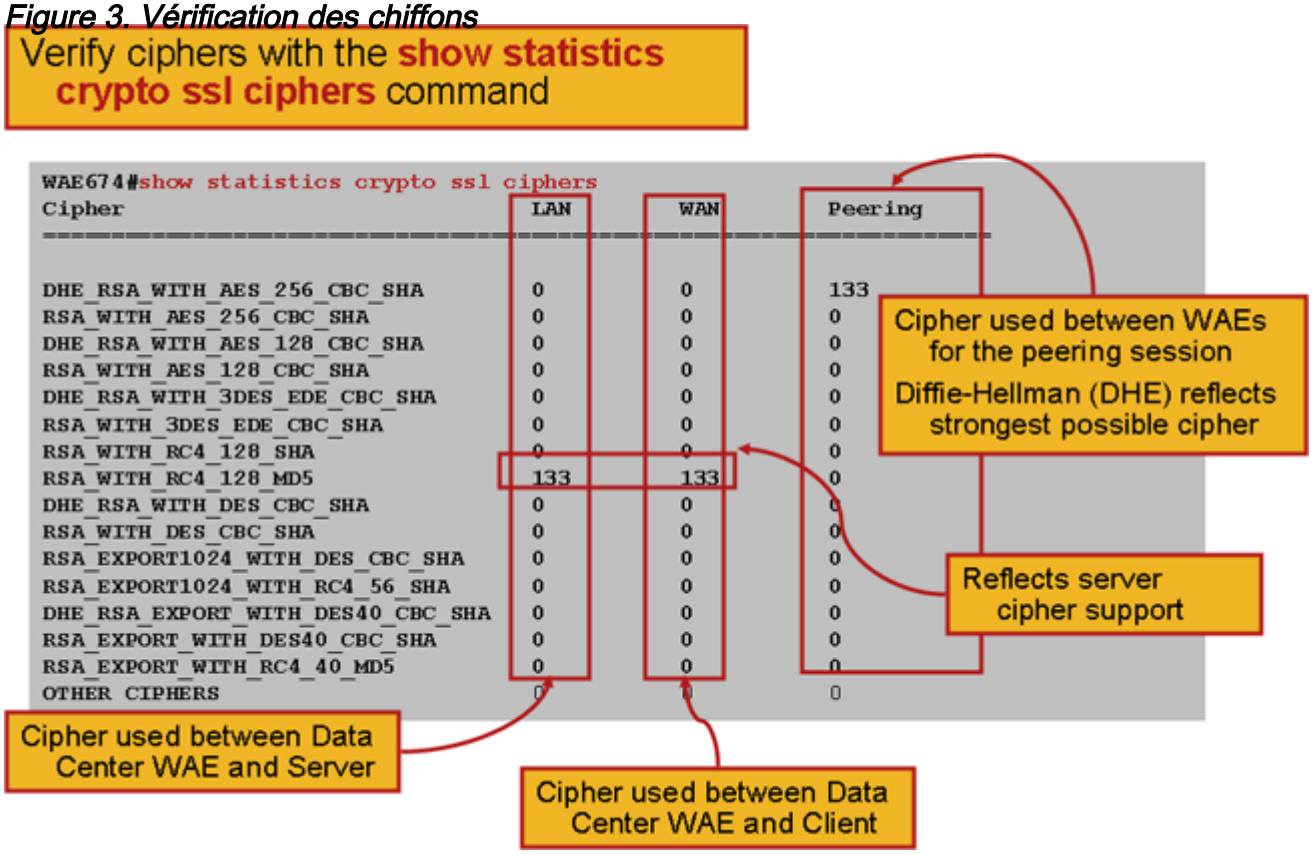
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

Vous pouvez vérifier les chiffrement utilisés avec les commandes **show statistics crypto ssl ciphers** , comme illustré à la Figure 3.

Figure 3. Vérification des chiffons



Vous pouvez vérifier que ces chiffrement correspondent à ceux configurés sur le serveur d'origine.
Note: Les chiffrement incluant DHE ne sont pas pris en charge par les serveurs Microsoft IIS.

Sur un serveur Apache, vous pouvez vérifier la version SSL et chiffrer les détails dans le fichier httpd.conf. Ces champs peuvent également se trouver dans un fichier distinct (sslmod.conf) référencé à partir de httpd.conf. Recherchez les champs SSLProtocol et SSLCipherSuite comme suit :

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

Pour vérifier l'émetteur du certificat sur un serveur Apache, utilisez la commande openssl pour lire le certificat comme suit :

```
> 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
```

Dans le navigateur, vous pouvez afficher un certificat et ses détails afin de déterminer la chaîne de certificat, la version, le type de clé de chiffrement, le nom commun de l'émetteur (CN) et le code de sujet/site. Dans Internet Explorer, cliquez sur l'icône de cadenas, sur **Afficher le certificat**, puis sur les onglets Détails et Chemin de certification pour obtenir ces informations.

La plupart des navigateurs exigent que les certificats clients soient au format PKCS12 plutôt qu'au format PEM X509. Pour exporter le format PEM X509 au format PKCS12, utilisez la commande openssl comme suit sur un serveur Apache :

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

Si les clés privées sont chiffrées, la phrase de passe est requise pour l'exportation. Le mot de passe d'exportation est de nouveau utilisé pour importer des informations d'identification sur le périphérique WAAS.

Utilisez la commande **show statistics Accelator ssl** pour afficher les statistiques AO SSL.

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

Les statistiques des sessions et des vérifications de certificat ayant échoué peuvent être utiles pour le dépannage et sont plus facilement récupérées à l'aide du filtre suivant de la commande **show statistics Accelator ssl** :

```
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
```

Les statistiques liées au DNS peuvent être utiles pour le dépannage du nom de serveur et de la configuration de domaine générique. Pour extraire ces statistiques, utilisez la commande **show statistics Accelator ssl**, comme suit :

```
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
 . . .
```

Les statistiques relatives au rétablissement SSL peuvent être utiles pour le dépannage et peuvent être récupérées à l'aide du filtre suivant de la commande **show statistics Accelator ssl** :

```
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
```

Utilisez la commande **show statistics connection optimiszed ssl** pour vérifier que le périphérique WAAS établit des connexions SSL optimisées. Vérifiez que « TDLS » apparaît dans la colonne Accel pour une connexion. « S » indique que l'AO SSL a été utilisé comme suit :

```
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"
```

Vous pouvez vérifier les statistiques de connexion pour les connexions fermées à l'aide de la commande **show statistics connection fermé ssl**.

Si les connexions ne sont pas optimisées, vérifiez si WCCP/PBR est correctement configuré et fonctionne, et vérifiez le routage asymétrique.

Vous pouvez afficher les statistiques de connexion SSL à l'aide de la commande **show statistics connection optized ssl detail**, où vous verrez la stratégie dynamique qui résulte du service SSL accéléré configuré. **Note**: La stratégie configurée est l'optimisation TFO uniquement, mais l'optimisation complète est appliquée à la suite du service SSL configuré.

```
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
. . .
```

Plus loin dans ce résultat, les détails du niveau de session SSL étendue sont présentés comme suit :

```
. . .
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
```

Dépannage des connexions HTTP AO à SSL AO

Si un client doit passer par un proxy pour atteindre un serveur HTTPS, la requête du client passe d'abord en tant que message HTTP CONNECT au proxy (avec l'adresse IP du serveur HTTPS réelle intégrée dans le message CONNECT). À ce stade, l'AO HTTP gère cette connexion sur les WAE homologues. Le proxy crée un tunnel entre le port client et le port serveur et relaie les données suivantes entre le client et l'adresse IP et le port du serveur. Le proxy répond au client avec un message “ 200 OK ” et désactive la connexion à l'AO SSL parce que le client a l'intention de parler au serveur via SSL. Le client lance ensuite une connexion SSL avec le serveur SSL via la connexion TCP (tunnel) configurée par le proxy.

Vérifiez les éléments suivants lors du dépannage des problèmes de connexion en mode déconnexion :

- Vérifiez le résultat de la commande **show statistics Accelator http** pour confirmer qu'une connexion a été gérée par l'AO HTTP, puis transmise à l'AO SSL. Examinez le nombre total de connexions traitées et le nombre total de connexions traitées aux compteurs SSL. En cas de problème, vérifiez les points suivants :
  - L'AO HTTP est activé et en état d'exécution sur les WAE homologues.
  - Le service SSL accéléré est configuré avec le port utilisé par le client dans l'URL CONNECT (ou le port implicite 443 si HTTPS est utilisé). Souvent, le port proxy est différent du port d'URL CONNECT et ce port proxy ne doit pas être configuré dans le service d'accélération SSL. Cependant, le port proxy doit être inclus dans le classificateur de trafic mappé à l'AO HTTP.
- Vérifiez le résultat de la commande **show statistics Accelator http** pour confirmer que cette connexion a été gérée et optimisée par l'AO SSL. Examinez les compteurs Total des connexions traitées et Total des connexions optimisées. Si les compteurs de statistiques ne sont pas corrects, effectuez un dépannage SSL de base, comme indiqué dans la section précédente.
- Sur le périphérique WAE du centre de données, vérifiez que la sortie de la commande **show statistics connection** indique le nom d'hôte, l'adresse IP et le port TCP du serveur SSL réel. Si ces champs ne sont pas définis correctement, vérifiez les éléments suivants :
  - Vérifiez que les paramètres du proxy du navigateur client sont corrects.
  - Vérifiez que le serveur DNS est configuré sur le périphérique WAE du data center et qu'il est accessible. Vous pouvez configurer un serveur DNS sur le WAE à l'aide de la commande **ip name-server** *A.B.C.D*.

Dépannage de la vérification des certificats de serveur

La vérification du certificat du serveur nécessite que vous importiez le certificat d'autorité de certification correct dans le WAE du centre de données.

Pour dépanner la vérification des certificats de serveur, procédez comme suit :

1. Inspectez le certificat du serveur et récupérez le nom de l'émetteur. Ce nom d'émetteur dans le certificat de serveur doit correspondre au nom de sujet dans le certificat d'autorité de certification correspondant. Si vous avez des certificats codés PEM, vous pouvez utiliser la commande

openssl suivante sur un serveur sur lequel openssl est installé :

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

2. Assurez-vous que la configuration crypto pki ca correspondante existe sur le périphérique WAE du centre de données à l'aide de la commande **show running-config**. Pour qu'un certificat d'autorité de certification soit utilisé par le WAE dans le processus de vérification, un élément de configuration de crypto pki ca est requis pour chaque certificat d'autorité de certification importé. Par exemple, si un certificat CA company1.ca est importé, la configuration suivante doit être effectuée sur le périphérique WAE du centre de données :

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

Note: Si un certificat d'autorité de certification est importé à l'aide de l'interface utilisateur graphique du Gestionnaire central, le Gestionnaire central ajoute automatiquement la configuration de la clé de certification crypto pki ci-dessus pour inclure le certificat d'autorité de certification importé. Cependant, si le certificat d'autorité de certification est importé via l'interface de ligne de commande, vous devez ajouter manuellement la configuration ci-dessus.

3. Si le certificat en cours de vérification comprend une chaîne de certificats, assurez-vous que la chaîne de certificats est cohérente et que le certificat CA de l'émetteur le plus important est importé sur le périphérique WAE. Utilisez la commande **openssl verify** pour vérifier le certificat séparément en premier.

4. Si la vérification échoue toujours, examinez le journal de débogage de l'accélérateur SSL. Utilisez les commandes suivantes pour activer la journalisation de débogage :

```
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. Lancez une connexion de test, puis examinez le fichier journal /local/local1/errorlog/sslao-errorlog.current. Ce fichier doit indiquer le nom de l'émetteur qui a été inclus dans le certificat du serveur. Assurez-vous que ce nom d'émetteur correspond exactement au nom d'objet du certificat CA.

S'il y a d'autres erreurs internes dans les journaux, il peut être utile d'activer des options de débogage supplémentaires.

6. Même si le nom de l'émetteur et le nom du sujet correspondent, le certificat de l'autorité de certification peut ne pas être le bon. Dans de tels cas, si le certificat du serveur est émis par une autorité de certification connue, alors un navigateur peut être utilisé pour accéder directement (sans WAAS) au serveur. Lorsque le navigateur configure la connexion, le certificat peut être examiné en cliquant sur l'icône Verrouiller qui apparaît en bas à droite de la fenêtre du navigateur ou dans la barre d'adresse du navigateur. Les détails du certificat peuvent indiquer le certificat d'autorité de certification approprié correspondant à ce certificat de serveur. Vérifiez le champ Numéro de série dans le certificat de l'autorité de certification. Ce numéro de série doit

correspondre au numéro de série du certificat importé sur le périphérique WAE du centre de données.

7. Si la vérification de révocation OCSP est activée, désactivez-la et vérifiez que la vérification du certificat fonctionne. Pour obtenir de l'aide sur le dépannage des paramètres OCSP, reportez-vous à la section « Dépannage du contrôle de révocation OCSP ».

Dépannage de la vérification du certificat client

La vérification du certificat client peut être activée sur le serveur d'origine et/ou sur le périphérique WAE du centre de données. Lorsque WAAS est utilisé pour accélérer le trafic SSL, le certificat client reçu par le serveur d'origine est le certificat indiqué dans la clé de certificat de l'ordinateur spécifiée dans la commande **crypto ssl services global-settings** sur le WAE du centre de données ou le certificat auto-signé de l'ordinateur WAE du centre de données, si la clé de certificat de l'ordinateur n'est pas configurée. Par conséquent, si la vérification du certificat client échoue sur le serveur d'origine, c'est peut-être parce que le certificat de l'ordinateur WAE du centre de données n'est pas vérifiable sur le serveur d'origine.

Si la vérification du certificat client sur le WAE du data center ne fonctionne pas, c'est probablement parce que le certificat CA correspondant au certificat client n'est pas importé sur le WAE du data center. Reportez-vous à la section « Dépannage de la vérification des certificats de serveur » pour savoir comment vérifier si le certificat d'autorité de certification correct est importé sur le WAE.

Dépannage de la vérification du certificat WAE homologue

Pour résoudre les problèmes de vérification de certificat homologue, procédez comme suit :

1. Vérifiez que le certificat en cours de vérification est un certificat signé par l'autorité de certification. Un certificat auto-signé par un périphérique WAE n'est pas vérifiable par un autre périphérique WAE. Par défaut, les WAE sont chargés avec des certificats auto-signés. Un certificat auto-signé doit être configuré à l'aide de la commande **crypto ssl services global-settings machine-cert-key**.

2. Vérifiez que le certificat CA correct est chargé sur le périphérique qui vérifie le certificat. Par exemple, si peer-cert-verify est configuré sur le WAE du centre de données, il est essentiel que le certificat WAE de la filiale soit signé par l'autorité de certification et que le même certificat de l'autorité de certification de signature soit importé sur le WAE du centre de données. N'oubliez pas de créer une autorité de certification à l'aide de la commande **crypto pki ca** pour utiliser le certificat importé, si vous importez le certificat manuellement via l'interface de ligne de commande. Une fois importé par l'interface utilisateur graphique de Central Manager, Central Manager crée automatiquement une configuration de crypto pki ca correspondante.

3. Si la vérification du WAE homologue échoue toujours, vérifiez les journaux de débogage comme décrit dans la section « Journalisation AO SSL ».

Dépannage du contrôle de révocation OCSP

Si le système ne parvient pas à établir des connexions SSL avec la vérification de révocation du protocole OCSP (Online Certificate Status Protocol) activée, procédez comme suit :

1. Assurez-vous que le service de répondeur OCSP est en cours d'exécution sur le serveur de réponse.

2. Assurez une bonne connectivité entre le périphérique WAE et le répondeur. Utilisez les commandes **ping** et **telnet** (vers le port approprié) du WAE pour vérifier.
3. Confirmez que le certificat en cours de validation est effectivement valide. La date d'expiration et l'URL correcte du répondeur sont généralement des zones où il y a des problèmes.
4. Vérifiez que le certificat des réponses OCSP est importé sur le WAE. Les réponses d'un répondeur OCSP sont également signées et le certificat CA correspondant aux réponses OCSP doit résider sur le WAE.
5. Vérifiez la sortie de la commande **show statistics Accelator ssl** pour vérifier les statistiques OCSP et vérifiez les compteurs correspondant aux échecs OCSP.
6. Si la connexion HTTP OCSP passe par un proxy HTTP, essayez de désactiver le proxy pour voir s'il aide. Si cela vous aide, vérifiez que la configuration du proxy n'entraîne pas l'échec de la connexion. Si la configuration du proxy est correcte, il peut y avoir une particularité d'en-tête HTTP qui peut provoquer une certaine incompatibilité avec le proxy. Capturez une trace de paquet pour plus d'informations.
7. Si tout le reste échoue, vous devrez peut-être capturer une trace de paquet de la requête OCSP sortante pour un débogage ultérieur. Vous pouvez utiliser les commandes **tcpdump** ou **téthérée** comme décrit dans la section « Capture et analyse de paquets » dans l'article de dépannage WAAS préliminaire.

L'URL utilisée par le périphérique WAE du data center pour atteindre un répondeur OCSP est dérivée de deux façons :

- URL OCSP statique configurée par la commande de configuration **crypto pki global-settings**
- URL OCSP spécifiée dans le certificat en cours de vérification

Si l'URL provient du certificat en cours de vérification, il est essentiel de s'assurer que l'URL est accessible. Activez les journaux de débogage OCSP de l'accélérateur SSL pour déterminer l'URL, puis vérifiez la connectivité au répondeur. Reportez-vous à la section suivante pour plus d'informations sur l'utilisation des journaux de débogage.

Dépannage de la configuration DNS

Si le système rencontre des problèmes lors de l'optimisation des connexions SSL avec le nom de serveur et les configurations de domaine de serveur, procédez comme suit :

1. Assurez-vous que le serveur DNS configuré sur le WAE est accessible et peut résoudre les noms. Utilisez la commande suivante pour vérifier le serveur DNS configuré :

```
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 !
```

Cette réponse indique que le nom ne peut pas être résolu par les serveurs de noms configurés.

Essayez ping/traceoute pour les serveurs de noms configurés afin de vérifier leur accessibilité et le temps de parcours aller-retour.

```
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. Si le serveur DNS est accessible et qu'il peut résoudre les noms et que les connexions SSL ne sont toujours pas optimisées, assurez-vous que le service accéléré configurant le domaine ou le nom d'hôte spécifié est actif et qu'il n'y a aucune alarme pour l'AO SSL. Utilisez les commandes suivantes :

```
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
```

La présence de l'alarme « accl_svc_inactive » indique qu'il y a une anomalie dans la configuration accélérée du service et qu'il peut y avoir un ou plusieurs services accélérés ayant une configuration qui se chevauche pour les entrées du serveur. Vérifiez la configuration accélérée du service et assurez-vous que la configuration est correcte. Utilisez la commande suivante pour vérifier la configuration :

```
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
```

Pour vérifier les détails d'un service accéléré particulier, utilisez la commande suivante :

```
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
```

L'une des raisons pour lesquelles l'état opérationnel du service accéléré peut être INACTIVE est une défaillance DNS. Par exemple, s'il existe un nom d'hôte de serveur dans la configuration accélérée du service et que le WAE ne peut pas résoudre l'adresse IP du serveur, il ne peut pas configurer la stratégie dynamique appropriée.

3. Si le compteur de statistiques pour “ Pipe-through en raison d'” de noms de domaine non correspondants augmente, cela indique que la connexion SSL est pour un serveur configuré pour l'optimisation. Vérifiez les entrées du moteur de stratégie à l'aide de la commande suivante :

```
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
```

Vérifiez l'état de la connexion à l'aide de la commande **show statistics connection**. La première connexion doit afficher un accélérateur de TSGDL et les connexions suivantes, jusqu'à la durée de vie de l'entrée de stratégie TIME_DENY, doivent être TDL.

4. Si le serveur DNS se trouve sur le WAN en ce qui concerne le WAE du centre de données ou si le temps de réponse DNS inverse est trop long, certaines connexions peuvent être supprimées. Cela dépend du délai d’attente du client et du temps de réponse rDNS. Dans ce cas, le compteur pour “ Nombre de recherches DNS inversées annulées ” augmente et la connexion est abandonnée. Cette situation indique que le serveur DNS ne répond pas ou est très lent et/ou que NSCD sur WAAS ne fonctionne pas. L'état du NSCD peut être vérifié à l'aide de la commande **show alarms**. La probabilité que cela se produise est très faible car dans la plupart des déploiements, le serveur DNS devrait se trouver sur le même réseau local que le périphérique WAE du data center.

Dépannage du chaînage AO HTTP à SSL

NOTE: Le chaînage HTTP vers SSL AO a été introduit dans WAAS version 4.3.1. Cette section ne s'applique pas aux versions WAAS antérieures.

Le chaînage permet à un AO d'insérer un autre AO à tout moment pendant la durée de vie d'un flux et les deux AO peuvent appliquer leur optimisation propre à l'AO indépendamment sur le flux. Le chaînage AO est différent de la fonction de transfert AO fournie par WAAS dans les versions antérieures à la version 4.3.1, car avec le chaînage AO, le premier AO continue d'optimiser le flux.

L'AO SSL gère deux types de connexions :

- Byte-0 SSL : L'AO SSL reçoit d'abord la connexion et termine la connexion SSL. Il analyse la partie initiale de la charge utile pour rechercher une méthode HTTP. Si la charge utile indique HTTP, elle insère l'AO HTTP ; sinon, il applique l'optimisation TSDL standard.
- CONNEXION proxy : L'AO HTTP reçoit d'abord la connexion. Il identifie la méthode d'en-tête

CONNECT dans la requête du client et insère l'AO SSL après confirmation par le proxy avec un message 200 OK.

L'AO SSL utilise un analyseur HTTP léger qui détecte les méthodes HTTP suivantes : GET, HEAD, POST, PUT, OPTIONS, TRACE, COPY, LOCK, POLL, BCOPY, BMOVE, MKCOL, DELETE, SEARCH, UNLOCK, BDELETE, PROPFIND, BPROPPATCH, SUBSCRIBE, BPROPPATCH, UNSUBSCRIBE ET X__EN_MS MAJUSCULES. Vous pouvez utiliser la commande **debug accélérator ssl parser** pour déboguer les problèmes liés à l'analyseur. Vous pouvez utiliser la commande **show stat accel ssl payload http/other** pour afficher les statistiques du trafic classifié en fonction du type de charge utile.

Conseils de dépannage :

1. Assurez-vous que la fonctionnalité HTTPS est activée dans la configuration AO HTTP, car elle appartient à l'AO HTTP. Pour plus de détails, consultez l'article Dépannage de l'AO HTTP.
2. Vérifiez l'état de la connexion à l'aide de la commande **show stat connection**. S'il est correctement optimisé, il doit afficher THSDL indiquant l'optimisation TCP, HTTP, SSL et DRE-LZ. Si l'une de ces optimisations est manquante, déboguez plus loin sur cet optimiseur (SSL, HTTP, etc.). Par exemple, si l'état de la connexion indique THDL, cela signifie que l'optimisation SSL n'a pas été appliquée à la connexion. Vous trouverez ci-dessous des détails sur les problèmes de débogage liés à l'AO SSL.
3. Assurez-vous que l'AO SSL est activé et qu'il est en état d'exécution (voir la section « Dépannage de l'AO SSL »).
4. Assurez-vous qu'il n'y a pas d'alarmes à l'aide de la commande **show alarms**.
5. Si le trafic SSL n'est pas optimisé, assurez-vous que l'adresse IP, le nom d'hôte ou le nom de domaine et le numéro de port du serveur sont ajoutés dans le cadre du service accéléré.
6. Assurez-vous que le service accéléré est à l'état ACTIVE à l'aide de la commande **show crypto ssl services accélération-service *ASVC-name*** (voir la section « Dépannage de la configuration DNS »).
7. Assurez-vous que le moteur de stratégie a une entrée pour ce serveur et ce port à l'aide de la commande **show policy-engine application dynamic**.
8. Si le serveur de destination utilise SSL sur un port non par défaut (la valeur par défaut est 443), assurez-vous que cela est reflété dans la configuration du moteur de stratégie. Le Gestionnaire central s'appuie sur ces informations pour signaler les données de trafic SSL.
9. Assurez-vous que le nom d'hôte configuré est résolu en adresse IP valide à l'aide de la commande **show crypto ssl services accélération-service *ASVC-name***. Si aucune adresse IP n'est trouvée, vérifiez si le serveur de noms est configuré correctement. Vérifiez également le résultat de la commande **dnslookup *IP-address***.

```
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
```

Journalisation AO SSL

Les fichiers journaux suivants sont disponibles pour le dépannage des problèmes d'AO SSL :

- Fichiers journaux des transactions : /local1/logs/tfo/working.log (et /local1/logs/tfo/tfo_log_*.txt)
- Fichiers journaux de débogage : /local1/errorlog/sslao-errorlog.current (et sslao-errorlog.*)

Pour faciliter le débogage, vous devez d'abord configurer une liste de contrôle d'accès pour limiter les paquets à un hôte.

```
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
```

Pour activer la journalisation des transactions, utilisez la commande de configuration **transaction-logs** comme suit :

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

Vous pouvez afficher la fin d'un fichier journal de transactions à l'aide de la commande **type-tail** comme suit :

```
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
```

Pour configurer et activer la journalisation de débogage de l'AO SSL, utilisez les commandes suivantes.

NOTE: La journalisation de débogage est gourmande en CPU et peut générer une grande quantité de sortie. Utilisez-le judicieusement et avec parcimonie dans un environnement de production.

Vous pouvez activer la journalisation détaillée sur le disque comme suit :

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

Vous pouvez activer la journalisation de débogage pour les connexions dans la liste de contrôle d'accès comme suit :

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

Les options de débogage AO SSL sont les suivantes :

```
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
```

Vous pouvez activer la journalisation de débogage pour les connexions SSL, puis afficher la fin du journal des erreurs de débogage comme suit :

```
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
```

Dépannage des alarmes d'expiration de certificat sur les modules NME et SRE

L'AO SSL génère des alarmes lorsque le certificat d'ordinateur auto-signé a expiré (ou est dans les 30 jours de l'expiration) et qu'un certificat d'ordinateur global personnalisé n'est pas configuré sur le périphérique WAAS. Le logiciel WAAS génère des certificats autosignés en usine avec une date d'expiration de 5 ans à compter du premier démarrage du périphérique WAAS.

L'horloge de tous les modules WAAS NME et SRE est définie au 1er janvier 2006 lors du premier démarrage, même si le module NME ou SRE est plus récent. Cela entraîne l'expiration du certificat auto-signé le 1er janvier 2011 et le périphérique génère des alarmes d'expiration du certificat.

Si vous n'utilisez pas le certificat d'usine par défaut comme certificat global et que vous utilisez plutôt un certificat personnalisé pour l'AO SSL, vous ne connaîtrez pas cette expiration inattendue et vous pouvez mettre à jour le certificat personnalisé chaque fois qu'il expire. En outre, si vous avez mis à jour le module NME ou SME avec une nouvelle image logicielle et que vous avez synchronisé l'horloge à une date plus récente, vous risquez de ne pas rencontrer ce problème.

Le symptôme de l'expiration du certificat est l'une des alarmes suivantes (illustrée ici dans la sortie de la commande **show alarms**) :

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

ou

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

L'interface utilisateur graphique de Central Manager signale l'alarme suivante : « Certificate__waas-self__.p12 est proche de l'expiration, il est configuré comme certificat de machine dans les paramètres globaux »

Vous pouvez utiliser l'une des solutions suivantes pour résoudre ce problème :

- Configurez un certificat différent pour les paramètres globaux :

```
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
```

- Mettez à jour le certificat d'usine auto-signé avec une date d'expiration ultérieure. Cette solution nécessite un script que vous pouvez obtenir en contactant le TAC Cisco.

NOTE: Ce problème est résolu par la résolution de la mise en garde CSCte05426, publiée dans les versions 4.1.7b, 4.2.3c et 4.3.3 du logiciel WAAS. La date d'expiration de la certification est remplacée par 2037.