WAAS - Resolución de problemas de SSL AO

Capítulo: Resolución de problemas de SSL AO

Este artículo describe cómo resolver problemas de SSL AO.

Contenido

Descripción General de SSL Accelerator

El acelerador SSL (disponible en 4.1.3 y versiones posteriores) optimiza el tráfico cifrado de capa de conexión segura (SSL) y seguridad de la capa de transporte (TLS). El acelerador SSL proporciona cifrado y descifrado del tráfico dentro de WAAS para habilitar la optimización del tráfico de extremo a extremo. El acelerador SSL también proporciona administración segura de los certificados y claves de cifrado.

En una red WAAS, el Data Center WAE actúa como nodo intermediario de confianza para las solicitudes SSL del cliente. La clave privada y el certificado del servidor se almacenan en el WAE del Data Center. El WAE del Data Center participa en el intercambio de señales SSL para derivar la clave de sesión, que se distribuye de forma segura en banda a la WAE de la sucursal, lo que permite a la WAE de la sucursal descifrar el tráfico del cliente, optimizarlo, volver a cifrarlo y enviarlo a través de la WAN al WAE del Data Center. El Data Center WAE mantiene una sesión SSL independiente con el servidor de origen.

Los siguientes servicios son relevantes para la optimización de SSL/TLS:

- Servicio acelerado: entidad de configuración que describe las características de aceleración que se aplicarán a un servidor SSL o a un conjunto de servidores. Especifica el certificado y la clave privada que se utilizarán mientras se presentan como intermediarios de confianza, los códigos que se utilizarán, la versión SSL permitida y la configuración de verificación de certificados.
- Servicio de iguales: entidad de configuración que describe las características de aceleración que se aplicarán a las conexiones SSL dentro de banda entre WAE de la sucursal y del Data Center. Este servicio se utiliza para transferir información de clave de sesión de Data Center a WAE de sucursales para optimizar las conexiones SSL.
- Central Manager Admin Service: no se utiliza directamente por el acelerador SSL, sino que lo utiliza un administrador para la administración de la configuración de los servicios acelerados SSL. También se utiliza para cargar certificados y claves privadas que se utilizarán en servicios acelerados SSL.
- Central Manager Management Service: no se utiliza directamente por el acelerador SSL, sino que se utiliza para la comunicación entre los dispositivos del acelerador de aplicaciones y el Central Manager. Este servicio se utiliza para la administración de la configuración, la recuperación de claves de cifrado de almacenamiento seguro y las actualizaciones de estado del dispositivo.

El almacén seguro de Central Manager es esencial para que SSL AO funcione, ya que almacena claves de cifrado seguras para todos los WAE. Después de cada recarga de Central Manager, el administrador necesita reabrir el almacén seguro proporcionando la frase de paso con el comando **cms secure-store open**. Un WAE recupera automáticamente su clave de cifrado de almacenamiento seguro del Central Manager cada vez que se reinicia el WAE, por lo que no se requiere ninguna acción en el WAE después de una recarga.

Si los clientes utilizan una solución de proxy HTTP, la conexión inicial es manejada por el AO HTTP, que lo reconoce como una solicitud de túnel SSL al puerto 443. El HTTP AO busca un servicio SSL acelerado que coincida definido en el WAE del Data Center y cuando encuentra una coincidencia, deja la conexión con el SSL AO. Sin embargo, el tráfico que el HTTP AO entrega a SSL AO para un proxy HTTPS se informa como parte de las estadísticas de la aplicación web, no en la aplicación SSL. Si el HTTP AO no encuentra una coincidencia, la conexión se optimiza según la configuración de política estática HTTPS (SSL).

El SSL AO puede utilizar certificados autofirmados en lugar de certificados firmados por CA, lo que puede ser útil para implementar sistemas de prueba de concepto (POC) y para solucionar

problemas de SSL. Mediante el uso de certificados autofirmados, puede implementar rápidamente un sistema WAAS sin tener que importar los certificados del servidor de origen, y puede eliminar los certificados como fuente potencial de problemas. Puede configurar un certificado autofirmado en el Administrador central al crear un servicio SSL acelerado. Sin embargo, cuando utilice un certificado autofirmado, el explorador del cliente mostrará una alerta de seguridad de que el certificado no es de confianza (porque no está firmado por una CA conocida). Para evitar esta advertencia de seguridad, instale el certificado en el almacén de Autoridades de certificación raíz de confianza en el navegador cliente. (En Internet Explorer, en la advertencia de seguridad, haga clic en **Ver certificado** y, a continuación, en el cuadro de diálogo Certificado, haga clic en **Instalar certificado** y complete el Asistente para importación de certificados.)

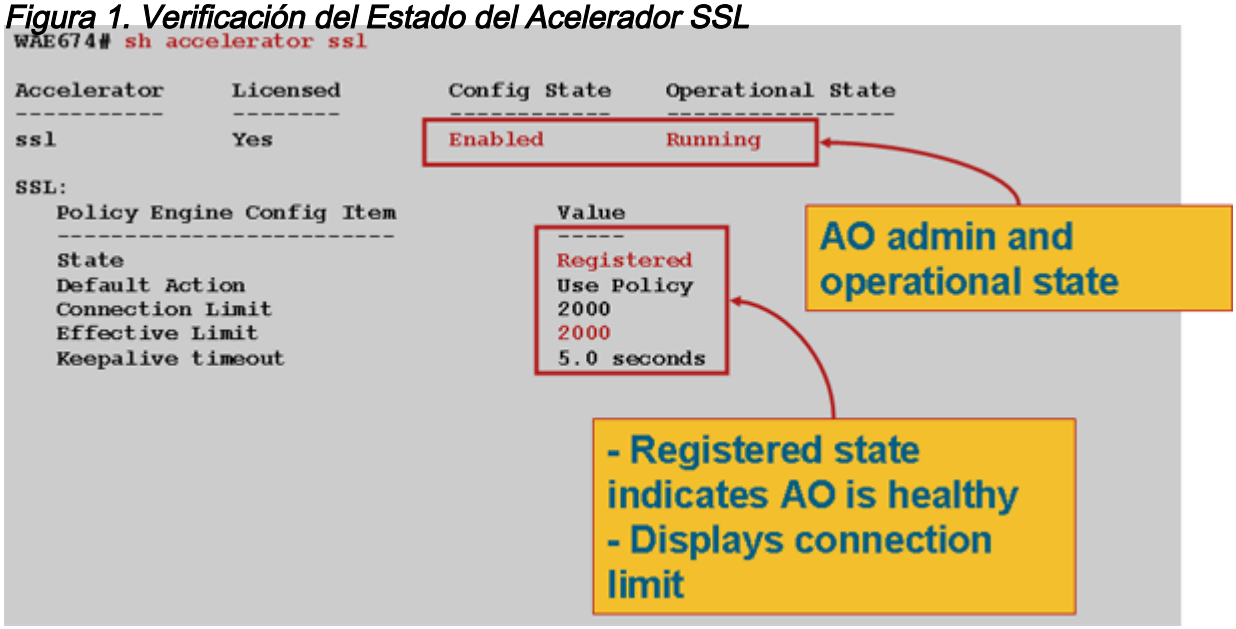
La configuración de los Servicios de administración SSL es opcional y le permite cambiar la versión SSL y la lista de cifrado utilizada para las comunicaciones de Central Manager a WAE y al navegador (para el acceso administrativo). Si configura los cifrados que no son compatibles con el explorador, perderá la conexión con el Administrador central. En este caso, utilice el comando de configuración **crypto ssl management-service** de la CLI para establecer la configuración del servicio de administración SSL nuevamente en el valor predeterminado.

Resolución de problemas de SSL AO

Puede verificar la configuración general de AO y el estado con los comandos **show Accelerator** y **show license**, como se describe en el artículo Troubleshooting Application Acceleration. La licencia Enterprise es necesaria para el funcionamiento del acelerador SSL.

A continuación, verifique el estado específico de SSL AO tanto en el Data Center como en los WAEs de la sucursal mediante el comando **show Accelerator ssl**, como se muestra en la Figura 1. Desea ver que SSL AO está habilitado, en ejecución y registrado, y que se muestra el límite de conexión. Si el estado de configuración está habilitado pero el estado operativo es apagado, indica un problema de licencia. Si el estado operativo está desactivado, puede deberse a que WAE no puede recuperar las claves SSL del almacén seguro de Central Manager, ya sea porque el almacén seguro no está abierto o porque no se puede acceder al Administrador central. Utilice los comandos **show cms info** y **ping** para confirmar que el Administrador Central es accesible.

Figura 1. Verificación del Estado del Acelerador SSL



Si ve un estado operativo de Gen Crypto Params, espere hasta que el estado se convierta en Running, que puede tardar unos minutos después de un reinicio. Si observa un estado de recuperación de claves desde CM durante más de unos minutos, podría indicar que el servicio

CMS en el Administrador central no se está ejecutando, que no hay conectividad de red con el Administrador central, que las versiones WAAS en el WAE y el Administrador central son incompatibles o que el almacén seguro de Central Manager no está abierto.

Puede verificar que el almacén seguro de Central Manager se inicializa y abre mediante el comando **show cms secure-store** de la siguiente manera:

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

Si el almacén seguro no se ha inicializado ni abierto, verá alarmas críticas como mstore_key_failure y secure-store. Puede abrir el almacén seguro con el comando **cms secure-store open** o desde Central Manager, elija **Admin > Secure Store**.

Consejo: Documentar la contraseña de almacenamiento seguro para evitar tener que restablecer el almacén seguro si olvida la contraseña.

Si hay un problema con el cifrado del disco en un WAE, esto también puede impedir que el SSL AO funcione. Utilice el comando **show disk details** para verificar que el cifrado del disco esté habilitado y verificar si las particiones CONTENT y SPOOL están montadas. Si se montan estas particiones, indica que las claves de cifrado del disco se recuperaron correctamente del Administrador central y que los datos cifrados se pueden escribir y leer de los discos. Si el comando **show disk details** muestra "El sistema se está inicializando", esto indica que las claves de cifrado todavía no se han recuperado del Central Manager y los discos aún no se han montado. WAE no proporcionará servicios de aceleración en este estado. Si el WAE no puede recuperar las claves de cifrado del disco del Central Manager, se producirá una alarma.

Puede verificar que el servicio acelerado SSL esté configurado y que su estado sea "Habilitado" en el Data Center WAE (en el Administrador central, elija el dispositivo y luego elija **Configurar > Aceleración > Servicios acelerados SSL**). Un servicio acelerado configurado y habilitado puede ser dejado inactivo por el acelerador SSL debido a las siguientes condiciones:

- El certificado configurado en el servicio acelerado se ha eliminado del WAE. Utilice el comando **show running-config** para determinar el certificado que se está utilizando en el servicio acelerado, luego utilice los comandos **show crypto certificates** y **show crypto certificate-details** para confirmar que el certificado está presente en el almacén seguro. Si falta el certificado, vuelva a importarlo.
- El certificado de servicio acelerado ha caducado. Utilice los comandos **show crypto certificates** y **show crypto certificate-details** para verificar la fecha de vencimiento del certificado.
- El certificado de servicio acelerado tiene una fecha válida que comienza en el futuro. Utilice los comandos **show crypto certificates** y **show crypto certificate-details** y verifique la sección de validez del resultado del comando. Además, asegúrese de que la información del reloj y de la zona horaria de WAE sea exacta.

Puede verificar que las conexiones SSL tengan la política correcta aplicada, es decir, que tengan una optimización completa con aceleración SSL, como se muestra en la figura 2. En Central Manager, elija el dispositivo WAE y luego elija **Monitor > Optimization > Connections Statistics**.

Figura 2 Verificación de la Política Correcta en Conexiones SSL

Utilice el comando **show running-config** para verificar que la política de tráfico HTTPS está configurada correctamente. Desea ver **optimizar DRE sin compresión ninguno** para la acción de aplicación SSL y desea ver las condiciones de coincidencia adecuadas enumeradas para el clasificador HTTPS, como se muestra a continuación:

```
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 servicio acelerado activo inserta políticas dinámicas correspondientes a la IP:puerto del servidor, nombre del servidor:puerto o dominio del servidor:puerto configurado dentro del servicio acelerado. Estas políticas se pueden inspeccionar mediante el comando **show policy-engine application dynamic**. El campo Dst de cada política mostrada indica la IP del servidor y el puerto que coinciden con el servicio acelerado. Para el dominio comodín (por ejemplo, dominio de servidor *.webex.com puerto 443), el campo Dst será 'Any:443'. Para la configuración de nombre de servidor, la búsqueda de DNS de reenvío se realiza cuando se activa el servicio acelerado y todas las direcciones IP devueltas en la respuesta de DNS se insertarán en el motor de políticas. Este comando es útil para detectar situaciones donde un servicio acelerado se marca "inservice" pero el servicio acelerado se representa inactivo debido a algún otro error. Por ejemplo, todos los servicios acelerados dependen del servicio de iguales y, si el servicio de iguales está inactivo debido a un certificado que falta o se elimina, un servicio acelerado también se marcará como inactivo aunque parezca estar "inservible" en el resultado de show running-config. Puede verificar que la política dinámica SSL esté activa en el WAE del Data Center mediante el comando **show policy-engine application dynamic**. Puede verificar el estado del servicio de peering usando el comando **show crypto ssl services host-service peering**.

Una configuración de servicio acelerada de SSL AO puede tener cuatro tipos de entradas de servidor:

- IP estática (server-ip): disponible en la versión 4.1.3 y posteriores

- Catch All (server-ip any) (disponible en 4.1.7 y versiones posteriores)
- Nombre de host (nombre de servidor): disponible en 4.2.1 y versiones posteriores
- Dominio comodín (dominio-servidor): disponible en 4.2.1 y versiones posteriores

Una vez recibida la conexión por el SSL AO, decide qué servicio acelerado debe utilizarse para la optimización. A la configuración IP estática se le da la preferencia más alta, seguida por el nombre del servidor, el dominio del servidor y luego el servidor ip any. Si ninguno de los servicios acelerados configurados y activados coincide con la IP del servidor para la conexión, la conexión se envía al AO genérico. La cookie insertada en el motor de políticas por el SSL AO se utiliza para determinar qué servicio acelerado y qué tipo de entrada de servidor coincide con una conexión determinada. Esta cookie del motor de políticas es un número de 32 bits y sólo tiene sentido para SSL AO. Los bits más altos se utilizan para indicar diferentes tipos de entrada de servidor y los bits más bajos indican el índice de servicio acelerado, como se muestra a continuación:

Valores de Cookie del Motor de Políticas SSL

Valor de cookies	Tipo de entrada del servidor	Comentarios
0x8 *xxxxxxx*	Dirección IP del servidor	Configuración de dirección IP estática
0x4 *xxxxxxx*	Nombre de host del servidor	Data Center WAE realiza una búsqueda de DNS de reenvío para el nombre de host y agrega las direcciones IP que se devuelven a la configuración de política dinámica. Actualizado cada 10 minutos de forma predeterminada.
0x2FFFFFFF	Nombre de dominio del servidor	El centro de datos WAE realiza una búsqueda de DNS inversa en la dirección IP del host de destino para determinar si coincide con el dominio. Si coincide, el tráfico SSL se acelera y, si no coincide, el tráfico se maneja de acuerdo con la política estática HTTPS.
0x1 *xxxxxxx*	Server Any	Todas las conexiones SSL se aceleran con esta configuración de servicio acelerada

Ejemplo 1: Servicio acelerado con configuración de servidor-ip:

```
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
```

La entrada correspondiente del motor de políticas se agrega de la siguiente manera:

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

Ejemplo 2: Servicio acelerado con configuración de nombre de servidor:

Esta configuración permite una implementación sencilla para optimizar las aplicaciones SSL empresariales. Se puede adaptar a los cambios de configuración de DNS y reduce las tareas administrativas de TI.

```
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
```

La entrada correspondiente del motor de políticas se agrega de la siguiente manera:

```
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
```

Ejemplo 3: Servicio acelerado con configuración de dominio de servidor:

Esta configuración permite a los dispositivos WAAS configurar un único dominio comodín que evita la necesidad de conocer las direcciones IP para todos los servidores. El Data Center WAE utiliza DNS inverso (rDNS) para hacer coincidir el tráfico que pertenece al dominio configurado. La configuración de un dominio comodín evita la configuración de varias direcciones IP, lo que hace que la solución sea escalable y aplicable a la arquitectura 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
```

La entrada correspondiente del motor de políticas se agrega de la siguiente manera:

```
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
```

Ejemplo 4: Servicio acelerado con configuración de cualquier servidor IP:

Esta configuración proporciona un mecanismo de detección. Cuando un servicio acelerado con **server-ip any port 443** se activa, permite que todas las conexiones en el puerto 443 sean optimizadas por el SSL AO. Esta configuración se puede utilizar durante los POC para optimizar todo el tráfico en un puerto determinado.

```
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
```

La entrada correspondiente del motor de políticas se agrega de la siguiente manera:

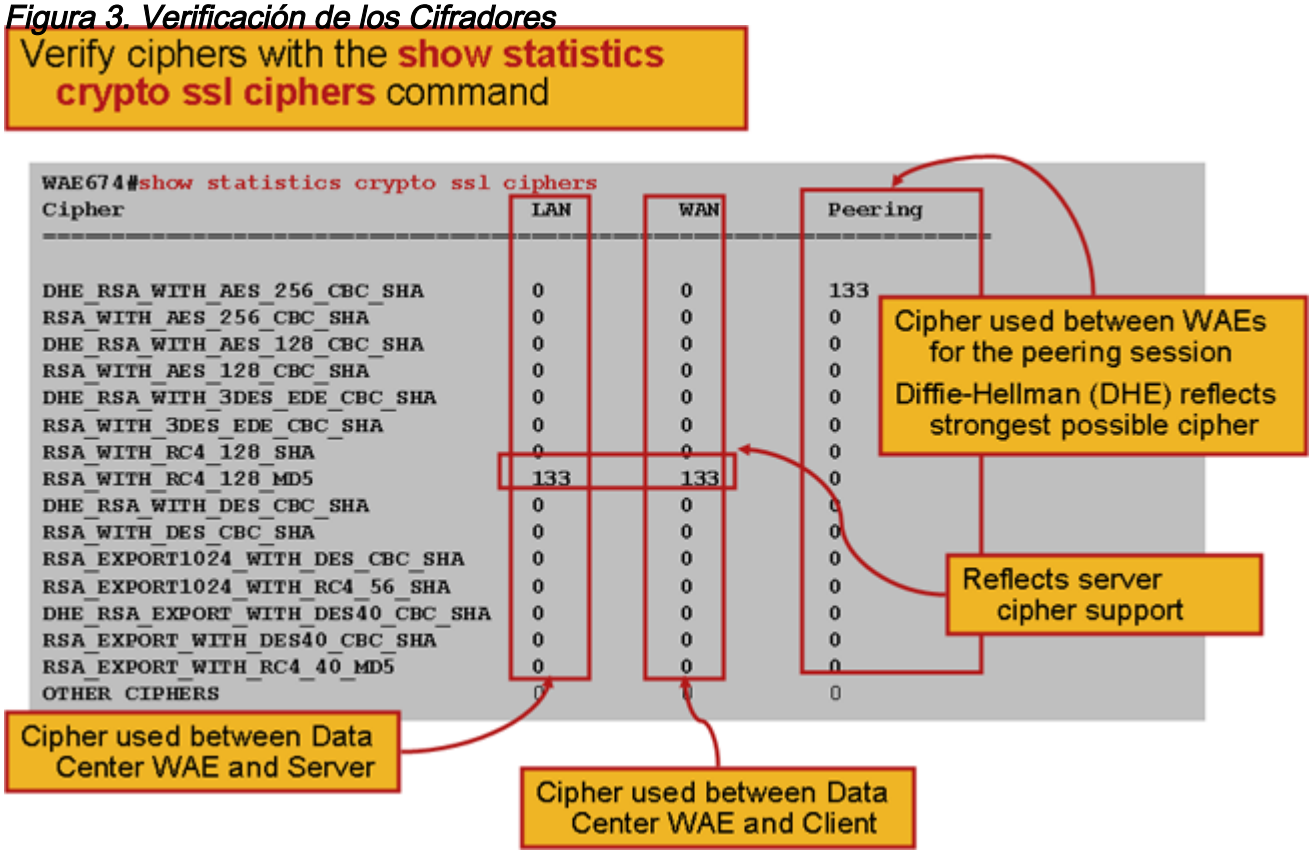
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

Puede verificar los cifrados que se utilizan con los comandos **show statistics crypto ssl ciphers**, como se muestra en la Figura 3.

Figura 3. Verificación de los Cifradores



Puede verificar que estos cifradores coincidan con los configurados en el servidor de origen. **Nota:** Los servidores IIS de Microsoft no admiten los cifrados que incluyen DHE.

En un servidor Apache, puede verificar la versión SSL y cifrar detalles en el archivo httpd.conf. Estos campos también pueden estar en un archivo independiente (sslmod.conf) al que se hace referencia desde httpd.conf. Busque los campos SSLProtocol y SSLCipherSuite de la siguiente manera:

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

Para verificar el emisor del certificado en un servidor Apache, utilice el comando openssl para leer el certificado de la siguiente manera:

```
> 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
```

En el explorador, puede ver un certificado y sus detalles para determinar la cadena de certificados, la versión, el tipo de clave de cifrado, el nombre común del emisor (CN) y el asunto/sitio CN. En Internet Explorer, haga clic en el icono de candado, haga clic en **Ver certificado** y, a continuación, consulte las fichas Detalles y Ruta de certificación para obtener esta información.

La mayoría de los exploradores requieren que los certificados de cliente estén en el formato PKCS12 en lugar del formato PEM X509. Para exportar el formato X509 PEM al formato PKCS12, utilice el comando openssl de la siguiente manera en un servidor Apache:

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

Si se cifran las claves privadas, se requiere la frase de paso para la exportación. La contraseña de exportación se utiliza de nuevo para importar credenciales al dispositivo WAAS.

Utilice el comando **show statistics Accelerator ssl** para ver las estadísticas de SSL AO.

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

Las sesiones fallidas y las estadísticas de verificaciones de certificados pueden ser útiles para la resolución de problemas y se recuperan más fácilmente utilizando el siguiente filtro en el comando **show statistics Accelerator 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
```

Las estadísticas relacionadas con DNS pueden ser útiles para la resolución de problemas de nombre de servidor y configuración de dominio comodín. Para recuperar estas estadísticas, utilice el comando **show statistics Accelerator ssl**, como se indica a continuación:

```
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
 . . .
```

Las estadísticas relacionadas con el intercambio de señales SSL pueden ser útiles para la resolución de problemas y se pueden recuperar usando el siguiente filtro en el comando **show statistics Accelerator 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
```

Utilice el comando **show statistics connection optimizada ssl** para verificar que el dispositivo WAAS está estableciendo conexiones SSL optimizadas. Verifique que "TDLS" aparezca en la

columna Accel para una conexión. "S" indica que el SSL AO se utilizó de la siguiente manera:

```
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"
```

Puede verificar las estadísticas de conexión para las conexiones cerradas usando el comando **show statistics connection Closed SSL**.

Si las conexiones no se están optimizando, verifique si WCCP/PBR está configurado y funcionando correctamente, y verifique si hay ruteo asimétrico.

Puede ver las estadísticas de conexión SSL usando el comando **show statistics connection optimizada ssl detail**, donde verá la política dinámica que resulta del servicio acelerado SSL configurado. **Nota:** La política configurada es solamente la optimización de TFO, pero la optimización completa se aplica como resultado del servicio SSL configurado.

```
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
. . .
```

Más adelante en este resultado, los detalles del nivel de sesión SSL extendido se muestran de la siguiente manera:

```
. . .
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
```

Resolución de problemas de conexiones de transferencia HTTP AO a SSL AO

Si un cliente debe pasar a través de un proxy para alcanzar un servidor HTTPS, la solicitud del cliente primero se envía como un mensaje HTTP CONNECT al proxy (con la dirección IP real del servidor HTTPS incrustada en el mensaje CONNECT). En este punto, el HTTP AO maneja esta conexión en los WAEs de peer. El proxy crea un túnel entre el cliente y el puerto del servidor y transmite los datos subsiguientes entre el cliente y esa dirección IP y puerto del servidor. El proxy responde al cliente con un mensaje "200 OK" y deja la conexión con el SSL AO porque el cliente pretende hablar con el servidor a través de SSL. A continuación, el cliente inicia un intercambio de señales SSL con el servidor SSL a través de la conexión TCP (túnel) configurada por el proxy.

Compruebe lo siguiente al resolver problemas con conexiones transferidas:

- Verifique el resultado del comando **show statistics Accelerator http** para confirmar que una conexión fue manejada por el HTTP AO y luego transferida al SSL AO. Observe el total de conexiones manejadas y conexiones totales transferidas a los contadores SSL. Si hay algún problema, verifique lo siguiente:
  - El HTTP AO está habilitado y en estado de ejecución en los WAEs de peer.
  - El servicio acelerado SSL se configura con el puerto utilizado por el cliente en la URL CONNECT (o con el puerto implícito 443 si se utiliza HTTPS). A menudo, el puerto proxy es diferente del puerto de URL CONNECT y este puerto proxy no se debe configurar en el servicio acelerado SSL. Sin embargo, el puerto proxy debe incluirse en el clasificador de tráfico asignado a HTTP AO.
- Verifique el resultado del comando **show statistics Accelerator http** para confirmar que esta conexión fue manejada y optimizada por SSL AO. Observe los contadores Total Handled Connections y Total Optimized Connections. Si los contadores de estadísticas no son correctos, realice la resolución de problemas básica de SSL, como se describe en la sección anterior.
- En el Data Center WAE, verifique que la salida del comando **show statistics connection optimized detail** muestre el nombre de host, la dirección IP y el puerto TCP del servidor SSL real. Si estos campos no están configurados correctamente, verifique lo siguiente:
  - Verifique que la configuración del proxy del navegador cliente sea correcta.
  - Verifique que el servidor DNS esté configurado en el WAE del Data Center y que sea accesible. Puede configurar un servidor DNS en el WAE con el comando **ip name-server** *A.B.C.D*.

Resolución de problemas de verificación de certificado del servidor

La verificación del certificado del servidor requiere que importe el certificado de CA correcto al WAE del Data Center.

Para resolver problemas de verificación del certificado del servidor, siga estos pasos:

1. Inspeccione el certificado del servidor y recupere el nombre del emisor. Este nombre del emisor dentro del certificado del servidor debe coincidir con el nombre del asunto dentro del certificado

CA correspondiente. Si tiene certificados codificados por PEM, puede utilizar el siguiente comando **openssl** en un servidor con openssl instalado:

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

2. Asegúrese de que exista la configuración crypto pki ca coincidente en el WAE del Data Center mediante el comando **show running-config**. Para que el WAE utilice un certificado de CA en el proceso de verificación, se requiere un elemento de configuración crypto pki ca para cada certificado de CA importado. Por ejemplo, si se importa un certificado de CA company1.ca, se debe realizar la siguiente configuración en el Data Center WAE:

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

Nota: Si se importa un certificado de CA mediante la GUI de Central Manager, el Central Manager agrega automáticamente la configuración crypto pki ca anterior para incluir el certificado de CA importado. Sin embargo, si el certificado de CA se importa a través de la CLI, deberá agregar manualmente la configuración anterior.

3. Si el certificado que se verifica incluye una cadena de certificados, asegúrese de que la cadena de certificados sea coherente y que el certificado de CA del emisor superior se importe en WAE. Utilice el comando **openssl verify** para verificar primero el certificado por separado.

4. Si la verificación aún falla, examine el registro de depuración del acelerador SSL. Utilice los siguientes comandos para habilitar el registro de depuración:

```
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. Inicie una conexión de prueba y, a continuación, examine el archivo de registro /local/local1/errorlog/sslao-errorlog.current. Este archivo debe indicar el nombre del emisor que se incluyó en el certificado del servidor. Asegúrese de que este nombre del emisor coincida exactamente con el nombre del asunto del certificado de CA.

Si hay otros errores internos en los registros, puede ser útil habilitar opciones de depuración adicionales.

6. Aunque el nombre del emisor y los nombres de asunto coincidan, es posible que el certificado de CA no sea el correcto. En tales casos, si el certificado del servidor es emitido por una CA conocida, se puede utilizar un explorador para alcanzar directamente (sin WAAS) el servidor. Cuando el explorador configura la conexión, se puede examinar el certificado haciendo clic en el icono de bloqueo que aparece en la parte inferior derecha de la ventana del explorador o en la barra de direcciones del explorador. Los detalles del certificado pueden indicar el certificado de CA adecuado que coincida con este certificado de servidor. Verifique el campo Número de serie dentro del certificado de CA. Este número de serie debe coincidir con el número de serie del certificado que se está importando en el WAE del Data Center.

7. Si tiene habilitada la verificación de revocación de OCSP, inhabilite y verifique que la verificación del certificado funcione por sí misma. Para obtener ayuda para la resolución de problemas de la configuración de OCSP, consulte la sección "Resolución de problemas de verificación de revocación de OCSP".

Resolución de problemas de verificación de certificado de cliente

La verificación del certificado de cliente puede estar habilitada en el servidor de origen y/o en el centro de datos WAE. Cuando WAAS se utiliza para acelerar el tráfico SSL, el certificado de cliente recibido por el servidor de origen es el certificado indicado en la clave de certificado de máquina especificada en el comando **crypto ssl services global-settings** en el WAE del Data Center o en el certificado autofirmado de la máquina WAE del Data Center, si la clave de certificado de máquina no está configurada. Como resultado, si la verificación del certificado del cliente falla en el servidor de origen, puede ser porque el certificado de máquina WAE del Data Center no es verificable en el servidor de origen.

Si la verificación del certificado de cliente en el WAE del Data Center no funciona, es probable que el certificado CA que coincide con el certificado de cliente no se importe en el WAE del Data Center. Consulte la sección "Resolución de problemas de verificación de certificados de servidor" para obtener instrucciones sobre cómo comprobar si se ha importado el certificado de CA correcto en WAE.

Resolución de problemas de verificación de certificado WAE de par

Para resolver problemas de verificación de certificados de peer, siga estos pasos:

1. Verifique que el certificado que se verifica sea un certificado firmado por CA. Otro WAE no puede verificar un certificado autofirmado por un WAE. Los WAE se cargan de forma predeterminada con certificados autofirmados. Se debe configurar un certificado autofirmado usando el comando **crypto ssl services global-settings machine-cert-key**.

2. Verifique que el certificado de CA correcto esté cargado en el dispositivo que verifica el certificado. Por ejemplo, si se configura peer-cert-verify en el Data Center WAE, es esencial que el certificado WAE de la sucursal esté firmado por CA y que el mismo certificado de CA de firma se importe en el Data Center WAE. No olvide crear una CA mediante el comando **crypto pki ca** para utilizar el certificado importado, si está importando el certificado manualmente a través de la CLI. Cuando lo importa la GUI de Central Manager, el Administrador Central crea automáticamente una configuración crypto pki ca coincidente.

3. Si la verificación del WAE del peer aún falla, verifique los registros de depuración como se describe en la sección "Registro de SSL AO".

Resolución de problemas de verificación de revocación de OCSP

Si el sistema tiene problemas para realizar conexiones SSL exitosas con la verificación de revocación del protocolo de estado de certificados en línea (OCSP) activada, siga estos pasos de solución de problemas:

1. Asegúrese de que el servicio de respuesta OCSP se esté ejecutando en el servidor de respuesta.
2. Garantizar una buena conectividad entre el WAE y el respondedor. Utilice los comandos **ping** y **telnet** (al puerto apropiado) del WAE para verificar.
3. Confirme que el certificado que se está validando es válido. La fecha de vencimiento y la

URL de respuesta correcta son generalmente áreas donde hay problemas.

4. Verifique que el certificado para las respuestas de OCSP se importe en el WAE. Las respuestas de un respondedor OCSP también se firman y el certificado CA que coincida con las respuestas OCSP debe residir en el WAE.
5. Verifique el resultado del comando **show statistics Accelerator ssl** para verificar las estadísticas de OCSP y verificar los contadores que corresponden a las fallas de OCSP.
6. Si la conexión HTTP de OCSP está atravesando un proxy HTTP, intente desactivar el proxy para ver si ayuda. Si ayuda, verifique que la configuración del proxy no esté causando la falla de conexión. Si la configuración del proxy es correcta, puede haber alguna peculiaridad de encabezado HTTP que pueda estar causando alguna incompatibilidad con el proxy. Capture un seguimiento de paquetes para una investigación más detallada.
7. Si todo lo demás falla, es posible que tenga que capturar un seguimiento de paquetes de la solicitud de OCSP saliente para una depuración adicional. Puede utilizar los comandos **tcpdump** o **teéreal** como se describe en la sección "Captura y análisis de paquetes" en el artículo de Troubleshooting de WAAS Preliminar.

La URL utilizada por el WAE del Data Center para llegar a un respondedor OCSP se deriva de una de estas dos maneras:

- La URL estática de OCSP configurada por el comando de configuración **crypto pki global-settings**
- La URL de OCSP especificada en el certificado que se está comprobando

Si la URL deriva del certificado que se está comprobando, es esencial asegurarse de que la URL sea accesible. Habilite los registros de depuración de OCSP del acelerador SSL para determinar la URL y luego verifique la conectividad con el respondedor. Consulte la siguiente sección para obtener detalles sobre el uso de los registros de depuración.

Resolución de problemas de configuración DNS

Si el sistema está teniendo problemas para optimizar las conexiones SSL con el nombre del servidor y las configuraciones del dominio del servidor, siga estos pasos de solución de problemas:

1. Asegúrese de que el servidor DNS configurado en el WAE sea accesible y pueda resolver los nombres. Utilice el siguiente comando para verificar el servidor DNS configurado:

```
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 !
```

Esta respuesta indica que los servidores de nombres configurados no pueden resolver el nombre.

Pruebe ping/traceoute para los servidores de nombres configurados para verificar su disponibilidad y el tiempo de ida y vuelta.

```
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 el servidor DNS es accesible y puede resolver nombres y aún así las conexiones SSL no se están optimizando, asegúrese de que el servicio acelerado que configura el dominio o nombre de host especificado esté activo y no haya alarmas para SSL AO. Utilice los siguientes comandos:

```
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 presencia de la alarma "accl_svc_idle" es una indicación de que hay alguna discrepancia en la configuración del servicio acelerado y puede haber uno o más servicios acelerados con configuración superpuesta para las entradas del servidor. Verifique la configuración del servicio acelerado y asegúrese de que la configuración sea correcta. Utilice el siguiente comando para verificar la configuración:

```
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
```

Para comprobar los detalles de un servicio acelerado determinado, utilice el siguiente comando:

```
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
```

Una de las razones por las que el estado operativo del servicio acelerado puede ser INACTIVO es una falla de DNS. Por ejemplo, si hay un nombre de host del servidor en la configuración de servicio acelerada y WAE no puede resolver la dirección IP del servidor, no puede configurar la política dinámica apropiada.

3. Si el contador de estadísticas para "Pipe-through debido a un nombre de dominio no coincidente" está aumentando, es una indicación de que la conexión SSL es para un servidor configurado para optimización. Verifique las entradas del motor de políticas utilizando el siguiente comando:

```
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
```

Verifique el estado de la conexión usando el comando **show statistics connection**. La primera conexión debe mostrar un Acelerador de TSGDL y las conexiones subsiguientes, hasta la duración de la entrada de política TIME_DENY, deben ser TDL.

4. Si el servidor DNS se encuentra a través de la WAN con respecto al WAE del Data Center o si el tiempo de respuesta del DNS inverso es demasiado largo, es posible que algunas conexiones se pierdan. Esto depende del tiempo de espera del cliente y del tiempo de respuesta de rDNS. En este caso, el contador de "Número de búsquedas de DNS inversas canceladas" aumenta y la conexión se interrumpe. Esta situación es una indicación de que el servidor DNS no responde o es muy lento y/o NSCD en WAAS no funciona. El estado de NSCD se puede verificar usando el comando **show alarms**. La probabilidad de que esto ocurra es muy baja, ya que en la mayoría de las implementaciones, se espera que el servidor DNS esté en la misma LAN que el WAE del Data Center.

Resolución de problemas de encadenamiento HTTP a SSL AO

NOTE: El encadenamiento de HTTP a SSL AO se introdujo en WAAS versión 4.3.1. Esta sección no se aplica a las versiones anteriores de WAAS.

El encadenamiento permite a un AO insertar otro AO en cualquier momento durante la vida útil de un flujo y ambos AO pueden aplicar su optimización específica de AO independientemente en el flujo. El encadenamiento de AO es diferente de la función de transferencia de AO proporcionada por WAAS en las versiones anteriores a 4.3.1 porque con el encadenamiento de AO el primer AO continúa optimizando el flujo.

El SSL AO gestiona dos tipos de conexiones:

- Byte-0 SSL: El SSL AO recibe primero la conexión y completa el intercambio de señales SSL. Analiza la parte inicial de la carga útil para comprobar un método HTTP. Si la carga útil indica HTTP, inserta el HTTP AO; si no, aplica la optimización de TSDL normal.
- CONEXIÓN DE Proxy: El HTTP AO recibe primero la conexión. Identifica el método del encabezado CONNECT en la solicitud del cliente e inserta el SSL AO después de que el

proxy confirme con un mensaje 200 OK.

El SSL AO utiliza un analizador HTTP ligero que detecta los siguientes métodos HTTP: GET, HEAD, POST, PUT, OPTIONS, TRACE, COPY, LOCK, POLL, BCOPY, BMOVE, MKCOL, DELETE, SEARCH, DESLOCK, BDELETE, PROPFINE, BPROPFINY, PROPPATCH, SUBSCRIBE, BPROPPATCH, UNSUBSCRIBE Y X__MS_ENUMATTS ... Puede utilizar el comando **debug Accelerator ssl parser** para depurar problemas relacionados con el analizador. Puede utilizar el **comando show stat accel ssl payload http/other** para ver las estadísticas del tráfico clasificado en función del tipo de carga útil.

Consejos de Troubleshooting:

1. Asegúrese de que la función HTTPS está habilitada en la configuración de HTTP AO ya que es propiedad de HTTP AO. Para obtener más información, vea el artículo Resolución de problemas del protocolo AO HTTP.
2. Verifique el estado de conexión usando el comando **show stat connection**. Si se optimiza correctamente, debe mostrar THSDL indicando la optimización de TCP, HTTP, SSL y DRE-LZ. Si falta alguna de estas optimizaciones, realice un debug adicional en ese optimizador (SSL, HTTP, etc.). Por ejemplo, si el estado de la conexión muestra THDL, significa que la optimización SSL no se aplicó en la conexión. A continuación se detallan los problemas de depuración relacionados con SSL AO.
3. Asegúrese de que SSL AO esté habilitado y en el estado en ejecución (consulte la sección "Resolución de problemas de SSL AO").
4. Asegúrese de que no haya alarmas usando el comando **show alarms**.
5. Si el tráfico SSL no se está optimizando, asegúrese de que la dirección IP del servidor, el nombre de host o el nombre de dominio y el número de puerto se agregan como parte del servicio acelerado.
6. Asegúrese de que el servicio acelerado esté en estado ACTIVO mediante el comando **show crypto ssl services Acceler-service *ASVC-name*** (consulte la sección "Resolución de problemas de configuración DNS").
7. Asegúrese de que el motor de políticas tenga una entrada para este servidor y puerto usando el comando **show policy-engine application dynamic**.
8. Si el servidor de destino está utilizando SSL en un puerto no predeterminado (el valor predeterminado es 443), asegúrese de que esto se refleje en la configuración del motor de políticas. El Administrador central se basa en esta información para informar de los datos de tráfico SSL.
9. Asegúrese de que el nombre de host configurado se resuelva en una dirección IP válida mediante el comando **show crypto ssl services Acceler-service *ASVC-name***. Si no se encuentra ninguna dirección IP, verifique si el servidor de nombres está configurado correctamente. También verifique el resultado del comando **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
```

Registro de SSL AO

Los siguientes archivos de registro están disponibles para resolver problemas de SSL AO:

- Archivos de registro de transacciones: /local1/logs/tfo/working.log (y /local1/logs/tfo/tfo_log_*.txt)
- Archivos de registro de depuración: /local1/errorlog/sslao-errorlog.current (y sslo-errorlog.*)

Para una depuración más sencilla, primero debe configurar una ACL para restringir los paquetes a un 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
```

Para habilitar el registro de transacciones, utilice el comando de configuración **Transaction-logs** de la siguiente manera:

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

Puede ver el final de un archivo de registro de transacciones utilizando el comando **type-tail** de la siguiente manera:

```
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
```

Para configurar y habilitar el registro de depuración de SSL AO, utilice los siguientes comandos.

NOTE: El registro de depuración hace un uso intensivo de la CPU y puede generar una gran cantidad de resultados. Utilícelo de manera sensata y moderada en un entorno de producción.

Puede habilitar el registro detallado en el disco de la siguiente manera:

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

Puede habilitar el registro de depuración para las conexiones en la ACL de la siguiente manera:

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

Las opciones para la depuración de SSL AO son las siguientes:

```
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
```

Puede habilitar el registro de depuración para las conexiones SSL y, a continuación, mostrar el final del registro de errores de depuración de la siguiente manera:

```
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
```

Resolución de problemas de alarmas de vencimiento de certificados en módulos NME y SRE

El SSL AO genera alarmas cuando el certificado de máquina autofirmado ha caducado (o está dentro de los 30 días de vencimiento) y no se ha configurado un certificado de máquina global personalizado en el dispositivo WAAS. El software WAAS genera certificados autofirmados de fábrica con una fecha de vencimiento de 5 años desde el primer inicio del dispositivo WAAS.

El reloj en todos los módulos WAAS NME y SRE se configura al 1 de enero de 2006 durante el primer inicio, aunque el módulo NME o SRE sea más reciente. Esto hace que el certificado autofirmado venza el 1 de enero de 2011 y el dispositivo genera alarmas de vencimiento del certificado.

Si no utiliza el certificado de fábrica predeterminado como certificado global y, en su lugar, está utilizando un certificado personalizado para SSL AO, no experimentará esta caducidad inesperada y podrá actualizar el certificado personalizado cada vez que caduque. Además, si ha actualizado el módulo NME o SME con una nueva imagen de software y ha sincronizado el reloj a una fecha más reciente, es posible que no experimente este problema.

El síntoma de vencimiento del certificado es una de las siguientes alarmas (se muestra aquí en el resultado del comando **show alarms**):

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

or

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

La GUI de Central Manager informa de la siguiente alarma: "Certificate__waas-self_.p12 está a punto de caducar y está configurado como certificado de máquina en configuraciones globales"

Puede utilizar una de las siguientes soluciones para resolver este problema:

- Configure un certificado diferente para la configuración global:

```
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
```

- Actualice el certificado de fábrica autofirmado con una fecha de vencimiento posterior. Esta solución requiere un script que puede obtener poniéndose en contacto con el TAC de Cisco.

NOTE: Este problema se soluciona mediante la resolución de advertencia CSCte05426, publicada en las versiones 4.1.7b, 4.2.3c y 4.3.3 del software WAAS. La fecha de vencimiento de la certificación se cambia a 2037.