Guía de Troubleshooting de Cisco WAAS para la versión 4.1.3 y más adelante

Capítulo: Resolver problemas el SSL AO

Este artículo describe cómo resolver problemas el SSL AO.

Co

Art
Co
WA
Tro
Re
Re
Re
Re
Re
Re
Re
Re
Re
Re
Re
Re
Re
Re
har
Re
Re
Re
Re

Contenido

Descripción del acelerador SSL

El acelerador SSL (adentro 4.1.3 y más adelante disponibles) optimiza el tráfico cifrado de Secure Sockets Layer (SSL) y de Transport Layer Security (TLS). El acelerador SSL proporciona a la encripción del tráfico y al desciframiento dentro de WAAS para activar la optimización del tráfico de extremo a extremo. El acelerador SSL también proporciona a la Administración segura de los Certificados y de las claves del cifrado.

En una red WAAS, el centro de datos WAE actúa como nodo intermediario de confianza para las peticiones SSL del cliente. La clave privada y el certificado de servidor se salvan en el centro de datos WAE. El centro de datos WAE participa en el contacto SSL para derivar la clave de la sesión, que distribuye con seguridad la en-banda a la bifurcación WAE, permitiendo que la bifurcación WAE desencripte el tráfico del cliente, optimice lo, el reencrypt él, y lo envíe sobre WAN al centro de datos WAE. El centro de datos WAE mantiene a una sesión SSL separada con el servidor de origen.

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

- Servicio acelerado – Una entidad de configuración que describe las características de la aceleración que se solicitarán un servidor SSL o un conjunto de los servidores. Especifica el certificado y la clave privada que se utilizarán mientras que presenta como un intermediario de confianza, las cifras que se utilizarán, SSL versión permitió, y configuración de la verificación del certificado.
- Servicio de mirada – Una entidad de configuración que describe las características de la aceleración que se solicitarán las conexiones SSL de la en-banda entre la bifurcación y el centro de datos WAEs. Este servicio se utiliza para transferir la información de clave de la sesión del centro de datos para ramificar WAEs para las conexiones SSL óptimas.
- Servicio central Admin del encargado – No utilizado directamente por el acelerador SSL, pero ser utilizado por un administrador para la administración de la configuración de los servicios acelerados SSL. También utilizado para cargar por teletratamiento los Certificados y las claves privadas que se utilizarán en los servicios acelerados SSL.
- Servicio de administración central del encargado – No utilizado directamente por el acelerador SSL, sino utilizado para la comunicación entre los dispositivos del acelerador de la aplicación y el encargado central. Este servicio se utiliza para la administración de la configuración, asegura la extracción de la clave de encripción del almacén, y las actualizaciones de estado del dispositivo.

El almacén seguro del encargado central es esencial para el SSL AO de actuar porque salva asegura las claves de encripción para todo el WAEs. Después de que cada recarga central del encargado, el administrador necesite abrir de nuevo el almacén seguro proveyendo de la frase de contraseña el **comando open del seguro-almacén CMS**. Un WAE extrae automáticamente su clave de encripción segura del almacén del encargado central siempre que el WAE reinicie, así que no se requiere ninguna acción en el WAE después de una recarga.

Si los clientes están utilizando una solución del proxy de HTTP, la conexión inicial es manejada por el HTTP AO, que la reconoce como petición del túnel SSL al puerto 443. El HTTP AO busca un servicio acelerado SSL que corresponde con definido en el centro de datos WAE y cuando encuentra una coincidencia, las manos de la conexión al SSL AO. Sin embargo, el tráfico que el HTTP AO da apagado al SSL AO para un proxy HTTPS consigue señalado como parte de las estadísticas de la aplicación de Web, no en la aplicación SSL. Si el HTTP AO no encuentra una coincidencia, la conexión se optimiza según la configuración de la política estática HTTPS (SSL).

El SSL AO puede utilizar los certificados autofirmados bastante que los Certificados Ca-firmados, que pueden ser útiles en los sistemas de la prueba de concepto que despliegan (PC) y en resolver problemas los problemas SSL. Usando los certificados autofirmados, usted puede desplegar rápidamente un sistema WAAS sin tener que importar los Certificados de servidor de origen, y usted puede eliminar los Certificados como fuente potencial de problemas. Usted puede configurar un certificado autofirmado en el encargado central al crear un servicio acelerado SSL. Sin embargo, cuando usted utiliza un certificado autofirmado, el buscador del cliente visualizará una alerta de seguridad que el certificado es untrusted (porque no es firmado por un CA bien conocido). Para evitar esta advertencia de seguridad, instale el certificado en el almacén de los Trusted Root Certification Authority en el buscador del cliente. (En el Internet Explorer, en la advertencia de seguridad, el **certificado de la opinión del** tecleo, después en el tecleo del diálogo del certificado **instala el certificado** y completa al Asisitente de la importación del certificado.)

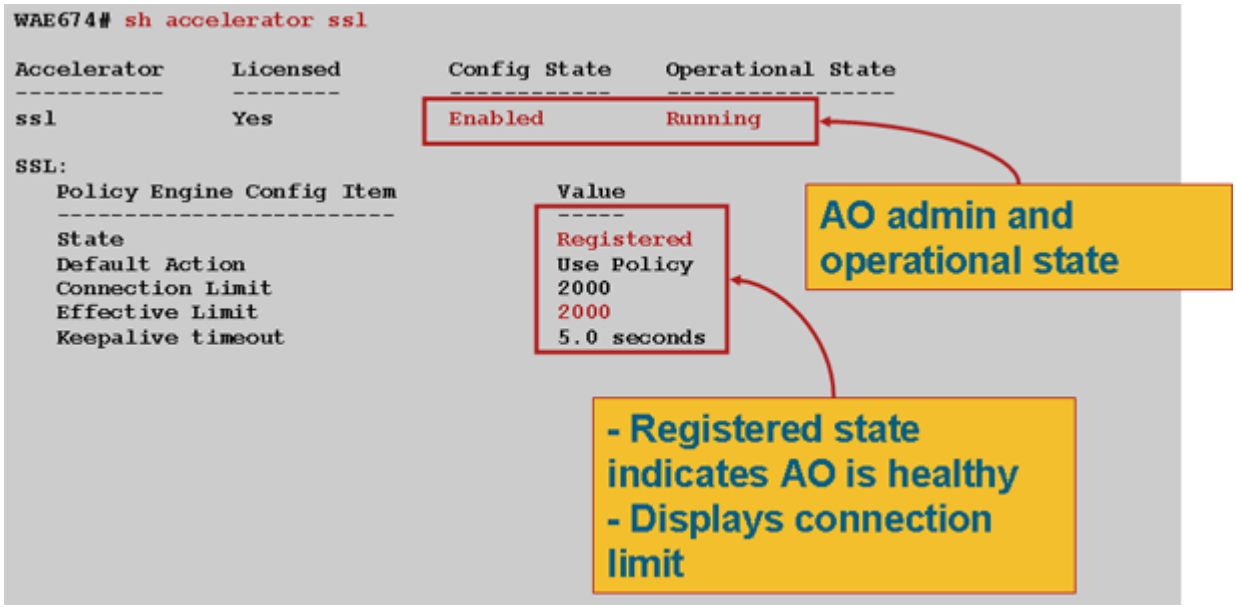
Configurar los servicios de administración SSL es opcional, y permite que usted cambie el SSL versión y la lista de la cifra usados para las comunicaciones centrales del encargado a WAEs y al navegador (para el acceso administrativo). Si usted configura las cifras que no son utilizadas por su navegador, usted perderá la conexión al encargado central. En este caso, utilice el comando configuration **crypto del servicio de administración SSL del** CLI de fijar las configuraciones del servicio de administración SSL de nuevo al valor por defecto.

Resolver problemas el SSL AO

Usted puede verificar la configuración general y el estatus AO con el **acelerador de la demostración** y **mostrar los comandos license**, según lo descrito en el artículo de la aceleración de la aplicación del troubleshooting. La licencia de la empresa se requiere para la operación del acelerador SSL.

Después, verifique el estatus que es específico al SSL AO en el centro de datos y la bifurcación WAEs usando el comando **SSL del acelerador de la demostración**, tal y como se muestra en del cuadro 1. Usted quiere ver que el SSL AO está activado, ejecutándose, y registrado, y que el límite de la conexión está visualizado. Si se activa el estado de los Config pero el estado operacional es parada normal, indica un problema de la autorización. Si inhabilitan al estado operacional, puede ser porque el WAE no puede extraer las claves SSL del almacén seguro del encargado central, cualquiera porque el almacén seguro no está abierto o el encargado central es inalcanzable. Utilice la **información** y los **comandos ping CMS de la demostración** de confirmar que el encargado central es accesible.

Cuadro 1. que verifica el estatus del acelerador SSL



Si usted ve a un estado operacional de Params Crypto GEN, espere hasta que el estatus llegue a ser que se ejecuta, que puede tardar algunos minutos que siguen una reinicialización. Si usted ve un estado de extraer las claves del cm para más que algunos minutos, podría indicar que el servicio de CMS en el encargado central no se está ejecutando, que no hay conectividad de red al encargado central, que las versiones WAAS en el WAE y el encargado central son incompatibles, o que el almacén seguro del encargado central no está abierto.

Usted puede verificar que el almacén seguro del encargado central esté inicializado y abrirse usando el comando del seguro-**almacén CMS de la demostración** como sigue:

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

Si el almacén seguro no se inicializa ni se abre, usted verá las Alarmas críticas tales como mstore_key_failure y seguro-almacén. Usted puede abrir el almacén seguro con el **comando open del seguro-almacén CMS** o del encargado central, elige **Admin > asegura el almacén**.

Consejo: Documente la contraseña segura del almacén para evitar tener que reajustar el almacén seguro si usted olvida la contraseña.

Si hay un problema con el cifrado del disco en un WAE, ése puede también evitar que el SSL AO actúe. Utilice el **comando show disk details** de verificar que el cifrado del disco está activado y controle si se montan las divisiones del CONTENIDO y del CARRETE. Si se montan estas divisiones, indica que las claves de encripción del disco fueron extraídas con éxito del encargado central y los datos encriptados pueden ser escritos y leer en los discos. Si el **comando show disk details** muestra el “sistema se está inicializando,” que indica que las claves de encripción todavía no se han extraído del encargado central y los discos todavía no se han montado. El WAE no proporcionará los servicios de la aceleración en este estado. Si el WAE no puede extraer las claves de encripción del disco del encargado central, aumentará una alarma.

Usted puede verificar que configuren al servicio acelerado SSL y su estatus “está activado” en el centro de datos WAE (en el encargado central, elija el dispositivo, después elija **configuran > aceleración > los servicios acelerados SSL**). Un servicio acelerado configurado y activado puede ser hecho inactivo por el acelerador SSL debido a las condiciones siguientes:

- El certificado configurado en el servicio acelerado suprimido del WAE. Utilice el **comando show running-config** de determinar el certificado que es utilizado en el servicio acelerado,

después utilice los **Certificados crypto de la demostración** y **muestre que los** comandos **crypto de los detalles del certificado** de confirmar que el certificado está presente asegure el almacén. Si el certificado falta, reimporte el certificado.

- El certificado del servicio acelerado ha expirado. Utilice los **Certificados crypto de la demostración** y **muestre a detalles del certificado crypto los** comandos de controlar la fecha de vencimiento del certificado.
- El certificado del servicio acelerado tiene una fecha válida que comienza en el futuro. Utilice los **Certificados crypto de la demostración** y **muestre a detalles del certificado crypto los** comandos y controle la sección de la validez de la salida del comando. También, asegúrese de que el reloj y el información. de la franja horaria WAE sea exactos.

Usted puede verificar que las conexiones SSL tengan la directiva correcta aplicada, es decir, tienen optimización completa con la aceleración SSL, tal y como se muestra en del cuadro 2. En el encargado central, elija el dispositivo WAE, después elija el **monitor > las estadísticas de la optimización > de las conexiones**.

Cuadro 2. que verifica la directiva correcta en las conexiones SSL

Utilice el **comando show running-config** de verificar que la política de tráfico HTTPS está configurada correctamente. Usted quiere ver **optimizar DRE ninguna compresión ningunos** para la acción y usted de la aplicación SSL quiere considerar que las condiciones apropiadas de la coincidencia enumeraron para el clasificador HTTPS, como sigue:

```
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 las directivas dinámicas correspondiente al IP del servidor: puerto, nombre de servidor: puerto, o dominio del servidor: puerto configurado dentro del servicio acelerado. Estas directivas se pueden examinar usando el **comando dynamic de la aplicación del**

motor de directivas de la demostración. El campo de Dst en cada directiva visualizada indica IP del servidor y el puerto que corresponde con el servicio acelerado. Para el dominio del comodín (por ejemplo, el puerto 443 del dominio del servidor *.webex.com), el campo de Dst será 'Any:443. Para la configuración del servidor-nombre, se realiza la búsqueda de DNS delantera cuando activan al servicio acelerado y todos los IP Addresses vueltos en la respuesta de DNS será insertado en el motor de directivas. Este comando es útil para coger las situaciones donde está “en servicio un servicio acelerado marcado” pero hacen al servicio acelerado inactivo debido a un cierto otro error. Por ejemplo, todos los servicios acelerados son dependientes en el servicio del peering, y si el servicio del peering está inactivo debido a un certificado que falta/suprimido, después un servicio acelerado también serán marcados como inactivo aunque aparezca ser “en servicio” en la salida de los ejecutar-config de la demostración. Usted puede verificar que la directiva dinámica SSL sea activa en el centro de datos WAE usando el **comando dynamic de la aplicación del showpolicy-motor**. Usted puede verificar el estatus del servicio del peering usando el **comando del peering del Servicio de host de los servicios SSL del** showcrypto.

Una configuración del servicio acelerado SSL AO puede tener cuatro tipos de Entradas de servidor:

- IP estático (IP del servidor)--disponible en la versión 4.1.3 y posterior
- Coja todos (IP del servidor ningunos)--adentro 4.1.7 y más adelante disponibles
- Hostname (servidor-nombre)--adentro 4.2.1 y más adelante disponibles
- Dominio del comodín (dominio del servidor)--adentro 4.2.1 y más adelante disponibles

Una vez que la conexión es recibida por el SSL AO, decide a qué servicio acelerado debe ser utilizado para la optimización. IP estático la configuración se da la mayor preferencia, seguida por el nombre de servidor, dominio del servidor, y entonces IP del servidor. Si ningunos de los servicios acelerados configurados y activados hacen juego con IP del servidor para la conexión, la conexión se empuja hacia abajo al AO genérico. El Cookie insertado en el motor de directivas por el SSL AO se utiliza para determinar qué servicio acelerado y qué tipo de Entrada de servidor se corresponde con para una conexión determinada. Este Cookie del motor de directivas es un número de 32 bits y es significativo solamente al SSL AO. Los bits más altos se utilizan para indicar que diversos tipos de la Entrada de servidor y los bits más bajos indican el índice del servicio acelerado, como sigue:

Valores del Cookie del motor de directivas SSL

Valor del Cookie	Tipo de la Entrada de servidor	Comentarios
0x8xxxxxx	Dirección IP del servidor	Configuración estática de la dirección IP
0x4xxxxxx	Hostname del servidor	El centro de datos WAE realiza una búsqueda de DNS delantera para el hostname y agrega los IP Addresses que se vuelven en la configuración de la política dinámica. Restauró cada 10 minutos por abandono.
0x2FFFFFFF	Domain Name del servidor	El centro de datos WAE realiza una búsqueda de DNS reversible en la dirección IP del host del destino para determinar si hace juego con el dominio. Si hace juego, después se acelera el tráfico SSL, y si no hace juego, el tráfico se maneja según la directiva estática HTTPS.

0x1xxxxxxx	Servidor	Todas las conexiones SSL se aceleran usando esta configuración del servicio acelerado

Ejemplo 1: Servicio acelerado con IP del servidor la configuración:

```
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
```

Se agrega la entrada correspondiente del motor de directivas como sigue:

```
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 la configuración del servidor-nombre:

Esta configuración permite el despliegue fácil para la optimización de las aplicaciones SSL de la empresa. Es adaptable a los cambios de Configuración de DNS y reduce las tareas administrativas TIC.

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

Se agrega la entrada correspondiente del motor de directivas como sigue:

```
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 la configuración del dominio del servidor:

Esta configuración permite que los dispositivos WAAS configuren un solo dominio del comodín que evite la necesidad de conocer los IP Addresses para todos los servidores. El centro de datos WAE utiliza DNS reverso (rDNS) para hacer juego el tráfico que pertenece al dominio configurado. Configurar un dominio del comodín evita configurar los IP Addresses múltiples, haciendo la solución escalable y aplicable para la arquitectura de SaaS.

```
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
```

Se agrega la entrada correspondiente del motor de directivas como sigue:

```
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 IP del servidor cualquier configuración:

Esta configuración proporciona a un mecanismo del atrapador. Cuando hacen un servicio acelerado con **IP del servidor cualquier puerto 443** active, permite que todas las conexiones en el puerto 443 sean optimizadas por el SSL AO. Esta configuración se puede utilizar durante POCs para optimizar todo el tráfico en un puerto determinado.

```
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
```

Se agrega la entrada correspondiente del motor de directivas como sigue:

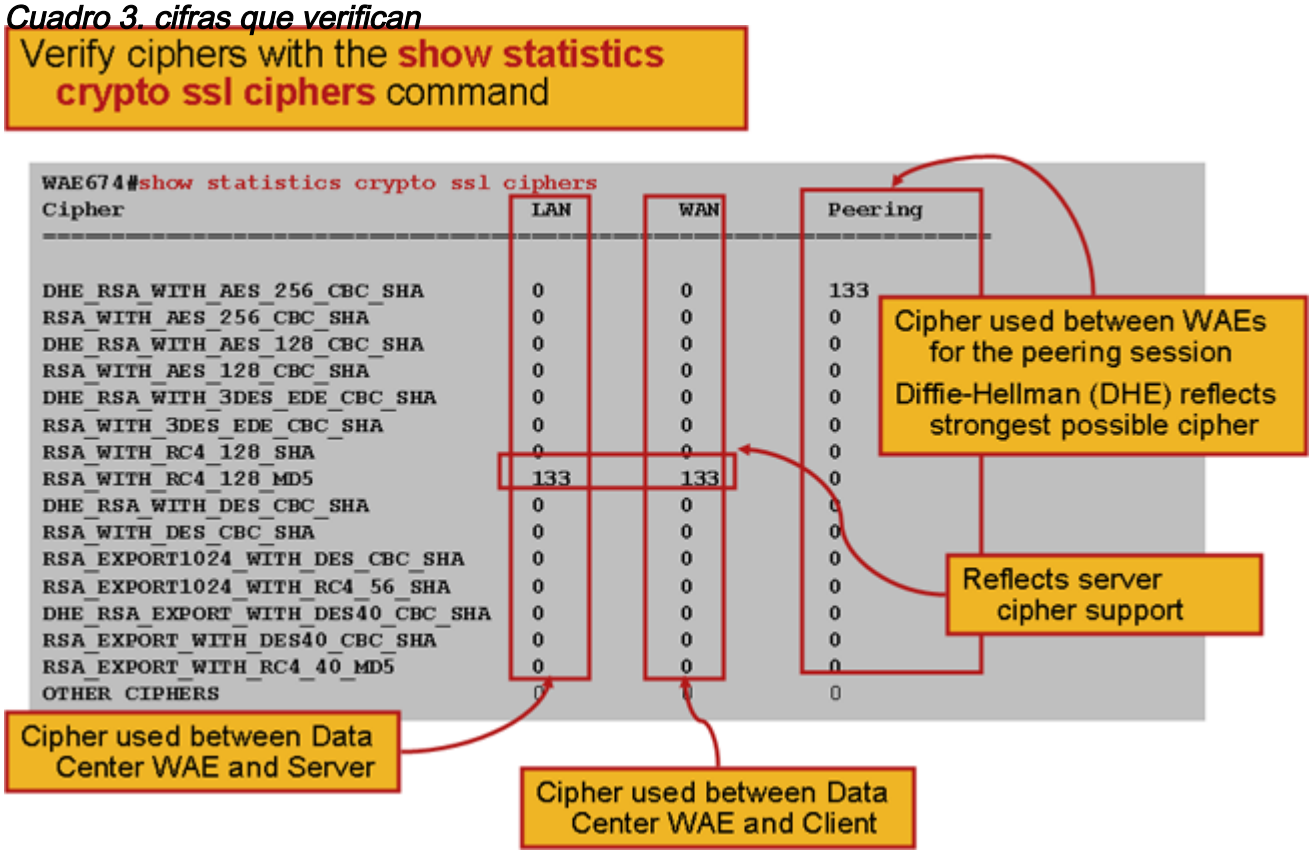
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

Usted puede verificar las cifras que son utilizadas con los comandos **estadísticas de cifrado de las cifras SSL de la demostración**, tal y como se muestra en del cuadro 3.

Cuadro 3. cifras que verifican



Usted puede verificar que estas cifras hagan juego ésos configurados en el servidor de origen.
Note: Las cifras que incluyen DHE no son utilizadas por los servidores IIS de Microsoft.

En un Apache Server, usted puede verificar que los detalles del SSL versión y de la cifra en el httpd.conf clasifíen. Estos campos pueden también estar en un archivo distinto (sslmod.conf) referido de httpd.conf. Busque los campos de SSLProtocol y de SSLCipherSuite como sigue:

```
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
```

Para verificar el emisor del certificado en un Apache Server, utilice el comando del openssl de leer el certificado como sigue:

```
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
```

En el navegador, usted puede ver un certificado y sus detalles para determinar la Cadena de certificados, la versión, el tipo de la clave de encripción, el nombre común del emisor (NC), y el NC del tema/del sitio. En el Internet Explorer, haga clic el icono del candado, haga clic el **certificado de la visión**, y después mire las tabulaciones de los detalles y del trayecto de certificación para esta información.

La mayoría de los navegadores requieren que los certificados del cliente estén en el formato PKCS12 bastante que el formato X509 PEM. Para exportar el formato X509 PEM al formato PKCS12, utilice el comando del openssl como sigue en un Apache Server:

```
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
```

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

Utilice el comando **SSL del acelerador de las estadísticas de la demostración** de ver las estadísticas 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 y las estadísticas falladas de las verificaciones del certificado pueden ser útiles para resolver problemas y se extraen más fácilmente usando el filtro siguiente en el comando **SSL del acelerador de las estadísticas de la demostración**:

```
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 DNS pueden ser útiles para resolver problemas el nombre de servidor y el comodín Domain Configuration (Configuración del dominio). Para extraer estas estadísticas utilice el comando **SSL del acelerador de las estadísticas de la demostración**, como sigue:

```
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 rehandshake SSL pueden ser útiles para resolver problemas y se pueden extraer usando el filtro siguiente en el comando **SSL del acelerador de las estadísticas de la demostración**:

```
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 **optimizado conexión SSL de las estadísticas de la demostración** de controlar que el dispositivo WAAS está estableciendo las conexiones SSL optimizadas. Verifique que “TDLS” aparezca en la columna de Accel para una conexión. “S” indica que el SSL AO fue utilizado como sigue:

```
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"
```

Usted puede controlar las estadísticas de conexión para saber si hay conexiones cerradas usando el comando **cerrado conexión SSL de las estadísticas de la demostración**.

Si las conexiones no están consiguiendo optimizadas, controle si WCCP/PBR es configurado

correctamente y de trabajo, y comprobación para saber si hay enrutamiento asimétrico.

Usted puede ver las estadísticas de la conexión SSL usando el **comando detail optimizado conexión SSL de las estadísticas de la demostración**, donde usted verá la directiva dinámica esa los resultados del servicio acelerado configurado SSL. **Note**: La directiva configurada es optimización TFO solamente, pero la optimización completa es aplicada como resultado del servicio configurado SSL.

```
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 esta salida, se muestran los detalles extendidos del nivel de la sesión SSL como sigue:

```
. . .
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
```

Resolver problemas HTTP AO a las conexiones de las manos SSL AO

Si un cliente debe pasar con un proxy alcanzar a un servidor HTTPS, la petición del cliente primero va como mensaje CONNECT HTTP al proxy (con la dirección IP real del servidor HTTPS integrada en el mensaje CONNECT). A este punto, el HTTP AO maneja esta conexión en el par WAEs. El proxy crea un túnel entre el puerto del cliente y servidor y retransmite los datos subsiguientes entre el cliente y esa dirección IP del servidor y puerto. El proxy responde de nuevo al cliente con “200” mensaje y manos ACEPTABLES de la conexión al SSL AO porque el cliente se prepone hablar con el servidor sobre el SSL. El cliente entonces inicia un contacto SSL con el servidor SSL sobre la conexión TCP (túnel) que fue puesta por el proxy.

Controle las cosas siguientes al resolver problemas los problemas con las conexiones dadas-apagado:

- Controle la salida del comando **HTTP del acelerador de las estadísticas de la demostración**

de confirmar que una conexión fue manejada por el HTTP AO y después dada apagado al SSL AO. Mire las conexiones manejadas totales y las conexiones totales dadas-apagado a los contadores SSL. Si hay algunos problemas, verifique el siguiente:
    - El HTTP AO se activa y en el estado de ejecución en el par WAEs.
    - Configuran al servicio acelerado SSL con el puerto usado por el cliente en la CONEXIÓN URL (o el puerto implicado 443 si se está utilizando el HTTPS). El puerto del proxy es a menudo diferente del puerto de la CONEXIÓN URL y este puerto del proxy no se debe configurar en el servicio acelerado SSL. Sin embargo, el puerto del proxy se debe incluir en el clasificador del tráfico que se asocia al HTTP AO.
- Controle la salida del comando **HTTP del acelerador de las estadísticas de la demostración** de confirmar que esta conexión fue manejada y optimizada por el SSL AO. Mire las conexiones manejadas totales y sume los contadores optimizados de las conexiones. Si los contadores de las estadísticas no están correctos, realice el troubleshooting básico SSL como se debate en la sección anterior.
- En el centro de datos WAE, verifique que la salida **optimizada conexión del comando detail de las estadísticas de la demostración** muestre el hostname del servidor SSL real, la dirección IP, y el puerto TCP. Si estos campos no se fijan correctamente, controle el siguiente:
    - Verifique que las configuraciones de representación del buscador del cliente estén correctas.
    - Verifique que el servidor DNS esté configurado en el centro de datos WAE y sea accesible. Usted puede configurar un servidor DNS en el WAE con el ***comando a.b.c.d del Servidor de nombres IP***.

Resolver problemas la verificación del certificado de servidor

La verificación del certificado de servidor requiere que usted importe el certificado CA correcto al centro de datos WAE.

Para resolver problemas la verificación del certificado de servidor siga los siguientes pasos:

1. Examine el certificado de servidor y extraiga el nombre del emisor. Este nombre del emisor dentro del certificado de servidor debe hacer juego el asunto dentro del certificado CA que corresponde con. Si usted tiene Certificados codificados PEM, usted puede utilizar el comando siguiente del **openssl** en un servidor con el openssl instalado:

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

2. Asegúrese de que la configuración crypto del pki que corresponde con Ca exista en el centro de datos WAE usando el **comando show running-config**. Para que un certificado CA sea utilizado por el WAE en el proceso de verificación, un item de configuración crypto del pki Ca se requiere para cada certificado CA importado. Por ejemplo, si se importa un certificado CA company1.ca, después la configuración siguiente se debe hacer en el centro de datos WAE:

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

Nota: Si un certificado CA se importa usando el GUI central del encargado, el encargado central agrega automáticamente la configuración crypto antedicha del pki Ca para incluir el certificado CA importado. Sin embargo, si el certificado CA se importa vía el CLI, después usted necesitará agregar manualmente la configuración antedicha.

3. Si el certificado que es verificado incluye una Cadena de certificados, después asegúrese de que la Cadena de certificados sea coherente, y el certificado CA del emisor superior se importa en el WAE. Utilice el **comando verify del openssl** de verificar el certificado por separado primero.

4. Si la verificación todavía falla, después examine el registro de la depuración del acelerador SSL. Utilice los comandos siguientes de activar el registro de debug:

```
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 después examine el archivo del registro de /local/local1/errorlog/sslao-errorlog.current. Este fichero debe indicar el nombre del emisor que fue incluido en el certificado de servidor. Asegúrese de que este nombre del emisor haga juego exactamente el asunto del certificado CA.

Si hay algunos otros errores internos en los registros, puede ser útil activar las opciones adicionales de la depuración.

6. Incluso si el nombre del emisor y los asuntos hacen juego, el certificado CA puede no ser el correcto. En estos casos, si el certificado de servidor es publicado por un CA bien conocido, después un navegador puede ser utilizado a directamente (sin WAAS) alcanza el servidor. Cuando el navegador puso la conexión, el certificado puede ser examinado haciendo clic el icono del bloqueo que aparece en el abajo a la derecha de la ventana del buscador o dentro de la barra de dirección del navegador. Los detalles del certificado pueden indicar el certificado CA apropiado que corresponde con este certificado de servidor. Controle el campo del número de serie dentro del certificado CA. Este número de serie debe hacer juego el número de serie del certificado que se está importando en el centro de datos WAE.

7. Si usted hace controlar de la revocación OCSP activar, inhabilitelo y controle que la verificación del certificado en sí mismo trabaja. Para la ayuda que resuelve problemas las configuraciones OCSP vea “resolver problemas la revocación OCSP que controla” la sección.

Resolver problemas la verificación del certificado del cliente

La verificación del certificado del cliente se puede activar en el servidor de origen y/o en el centro de datos WAE. Cuando WAAS se utiliza para acelerar el tráfico SSL, el certificado del cliente recibido por el servidor de origen es el certificado indicado en la máquina-CERT-clave especificada en los **servicios crypto SSL que las configuraciones globales** ordenan en el centro de datos WAE o el certificado firmado del uno mismo de la máquina del centro de datos WAE, si la máquina-CERT-clave no se configura. Como consecuencia, si la verificación del certificado del cliente está fallando en el servidor de origen, puede ser porque el certificado de la máquina del centro de datos WAE no es comprobable en el servidor de origen.

Si la verificación del certificado del cliente en el centro de datos WAE no está trabajando, es probable porque el certificado CA que corresponde con el certificado del cliente no se importa en el centro de datos WAE. Vea “la sección de la verificación del certificado de servidor del troubleshooting” para las instrucciones cómo controlar si usted tiene el certificado CA correcto importado en el WAE.

Resolver problemas la verificación del certificado del par WAE

Para resolver problemas los problemas de la verificación del certificado de peer siga los siguientes pasos:

1. Verifique que el certificado que es verificado sea un certificado firmado CA. Un certificado firmado del uno mismo por un WAE no es comprobable por otro WAE. WAEs por abandono se carga con los certificados firmados del uno mismo. Un certificado firmado del uno mismo se debe configurar usando el comando **crypto de la máquina-CERT-clave de las configuraciones globales de los servicios SSL**.

2. Verifique que el certificado CA correcto esté cargado en el dispositivo que está verificando el certificado. Por ejemplo, si par-CERT-verifique se configura en el centro de datos WAE, después él es esencial para que el certificado de la bifurcación WAE Ca-sea firmado y el mismo certificado Ca de firma se debe importar en el centro de datos WAE. No olvide crear un CA usando el comando **crypto del pki Ca** de utilizar el certificado importado, si usted está importando el certificado manualmente con el CLI. Cuando es importado por el GUI central del encargado, el encargado central crea automáticamente una configuración crypto del pki que corresponde con Ca.

3. Si la verificación del par WAE todavía falla, controle los registros de la depuración según lo descrito en [“la](#) sección del [registro SSL AO”](#).

Resolver problemas controlar de la revocación OCSP

Si el sistema está teniendo problema que hace las conexiones SSL acertadas con controlar en línea de la revocación del protocolo status del certificado (OCSP) activado, siga estos pasos de troubleshooting:

1. Asegúrese de que el servicio del respondedor OCSP se esté ejecutando en el servidor del respondedor.
2. Asegure la buena Conectividad entre el WAE y el respondedor. Utilice el **ping** y los **comandos telnet** (al puerto apropiado) del WAE de controlar.
3. Confirme que el certificado que es validado es de hecho válido. La fecha de vencimiento y el respondedor correcto URL son típicamente áreas donde hay problemas.
4. Verifique que el certificado para las respuestas OCSP esté importado en el WAE. Las respuestas de un respondedor OCSP también se firman y el certificado CA que corresponde con las respuestas OCSP debe residir en el WAE.
5. Controle la salida del comando **SSL del acelerador de las estadísticas de la demostración** para controlar para saber si hay estadísticas OCSP y para controlar los contadores correspondiente a los errores OCSP.
6. Si la conexión OCSP HTTP está pasando con un proxy de HTTP, intente inhabilitar el proxy para ver si ayuda. Si ayuda, después controle que la configuración de representación no está causando el error de la conexión. Si la configuración de representación está muy bien, después puede haber una cierta encabezado HTTP particularidad que puede causar una cierta incompatibilidad con el proxy. Capture un rastro del paquete para la investigación adicional.
7. Si todo falla, usted puede tener que capturar un rastro del paquete del pedido saliente OCSP el depuración adicional. Usted puede utilizar el **tcpdump** o los comandos **tethereal** según lo descrito en la sección [“que captura y que analiza los paquetes”](#) en el artículo preliminar del

troubleshooting WAAS.

El URL usado por el centro de datos WAE para alcanzar a un respondedor OCSP se deriva en una de dos maneras:

- El OCSP estático URL configurado por el comando configuration **crypto de las configuraciones globales del pki**
- El OCSP URL especificado en el certificado que es controlado

Si el URL se deriva del certificado que es controlado, después es esencial asegurarse de que el URL es accesible. Permita a los registros de la depuración del acelerador OCSP SSL determinar el URL y después controlar para saber si hay Conectividad al respondedor. Vea la siguiente sección para los detalles en usar los registros de la depuración.

Resolver problemas la Configuración de DNS

Si el sistema está teniendo conexiones SSL óptimas del problema con las configuraciones del nombre y del dominio del servidor de servidor, siga estos pasos de troubleshooting:

1. Asegúrese de que el servidor DNS configurado en el WAE sea accesible y pueda resolver los nombres. Utilice el comando siguiente de controlar 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 el nombre no se puede resolver por los Servidores de nombres configurados.

Intente el ping/el traceoute para que los Servidores de nombres configurados controlen su reachability 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 los nombres y todavía las conexiones SSL no están consiguiendo optimizadas, asegúrese de que el servicio acelerado que configura el dominio especificado o el hostname sea activo y no hay alarmas para el SSL AO. Utilice después de los 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_inactive” es una indicación que hay una cierta discrepancia en la configuración del servicio acelerado y pudo haber uno o más servicios acelerados que tenían configuración que solapaba para las Entradas de servidor. Controle la configuración del servicio acelerado y asegúrese de que la configuración está correcta. Utilice el comando siguiente de 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 controlar los detalles sobre un servicio acelerado determinado utilizan el comando siguiente:

```
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 razón que el estado operacional del servicio acelerado pudo estar INACTIVO es un error de DNS. Por ejemplo, si hay un hostname del servidor en la configuración del servicio acelerado y el WAE no puede resolver la dirección IP del servidor, después no puede configurar la directiva dinámica apropiada.

3. Si las estadísticas contradicen para “Tubo-por debido al Domain Name no-que corresponde con” están aumentando, él son una indicación que la conexión SSL está para un servidor que se configure para la optimización. Controle las entradas del motor de directivas usando el comando siguiente:

```
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
```

Controle el estado de la conexión que usa el **comando connection de las estadísticas de la demostración**. La primera conexión debe mostrar un acelerador de TSGDL y las conexiones subsiguientes, hasta que el curso de la vida de la entrada de política TIME_DENY, deben ser TDL.

4. Si el servidor DNS está a través de WAN en cuanto al centro de datos WAE, o si el tiempo reverso de la respuesta de DNS es demasiado largo, después algunas conexiones pueden ser caídas. Esto depende del tiempo de espera agotado del cliente y del tiempo de respuesta del rDNS. En este caso, el contador para el “número de búsquedas de DNS reversibles canceladas” aumenta y se cae la conexión. Esta situación es una indicación que el servidor DNS no es responsivo o muy lento y/o NSCD en WAAS no está trabajando. El estatus NSCD se puede controlar usando el **comando show alarms**. La probabilidad de esto que sucede es muy baja puesto que en la mayoría de las implementaciones, se espera que el servidor DNS esté en el mismo LAN que el centro de datos WAE.

Resolver problemas el HTTP al encadenamiento SSL AO

NOTA: El HTTP al encadenamiento SSL AO fue introducido en la versión 4.3.1 WAAS. Esta sección es no corresponde a versiones anteriores WAAS.

El encadenamiento permite que un AO inserte otro AO en cualquier momento durante el curso de la vida de un flujo y ambo el AOs puede aplicar su optimización AO-específica independientemente en el flujo. El encadenamiento AO es diferente de la característica de las manos AO proporcionada por WAAS en las versiones pre-4.3.1 porque con el AO el encadenamiento del primer AO continúa optimizando el flujo.

El SSL AO maneja dos tipos de conexión:

- Byte-0 SSL: El SSL AO recibe la conexión primero y completa el contacto SSL. Analiza a la parte de inicial el payload para controlar para saber si hay un método HTTP. Si el payload indica el HTTP, inserta el HTTP AO; si no, aplica la optimización regular TSDL.
- El proxy CONECTA: El HTTP AO recibe la conexión primero. Identifica el método de la encabezado de la CONEXIÓN en la petición del cliente e inserta el SSL AO después de que el proxy confirme con un mensaje de 200 AUTORIZACIONES.

El SSL AO utiliza un analizador de sintaxis ligero HTTP que detecte los métodos siguientes HTTP: CONSIGA, DIRIJA, FIJE, PONGA, las OPCIONES, RASTRO, COPIA, BLOQUEO, ENCUESTA, BCOPY, BMOVE, MKCOL, CANCELACIÓN, BÚSQUEDA, DESBLOQUEE, BDELETE, PROPFIND, BPROPFIND, PROPPATCH, SUSCRIBA, BPROPPATCH, DÉSE DE BAJA, y X__MS_ENUMATTS. Usted puede utilizar el comando del **analizador de sintaxis SSL del acelerador de la depuración** de poner a punto los problemas relacionados con el analizador de sintaxis. Usted puede utilizar el **HTTP del payload SSL del accel stat de la demostración/el otro** comando de ver las estadísticas del tráfico clasificadas sobre la base del tipo de carga útil.

Extremidades de troubleshooting:

1. Asegúrese de que la característica HTTPS esté activada en la configuración HTTP AO mientras que esto es poseída por el HTTP AO. Para los detalles, vea el troubleshooting el

artículo HTTP AO.

2. Controle al estado de la conexión que usa el **comando connection stat de la demostración**. Si está optimizado correctamente, debe mostrar THSDL que indica la optimización TCP, HTTP, SSL y DRE-LZ. Si ninguno de estos optimizaciones faltan, ponga a punto más lejos en ese optimizador (SSL, HTTP, y así sucesivamente). Por ejemplo, si el estado de la conexión muestra THDL, significa que optimización SSL no fue aplicado en la conexión. Los detalles en los problemas del depuración relacionados con el SSL AO siguen.
3. Asegúrese de que el SSL AO esté activado y que esté en el estado de ejecución (véase la sección el "resolver problemas del 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, el hostname, o el Domain Name y el número del puerto del servidor esté agregada como parte del servicio acelerado.
6. Asegúrese de que el servicio acelerado esté en el estado ACTIVO usando el comando **crypto del ASVC-*nombre del* servicio acelerado de los servicios SSL de la demostración** (véase "la sección de la Configuración de DNS del troubleshooting").
7. Asegúrese de que el motor de directivas tenga una entrada para este servidor y puerto usando el **comando dynamic de la aplicación del motor de directivas de la demostración**.
8. Si el servidor de destino está utilizando el SSL en un puerto del no-valor por defecto (el valor por defecto es 443), asegúrese de que esto esté reflejada en la configuración del motor de directivas. El encargado central confía en esta información para señalar los datos del tráfico SSL.
9. Asegúrese de las resoluciones configuradas del hostname a una dirección IP válida usando el comando **crypto del ASVC-*nombre del* servicio acelerado de los servicios SSL de la demostración**. Si no se encuentra ninguna dirección IP, controle si configuran al Servidor de nombres correctamente. También controle la salida del ***comando ip-address del dnslookup***.

```
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 SSL AO

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

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

Para un depuración más fácil, usted debe primero poner un 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 activar el registro de transacciones, utilice el comando configuration de los **registros de transacciones** como sigue:

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

Usted puede ver el extremo de un archivo de registro de transacción usando el comando del tipo-**Tail** como sigue:

```
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 poner y para activar el registro de debug del SSL AO, utilice los comandos siguientes.

NOTA: El registro de debug es uso intensivo de la CPU y puede generar una gran cantidad de salida. Utilícelo juicioso y escasamente en un entorno de producción.

Usted puede activar el registro detallado al disco como sigue:

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

Usted puede activar el registro de debug para las conexiones en el ACL como sigue:

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

Las opciones para el depuración SSL AO son como sigue:

```
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
```

Usted puede activar el registro de debug para las conexiones SSL y después visualizar el extremo del registro de error de la depuración como sigue:

```
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
```

Resolver problemas las alarmas del vencimiento del certificado en los módulos NME y SRE

Ha expirado El SSL AO genera las alarmas cuando el certificado de la máquina uno mismo-firmado (o es en el plazo de 30 días de expiración) y un certificado de la máquina global de

encargo no se configura en el dispositivo WAAS. El software WAAS genera los certificados autofirmados de la fábrica con una fecha de caducidad de 5 años del primer lanzamiento del dispositivo WAAS.

El reloj en todos los módulos WAAS NME y SRE se fija a 1 de enero de 2006 durante el primer lanzamiento, aunque el módulo NME o SRE es más reciente. Esto hace el certificado autofirmado expirar el 1 de enero de 2011 y el dispositivo genera las alarmas de la expiración del certificado.

Si usted no está utilizando el certificado de la predeterminada de fábrica como el certificado global, y en lugar de otro está utilizando un certificado de encargo para el SSL AO, usted no experimentará esta expiración inesperada y usted puede poner al día el certificado de encargo siempre que expire. También, si usted ha puesto al día el módulo NME o PME con una nueva imagen del software y ha sincronizado el reloj a una fecha más reciente, usted no puede experimentar este problema.

El síntoma de la expiración del certificado es una de las alarmas siguientes (mostradas aquí en la salida del comando show alarms):

```
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
```

or

```
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
```

El GUI del encargado de la central señala la alarma siguiente: "Certificate__waas-self__.p12 es expiración cercana que se configura como CERT de la máquina en configuraciones globales”

Usted puede utilizar una de las soluciones siguientes para resolver este problema:

- Configure un diverso certificado para las configuraciones globales:

```
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
```

- Ponga al día el certificado uno mismo-firmado de la fábrica con una fecha de caducidad posterior. Esta solución requiere un script que usted pueda obtener por el TAC de Cisco que entra en contacto con.

NOTE: Este problema es fijado por la resolución de la advertencia CSCte05426, release/versión en las versiones de software 4.1.7b, 4.2.3c, y 4.3.3 WAAS. La fecha de caducidad de la certificación se cambia a 2037.