WAAS - Identificação e solução de problemas do SSL AO

Capítulo: Troubleshooting de SSL AO

Este artigo descreve como solucionar problemas do SSL AO.

Co

Art
En
trá
So
Oti
Tro
Tro
Tro
Tro
Tro
Tro
Tro
So
Tro
Tro
Tro
So
So
So
So
So
Tro

Contents

Visão geral do SSL Accelerator

O acelerador SSL (disponível na versão 4.1.3 e posterior) otimiza o tráfego criptografado de SSL

(Secure Sockets Layer) e TLS (Transport Layer Security). O acelerador SSL fornece criptografia e descriptografia de tráfego no WAAS para permitir a otimização de tráfego de ponta a ponta. O acelerador SSL também fornece gerenciamento seguro de certificados e chaves de criptografia.

Em uma rede WAAS, o WAE do data center atua como um nó intermediário confiável para solicitações SSL pelo cliente. A chave privada e o certificado do servidor são armazenados no WAE do data center. O WAE do data center participa do handshake SSL para derivar a chave da sessão, que distribui com segurança na banda para o WAE da filial, permitindo que o WAE da filial descriptografe o tráfego do cliente, otimize-o, recriptografe-o e envie-o pela WAN para o WAE do data center. O WAE do data center mantém uma sessão SSL separada com o servidor de origem.

Os seguintes serviços são relevantes para a otimização de SSL/TLS:

- Serviço acelerado - uma entidade de configuração que descreve as características de aceleração a serem aplicadas a um servidor SSL ou conjunto de servidores. Especifica o certificado e a chave privada a serem usados durante a criação como um intermediário confiável, cifras a serem usadas, versão SSL permitida e configurações de verificação de certificado.
- Peering Service - uma entidade de configuração que descreve as características de aceleração a serem aplicadas para conexões SSL em banda entre WAEs de filial e data center. Esse serviço é usado para transferir informações chave da sessão do data center para os WAEs da filial para otimizar conexões SSL.
- Central Manager Admin Service - Não usado diretamente pelo acelerador SSL, mas para ser usado por um administrador para o gerenciamento de configuração de serviços acelerados SSL. Também usado para carregar certificados e chaves privadas a serem usados em serviços acelerados por SSL.
- Central Manager Management Service - Não usado diretamente pelo acelerador SSL, mas usado para comunicação entre dispositivos do acelerador de aplicativos e o Central Manager. Esse serviço é usado para gerenciamento de configuração, recuperação de chave de criptografia de armazenamento seguro e atualizações de status de dispositivo.

O armazenamento seguro do Central Manager é essencial para que o SSL AO opere porque ele armazena chaves de criptografia seguras para todos os WAEs. Após cada recarregamento do Central Manager, o administrador precisa reabrir o armazenamento seguro fornecendo a senha com o comando **cms secure-store open**. Um WAE recupera automaticamente sua chave de criptografia de armazenamento seguro do Central Manager sempre que o WAE é reinicializado, portanto nenhuma ação é necessária no WAE após um recarregamento.

Se os clientes estiverem usando uma solução de proxy HTTP, a conexão inicial será tratada pelo HTTP AO, que a reconhece como uma solicitação de túnel SSL para a porta 443. O HTTP AO procura um serviço acelerado SSL correspondente definido no WAE do data center e quando ele encontra uma correspondência, transfere a conexão para o SSL AO. No entanto, o tráfego que o HTTP AO entrega ao SSL AO para um proxy HTTPS é relatado como parte das estatísticas do aplicativo Web, não no aplicativo SSL. Se o HTTP AO não encontrar uma correspondência, a conexão será otimizada de acordo com a configuração da política de HTTPS (SSL) estática.

O SSL AO pode usar certificados autoassinados em vez de certificados assinados por CA, o que pode ser útil na implantação de sistemas de prova de conceito (POC) e na solução de problemas de SSL. Usando certificados autoassinados, você pode implantar rapidamente um sistema WAAS sem precisar importar os certificados do servidor de origem e pode eliminar os certificados como uma fonte potencial de problemas. Você pode configurar um certificado autoassinado no Central

Manager ao criar um serviço SSL Accelerated. No entanto, quando utilizar um certificado autoassinado, o browser do cliente irá apresentar um alerta de segurança de que o certificado não é fidedigno (porque não está assinado por uma AC bem conhecida). Para evitar este aviso de segurança, instale o certificado no arquivo de Autoridades de Certificação de Raiz Confiáveis no navegador do cliente. (No Internet Explorer, no aviso de segurança, clique em **Exibir certificado** e, na caixa de diálogo Certificado, clique em **Instalar certificado** e conclua o Assistente de importação de certificado.)

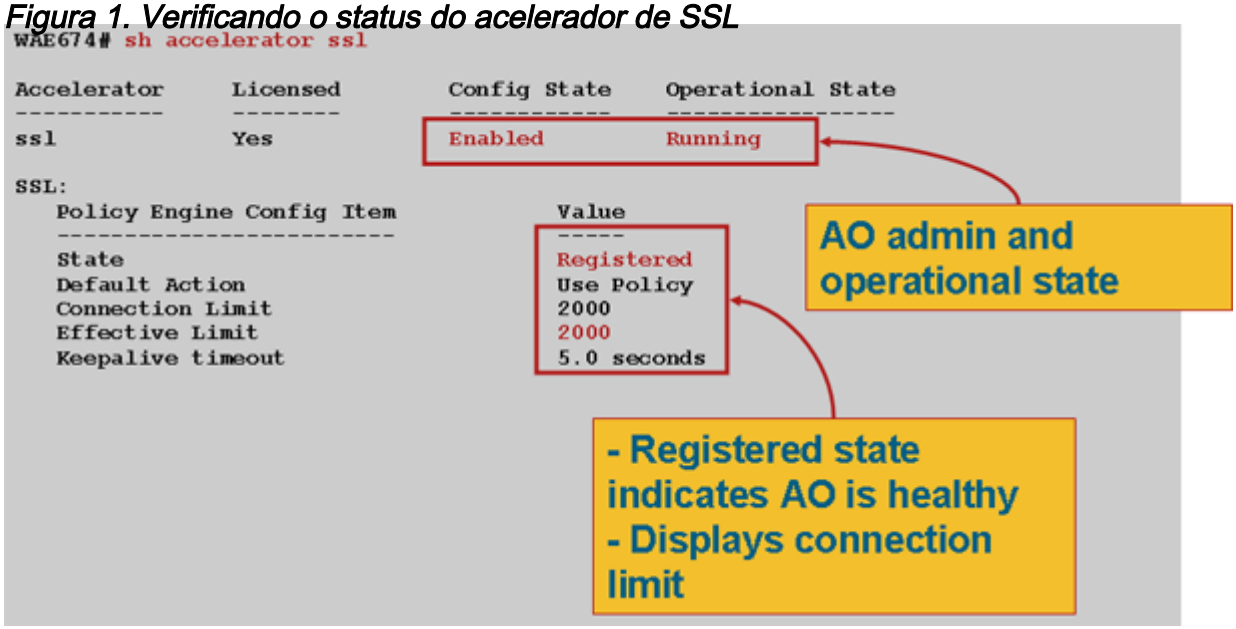
A configuração dos Serviços de Gerenciamento SSL é opcional e permite que você altere a versão SSL e a lista de cifras usadas para comunicações do Central Manager para WAEs e para o navegador (para acesso administrativo). Se você configurar cifras que não são suportadas pelo seu navegador, perderá a conexão com o Central Manager. Nesse caso, use o comando de configuração **crypto ssl management-service** da CLI para definir as configurações do serviço de gerenciamento SSL de volta ao padrão.

Troubleshooting de SSL AO

Você pode verificar a configuração e o status gerais do AO com os comandos **show accelerator** e **show license**, conforme descrito no artigo Troubleshooting Application Acceleration. A licença Enterprise é necessária para a operação do acelerador SSL.

Em seguida, verifique o status específico do SSL AO no data center e nos WAEs da filial usando o comando **show accelerator ssl**, como mostrado na Figura 1. Você deseja ver que SSL AO está Habilitado, em Execução e Registrado e que o limite de conexão é exibido. Se o estado de configuração estiver ativado, mas o estado operacional estiver desativado, isso indica um problema de licenciamento. Se o estado operacional estiver desativado, pode ser porque o WAE não pode recuperar as chaves SSL do repositório seguro do Central Manager, porque o armazenamento seguro não está aberto ou o Central Manager não pode ser alcançado. Use os comandos **show cms info** e **ping** para confirmar se o Central Manager está acessível.

Figura 1. Verificando o status do acelerador de SSL



Se você vir um estado operacional de Gen Crypto Params, aguarde até que o status se torne em execução, o que pode levar alguns minutos após a reinicialização. Se você vir um estado de Recuperação de Chaves do CM por mais de alguns minutos, poderá indicar que o serviço CMS no Central Manager não está em execução, que não há conectividade de rede com o Central Manager, que as versões do WAAS no WAE e no Central Manager são incompatíveis ou que o armazenamento seguro do Central Manager não está aberto.

Você pode verificar se o armazenamento seguro do Central Manager está inicializado e aberto usando o comando **show cms secure-store** da seguinte maneira:

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

Se o armazenamento seguro não for inicializado ou aberto, você verá alarmes críticos como mstore_key_failure e secure-store. Você pode abrir a loja segura com o comando **cms secure-store open** ou, no Central Manager, escolha **Admin > Secure Store**.

Tip: Documente a senha do armazenamento seguro para evitar ter que redefinir o armazenamento seguro se você esquecer a senha.

Se houver um problema com a criptografia de disco em um WAE, isso também pode impedir que o SSL AO opere. Use o comando **show disk details** para verificar se a criptografia de disco está habilitada e verificar se as partições CONTENT e SPOOL estão montadas. Se essas partições forem montadas, isso indica que as chaves de criptografia do disco foram recuperadas com êxito do Central Manager e que os dados criptografados podem ser gravados e lidos dos discos. Se o comando **show disk details** mostrar "O sistema está inicializando", que indica que as chaves de criptografia ainda não foram recuperadas do Central Manager e que os discos ainda não foram montados. O WAE não fornecerá serviços de aceleração neste estado. Se o WAE não puder recuperar chaves de criptografia de disco do Central Manager, ele disparará um alarme.

Você pode verificar se o serviço acelerado SSL está configurado e seu status é "Enabled" (Habilitado) no WAE do data center (no Central Manager, escolha o dispositivo e escolha **Configure > Acceleration > SSL Accelerated Services**). Um serviço acelerado configurado e habilitado pode ser inativo pelo acelerador SSL devido às seguintes condições:

- O certificado configurado no serviço acelerado foi excluído do WAE. Use o comando **show running-config** para determinar o certificado que está sendo usado no serviço acelerado e use os comandos **show crypto certificate** e **show crypto certificate-details** para confirmar se o certificado está presente no armazenamento seguro. Se o certificado estiver faltando, importe-o novamente.
- O certificado de serviço acelerado expirou. Use os comandos **show crypto certificate** e **show crypto certificate-details** para verificar a data de expiração do certificado.
- O certificado de serviço acelerado tem uma data válida que começa no futuro. Use os comandos **show crypto certificate** e **show crypto certificate-details** e verifique a seção de validade da saída do comando. Além disso, certifique-se de que as informações de relógio e fuso horário do WAE estejam corretas.

Você pode verificar se as conexões SSL têm a política correta aplicada, ou seja, têm otimização total com aceleração SSL, como mostrado na Figura 2. No Central Manager, escolha o dispositivo WAE e escolha **Monitor > Otimization > Connections Statistics**.

Figura 2. Verificando a política correta em conexões SSL

Use o comando **show running-config** para verificar se a política de tráfego HTTPS está configurada corretamente. Deseja ver **Otimizar DRE sem compactação nenhuma** para a ação de aplicação SSL e desejar ver as condições de correspondência adequadas listadas para o classificador HTTPS, da seguinte forma:

```
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
```

Um serviço acelerado ativo insere políticas dinâmicas correspondentes ao servidor IP:porta, nome do servidor:porta ou domínio do servidor:porta configurada no serviço acelerado. Essas políticas podem ser inspecionadas usando o comando **show policy-engine application dynamic**. O campo Dst em cada política exibida indica o IP do servidor e a porta que correspondem ao serviço acelerado. Para o domínio curinga (por exemplo, server-domain *.webex.com port 443), o campo Dst será 'Any:443'. Para a configuração do nome do servidor, a pesquisa de encaminhamento de DNS é executada quando o serviço acelerado é ativado e todos os endereços IP retornados na resposta de DNS serão inseridos no mecanismo de política. Esse comando é útil para capturar situações em que um serviço acelerado é marcado como "inservice", mas o serviço acelerado é tornado inativo devido a algum outro erro. Por exemplo, todos os serviços acelerados dependem do serviço de peering e, se o serviço de peering estiver inativo devido a um certificado ausente/excluído, um serviço acelerado também será marcado como inativo, embora pareça estar "em serviço" na saída show running-config. Você pode verificar se a política dinâmica SSL está ativa no WAE do data center usando o comando **show policy-engine application dynamic**. Você pode verificar o status do serviço de peering usando o comando **show crypto ssl services host-service peering**.

Uma configuração de serviço acelerada SSL AO pode ter quatro tipos de entradas de servidor:

- IP estático (server-ip)—disponível na versão 4.1.3 e posterior
- Capturar tudo (server-ip any)—disponível na versão 4.1.7 e posterior

- Nome do host (nome do servidor)—disponível na versão 4.2.1 e posterior
- Domínio curinga (domínio do servidor)—disponível na versão 4.2.1 e posterior

Quando a conexão é recebida pelo SSL AO, ele decide qual serviço acelerado deve ser usado para otimização. A configuração de IP estático recebe a maior preferência, seguida pelo nome do servidor, domínio do servidor e, em seguida, pelo ip any do servidor. Se nenhum dos serviços acelerados configurados e ativados corresponder ao IP do servidor para a conexão, a conexão será enviada para o AO genérico. O cookie inserido no mecanismo de política pelo SSL AO é usado para determinar qual serviço acelerado e que tipo de entrada de servidor corresponde para uma conexão específica. Este cookie de mecanismo de política é um número de 32 bits e é significativo somente para o SSL AO. Os bits mais altos são usados para indicar diferentes tipos de entrada de servidor e os bits mais baixos indicam o índice de serviço acelerado, como a seguir:

Valores de cookies do SSL Policy Engine

Valor do cookie	Tipo de entrada do servidor	Comentários
0x8*xxxxxxx*	Endereço IP do servidor	Configuração de endereço IP estático
0x4*xxxxxxx*	Nome de host do servidor	O WAE do data center executa uma pesquisa de DNS de encaminhamento para o nome do host e adiciona os endereços IP que são retornados à configuração de política dinâmica. Atualizado a cada 10 minutos por padrão.
0x2FFFFFFF	Nome de domínio do servidor	O WAE do data center executa uma pesquisa de DNS reversa no endereço IP do host de destino para determinar se ele corresponde ao domínio. Se ele corresponder, o tráfego SSL será acelerado e, se não corresponder, o tráfego será tratado de acordo com a política HTTPS estática.
0x1*xxxxxxx*	Servidor Qualquer	Todas as conexões SSL são aceleradas usando esta configuração de serviço acelerado

Exemplo 1: Serviço acelerado com configuração server-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
```

A entrada correspondente do mecanismo de política é adicionada da seguinte forma:

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

Exemplo 2: Serviço acelerado com configuração de nome de servidor:

Essa configuração permite fácil implantação para otimização de aplicativos SSL corporativos. Ele é adaptável às alterações de configuração de DNS e reduz as tarefas 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
```

A entrada correspondente do mecanismo de política é adicionada da seguinte forma:

```
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
```

Exemplo 3: Serviço acelerado com configuração de domínio de servidor:

Essa configuração permite que os dispositivos WAAS configurem um único domínio curinga que evita a necessidade de conhecer endereços IP para todos os servidores. O WAE do data center usa DNS reverso (rDNS) para corresponder o tráfego pertencente ao domínio configurado. Configurar um domínio curinga evita configurar vários endereços IP, tornando a solução escalável e aplicável para a arquitetura 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
```

A entrada correspondente do mecanismo de política é adicionada da seguinte forma:

```
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
```

Exemplo 4: Serviço acelerado com configuração server-ip any:

Essa configuração fornece um mecanismo catch-all. Quando um serviço acelerado com **server-ip any port 443** é ativado, ele permite que todas as conexões na porta 443 sejam otimizadas pelo SSL AO. Essa configuração pode ser usada durante POCs para otimizar todo o tráfego em uma porta específica.

```
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
```

A entrada correspondente do mecanismo de política é adicionada da seguinte forma:

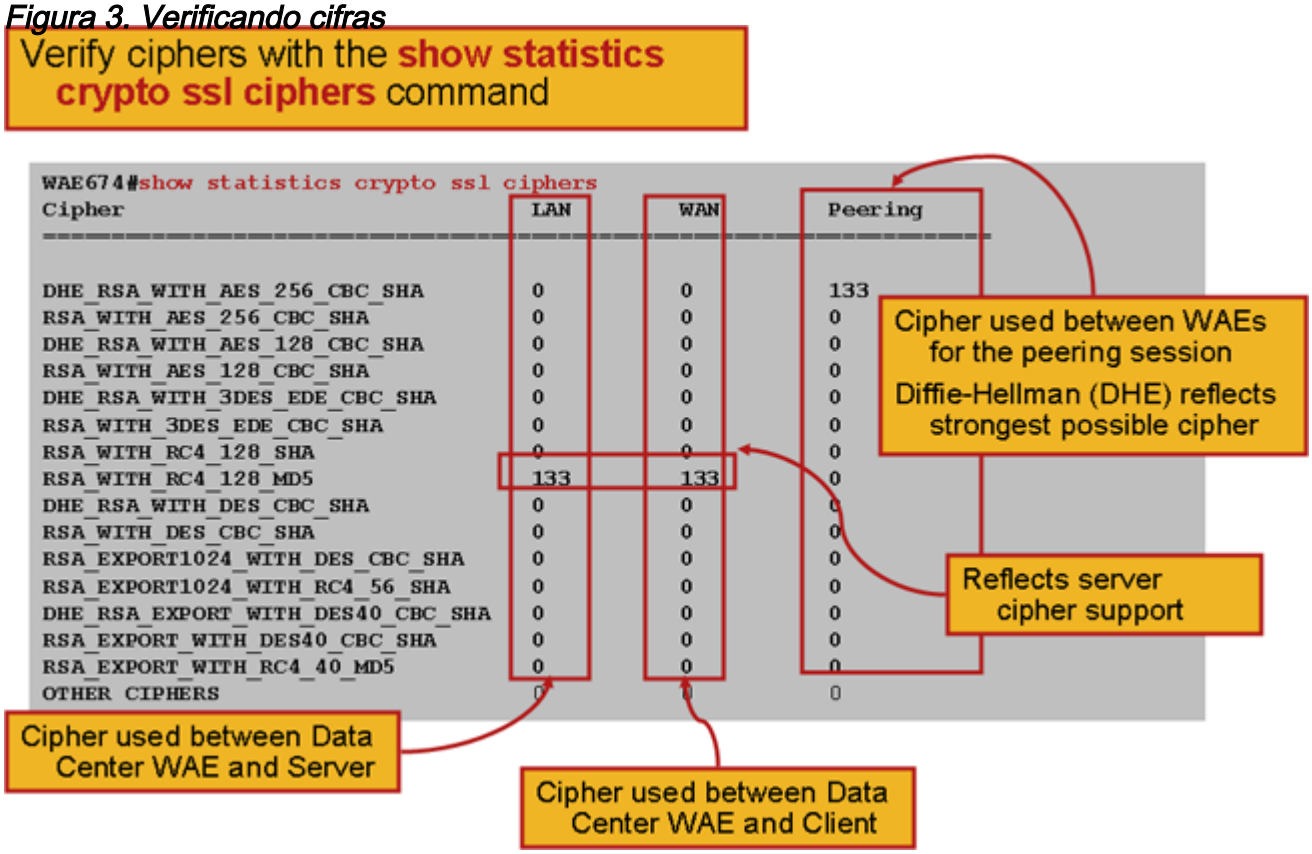
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

Você pode verificar as cifras que estão sendo usadas com os comandos **show statistics crypto ssl ciphers**, como mostrado na Figura 3.

Figura 3. Verificando cifras



Você pode verificar se esses cifras correspondem aos configurados no servidor de origem. **Note**: Os cifras que incluem DHE não são suportados pelos servidores Microsoft IIS.

Em um servidor Apache, você pode verificar a versão SSL e os detalhes da cifra no arquivo httpd.conf. Esses campos também podem estar em um arquivo separado (sslmod.conf) referenciado de httpd.conf. Procure os campos do protocolo SSLP e do conjunto de IPs SSLC da seguinte maneira:

```
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 o emissor do certificado em um servidor Apache, use o comando openssl para ler o certificado da seguinte maneira:

```
> 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
```

No navegador, você pode visualizar um certificado e seus detalhes para determinar a cadeia de certificados, a versão, o tipo de chave de criptografia, o nome comum do emissor (CN) e o CN do assunto/site. No Internet Explorer, clique no ícone de cadeado, clique em **Exibir certificado** e, em seguida, consulte as guias Detalhes e Caminho de certificação para obter essas informações.

A maioria dos navegadores exige que os certificados de cliente estejam no formato PKCS12 em vez do formato PEM X509. Para exportar o formato X509 PEM para o formato PKCS12, use o comando openssl da seguinte forma em um servidor Apache:

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

Se as chaves privadas forem criptografadas, a senha será necessária para exportação. A senha de exportação é usada novamente para importar credenciais para o dispositivo WAAS.

Use o comando **show statistics accelerator ssl** para ver as estatísticas 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              <-------
---------
. . .
```

Sessões com falha e estatísticas de verificação de certificado podem ser úteis para a solução de problemas e são recuperados mais facilmente usando o seguinte filtro no 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
```

As estatísticas relacionadas ao DNS podem ser úteis para a identificação e solução de problemas de nome do servidor e configuração de domínio curinga. Para recuperar essas estatísticas, use o comando **show statistics accelerator ssl**, da seguinte forma:

```
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
 . . .
```

As estatísticas relacionadas ao handshake SSL podem ser úteis para a solução de problemas e podem ser recuperadas usando o seguinte filtro no 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
```

Use o comando **show statistics connection otimized ssl** para verificar se o dispositivo WAAS está estabelecendo conexões SSL otimizadas. Verifique se "TDLS" aparece na coluna Accel para uma conexão. "S" indica que o SSL AO foi usado da seguinte forma:

```
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"
```

Você pode verificar as estatísticas da conexão para conexões fechadas usando o comando **show statistics connection closed ssl**.

Se as conexões não estiverem sendo otimizadas, verifique se o WCCP/PBR está configurado e funcionando corretamente e verifique se há roteamento assimétrico.

Você pode exibir as estatísticas da conexão SSL usando o comando **show statistics connection otimized ssl detail**, onde você verá a política dinâmica resultante do serviço acelerado SSL configurado. **Note**: A política configurada é somente a otimização de TFO, mas a otimização total é aplicada como resultado do serviço 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
. . .
```

Mais adiante nesta saída, os detalhes do nível de sessão SSL estendida são mostrados da seguinte forma:

```
. . .
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
```

Troubleshooting de Conexões de Entrega de HTTP AO para SSL AO

Se um cliente precisar passar por um proxy para acessar um servidor HTTPS, a solicitação do cliente primeiro vai como uma mensagem HTTP CONNECT para o proxy (com o endereço IP do servidor HTTPS real incorporado na mensagem CONNECT). Neste ponto, o HTTP AO lida com essa conexão nos WAEs do peer. O proxy cria um túnel entre a porta do cliente e do servidor e retransmite os dados subsequentes entre o cliente e o endereço IP e a porta desse servidor. O proxy responde ao cliente com uma mensagem "200 OK" e desliga a conexão com o SSL AO porque o cliente pretende falar com o servidor via SSL. Em seguida, o cliente inicia um handshake SSL com o servidor SSL pela conexão TCP (túnel) que foi configurada pelo proxy.

Verifique os seguintes itens ao solucionar problemas com conexões de transferência:

- Verifique a saída do comando **show statistics accelerator http** para confirmar se uma conexão foi tratada pelo HTTP AO e, em seguida, transferida para o SSL AO. Observe o Total de conexões tratadas e Total de conexões transferidas para contadores SSL. Se houver algum problema, verifique o seguinte:
  - O HTTP AO está ativado e no estado em execução nos WAEs do peer.
  - O serviço acelerado SSL é configurado com a porta usada pelo cliente no URL CONNECT (ou a porta implícita 443 se o HTTPS estiver sendo usado). Frequentemente, a porta de proxy é diferente da porta de URL CONNECT e essa porta de proxy não deve ser configurada no serviço acelerado SSL. No entanto, a porta proxy deve ser incluída no classificador de tráfego que é mapeado para o HTTP AO.
- Verifique a saída do comando **show statistics accelerator http** para confirmar se essa conexão foi tratada e otimizada pelo SSL AO. Observe o Total de conexões tratadas e o Total de contadores de conexões otimizadas. Se os contadores de estatísticas não estiverem corretos, execute a solução básica de problemas de SSL conforme discutido na seção anterior.
- No WAE do data center, verifique se a saída do comando **show statistics connection otimized detail** mostra o nome de host, o endereço IP e a porta TCP do servidor SSL real. Se esses campos não estiverem definidos corretamente, verifique o seguinte:
  - Verifique se as configurações de proxy do navegador do cliente estão corretas.
  - Verifique se o servidor DNS está configurado no WAE do data center e está acessível. Você pode configurar um servidor DNS no WAE com o comando **ip name-server** *A.B.C.D* .

Solução de problemas de verificação de certificado do servidor

A verificação do certificado do servidor exige que você importe o certificado CA correto para o WAE do data center.

Para solucionar problemas de verificação de certificado do servidor, siga estas etapas:

1. Inspecione o certificado do servidor e recupere o nome do Emitente. O nome do Emitente no certificado do servidor deve corresponder ao nome do assunto no certificado CA correspondente. Se você tiver certificados codificados PEM, poderá usar o seguinte comando **openssl** em um servidor com openssl instalado:

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

2. Certifique-se de que a configuração correspondente de crypto pki ca existe no WAE do data center usando o comando **show running-config**. Para que um certificado CA seja usado pelo WAE no processo de verificação, um item de configuração crypto pki ca é necessário para cada certificado CA importado. Por exemplo, se uma CA certificate company1.ca for importada, a seguinte configuração deve ser feita no WAE do data center:

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

Note: Se um certificado CA for importado usando a GUI do Central Manager, o Central Manager adicionará automaticamente a configuração do crypto pki ca acima para incluir o certificado CA importado. No entanto, se o certificado CA for importado via CLI, você precisará adicionar manualmente a configuração acima.

3. Se o certificado que está sendo verificado incluir uma cadeia de certificados, assegure-se de que a cadeia de certificados seja coerente e que o certificado CA mais importante do emitente seja importado no WAE. Use o comando **openssl verify** para verificar o certificado separadamente primeiro.

4. Se a verificação ainda falhar, examine o log de depuração do acelerador SSL. Use os seguintes comandos para ativar o registro de depuração:

```
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 uma conexão de teste e examine o arquivo de log /local/local1/errorlog/sslao-errorlog.current. Esse arquivo deve indicar o nome do emissor que foi incluído no certificado do servidor. Certifique-se de que este nome do emissor corresponde exatamente ao nome do requerente do certificado CA.

Se houver qualquer outro erro interno nos registros, pode ser útil habilitar outras opções de depuração.

6. Mesmo se o nome do Emitente e o nome do Assunto coincidirem, o certificado CA pode não ser o correto. Nesses casos, se o certificado do servidor for emitido por uma CA bem conhecida, um navegador poderá ser usado para acessar diretamente (sem WAAS) o servidor. Quando o navegador configura a conexão, o certificado pode ser examinado clicando no ícone Bloquear exibido na parte inferior direita da janela do navegador ou na barra de endereços do navegador. Os detalhes do certificado podem indicar o certificado CA adequado correspondente a este certificado de servidor. Verifique o campo Número de série no certificado CA. Esse número de série deve corresponder ao número de série do certificado que está sendo importado no WAE do data center.

7. Se você tiver a verificação de revogação de OCSP habilitada, desative-a e verifique se a verificação de certificado por si só funciona. Para obter ajuda na solução de problemas de

configurações de OCSP, consulte a seção "Troubleshooting OCSP Revocation Checking".

Solução de problemas de verificação de certificado do cliente

A verificação do certificado do cliente pode ser habilitada no servidor de origem e/ou no WAE do data center. Quando o WAAS é usado para acelerar o tráfego SSL, o certificado do cliente recebido pelo servidor de origem é o certificado indicado na chave de certificado da máquina especificada no comando **crypto ssl services global-settings** no WAE do data center ou no certificado autoassinado da máquina WAE do data center, se a chave de certificado da máquina não estiver configurada. Como resultado, se a verificação do certificado do cliente estiver falhando no servidor de origem, pode ser porque o certificado da máquina WAE do data center não é verificável no servidor de origem.

Se a verificação do certificado do cliente no WAE do data center não estiver funcionando, é provável que o certificado CA correspondente ao certificado do cliente não seja importado no WAE do data center. Consulte a seção "Solução de problemas de verificação de certificado do servidor" para obter instruções sobre como verificar se o certificado CA correto foi importado no WAE.

Troubleshooting de Verificação de Certificado WAE Par

Para solucionar problemas de verificação de certificado de peer, siga estas etapas:

1. Verifique se o certificado que está sendo verificado é um certificado assinado pela CA. Um certificado autoassinado por um WAE não pode ser verificado por outro WAE. Por padrão, os WAEs são carregados com certificados autoassinados. Um certificado autoassinado deve ser configurado usando o comando **crypto ssl services global-settings machine-cert-key**.

2. Verifique se o certificado CA correto está carregado no dispositivo que está verificando o certificado. Por exemplo, se peer-cert-verify estiver configurado no WAE do data center, é essencial que o certificado WAE da filial seja assinado pela autoridade de certificação e o mesmo certificado da autoridade de certificação assinado seja importado no WAE do data center. Não se esqueça de criar uma CA usando o comando **crypto pki ca** para usar o certificado importado, se você estiver importando o certificado manualmente através da CLI. Quando importado pela GUI do Central Manager, o Central Manager cria automaticamente uma configuração de crypto pki ca correspondente.

3. Se a verificação do peer WAE ainda falhar, verifique os logs de depuração conforme descrito na seção "SSL AO Logging".

Troubleshooting de Verificação de Revogação de OCSP

Se o sistema tiver problemas para fazer conexões SSL bem-sucedidas com a verificação de revogação do Protocolo de Status do Certificado Online (OCSP) ativada, siga estas etapas de solução de problemas:

1. Verifique se o serviço de respondente OCSP está em execução no servidor de respondente.
2. Garanta uma boa conectividade entre o WAE e o respondedor. Use os comandos **ping** e **telnet** (para a porta apropriada) do WAE para verificar.
3. Confirme se o certificado validado é realmente válido. A data de expiração e a URL do respondente correta são geralmente áreas onde há problemas.
4. Verifique se o certificado para respostas OCSP é importado no WAE. As respostas de um respondente OCSP também são assinadas e o certificado CA correspondente às respostas

OCSP deve residir no WAE.

5. Verifique a saída do comando **show statistics accelerator ssl** para verificar as estatísticas de OCSP e verificar os contadores correspondentes às falhas de OCSP.
6. Se a conexão HTTP do OCSP estiver passando por um proxy HTTP, tente desabilitar o proxy para ver se ele ajuda. Se isso ajudar, verifique se a configuração do proxy não está causando a falha de conexão. Se a configuração de proxy estiver correta, pode haver alguma peculiaridade do cabeçalho HTTP que pode estar causando alguma incompatibilidade com o proxy. Capturar um rastreamento de pacote para investigação posterior.
7. Se tudo o mais falhar, talvez seja necessário capturar um rastreamento de pacote da solicitação de OCSP de saída para mais depuração. Você pode usar os comandos **tcpdump** ou **tethereal** conforme descrito na seção "Capturando e Analisando Pacotes" no artigo Preliminar Solução de Problemas do WAAS.

O URL usado pelo WAE do data center para acessar um respondente OCSP é derivado de uma das duas maneiras:

- A URL de OCSP estática configurada pelo comando de configuração **crypto pki global-settings**
- O URL do OCSP especificado no certificado que está sendo verificado

Se o URL derivar do certificado que está sendo verificado, então é essencial garantir que o URL esteja acessível. Ative os registros de depuração do OCSP do acelerador SSL para determinar a URL e verificar a conectividade com o respondente. Consulte a próxima seção para obter detalhes sobre como usar logs de depuração.

Solução de problemas de configuração de DNS

Se o sistema tiver problemas para otimizar as conexões SSL com o nome do servidor e as configurações de domínio do servidor, siga estas etapas de solução de problemas:

1. Certifique-se de que o servidor DNS configurado no WAE esteja acessível e possa resolver nomes. Use o seguinte comando para verificar o 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 !
```

Essa resposta indica que o nome não pode ser resolvido pelos servidores de nome configurados.

Tente fazer ping/trace para os servidores de nome configurados para verificar sua acessibilidade e o tempo de ida e volta.

```
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. Se o servidor DNS estiver acessível e puder resolver nomes e ainda assim as conexões SSL não estiverem sendo otimizadas, verifique se o serviço acelerado configurando o domínio ou nome de host especificado está ativo e se não há alarmes para o SSL AO. Use os seguintes 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
```

A presença do alarme "accl_svc_inative" é uma indicação de que há alguma discrepância na configuração de serviço acelerado e que pode haver um ou mais serviços acelerados com configuração sobreposta para entradas de servidor. Verifique a configuração acelerada do serviço e verifique se a configuração está correta. Use o seguinte comando para verificar a configuração:

```
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 verificar os detalhes sobre um determinado serviço acelerado, use o seguinte 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
```

Um motivo pelo qual o estado operacional do serviço acelerado pode ser INATIVO é uma falha de DNS. Por exemplo, se houver um nome de host de servidor na configuração de serviço acelerado e o WAE não puder resolver o endereço IP do servidor, ele não poderá configurar a política

dinâmica apropriada.

3. Se o contador de estatísticas para "Pipe-through devido a nome de domínio não correspondente" estiver aumentando, é uma indicação de que a conexão SSL é para um servidor configurado para otimização. Verifique as entradas do mecanismo de política usando o seguinte 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 o status da conexão usando o comando **show statistics connection**. A primeira conexão deve mostrar um Accelerator do TSGDL e as conexões subsequentes, até o tempo de vida da entrada da política TIME_DENY, devem ser TDL.

4. Se o servidor DNS estiver na WAN em relação ao WAE do data center ou se o tempo de resposta do DNS reverso for muito longo, algumas conexões poderão ser descartadas. Isso depende do tempo limite do cliente e do tempo de resposta rDNS. Nesse caso, o contador para "Número de pesquisas de DNS reverso canceladas" aumenta e a conexão é interrompida. Essa situação é uma indicação de que o servidor DNS não está respondendo ou muito lento e/ou que o NSCD no WAAS não está funcionando. O status do NSCD pode ser verificado usando o comando **show alarms**. A probabilidade de isso acontecer é muito baixa, pois na maioria das implantações, espera-se que o servidor DNS esteja na mesma LAN que a WAE do data center.

Troubleshooting de HTTP para SSL AO Chaining

NOTE: O encadeamento HTTP para SSL AO foi apresentado na versão 4.3.1 do WAAS. Esta seção não se aplica a versões anteriores do WAAS.

O encadeamento permite que um AO insira outro AO a qualquer momento durante o tempo de vida de um fluxo e ambos os AOs podem aplicar sua otimização específica ao AO independentemente do fluxo. O encadeamento AO é diferente do recurso de transferência AO fornecido pelo WAAS em versões anteriores à 4.3.1 porque com o encadeamento do AO o primeiro AO continua a otimizar o fluxo.

O SSL AO lida com dois tipos de conexões:

- SSL do byte 0: O SSL AO recebe a conexão primeiro e conclui o handshake SSL. Ele analisa a parte inicial do payload para verificar se há um método HTTP. Se o payload indicar HTTP, insere o HTTP AO; caso contrário, ela aplica a otimização TSDL regular.
- CONEXÃO DE Proxy: O HTTP AO recebe a conexão primeiro. Ele identifica o método de cabeçalho CONNECT na solicitação do cliente e insere o SSL AO depois que o proxy confirma com uma mensagem 200 OK.

O SSL AO usa um analisador HTTP leve que detecta os seguintes métodos HTTP: GET, HEAD, POST, PUT, OPTIONS, TRACE, COPY, LOCK, POLL, BCOPY, BMOVE, MKCOL, DELETE,

SEARCH, UNLOCK, BDELETE, PROPFIND, BPROPFIND, PROPPATCH, SUBSCRIBE, BPROPPATCH, UNSUBSCRIBE e X__MS_ENUMATCH TS. Você pode usar o comando **debug accelerator ssl parser** para depurar problemas relacionados ao analisador. Você pode usar o **comando show stat accel ssl payload http/other** para exibir estatísticas de tráfego classificado com base no tipo de payload.

Dicas de solução de problemas:

1. Certifique-se de que o recurso HTTPS esteja habilitado na configuração HTTP AO, pois ele é de propriedade do HTTP AO. Para obter detalhes, consulte o artigo Troubleshooting do HTTP AO.
2. Verifique o estado da conexão usando o comando **show stat connection**. Se otimizado corretamente, ele deve mostrar o THSDL indicando otimização de TCP, HTTP, SSL e DRE-LZ. Se alguma dessas otimizações estiver faltando, faça debug ainda mais nesse otimizador (SSL, HTTP e assim por diante). Por exemplo, se o estado da conexão mostrar THDL, significa que a otimização SSL não foi aplicada na conexão. Detalhes sobre problemas de depuração relacionados ao SSL AO a seguir.
3. Certifique-se de que o SSL AO esteja habilitado e no estado em execução (consulte a seção "Troubleshooting the SSL AO").
4. Certifique-se de que não há alarmes usando o comando **show alarms**.
5. Se o tráfego SSL não estiver sendo otimizado, certifique-se de que o endereço IP do servidor, o nome do host ou o nome do domínio e o número da porta sejam adicionados como parte do serviço acelerado.
6. Certifique-se de que o serviço acelerado está no estado ATIVE usando o comando **show crypto ssl services accelerosl service *ASVC-name*** (consulte a seção "Solução de problemas de configuração de DNS").
7. Certifique-se de que o mecanismo de política tenha uma entrada para este servidor e porta usando o comando **show policy-engine application dynamic**.
8. Se o servidor de destino estiver usando SSL em uma porta não padrão (o padrão é 443), verifique se isso está refletido na configuração do mecanismo de política. O Central Manager conta com essas informações para reportar dados de tráfego SSL.
9. Certifique-se de que o nome de host configurado seja resolvido para um endereço IP válido usando o comando **show crypto ssl services accelerosl service *ASVC-name***. Se nenhum endereço IP for encontrado, verifique se o servidor de nomes está configurado corretamente. Verifique também a saída do 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 SSL AO

Os seguintes arquivos de log estão disponíveis para solução de problemas de SSL AO:

- Arquivos de log de transação: /local1/logs/tfo/working.log (e /local1/logs/tfo/tfo_log_*.txt)
- Depurar arquivos de log: /local1/errorlog/sslao-errorlog.current (e sslao-errorlog.*)

Para facilitar a depuração, você deve primeiro configurar uma ACL para restringir pacotes a um 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 ativar o registro de transações, use o comando de configuração **transaction-logs** da seguinte maneira:

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

Você pode exibir o final de um arquivo de log de transações usando o comando **type-tail** da seguinte maneira:

```
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 e ativar o registro de depuração do SSL AO, use os seguintes comandos.

NOTE: O registro de depuração exige muito da CPU e pode gerar uma grande quantidade de saída. Use-o de forma inteligente e moderna em um ambiente de produção.

Você pode ativar o registro detalhado no disco da seguinte maneira:

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

Você pode ativar o registro de depuração para conexões na ACL da seguinte maneira:

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

As opções para depuração SSL AO são as seguintes:

```
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
```

Você pode ativar o registro de depuração para conexões SSL e, em seguida, exibir o fim do registro de erros de depuração da seguinte maneira:

```
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
```

Troubleshooting de Alarmes de Expiração de Certificado nos Módulos NME e SRE

O SSL AO gera alarmes quando o certificado de máquina autoassinado expirou (ou está dentro de 30 dias do vencimento) e um certificado de máquina global personalizado não está configurado no dispositivo WAAS. O software WAAS gera certificados autoassinados de fábrica com uma data de expiração de 5 anos a partir da primeira inicialização do dispositivo WAAS.

O relógio em todos os módulos WAAS NME e SRE é definido para 1º de janeiro de 2006 durante a primeira inicialização, mesmo que o módulo NME ou SRE seja mais recente. Isso faz com que o certificado autoassinado expire em 1º de janeiro de 2011 e o dispositivo gera alarmes de expiração de certificado.

Se você não estiver usando o certificado de fábrica padrão como o certificado global e, em vez disso, estiver usando um certificado personalizado para o SSL AO, você não terá essa expiração inesperada e poderá atualizar o certificado personalizado sempre que ele expirar. Além disso, se você atualizou o módulo NME ou SME com uma nova imagem de software e sincronizou o relógio para uma data mais recente, talvez esse problema não ocorra.

O sintoma de expiração de certificado é um dos seguintes alarmes (mostrado aqui na saída do 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
```

A GUI do Central Manager relata o seguinte alarme: "Certificate__waas-self__.p12 está prestes a expirar, ele é configurado como certificado da máquina em configurações globais"

Você pode usar uma das seguintes soluções para resolver esse problema:

- Configure um certificado diferente para configurações globais:

```
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
```

- Atualize o certificado de fábrica autoassinado com uma data de expiração posterior. Essa

solução requer um script que você pode obter entrando em contato com o Cisco TAC.

NOTE: Esse problema é corrigido pela resolução da advertência CSCte05426, lançada nas versões 4.1.7b, 4.2.3c e 4.3.3 do software WAAS. A data de vencimento da certificação é alterada para 2037.