WAAS:SSL AOのトラブルシューティング

章：SSL AOのトラブルシューティング

この記事では、SSL AOのトラブルシューティング方法について説明します。

内容

SSLアクセラレータの概要

SSLアクセラレータ(4.1.3以降で利用可能)は、暗号化されたセキュアソケットレイヤ(SSL)およびトランスポートレイヤセキュリティ(TLS)トラフィックを最適化します。SSLアクセラレータは、WAAS内でトラフィックの暗号化と復号化を行い、エンドツーエンドのトラフィック最適化を可能にします。SSLアクセラレータは、暗号化証明書と鍵のセキュアな管理も提供します。

WAASネットワークでは、データセンターWAEは、クライアントによるSSL要求の信頼できる中継ノードとして機能します。秘密キーとサーバ証明書は、データセンターWAEに保存されます。データセンターWAEは、SSLハンドシェイクに参加してセッションキーを取得し、ブランチWAEに安全にインバンドで配信し、クライアントトラフィックの復号化、最適化、再暗号化、WAN経由でのデータセンターWAEへの送信を許可します。データセンターのWAEは、オリジンサーバとの別のSSLセッションを維持します。

SSL/TLS最適化には、次のサービスが関連しています。

- Accelerated Service:SSLサーバまたはサーバのセットに適用されるアクセラレーション特性を記述する構成エンティティ。信頼できる仲介者、使用する暗号、SSLバージョンの許可、および証明書の検証設定として使用する証明書と秘密キーを指定します。
- ピアリングサービス：ブランチWAEとデータセンターWAE間のインバンドSSL接続に適用されるアクセラレーション特性を記述する構成エンティティ。このサービスは、SSL接続を最適化するために、データセンターからブランチWAEにセッションキー情報を転送するために使用されます。
- Central Manager Admin Service:SSLアクセラレータでは直接使用されませんが、SSLアクセラレーションサービスの構成管理には管理者が使用します。また、SSLアクセラレーションサービスで使用する証明書と秘密鍵のアップロードにも使用されます。
- Central Manager Management Service:SSLアクセラレータでは直接使用されませんが、アプリケーションアクセラレータデバイスとCentral Manager間の通信に使用されます。このサービスは、構成管理、Secure Store Encryption Keyの取得、およびデバイスステータスの更新に使用されます。

Central Managerのセキュアストアは、すべてのWAEのセキュアな暗号キーを格納するため、SSL AOを動作させるために不可欠です。Central Managerをリロードするたびに、管理者は**cms secure-store open**コマンドを使用してパスフレーズを入力し、セキュアストアを再オープンする必要があります。WAEは、WAEがリブートするたびにCentral ManagerからSecure Storeの暗号化キーを自動的に取得するため、リロード後にWAEに対するアクションは不要です。

クライアントがHTTPプロキシソリューションを使用している場合、初期接続はHTTP AOによって処理され、ポート443へのSSLトンネル要求として認識されます。HTTP AOはデータセンターWAEで定義された一致するSSLアクセラレーションサービスを検索します。ただし、HTTPSプロキシのHTTP AOがSSL AOに渡すトラフィックは、SSLアプリケーションではなく、Webアプリケーションの統計情報の一部として報告されます。HTTP AOが一致するエントリを検出しない場合、スタティックHTTPS(SSL)ポリシー設定に従って接続が最適化されます。

SSL AOは、CA署名付き証明書ではなく自己署名証明書を使用できます。これは、概念実証(POC)システムの導入やSSL問題のトラブルシューティングに役立ちます。自己署名証明書を使用すると、元のサーバ証明書をインポートしなくてもWAASシステムを迅速に導入でき、問題の原因となる可能性のある証明書を排除できます。SSL Accelerated Serviceの作成時に、Central Managerで自己署名証明書を設定できます。ただし、自己署名証明書を使用すると、クライアントブラウザに、証明書が信頼できないというセキュリティアラートが表示されます（既知のCAによって署名されていないため）。 このセキュリティ警告を回避するには、クライアントブラウザの[Trusted Root Certification Authorities]ストアに証明書をインストールします。(Internet Explorerのセキュリティ警告で、[証明書の表示]をクリックして、証明書ダイアログで[証明書のインストール]**をクリック**し、証明書のインポートウィザードを完了します)。

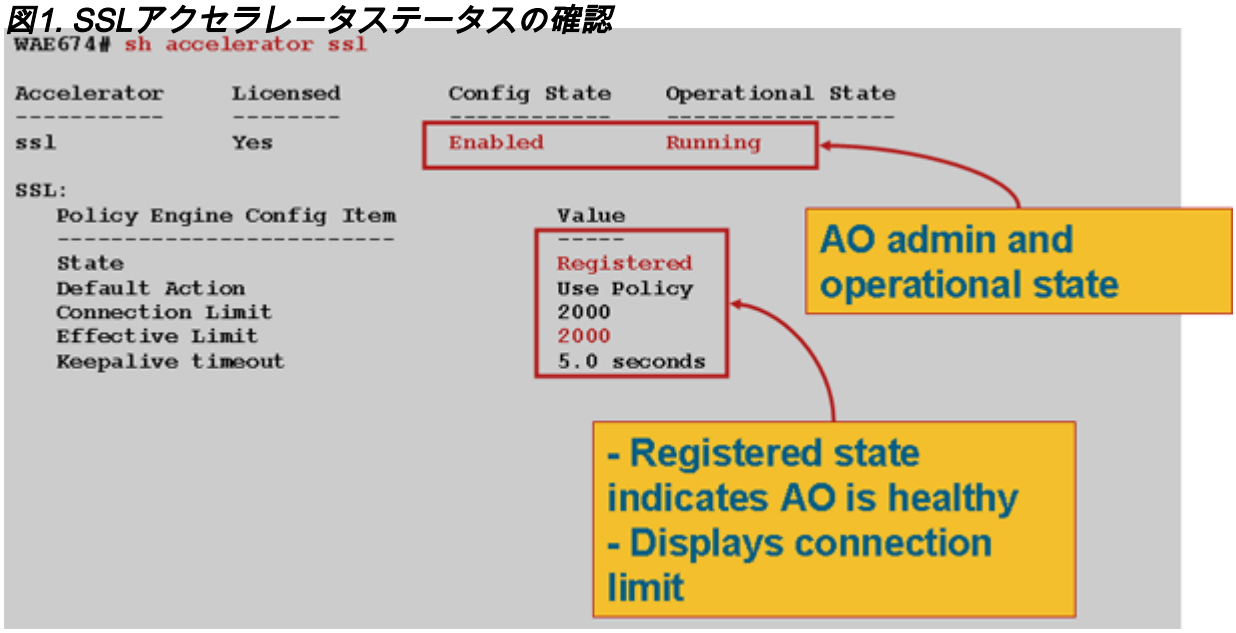
SSL Management Servicesの設定はオプションで、Central Managerの通信に使用するSSLバージョンと暗号リストをWAEおよびブラウザ（管理アクセス用）に変更できます。 ブラウザでサポートされていない暗号を設定すると、Central Managerへの接続が失われます。この場合、CLIから**crypto ssl management-service**コンフィギュレーションコマンドを使用して、SSL管理サービス設定をデフォルトに戻します。

SSL AOのトラブルシューティング

一般的なAOの設定とステータスは、**show acceleratorコマンド**と**show licenseコマンド**で確認できます(「Troubleshooting Application Acceleration」の記事を参照してください)。Enterpriseライセンスは、SSLアクセラレータの動作に必要です。

次に、図1に示すように、**show accelerator sslコマンドを使用して、データセンターとブランチWAEの両方のSSL AOに固有のステータスを確認します。SSL AOが有効、実行中、登録済みで、接続制限が表示されることを確認します。**Config StateがEnabledで、Operational StateがShutdownの場合は、ライセンスの問題を示しています。[Operational State]が[Disabled]の場合は、Central Managerのセキュアストアが開いていないか、Central Managerが到達不能であるため、WAEがCentral Managerのセキュアストアから SSLキーを取得できないことが原因である可能性があります。**show cms info**コマンドと**pingコマンドを**使用して、Central Managerが到達可能であることを確認します。

図1. SSLアクセラレータステータスの確認



Gen Crypto Paramsの[Operational State]が表示された場合は、ステータスが[Running]になるまで待ちます。この場合、リブート後に数分かかることがあります。CMからのキーの取得の状態が数分以上表示される場合は、Central ManagerのCMSサービスが実行されていないか、Central Managerへのネットワーク接続がないか、WAEとCentral ManagerのWAASバージョンに互換性がないか、Central Managerのセキュアストアが開されていない可能性があります。

Central Managerのセキュアストアが初期化され、開いていることを確認するには、次のように**show cms secure-storeコマンド**を使用します。

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

Secure Storeが初期化されていない、または開いていない場合、mstore_key_failureやsecure-storeなどの重大なアラームが表示されます。**cms secure-store open**コマンドを使用してセキュア・ストアを開くこともでき、Central Managerから**[Admin] > [Secure Store]を選択します。**

ヒント：パスワードを忘れた場合にSecure Storeをリセットする必要がないように、Secure Storeのパスワードを文書化します。

WAEでのディスク暗号化に問題がある場合は、SSL AOの動作を妨げる可能性もあります。**show disk details**コマンドを使用して、ディスク暗号化が有効になっていることを確認し、CONTENTパーティションとSPOOLパーティションがマウントされているかどうかを確認します。これらのパーティションがマウントされている場合は、ディスク暗号化キーがCentral Managerから正常に取得され、暗号化されたデータをディスクから書き込んで読み取ることができることを示します。**show disk detailsコマンド**で「System is initializing」と表示される場合は、暗号化キーがまだCentral Managerから取得されておらず、ディスクがまだマウントされていないことを示します。この状態では、WAEはアクセラレーションサービスを提供しません。WAEがCentral Managerからディスク暗号化キーを取得できない場合、アラームが発生します。

SSLアクセラレーションサービスが設定され、そのステータスがデータセンターWAEで「有効」になっていることを確認できます(Central Managerでデバイスを選択し、[設定(Configure)] > [アクセラレーション(Acceleration)] > [SSLアクセラレーションサービス(SSL Accelerated Services)]を選択します)。設定および有効化されたアクセラレーションサービスは、次の条件により、SSLアクセラレータによって非アクティブに設定される場合があります。

- 高速サービスで設定された証明書がWAEから削除されました。**show running-config**コマンドを使用して、アクセラレーションサービスで使用されている証明書を判別し、次に**show crypto certificates**コマンドと**show crypto certificate-details**コマンドを使用して、証明書がセキュアストアにあることを確認します。証明書がない場合は、証明書を再インポートします。
- サービス証明書の有効期限が切れています。**show crypto certificates**コマンドと**show crypto certificate-detailsコマンドを使用して**、証明書の有効期限を確認します。
- アクセラレーションサービス証明書には、将来に有効な日付があります。**show crypto certificates**コマンドと**show crypto certificate-detailsコマンドを使用**し、コマンド出力の妥当性セクションを確認します。また、WAEのクロックおよびタイムゾーン情報が正確であることを確認します。

図2に示すように、SSL接続に正しいポリシーが適用されていること、つまり、SSLアクセラレーションによる完全な最適化が行われていることを確認できます。Central ManagerでWAEデバイスを選択し、**[Monitor] > [Optimization] > [Connections Statistics]を選択します**。

図2. SSL接続の正しいポリシーの確認

show running-configコマンドを使用して、HTTPSトラフィックポリシーが正しく設定されている

ことを確認します。SSLアプリケーションのアクションに対してoptimize DRE no compression noneを表示し、次のようにHTTPS分類子に対して適切な照合条件を表示する必要があります。

```
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
```

アクティブな高速サービスは、高速サービス内で設定されたサーバIP:port、server name:port、またはserver domain:portに対応するダイナミックポリシーを挿入します。これらのポリシーは、show policy-engine application dynamicコマンドを使用して検査できます。表示される各ポリシーの[Dst]フィールドは、高速サービスに一致するサーバIPとポートを示します。ワイルドカードドメイン（たとえば、server-domain *.webex.comポート443）の場合、Dstフィールドは「Any:443」になります。 サーバ名の設定の場合、転送DNSルックアップは、高速サービスがアクティブ化されたときに実行され、DNS応答で返されたすべてのIPアドレスがポリシーエンジンに挿入されます。このコマンドは、アクセラレーションサービスが「インサービス」とマークされているものの、他のエラーが原因でアクセラレーションサービスが非アクティブにレンダリングされている状況を検出するのに便利です。たとえば、すべてのアクセラレーションサービスはピアリングサービスに依存し、証明書の欠落または削除が原因でピアリングサービスが非アクティブの場合、アクセラレーションサービスも非アクティブとしてマークされます（show running-configの出力では「inservice」と表示されます）。SSLダイナミックポリシーがデータセンターWAEでアクティブであることを確認するには、show policy-engine application dynamicコマンドを使用します。ピアリングサービスのステータスを確認するには、show crypto ssl services host-service peeringコマンドを使用します。

SSL AOアクセラレーションサービス設定には、次の4種類のサーバエントリがあります。

- スタティックIP(server-ip)：バージョン4.1.3以降で使用可能
- Catch All(server-ip any):4.1.7以降で使用可能
- ホスト名（サーバ名）:4.2.1以降で使用可能
- ワイルドカードドメイン（サーバドメイン）:4.2.1以降で使用可能

接続がSSL AOで受信されると、最適化に使用する必要がある高速サービスが決定されます。スタティックIP設定には、サーバ名、サーバドメイン、サーバip anyの順に最も高い優先順位が与えられます。設定済みのアクティブ化された高速サービスが、接続用のサーバIPと一致しない場合、その接続は汎用AOにプッシュされます。SSL AOによってポリシーエンジンに挿入されたCookieは、高速化されたサービスと、特定の接続にどのタイプのサーバエントリが一致するかを決定するために使用されます。このポリシーエンジンCookieは32ビットの数値であり、SSL AOに対してのみ意味を持ちます。上位のビットは異なるサーバエントリタイプを示すために使用され、下位のビットは高速サービスインデックスを示します。

SSLポリシーエンジンCookieの値

Cookie値	サーバエントリタイプ	注
0x8 *xxxxxxx*	サーバ IP アドレス	スタティックIPアドレスの設定

0x4 *xxxxxxx*	サーバホスト名	データセンターのWAEは、ホスト名に対して前方DNSルックアッ
0x2FFFFFFF	サーバドメイン名	データセンターWAEは、宛先ホストのIPアドレスで逆DNSルックア
0x1 *xxxxxxx*	Server Any	この高速サービス設定を使用して、すべてのSSL接続が高速化され

例 1：Accelerated Service with server-ip Configuration:

```
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
```

対応するポリシーエンジンエントリが次のように追加されます。

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

例 2：サーバ名の設定によるサービスの高速化：

この設定により、企業のSSLアプリケーションを簡単に導入できます。DNS設定の変更に対応し、IT管理タスクを削減します。

```
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
```

対応するポリシーエンジンエントリが次のように追加されます。

```
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
```

例 3：サーバドメイン設定によるサービスの高速化：

この設定により、WAASデバイスは単一のワイルドカードドメインを設定できるため、すべてのサーバのIPアドレスを知る必要がなくなります。データセンターのWAEは、リバースDNS(rDNS)を使用して、設定されたドメインに属するトラフィックを照合します。ワイルドカードドメインを設定すると、複数のIPアドレスを設定する必要がなくなり、SaaSアーキテクチャに対してスケーラブルで適用可能なソリューションになります。

```
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
```

対応するポリシーエンジンエントリが次のように追加されます。

```
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
```

例 4：Accelerated Service with server-ip any Configuration:

この設定は、キャッチオールメカニズムを提供します。server-ip anyポート443を使用した高速サービスがアクティブになると、ポート443上のすべての接続がSSL AOによって最適化されます。この設定は、POC中に使用して、特定のポート上のすべてのトラフィックを最適化できます。

```
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
```

対応するポリシーエンジンエントリが次のように追加されます。

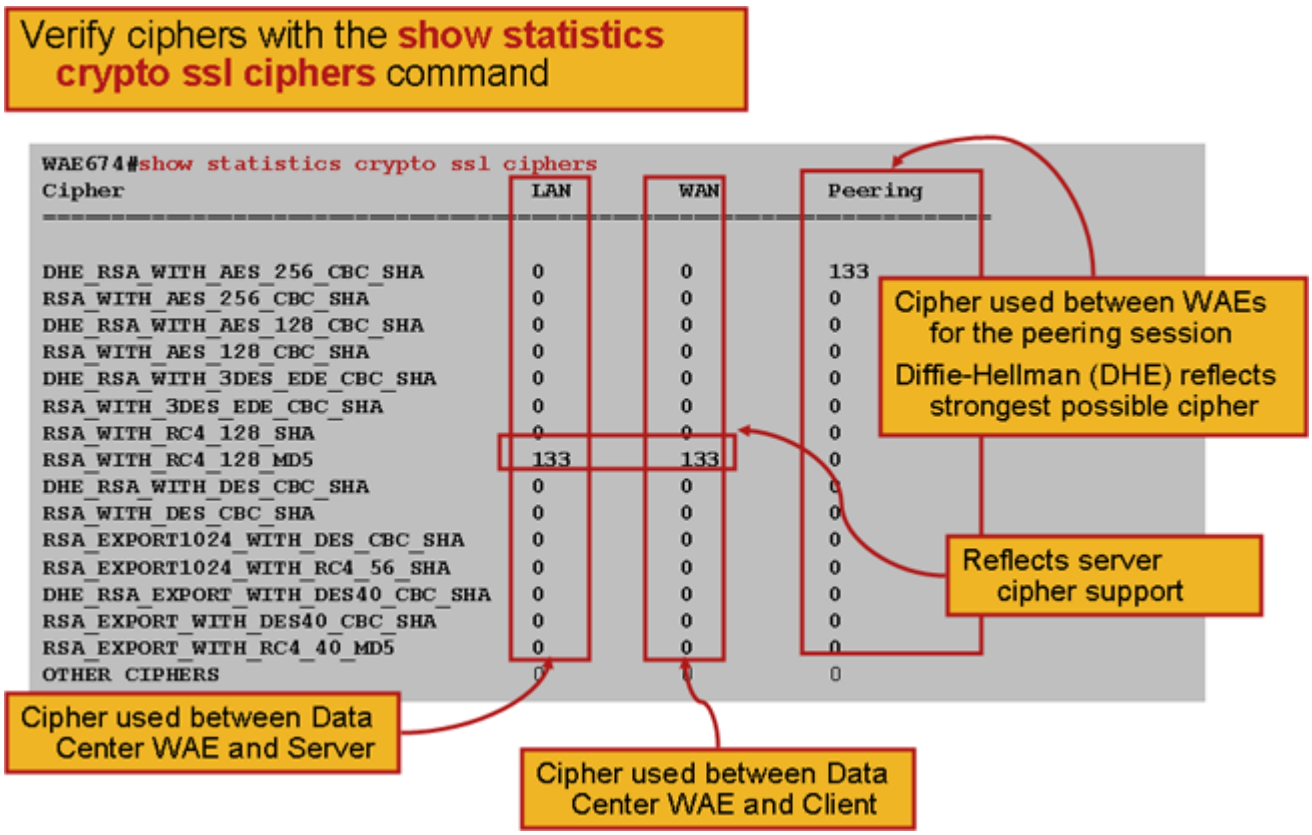
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

図3に示すように、show statistics crypto ssl ciphersコマンドで使用されている暗号を確認できます。

図3.暗号の確認



これらの暗号が発信元サーバに設定されている暗号と一致していることを確認できます。**注：** DHEを含む暗号は、Microsoft IISサーバーではサポートされていません。

Apacheサーバでは、httpd.confファイルのSSLバージョンと暗号の詳細を確認できます。これらのフィールドは、httpd.confから参照される別のファイル(sslmod.conf)に存在する場合もあります。次のように、SSLProtocolフィールドとSSLCipherSuiteフィールドを探します。

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

Apacheサーバの証明書発行者を確認するには、openssl**コマンドを使用して証明書を次のように読み取ります。**

```
> 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
```

ブラウザでは、証明書とその詳細を表示して、証明書チェーン、バージョン、暗号化キータイプ、発行者名(CN)、およびサブジェクト/サイトCNを確認できます。Internet Explorerで、南京錠のアイコンをクリックし、[証明書の表**示]をクリックし**て、[詳細]タブと[証明書のパス]タブを参照してください。

ほとんどのブラウザでは、クライアント証明書がX509 PEM形式ではなくPKCS12形式であることが必要です。X509 PEM形式をPKCS12形式にエクスポートするには、Apacheサーバで openssl**コマンドを次のように使用します。**

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

秘密鍵が暗号化されている場合、エクスポートにはパスフレーズが必要です。エクスポートパスワードは、WAASデバイスへのクレデンシャルのインポートに再度使用されます。

show statistics accelerator sslコマンドを使用して、SSL AOの統計情報を表示します。

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

失敗したセッションおよび証明書の検証の統計情報は、トラブルシューティングに役立つ可能性があり、**show statistics accelerator sslコマンドで**次のフィルタを使用して、より簡単に取得できます。

```
WAE# show statistics accelerator ssl | inc Failed
  Total Failed Handshakes:                                          47
  Total Failed Certificate Verifications:                           28
  Failed certificate verifications due to invalid certificates:     28
  Failed Certificate Verifications based on OCSP Check:             0
  Failed Certificate Verifications (non OCSP):                      28
  Total Failed Certificate Verifications due to Other Errors:       0
  Total Failed OCSP Requests:                                       0
```

```
  Total Failed OCSP Requests due to Other Errors:                    0
  Total Failed OCSP Requests due to Connection Errors:               0
  Total Failed OCSP Requests due to Connection Timeouts:             0
  Total Failed OCSP Requests due to Insufficient Resources:          0
```

DNS関連の統計情報は、サーバ名とワイルドカードドメイン設定のトラブルシューティングに役立ちます。これらの統計情報を取得するには、次のようにshow statistics accelerator sslコマンドを使用します。

```
WAE# show statistics accelerator ssl
 . . .
 Number of forward DNS lookups issued:                              18
 Number of forward DNS lookups failed:                              0
 Number of flows with matching host names:                          8
 Number of reverse DNS lookups issued:                              46
 Number of reverse DNS lookups failed:                              4
 Number of reverse DNS lookups cancelled:                           0
 Number of flows with matching domain names:                        40
 Number of flows with matching any IP rule:                         6
 . . .
 Pipe-through due to domain name mismatch:                          6
 . . .
```

SSL再ハンドシェイクに関連する統計情報は、トラブルシューティングに役立ちます。また、show statistics accelerator sslコマンドで次のフィルタを使用して取得できます。

```
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
```

show statistics connection optimized sslコマンドを使用して、WAASデバイスが最適化されたSSL接続を確立していることを確認します。接続の[Accel]列に「TDLS」が表示されることを確認します。「S」は、SSL AOが次のように使用されたことを示します。

```
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"
```

閉じた接続の接続統計情報を確認するには、show statistics connection closed sslコマンドを使用します。

接続が最適化されていない場合は、WCCP/PBRが正しく設定され、動作しているかどうかを確認し、非対称ルーティングを確認します。

SSL接続の統計情報を表示するには、**show statistics connection optimized ssl detail**コマンドを使用します。このコマンドを使用すると、設定されたSSL高速化サービスから得られるダイナミックポリシーが表示されます。**注**：設定されたポリシーはTFO最適化のみですが、設定されたSSLサービスの結果として完全な最適化が適用されます。

```
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
. . .
```

この出力の後半では、拡張SSLセッションレベルの詳細を次に示します。

```
. . .
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
```

HTTP AOからSSL AOへのハンドオフ接続のトラブルシューティング

クライアントがプロキシを経由してHTTPSサーバに到達する必要がある場合、クライアントの要求は最初にHTTP CONNECTメッセージとしてプロキシに送信されます（CONNECTメッセージに実際のHTTPSサーバのIPアドレスが埋め込まれています）。 この時点で、HTTP AOはピアWAEでこの接続を処理します。プロキシは、クライアントとサーバポートの間にトンネルを作成し、クライアントとそのサーバのIPアドレスおよびポートの間で後続のデータをリレーします。プロキシは「200 OK」メッセージをクライアントに返し、クライアントがSSL経由でサーバと通信しようとするため、SSL AOに接続を渡します。次に、クライアントは、プロキシによって設定されたTCP接続（トンネル）を介して、SSLサーバとのSSLハンドシェイクを開始します。

ハンドオフ接続に関する問題のトラブルシューティングを行う際は、次の点を確認してください。

- **show statistics accelerator http**コマンドの出力をチェックして、接続がHTTP AOによって処理され、SSL AOに渡されたことを確認します。Total Handled ConnectionsおよびTotal Connections Handled-off to SSLカウンタを確認します。問題がある場合は、次の点を確認します。
  - HTTP AOが有効で、ピアWAEで実行状態になっている。

- SSLアクセラレーションサービスは、クライアントがCONNECT URLで使用するポート（HTTPSを使用している場合は暗黙的なポート443）で設定されます。プロキシポートがCONNECT URLポートと異なることが多く、このプロキシポートはSSLアクセラレーションサービスで設定しないでください。ただし、プロキシポートは、HTTP AOにマッピングされるトラフィック分類器に含める必要があります。

- **show statistics accelerator http**コマンドの出力を確認して、この接続がSSL AOによって処理および最適化されたことを確認します。Total Handled ConnectionsカウンタとTotal Optimized Connectionsカウンタを調べます。統計情報カウンタが正しくない場合は、前のセクションで説明したように、基本的なSSLトラブルシューティングを実行します。
- データセンターWAEで、**show statistics connection optimized detail**コマンドの出力に、実際のSSLサーバのホスト名、IPアドレス、およびTCPポートが表示されることを確認します。これらのフィールドが正しく設定されていない場合は、次の点を確認してください。
  - クライアントブラウザのプロキシ設定が正しいことを確認します。
  - DNSサーバがデータセンターWAEに設定され、到達可能であることを確認します。WAE上でDNSサーバを設定するには、**ip name-server *A.B.C.D*コマンドを使用**します。

サーバ証明書の検証のトラブルシューティング

サーバ証明書の検証では、データセンターWAEに正しいCA証明書をインポートする必要があります。

サーバ証明書の検証をトラブルシューティングするには、次の手順を実行します。

1.サーバー証明書を検査し、発行者名を取得します。サーバ証明書内のこの発行者名は、一致するCA証明書内のサブジェクト名と一致する必要があります。PEMでエンコードされた証明書がある場合は、opensslがインストールされているサーバで次の**openssl**コマンドを使用できます。

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

2. **show running-configコマンド**を使用して、一致するcrypto pki ca設定がデータセンターWAE上に存在することを確認します。検証プロセスでWAEによって使用されるCA証明書には、インポートされる各CA証明書にcrypto pki ca設定項目が必要です。たとえば、CA証明書company1.caをインポートする場合、データセンターWAEで次の設定を行う必要があります。

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

注：Central Manager GUIを使用してCA証明書をインポートすると、Central Managerは上記のcrypto pki ca設定を自動的に追加して、インポートされたCA証明書を含めます。ただし、CLIを使用してCA証明書をインポートする場合は、上記の設定を手動で追加する必要があります。

3.検証する証明書に証明書チェーンが含まれている場合は、証明書チェーンが整合性があり、一番上の発行者のCA証明書がWAEにインポートされていることを確認します。**openssl verify**コマンドを使用して、最初に証明書を個別に確認します。

4.それでも検証が失敗する場合は、SSLアクセラレータのデバッグログを調べます。デバッグロギングを有効にするには、次のコマンドを使用します。

```
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.テスト接続を開始し、/local/local1/errorlog/sslao-errorlog.currentログファイルを調べます。このファイルは、サーバ証明書に含まれている発行者名を示している必要があります。この発行者名が、CA証明書のサブジェクト名と完全に一致していることを確認します。

ログに他の内部エラーがある場合は、追加のデバッグオプションを有効にすると便利です。

6.発行者名とサブジェクト名が一致しても、CA証明書が正しくない可能性があります。このような場合、既知のCAによってサーバ証明書が発行されると、ブラウザを使用して（WAASなしで）サーバに直接到達できます。ブラウザが接続を設定すると、ブラウザウィンドウの右下またはブラウザのアドレスバーに表示されるロックアイコンをクリックして、証明書を確認できます。証明書の詳細は、このサーバ証明書に一致する適切なCA証明書を示す場合があります。CA証明書内の[Serial Number]フィールドを確認します。このシリアル番号は、データセンターWAEにインポートされる証明書のシリアル番号と一致する必要があります。

7. OCSP失効チェックを有効にしている場合は、無効にして、証明書検証が機能することを確認します。OCSP設定のトラブルシューティングに関するヘルプについては、「OCSP取り消しチェックのトラブルシューティング」セクションを参照してください。

クライアント証明書の検証のトラブルシューティング

クライアント証明書の検証は、元のサーバまたはデータセンターWAEで有効にできます。WAASを使用してSSLトラフィックを高速化すると、オリジンサーバが受信するクライアント証明書は、データセンターWAEの**crypto ssl services global-settingsコマンドで指定されたmachine-cert-keyに指定された証明書またはデータセンターWAEマシン自己署名証明書です。**その結果、オリジンサーバでクライアント証明書の検証が失敗した場合、データセンターのWAEマシン証明書がオリジンサーバで検証できないことが原因である可能性があります。

データセンターWAEのクライアント証明書の検証が機能しない場合、クライアント証明書に一致するCA証明書がデータセンターWAEにインポートされていないことが原因である可能性があります。WAEに正しいCA証明書がインポートされているかどうかを確認する方法については、「サーバ証明書の検証のトラブルシューティング」セクションを参照してください。

ピアWAE証明書の検証のトラブルシューティング

ピア証明書の検証問題をトラブルシューティングするには、次の手順を実行します。

1.検証する証明書がCA署名付き証明書であることを確認します。あるWAEによる自己署名証明書は、別のWAEでは検証できません。デフォルトでは、WAEには自己署名証明書がロードされます。自己署名証明書は、**crypto ssl services global-settings machine-cert-keyコマンドを使用して設定する必要があ**ります。

2.証明書を検証しているデバイスに正しいCA証明書がロードされていることを確認します。たとえば、データセンターWAEでpeer-cert-verifyが設定されている場合、ブランチWAE証明書をCA署名付きにし、同じ署名CA証明書をデータセンターWAEにインポートする必要があります。CLIを使用して証明書を手動でインポートする場合は、**crypto pki caコマンドを使用**してCAを作成することを忘れないでください。Central Manager GUIによってインポートされると、Central Managerは一致するcrypto pki ca設定を自動的に作成します。

3.ピアWAEの検証が引き続き失敗する場合は、「SSL AOロギング」の項の説明に従ってデバッグログを確認してください。

OCSP失効確認のトラブルシューティング

Online Certificate Status Protocol(OCSP)失効チェックが有効になっている状態で、システムが正常なSSL接続を確立できない場合は、次のトラブルシューティング手順を実行します。

1. OCSPレスポンダサービスがレスポンダサーバで実行されていることを確認します。
2. WAEとレスポンダ間の接続が良好であることを確認します。WAEから**ping**および**telnet**コマンド（該当するポート）を使用して確認します。
3. 検証する証明書が実際に有効であることを確認します。有効期限と正しい応答側URLは、通常、問題のある領域です。
4. OCSP応答の証明書がWAEにインポートされることを確認します。OCSPレスポンダからの応答も署名され、OCSP応答に一致するCA証明書がWAE上に存在する必要があります。
5. **show statistics accelerator ssl**コマンドの出力**をチェック**して、OCSPの統計情報を確認し、OCSPの障害に対応するカウンタを確認します。
6. OCSP HTTP接続がHTTPプロキシを経由している場合は、プロキシを無効にして、それが役立つかどうかを確認してください。問題が解決しない場合は、プロキシ設定によって接続障害が発生していないことを確認します。プロキシ設定に問題がない場合は、HTTPヘッダーの特性が存在し、プロキシとの互換性が低下する可能性があります。詳細な調査のためにパケットトレースをキャプチャします。
7. それ以外の方法で障害が発生した場合は、さらにデバッグを行うために、発信OCSP要求のパケットトレースをキャプチャする必要があります。Preliminary WAAS Troubleshootingの記事の「Capting and Analyzing Packets」の項で説明されているtcpdumpコマンドまたはtelethereal**コマンドを使用できます。**

データセンターWAEがOCSPレスポンダに到達するために使用するURLは、次の2つの方法のいずれかで導出されます。

- **crypto pki global-settings**コンフィギュレーションコマンドで設定されたスタティックOCSP URL
- チェック対象の証明書で指定されたOCSP URL

URLがチェックされている証明書から取得されている場合は、URLが到達可能であることを確認する必要があります。SSLアクセラレータのOCSPデバッグログを有効にしてURLを判別し、レスポンダへの接続を確認します。デバッグログの使用方法については、次のセクションを参照してください。

DNS設定のトラブルシューティング

システムでサーバ名とサーバドメインの設定によるSSL接続の最適化に問題がある場合は、次のトラブルシューティング手順を実行します。

1. WAEに設定されているDNSサーバに到達可能で、名前を解決できることを確認します。次のコマンドを使用して、設定されたDNSサーバを確認します。

```
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 !
```

この応答は、設定されたネームサーバでは名前を解決できないことを示します。

設定済みのネームサーバに対してping/traceouteを実行し、到達可能性とラウンドトリップ時間を確認します。

```
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. DNSサーバが到達可能で、名前が解決してもSSL接続が最適化されない場合は、指定されたドメインまたはホスト名を設定する高速サービスがアクティブで、SSL AOのアラームがないことを確認します。次のコマンドを使用します。

```
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
```

「accl_svc_inactive」アラームの存在は、サービスの高速化の設定に何らかの不一致があり、サーバエントリの設定が重複しているサービスが1つ以上ある可能性があることを示しています。高速サービス設定を確認し、設定が正しいことを確認します。次のコマンドを使用して、設定を確認します。

```
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
```

特定の高速サービスの詳細を確認するには、次のコマンドを使用します。

```
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
```

高速化されたサービスの動作状態が非アクティブである可能性がある理由の1つは、DNSの障害です。たとえば、高速サービス設定にサーバのホスト名があり、WAEがサーバのIPアドレスを解決できない場合、適切なダイナミックポリシーを設定できません。

3.「ドメイン名の不一致によるパススルー」の統計カウンタが増加している場合は、SSL接続が最適化用に構成されたサーバー用であることを示しています。次のコマンドを使用して、ポリシーエンジンエントリを確認します。

```
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
```

show statistics connectionコマンドを使用して、接続ステータス**を確認**します。最初の接続はTSGDLのアクセラレータを示し、TIME_DENYポリシーエントリのライフタイムまで後続の接続はTDLである必要があります。

4. DNSサーバがデータセンターWAEに関してWAN上にある場合、または逆DNS応答時間が長すぎる場合は、一部の接続が切断される可能性があります。これは、クライアントのタイムアウトとrDNS応答時間によって異なります。この場合、「Number of reverse DNS lookup canceled」のカウンタが増加し、接続がドロップされます。この状況は、DNSサーバが応答しないか、非常に遅く、WAAS上のNSCDが動作していないことを示しています。NSCDのステータスは、**show alarms**コマンドを使用して**確認で**きます。ほとんどの導入では、DNSサーバがデータセンターのWAEと同じLAN上にあることが予想されるため、この問題が発生する可能性は非常に低くなります。

HTTPからSSL AOチェーンのトラブルシューティング

注：HTTPからSSLへのAOチェーンは、WAASバージョン4.3.1で導入されました。このセクションは、以前のWAASバージョンには適用されません。

チェーンを使用すると、AOはフローのライフタイム中にいつでも別のAOを挿入でき、両方のAOはフローに独自にAO固有の最適化を適用できます。AOチェーニングは、4.3.1より前のリリースでWAASが提供するAOハンドオフ機能とは異なります。これは、AOチェーニングによって最初のAOがフローを最適化し続けるためです。

SSL AOは2種類の接続を処理します。

- バイト0 SSL:SSL AOは最初に接続を受信し、SSLハンドシェイクを完了します。ペイロードの最初の部分を解析して、HTTPメソッドをチェックします。ペイロードがHTTPを示す場合は、HTTP AOを挿入します。そうでない場合は、通常のTSDL最適化が適用されます。
- プロキシ接続：HTTP AOが最初に接続を受信します。クライアントの要求でCONNECTヘッダー方式を識別し、プロキシが200 OKメッセージで確認した後にSSL AOを挿入します。

SSL AOは、次のHTTPメソッドを検出する軽量HTTPパーサーを使用します。GET、HEAD、POST、PUT、OPTIONS、TRACE、COPY、LOCK、POLL、BCOPY、BMOVE、MKCOL、DELETE、SEARCH、UNLOCK、BPROPFIND、PROPPATCH、SUBSCRIBE、BPROPPATCH、UNSUBSCRIBE、AND x__MS_ENUMATTSdebug accelerator ssl parserコマンドを使用して、パーサに関する問題をデバッグできます。**show stat accel ssl payload http/other**コマンドを使用すると、ペイロードタイプに基づいて分類されたトラフィックの統計情報を表示できます。

トラブルシューティングのヒント:

1. HTTP AO設定でHTTPS機能が有効になっていることを確認します。これはHTTP AOが所有しているためです。詳細については、「HTTP AOのトラブルシューティング」の記事を参照してください。
2. **show stat connection**コマンドを使用して、接続状態を確認します。正しく最適化されている場合は、TCP、HTTP、SSL、およびDRE-LZの最適化を示すTHSDLが表示されます。これらの最適化が欠落している場合は、そのオプティマイザ（SSL、HTTPなど）でさらにデバッグします。 たとえば、接続状態がTHDLと表示されている場合、SSL最適化が接続に適用されなかったことを意味します。SSL AOに関連するデバッグ問題の詳細は、次のとおりです。
3. SSL AOが有効で、実行状態であることを確認します(「SSL AOのトラブルシューティング」の項を参照してください)。
4. **show alarms**コマンドを使用して、アラームが発生していないことを確認します。
5. SSLトラフィックが最適化されていない場合は、サーバのIPアドレス、ホスト名、またはドメイン名とポート番号がアクセラレーションサービスの一部として追加されていることを確認します。
6. **show crypto ssl services accelerated-service *ASVC-name*コマンド**を使用して、高速化されたサービスがACTIVE状態であることを確認します(「DNS設定のトラブルシューティング」セクションを参照してください)。
7. **show policy-engine application dynamic**コマンドを使用して、ポリシーエンジンにこのサーバとポートのエントリがあることを確認します。
8. 宛先サーバがデフォルト以外のポート（デフォルトは443）でSSLを使用している場合は、これがポリシーエンジン設定に反映されていることを確認します。Central Managerは、SSLトラフィックデータをレポートするためにこの情報を使用します。
9. **show crypto ssl services accelerated-service *ASVC*-name**コマンドを使用して、設定したホスト名が有効なIPアドレスに解決されることを確認します。IPアドレスが見つからない場合は、ネームサーバが正しく設定されているかどうかを確認します。また、dnslookup ***IP*-address**コマンドの出力を確認してください。

```
wae# sh run no-policy
. . .
crypto ssl services accelerated-service sslc
  version all
  server-cert-key test.p12
```

```
  server-ip 2.75.167.2 port 4433
  server-ip any port 443
  server-name mail.yahoo.com port 443
  server-name mail.google.com port 443
  inservice


wae# sh crypto ssl services accelerated-service sslc
Name: sslc
Config state: ACTIVE, Oper state: ACTIVE, Cookie: 0x0, Error vector: 0x0

   The following server IP addresses are configured:
     2.75.167.2 port 4433
     any port 443

   The following server host names are configured:
     mail.yahoo.com port 443
         Host 'mail.yahoo.com' resolves to following IPs:
         66.163.169.186

     mail.google.com port 443
         Host 'mail.google.com' resolves to following IPs:
         74.125.19.17
         74.125.19.18
         74.125.19.19
         74.125.19.83


wae# dnslookup mail.yahoo.com
Official hostname: login.lga1.b.yahoo.com
         address: 66.163.169.186
Aliases: mail.yahoo.com
Aliases: login.yahoo.com
Aliases: login-global.lgg1.b.yahoo.com

wae# dnslookup mail.google.com
Official hostname: googlemail.l.google.com
         address: 74.125.19.83
         address: 74.125.19.17
         address: 74.125.19.19
         address: 74.125.19.18
Aliases: mail.google.com
```

SSL AOロギング

SSL AOの問題のトラブルシューティングには、次のログファイルを使用できます。

- トランザクションログファイル：/local1/logs/tfo/working.log(および /local1/logs/tfo/tfo_log_*.txt)
- デバッグログファイル：/local1/errorlog/sslao-errorlog.current (およびsslao-errorlog.*)

デバッグを簡単にするには、まずACLを設定して、パケットを1つのホストに制限する必要があります。

```
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
```

トランザクションロギングを有効にするには、次のようにtransaction-logs設定コマンドを使用します。

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

次のようにtype-tailコマンドを使用して、トランザクションログファイルの終わりを表示できます。

```
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
```

SSL AOのデバッグロギングを設定および有効にするには、次のコマンドを使用します。

注：デバッグロギングはCPUに負荷がかかり、大量の出力を生成する可能性があります。実稼働環境では慎重に慎重に使用してください。

ディスクへの詳細なロギングは、次のように有効にできます。

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

ACLの接続のデバッグロギングは、次のように有効にできます。

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

SSL AOデバッグのオプションは次のとおりです。

```
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
```

SSL接続のデバッグロギングを有効にして、デバッグエラーログの最後を次のように表示できます。

```
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
```

NMEおよびSREモジュールの証明書期限切れアラームのトラブルシューティング

SSL AOは、自己署名マシン証明書が期限切れ（または有効期限が30日以内）で、WAASデバイスでカスタムグローバルマシン証明書が設定されていない場合にアラームを生成します。WAASソフトウェアは、WAASデバイスの最初の起動から5年間の有効期限を持つ自己署名証明書を生成します。

すべてのWAAS NMEおよびSREモジュールのクロックは、NMEまたはSREモジュールが新しい場合でも、最初の起動時に2006年1月1日に設定されます。これにより、自己署名証明書が2011年1月1日に期限切れになり、デバイスは証明書の期限切れアラームを生成します。

デフォルトのファクトリ証明書をグローバル証明書として使用せず、代わりにSSL AOのカスタム証明書を使用している場合、予期しない有効期限が発生せず、有効期限が切れた場合にカスタム証明書を更新できます。また、NMEまたはSMEモジュールを新しいソフトウェアイメージで更新し、クロックをより新しい日付に同期した場合は、この問題が発生しない可能性があります。

証明書の期限切れの症状は、次のいずれかのアラームです(**show alarms**コマンドの出力に示されます)。

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

または

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

Central Manager GUIで次のアラームが報告されます。「Certificate__waas-self__.p12は有効期限が近づいており、グローバル設定でマシン証明書として設定されています」

この問題を解決するには、次のいずれかの方法を使用できます。

- グローバル設定用に別の証明書を設定します。

```
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
```

- 自己署名証明書を後の有効期限で更新します。このソリューションには、Cisco TACに連絡して取得できるスクリプトが必要です。

注：この問題は、WAASソフトウェアバージョン4.1.7b、4.2.3c、および4.3.3でリリースされた警告CSCte05426の解決策によって修正されています。認定の有効期限は2037に変更されています。