WAAS - أستكشاف أخطاء SSL AO وإصلاحها

الفصل: أستكشاف أخطاء SSL AO وإصلاحها

يوضح هذا المقال كيفية أستكشاف أخطاء SSL AO وإصلاحها.

المحتويات

نظرة عامة على مسرع SSL

ليصوتلا ذخآم ةقبط رورم ةكرح (ثدحألا تارادصإلاو 4.1.3 يف رفوتم) SSL عرسم نسحي الآمنة المشفرة (SSL) وطبقة أمان طبقة النقل (TLS). يوفر مسرع SSL تشفير حركة مرور البيانات وفك تشفيرها داخل WAAS لتمكين تحسين حركة المرور من نهاية إلى نهاية. كما يوفر مسرع SSL إدارة آمنة لشهادات التشفير والمفاتيح.

في شبكة WAAS، يعمل مركز البيانات WAE كعقدة ووسيط موثوق به لطلبات SSL بواسطة العميل. يتم تخزين المفتاح الخاص وشهادة الخادم على مركز البيانات WAE. يشارك WAE مركز البيانات في مصافحة SSL لاستخلاص مفتاح الجلسة، والذي يقوم بتوزيعه بشكل آمن داخل النفق إلى WAE الفرعي، مما يسمح ل WAE الفرعي بفك تشفير حركة مرور العميل، وتحسينها، وإعادة تشفيرها، وإرسالها عبر WAN إلى WAE مركز البيانات. يحتفظ WAE لمركز البيانات بجلسة عمل SSL منفصلة مع خادم الأصل.

تعد الخدمات التالية ذات صلة لتحسين SSL/TLS:

- الخدمة السريعة - وحدة تكوين تصف خصائص السرعة المراد تطبيقها على خادم SSL أو مجموعة من الخوادم. تحدد الشهادة والمفتاح الخاص المراد استخدامها أثناء التمثيل كوسيط موثوق به والشفرات المراد استخدامها وإصدار SSL المسموح به وإعدادات التحقق من الشهادة.
- خدمة التجميع - كيان تكوين يصف خصائص السرعة التي يتم تطبيقها على الاتصالات SSL داخل النفق بين شبكات WAE الفرعية ومراكز البيانات. يتم استخدام هذه الخدمة لتحسين الفرعية WAEs إلى البيانات مركز من العمل جلسة مفتاح معلومات لنقل اتصالات SSL.
- خدمة Central Manager Admin (خدمة إدارة المدير المركزي) - ال يتم استخدامها مباشرة بواسطة مسرع SSL، ولكن يتم استخدامها من قبل مسؤول الإدارة لتكوين خدمات SSL السريعة. يستخدم أيضا لتحميل الشهادات والمفاتيح الخاصة التي سيتم استخدامها في خدمات SSL السريعة.
- خدمة إدارة الإدارة المركزية - ال يتم استخدامها مباشرة من قبل مسرع SSL، ولكنها تستخدم للاتصال بين أجهزة مسرع التطبيق و Central Manager. يتم استخدام هذه الخدمة لإدارة التكوين واستردادات مفتاح تشفير المخزن الآمن وتحديثات حالة الجهاز.

يعد المخزن الآمن الخاص بالمدير المركزي ضروريا لتشغيل SSL AO لأنه يقوم بتخزين مفاتيح التشفير الآمنة لجميع WAE. بعد كل عملية إعادة تحميل "للمدير المركزي"، يحتاج المسؤول إلى إعادة فتح المخزن الآمن من خلال توفير عبارة المرور باستخدام الأمر **cms secure-store open**. يسترجع WAE تلقائيا مفاتيح تشفير المخزن الآمن الخاص به من الإدارة المركزية كلما أعيد تمهيد WAE، لذلك لا يتطلب أي إجراء على WAE بعد إعادة التحميل.

إذا كان العملاء يستخدمون حلول وكيل HTTP، تتم معالجة الاتصال الأولي بواسطة HTTP AO، والذي يتعرف عليه كطلب نفق SSL 443. يبحث HTTP AO عن خدمة سريعة SSL ومع مطابقة معرفة في WAE مركز البيانات وعندما يجد تطابق، يدع الاتصال إلى SSL AO. يعزز وكيل HTTPS إلى SSL AO الذي يسلمها مرور حركة عن الإبلاغ يتم ذلك، من إحصائيات تطبيق الويب، ولكن في تطبيق SSL. إذا لم يعثر HTTP AO على تطابق، يتم تحسين الاتصال وفقا لتكوين نهج HTTPS (SSL) الثابت.

يمكن أن تستخدم SSL AO الشهادات الموقعة ذاتيا بدلا من الشهادات الموقعة من CA، مما يمكن أن يكون مفيدا في نشر أنظمة إثبات صحة المفاهيم (POC) وفي استكشاف أخطاء SSL وإصلاحها. باستخدام شهادات ذاتية التوقيع، يمكنك نشر نظام WAAS بدون سرعة كمصدر موثوق للشهادات ويمكنك استبعاد الأصول الخادم شهادات استيراد الحاجة عند إنشاء خدمة SSL في "الإدارة المركزية" يمكنك تكوين شهادة موقعة ذاتيا للمشكلات. ومع ذلك، عند استخدام شهادة موقعة ذاتيا، يعرض مستعرض العميل تحذيرا بأن الشهادة غير موثوق بها (لأنها غير موقعة من قبل مرجع مصدق معروف). يجب على الأمان، هذا، قم بتثبيت الشهادة في مخزن "المراجع المصدقة الجذر الموثوق بها" على مستعرض العميل. (في Internet Explorer، انقر فوق **عرض الشهادة**، ثم انقر على **تثبيت**

الشهادة من مربع حوار الشهادة وإكمال معالج إستيراد الشهادات.)

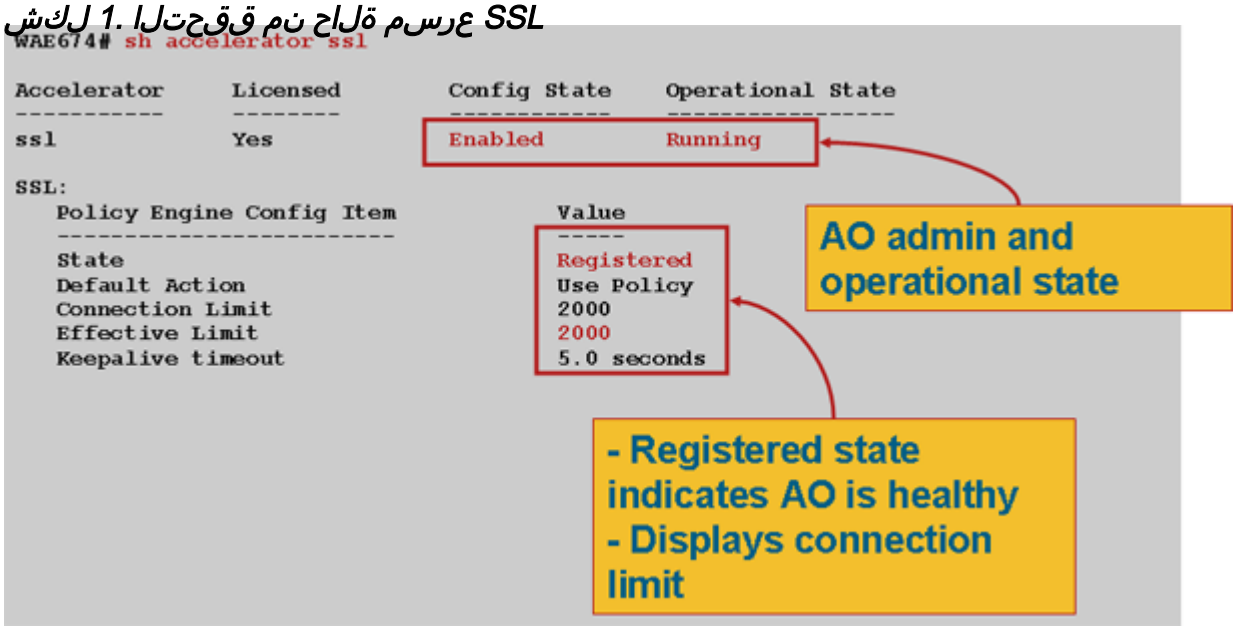
تكوين خدمات إدارة SSL إختياري، ويسمح لك بتغيير إصدار SSL وقائمة التشفير المستخدمة للاتصالات Central Manager إلى WAE وإلى المستعرض (للوصول الإداري). إذا قمت بتكوين التشفير غير المعتمد من قبل المستعرض، فستفقد الاتصال بالمدير المركزي. في هذه الحالة، أستخدم أمر التكوين **crypto ssl management-service** من واجهة سطر الأوامر (CLI) لتعيين إعدادات خدمة إدارة SSL مرة أخرى إلى الإعداد الافتراضي.

أستكشاف أخطاء SSL AO وإصلاحها

يمكنك التحقق من تكوين وحدة التحكم في الوصول (AO) العام وحالتها باستخدام أوامر **show accelerator** و**show license**، كما هو موضح في القسم [أستكشاف أخطاء التطبيقات وإصلاحها](#) وتسريع التطبيقات. ترخيص المؤسسة مطلوب لتشغيل مسرع SSL.

بعد ذلك، تحقق من الحالة المحددة ل SSL AO على كل من مركز البيانات و WAEs الفرعية باستخدام الأمر **show accelerator ssl**، كما هو موضح في الشكل 1. تريد أن ترى تمكين SSL AO وتشغيله وتسجيله، وعرض حد الاتصال. إذا تم تمكين حالة التكوين ولكن تم إيقاف تشغيل حالة التشغيل، فإنها تشير إلى مشكلة في الترخيص. إذا كانت حالة التشغيل معطلة، فقد يكون ذلك بسبب تعذر إستيراد WAE لمفاتيح SSL من مخزن Central Manager الآمن، إما لأن المخزن الآمن غير مفتوح أو أن الإدارة المركزية تتعذر الوصول إليها. أستخدم الأمر **show cms info** و**ping** لتأكيد إمكانية الوصول إلى الإدارة المركزية.

شكل 1. التحقق من حالة مسرع SSL



إذا رأيت حالة تشغيل ألأجزاء التشفير العام، فانتظر حتى تصبح الحالة قيد التشغيل، مما قد يستغرق دقائق قليلة بعد إعادة التشغيل. إذا رأيت حالة إستيراد المفاتيح من CM لأكثر من دقائق قليلة، فقد تشير إلى أن خدمة CMS على "الإدارة المركزية" ال تعمل، أو أنه قد يوجد اتصال شبكة بالمدير المركزي، أو أن إصدارات WAAS الموجودة على WAE و Central Manager غير متوافقة، أو أن المخزن الآمن ل Central Manager غير مفتوح.

يمكنك التحقق من تهيئة مخزن الإدارة المركزية الآمن وفتحه باستخدام الأمر **show cms secure-store** كما يلي:

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

في حالة عدم تهيئة المخزن الآمن أو فتحه، ستر أجهزة التنبيه الهامة مثل mstore_key_failure و secure-store. يمكنك فتح المخزن الآمن باستخدام الأمر **cms secure-store**

open أو من المدير المركزي، أختر **Admin > Secure Store**.

تلميح: مق قيثوتب ةملك رورم المخزن الآمن لتجنب الحاجة إلى إعادة ضبط المخزن الآمن إذا نسيت ةملك المرور.

إذا كانت هناك مشكلة في تشفير القرص على WAE، فيمكن أن يمنع ذلك أيضا SSL AO من التشغيل. أستخدم الأمر **show disk details** للتحقق من تمكين تشفير القرص والتحقق من تحميل أقسام "المحتوى" و SPOOL. في حالة تحميل هذه الأقسام، فإنها تشير إلى إسترداد مفاتيح تشفير القرص بنجاح من "الإدارة المركزية" ويمكن تخزين البيانات المشفرة وقراءتها من الأقراص. إذا كان الأمر **show disk details** يظهر "تهيئة النظام"، يشير إلى أنه لم يتم إسترداد مفاتيح التشفير من "الإدارة المركزية" ولم يتم تحميل الأقراص بعد. لن يوفر WAE خدمات تسريع في هذه الحالة. إذا لم يتمكن WAE من إسترداد مفاتيح تشفير القرص من "الإدارة المركزية"، سيقوم بتشغيل تنبيه.

يمكنك التحقق من تكوين خدمة SSL المتسارعة والتحقق من أنها "تمكين" على WAE لمركز البيانات (في الإدارة المركزية، أختر الجهاز، ثم أختر **تكوين > تسريع > SSL خدمات متسارعة**). يجب أن تكون خدمة المعجلة التي تم تكوينها وتمكينها غير نشطة بواسطة مسرع SSL قد تصبح الخدمة المعجلة التي تم تكوينها وتمكينها غير نشطة بواسطة مسرع SSL انظر للشروط التالية:

- تم حذف الشهادة التي تم تكوينها في الخدمة السريعة من WAE. أستخدم الأمر **show running-config** لتحديد الشهادة التي يتم إستخدامها في الخدمة السريعة، ثم أستخدم الأمر **show crypto certificates** و**show crypto certificate-details** للتأكد من أن الشهادة موجودة في مخزن آمن. إذا كانت الشهادة مفقودة، أعد إستيراد الشهادة.
- انتهت صلاحية شهادة الخدمة المعجلة. أستخدم الأمر **show crypto certificates** و**show crypto certificate-details** للتحقق من تاريخ انتهاء صلاحية الشهادة.
- تحتوي شهادة الخدمة المعجلة على خيارات خاصة حل أدبي في المستقبل. أستخدم الأمر **show crypto certificates** و**show crypto certificate-details** وتحقق من قسم الصحة في إخراج الأمر. تأكد أيضا من دقة معلومات ساعة WAE والمنطقة الزمنية.

يمكنك التحقق من أن إتصالات SSL لديها السياسة الصحيحة المطبقة، أي أن لديها تحسين كامل مع تسريع SSL، كما هو موضح في الشكل 2. في الإدارة المركزية، أختر جهاز WAE، ثم أختر **شاشة > تحسين > إحصائيات الاتصالات**.

شكل 2. التحقق من النهج الصحيح على إتصالات SSL

أستخدم الأمر **show running-config** للتحقق من تكوين سياسة حركة مرور بيانات HTTPS. ترى أن تريد أن ترى **DRE no compression none** ل SSL تطبيق إجراء وتريد أن تبحث للشكل صحيح. أنت تريد أن ترى فئة مطابقة مناسبة لمرسدة مصنف HTTPS، كما يلي:

```
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
```

موقت المدخلة النشطة المسرعة بإدراج السياسات الديناميكية المتوافقة مع الخادم ip:port، اسم الخادم:port، أو المجال الخادم:port التي تم تكوينها ضمن المدخلة المسرعة. يمكن فحص هذه لك في DST حقل يشير. show policy-engine application dynamic الأمر باستخدام السياسات بالنسبة. المعجلة المدخلة مع تطابقين المنفذ والمخادم بالخادم IP إلى موضوعة سياسة DST حقل سيكون ،(443 port ‎*.webex.com مجال الخادم، المثال سبيل على) البدل أحرف لمجال و "Any:443". بالنسبة لتكوين اسم الخادم، يتم إجراء بحث DNS إعادة التوجيه عند تنشيط DNS في مرحلة استجابة في إعادتها تم التي IP عناوين جميع إدراج ويتم السريعة المدخلة المدخلات لكن "داخل المدخلة" مميزة تكون مسرعة مدخلة حيث حالة تتطلب أن مفيد أمر هذا .النهج المدخلات جميع تتعدد ،المثال سبيل على. آخر أطخ بسبب كاملة اهرييصت متي عسرمل المسرعة هادئة بسبب نشطة غير التجميع، وإذا كانت مدخلة التجميع، المدخلة على المستعارة أنها غير نشطة أم أنها، مفوذخة/مدققة المدخلة تمييز أيضا سيتم أنها غير نشطة على المستعارة وتبدو "في المدخلة" في إخراج show running-config. يمكنك التحقق من أن نهج SSL الديناميكي يظهر على WAE مركز البيانات باستخدام الأمر show policy-engine application dynamic. يمكنك التحقق من حالة مدخلة نظير باستخدام أمر show crypto ssl services host-service peering.

يمكن أن يحتوي تكوين المدخلة السريعة SSL AO على أربعة أنواع من إدخالات الخادم:

- IP سكان إستاتيكي (server-ip)—متاح في الإصدار 4.1.3 والإصدارات الأحدث
- يمكنك اصطياد الكل (server-ip any) — متوفر في 4.1.7 والإصدارات الأحدث
- اسم المضيف (اسم الخادم)—متوفر في 4.2.1 والإصدارات الأحدث
- مجال Wildcard (مجال الخادم)—متوفر في 4.2.1 والإصدارات الأحدث

بمجرد تلقي الاتصال من قبل SSL AO، فإنها تقرر أي مدخلة مسرعة يجب استخدامها ثم، الخادم، مجال الخادم، اسم الخادم، ويليه تفضيل على أعلى الثابت IP يكون يعطي. الأداء نحسين الخادم ip any. في حالة عدم تطابق أي من المدخلات المستعارة التي تم تكوينها وتنشيطها عم IP الخادم بالخادم للاتصال، يتم دفع الاتصال إلى فصل الاتصال وحدة التحكم في الوصول (AO) العامة. يتم إستخدام معرف الارتباط الذي يتم إدخاله في مرحلة النهج بواسطة معرف. يعين الاتصال المتطابق الخادم إدخال نوع والمعجلة المدخلة لتحديد SSL AO إرتباط مرحلة النهج هذا هو رقم 32 بت وهو ذو معنى فقط ل SSL AO. يتم إستخدام وحدات بت إلى الأدنى بت وحدات تشير بينما الخادم، مدخلات من مختلفة أنواع إلى للإشارة الأعلى فهرس المدخلة المعجل، كما يلي:

SSL قيم ملف تعريف الارتباط لمرحلة نهج

قيمة ملف تعريف الارتباط	نوع إدخال الخادم	التعليقات
0x8*xxxxx*	عنوان	تكوين عنوان IP الثابت

	IP للخادم	
0x4*xxxxx*	اسم مضيف الخادم	يقوم مركز البيانات WAE بإجراء بحث DNS للأمام لاسم المضيف ويضيف عناوين IP التي يتم إرجاعها إلى تكوين النهج الديناميكي. يتم تحديثها كل 10 دقائق بشكل افتراضي.
0x2FFFFF	اسم الخادم	يقوم مركز البيانات WAE بإجراء بحث DNS عكسي على عنوان IP للمضيف الوجهة لتحديد ما إذا كان مطابق للمجال. إذا تطابقت، يتم تسريع حركة مرور SSL، وإذا لم تتطابق، تتم معالجة حركة المرور وفقا لسياسة HTTPS الثابتة.
0x1*xxxxx*	الخادم أي	يتم تسريع جميع إتصالات SSL باستخدام تكوين الخدمة السريع هذا

مثال 1: الخدمة السريعة مع تكوين الخادم-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
```

يتم إضافة إدخال محرك السياسة المتوافق كما يلي:

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

مثال 2: الخدمة السريعة بتكوين اسم الخادم:

ويتيح هذا التكوين إمكانية النشر بسهولة تامة لتحسين تطبيقات SSL للمؤسسات. وهو قابل للتكيف مع تغييرات تهيئة DNS ويقلل من المهام الإدارية لتقنية المعلومات.

```
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
```

يتم إضافة إدخال محرك السياسة المتوافق كما يلي:

```
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
```

المثال 3: الخدمة المعجلة مع تكوين مجال الخادم:

يسمح هذا التكوين لأجهزة WAAS بتكوين مجال حرف بدل مفرد يتجنب الحاجة إلى معرفة مطابقة (rDNS) العكسية DNS لمركز البيانات WAE يستخدم لجميع الخوادم. عناوين IP. يتجنب تكوين مجال حرف بدل تكوين حركة المرور التي تنتمي إلى المجال الذي تم تكوينه. عناوين IP متعددة، مما يجعل الحل قابل للتطبيق لبنية 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
```

يتم إضافة إدخال محرك السياسة المتوافق كما يلي:

```
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
```

المثال 4: زيادة سرعة الخدمة مع ميزة التهيئة عبر بروتوكول IP للخادم:

يوفر هذه التكوين آلية شاملة. عند تنشيط خدمة مسرعة مع **server-ip أي منفذ 443**، فإنها تسمح بتحسين جميع الاتصالات على المنفذ 443 بواسطة SSL AO. يمكن إستخدام هذه التكوين أثناء نقاط الوصول (POCs) لتحسين جميع حركة مرور البيانات على منفذ معين.

```
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
```

يتم إضافة إدخال محرك السياسة المتوافق كما يلي:

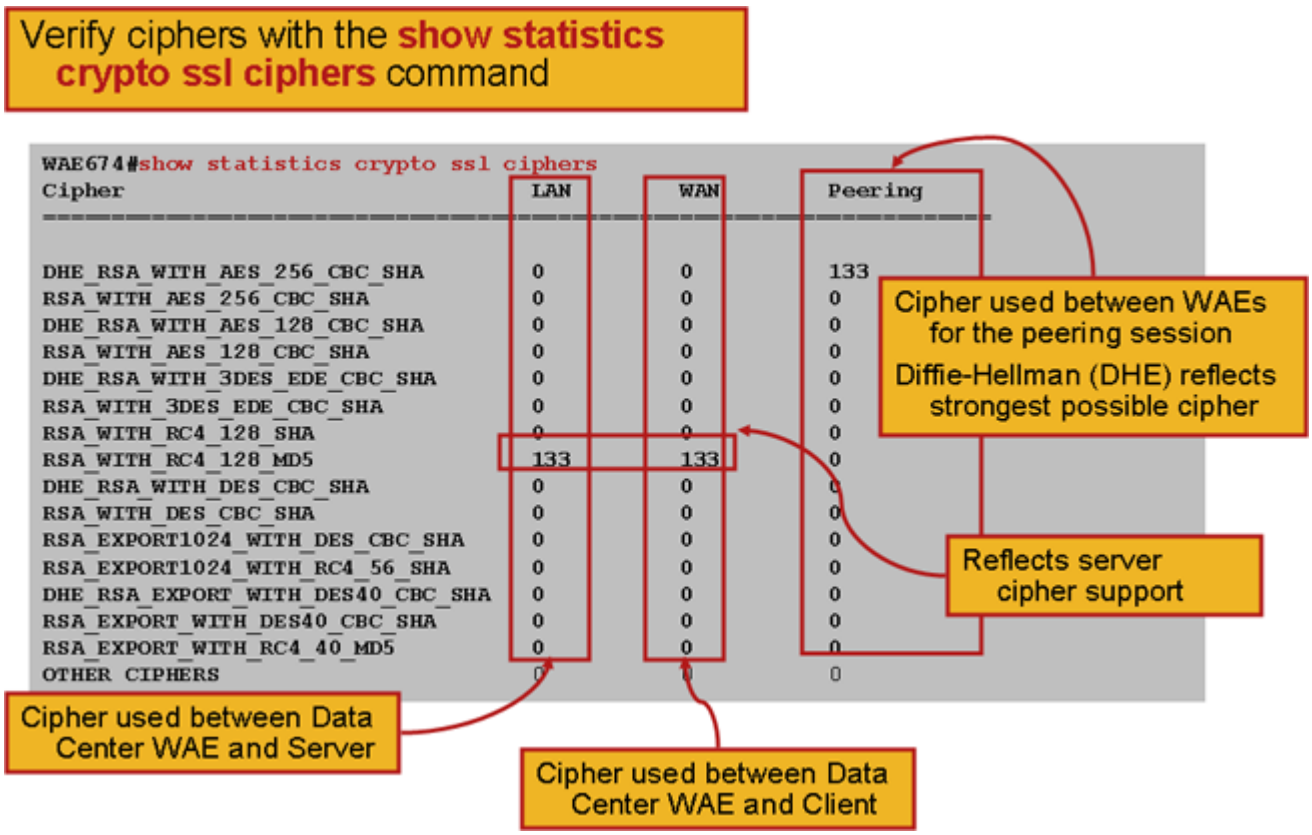
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

يمكنك التحقق من التشفير الذي يتم إستخدامه مع أوامر **show statistics crypto ssl ciphers**، كما هو موضح في الشكل 3.

شكل 3. التحقق من التشفير



يمكنك التحقق من تطابق هذه المشفرات مع تلك التي تم تكوينها على الخادم الأصلي.
ملاحظة: لا تدعم خوادم Microsoft IIS الشفرات التي تتضمن DHE.

على خادم Apache، يمكنك التحقق من إصدار SSL وتفاصيل التشفير في ملف httpd.conf. قد تكون هذه الحقول أيضا في ملف منفصل (sslmod.conf) مشار إليه من httpd.conf. ابحث عن حقلي بروتوكول SSLProtocol و SSLCipherSuite كما يلي:

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

للتحقق من مصدر الشهادة على خادم Apache، أستخدم الأمر openSSL لقراءة الشهادة كما يلي:

```
> 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
```

في المستعرض، يمكنك عرض شهادة وتفاصيلها لتحديد سلسلة الشهادات والإصدار ونوع مفتاح التشفير والاسم الشائع للمصدر (CN) والموضوع/الموقع CN. في Internet Explorer، انقر فوق رمز القفل، ثم انقر فوق **عرض الشهادة**، ثم انظر إلى تبويب مسار الشهادات للحصول على هذه المعلومات.

تتطلب معظم المستعرضات أن تكون شهادات العميل بتنسيق PKCS12 بدلا من تنسيق PEM X509. لتصدير تنسيق X509 PEM إلى تنسيق PKCS12، أستخدم الأمر OpenSSL كما يلي على خادم Apache:

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

إذا تم تشفير المفاتيح الخاصة، تكون عبارة المرور مطلوبة للتصدير. يتم إستخدام كلمة مرور التصدير مرة أخرى لاستيراد بيانات الاعتماد إلى جهاز WAAS.

أستخدم الأمر **show statistics accelerator ssl** لعرض إحصائيات 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              <-------
---------
. . .
```

يمكن أن تكون إحصائيات عمليات التحقق من الشهادات وجلسات العمل الفاشلة مفيدة لاستكشاف الأخطاء وإصلاحها، كما يمكنك إسترجاعها بسهولة باستخدام عامل التصفية التالي على الأمر **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
```

يمكن أن تكون الإحصائيات المتعلقة ب DNS مفيدة لاستكشاف أخطاء اسم الخادم وتكوينه وإصلاحه. لاسترداد هذه الإحصائيات، أستخدم الأمر **show statistics accelerator ssl**، كما يلي:

```
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
 . . .
```

يمكن أن تكون الإحصائيات المتعلقة بإعادة توجيه SSL مفيدة لاستكشاف الأخطاء وإصلاحها ويمكن إسترداده باستخدام عامل التصفية التالي على الأمر **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
```

أستخدم الأمر **show statistics connection optimized ssl** للتحقق من أن جهاز WAAS يقوم بإنشاء إتصالات SSL محسنة. تحقق من ظهور "TDLS" في عمود Accel الصال. يشير "S" إلى إستخدام SSL AO كما يلي:

```
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"
```

يمكنك التحقق من إحصائيات الاتصال للاتصالات المغلقة باستخدام الأمر **show statistics connection closed ssl**.

إذا لم يتم تحسين الاتصالات، فتحقق مما إذا كان WCCP/PBR تم تكوينه ويعمل بشكل

صحيح، وفحص بحث عن التوجيه غير المتماثل.

يمكنك عرض إحصائيات اتصال SSL باستخدام أمر **show statistics connection optimized ssl detail**، حيث سترى النهج الديناميكي الذي ينتج عن خدمة SSL السريعة التي تم تكوينها. **ملاحظة**: السياسة التي تم تكوينها هي تحسين TFO فقط، ولكن يتم تطبيق التحسين الكامل كنتيجة لخدمة SSL التي تم تكوينها.

```
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
. . .
```

في ما بعد في هذا الإخراج، يتم عرض تفاصيل مستوى جلسة عمل SSL الموسعة كما يلي:

```
. . .
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
```

أستكشاف أخطاء إتصالات HTTP AO إلى SSL AO Delivery

إذا كان يجب على العميل الانتقال من خلال وكيل للوصول إلى خادم HTTPS، فيتم أولا توجيه طلب العميل كرسالة اتصال HTTP إلى الوكيل (مع عنوان IP الفعلي لخادم HTTPS المضمن في رسالة CONNECT). عند هذه النقطة، تتعامل HTTP AO مع هذا الاتصال على WAEs النظيرة. يقوم الوكيل بإنشاء نفق بين العميل والخادم المنفذ ويرسل البيانات التالية بين العميل وعنوان IP ذلك الخادم والمنفذ. يرد الوكيل على العميل برسالة "200 موافق" ويتم سحب الاتصال إلى SSL AO لأن العميل يعتزم التحدث مع الخادم عبر SSL. بعد ذلك يقوم العميل ببدء مصافحة SSL مع خادم SSL عبر اتصال TCP (النفق) الذي تم إعداده بواسطة الوكيل.

تحقق من الأمور التالية عند أستكشاف المشكلات المتعلقة باتصالات التسليم وإصلاحها:

- تحقق من إخراج الأمر **show statistics accelerator http** لتأكيد معالجة اتصال HTTP بواسطة AO ثم تم تسليمه إلى SSL AO. راجع إجمالي الاتصالات التي تمت معالجتها وإجمالي الاتصالات التي تم تسليمها إلى عدادات SSL. إذا كانت هناك أي مشاكل، فتحقق مما

يلي:
  - تم تمكين HTTP AO وفي حالة التشغيل على WAEs النظيرة.
  - يتم تكوين خدمة SSL المستمرة باستخدام المنفذ المستخدم من قبل العميل في عنوان URL الخاص بالاتصال (أو المنفذ الضمني 443 إذا كان HTTPS قيد الاستخدام). إلا إذا كان عنوان URL الخاص بالاتصال يحدد منفذ مختلفا عن منفذ الوكيل يكون منفذ الوكيل ما لم يحدد غالبا ضمنيا. ومع ذلك، يجب أن يتم تكوين منفذ الوكيل هذا في خدمة مسرعة SSL. يتم تعيين ه على HTTP AO الذي يتم تعيين حركة المرور الوكيل في تصنيف الوكيل.
- تحقق من إخراج الأمر **show statistics accelerator http** للتأكد من معالجة هذه الاتصالات وتحسينه بواسطة SSL AO. انظر إلى إجمالي الاتصالات التي تمت معالجتها وإجمالي عدادات الاتصالات المحسنة. إذا لم تكن عدادات الإحصائيات صحيحة، فقم باتباع أسلوب تنفيذ استكشاف أخطاء SSL الأساسية وإصلاحها كما هو موضح في القسم السابق.
- على Data Center WAE، تحقق من أن إخراج الأمر **show statistics connection optimized detail** يعرض اسم المضيف وعنوان IP ومنفذ TCP الفعلي لخادم SSL. إذا لم يتم تعيين هذه الحقول بشكل صحيح، فتحقق مما يلي:
  - تحقق من صحة إعدادات وكيل مستعرض العميل.
  - تحقق من تكوين خادم DNS على WAE لمركز البيانات ومن إمكانية الوصول إليه. يمكنك تكوين خادم DNS على WAE باستخدام الأمر **ip name-server *a.b.c.d***.

التحقق من شهادة الخادم وإصلاحها

يتطلب التحقق من شهادة الخادم إستيراد شهادة CA الصحيحة إلى WAE لمركز البيانات.

لاستكشاف أخطاء التحقق من شهادة الخادم وإصلاحها، اتبع الخطوات التالية:

1. افحص شهادة الخادم واسترداد اسم المصدر. يجب أن يتطابق اسم المصدر هذا الموجود في شهادة الخادم مع اسم الموضوع الموجود في شهادة المرجع المصدق المطابقة. إذا كانت لديك شهادات PEM مرمزة، يمكنك إستخدام الأمر **openssl** التالي على خادم مثبت عليه OpenSSL:

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

2. تأكد من وجود تكوين PKI المطابق على WAE لمركز البيانات باستخدام الأمر **show running-config**. للحصول على شهادة CA يتم إستخدامها من قبل WAE في عملية التحقق، يلزم وجود عنصر تكوين PKI تشفير لكل شهادة CA يتم إستيرادها. على سبيل المثال، إذا تم إستيراد شهادة شركة CA1.ca، فيجب إجراء التكوين التالي على WAE لمركز البيانات:

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

ملاحظة: إذا تم إستيراد شهادة CA باستخدام واجهة المستخدم الرسومية (GUI) للمدير المركزي، فإن المدير المركزي يضيف تكوين PKI المشفر أعلاه تلقائيا لتضمين شهادة CA المستوردة. ومع ذلك، إذا تم إستيراد شهادة CA عبر واجهة سطر الأوامر، ستحتاج إلى إضافة التكوين أعلاه يدويا.

3. إذا كانت الشهادة التي يتم التحقق منها تحتوي على سلسلة شهادات، فتأكد من أن سلسلة الشهادات متماسكة، ومن إستيراد شهادة CA المصدر الأعلى على WAE. أستخدم الأمر **openSSL verify** للتحقق من الشهادة بشكل مستقل أولا.

4. إذا فشل التحقق، فافحص سجل تصحيح أخطاء مسرع SSL. أستخدم الأوامر التالية لتمكين تسجيل تصحيح الأخطاء:

```
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. ابدأ إختبار الاتصال ثم اختبر ملف السجل /local/local1/errorlog/sslao-errorlog.current. يجب أن يشير هذا الملف إلى اسم المصدر الذي تم تضمينه في شهادة الخادم. تأكد من تطابق اسم المصدر هذا تمامًا مع اسم موضوع شهادة المرجع المصدق.

في حالة وجود أي أخطاء داخلية أخرى في السجلات، قد يكون من المفيد تمكين خيارات تصحيح أخطاء إضافية.

6. حتى في حالة مطابقة اسم المصدر أو اسماء الموضوعات، قد لا تكون شهادة المرجع المصدق هي الشهادة الصحيحة. في مثل هذه الحالات، إذا تم إصدار شهادة الخادم من مرجع مصدق معروف، يمكن إستخدام المستعرض للوصول مباشرة (دون WAAS) إلى الخادم. عندما يقوم المستعرض بإعداد الاتصال، يمكن فحص الشهادة بالنقر فوق رمز القفل الذي يظهر في أسفل يمين نافذة المستعرض أو داخل شريط عنوان المستعرض. قد تشير تفاصيل الشهادة إلى شهادة المرجع المصدق المناسبة المطابقة لشهادة الخادم هذه. تحقق من حقل الرقم التسلسلي داخل شهادة المرجع المصدق. يجب أن يتطابق هذا الرقم التسلسلي مع الرقم التسلسلي للشهادة التي تم إستيرادها على WAE لمركز البيانات.

7. إذا تم تمكين التحقق من إبطال OCSP، قم بتعطيله والتحقق من أن التحقق من الشهادة يعمل في حد ذاته. للحصول على تعليمات حول أستكشاف أخطاء إعدادات OCSP وإصلاحها، راجع قسم "أستكشاف أخطاء OCSP وإصلاحها عند إبطال".

التحقق من شهادة العميل وإصلاحها

قد تم تمكين التحقق من شهادة العميل على الخادم الأصلي و/أو على WAE لمركز البيانات. عند إستخدام WAAS لتسريع حركة مرور SSL، فإن شهادة العميل التي تم إستقبالها بواسطة الخادم الأصلي هي الشهادة المشار إليها في الأمر machine-cert-key المحدد في الأمر **crypto ssl services global-settings** على شهادة WAE لمركز البيانات أو شهادة WAE الخاصة بجهاز مركز البيانات، إذا لم يتم تكوين Machine-cert-key. ونتيجة لذلك، إذا فشلت عملية التحقق من شهادة العميل على الخادم الأصلي، فقد يكون ذلك بسبب عدم إمكانية التحقق من شهادة جهاز WAE لمركز البيانات على الخادم الأصلي.

إذا لم يكن التحقق من شهادة العميل في WAE مركز البيانات يعمل، فمن المحتمل أن يكون ذلك بسبب عدم إستيراد شهادة CA المطابقة لشهادة العميل في WAE مركز البيانات. راجع قسم "التحقق من شهادة خادم أستكشاف الأخطاء وإصلاحها" للحصول على تعليمات حول كيفية التحقق من وجود شهادة CA صحيحة تم إستيرادها على WAE.

أستكشاف أخطاء التحقق من شهادة WAE النظير وإصلاحها

لاستكشاف أخطاء التحقق من شهادة النظير وإصلاحها اتبع الخطوات التالية:

1. تأكد من أن الشهادة التي يتم التحقق منها هي شهادة CA موقعة. ال يمكن التحقق من شهادة موقعة ذاتيا من قبل WAE آخر من قبل WAE. يتم تحميل WAEs بشكل افتراضي باستخدام شهادات موقعة ذاتيا. يجب تكوين شهادة موقعة ذاتيا باستخدام الأمر **crypto ssl services global-settings machine-cert-key**.

2. تحقق من تحميل شهادة المرجع المصدق الصحيحة على الجهاز الذي يقوم بالتحقق من الشهادة. على سبيل المثال، إذا تم تكوين Peer-cert-verify على WAE الخاص بمركز البيانات،

فمن الضروري أن تكون شهادة WAE الفرعية موقعة من CA، كما يجب إستيراد نفس شهادة CA's الموقعة على WAE الخاص بمركز البيانات. التنسيق إنشاء مرجع مصدق باستخدام الأمر **crypto pki ca** للاستخدام الشهادة المستوردة، إذا كنت تستورد الشهادة يدوياً من خلال CLI (واجهة سطر الأوامر). عند الاستيراد بواسطة واجهة المستخدم الرسومية (GUI) الخاصة بالمدير المركزي، يقوم المدير المركزي تلقائياً بإنشاء تكوين PKI مشفر مطابق.

3. في حالة إستمرار فشل التحقق من WAE النظير، فتحقق من سجلات تصحيح الأخطاء كما هو موضح في قسم "تسجيل SSL AO".

أستكشاف أخطاء OCSP وإصلاحها عند إلغاء الفحص

إذا كان النظام يواجه مشكلة في إجراء إتصالات SSL ناجحة مع تمكين التحقق من إبطال بروتوكول حالة الشهادة عبر الإنترنت (OCSP)، اتبع خطوات أستكشاف الأخطاء وإصلاحها التالية:

1. تأكد من تشغيل خدمة المستجيب OCSP على خادم المستجيب.
2. تأكد من الاتصال الجيد بين WAE والمستجيب. استعملت **العملية زيارة** وtelnet أمر (إلى الميناء مناسب) من ال WAE أن يفحص.
3. تأكد من أن الشهادة التي يتم التحقق من صحتها صحيحة بالفعل. عادة ما يكون تاريخ انتهاء الصلاحية وعنوان URL الخاص بالمستجيب الصحيح من المناطق التي توجد بها مشاكل.
4. تحقق من إستيراد الشهادة الخاصة باستجابات OCSP على WAE. كما يتم توقيع الردود الواردة من المستجيب OCSP ويجب أن تكون شهادة CA المطابقة لاستجابات OCSP موجودة على WAE.
5. تحقق من إخراج الأمر **show statistics accelerator ssl** للتحقق من إحصائيات OCSP والتحقق من العدادات المقابلة لفشل OCSP.
6. إذا كان اتصال OCSP HTTP يمر عبر وكيل HTTP، فحاول تعطيل الوكيل لمعرفة ما إذا كان يساعد. إذا كان هذا الإجراء مفيداً، فتحقق من أن تكوين الوكيل ال يتسبب في فشل الاتصال. إذا كان تكوين الوكيل جيداً، فقد يكون هناك بعض خصوصية رأس HTTP والتي قد تتسبب في بعض عدم التوافق مع الوكيل. التقاط تتبع حزمة لمزيد من التحقيق.
7. إذا فشل الكل الآخر، فقد تضطر إلى التقاط تتبع حزمة لطلب OCSP الصادر لمزيد من تصحيح الأخطاء. يمكنك إستخدام أوامر **tcpdump** أو **tethereal** كما هو موضح في القسم "التقاط الحزم وتحليلها" في مقالة أستكشاف الأخطاء وإصلاحها في WAAS الأولية.

تم اشتقاق عنوان URL المستخدم من قبل WAE لمركز البيانات للوصول إلى مستجيب OCSP بإحدى الطريقتين:

- ال ساكن إستاتيكي OCSP URL يشكل ب **ال crypto PKI شامل عملية** تشكيل أمر
- عنوان OCSP المحدد في الشهادة التي يتم فحصها

إذا كان عنوان URL مشتق من الشهادة التي يتم فحصها، فمن الضروري التأكد من إمكانية الوصول إلى عنوان URL. قم بتمكين سجلات تصحيح أخطاء OCSP لمسرع SSL لتحديد عنوان URL ثم تحقق من الاتصال بالمستجيب. راجع القسم التالي للحصول على تفاصيل حول إستخدام سجلات التصحيح.

أستكشاف أخطاء تكوين DNS وإصلاحها

إذا كان النظام يواجه مشكلة في تحسين إتصالات SSL باسم الخادم وتكوينات مجال الخادم، فاتبع خطوات أستكشاف الأخطاء وإصلاحها التالية:

1. تأكد من إمكانية الوصول إلى خادم DNS الذي تم تكوينه على WAE وإمكانية حل الأسماء. استخدم الأمر التالي للتحقق من خادم DNS الذي تم تكوينه:

```
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 !
```

تشير هذه الاستجابة إلى عدم إمكانية حل الاسم بواسطة خوادم الأسماء التي تم تكوينها.

حاول إختبار الاتصال/traceoute لخوادم الأسماء التي تم تكوينها للتحقق من إمكانية الوصول إليها وتوقيت الذهاب والعودة.

```
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. إذا كان خادم DNS يمكن الوصول إليه ويمكنه حل الأسماء ومع ذلك لم يتم تحسين إتصالات SSL، فتأكد من أن الخدمة السريعة التي يتم تكوينها بموقع المجال المحدد أو اسم المضيف نشطة ولا يوجد أي تنبيهات ل SSL AO. أستخدم الأوامر التالية:

```
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
```

يشير وجود تنبيه "acl_svc_inactive" إلى وجود بعض الاختلافات في تكوين الخدمة السريعة. تحقق من وجود أخطاء في تكوين الخادم أو أكثر من خدمة سريعة واحدة وقد يكون هناك خطأ في إدخالات الخادم. تحقق من صحة التكوين. أستخدم الأمر التالي للتحقق من التكوين وتأكد من تكوين الخدمة المعجل:

```
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
```

للتحقق من تفاصيل حول خدمة معينة مسرعة، أستخدم الأمر التالي:

```
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
```

أحد الأسباب التي قد تكون فيها حالة التشغيل للخدمة المعجلة غير نشطة هو فشل DNS. على سبيل المثال، إذا كان هناك اسم مضيف للخادم في تكوين الخدمة المعجل ولم يتمكن WAE من حل عنوان IP للخادم، فلا يمكن تكوين النهج الديناميكي المناسب.

3. إذا كان عداد الإحصائيات الخاص ب "التوجيه من الخلل بسبب اسم مجال غير مطابق" في تزايد، فهذا يشير إلى أن اتصال SSL خاص بخادم تم تكوينه للتحسين. تحقق من الإدخالات كرحم السياسة باستخدام الأمر التالي:

```
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
```

تحقق من حالة الاتصال باستخدام الأمر **show statistics connection**. يجب أن يظهر الاتصال الأول عرسم TSGDL والاتصالات التالية، حتى مدة صلاحية إدخال نهج TIME_DENY، يجب أن تكون TDL.

4. إذا كان خادم DNS عبر شبكة WAN فيما يتعلق ب WAE مركز البيانات، أو إذا كان وتقت إستجابة DNS العكسي طويل جدا، فقد يتم إسقاط بعض الاتصالات. يعتمد هذا على مهلة العميل وتوقيت إستجابة rDNS. في هذه الحالة، يزيد عداد "عدد عمليات بحث DNS العكسية التي تم إلغاؤها" ويتم إسقاط الاتصال. يشير هذا العضو إلى أن خادم DNS ال يستجيب أو بطيء جدا و/أو NSCD على WAAS ال يعمل. يمكن التحقق من حالة NSCD باستخدام الأمر **show alarms**. نظرا لأن هذه العملية ضعيفة جدا لذلك تحدث في معظم عمليات النشر، من المتوقع أن يكون خادم DNS على نفس شبكة LAN التي يعمل بها مركز البيانات WAE.

أستكشاف أخطاء HTTP وإصلاحها إلى سلسلة SSL AO

ملاحظة: تم تقديم HTTP إلى SSL AO Sequence في الإصدار 4.3.1 من WAAS. ال ينطبق هذا القسم على إصدارات WAAS السابقة.

يسمح التشابك لوحدة التحكم بإدخال وحدة تحكم في الوصول (AO) أخرى في أي وقت الخلال عمر

التدفق، كما يمكن لكل من وحدتي التحكم في الوصول (AO) تطبيق التحسين الخاص بوحدة التحكم في الوصول (AO) بشكل مستقل على التدفق. تختلف سلسلة وحدة التحكم في الوصول عن ميزة التسليم المخصصة لعملية النقل التي توفرها وحدة التحكم في الوصول للبنية الأساسية (WAAS) في إصدارات ما قبل 4.3.1 لأنه مع قيام وحدة التحكم في الوصول (AO) بتوصيل وحدة التحكم في الوصول (AO) الأولى يستمر في تحسين التدفق.

يعالج SSL AO نوعين من الاتصالات:

- BYTE-0 SSL: يستلم SSL AO الاتصال أولا ويكمل مصافحة SSL. وهو يحلل الجزء الأولي من الحمولة للتحقق من أسلوب HTTP. إذا كانت الحمولة تشير إلى HTTP، فإنها تدخل HTTP AO؛ وإذا لم تكن هناك مساحة، فإنها تطبق تحسين TSDL العادي.
- اتصال الوكيل: يتلقى HTTP AO الاتصال أولا. وهو يحدد أسلوب رأس الاتصال في طلب العميل ويدخل SSL AO بعد تأكيد الوكيل باستخدام رسالة 200 OK.

يستخدم SSL AO محلل HTTP خفيف الوزن الذي يكشف طرق HTTP التالية: get، head، post، put، options، trace، copy، lock، إستعراض، bcopy، bmove، mkcol، delete، search، unlock، bdelete، propfind، bpropfind، proppatch، اشتراك، bproppatch، unsubscribe، و x_ms_enumtes. يمكنك إستخدام أمر **debug accelerator ssl parser** لتصحيح أخطاء تتعلق بالمحلل. يمكنك إستخدام الأمر **show stat access ssl payload http/other** لعرض إحصائيات حركة المرور المصنفة استنادا إلى نوع الحمولة.

تلميحات أستكشاف المشكلات وإصلاحها:

1. تأكد من تمكين ميزة HTTPS في تكوين HTTP AO حيث أن هذا مكمل ل HTTP AO. لمزيد من التفاصيل، راجع مقالة [أستكشاف أخطاء HTTP AO وإصلاحها].
2. تحقق من حالة الاتصال باستخدام أمر **show stat connection**. إذا تم تحسينه بشكل صحيح، فيجب أن يعرض بروتوكول THSDL الذي يشير إلى تحسين TCP و HTTP و SSL و DRE-LZ. إذا كان أي من هذه التحسينات غير موجود، فقم بتصحيح الأخطاء بشكل إضافي على هذا المحسن (SSL و HTTP وما إلى ذلك). على سبيل المثال، إذا كانت حالة الاتصال تعرض THDL، فهذا يعني أن تحسين SSL لم يتم تطبيقه على الاتصال. تفاصيل حول مشاكل تصحيح الأخطاء المتعلقة بإتباع SSL AO.
3. تأكد من تمكين SSL AO ومن أنه في حالة التشغيل (راجع القسم ["أستكشاف أخطاء SSL AO وإصلاحها"]).
4. تأكد من عدم وجود أية تنبيهات باستخدام الأمر **show alarms**.
5. إذا لم يتم تحسين حركة مرور SSL، فتأكد من إضافة عنوان IP للخادم أو اسم المضيف أو اسم المجال ومقرر المنفذ كجزء من الخدمة السريعة.
6. تأكد من أن الخدمة المسرعة في الحالة ACTIVE باستخدام الأمر **show crypto ssl services accelerated-service** ***asvc-name*** (راجع قسم ["تكوين DNS] لاستكشاف الأخطاء وإصلاحها).
7. تأكد من أن محرك النهج لديه إدخال لهذا الخادم والمنفذ باستخدام الأمر **show policy-engine application dynamic**.
8. إذا كان الخادم الوجهة يستخدم SSL على منفذ غير افتراضي (الافتراضي هو 443)، فتأكد من عكس ذلك في تكوين محرك السياسة. يعتمد "المدير المركزي" على هذه المعلومات للإبلاغ عن بيانات حركة مرور SSL.
9. تأكد من أن اسم المضيف الذي تم تكوينه يتم الحل إلى عنوان IP صالح باستخدام الأمر **show crypto ssl services accelerated-service** ***asvc-name***. إذا لم يتم العثور على عنوان IP، فتحقق مما إذا كان خادم الاسم قد تم تكوينه بشكل صحيح. تحقق أيضا من إخراج الأمر **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
```

تسجيل دخول SSL AO

تتوفر ملفات السجل التالية لاستكشاف أخطاء SSL AO وإصلاحها:

- ملفات سجل المعاملات: /local1/logs/tfo/working.log (و /local1/log/tfo/tfo_log_*.txt)
- ملفات سجل التصحيح: /local1/errorlog/sslao-errorlog.current (و sslao-errorlog.*)

لتصحيح الأخطاء بشكل أسهل، يجب عليك أولاً إعداد قائمة تحكم في الوصول لتقييد الحزم بمضيف واحد.

```
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
```

لتمكين تسجيل المعاملات، أستخدم أمر تكوين **حركة-log** كما يلي:

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

يمكنك عرض ملف نهاية سجل المعاملات باستخدام الأمر **type-tail** كما يلي:

```
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
```

لإعداد تسجيل تصحيح الأخطاء الخاص ب SSL AO وتمكينه، أستخدم الأوامر التالية.

ملاحظة: تسجيل تصحيح الأخطاء هو وحدة المعالجة المركزية (CPU) المكثفة ويمكن أن يقوم بإنشاء كمية كبيرة من الإخراج. إستعمل هذه الأوامر بحكمة وقليل في بيئة إنتاج.

يمكنك تمكين التسجيل التفصيلي إلى القرص كما يلي:

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

يمكنك تمكين تسجيل تصحيح الأخطاء للاتصالات في قائمة التحكم في الوصول كما يلي:

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

الخيارات الخاصة بتصحيح SSL AO هي كما يلي:

```
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
```

حيحصت ءاطخأ لجس ةياهن ضرع مث SSL تالاصتال ءاطخألا حيحصت ليجست نيكمت كنكمي ءاطخألا امك يلي:

```
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
```

أستكشاف أخطاء أجهزة الإنذار بانتهاء صلاحية الشهادة وإصلاحها على الوحدات النمطية ل NME و SRE

اهتيحالص تهتنا دق ايتاذ عقوملا زاهجلا ةداهش نوكت امدنع تاهيبنت ءاشنإب SSL AO موقت صصخم يمومع زاهج ةداهش نيوكت متي الو (ةيحالصلا ءاهتنا نم اموي 30 نوضغ يف اهنأ وأ) خيرات عم عنصملا نم ايتاذ ةعقوم تاداهش ءاشنإب WAAS جمانرب موقي .WAAS زاهج ىلع ءاهتنا ةيحالص ةدم 5 تاونس نم لوأ ءدب ليغشت زاهجلا WAAS.

ليغشتلا ءدب ءانثأ 2006 رياني 1 ىلإ SRE و WAAS NME تادحو عيمج يف ةعاسلا نييعت مت لوألا، ىلع مغرلا نم نأ ةدحو NME وأ SRE ثدحأ. يدؤي كلذ ىلإ ءاهتنا ةيحالص ةداهشلا ةعقوملا ذاتيا يف 1 رياني/نوناك الثاني 2011، دلويو زاهجلا تاهيبنت ءاهتنا ةيحالص ةداهشلا.

اذإ مل نكت مدختست ةداهش عنصملا ةيضارتفالا كةداهش ةيمومع، الدبو نم كلذ مدختست ةداهش ةصصخم ةدحول مكحتلا يف لوصولا ىلإ ةلاحلا ةقبطلا (SSL AO)، نلف ثدحت ءاهتنا ةيحالص ةداهشلا ةصصخملا امدنع يهتنت اهتيحالص. اضيأ، اذإ ةيحالص ريغ عقوتم كنكميو ثيدحت ةدحو NME وأ SME باستخدام جمانرب ةروص ةديدج تقوو ثيدحتب تقو ىلإ ةعاسلا ةنمازمب تقم ثدحأ خيرات، دقف ال هجاوت هذه ةلكشملا.

نإ ضرع ءاهتنا ةيحالص ةداهشلا وه دحأ تاراذنإلا ةيلاتلا (ةضورعملا انه يف تاجرخم رمأ **show alarms**):

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

وأ

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

تشير واجهة المستخدم الرسومية (GUI) للمدير المركزي إلى الإنذار التالي: "Certificate__waas-self_.p12 ىلع كشو الانتهاء تم تكوينها كوحدة تحكم جهاز في الإعدادات العمومية"

يمكنك إستخدام أحد الحلول التالية لحل هذه المشكلة:

- تكوين شهادة مختلفة للإعدادات العمومية:

```
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
```

- تحديث شهادة المصنع الموقعة ذاتيا بتاريخ انتهاء صلاحية لاحق. يتطلب هذا حل نص تنفيذي يمكنك الحصول عليه بالاتصال ب cisco TAC.

ملاحظة: يتم إصلاح هذه المشكلة عن طريق تحليل تذكير CSCte05426، الصادر في إصدارات برنامج WAAS، الإصدار 4.1.7b، 4.2.3c، و 4.3.3. تم تغيير تاريخ انتهاء صلاحية الشهادة إلى 2037.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).