إستخدام أفضل ممارسات جهاز الويب الآمن

المحتويات

المقدمة

معلومات أساسية

NetworkEnvironment

- ICMP
- جدران الحماية
- إعادة توجيه المسار العكسي للبث الأحادي
- إنتحال عناوين IP باستخدام WCCP

تكوين شبكة SWA

- الواجهات
- توجيه شبكة الإدارة
- تتبع بيانات تلوس
- DNS
- موازنة التحميل
- المصادقة النشطة
- المصادقة الخاملة

تكوين الخدمات

- وكيل ويب
- وكيل HTTPS
- مراقبة حركة مرور الطبقة الرابعة (L4TM)

تكوين النهج

- تعريف
- ملفات تعريف
- سياسات فك التشفير
- سياسات الوصول
- فئات عنوان URL المخصص والخارجي

الإشارات والتنبيهات

- إشارات CLI
- التسجيل
- التقارير المتقدمة لأمان الويب (AWSR)
- التنبيهات بالبريد الإلكتروني
- مراقبة التوفر
- مراقبة SNMP

القرار

المقدمة

يصف هذا المستند أفضل ممارسات كيفية تكوين جهاز الويب الآمن من Cisco (SWA).

معلومات أساسية

يهدف هذا الدليل إلى أن يكون مرجعا لتكوين أفضل الممارسات ويتناول العديد من جوانب نشر SWA، بما في ذلك بيئة الشبكة المدعومة وتكوين السياسة والمراقبة واستكشاف الأخطاء وإصلاحها. في حين أن أفضل الممارسات المذكورة هنا مهمة لجميع الإداريين والمهندسين المعماريين والمشغلين لفهمها، إلا أنها مجرد إرشادات ويجب التعامل معها على هذا الأساس. لكل شبكة متطلباتها وتحدياتها الخاصة.

كجهاز أمان، تتفاعل SWA مع الشبكة بعدة طرق فريدة. وهو مصدر وغاية لحركة مرور الويب. يعمل في نفس الوقت كخادم ويب وعميل ويب. يستخدم هذا الطراز، كحد أدنى، انتحال عناوين IP على جانب الخادم وتقنيات الدخيل لفحص معاملات HTTPS. كما يمكن أن يؤدي إلى انتحال عناوين IP الخاصة بالعميل، مما يضيف طبقة أخرى من التعقيد إلى النشر ويفرض متطلبات إضافية على تكوين الشبكة المدعومة. يتناول هذا الدليل المشاكل الأكثر شيوعا المتعلقة بتكوين جهاز الشبكة ذي الصلة.

إن تكوين سياسة SWA له تبعات ليس فقط على فعالية الأمن وإنفاذه، بل أيضا على أداء الجهاز. يتناول هذا الدليل كيفية تأثير تعقيد تكوين على موارد النظام. ويوضح التعقيدات في هذا السياق وكيفية تقليلها في تصميم السياسات. كما يتم الاهتمام بمميزات معينة وكيف يجب تهيئتها لزيادة الأمان وقابلية التطوير والفعالية.

يوضح قسم المراقبة والتنبيه في هذا المستند أكثر الطرق فعالية لمراقبة الجهاز، كما يغطي مراقبة الأداء والتوفر، بالإضافة إلى إستخدام موارد النظام. كما يوفر معلومات مفيدة في أستكشاف الأخطاء الأساسية وإصلاحها.

بيئة الشبكة

ICMP

اكتشاف وحدة الحد الأقصى للنقل (MTU) للمسار، كما هو محدد في RFC 1191، تحدد الآلية الحجم الأقصى للحزمة على المسارات العشوائية. في حالة IPv4، يمكن للجهاز تحديد وحدة الإرسال القصوى (MTU) لأي حزمة على مسار بضبط وحدة بت عدم التجزئة (DF) في رأس IP للحزمة. إذا تعذر على الجهاز، في إرتباط ما على المسار، إعادة توجيه الحزمة دون تجزئتها، فإن الرسالة (النوع 3، الرمز 4) الخاصة ببروتوكول رسائل التحكم في الإنترنت (ICMP) يتم إرسالها مرة أخرى إلى المصدر. ثم يقوم العميل بإعادة إرسال حزمة أصغر حجما. ويستمر الحال هكذا حتى يتم اكتشاف وحدة الحد الأقصى للنقل (MTU) للمسار الكامل. الدعم IPv6 التجزئة، ويستخدم حزمة كبيرة جدا (النوع 2) من رسائل ICMPv6 للإشارة إلى عدم القدرة على إحتواء الحزمة من خلال إرتباط محدد.

لأن عملية تجزئة الحزم يمكن أن يكون لها تأثيرات شديدة على أداء تدفق TCP، تستخدم SWA اكتشاف وحدة الحد الأقصى للنقل (MTU) للمسار. يجب تمكين رسائل ICMP المذكورة في أجهزة الشبكة ذات الصلة للسماح لـ SWA بتحديد MTU للمسار الخاص بها من خلال الشبكة. يمكن تعطيل هذا السلوك في SWA يستخدم أمر سطر أوامر pathDiscovery (CLI).

يؤدي القيام بذلك إلى انخفاض وحدات الحد الأقصى للنقل (MTU) الافتراضية إلى 576 بايت (لكل RFC 879)، مما يؤثر بشدة على الأداء. يجب أن تتخذ المسؤول الخطوة الإضافية لتكوين وحدة الحد الأقصى للنقل (MTU) يدويا في SWA من أمر واجهة سطر الأوامر (CLI) etherConfig.

في حالة بروتوكول إتصالات ذاكرة التخزين المؤقت للويب (WCCP)، تتم إعادة توجيه حركة مرور بيانات الويب إلى SWA من جهاز شبكة آخر على مسار العميل إلى الإنترنت. في هذه الحالة، ال تتم إعادة توجيه البروتوكولات الأخرى، مثل ICMP، إلى SWA. هناك احتمال أن تؤدي ICMP المطلوبة من موجه على الشبكة، ولكن لن يتم SWA إلى تشغيل رسالة تجزئة تسليم الرسالة إلى SWA. إذا كان هذا الإحتمال في الشبكة، فيجب تعطيل الكشاف وحدة الحد الأقصى للنقل (MTU) للمسار. وكما ذكرنا، عم هذا التكوين، يلزم الخطوة الإضافية لإعداد وحدة الحد الأقصى للنقل (MTU) يدويا على شبكة SWA باستخدام أمر واجهة سطر الأوامر EtherConfig.

جدران الحماية

في التكوين الافتراضي، ال تفسد SWA عنوان IP للعميل عند وكيل اتصال. هذا يعني أن كل حركة مرور الويب الصادرة يتم الحصول عليها من عنوان IP ل SWA. من الضروري التأكد من أن أجهزة ترجمة عنوان الشبكة (NAT) تحتوي على مجموعة كبيرة كافية من العناوين الخارجية والمنافذ لاستيعاب هذا. من الجيد تخصيص عنوان محدد لهذا الغرض.

تستخدم بعض جدران الحماية أجهزة الحماية من رفض الخدمة (DoS) أو ميزات الأمان الأخرى التي تشغيلها عندما يتم الحصول على أعداد كبيرة من الاتصالات المتزامنة من عنوان IP يتم عميل واحد. عند عدم تمكين انتحال عنوان IP للعميل، يجب إستثناء عنوان IP ل SWA من أجهزة الحماية هذه.

إعادة توجيه المسار العكسي للبث الأحادي

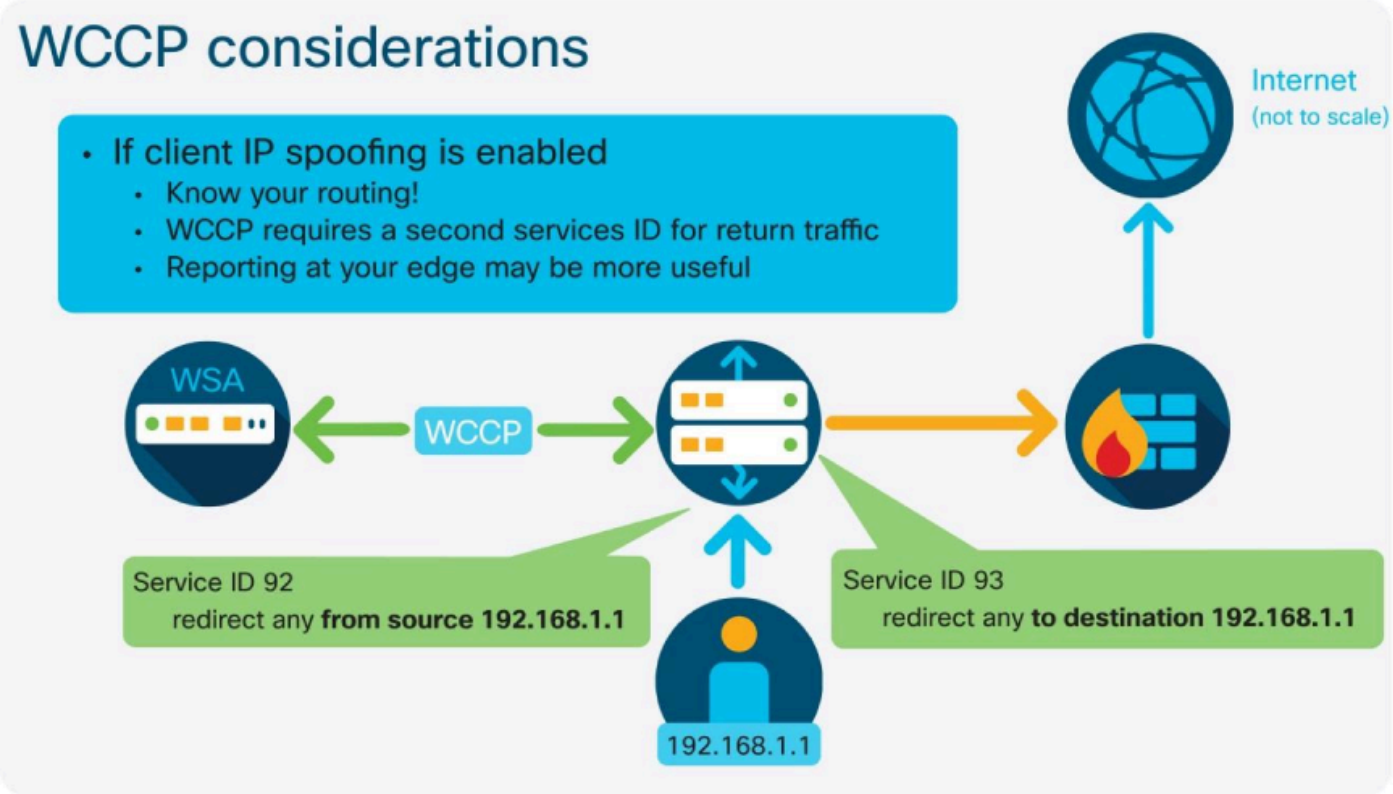
تقوم SWA بمصادرة عنوان IP للخادم عند الاتصال بعميل، ويمكن تكوينها إختياريا ليتم انتحال عنوان IP الخاص بالعميل عند إتصاله بخادم الخادم الخادم. يمكن تمكين أجهزة الحماية مثل إعادة توجيه المسار العكسي للبث الأحادي (uRPF) على المحولات لضمان تطابق الحزمة الواردة مع منفذ المدخل المتوقع. تحقق أجهزة الحماية هذه من واجهة المصدر للحزمة مقابل جدول التوجيه لضمان وصولها إلى المنفذ المتوقع. ويجب إعفاء قانون المرآة من تدابير الحماية هذه عند القضاء.

انتحال عناوين IP باستخدام WCCP

عند تمكين ميزة انتحال عناوين IP في SWA، تترك الطلبات الصادرة الجهاز يستخدم عنوان المصدر الخاص بطلب العميل الأصلي. وهذا يتطلب تكوين إضافي للبنية الأساسية للشبكة ذات الصلة لضمان توجيه حزم الإرجاع إلى واجهة SWA الصادرة، بدلا من العميل الذي أنشأ الطلب.

عند تنفيذ WCCP على جهاز شبكة (موجه أو محول أو جدار حماية)، يتم تعريف معرف الخدمة الذي يطابق حركة المرور استنادا إلى قائمة التحكم في الوصول (ACL). ثم يتم تطبيق

مع الخدمة على واجهة ويتم إستخدامه لمطابقة حركة المرور لإعادة التوجيه. إذا تم تمكين انتحال عنوان IP، يجب إنشاء مع خدمة ثان لضمان إعادة توجيه حركة المرور العائدة أيضا إلى SWA.



تكوين شبكة SWA

الواجهات

يحتوي SWA على خمس واجهات شبكة قابلة للاستخدام: M1، P1، P2، T1، و T2. ويجب الاستفادة من كل من هذه الوسائل لتحقيق غرضها المحدد كلما أمكن ذلك. من المفيد إستخدام كل ميناء لأسبابه الخاصة. يجب توصيل واجهة M1 بشبكة إدارة مخصصة، كما يجب تمكين توجيه التقسيم للحد من تعرض الخدمات الإدارية. يمكن قصر P1 على حركة مرور طلب العميل، على العكس، غير مسموح ل P2 بقبول طلبات الوكيل الصريحة. وهذا يقلل مقدار حركة المرور على كل واجهة ويسمح بتجزئة أفضل في تصميم الشبكة.

يتوفر منفذا T1 و T2 لميزة مراقبة حركة مرور البيانات من الطبقة الرابعة (L4TM). يراقب هذا سمة يعكس طبقة 2 ميناء ويضيف القدرة أن يمنع حركة مرور يؤسس على قائمة ميالن إلى جانب من معروف يضار عنوان والمجال اسم. وهو يقوم بذلك من خالل النظر إلى عنواين IP للمصدر والوجهة لحركة المرور وإرسال حزمة إعادة تعييني TCP، أو رسالة منفذ يتعذر الوصول إليه إذا كانت القائمة المحظورة متطابقة. يمكن حظر حركة المرور المرسلة مع أي بروتوكول باستخدام هذه الميزة.

حتى في حالة عدم تمكين ميزة L4TM، يمكن تحسين المجازة الشفافة عندما T1 و T2 ربطت ميناء إلى يعكس ميناء. في حالة WCCP، تعرف SWA عنوان IP المصدر والوجهة فقط للحزمة

لحب SWA موقت .تامولعملا كلت ىلع ءانب هزواجتت وأ ،اهليومتب ارارق ذختت نأ بجيو ةدراولا ليغشتلل لجسلا ةدم نع رظنلا ضغب ،ةقيقد 30 لك زواجتلا تادادعإ ةمئاق يف تالاخدإ يأ ةربكملا DNS تامالعتسا SWA مدختست نأ نكمي ،L4TM ةزيم نيكمت مت اذإ ،كلذ عمو .(TTL) ويرانيس يف ببسلي أطخ ثودح رطخ نم للقي اذهو .ارتاوت رثكأ لكشب تالجسلا هذه ثيدحتل ثيح ماق العميل لحب ناونع فلتخم نع SWA.

ةرادإلا ةكبش هيجوت

لك نيوكت نكمي ،تنرتنإلا ىلإ لوصولا ةيناكمإ ةصصخملا ةرادإلا ةكبشل رفوتت مل اذإ ،ةكبشلا طاطخم مئالیل ئیاهلا اذه صيصخت نكميو .تانايبلا هيجوت لودج مادختسال ةمدخ تانايبلا ةكبشو ماظنلا تامدخ عيمجل ةرادإلا ةكبش مادختساب ىصوي ،ماع لكشب نكلو نييعت نكمي يتلا تامدخلا نوكت ،AsyncOS نم 11.0 رادصإلا نم اراابتعا .ءالمعلا رورم ةكرحل يه اهل هيجوتلا:

- بيو زجوم URL يجراخلا
- ةراضلا جماربلا نم ةيامحلا فلمل مدقتملا ليلحتلاو ةعمسلا
- تايقرتلاو تاثيدحتلا
- DNS
- طشنلا ليلدلا

ةتباثلا نيوانعلا نيوكت نكمي ،ةرادإلا رورم ةكرحل ةيفاضإ جورخ ةيفصت ىلع لوصحلل :تامدخلا هذه يف مادختسالل

- بيو زجوم URL يجراخلا:
  1. هيف مهتفاضتسإ متي يذلا ناكملا ىلع صصخملا دمتعي
  2. هليلحتو AMP فلم ةعمس
  3- cloud-sa.amp.cisco.com (ةيلامشلا اكيرمأ)
  4. cloud-sa.eu.amp.cisco.com (ابوروأ)
  5- cloud-sa.apjc.amp.cisco.com (ئداهلا طيحملاو ايسآ)

- تايقرتلاو ثيدحتلا:
  1. downloads-static.ironport.com
  2. updates-static.ironport.com

سولات تانايب عبتت

تانايبلا عيمج .ةئشانلاو ةديدجلا تاديدهتلا ديدحتب اديج ةفورعم Cisco Talos ةعومجم .ةدحتملا تايالولا يف تانايبلا زكارم يف اهنيزخت متيو ةفورعم ريغ Talos ىلإ ةلسرملا يدؤت امك ،اهديدحتو بيولا تاديدهت فينصت نيسحت ىلإ SensorBase يف ةكراشملا يدؤت .Cisco نم ىرخألا نامألا لولح ىلإ ةفاضإلاب ،SWA نم لضفأ ةيامح ىلإ

DNS

ةكبش لك فيضتست نأ بجي هنأ (DNS) لاجملا مسا مداخ نامأ تاسرامم لضفأ حرتقت تالاجملا رركتملا ليلحتلل رخآلاو يلحم لاجم لخاد نم ةلوخملا تالجسلل امهدحأ :DNS يللحم ةلاح يف .ةددحم تالاجملا DNS مداوخ نيوكتب SWA حمست ،رمألا اذه باعيتسالو .تنرتنإلا يف عض ،ةرركتملا تامالعتسالاو ةيلحملا تامالعتسالا نم لكل طقف دحاو DNS مداخ رفوت

الاعتبار الحمل الإضافي الذي يضيفه عند إستخدامه لجميع استعلامات SWA. يمكن أن يكون الخيار الأفضل هو إستخدام المحلل الداخلي للمجالات المحلية ومحولات إنترنت الجذر للمجالات الخارجية. وهذا يتوقف على مقدار المخاطر التي تتعرض لها المؤسسة ومدى تسامحه.

بشكل افتراضي، تكون ذاكرة التخزين المؤقت ل SWA لسجل DNS لمدة 30 دقيقة كحد أدنى، بغض النظر عن مدة TTL الخاصة بالسجل. تحتوي المواقع الحديثة التي تستخدم شبكات توصيل المحتوى (CDN) بشكل كبير على سجلات ذات مدة البقاء (TTL) منخفضة نظرا لتغيير عناوين IP الخاصة بها بشكل متكرر. قد يؤدي هذا إلى تخزين عميل مؤقت لعنوان IP واحد لخادم محدد وتخزين SWA المؤقت لعنوان مختلف لنفس الخادم. ولمواجهة ذلك، يمكن خفض مدة البقاء (TTL) الافتراضية ل SWA إلى خمس دقائق من أوامر CLI التالية:

```
SWA_CLI> dnsconfig
...
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]> SETUP
...
Enter the minimum TTL in seconds for DNS cache.
...
```

يجب تكوين خوادم DNS الثانوية في حالة عدم توفر الأساسي. إذا تم تكوين جميع الخوادم بنفس الأولوية، يتم إختيار IP للخادم بشكل عشوائي. وفقا لعدد الخوادم التي تم تكوينها، يمكن أن تختلف مهلة الخادم المحدد. الجدول هو المهلة للاستعلام لما يصل إلى ستة خوادم DNS:

عدد خوادم DNS	مهلة الاستعلام (بالتسلسل)
1	60
2	5، و45
3	45 و 10 و 5
4	45 و 11 و 3 و 1
5	1، 3، 11، 45، 1
6	1، 3، 11، 45، 1، 1

هناك أيضا خيار DNS متقدم يتوفر فقط من خلال CLI. تتوفر هذه الخيارات في CLI باستخدام الأمر advancedProxyConfig > DNS.

حدد أحد الخيارات التالية:

- 0—أستخدم دائما إجابات DNS بالترتيب

- 1—أستخدم العنوان الذي يقدمه العميل ثم DNS
- 2—إستخدام محدود لنظام أسماء النطاقات
- 3—إستخدام DNS محدود للغاية

بالنسبة للخيارين 1 و 2، يتم إستخدام DNS إذا تم تمكين سمعة الويب.

بالنسبة للخيارين 2 و 3، يتم إستخدام DNS لطلبات الوكيل الصريحة، في حالة عدم وجود وكيل تدفق أو في حالة فشل وكيل تدفق البيانات الذي تم تكوينه.

لكل الخيارات، يتم إستخدام DNS عند إستخدام عناوين IP للوجهة في عضوية السياسة.

تتحكم هذه الخيارات في كيفية تقرير SWA على عنوان IP للاتصال به عند تقييم طلب عميل. عند تلقي طلب، ترى SWA عنوان IP للوجهة واسم المضيف. يجب أن تقرر SWA ما إذا كانت تثق في عنوان IP للوجهة الأصلية لاتصال TCP، أو أن تقوم بحل DNS الخاص بها وتستخدم العنوان الذي تم حله. الإعداد الافتراضي هو "0 = إستخدام إجابات DNS دائما بالترتيب"، مما يعني أن SWA ال تثق في العميل في توفير عنوان IP.

- الخيار 1- تحاول SWA عنوان IP الذي يقدمه العميل للاتصال، ولكنها ترجع إلى العنوان الذي تم حله في حالة فشل ذلك. يتم إستخدام العنوان الذي تم تحليله لتقييم النهج (فئة ويب وسمعة الويب وما إلى ذلك).
- الخيار 2- ال تستخدم SWA إال العنوان الذي يقدمه العميل للاتصال وال تتراجع عنه. يتم إستخدام العنوان المحدد لتقييم النهج (فئة ويب وسمعة الويب وما إلى ذلك).
- الخيار 3- ال تستخدم SWA إال العنوان الذي يقدمه العميل للاتصال وال تتراجع عنه. يتم إستخدام عنوان IP الذي يقدمه العميل لتقييم النهج (فئة ويب وسمعة الويب وما إلى ذلك).

يعتمد الخيار المختار على مقدار الثقة التي يجب أن يضعها المسؤول في العميل عند تحديد العنوان الذي تم تحليله السم المضيف المحدد. إذا كان العميل وكيل تدفق، فأختر الخيار 3 لتجنب زمن الوصول الإضافي لعمليات بحث DNS غير الضرورية.

موازنة التحميل

يسمح WCCP بموازنة حمل حركة المرور الشفافة عند إستخدام ما يصل إلى ثمانية أجهزة. وهو يسمح بموازنة تدفقات حركة مرور البيانات استنادا إلى التجزئة أو القناع، ويمكن ترجيحه في حالة وجود مزيج من طرز الأجهزة في الشبكة، كما يمكن إضافة الأجهزة وإزالتها من تجمع الخدمات دون وقت توقف عن العمل. وبمجرد أن تتجاوز الحاجة ما يمكن معالجته باستخدام ثمانية معايير SWA، يوصى باستخدام موازن حمل مخصص.

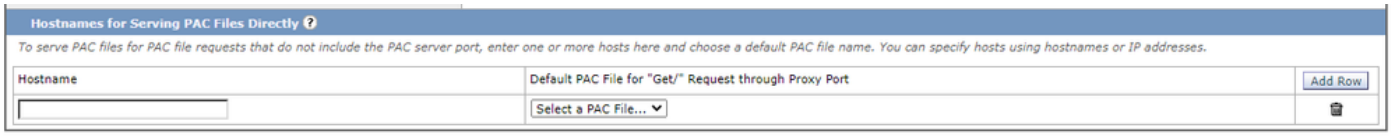
تختلف أفضل الممارسات المحددة لتكوين WCCP بناء على النظام الأساسي المستخدم. بالنسبة لمحوالت Cisco Catalyst® switches، يتم توثيق أفضل الممارسات في التقرير الرسمي لحل الوصول الفوري من Cisco Catalyst .

WCCP له قيود عند إستخدامه مع جهاز الأمان القابل للتكيف (ASA) من Cisco. تحديدا، انتحال عناوين IP الخاصة بالعميل غير مدعوم. وبالإضافة إلى ذلك، يجب أن يكون العمالء ونهج الوصول الموحد وراء نفس الواجهة. ولهذا السبب، يكون إستخدام محول أو موجه من الطبقة

الرابعة إلعادة توجيه حركة مرور البيانات أكثر مرونة. يتم وصف تكوين WCCP على منصة ASA في [WCCP على ASA: المفاهيم والحدود والتكوين.]

بالنسبة لعمليات النشر الواضحة، يكون ملف التكوين التلقائي للوكيل (PAC) وهو الطريقة الأكثر انتشارا، ولكنه يحتوي على العديد من العيوب والآثار الأمنية التي تقع خارج نطاق هذا المستند. إذا تم نشر ملف مسوغات الوصول المحمي، فمن المقترح إستخدام كائنات نهج المجموعة (GPOs) لتكوين الموقع بدلا من الاعتماد على بروتوكول الكشف التلقائي لوكيل الويب (WPAD) الذي يعد ده افا مشتركا للمهاجمين ويمكن إستخدامه بسهولة إذا تم تكوينه بشكل غير صحيح. يمكن أن تستضيف SWA ملفات PAC متعددة وتتحكم في انتهاء صلاحيتها في ذاكرة التخزين المؤقت للمستعرض.

يمكن طلب ملف مسوغات وصول محمي مباشرة من SWA من رقم منفذ TCP قابل للتكوين (9001 بشكل افتراضي). إذا لم يتم تحديد منفذ، يمكن إرسال الطلب إلى عملية الوكيل نفسها كما لو كان طلب ويب صادر. في هذه الحالة، من الممكن خدمة ملف PAC معين استنادا إلى رأس مضيف HTTP الموجود في الطلب.



يجب تكوين Kerberos بشكل مختلف عند إستخدامه في بيئة عالية التوفر. توفر SWA الدعم لملفات عالمة التبويب الرئيسية، والتي تسمح باقتران أسماء المضيف المتعددة باسم قاعدة الخدمة (SPN). لمزيد من المعلومات، راجع [إنشاء حساب خدمة في Windows Active Directory لمصادقة Kerberos في عمليات النشر عالية التوفر] .

المصادقة النشطة

Kerberos هو بروتوكول مصادقة أكثر أمانا ومدعوما بشكل واسع من موفر دعم أمان مدير شبكة LAN NT (NTLMSSP). الدعم نظام التشغيل Apple OS X لبروتوكول NTLMSSP، ولكن يمكن إستخدام Kerberos للمصادقة في حالة انضمام المجال. يجب عدم إستخدام المصادقة الأساسية، حيث إنها ترسل بيانات الاعتماد غير مشفرة في رأس HTTP ويمكن تشميمها بسهولة بواسطة المهاجم على الشبكة. إذا كان يجب إستخدام المصادقة الأساسية، فيجب تمكين تشفير بيانات الاعتماد لضمان إرسال بيانات الاعتماد عبر نفق مشفر.

يجب إضافة أكثر من وحدة تحكم بالمجال إلى التكوين لضمان التوفر، ولكن الا يوجد موازنة أحمال مدمجة لحركة المرور هذه. توقوم SWA بإرسال حزمة TCP syn إلى جميع وحدات التحكم بالمجال التي تم تكوينها ويتم إستخدام أول إستجابة للمصادقة.

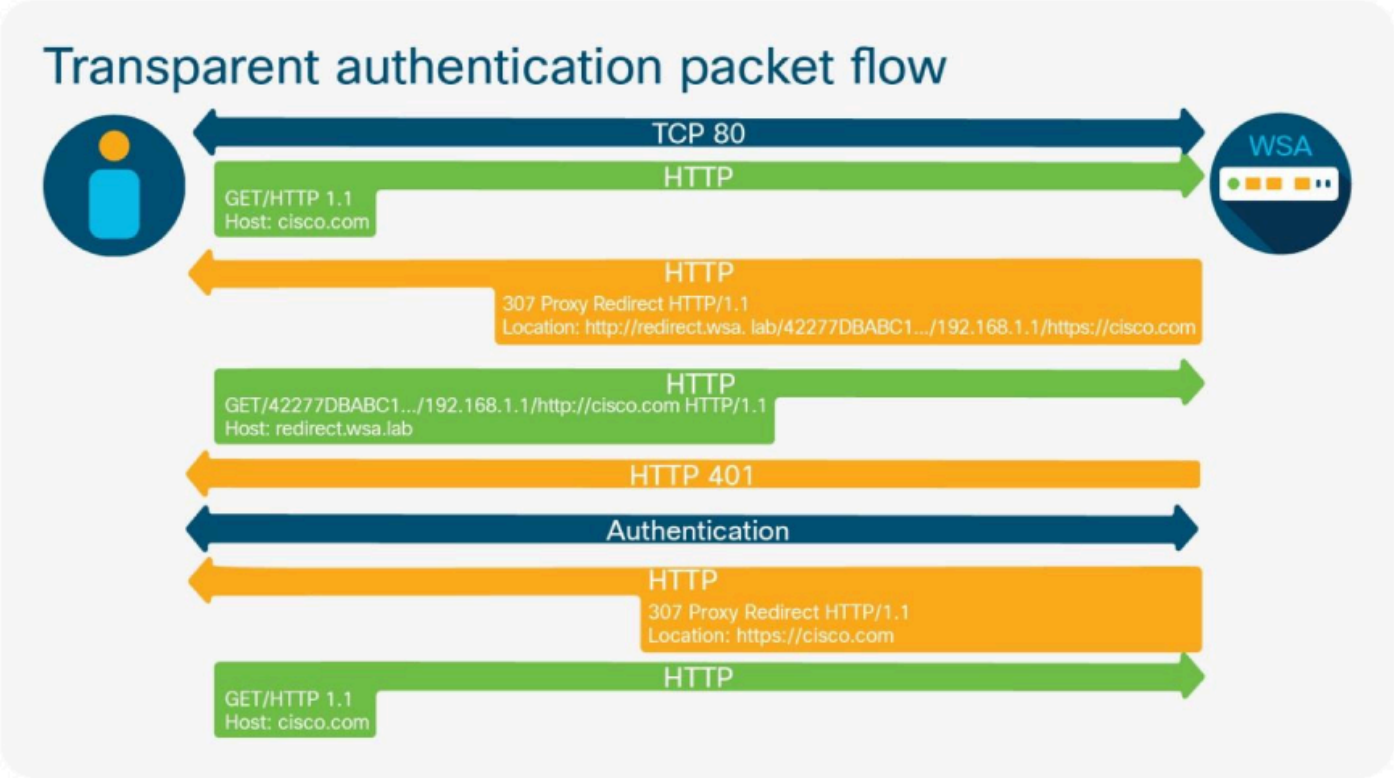
يحدد اسم المضيف المعاد توجيهه الذي تم تكوينه في صفحة إعدادات المصادقة مكان إرسال عميل شفاف من أجل إكمال المصادقة. لكي يتمكن عميل Windows من إكمال المصادقة بسلاسة وتحقيق تسجيل الدخول الأحادي (SSO)، يجب أن يكون اسم المضيف المعاد توجيهه في منطقة المواقع الموثوق بها في لوحة التحكم خيارات الإنترنت. يتطلب بروتوكول Kerberos إستخدام اسم المجال المؤهل بالكامل (FQDN) لتحديد موارد المهام، مما يعني عدم إستخدام "shortName" (أو اسم "netbios") إذا كان Kerberos هو آلية المصادقة المقصودة.

يجب إضافة FQDN ويدوياً إلى المواقع الموثوق بها (على سبيل المثال، من خلال نهج المجموعة). وبالإضافة إلى ذلك، يجب تعيين تسجيل الدخول التلقائي باسم المستخدم وكلمة المرور في لوحة تحكم خيارات الإنترنت.

كما يلزم وجود إعدادات إضافية في Firefox لكي يتمكن المستعرض من إكمال المصادقة باستخدام بروكسيات الشبكة. يمكن تكوين هذه الإعدادات في صفحة about:config. لكي تكتمل Kerberos بنجاح، يجب إضافة اسم المضيف لإعادة التوجيه إلى الخيار network.negotiate-auth.trusted-uris. بالنسبة لـ NTLMSSP، يجب إضافته إلى خيار network.auto-ntlm-auth.trusted-uris.

يتم استخدام بادئ المصادقة لتذكر مستخدم تمت مصادقته لمدة معينة بعد اكتمال المصادقة. يجب استخدام بادئ IP كلما أمكن ذلك للحد من عدد أحداث المصادقة النشطة التي تحدث. مصادقة عميل بشكل نشط هي مهمة كثيفة الموارد، خاصة عند استخدام Kerberos. المهلة البديلة هي 3600 ثانية (ساعة واحدة) بشكل افتراضي ويمكن خفضها، ولكن أقل قيمة موصى بها هي 900 ثانية (15 دقيقة).

تظهر هذه الصورة كيفية استخدام "redirect.wsa.lab" كاسم المضيف المعاد توجيهه:



المصادقة الخاملة

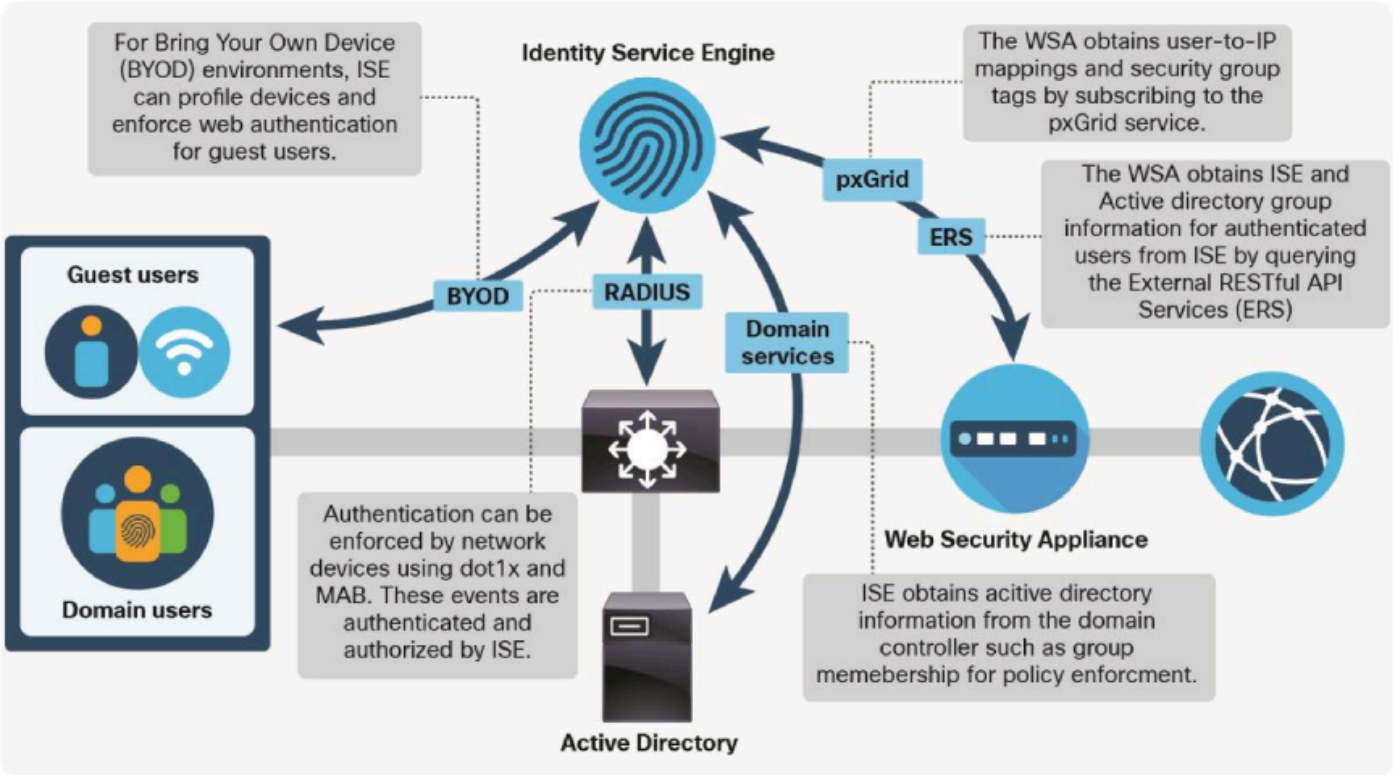
يمكن أن تستفيد SWA من منصات أمان Cisco الأخرى لتحديد مستخدمي الويب بشكل سلبي. تؤدي ميزة التعرف على المستخدمين بشكل خامل إلى التخلص من الحاجة إلى مواجهة تحدي للمصادقة المباشرة وأي اتصال عبر خدمة Active Directory من خلال إدارة الاتصال بالشبكة (SWA)، مما يقلل بدوره من زمن الوصول ومن استخدام الموارد على الجهاز. تتم الآليات المتوفرة حالياً للمصادقة السلبية من خلال وكيل دليل السياق (CDA)

ومحرك خدمات الهوية (ISE) وموصل الهوية الخامل لموصل خدمات الهوية (ISE-PIC).

ISE منتج غني بالميزات يساعد المسؤولين على تمركز خدمات المصادقة الخاصة بهم والاستفادة من مجموعة شاملة من عناصر التحكم في الوصول إلى الشبكة. عندما يتعرف ISE على حدث مصادقة المستخدم (إما من خلال مصادقة Dot1x أو إعادة توجيه مصادقة الويب)، فإنه يقوم بتعميم قاعدة بيانات جلسة عمل تحتوي على معلومات حول المستخدم والجهاز المشمول في المصادقة. تتصل SWA ب ISE عبر Platform Exchange Grid (pxGrid) وتحصل على علامة مجموعة الأمان (SGT) المرتبطة باتصال الوكيل. بما أن AsyncOS صيغة 11.7، يمكن أن تستفسر SWA أيضا عن خدمة إعادة الاستخدام الخارجية (ERS) على ISE للحصول على معلومات المجموعة.

الإصدارات المقترحة هي ISE 3. 1 و SWA 14. 0.2-X والإصدارات الأحدث، للحصول على مزيد من المعلومات حول مصفوفة توافق ISE ل SWA، راجع مصفوفة توافق ISE ل Secure Web Appliance .

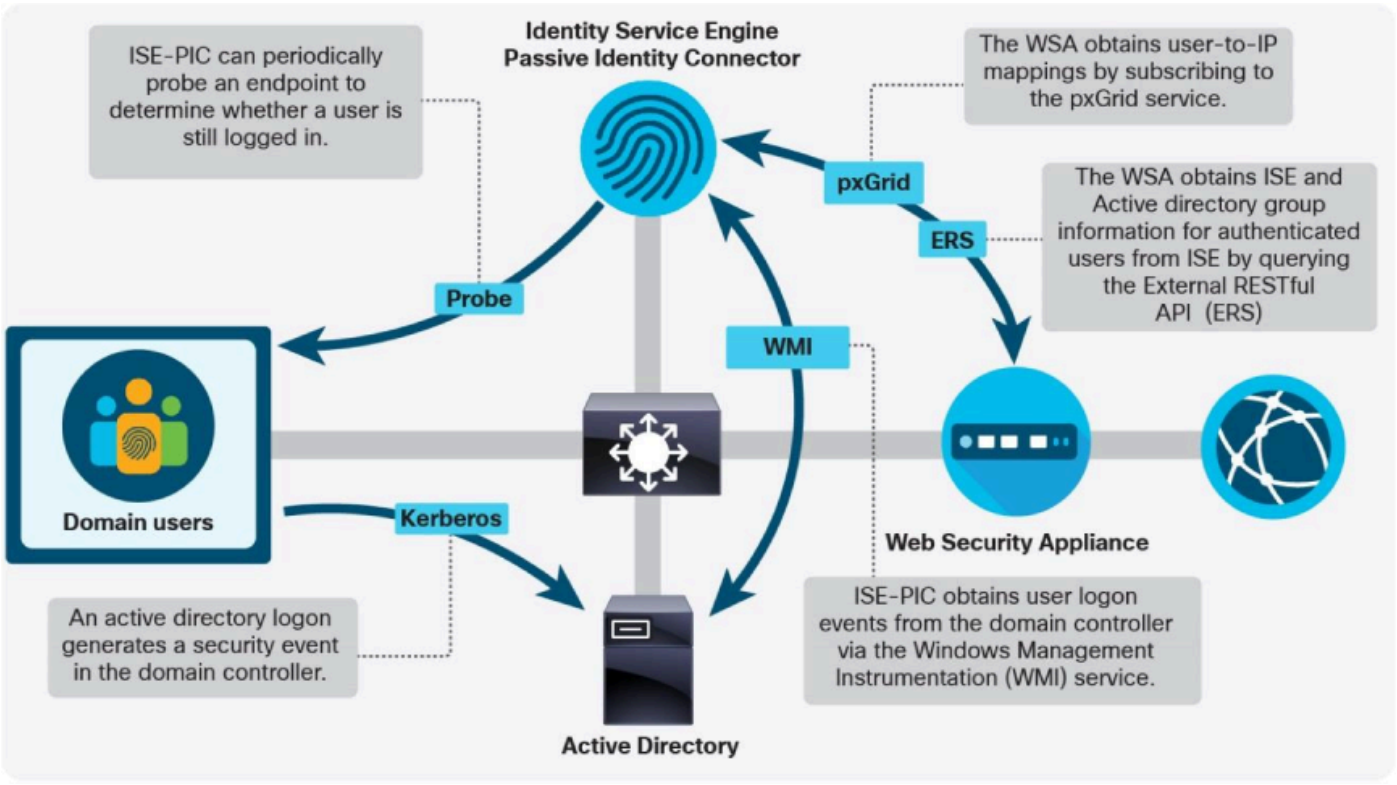
لمزيد من المعلومات حول خطوات التكامل الكامل، راجع دليل المستخدم النهائي لجهاز أمان الويب.



تعلن Cisco نهاية العمر لبرنامج عميل دليل السياق (CDA) من Cisco، راجع دليل وكيل السياق (CDA) من Cisco.

حتى حزمة CDA 6، متوافقة مع Microsoft Server 2016. ومع ذلك، يتم تشجيع المسؤولين WMI بشكل نشط على ترحيل عمليات نشر CDA إلى ISE-PIC. يستخدم الحلين الـ IP (تعرف باسم للاشتراك في سجل أحداث أمان Windows لإنشاء تعيينات من مستخدم إلى "جلسات العمل"). في حالة CDA، تستعلم SWA عن هذه التعيينات باستخدام RADIUS. في حالة ISE-PIC، يتم إستخدام نفس إتصالات PxGrid و ERS كما هو الحال في نشر ISE الكامل.

تتوفر وظائف ISE-PIC في تثبيت ISE بالكامل، وكذلك في جهاز ظاهري مستقل.

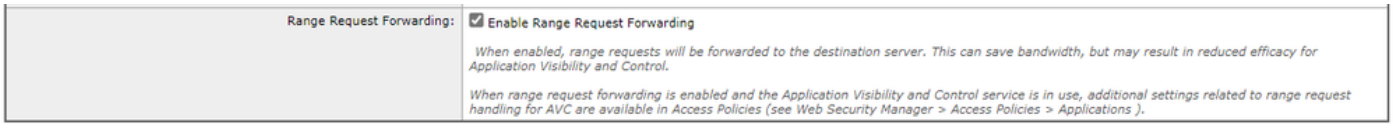


تكوين الخدمات

وكيل ويب

يجب تمكين التخزين المؤقت في تكوين وكيل الويب من أجل حفظ النطاق الترددي وتعزيز الأداء. ويصبح هذا الأمر أقل أهمية نظرا لزيادة النسبة المئوية لحركة مرور HTTPS لأن SWA لا تعمل بشكل افتراضي على تخزين حركات HTTPS مؤقتا. إذا تم نشر الوكيل لخدمة العملاء الصريحيين فقط، فيجب تحديد وضع إعادة التوجيه لرفض أي حركة مرور غير موجهة بشكل محدد لخدمة الوكيل. وبهذه الطريقة، يتم تقليل سطح هجوم الجهاز ويطبق مبدأ أمني جيد، ألا وهو إيقاف تشغيله إذا لم تكن هناك حاجة إليه.

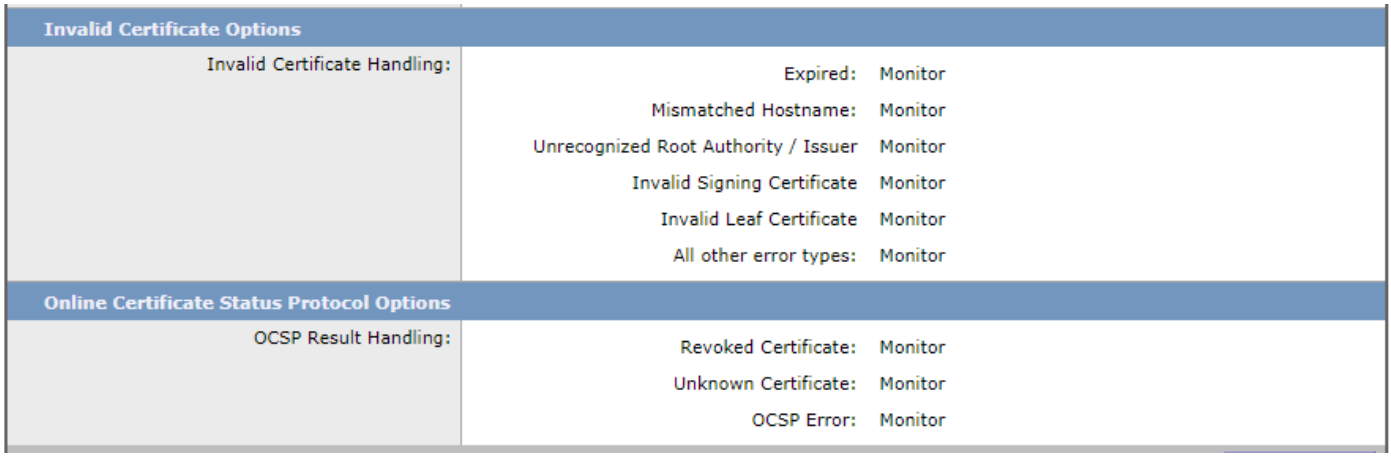
يتم إستخدام رؤوس طلبات النطاق في طلبات HTTP لتحديد نطاق البايت للملف الذي سيتم تنزيله. يستخدم هذا الخيار بشكل شائع من قبل برامج تحديث أنظمة التشغيل والتطبيقات لنقل أجزاء صغيرة من الملف في كل مرة. بشكل افتراضي، تجرد SWA هذه الرؤوس حتى تتمكن من الحصول على الملف بالكامل لأغراض الفحص ضد الفيروسات (AV)، وسمعة الملف وتحليله، والتحكم في رؤية التطبيق (AVC). يسمح تمكين إعادة توجيه رؤوس طلبات النطاق بشكل عام في إعدادات الوكيل للمستخدمين بإنشاء نهج وصول فردية تقوم بإعادة توجيه هذه الرؤوس أو تجريدها. يتم شرح مزيد من المعلومات حول هذا التكوين في قسم نهج الوصول.



وكيل HTTPS

تشير أفضل ممارسات الأمان إلى أنه يجب إنشاء المفاتيح الخاصة على الجهاز حيث يتم إستخدامها والا يتم نقلها مطلقا إلى مكان آخر. يتيح معالج وكيل HTTPS إنشاء زوج المفاتيح والشهادة المستخدمة لفك تشفير إتصالات أمان طبقة النقل (TLS). يمكن بعد ذلك تنزيل طلب توقيع الشهادة (CSR) وتوقيعه من قبل مرجع مصدق داخلي (CA). في بيئة Active Directory (AD)، تعد هذه أفضل طريقة لأن المرجع المصدق المدمج في AD موثوق به تلقائيا بواسطة جميع أعضاء المجال والا يتطلب خطوات إضافية لنشر الشهادة.

تتمثل إحدى وظائف الأمان الخاصة بوكيل HTTPS في التحقق من شهادات الخادم. تشير أفضل الممارسات إلى أن الشهادات غير الصالحة تتطلب إسقاط الاتصال. يسمح تمكين هذا بتقديم صفحة كتلة توضح سبب الكتلة. بدون تمكين هذا، يؤدي أي موقع HTTPS تم حظره إلى حدوث خطأ في المستعرض. وهذا يؤدي إلى زيادة عدد الشكاوى والمساعدة وإلى افتراض من جانب المستخدم بأن هناك شيئا ما معطلا، بدلا من العلم بأن جهة محترفي الخدمة (SWA) قد منعت الاتصال. يجب تعيين كافة خيارات الشهادة غير الصالحة على الأقل. يؤدي ترك أي من هذه الخيارات كشاشة إلى عدم تسجيل رسائل خطأ مفيدة في حالة أن مشكلة الشهادة تمنع تحميل موقع ما.



وبالمثل، يجب ترك عمليات التحقق من بروتوكول خدمات الشهادات عبر الإنترنت (OCSP) ممكنة ويجب عدم إستخدام جهاز المراقبة لأي خيار. يجب إسقاط الشهادات الملغاة ويجب تعيين كافة الشهادات الأخرى على الأقل على "فك التشفير" للسماح بتسجيل رسائل الخطأ ذات الصلة. مطراقة الوصول إلى معلومات السلطة (مطراقة AIA) هي وسيلة يمكن للعميل من خلالها الحصول على الموقع الخاص بالشهادة، وعنوان ربط يمكن جلب شهادات إضافية منه. على سبيل المثال، إذا كانت سلسلة الشهادات المستلمة من خادم غير مكتملة (تفتقد إلى شهادة وسيطة أو جذر)، يمكن لـ SWA التحقق من حقل AIA واستخدامه لجلب الشهادات المفقودة والتحقق من صحتها. يتوفر هذا الإعداد فقط في CLI (واجهة سطر الأوامر) من الأوامر التالية:

```
SWA_CLI> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
```

```
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> HTTPS
...
Do you want to enable automatic discovery and download of missing Intermediate Certificates?
[Y]>
...
```

ملاحظة: يتم تمكين هذا الإعداد بشكل افتراضي ويجب عدم تعطيله، نظرا لأن العديد من الخوادم الحديثة تعتمد على هذه الآلية لتوفير سلسلة ثقة كاملة للعملاء.

مراقب حركة مرور الطبقة الرابعة (L4TM)

تعد L4TM طريقة فعالة للغاية لتوسيع نطاق وصول SWA لتضمين حركة المرور الضارة التي لا تجتاز الوكيل، بالإضافة إلى تضمين حركة مرور البيانات على جميع منافذ TCP و UDP. تيون لا T1 و T2 ميناء أن يكون رابطت إلى اما شبكة لمس، أو مفتاح مدرب جلسة. وهذا يسمح ل SWA بمراقبة كل حركة المرور من العملاء بشكل سلبي. إذا تم عرض حركة المرور المهاجمة لعنوان IP ضار، يمكن أن يقوم SWA بإنهاء جلسات TCP بإرسال RST أثناء انتحال عنوان IP الداخلي. حركة مرور UDP، يمكن أن يرسل رسالة منفذ يتعذر الوصول إليه. عند تكوين جلسة المراقبة، من الأفضل استبعاد أي حركة مرور هجومة ولاجهة إدارة SWA لمنع الميزة من التدخل المحتمل في الوصول إلى الجهاز.

بالإضافة إلى مراقب حركة المرور الضارة، يوفق L4TM أيضا بالتطفل على استعلامات DNS لتحديث قائمة إعدادات الزوائح. يتم استخدام هذه القائمة في عمليات نشر WCCP لإجراء طلبات معينة إلى موجه WCCP للتوجيه المباشر إلى داخل الويب. لا تتم معالجة الحزم التي تطابق قائمة إعدادات الزوائح بواسطة الوكيل. يمكن أن تحتوي القائمة على عناوين IP أو أسماء الخوادم. يوفق SWA بحل أي إدخالات في قائمة إعدادات التجاوز كل 30 دقيقة، بغض النظر عن مدة البقاء (TTL) للسجل. ومع ذلك، إذا تم تمكين ميزة L4TM، يمكن أن تستخدم SWA استعلامات DNS المكرر لتحديث هذه السجلات بشكل أكثر تواترا. وهذا يقلل من خطر حدوث أخطاء سلبية في سيناريوهات حيث قام العميل بحل عنوان مختلف عن SWA.

تكوين النهج

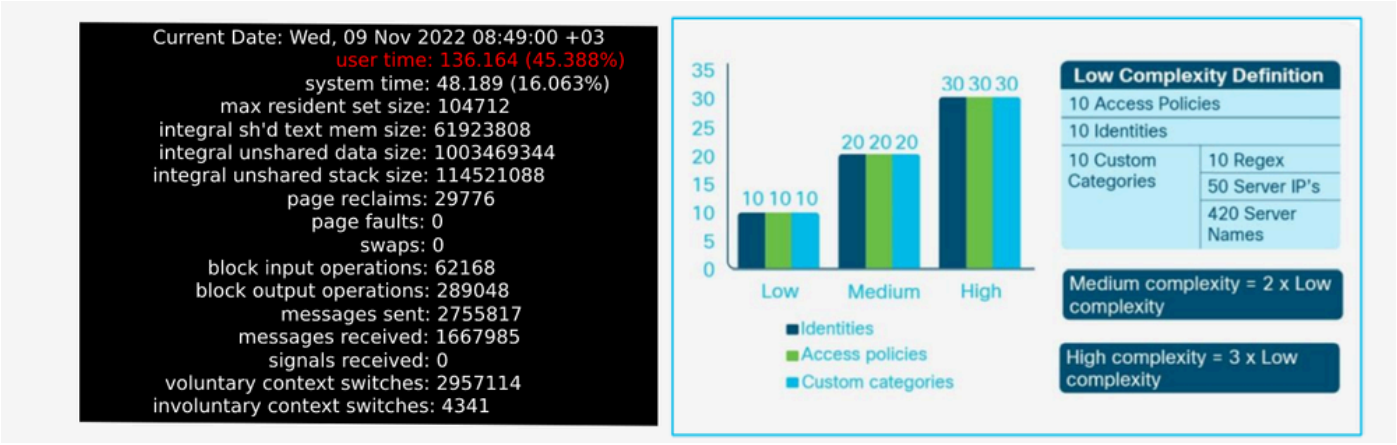
يعد التكوين الصحيح للنهج أمرا محوريا في أداء وإمكانية توسع SWA. ويصدق هذا ليس فقط بسبب فعالية السياسات نفسها في حماية العملاء وإنفاذ متطلبات الشركة، بل أيضا لأن السياسات التي يتم تكوينها لها تأثير مباشر على إستخدام الموارد وعلى صحة وأداء الوحدة بوجه عام. ذلك أن مجموعة مفرطة التعقيد أو سيئة التصميم من السياسات من الممكن أن تتسبب في عدم الاستقرار وبطء الاستجابة من جانب الجهاز.

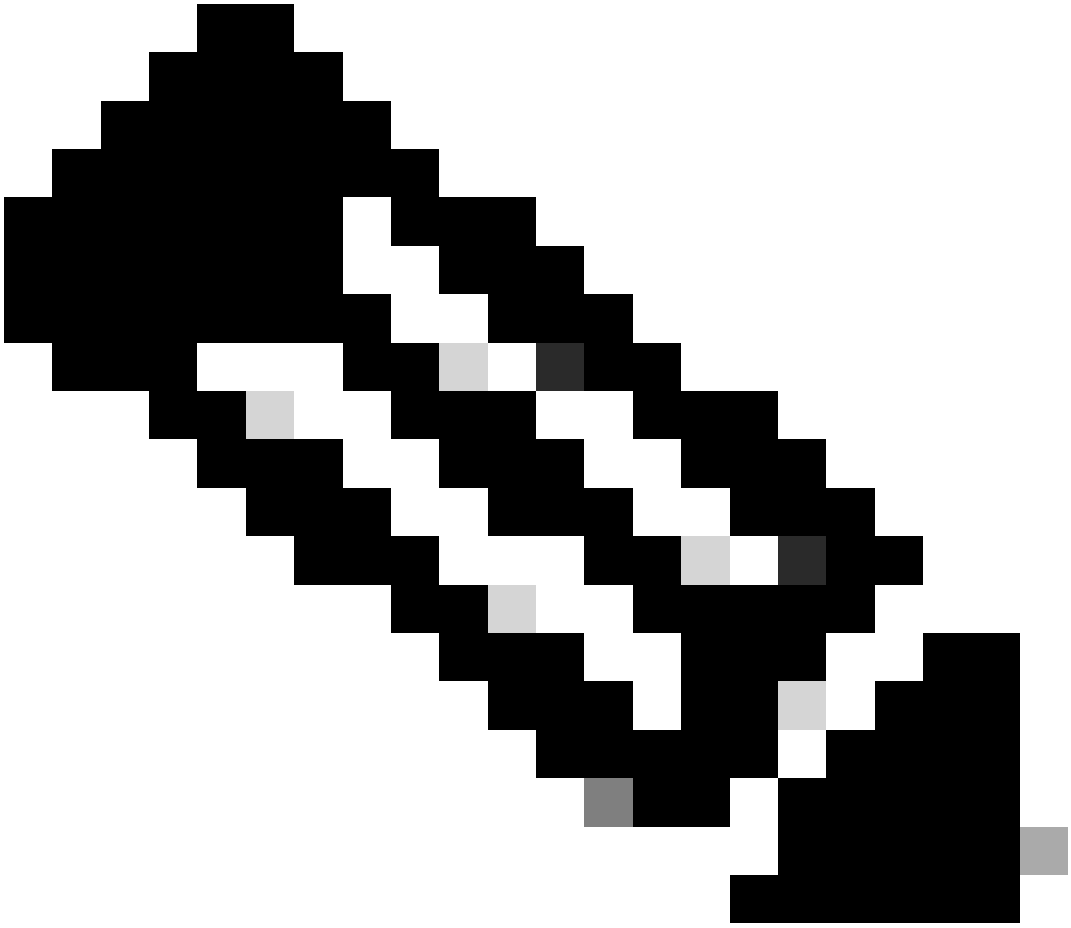
تعقيد

وتستخدم مختلف عناصر السياسة العامة في وضع سياسات النهج القطاعية الشاملة. يتم إستخدام ملف XML الذي يتم إنشاؤه من التكوين لإنشاء عدد من ملفات التكوين الطرفية وقواعد الوصول. كلما زاد التكوين تعقيدا، زادت المدة التي تستغرقها عملية الوكيل في تقييم مجموعات القواعد المختلفة لكل عملية. وعند وضع معايير للنهج المتبع في الإدارة وحجمه، يتم إنشاء مجموعة أساسية من عناصر السياسة العامة تمثل ثلاثة مستويات من تعقيد التكوين. يعد تكوين تكوين منخفض التعقيدات عشرة ملفات تعريف هوية، وسياسات فك تشفير، وسياسات وصول، بالإضافة إلى عشر فئات مخصصة تحتوي على عشرة إدخالات regex، وخمسين عنوانا IP للخوادم، و 420 اسم مضيف للخادم. وضرب كل من هذه الأرقام باثنين وثلاثة يؤدي إلى تعقيد متوسط وتعقيد عال، على التوالي.

عندما يصبح التكوين معقدا جدا، تتضمن الأعراض الأولى عادة إستجابة بطيئة في واجهة الويب و CLI (واجهة سطر الأوامر). ال يمكن أن يكون هناك تأثير كبير على المستخدمين في البداية. ولكن كلما كان التكوين أكثر تعقيدا، زاد الوقت الذي يجب أن تقضيه عملية الوكيل في وضع المستخدم. ولهذا السبب، يمكن أن يكون التحقق من نسبة الوقت المستغرق في هذا الوضع طريقة مفيدة لتشخيص التكوين بالغ التعقيد كسبب ظهور SWA بطيء.

يتم تسجيل وقت وحدة المعالجة المركزية (CPU)، بالثواني، في سجل track_stats كل خمس دقائق. وهذا يعني أنه يمكن حساب النسبة المئوية لوقت المستخدم على أنها (وقت المستخدم + وقت النظام)/300. مع اقتراب وقت المستخدم من 270، فإن العملية تقضي الكثير من دورات وحدة المعالجة المركزية (CPU) في وضع المستخدم، وهذا دائما تقريبا لأن التكوين معقد للغاية بحيث يتعذر تحليله بكفاءة.





ملاحظة: حتى الآن، لا تتجاوز حدود SWA 60000 اتصال عميل متزامن و 60000 اتصال خادم متزامن.

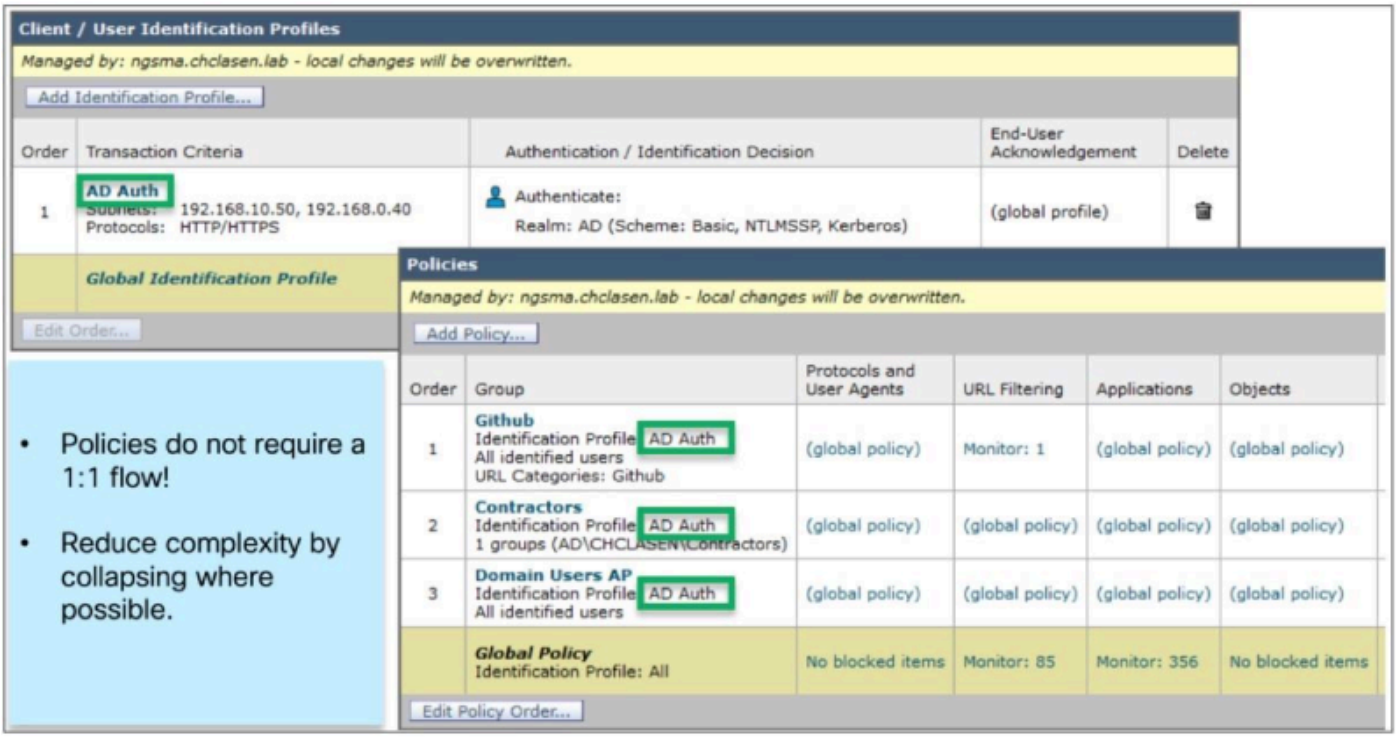
ملفات تعريف

تعد ملفات تعريف التعريف (ID) عناصر النهج الأولى التي يتم تقييمها عند تلقي طلب جديد. يتم تقييم جميع المعلومات التي تم تكوينها في القسم الأول من ملف تعريف المعرف باستخدام AND منطقي. وهذا يعني أنه يجب تطابق كل المعايير للطلب لكي يطابق ملف التعريف. عند إنشاء سياسة، يجب أن تكون محددة حسب الضرورة القصوى. غالبا ما تكون ملفات التعريف التي تتضمن عناوين مضيف فردية ضرورية، وقد تؤدي إلى تكوينات مترامية الأطراف. تعتبر الاستفادة من سلسلة وكيل المستخدم الموجودة في رؤوس HTTP أو قائمة الفئات المخصصة أو الشبكة الفرعية بشكل عام إستراتيجية أفضل للحد من نطاق ملف التعريف.

بشكل عام، يتم تكوين السياسات التي تتطلب المصادقة في الجزء السفلي مع إضافة الاستثناءات فوقها. عند طلب السياسات التي لا تتطلب المصادقة، يجب أن تكون السياسات الأكثر إستخداما هي الأقرب إلى الأعلى قدر الإمكان. لا تعتمد على المصادقة

الفاشلة لتقييد الوصول. إذا كان معروفا أن أحد العملاء على الشبكة غير قادر على المصادقة إلى وكيل، فيجب إعفائه من المصادقة ومنعه في سياسات الوصول. يرسل العملاء الذين ال يمكنهم المصادقة بشكل متكرر طلبات غير مصدق عليها إلى SWA، والتي تستخدم الموارد ويمكن أن تتسبب في إستخدام مفرط لوحدة المعالجة المركزية والذاكرة.

من المفاهيم الخاطئة الشائعة للمسؤولين أنه يجب أن يكون هناك ملف تعريف معرف فريد ونهج فك تشفير ونهج وصول متماثلان. وهي إستراتيجية غير فعالة في تكوين السياسات. عند الإمكان، يجب أن تكون السياسات "مطوية" بحيث يمكن أن يقترن ملف تعريف معرف واحد بالعديد من سياسات فك التشفير والوصول. هذا ممكن لأن كل المعايير في سياسة معينة يجب أن تتطابق لكي تتطابق حركة المرور مع السياسة. ونظرا لأن سياسة المصادقة أكثر عمومية وأكثر تحديدا في السياسات الناتجة، فإن ذلك يسمح بوضع سياسات أقل كلل.



سياسات فك التشفير

وكما هو الحال مع ملف تعريف المعرف، يتم أيضا تقييم المعايير المحددة في سياسة فك التشفير كمعيار منطقي، مع إستثناء مهم واحد عند إستخدام المعلومات من ISE. فيما يلي كيفية عمل مطابقة السياسة، اعتمادا على العناصر التي تم تكوينها (مجموعة AD أو المستخدم أو الرقيب):

- مجموعات AD والمستخدمين—ال يوجد تغيير في السلوك السابق، ويتم مطابقة السياسة إذا كان المستخدم عضوا في مجموعة أو إذا كان المستخدم محدد في السياسة.
- الرقيب ومجموعات الإعالن والمستخدمين - تتم مطابقة السياسة إذا كان المستخدم مقترنا بالرقيب وكان عضوا في مجموعة الإعالن، أو إذا كان المستخدم محددا في السياسة.
- الرقيب والمستخدمين — تتم مطابقة السياسة إذا كان المستخدم مقترنا بالرقيب أو كان المستخدم محددا في السياسة.

من بين جميع الخدمات التي تؤديءاه الوحدة الخاصة بلبنان، يعد تقييم حركة مرور بيانات HTTPS وه الأكثر أهمية من وجهة نظر الأداء. تؤثر النسبة المئوية لحركة المرور التي تم فك تشفيرها بشكل مباشر على كيفية حجم الجهاز. يمكن أن يعتمد المسؤول على 75٪ على الأقل من حركة مرور الويب تتصل بـ HTTPS.

بعد التثبيت الأولي، يجب تحديد النسبة المئوية لحركة المرور التي تم فك تشفيرها لضمان تحديد توقعات النمو في المستقبل بدقة. بعد النشر، يجب التحقق من هذا الرقم مرة كل ربع عام. من السهل العثور على النسبة المئوية لحركة مرور HTTPS التي تم فك تشفيرها بواسطة SWA باستخدام نسخة من access_log، حتى بدون برامج إضافية للإدارة السجل. يمكن استخدام أوامر Simple Bash أو PowerShell للحصول على هذا الرقم. فيما يلي الخطوات الموصوفة لكل بيئة:

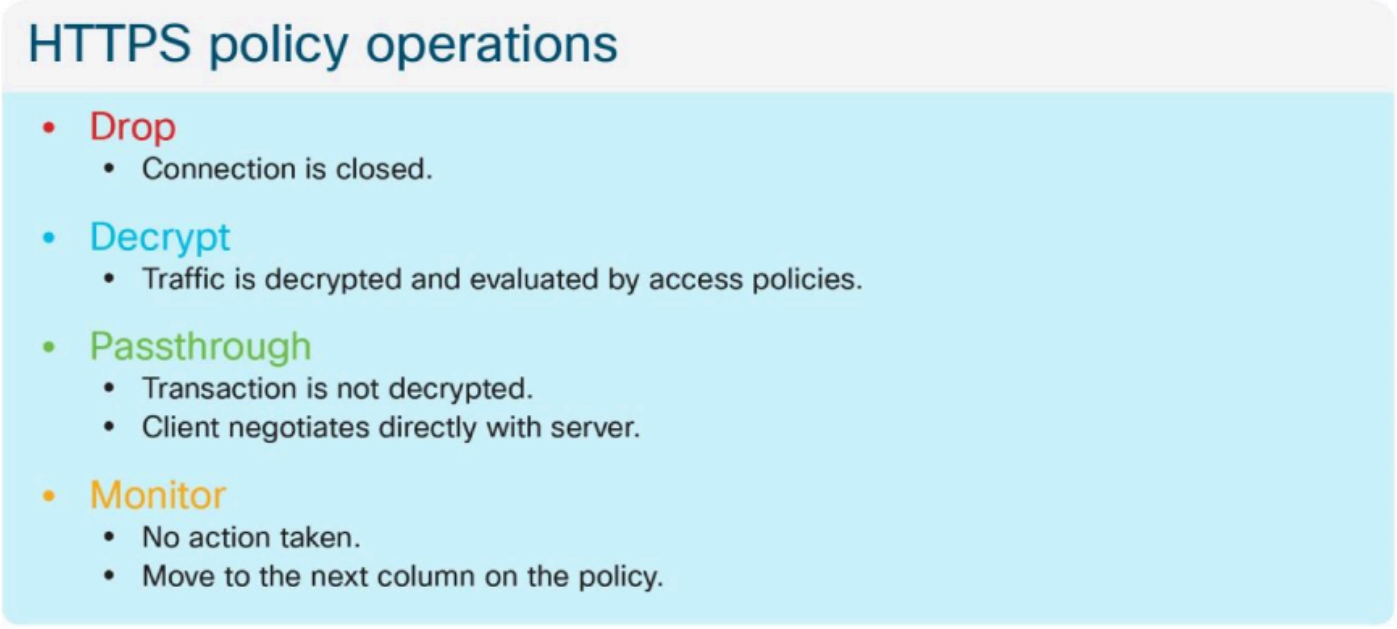
1. أمر Linux:

```
cat aclog.current | grep -Ev "\/407|\/401" | awk 'BEGIN { total=0; decrypt=0; ssl=0;} {total++; if($0 ~
```

2. أمر powershell:

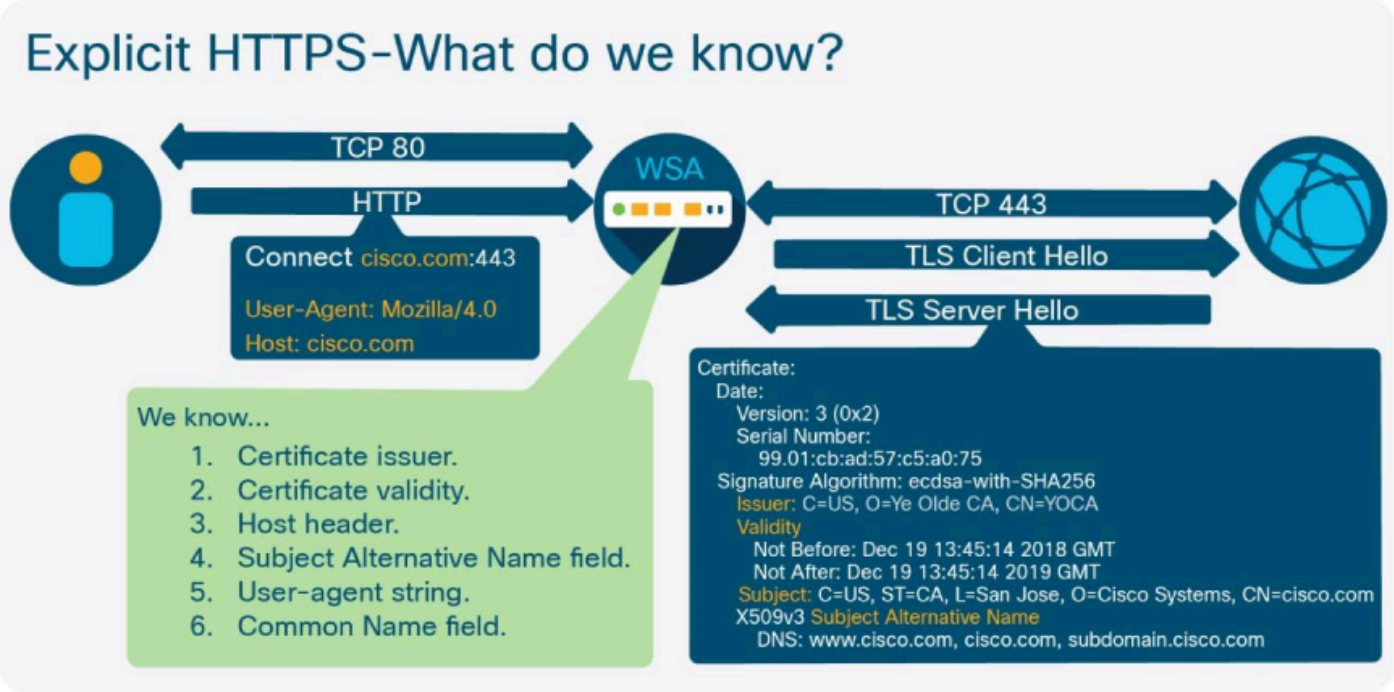
```
$lines = Get-Content -Path "aclog.current" | Where-Object { $_ -notmatch "/407|/401" }; $total = 0; $de
```

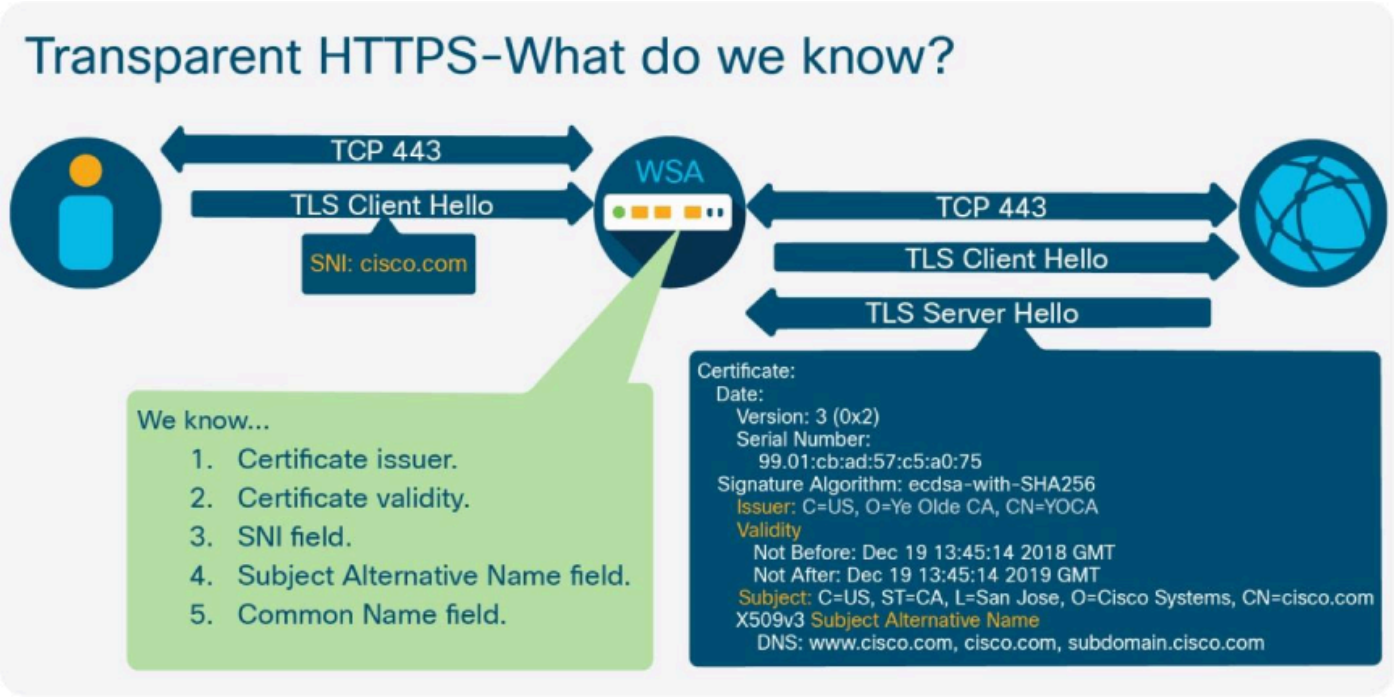
عند تصميم سياسات فك التشفير، من المهم فهم كيفية تسبب الإجراءات المختلفة إتصالات تقييم في الجهاز للسياسة المدرجة في HTTPS. يتم استخدام إجراء المرور عندما SWA موقت أن دون بهم خاصة TLS جلسة من نهاية إلى نهاية كل إنشاء بالخادم والعميل السماح يجب بفك تشفير كل حزمة. حتى في حالة تعيين عقوم على المرور، يجب أن تظل SWA مطلوبة لإكمال مصافحة TLS واحدة مع الخادم. وذلك لأن SWA يجب أن تتخذ قرار حظر اتصال بناء على حصة الشهادة، ويجب أن تبدأ اتصال TLS مع الخادم للحصول على الشهادة. إذا كانت الشهادة صحيحة، فإن SWA تغلق الاتصال وتسمح للعميل بمواصلة إعداد الجلسة مباشرة مع الخادم.



تكون الحالة الوحيدة التي لا تقوم فيها SWA بأي مصافحة TLS هي عندما يكون اسم الخادم أو عنوان IP موجودا في فئة مخصصة، يتم تعيينها على المرور، ويتوفر اسم الخادم إما في اتصال HTTP أو في ترحيب عميل TLS. في سيناريو صريح، يوفر العميل اسم المضيف الخاص بالخادم للوكيل قبل بدء جلسة عمل TLS (في رأس المضيف)، وبالتالي يتم التحقق من هذا الحقل مقابل الفئة المخصصة. في عملية نشر شفافة، يتحقق SWA من حقل إشارة اسم الخادم (SNI) في رسالة "ترحيب عميل TLS" ويقيمها مقابل الفئة المخصصة. إذا لم يكن رأس المضيف أو SNI موجودا، يجب أن تواصل SWA المصافحة مع الخادم للتحقق من حقلي الاسم البديل للموضوع (SAN) والاسم الشائع (CN) في الشهادة، بهذا الترتيب.

ما يعنيه هذا السلوك لتصميم السياسة هو أنه يمكن تقليل عدد رسائل تأكيد TLS من خلال تحديد الخوادم المعروفة جيدا والموثوق بها داخليا وإعدادها للمرور من قائمة فئات مخصصة، بدلا من الاعتماد على فئة الويب ودرجة السمعة، التي لا تزال تتطلب من SWA إكمال مصافحة TLS مع الخادم. غير أنه من المهم ملاحظة أن هذا يمنع أيضا التحقق من صحة الشهادة.





نظرا لسرعة ظهور مواقع جديدة على الويب، من المحتمل أن يتم العثور على عدد من المواقع غير مصنفة بواسطة قواعد بيانات السمعة والتصنيفات الخاصة بالويب المستخدمة من قبل SWA. الا يشير ذلك إلى أن الموقع من المحتمل أن يكون ضارا بشكل أكبر بالضرورة، وبالإضافة إلى ذلك، الا تزال جميع هذه المواقع تخضع للمسح الضوئي للمركبات (AV)، وسمعة ملف AMP وتحليله، وأي حظر على الكائنات أو مسحها ضوئيا تم تكوينه. ولهذه الأسباب، الا يوصى بإسقاط المواقع غير المصنفة في معظم الظروف. من الأفضل تعيينها ليتم فك تشفيرها ومسحها ضوئيا بواسطة محركات AV وتقييمها بواسطة AVC و AMP وسياسات الوصول وما إلى ذلك. يوجد مزيد من المعلومات حول المواقع غير المصنفة في قسم نهج الوصول.

سياسات الوصول

وكما هو الحال مع ملف تعريف المعرف، يتم أيضا تقييم المعاييير المحدددة في سياسة كف التشفير كمعايير منطقية ومع إستثناء واحد مهم عند إستخدام المعلومات من ISE. ثم يتم حرش كولس مضاهاة السياسات بعد ذلك، استنادا إلى العناصر التي يتم تكوينها (المجموعة الإعلانية أو المستخدم أو الرقيب):

- مجموعات AD والمستخدمين—ال يوجد تغيير في السلوك السابق، ويتم مطابقة السياسة إذا كان المستخدم موضع في مجموعة أو إذا كان المستخدم محددا في السياسة.
- الرقيب ومجموعات الإعلان والمستخدمين - تتم مطابقة السياسة إذا كان المستخدم مقترنا بالرقيب وكان موضع في مجموعة الإعلان، أو إذا كان المستخدم محددا في السياسة.
- الرقيب والمستخدمين — تتم مطابقة السياسة إذا كان المستخدم مقترنا بالرقيب أو كان المستخدم محددا في السياسة.

يتم تقييم حركة مرور HTTP مقابل سياسات الوصول مباشرة بعد مصادقتها. يتم تقييم حركة مرور HTTPS بعد مصادقتها، وإذا تم تطبيق إجراء كف التشفير وفقا لنهج كف التشفير المطابق. بالنسبة للطلبات التي تم كف تشفيرها، يوجد إدخالا access_log. يظهر إدخال السجل الأول للإجراء المطبق على اتصال TLS الأولي (الذي تم كف تشفيره)، ويظهر إدخال سجل ثان الإجراء المطبق بواسطة نهج الوصول على طلب HTTP الذي تم كف تشفيره.

كما هو موضح في قسم ويكي الويب، يتم إستخدام سوور طلبات النطاق بطلب نطاق بايت محدد من الملف ويتم إستخدامها بشكل شائع بواسطة خدمات تحديث التطبيق ونظام التشغيل. موقت SWA، بشكل افتراضي، بشطب هذه الرؤوس من الطلبات الصادرة، لأنه بدون الملف بأكمله، من المستحيل إجراء مسح ضوئي للبرامج الضارة أو إستخدام ميزات AVC. إذا كان العديد من الأجهزة المضيفة على الشبكة طلبات نطاق بايت صغيرة بشكل تحديثات التحديثات المتكررة، فقد يؤدي ذلك إلى تشغيل SWA لتنزيل الملف بالكامل عدة مرات في نفس الوقت. وهذا يمكن أن يستنزف عرض النطاق الترددي المتاح للإنترنت بسرعة ويتسبب في انقطاع الخدمة. أكثر الأسباب شيوعا لسيناريو هذا الفشل هي أنظمة التشغيل Microsoft Windows Update و Adobe Software Update.

للتخفيف من هذه المشكلة، فإن الحل الأفضل لها هو تخطي في توجيه حركة المرور هذه للتخلص من هذه المشكلة. وفي هذه الحالات، فإن الخيار الأفضل هو إنشاء سياسات وصول مخصصة لحركة المرور وتمكين إعادة توجيه رأس طلب النطاق على تلك السياسات. يجب أن تكون على دراية بأنه لا يمكن إجراء مسح ضوئي للبرامج الضارة أو فحص الفئات وفحص الأشعة تحت الحمراء لهذه الطلبات، وبالتالي يجب أن تكون الغاية من إستخدام هذه السياسات يجب تصميمها طبقا لذلك ومقصودة لحركة المرور الموجودة في رأس المستخدم وكل سلسلة مطابقة هي ذلك لتحقيق أفضل طريقة للتحديثات الشائعة للمستخدمين المدعومين وكل سلسلة على عثور يمكن بالطلب. لا تستخدم معظم الإنترنت، أو يمكن التقاط الطلبات بواسطة الموسوعات وفحصها عبر خدمات التحديث، بما في ذلك Microsoft Windows وتحديثات برامج Adobe HTTPS.

كما هو موضح في قسم سياسات كف التشفير، لا يوصى بإسقاط المواقع غير المصنفة في سياسات كف التشفير. ولنفس الأسباب، لا يوصى بحظرها في سياسات الوصول. يمكن لمحرك "التحليل الديناميكي للمحتوى" (DCA) إستخدام محتوى موقع معين،

باإلضافة إلى البيانات االستكشافية الأخرى إلى مواقع مصنفة التي لول ذلك سيتم وضع عالمة عليها غير مصنفة بواسطة عمليات البحث في قاعدة بيانات URL. يقلل تمكين هذه المميزة عدد الأحكام غير المصنفة في SWA.

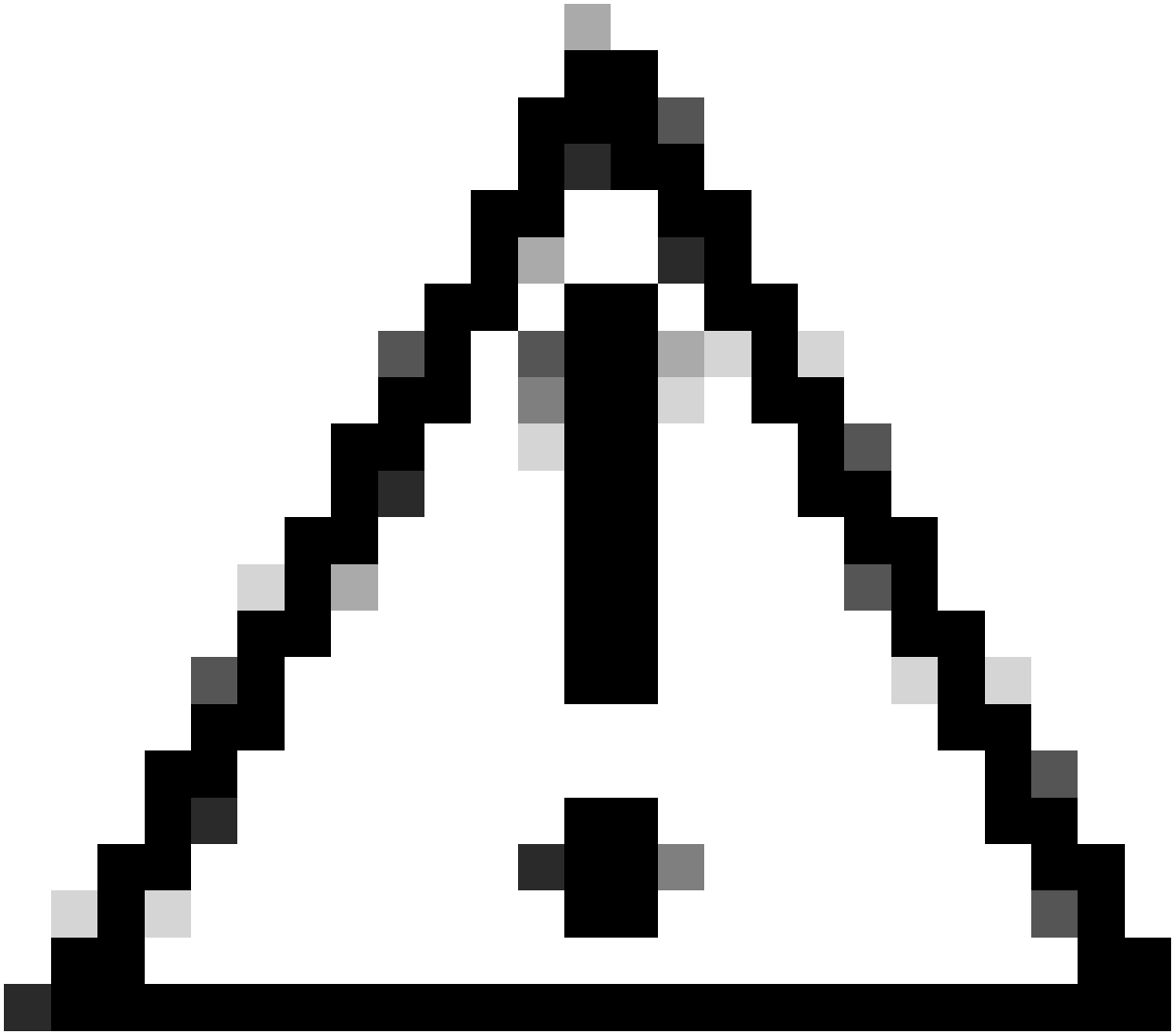
توفر إعدادات مسح الكائنات لنهج الوصول إمكانية فحص أنواع عديدة من ملفات الأرشيف. إذا كانت الشبكة تقوم بتنزيل ملفات الأرشيف بانتظام كجزء من تحديثات التطبيق، فإن تمكين فحص ملفات الأرشيف يمكن أن يزيد من استخدام وحدة المعالجة المركزية بشكل كبير. يجب تحديد حركة المرور هذه مسبقا وإعفائها إذا كانت النية هي فحص جميع ملفات الأرشيف. أول مكان للتحقيق في الطرق المحتملة لتعريف حركة المرور هذه هو سلسلة وكيل المستخدم، حيث يمكن أن يساعد ذلك في تجنب قوائم IP الممسوح بها التي يمكن أن تصبح مرهقة للحفاظ عليها.

فئات عنوان URL المخصص والخارجي

يتم إستخدام قوائم الفئات المخصصة لتعريف الخادم بواسطة عنوان IP أو اسم المضيف. من الممكن إستخدام التعبيرات العادية (regex) لتعيين الحشوات التي من خاللها يمكن مطابقة أسماء الخوادم. يتطلب إستخدام نمط regex لمطابقة اسم خادم موارد كثيرة مقارنة باستخدام مطابقة سلسلة عرفية، ولذلك يجب إستخدامها فقط عند الضرورة القصوى. يمكن إضافة "." إلى بداية اسم مجال لمطابقة مجال فرعي دون الحاجة إلى regex. على سبيل المثال، تطابق ".cisco.com" أيضا "www.cisco.com."
وكما هو موضح في قسم التعقيد، يتم تعريف التعقيد المنخفض على أنه عشر قوائم فئات مخصصة، ومتوسط تعقيد عشريني، ومتوسط تعقيد كبير ثالثون. يوصى بإبقاء هذا العدد دون العشريني، خاصة إذا كانت القوائم تستخدم أنماط regex أو تحتوي على عدد كبير من الإدخالات. ارجع إلى قسم سياسات الوصول للحصول على تفاصيل إضافية حول عدد الإدخالات لكل نوع.

تكون موجزات URL الخارجية أكثر مرونة من قوائم الفئات المخصصة الثابتة، ويمكن أن يكون لزيادة االستفادة منها تأثير مباشر على الأمان لأنها تزيل حاجة المسؤول إلى صيانتها يدويا. نظرا لأنه يمكن إستخدام هذه المميزة لاستيراد القوائم التي ال يتم صيانتها أو التحكم فيها بواسطة مسؤول SWA، تمت إضافة القدرة على إضافة إستثناءات فردية إلى العناوين التي تم تنزيلها في الإصدار 11.8 من AsyncOS.

وتعد واجهة برمجة تطبيقات Office365 مفيدة بشكل خاص التخاذ قرارات تتعلق بالسياسات بشأن هذه الخدمة المنشورة بشكل شائع ويمكن االستفادة منها في التطبيقات الفردية (PowerPoint و Skype و Word وما إلى ذلك). توصي Microsoft بتجاوز الوكالء لكافة حركات مرور Office365 لتحسين الأداء. تذكر وثائق Microsoft:



تحذير: في حين أن فاصل SSL وفحصه يخلق أكبر زمن وصول، فإن الخدمات الأخرى مثل مصادقة الوكيل والبحث عن السمعة يمكن أن تتسبب في أداء ضعيف وتجربة مستخدم سيئة. وبالإضافة إلى ذلك، تحتاج أجهزة شبكة النطاق هذه إلى سعة كافية لمعالجة جميع طلبات اتصال الشبكة. نوصي بتجاوز الوكيل وأجهزة الفحص لطلبات شبكة Office 365 المباشرة. - https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide

---

قد يكون من الصعب إستخدام هذا التوجيه في بيئة وكيل شفافة. بداية من الإصدار 11.8 من AsyncOS، من الممكن إستخدام قائمة الفئات الديناميكية التي تم إستردادها من Office365 API لملء قائمة إعدادات الالتفاف. يتم إستخدام هذه القائمة لإرسال حركة مرور البيانات التي تمت إعادة توجيهها بشكل شفاف إلى جهاز WCCP للتوجيه المباشر.

يؤدي تجاوز كافة حركات مرور Office365 إلى إنشاء نقطة غير مباشرة للمستخدمين الذين يحتاجون إلى بعض عناصر التحكم الأساسية في الأمان والإبلاغ عن حركة المرور هذه. إذا لم يتم تجاوز حركة مرور Office365 بواسطة SWA، فمن المهم فهم التحديات التقنية المحددة التي يمكن أن تحدث. أحد هذه الأرقام هو عدد الاتصالات المطلوبة بواسطة التطبيقات. يجب

تعديل الحجم بشكل مناسب لاستيعاب إتصالات TCP المتواصلة الإضافية التي تتطلبها تطبيقات Office365. يمكن أن يزيد هذا العدد الإجمالي للاتصالات بما بين عشر إلى خمس عشرة جلسة عمل TCP متواصلة لكل مستخدم.

تعمل إجراءات فك التشفير وإعادة التشفير التي يتم تنفيذها بواسطة وكيل HTTPS على توفير قدر صغير من زمن الانتقال إلى الاتصالات. يمكن لتطبيقات Office365 أن تكون حساسة جدا لزمن الوصول، وإذا كانت هناك عوامل أخرى مثل بطء اتصال شبكة WAN والموقع الجغرافي المتباين قد تتسبب في تعقيد هذا الأمر، فيمكن أن تعاني خبرة المستخدم.

تستخدم بعض تطبيقات Office365 معلمات TLS الخاصة التي تمنع وكيل HTTPS من إكمال عملية مصافحة مع خادم التطبيق. هذا مطلوب للتحقق من صحة الشهادة أو إسترداد اسم المضيف. وعندما يتم دمج هذا مع تطبيق مثل Skype for Business الذي لا يرسل حقل إشارة اسم الخادم (SNI) في رسالة Hello الخاصة بعميل TLS الخاصة به، يصبح من الضروري تجاوز حركة مرور البيانات هذه بالكامل. قدم AsyncOS 11.8 القدرة على تجاوز حركة المرور استنادا إلى عنوان IP للوجهة فقط، دون تدقيقات الشهادات لمعالجة هذا السيناريو.

الشاشات والتنبيهات

شاشات CLI

توفر واجهة سطر أوامر (CLI) SWA أوامر للمراقبة في الوقت الفعلي للعمليات المهمة. الأكثر فائدة هي الأوامر التي تظهر الإحصائيات المتعلقة بعملية prox. يعد الأمر status detail مصدرا جيدا لملخص إستخدام الموارد ومقاييس الأداء، بما في ذلك وقت التشغيل والنطاق الترددي المستخدم وزمن الوصول للاستجابة وعدد الاتصالات وغير ذلك الكثير. هنا مثال إنتاج من هذا أمر:

```
SWA_CLI>  status detail

Status as of:                  Fri Nov 11 14:06:52 2022 +03
Up since:                      Fri Apr 08 10:15:00 2022 +03 (217d 3h 51m 52s)
System Resource Utilization:
  CPU                                    3.3%
  RAM                                    6.2%
  Reporting/Logging Disk                45.6%
Transactions per Second:
  Average in last minute                   55
  Maximum in last hour                    201
  Average in last hour                     65
  Maximum since proxy restart            1031
  Average since proxy restart              51
Bandwidth (Mbps):
  Average in last minute                4.676
  Maximum in last hour                327.258
  Average in last hour                 10.845
  Maximum since proxy restart        1581.297
  Average since proxy restart          11.167
Response Time (ms):
  Average in last minute                  635
```

```
  Maximum in last hour                  376209
  Average in last hour                     605
  Maximum since proxy restart          2602943
  Average since proxy restart              701
Cache Hit Rate:
  Average in last minute                     0
  Maximum in last hour                       2
  Average in last hour                       0
  Maximum since proxy restart               15
  Average since proxy restart                0
Connections:
  Idle client connections                  186
  Idle server connections                  184
  Total client connections                3499
  Total server connections                3632
SSLJobs:
  In queue Avg in last minute                4
  Average in last minute                 45214
  SSLInfo Average in last min               94
Network Events:
  Average in last minute                   0.0
  Maximum in last minute                    35
  Network events in last min            124502
```

يعرض أمر المعدل معلومات الوقت الفعلي حول النسبة المئوية لوحدة المعالجة المركزية (CPU) المستخدمة من قبل عملية PROX، بالإضافة إلى عدد الطلبات في الثانية (RPS) وإحصاءات ذاكرة التخزين المؤقت. يستمر هذا الأمر في الاستقصاء وعرض مخرجات جديدة حتى يتم مقاطعتها. هذا مثال من إنتاج من هذا أمر:

```
SWA_CLI>  rate

Press Ctrl-C to stop.
  %proxy  reqs                          client    server    %bw  disk  disk
     CPU  /sec   hits blocks misses     kb/sec    kb/sec  saved   wrs   rds
  5.00    51      1    147    370       2283      2268    0.6    48    37
  4.00    36      0    128    237      21695     21687    0.0    47    38
  4.00    48      2    179    307       8168      8154    0.2    65    33
  5.00    53      0    161    372       2894      2880    0.5    48    32
  6.00    52      0    198    328      15110     15100    0.1    63    33
  6.00    77      0    415    363       4695      4684    0.2    48    34
  7.00    85      1    417    433       5270      5251    0.4    49    35
  7.00    67      1    443    228       2242      2232    0.5    85    44
```

يعرض الأمر tcpservices معلومات حول منافذ الاستماع للعملية المحددة. كما يتم عرض شرح لكل عملية ومجموعة العناوين والمنفذ:

```
SWA_CLI> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
```

```
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  coeuslogd    - Main WSA controller
  gui          - GUI process
  hermes       - Mail server for sending alerts, etc.
  java         - Processes for storing and querying Web Tracking data
  musd         - AnyConnect Secure Mobility server
  pacd         - PAC file hosting daemon
  prox         - WSA proxy
  trafmon      - L4 Traffic Monitor
  uds          - User Discovery System (Transparent Auth)
  wccpd        - WCCP daemon

COMMAND      USER         TYPE NODE   NAME
connector    root         IPv4 TCP    127.0.0.1:8823
java         root         IPv6 TCP    [::127.0.0.1]:18081
hybridd      root         IPv4 TCP    127.0.0.1:8833
gui          root         IPv4 TCP    172.16.40.80:8443
ginetd       root         IPv4 TCP    172.16.40.80:ssh
nginx        root         IPv6 TCP    *:4431
nginx        root         IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
api_serve    root         IPv4 TCP    172.16.40.80:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    172.16.40.80:6443
chimera      root         IPv4 TCP    127.0.0.1:6380
nectar       root         IPv4 TCP    127.0.0.1:6382
redis-ser    root         IPv4 TCP    127.0.0.1:6383
redis-ser    root         IPv4 TCP    127.0.0.1:6379
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
```

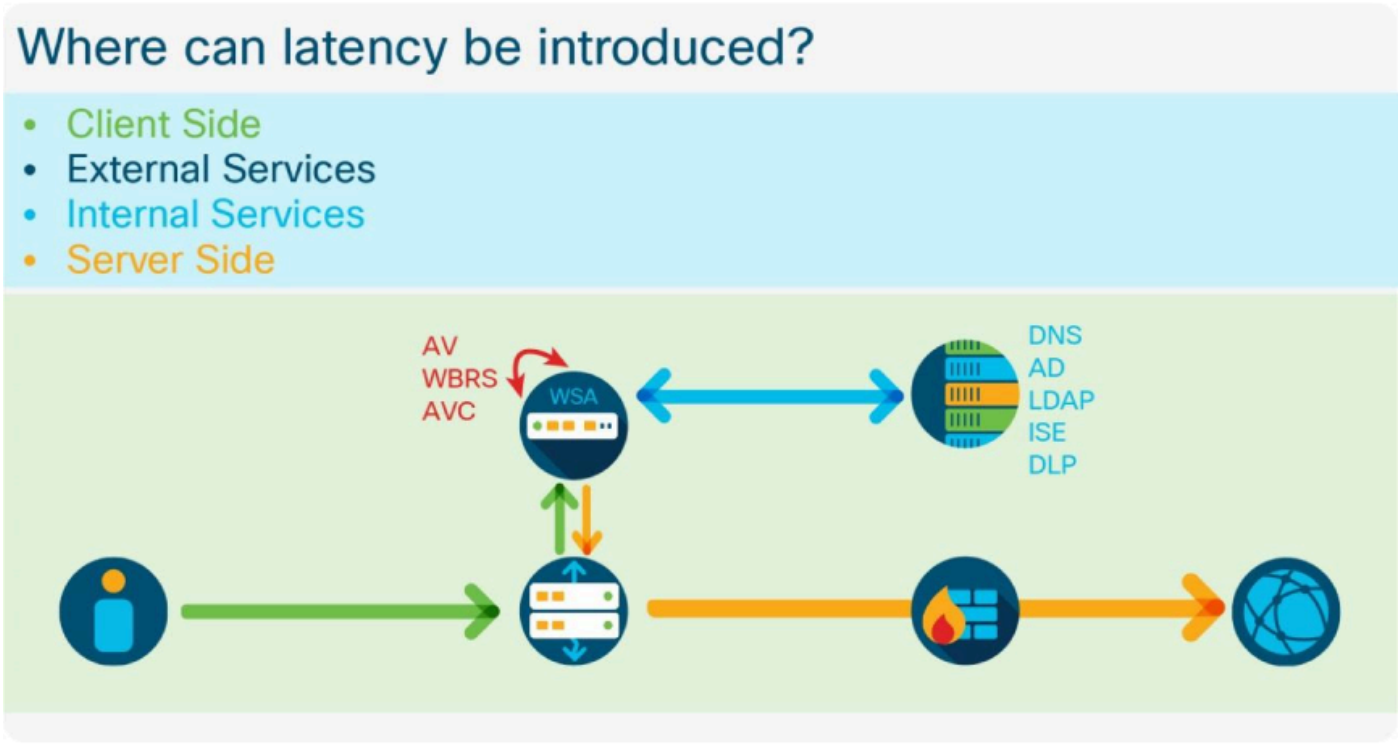
```
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25255
prox         root         IPv4 TCP    127.0.0.1:socks
prox         root         IPv6 TCP    [::1]:socks
prox         root         IPv4 TCP    172.16.11.69:socks
prox         root         IPv4 TCP    172.16.11.68:socks
prox         root         IPv4 TCP    172.16.11.252:socks
prox         root         IPv4 TCP    127.0.0.1:ftp-proxy
prox         root         IPv6 TCP    [::1]:ftp-proxy
prox         root         IPv4 TCP    172.16.11.69:ftp-proxy
prox         root         IPv4 TCP    172.16.11.68:ftp-proxy
prox         root         IPv4 TCP    172.16.11.252:ftp-proxy
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25256
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.21.11.69:https
prox         root         IPv4 TCP    172.21.11.68:https
prox         root         IPv4 TCP    172.21.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25257
smart_age    root         IPv6 TCP    [::127.0.0.1]:65501
smart_age    root         IPv6 TCP    [::127.0.0.1]:28073
interface    root         IPv4 TCP    127.0.0.1:domain
stunnel      root         IPv4 TCP    127.0.0.1:32137
```

التسجيل

حركة مرور الويب ديناميكية ومتنوعة. بعد اكتمال عملية نشر الوكيل، من المهم إعادة تقييم كمية وكمية حركة المرور التي يتم تمريرها عبر الجهاز بشكل دوري. يجب عليك

التحقق من النسبة المئوية لحركة المرور التي تم فك تشفيرها بشكل منتظم (مرة كل ربع عام) لضمان توافق الحجم مع توقعات التثبيت الأولي ومواصفاته. ويمكن القيام بذلك باستخدام منتج إدارة سجل مثل التقارير المتقدمة لأمان الويب (AWSR) أو باستخدام أوامر Basic أو PowerShell البسيطة مع سجلات الوصول. كما يجب إعادة تقييم عدد وحدات التزويد بالطاقة (RPS) بشكل منتظم لضمان توفر مصروفات عامة كافية في الجهاز لمراعاة الزيادات الهائلة في حركة المرور واحتمال تجاوز الأعطال في تكوين يتسم بالتوفر الفائق والتوازن في الأحمال.

يتم إلحاق سجل track_stats لكل خمس دقائق، وهو يتضمن العديد من أقسام الإخراج المتعلقة مباشرة بعملية prox وكائناتها في الذاكرة. وأكثر الأقسام فائدة في مراقبة الأداء هي الأقسام التي تظهر متوسط زمن الوصول لعمليات الطلبات المختلفة، وتتضمن وقت البحث عن نظام أسماء المجالات (DNS)، ووقت مسح محرك الصوت/الفيديو، والعديد من الحقول الأكثر فائدة. الا يمكن تكوين هذا السجل من واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI) ويمكن الوصول إليه فقط من خلال بروتوكول النسخ الآمن (SCP) أو بروتوكول نقل الملفات (FTP). هذا هو السجل الأكثر أهمية الذي يتم الحصول عليه عند استكشاف الأخطاء وإصلاحها للأداء، لذلك يجب إجراء استفتاء عليه بشكل متكرر.



Client side latency

```
Client Time       1.0 ms     15575
Client Time       1.6 ms     185
Client Time       2.5 ms     855
Client Time       4.0 ms     573
Client Time       6.3 ms     180
Client Time      10.0 ms     264
Client Time      15.8 ms     580
Client Time      25.1 ms     924
Client Time      39.8 ms     1330
Client Time      63.1 ms     4936
Client Time     100.0 ms     5278
Client Time     158.5 ms     10
Client Time     251.2 ms     13
Client Time     398.1 ms     0
Client Time     631.0 ms     0
Client Time    1000.0 ms     0
Client Time    1584.9 ms     0
Client Time    2511.9 ms     0
Client Time    3981.1 ms     0
Client Time    6309.6 ms     30328
```

- **"Client Time"** in **track_stats** log.
- The amount of time in milliseconds that the client was waiting for a response.
- May indicate an upstream issues-keep investigating!
- Access logs can show this in custom field **% : 1>**

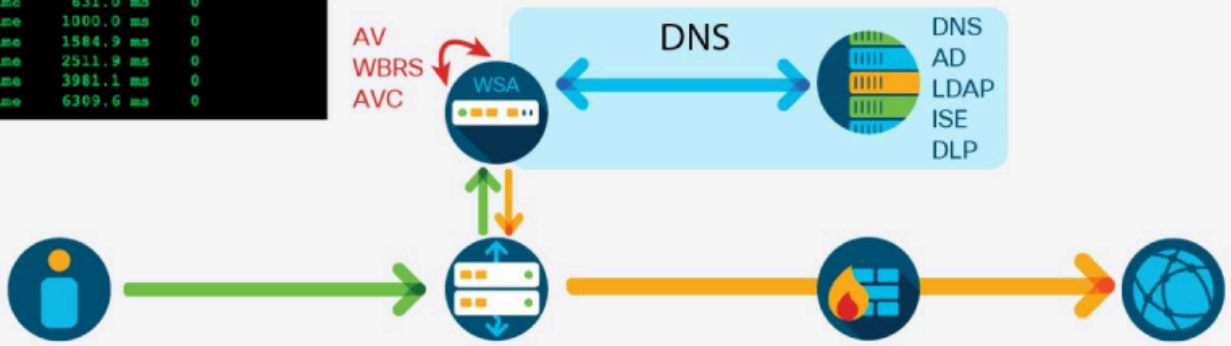
%:1>	x-p2c-first-byte-time	Wait-time for first byte written to client

DNS latency

```
DNS Time       1.0 ms     51
DNS Time       1.6 ms     347
DNS Time       2.5 ms     152
DNS Time       4.0 ms     71
DNS Time       6.3 ms     98
DNS Time      10.0 ms     7
DNS Time      15.8 ms     11
DNS Time      25.1 ms     13
DNS Time      39.8 ms     2
DNS Time      63.1 ms     3
DNS Time     100.0 ms     7
DNS Time     158.5 ms     16
DNS Time     251.2 ms     4
DNS Time     398.1 ms     1
DNS Time     631.0 ms     0
DNS Time    1000.0 ms     0
DNS Time    1584.9 ms     0
DNS Time    2511.9 ms     0
DNS Time    3981.1 ms     0
DNS Time    6309.6 ms     0
```

- The amount of time in milliseconds that the WSA waited for a DNS response.
- Calls for investigation for your DNS resolvers (or path to them).
- **access logs** can show this in custom field **% : >d**

%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS Process to send a DNS result to ehe Web proxy.

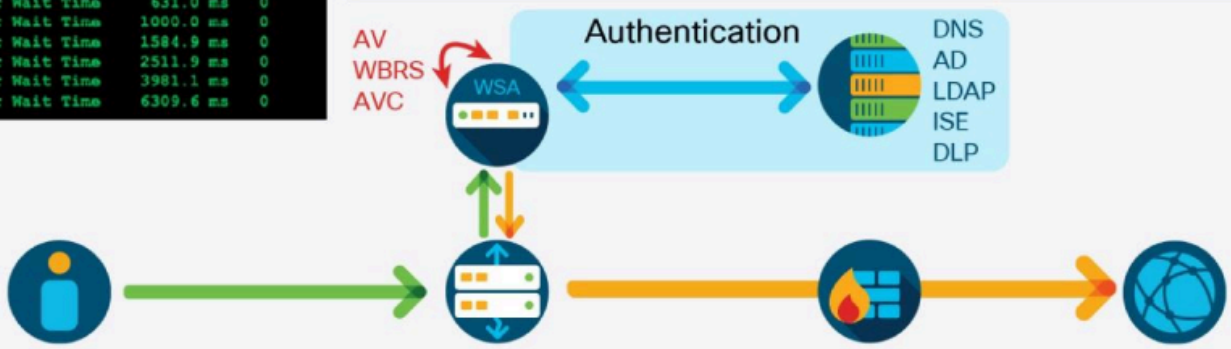


Authentication latency

```
Server Wait Time       1.0 ms   0
Server Wait Time       1.6 ms   0
Server Wait Time       2.5 ms   0
Server Wait Time       4.0 ms   0
Server Wait Time       6.3 ms   0
Server Wait Time      10.0 ms   0
Server Wait Time      15.8 ms   0
Server Wait Time      25.1 ms   0
Server Wait Time      39.8 ms   0
Server Wait Time      63.1 ms   0
Server Wait Time     100.0 ms   0
Server Wait Time     158.5 ms   1
Server Wait Time     251.2 ms   1
Server Wait Time     398.1 ms   0
Server Wait Time     631.0 ms   0
Server Wait Time    1000.0 ms   0
Server Wait Time    1584.9 ms   0
Server Wait Time    2511.9 ms   0
Server Wait Time    3981.1 ms   0
Server Wait Time    6309.6 ms   0
```

- There are two metrics: **"Auth Helper Wait Time"** and **"Auth Helper Service Wait Time."**
- Use the first to get pure auth time without the request time added.
- **access logs** can show this in custom field **% : >a**

%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.

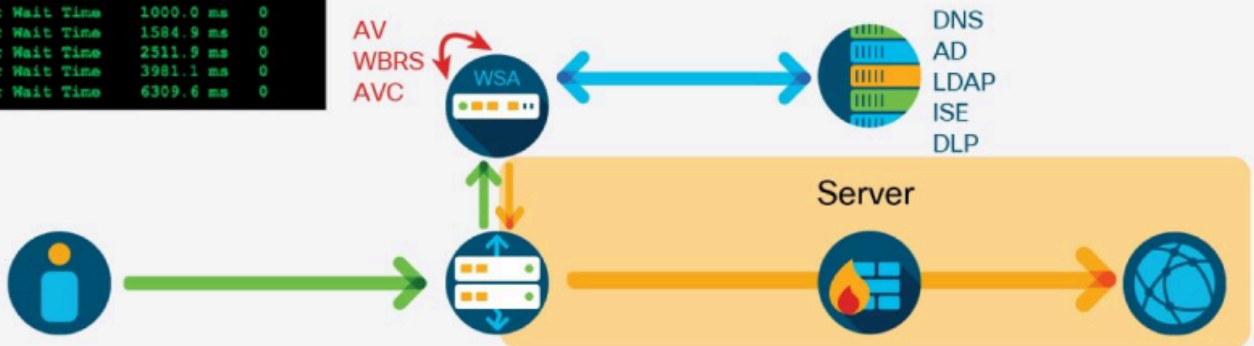


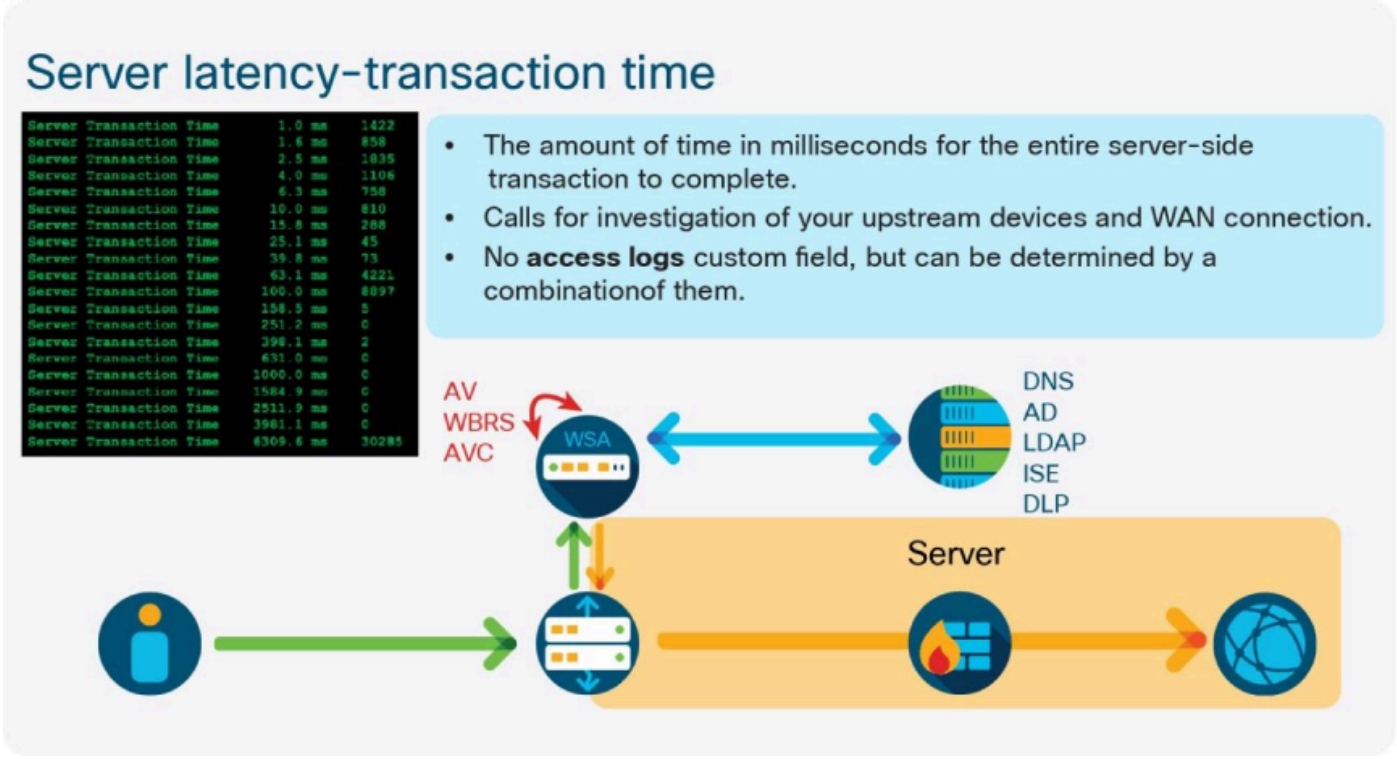
Server latency-wait time

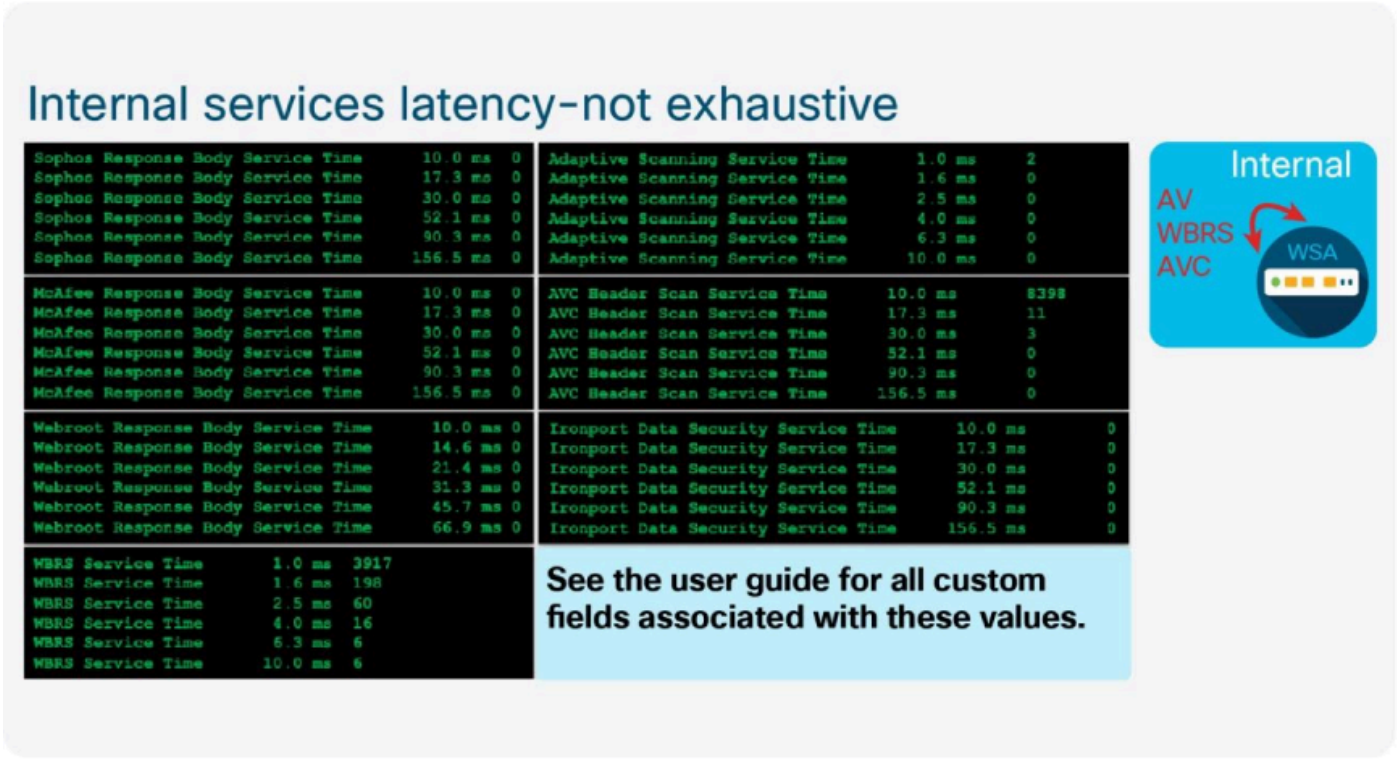
```
Server Wait Time       1.0 ms   0
Server Wait Time       1.6 ms   0
Server Wait Time       2.5 ms   0
Server Wait Time       4.0 ms   0
Server Wait Time       6.3 ms   0
Server Wait Time      10.0 ms   0
Server Wait Time      15.8 ms   0
Server Wait Time      25.1 ms   0
Server Wait Time      39.8 ms   0
Server Wait Time      63.1 ms   0
Server Wait Time     100.0 ms   0
Server Wait Time     158.5 ms   1
Server Wait Time     251.2 ms   1
Server Wait Time     398.1 ms   0
Server Wait Time     631.0 ms   0
Server Wait Time    1000.0 ms   0
Server Wait Time    1584.9 ms   0
Server Wait Time    2511.9 ms   0
Server Wait Time    3981.1 ms   0
Server Wait Time    6309.6 ms   0
```

- The amount of time in milliseconds that the WSA waited for the first byte of the server response.
- Calls for investigation of your upstream devices and WAN connection.
- **access logs** can show this in custom field **% : >1**

%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server







تتم كتابة بند سجل SHD فردي كل 60 ثانية ويحتوي على العديد من الحقول الهامة لمراقبة الأداء، بما في ذلك زمن الوصول و RPS وإجمالي الاتصالات من جانب العميل ومن جانب الخادم. هذا مثال على سطر سجل SHD:

```
Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 61
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 77
Fri Nov 11 14:18:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.6 Reqs 48 Band 7285 Latency 579
Fri Nov 11 14:19:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.6 Reqs 52 Band 34294 Latency 79
Fri Nov 11 14:20:43 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 8696 Latency 691
```

```
Fri Nov 11 14:21:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 49 Band 7064 Latency 140
Fri Nov 11 14:22:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.8 Reqs 41 Band 5444 Latency 788
Fri Nov 11 14:23:43 2022 Info: Status: CPULd 2.2 DskUtil 45.7 RAMUtil 6.8 Reqs 48 Band 6793 Latency 820
Fri Nov 11 14:24:44 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 44 Band 8735 Latency 673
Fri Nov 11 14:25:44 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 53 Band 8338 Latency 731
```

يمكن إضافة حقول مخصصة إضافية إلى ACCESS_LOG التي تشير إلى معلومات زمن الوصول للطلبات الفردية. تتضمن هذه الحقول إستجابة الخادم ودقة DNS وزمن وصول الماسح الضوئي AV. يجب إضافة الحقول إلى السجل للحصول على معلومات قيمة استخدامها في أستكشاف الأخطاء وإصلاحها. هذه هي سلسلة الحقول المخصصة الموصى بها للاستخدام:

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)
```

```
, Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<,
```

```
a; DNS response = %:
```

```
d, WBRS response = %:
```

```
r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respon
```

```
s, AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ][Client Port = %F, Server IP = %k
```

معلومات الأداء المستمدة من هذه القيم هي كما يلي:

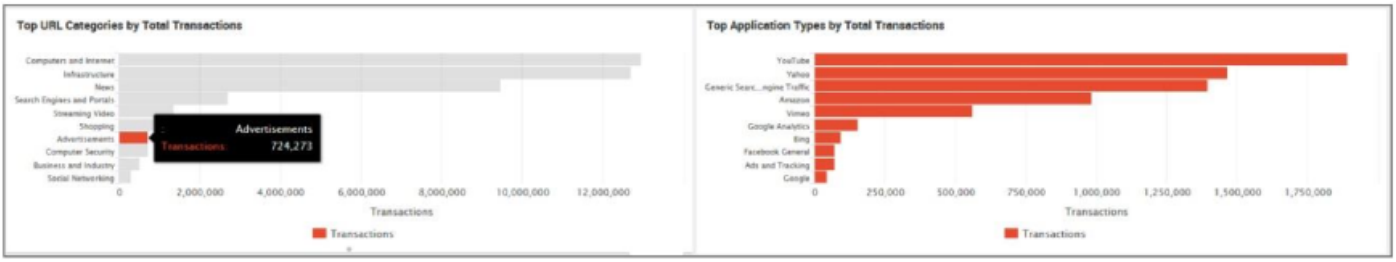
حقل مخصص	الوصف
%:<a	انتظر وقت تلقي الاستجابة من عملية مصادقة وكيل الويب، بعد أن قام وكيل الويب بإرسال الطلب.
%:<b	انتظر وقت كتابة نص الطلب إلى الخادم بعد الرأس.
%:<d	انتظر وقت تلقي الاستجابة من عملية DNS الخاصة بوكيل الويب، بعد أن قام وكيل الويب بإرسال الطلب.
%:<h	انتظر وقت كتابة رأس الطلب إلى الخادم بعد البايت الأول.
%:<r	انتظار وقت تلقي الاستجابة من عوامل تصفية سمعة الويب، بعد أن قام وكيل ويب بإرسال الطلب.
%:<s	انتظر وقت تلقي الحكم من عملية مكافحة برامج التجسس لوكيل الويب، بعد أن قام وكيل ويب بإرسال الطلب.
%:>	وقت الانتظار للحصول على بايت الاستجابة الأولى من الخادم.
%:>a	انتظار وقت تلقي الاستجابة من عملية مصادقة وكيل الويب، يتضمن الوقت المطلوب لوكيل الويب لإرسال الطلب.
%:>ب	انتظر وقت إكمال نص الاستجابة بعد إستلام الرأس.
%:>ج	الوقت المطلوب لوكيل ويب لقراءة إستجابة من ذاكرة التخزين المؤقت للقرص.
%:>d	انتظار وقت تلقي الاستجابة من عملية DNS لوكيل الويب، يتضمن الوقت المطلوب لوكيل الويب لإرسال الطلب.
%:>h	وقت الانتظار لرأس الخادم بعد بايت الاستجابة الأولى.
%:>r	انتظار وقت تلقي الحكم من عوامل تصفية سمعة الويب، يتضمن الوقت المطلوب لوكيل ويب لإرسال الطلب.
%:>s	انتظار وقت تلقي الحكم من عملية مكافحة برامج التجسس لوكيل ويب، يتضمن الوقت المطلوب لوكيل ويب لإرسال الطلب.
%:1<	وقت الانتظار لبايت الطلب الأول من اتصال العميل الجديد.
%:1>	انتظر وقت كتابة أول بايت إلى العميل.
%:b<	وقت الانتظار لإكمال نص العميل.
%:b>	انتظر وقت كتابة النص بالكامل إلى العميل.
%:e>	انتظار وقت تلقي الاستجابة من محرك المسح الضوئي AMP، بعد أن قام وكيل ويب بإرسال الطلب.
%:e<	وقت الانتظار لتلقي الحكم من محرك الفحص AMP، يتضمن الوقت المطلوب لوكيل الويب لإرسال الطلب.

%:h<	وقت الانتظار لرأس العميل الكامل بعد البايت الأول.
%:h>	انتظر وقت كتابة الرأس الكامل إلى العميل.
%:m<	وقت الانتظار لتلقي الحكم من محرك المسح الضوئي McAfee، يتضمن الوقت المطلوب لوكيل ويب لإرسال الطلب.
%:m>	انتظر وقت تلقي الاستجابة من محرك المسح الضوئي McAfee، بعد أن قام وكيل الويب بإرسال الطلب.
%f	منفذ مصدر العميل.
%p	منفذ خادم ويب.
%k	عنوان IP لمصدر البيانات (عنوان IP لخادم الويب).
%:w<	وقت الانتظار لتلقي الحكم من محرك المسح الضوئي ل Webroot، يتضمن الوقت المطلوب لوكيل ويب لإرسال الطلب.
%:w>	انتظر وقت تلقي الاستجابة من محرك المسح الضوئي ل Webroot، بعد أن قام وكيل الويب بإرسال الطلب.

يسمح نموذج ترخيص SWA بإعادة استخدام تراخيص الأجهزة المادية للأجهزة الظاهرية. يمكنك الاستفادة من هذا ونشر أجهزة SWAv للاختبار الاستخدام في بيئة المختبر. يمكن تجريب الميزات والتكوينات الجديدة بهذه الطريقة لضمان الاستقرار والموثوقية من دون خرق شروط الترخيص وفي الوقت نفسه عدم انتهاكها.

التقارير المتقدمة لأمان الويب (AWSR)

يجب الاستفادة من AWSR لتحقيق أقصى إستفادة من بيانات التقارير من SWA. خاصة في البيئات التي يتم فيها نشر العديد من النهج المتفرعة عن النطاق (SWA)، يكون هذا الحل أكثر قابلية للتطوير بعدة مرات من إستخدام إعداد تقارير مركزية على جهاز إدارة الأمان (SMA) فضلا عن توفير سمات إعداد تقارير مخصصة تضيف قدرا هائلا من العمق والتخصيص للبيانات. يمكن تجميع التقارير وتخصيصها لتلبية إحتياجات أية مؤسسة. يجب الاستفادة من مجموعة الخدمات المتقدمة من Cisco في تحديد الحجم ل AWSR.



التنبيه بالبريد الإلكتروني

يتم الاستفادة من نظام تنبيه البريد الإلكتروني المضمن في SWA على أفضل نحو كنظام تنبيه للخط الأساسي. ويجب تنقيطها على نحو مناسب لتلبية إحتياجات المسؤول، لأنها قد تكون مشوشة جدا إذا تم تمكين جميع الأحداث الإعلامية. من المهم الحد من التنبيهات ومراقبتها بفعالية أكثر من التنبيهات وتجاهلها كبريد عشوائي.

إعدادات التنبيه	التكوين
من العنوان المراد إستخدامه عند إرسال التنبيهات	تم الإنشاء تلقائيا
عدد الثواني الأولي للانتظار قبل إرسال	300 ثانية

تنبيه مكرر	
الحد الأقصى لعدد الثواني للانتظار قبل إرسال تنبيه مكرر	3600 ثانية

مراقبة التوفر

هناك طريقتان يمكن إستخدامهما لمراقبة توفر وكيل ويب.

1. الأولى هي مراقبة الطبقة 3 (L3)، والتي تختبر ما إذا كان عنوان IP للجهاز يمكن الوصول إليه على الشبكة. وأبسط طريقة لاختبار هذا الإجراء هي إرسال طلب صدى ICMP (ping) إلى العنوان على واصل زمنية منتظمة والتحقق من حزمة الرد. يمكن تحليل سمات الرد، مثل TTL وزمن الوصول لتحديد سلامة طبقة الشبكة.
2. من الممكن أن يكون الجهاز مستجيبا للاختلاط ولكن تكون عمليات الوكلاء غير مستجيبة أو متقطعة. ولهذا السبب، من المستحسن إستخدام شاشة من الطبقة 7 (L7)، التي ترسل طلب وكيل صريح إلى الجهاز وتتوقع رمز إستجابة HTTP 200 موافق. والذي يختبر هذا الأمر إمكانية الوصول إلى واجهة الشبكة فحسب، بل أيضا مدى إستجابة الخدمات الوكيلة وإمكانية إستمرارية خدمات الخادم في حالة طلب مرور خارجي. يتخذ هذا النوع من المراقبة عادة شكل طلب HTTP HEAD صريح يطلب من الوكيل الاتصال بمرور. يطلب أسلوب HEAD الرؤوس التي سيتم إرجاعها يجب على العميل إرسال طلب GET، ولكنه يتضمن رؤوس الردود فقط والبيانات.
   - إذا كنت تستخدم أداة أو برنامج نصي لمراقبة المستوى 7، فمن المهم التأكد من أن حركة المرور معافاة من المصادقة. وإلا فإن هذا يؤدي إلى حدوث حالات فشل في المصادقة المنتظمة واستهلاك المواراد. عند إستخدام سلسلة وكيل مستخدم مخصصة في أداة المراقبة يجب إستخدامه لتعريف حركة المرور. على الرغم من أن حركة المرور معافاة من المصادقة، إلا أنه لا يزال من الممكن تقييدها من الوصول غير الضروري إلى الإنترنت من خلال سياسات الوصول.

عند إستخدام طريقة أو أكثر من هذه الأساليب، يجب على المسؤول وضع خط أساس من المقاييس المقبولة حول إستجابة الوكيل واستخدام ذلك لإنشاء حدود تنبيهات. يجب أن تخصص وقتا لتجميع استجابات هذه التحقيقات وقبل أن تقرر كيفية تكوين الحدود والتنبيه.

مراقبة SNMP

بروتوكول إدارة الشبكة البسيط (SNMP) هو الطريقة الأساسية لمراقبة سلامة الجهاز. يمكن إستخدامه لاستلام تنبيهات من الجهاز (المصائد) أو لاستطلاع معرفات كائنات مختلفة (OIDs) لجمع المعلومات. هناك العديد من معرفات الأجهزة (OID) المتوفرة على SWA والتي تغطي كل شيء بدءا من الأجهزة وحتى إستخدام المواراد إلى معلومات العملية الفردية وإحصاءات الطلب.

هناك عدد من قاعدة معلومات الأجهزة (MIB) المحددة التي يجب مراقبتها لكل من الأسباب المتعلقة بالأجهزة والأداء. ويمكن الاطلاع على القائمة الكاملة لممثلي الإدارة هنا: https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt.

هذه قائمة بتقارير الإدارة (MIB) الموصى بها للمراقبة وليست قائمة شاملة:

معرف الجهاز OID	الاسم

1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	RAIDstatus
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	لودجلا ةحورم
1.3.6.1.4.1.15497.1.1.1.9.1.2	درجة مئوية

هذه هي خريطة OIDs مباشرة إلى إخراج أمر واجهة سطر الأوامر (CLI) تفصيل الحالة:

OID	الاسم	حقل تفاصيل الحالة
موارد النظام		
1.3.6.1.4.1.15497.1.1.1.2.0	perCentCPUUtile	وحدة المعالجة المركزية
1.3.6.1.4.1.15497.1.1.1.1.0	perCentMemoryUtilization	ذاكرة الوصول العشوائي
الحركات في الثانية		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	متوسط الحركات في الثانية في الدقيقة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	الحد الأقصى للحركات في الثانية في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	متوسط الحركات في الثانية في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	الحد الأقصى للحركات في الثانية منذ إعادة تشغيل الوكيل.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	متوسط الحركات في الثانية منذ إعادة تشغيل الوكيل.
النطاق الترددي		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalNow	متوسط النطاق الترددي في الدقيقة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	الحد الأقصى عرض النطاق الترددي في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	متوسط النطاق الترددي في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	الحد الأقصى للنطاق الترددي منذ إعادة تشغيل الوكيل.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	متوسط النطاق الترددي منذ إعادة تشغيل الوكيل.
وقت الاستجابة		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	متوسط معدل الوصول إلى ذاكرة التخزين المؤقت في الدقيقة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	الحد الأقصى لمعدل الوصول إلى

		ذاكرة التخزين المؤقت في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	متوسط معدل الوصول إلى ذاكرة التخزين المؤقت في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	الحد الأقصى لمعدل الوصول إلى ذاكرة التخزين المؤقت منذ إعادة تشغيل الوكيل.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	متوسط معدل الوصول إلى ذاكرة التخزين المؤقت منذ إعادة تشغيل الوكيل.
معدل الوصول إلى ذاكرة التخزين المؤقت		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	متوسط معدل الوصول إلى ذاكرة التخزين المؤقت في الدقيقة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	الحد الأقصى لمعدل الوصول إلى ذاكرة التخزين المؤقت في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	متوسط معدل الوصول إلى ذاكرة التخزين المؤقت في الساعة الأخيرة.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	الحد الأقصى لمعدل الوصول إلى ذاكرة التخزين المؤقت منذ إعادة تشغيل الوكيل.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	متوسط معدل الوصول إلى ذاكرة التخزين المؤقت منذ إعادة تشغيل الوكيل.
الاتصالات		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	إتصالات العميل الخاملة.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	إتصالات الخادم الخامل.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	إجمالي إتصالات العميل.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	إجمالي إتصالات الخادم.

القرار

يسعى هذا الدليل إلى وصف أهم جوانب تكوين SWA ونشره ومراقبته. وهدفه، كدليل مرجعي، هو توفير معلومات قيمة لأولئك الذين أرادوا ضمان الاستخدام الأكثر فعالية للنهج الاستراتيجي. إن أفضل الممارسات الموضحة هنا مهمة لاستقرار الجهاز وقابلية توسيعه وفعاليته كأداة أمان. كما يسعى هذا البرنامج إلى أن يظل مواكبا لكل مضت قدما، ومن ثم يجب تحديثه بشكل متكرر ليعكس التغييرات في بيئات الشبكات ومجموعات ميزات المنتجات.

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).