تجاوز حركة مرور تحديثات Microsoft في جهاز ويب الآمن

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

تحديثات Microsoft

تجاوز تحديثات Microsoft

تجاوز حركة المرور في SWA

خطوات تمرير تحديثات Microsoft

معلومات ذات صلة

المقدمة

يصف هذا المستند الخطوات اللازمة لتجاوز حركة مرور تحديثات Microsoft في تطبيق ويب الآمن (SWA).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أدارة /سوا/.

توصي Cisco بتثبيت هذه الأدوات:

- SWA المادية أو الافتراضية
- الوصول الإداري إلى واجهة المستخدم الرسومية (GUI) ل SWA

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تحديثات Microsoft

تعد تحديثات Microsoft تصحيحات أساسية وتحديثات أمان وتحسينات مميزات تم إصدارها بواسطة Microsoft لأنظمة التشغيل وتطبيقات البرامج الخاصة بها. تعد هذه التحديثات أمرا بالغ الأهمية للحفاظ على أمان أجهزة الكمبيوتر وأجهزة الشبكة واستقرارها وأدائها. فهي تضمن حماية الأنظمة من نقاط الضعف، وتثبيت الأخطاء، ودمج مميزات أو تحسينات جديدة في البرنامج.

يمكن أن يكون تأثير تحديثات Microsoft على الخوادم الوكيل، مثل Cisco SWA، كبيرا. تتضمن هذه التحديثات في كثير من الأحيان تنزيل ملفات كبيرة أو ملفات أصغر، مما قد يؤدي إلى إستهلاك نطاق ترددي كبير وموارد معالجة كبيرة على الوكيل. وقد يؤدي ذلك إلى حدوث إزدحام شديد وأداء أبطأ للشبكة وتحميل متزايد على البنية الأساسية للوكيل، مما قد يؤثر على تجربة المستخدم الإجمالية وغيرها من عمليات الشبكة بالغة الأهمية.

يمكن أن يكون تجاوز حركة مرور Microsoft Update من الوكيل طريقة آمنة وفعالة لإدارة هذه التحديات. ونظرا لأن تحديثات Microsoft يتم الحصول عليها من خوادم Microsoft الموثوق بها، فإن السماح لحركة المرور هذه بتجاوز الوكيل يمكن أن يساعد في تقليل الحمل على الخادم الوكيل دون المساس بأمان الشبكة. وهذا يضمن توفير التحديثات الأساسية بكفاءة مع الحفاظ على موارد الوكيل لمهام الأمان وتصفية المحتوى الأخرى. ومع ذلك، من المهم تنفيذ هذه التكوينات الالتفافية بعناية للحفاظ على أمان الشبكة العام والامتثال للسياسات التنظيمية.

تجاوز تحديثات Microsoft

إذا كنت تفكر في تجنب وكيل حركة مرور تحديثات Microsoft، فهناك نهجان رئيسيان:

1. تجاوز: وهذا يتضمن تكوين الشبكة لإعادة توجيه حركة المرور حتى لا تصل إلى SWA أبدا.
2. المرور: وهذا يتضمن تكوين SWA بحيث لا تقوم بفك تشفير حركة مرور تحديثات Microsoft أو مسحها ضوئيا، مما يسمح لها بالمرور عبر الوكيل دون فحص.

تجاوز حركة المرور في SWA

ولتجاوز حركة مرور تحديثات Microsoft في الشبكات المزودة ب SWA، يختلف هذا النهج باختلاف إعداد نشر الوكيل الخاص بك:

نوع النشر	تجاوز حركة المرور
النشر الشفاف	يمكنك إعادة توجيه حركة مرور تحديثات Microsoft في الموجه أو محولات الطبقة 4 المسؤولة عن إعادة توجيه حركة مرور البيانات إلى الخادم الوكيل.
	أنت يستطيع شكلت مجرى جانبي عملية إعداد مباشرة ضمن ال SWA graphical مستعمل قارن (GUI).

نشر صريح	لمنع حركة مرور تحديثات Microsoft من الوصول إلى SWA، يجب تكوين الالتفاف في المصدر. وهذا يعني إعفاء عناوين URL ذات الصلة على أجهزة العميل لضمان عدم إعادة توجيه حركة المرور إلى SWA.

إذا كان تجاوز حركة مرور معينة يتطلب إعادة تصميم شبكة واسعة النطاق وهو أمر غير ممكن، فإن هناك نهجا بديلا يتمثل في تكوين SWA للمرور عبر أنواع معينة من حركة المرور. يمكن تحقيق ذلك من خلال ضبط SWA على عدم فك تشفير حركة المرور المحددة أو مسحها ضوئيا، والسماح لها بالمرور عبر الوكيل دون فحص. تضمن هذه الطريقة توفير حركة مرور البيانات الأساسية بكفاءة مع تقليل التأثير على أداء الشبكة ومواردالوكيل إلى الحد الأدنى.

خطوات تمرير تحديثات Microsoft

هناك أربع مراحل رئيسية لعبور عمليات تحديث Microsoft:

مرحلة	خطوات
1. إنشاء فئة عنوان URL مخصص لعناوين URL الخاصة بتحديثات Microsoft	الخطوة 1. من واجهة المستخدم الرسومية، أختر إدارة أمان الويب ثم انقر فوق فئات عنوان URL المخصص والخارجي. الخطوة 2.انقر فوق إضافة الفئة لإضافة فئة URL مخصصة. الخطوة 3. قم بتعيين اسم فئة فريد. الخطوة 4. (إختياري) أضف وصفا. الخطوة 5. من ترتيب القائمة، أختر الفئة الأولى التي تريد وضعها في الأعلى. الخطوة 6. من القائمة المنسدلة للفئة، أختر فئة مخصصة محلية. الخطوة 7. أضف عناوين URL الخاصة بتحديثات Microsoft في قسم المواقع.

تلميح: يمكنك التحقق من قائمة تحديثات Microsoft من هذا الارتباط: الخطوة 2 - تكوين WSU | Microsoft Learn

تحذير: لا تنسخ/تلصق عناوين URL كما هو الحال في مستندات Microsoft؛ قم بتكوينهم بشكل صحيح كتنسيق SWA. لمزيد من المعلومات، يرجى زيارة: تكوين فئات URL المخصصة في

	جهاز ويب الآمن - Cisco الخطوة 8. إرسال.
2. إنشاء ملف تعريف لإعفاء حركة مرور تحديثات Microsoft من المصادقة	الخطوة 9.من واجهة المستخدم الرسومية، أختر مدير أمان الويب ثم انقر على ملفات تعريف. الخطوة 10.انقر على إضافة ملف تعريف لإضافة ملف تعريف. الخطوة 11. أستخدم مربع تمكين ملف التعريف لتمكين ملف التعريف هذا، أو لتعطيله بسرعة دون حذفه. الخطوة 12.قم بتعيين اسم ملف تعريف فريد. الخطوة 13. (إختياري) أضف وصفا. الخطوة 14.من القائمة إدراج ما سبق ذكره المنسدلة، أختر مكان ظهور ملف التعريف هذا في الجدول. الخطوة 15. في MethodSection لتعريف المستخدم، أخترExempt من المصادقة/التعريف. الخطوة 16.في تحديد الأعضاء بواسطة الشبكة الفرعية، إذا كنت ترغب في مرور بيانات Microsoft لبعض المستخدمين المحددين، فأدخل عناوين IP أو الشبكات الفرعية التي تنطبق، أو أترك هذا الحقل فارغا لتضمين جميع عناوين IP. الخطوة 17. من قسم متقدم، أختر فئات عنوان URL المخصصة. الخطوة 18. أضف فئة عنوان URL المخصص التي تم إنشاؤها لتحديثات Microsoft. الخطوة 19. انقر فوق تم. الخطوة 20. إرسال.
3. إنشاء سياسة فك تشفير لنقل بيانات تحديثات Microsoft	الخطوة 21. من واجهة المستخدم الرسومية، أختر إدارة أمان الويب ثم انقر فوق نهج فك التشفير. الخطوة 22. انقر فوق إضافة نهج لإضافة سياسة فك تشفير. الخطوة 23. أستخدم خانة الاختيار تمكين النهج لتمكين هذا النهج. الخطوة 24.قم بتعيين اسم نهج فريد.

	الخطوة 25. (إختياري) أضف وصفا. الخطوة 26. من القائمة المنسدلة إدراج أعلاه للنهج، أختر النهج الأول. الخطوة 27.من توصيفات التعريف والمستخدمين، أختر ملف تعريف التعريف الذي أنشأته في الخطوات السابقة. الخطوة 28. إرسال. الخطوة 29.في نهج فك التشفير، ضمن تصفية URL، انقر فوق الارتباط المرتبط بنهج فك التشفير الجديد هذا. الخطوة 30.SelectPassthroughas الإجراء الخاص بفئة عنوان URL لتحديثات Microsoft. الخطوة 31. إرسال.
4. قم بإنشاء نهج Access للسماح بحركة مرور تحديثات Microsoft	الخطوة 32. من واجهة المستخدم الرسومية، أختر إدارة أمان الويب ثم انقر فوق نهج الوصول. الخطوة 33. انقر فوق إضافة نهج لإضافة سياسة وصول. الخطوة 34. أستخدم خانة الاختيار تمكين النهج لتمكين هذا النهج. الخطوة 35.قم بتعيين اسم نهج فريد. الخطوة 36. (إختياري) أضف وصفا. الخطوة 37. من القائمة المنسدلة إدراج أعلاه للنهج، أختر النهج الأول. الخطوة 38.من توصيفات التعريف والمستخدمين، أختر ملف تعريف التعريف الذي أنشأته في الخطوات السابقة. الخطوة 39. إرسال. الخطوة 40. في صفحة سياسات الوصول، ضمن تصفية URL، انقر فوق الارتباط المقترن بنهج الوصول الجديد هذا الخطوة 41. حدد الإجراء Allowas لفئة URL المخصصة التي تم إنشاؤها ل Microsoft Update. الخطوة 42. إرسال. الخطوة 43. إجراء التغييرات.

معلومات ذات صلة

- دليل المستخدم ل AsyncOS 15.0 ل Cisco Secure Web Appliance - GD(نشر عام) - تصنيف المستخدمين النهائيين لتطبيق السياسة [جهاز الويب الآمن من Cisco] - Cisco
- تكوين فئات عنوان URL المخصصة في جهاز ويب الآمن - Cisco
- كيفية إستثناء حركة مرور Office 365 من المصادقة وفك التشفير على جهاز أمان الويب (WSA) من Cisco - Cisco
- إستخدام أفضل ممارسات جهاز الويب الآمن - Cisco
- تجاوز المصادقة في جهاز الويب الآمن - Cisco

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 دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).