نم (WSA) بيولا نامأ زاهج جلاعي فيك Cisco نم (Skype رورم ةكرح

المحتويات

<u>سؤال:</u>

سؤال:

كيف يعالج جهاز أمان الويب (WSA) من Cisco حركة مرور Skype؟

Cisco WSA، Skype :البيئة

Skype هو شبكة هاتفية خاصة بالإنترنت (VoIP). ويعمل سكايب في المقام الأول كبرنامج نظير إلى نظير، وبالتالي فهو لا يتصل بشكل مباشر مع خادم مركزي ليعمل. وقد يكون حظر سكايب أمرا صعبا بشكل خاص لأنه سيحاول الاتصال بعدة طرق مختلفة.

يتصل Skype بالترتيب التالي للأفضلية:

- 1. توجيه حزم UDP إلى النظراء الآخرين باستخدام أرقام المنافذ العشوائية
- 2. توجيه حزم TCP إلى النظراء الآخرين باستخدام أرقام المنافذ العشوائية
- 3. توجيه حزم TCP إلى النظراء الآخرين باستخدام المنفذ 80 و/أو المنفذ 443
 - 4. الحزم المنضمة عبر وكيل ويب باستخدام اتصال HTTP بالمنفذ 443

عند النشر في بيئة وكيل صريحة، لن يتم إرسال الطرق 1-3 إلى Cisco WSA أبدا. لحظر Skype، يجب أولا حظره من موقع آخر في الشبكة. يمكن حظر خطوات 3-1 Skype باستخدام:

- جدار الحماية: إستخدام NBAR لحظر الإصدار 1 من Skype. يتوفر المزيد من المعلومات على موقع http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
 - Cisco IPS (ASA): يمكن أن يقوم Cisco ASA باكتشاف Skype وحظره عبر التوقيعات.

عندما يعود Skype إلى إستخدام وكيل صريح، لا يقدم Skype عمدا أي تفاصيل عميل في طلب اتصال HTTP (لا توجد سلسلة وكيل مستخدم أيضا). وهذا يجعل من الصعب التمييز بين طلب Skype وطلب Connect صالح. سيتصل Skype دائما بالمنفذ 443 ويكون عنوان الوجهة دائما عنوان IP.

<u>مثال:</u>

الاتصال برقم http/1.0 10.129.88.11:443 اتصال الوكيل: البقاء على قيد الحياة

سيؤدي نهج الوصول التالي إلى حظر أي طلبات اتصال من خلال WSA التي تطابق عناوين IP والمنفذ 443. سيطابق هذا كل حركة مرور Skype. ومع ذلك، فإن البرامج التي لا تستخدم Skype والتي تحاول النفق إلى عنوان IP على المنفذ 443 سيتم حظرها أيضا.

حظر Skype - بيئة صريحة مع تعطيل وكيل HTTPS

قم بإنشاء فئة عنوان URL مخصصة لمطابقة حركة مرور IP ومنفذ 443:

1. انتقل إلى "إدارة الأمان" -> "فئات عنوان URL المخصصة" -> "إضافة فئة مخصصة". 2. املأ "اسم الفئة" ووسع "متقدم". 3. أستخدم "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+.[0-9]+" في نافذة التعبير العادي. تعيين هذه الفئة للرفض في نهج الوصول: 1. انتقل إلى "إدارة أمان الويب" -> "سياسات الوصول".

1. انتقل إلى "إدارة أمان الويب" -> "سياسات الوصول". 2. انقر فوق الارتباط الموجود ضمن العمود "فئات عنوان URL" لمجموعة النهج المناسبة. 3. في قسم "تصفية فئة URL المخصص"، أختر "حظر" لفئة Skype الجديدة. 4. إرسال التغييرات وتنفيذها <u>ملاحظة:</u> لا يمكن حظر طلبات الاتصال الصريحة إلا في حالة تعطيل خدمة وكيل HTTPS!

عند تمكين فك تشفير WSA HTTPS، قد تنقطع حركة مرور Skype على الأرجح لأنها ليست حركة مرور HTTPS فقط (برغم إستخدام Connect و Port 443). سيؤدي ذلك إلى حدوث خطأ 502 تم إنشاؤه بواسطة WSA وسيتم إسقاط الاتصال. ستستمر أي حركة مرور ويب حقيقية ل HTTPS إلى عنوان IP في العمل (رغم أنه سيتم فك تشفيرها على WSA).

حظر Skype - بيئة واضحة/شفافة مع تمكين وكيل HTTPS

قم بإنشاء فئة مخصصة لمطابقة IP وحركة مرور المنفذ 443:

- 1. انتقل إلى "إدارة الأمان" -> "فئات عنوان URL المخصصة" -> "إضافة فئة مخصصة".
 - 2. املأ "اسم الفئة" ووسع "متقدم".
 - 3. أستخدم "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" في نافذة التعبير العادي.

تعيين هذه الفئة لفك التشفير في نهج فك التشفير:

1. انتقل إلى "إدارة أمان الويب" -> "سياسات فك التشفير".

2. انقر فوق الارتباط الموجود ضمن العمود "فئات عنوان URL" لمجموعة النهج المناسبة.

3. في قسم "تصفية فئة URL المخصص"، أختر "فك تشفير" لفئة Skype الجديدة.

4. إرسال التغييرات وتنفيذها.

<u>ملاحظة:</u> نظرا لأنه يتم إرسال حركة مرور Skype إلى IP، فسوف يتم اعتبارها كجزء من "عناوين URL غير المصنفة". سيحدث نفس التأثير المذكور أعلاه بناء على ما إذا كان الإجراء هو فك التشفير أو المرور.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما