اكتشاف البوابة المقيدة لـ AnyConnect ومعالجتها

المحتويات

المقدمة

يصف هذا المستند ميزة اكتشاف المنفذ المقيد Cisco AnyConnect Mobility Client ومتطلبات عمله بشكل صحيح. تستخدم العديد من النقاط الفعالة اللاسلكية في الفنادق والمطاعم والمطارات والأماكن العامة الأخرى البوابات الأسيرة لحجب وصول المستخدمين إلى الإنترنت. يقومون بإعادة توجيه طلبات HTTP إلى مواقع الويب الخاصة بهم التي تتطلب من المستخدمين إدخال بيانات الاعتماد الخاصة بهم أو الإقرار بالأحكام والشروط الخاصة بمضيف النقاط الساخنة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بـ Cisco AnyConnect Secure Mobility Client.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- AnyConnect الإصدار 3.1.04072
- أجهزة الأمان المعدلة (Cisco Adaptive Security Appliance (ASA، الإصدار 9.1.2

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

معلومات أساسية

تتطلب العديد من المنشآت التي توفر شبكة Wi-Fi وإمكانية الوصول السلكي، مثل المطارات والمقاهي والفنادق، أن يدفع المستخدمون قبل الحصول على إمكانية الوصول، أو أن يوافقوا على الالتزام بسياسة إستخدام مقبولة، أو كليهما. وتستخدم هذه المرافق أسلوبا يسمى المدخل الأسير لمنع التطبيقات من الاتصال إلى أن يفتح المستخدمون متصفحا ويقبلون شروط الوصول.

متطلبات إصلاح البوابة المأسورة

يتطلب دعم كل من اكتشاف البوابة المقيدة ومعالجتها أحد هذه التراخيص:

- إصدار VPN الخاص ب AnyConnect Premium (طبقة مآخذ التوصيل الآمنة (SSL))
- Cisco AnyConnect Secure Mobility

يمكنك إستخدام ترخيص Cisco AnyConnect Secure Mobility من أجل توفير الدعم لاكتشاف البوابة المقيدة ومعالجتها بالاقتران مع أي من AnyConnect Essentials أو ترخيص AnyConnect Premium.

ملاحظة: يتم دعم اكتشاف المدخل الموقوف ومعالجته على نظامي التشغيل Microsoft Windows و Macintosh OS X مدعومين بإصدار AnyConnect قيد الاستخدام.

اكتشاف نقطة اتصال البوابة المقيدة

يعرض AnyConnect **ال يعجز أن يتصل VPN نادل** رسالة على ال gui إن هو يستطيع لا يربط، regardless of السبب. يحدد خادم VPN البوابة الآمنة. في حالة تمكين "الاتصال الدائم" وعدم وجود مدخل أسير، يستمر العميل في محاولة الاتصال بالشبكة الخاصة الظاهرية (VPN) وتحديث رسالة الحالة وفقا لذلك.

في حال تمكين الشبكة الخاصة الظاهرية (VPN) "الدائمة"، يتم إغلاق سياسة فشل الاتصال وتعطيل إصلاح البوابة المقيدة، ويكشف AnyConnect عن وجود بوابة أسيرة، ثم يعرض واجهة المستخدم الرسومية (GUI) ل AnyConnect هذه الرسالة مرة واحدة لكل اتصال ومرة واحدة لكل إعادة اتصال:

```
.The service provider in your current location is restricting access to the Internet
The AnyConnect protection settings must be lowered for you to log on with the service
.provider. Your current enterprise security policy does not allow this
```

إذا كشف AnyConnect عن وجود مدخل أسير ويختلف تكوين AnyConnect عن التكوين الذي تم وصفه مسبقا، فإن واجهة المستخدم الرسومية (GUI) ل AnyConnect تعرض هذه الرسالة مرة واحدة لكل اتصال ومرة واحدة لكل إعادة اتصال:

```
.The service provider in your current location is restricting access to the Internet
.You need to log on with the service provider before you can establish a VPN session
.You can try this by visiting any website with your browser
```

تحذير: يتم تمكين الكشف عن المدخل المتنقل بشكل افتراضي وهو غير قابل للتكوين. لا يقوم AnyConnect بتعديل أي إعدادات تكوين للمستعرض أثناء اكتشاف البوابة المقيدة.

إصلاح نقطة اتصال المدخل المتنقل

يقصد ب Captive Portal Relmediation العملية التي تستوفي فيها متطلبات نقطة اتصال عبر المدخل موجودة في الأسر للحصول على إمكانية الوصول إلى الشبكة.

لا يقوم AnyConnect بإصلاح البوابة المقيدة، وهو يعتمد على المستخدم النهائي لإجراء عملية الإصلاح.

لتنفيذ عملية إصلاح البوابة المقيدة، يلبي المستخدم النهائي متطلبات موفر النقاط الساخنة. وقد تشمل هذه المتطلبات

دفع رسم للوصول إلى الشبكة، أو توقيع على سياسة إستخدام مقبولة، أو اشتراط آخر يحدده الموفر.

يجب السماح بشكل صريح بمعالجة المدخل المتنقل في ملف تعريف عميل AnyConnect VPN إذا تم تمكين AnyConnect Always-on وتم تعيين نهج فشل الاتصال على "مغلق". إذا تم تمكين "الاتصال الدائم" وتم تعيين نهج فشل الاتصال على "فتح"، فلن تحتاج إلى السماح بشكل صريح بمعالجة البوابة المقيدة في ملف تعريف عميل AnyConnect VPN لأن المستخدم غير مقيد من الوصول إلى الشبكة.

اكتشاف البوابة المقيدة خطأ

يمكن أن يفترض AnyConnect بشكل زائف أنه في بوابة أسيرة في هذه الحالات.

- إذا حاول AnyConnect الاتصال ب ASA مع شهادة تحتوي على اسم خادم (CN) غير صحيح، فسيظن عميل AnyConnect أنه في بيئة مدخل احتيالية.

  لمنع هذه المشكلة، تأكد من تكوين شهادة ASA بشكل صحيح. يجب أن تتطابق قيمة CN في الشهادة مع اسم خادم ASA في ملف تعريف عميل VPN.

- إذا كان هناك جهاز آخر على الشبكة قبل ASA يستجيب لمحاولة العميل الاتصال ب ASA عن طريق حظر وصول HTTPS إلى ASA، عندئذ سيظن عميل AnyConnect أنه في بيئة مدخل احتيالية. يمكن أن يحدث هذا الموقف عندما يكون المستخدم على شبكة داخلية ويتصل من خلال جدار حماية للاتصال ب ASA.

  إذا كان يجب عليك تقييد الوصول إلى ASA من داخل الشركة، فقم بتكوين جدار الحماية بحيث لا ترجع حركة مرور HTTP و HTTPS إلى عنوان ASA حالة HTTP. يجب السماح بوصول HTTP/HTTPS إلى ASA أو حظره بالكامل (المعروف أيضا باسم Black-holed) لضمان عدم إرجاع طلبات HTTP/HTTPS المرسلة إلى ASA إستجابة غير متوقعة.

سلوك AnyConnect

يوضح هذا القسم كيفية تصرف AnyConnect.

يحاول AnyConnect أستكشاف HTTPS إلى اسم المجال المؤهل بالكامل (FQDN) المحدد في ملف تعريف XML.

2. إذا كان هناك خطأ في الشهادة (FQDN غير موثوق به/خطأ)، فسيحاول AnyConnect تحقيق HTTP إلى FQDN المحدد في ملف تعريف XML. في حالة وجود أي إستجابة أخرى غير 302 HTTP، فإنها تعتبر نفسها خلف بوابة أسيرة.

تم اكتشاف البوابة المقيدة بشكل غير صحيح مع IKEv2

عند محاولة اتصال الإصدار 2 من مفتاح الإنترنت (IKEv2 Internet Key Exchange) ب ASA مع تعطيل مصادقة SSL التي تشغل مدخل إدارة أجهزة الأمان المعدلة (ASDM) على المنفذ 443، ينتج عن تحقيق HTTPS الذي تم إجراؤه للكشف عن المدخل المتنقل إعادة التوجيه إلى مدخل **/admin/public/index.html**) ASDM). نظرا لأن العميل لا يتوقع هذا، فيبدو كعملية إعادة توجيه للمدخل الموقوف، ويتم منع محاولة الاتصال لأنه يبدو أنه يلزم إجراء إصلاح للمدخل الموقوف.

الحلول

إذا واجهت هذه المشكلة، ففيما يلي بعض الحلول البديلة:

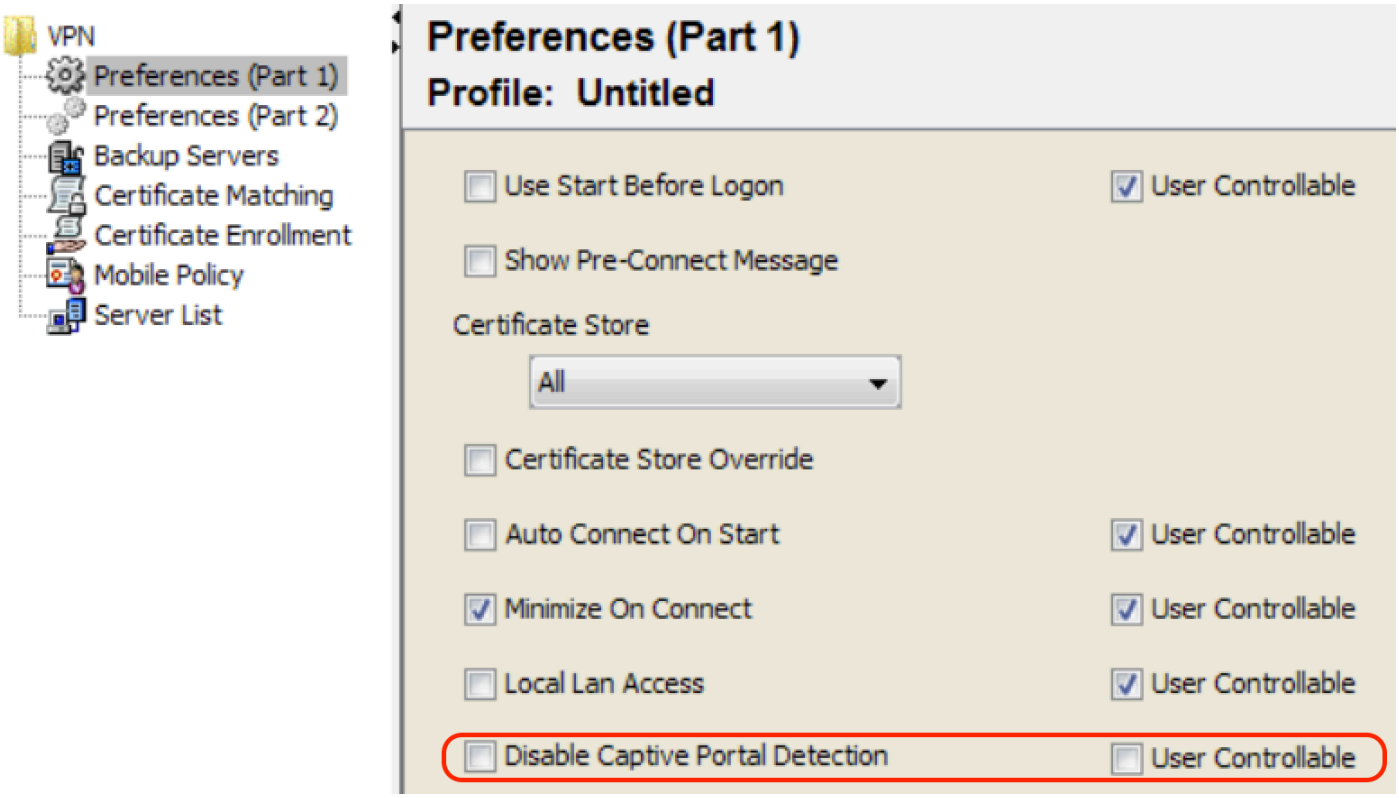
- قم بإزالة أوامر HTTP على هذه الواجهة حتى لا ينصت ASA إلى إتصالات HTTP على الواجهة.
- قم بإزالة TrustPoint ل SSL على الواجهة.
- تمكين خدمات عميل IKEV2.
- تمكين WebVPN على الواجهة.

حللت هذا إصدار ب cisco بق CSCud17825 id في صيغة 3.1(3103).

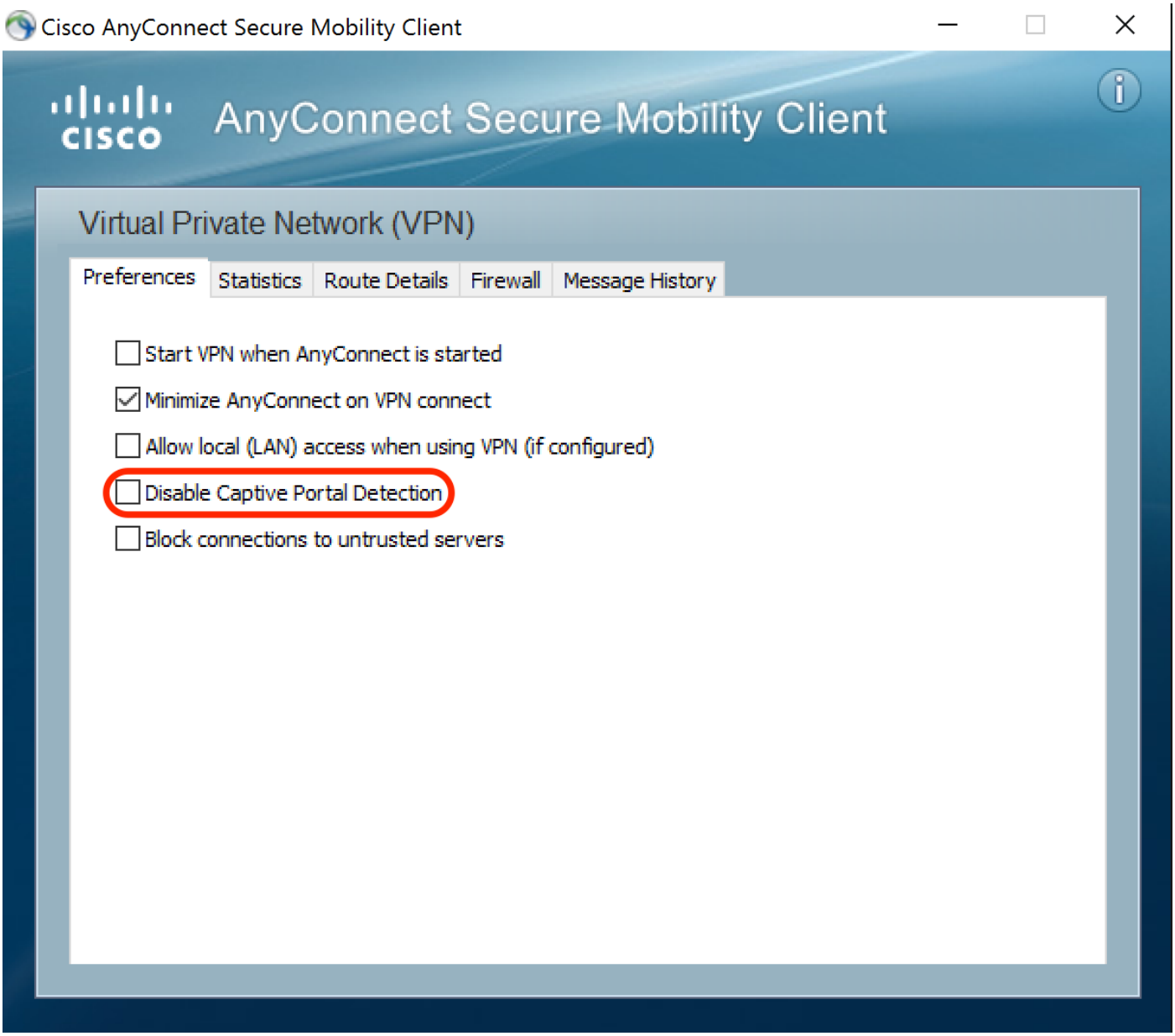
تحذير: توجد المشكلة نفسها لموجهات Cisco IOS®. إذا تم تمكين **ip http server** على برنامج Cisco IOS، والذي يكون مطلوبا إذا تم إستخدام نفس المربع كخادم PKI، فإن AnyConnect يكتشف البوابة المقيدة بشكل زائف. الحل البديل هو إستخدام **ip http access-class** لإيقاف الاستجابات لطلبات AnyConnect HTTP، بدلا من طلب المصادقة.

تعطيل ميزة "المدخل الأسير"

من الممكن تعطيل ميزة "المدخل الأسير" في الإصدار 4.2.00096 من AnyConnect client والإصدارات الأحدث (راجع معرف تصحيح الأخطاء من Cisco CSCud97386). يمكن للمسؤول تحديد ما إذا كان يجب أن يكون الخيار قابلا للتكوين من قبل المستخدم أم معطلا. يتوفر هذا الخيار تحت قسم التفضيلات (الجزء 1) في محرر ملف التخصيص. يمكن أن يختار المسؤول **تعطيل الكشف عن المدخل المتنقل** أو **تحكم المستخدم** كما هو موضح في لقطة محرر ملف التعريف هذه:



إذا تم تحديد إمكانية تحكم المستخدم، يظهر مربع الاختيار في علامة التبويب "تفضيلات" بواجهة مستخدم AnyConnect Secure Mobility Client كما هو موضح هنا:


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Start VPN when AnyConnect is started
Minimize AnyConnect on VPN connect
Allow local (LAN) access when using VPN (if configured)
Disable Captive Portal Detection
Block connections to untrusted servers

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).