التشغيل البيني بين AnyConnect وعميل OpenDNS المتجول

المحتويات

المقدمة

يصف هذا المستند بعض القيود الحالية والحلول البديلة المتاحة لجعل AnyConnect و OpenDNS Roaming Client يعملان معا. يعتمد عملاء Cisco على عميل AnyConnect VPN لإجراء إتصالات آمنة ومشفرة بشبكات شركاتهم. وبالمثل، يتيح عميل OpenDNS المتجول للمستخدمين إمكانية إستخدام خدمات DNS بأمان بمساعدة خوادم OpenDNS العامة. يضيف كلا هذين العملين مجموعة غنية من ميزات الأمان على نقطة النهاية، وبالتالي من المهم بالنسبة لهما التفاعل مع بعضهما البعض.

المتطلبات الأساسية

معرفة العمل الخاصة بالعميل المتجول AnyConnect و OpenDNS.

معرفة بتكوين وحدة الاستقبال والبث ASA أو tunnel-group/group-policy) IOS/IOS-XE) ل AnyConnect VPN.

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة الاستقبال والبث ASA أو IOS/IOS-XE
- نقطة النهاية التي تشغل عميل AnyConnect VPN وعميل تجوال OpenDNS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة الاستقبال والبث الخاصة ب ASA، الإصدار 9.4
- نظام التشغيل Windows 7
- AnyConnect Client 4.2.00096
- OpenDNS Roaming Client 2.0.154

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

يقوم OpenDNS بتطوير مكون إضافي ل AnyConnect مع فريق Cisco AnyConnect لكي يكون متوفرا في المستقبل. على الرغم من عدم تعيين أي تواريخ، إلا أن هذا التكامل سيسمح للعميل المتجول بالعمل مع عميل AnyConnect دون إستخدام الحلول التي يتم معالجتها. سيؤدي هذا أيضا إلى تمكين AnyConnect من أن يكون آلية تسليم للعميل المتجول.

الوظائف

معالجة DNS ل AnyConnect

يمكن تكوين وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN) بعدة طرق مختلفة لمعالجة حركة مرور البيانات من عميل AnyConnect.

تكوين النفق الكامل (tunnel-all): يفرض هذا حركة مرور البيانات من نقطة النهاية التي سيتم إرسالها عبر نفق VPN مشفرة، وبالتالي لا تترك حركة مرور البيانات محول الواجهة العامة في نص واضح أبدا
تكوين نفق التقسيم:
أ. تقسيم التضمين النفقي: يتم إرسال حركة المرور الموجهة فقط إلى شبكات فرعية أو مضيفات محددة على وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN) عبر النفق، ويتم إرسال جميع حركات المرور الأخرى خارج النفق في نص واضح

ب. الاتصال النفقي بإستثناء الانقسام: يتم إستبعاد حركة المرور الموجهة فقط إلى شبكات فرعية أو مضيفات معينة معرفة على وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN) من التشفير وتغادر الواجهة

العامة في نص واضح، ويتم تشفير جميع حركات المرور الأخرى ويتم إرسالها عبر النفق فقط

يحدد كل تكوين من هذه التكوينات كيفية معالجة تحليل DNS بواسطة عميل AnyConnect، اعتمادا على نظام التشغيل على نقطة النهاية. حدث تغيير في السلوك في آلية معالجة DNS على AnyConnect ل Windows، في الإصدار 4.2 بعد إصلاح CSCuf07885.

نظام التشغيل Windows 7+

تكوين Tunnel-all (وتقسيم الاتصال النفقي مع تمكين جميع DNS للنفق)

قبل AnyConnect 4.2:

مسموح فقط بطلبات DNS إلى خوادم DNS التي تم تكوينها ضمن نهج المجموعة (خوادم DNS للنفق). يستجيب برنامج تشغيل AnyConnect لجميع الطلبات الأخرى باستجابة "بدون مثل هذا الاسم". ونتيجة لذلك، يمكن تنفيذ دقة DNS فقط باستخدام خوادم DNS النفق.

AnyConnect 4.2 +

يسمح بطلبات DNS إلى أي من خوادم DNS، طالما تم إنشاؤها من محول VPN ويتم إرسالها عبر النفق. يتم الاستجابة لجميع الطلبات الأخرى باستخدام الاستجابة "بدون هذا الاسم"، ويمكن إجراء تحليل DNS فقط عبر نفق VPN

قبل إصلاح CSCuf07885، يقيد AC خوادم DNS الهدف، ومع ذلك مع إصلاح CSCuf07885، فإنه يقيد أي مهايئات الشبكة يمكن أن تبدأ طلبات DNS.

تكوين Split-include (Tunnel-all DNS معطل و no split-DNS)

لا يتعارض برنامج تشغيل AnyConnect مع محلل DNS الأصلي. وبالتالي، يتم إجراء تحليل DNS بناء على ترتيب مهايئات الشبكة، ودائما ما يكون AnyConnect هو المحول المفضل عندما تكون الشبكة الخاصة الظاهرية (VPN) متصلة. لذلك سيتم إرسال استعلام DNS أولا عبر النفق وإذا لم يتم حله، فسيحاول المحلل حله عبر الواجهة العامة. يجب أن تتضمن قائمة الوصول ذات التضمين المقسم الشبكة الفرعية التي تغطي خادم (خوادم) DNS للنفق. بدءا من AnyConnect 4.2، تتم إضافة المسارات المضيفة لخادم (خوادم) DNS للنفق تلقائيا كشبكات مقسمة-مضمنة (مسارات آمنة) بواسطة عميل AnyConnect، وبالتالي فإن قائمة الوصول المنقسم-include لم تعد تتطلب إضافة صريحة للشبكة الفرعية لخادم DNS للنفق.

تكوين Split-exclude (Tunnel-all DNS معطل و no split-DNS)

لا يتعارض برنامج تشغيل AnyConnect مع محلل DNS الأصلي. وبالتالي، يتم إجراء تحليل DNS بناء على ترتيب مهايئات الشبكة، ودائما ما يكون AnyConnect هو المحول المفضل عندما تكون الشبكة الخاصة الظاهرية (VPN) متصلة. لذلك سيتم إرسال استعلام DNS أولا عبر النفق وإذا لم يتم حله، فسيحاول المحلل حله عبر الواجهة العامة. يجب ألا تتضمن قائمة الوصول المستثناة الشبكة الفرعية التي تغطي خادم (خوادم) DNS للنفق. بدءا من AnyConnect 4.2، تتم إضافة المسارات المضيفة لخادم (خوادم) DNS للنفق تلقائيا كشبكات مقسمة (مسارات آمنة) بواسطة عميل AnyConnect، وبالتالي فإن هذا سيمنع التكوين غير الصحيح في قائمة الوصول للاستبعاد المقسم.

Split-DNS (Tunnel-all DNS معطل، split-include يشكل)

قبل AnyConnect 4.2

يسمح لطلبات DNS المطابقة لمجالات DNS المقسمة بأن تنفق خوادم DNS، ولكن غير مسموح بها لخوادم DNS الأخرى. لمنع استعلامات DNS الداخلية هذه من تسريب النفق، يستجيب برنامج تشغيل AnyConnect ب "لا يوجد مثل هذا الاسم" إذا تم إرسال الاستعلام إلى خوادم DNS أخرى. لذلك يمكن حل مجالات Split-DNS فقط من خلال خوادم DNS للنفق.

يسمح لطلبات DNS التي لا تطابق مجالات DNS المقسمة إلى خوادم DNS أخرى، ولكن غير مسموح لها بنفق خوادم DNS. حتى في هذه الحالة، يستجيب برنامج تشغيل AnyConnect ب "لا يوجد اسم كهذا" إذا تمت محاولة الاستعلام عن مجالات غير مقسمة عبر النفق. لذلك يمكن حل المجالات غير المقسمة إلى DNS فقط عبر خوادم DNS العامة خارج النفق.

AnyConnect 4.2 +

يسمح لطلبات DNS التي تطابق مجالات DNS المقسمة إلى أي خوادم DNS، طالما أنها تنشأ من محول VPN. إذا تم إنشاء الاستعلام بواسطة الواجهة العامة، فإن برنامج تشغيل AnyConnect يستجيب ب "لا يوجد اسم من هذا القبيل" لإجبار المحلل على إستخدام النفق دائما لحل الاسم. لذلك يمكن حل مجالات Split-DNS فقط عبر النفق.

يسمح لطلبات DNS التي لا تطابق مجالات DNS المقسمة إلى أي من خوادم DNS طالما أنها تنشأ من المهايئ الفعلي. إذا تم إنشاء الاستعلام بواسطة محول الشبكة الخاصة الظاهرية (VPN)، فإن AnyConnect يستجيب ب "لا يوجد اسم كهذا" لإجبار المحلل على محاولة تحليل الاسم دائما عبر الواجهة العامة. لذلك لا يمكن حل المجالات التي ليس لها تقسيم DNS إلا من خلال الواجهة العامة.

ماك أو إس إكس

تكوين Tunnel-all (وتقسيم الاتصال النفقي مع تمكين جميع DNS للنفق)

عند اتصال AnyConnect، يتم الاحتفاظ بخوادم DNS للنفق فقط في تكوين DNS للنظام، وبالتالي يمكن إرسال طلبات DNS فقط إلى خادم (خوادم) DNS للنفق.

تكوين Split-include (Tunnel-all DNS معطل و no split-DNS)

لا يتعارض AnyConnect مع محلل DNS الأصلي. يتم تكوين خوادم DNS للنفق كحلول مفضلة، مع إعطاء الأولوية على خوادم DNS العامة، وبالتالي ضمان إرسال طلب DNS الأولي لدقة الاسم عبر النفق. بما أن إعدادات DNS عمومية على Mac OS X، فلا يمكن لاستعلامات DNS إستخدام خوادم DNS العامة خارج النفق كما هو موثق في CSCtf20226 . بدءا من AnyConnect 4.2، تتم إضافة المسارات المضيفة لخادم (خوادم) DNS للنفق تلقائيا كشبكات مقسمة-مضمنة (مسارات آمنة) بواسطة عميل AnyConnect، وبالتالي فإن قائمة الوصول المنقسم-include لم تعد تتطلب إضافة صريحة للشبكة الفرعية لخادم DNS للنفق.

تكوين Split-exclude (Tunnel-all DNS معطل و no split-DNS)

لا يتعارض AnyConnect مع محلل DNS الأصلي. يتم تكوين خوادم DNS للنفق كحلول مفضلة، مع إعطاء الأولوية على خوادم DNS العامة، وبالتالي ضمان إرسال طلب DNS الأولي لدقة الاسم عبر النفق. بما أن إعدادات DNS عمومية على Mac OS X، فلا يمكن لاستعلامات DNS إستخدام خوادم DNS العامة خارج النفق كما هو موثق في

CSCtf20226 . بدءا من AnyConnect 4.2، تتم إضافة المسارات المضيفة لخادم (خوادم) DNS للنفق تلقائيا كشبكات مقسمة-مضمنة (مسارات آمنة) بواسطة عميل AnyConnect، وبالتالي فإن قائمة الوصول المنقسم-include لم تعد تتطلب إضافة صريحة للشبكة الفرعية لخادم DNS للنفق.

Split-DNS (Tunnel-all DNS معطل، split-include يشكل)

إذا تم تمكين Split-DNS لكل من بروتوكولات IP (IPv4 و IPv6) أو تم تمكينه فقط لبروتوكول واحد ولا يوجد تجمع عناوين تم تكوينه للبروتوكول الآخر:
يتم فرض تقسيم DNS الحقيقي، المماثل ل Windows. يعني True Split-DNS أن الطلبات التي تطابق مجالات DNS المقسمة يتم حلها فقط عبر النفق، ولا يتم تسريبها إلى خوادم DNS خارج النفق.

إذا تم تمكين Split-DNS لبروتوكول واحد فقط وتم تعيين عنوان عميل للبروتوكول الآخر، يتم فرض "DNS backback for split-tunneling" فقط. هذا يعني أن AC يسمح فقط لطلبات DNS التي تطابق مجالات DNS المقسمة عبر النفق (يتم الرد على الطلبات الأخرى بواسطة AC مع إستجابة "مرفوض" لفرض تجاوز الفشل إلى خوادم DNS العامة)، ولكن لا يمكنه فرض عدم إرسال الطلبات التي تطابق مجالات DNS المقسمة في المسح، عبر المهايئ العام.

لينكس

تكوين Tunnel-all (وتقسيم الاتصال النفقي مع تمكين جميع DNS للنفق)

عند اتصال AnyConnect، يتم الاحتفاظ بخوادم DNS للنفق فقط في تكوين DNS للنظام، وبالتالي يمكن إرسال طلبات DNS فقط إلى خادم (خوادم) DNS للنفق.

تكوين Split-include (Tunnel-all DNS معطل و no split-DNS)

لا يتعارض AnyConnect مع محلل DNS الأصلي. يتم تكوين خوادم DNS للنفق كحلول مفضلة، مع إعطاء الأولوية على خوادم DNS العامة، وبالتالي ضمان إرسال طلب DNS الأولي لدقة الاسم عبر النفق.

تكوين Split-exclude (Tunnel-all DNS معطل و no split-DNS)

لا يتعارض AnyConnect مع محلل DNS الأصلي. يتم تكوين خوادم DNS للنفق كحلول مفضلة، مع إعطاء الأولوية على خوادم DNS العامة، وبالتالي ضمان إرسال طلب DNS الأولي لدقة الاسم عبر النفق.

Split-DNS (Tunnel-all DNS معطل، split-include يشكل)

إذا تم تمكين Split-DNS، يتم فرض "DNS backback for split-tunneling" فقط. هذا يعني أن AC يسمح فقط لطلبات DNS التي تطابق مجالات DNS المقسمة عبر النفق (يتم الرد على الطلبات الأخرى بواسطة AC مع إستجابة "مرفوض" لفرض تجاوز الفشل إلى خوادم DNS العامة)، ولكن لا يمكنه فرض عدم إرسال الطلبات التي تطابق مجالات DNS المقسمة في المسح، عبر المهايئ العام.

عميل تجوال OpenDNS

العميل المتجول هو جزء من برنامج يدير خدمات DNS على نقطة النهاية، ويستخدم خوادم OpenDNS العامة لتأمين حركة مرور DNS وتشفيرها.

من الناحية المثالية، يجب أن يكون العميل في حالة محمية ومشفرة. ومع ذلك، إذا تعذر على العميل إنشاء جلسة TLS باستخدام خادم الحلول العامة ل OpenDNS (208.67.222.222)، فإنه يحاول إرسال حركة مرور DNS غير مشفرة على منفذ UDP من 53 إلى 208.67.222.222. يستخدم العميل المتجول بشكل حصري عنوان IP للمحلل العام ل OpenDNS 208.67.222.222 (هناك القليل من العناوين الأخرى مثل 208.67.220.220 و 208.67.222.20 و 208.67.220.2222). يعمل العميل المتجول بمجرد تثبيته على تعيين 127.0.0.1 (localhost) كخادم DNS محلي ويتجاوز إعدادات DNS الحالية لكل واجهة. يتم تخزين إعدادات DNS الحالية في ملفات resolv.conf المحلية (حتى في Windows) ضمن مجلد تكوين "عميل التجوال". سيقوم OpenDNS بإجراء نسخ إحتياطي حتى خوادم DNS التي تم التعرف عليها من خلال محول AnyConnect. على سبيل المثال، إذا كان 192.168.92.2 هو خادم DNS على المحول العام، سيقوم OpenDNS بإنشاء resolution.conf في الموقع التالي:

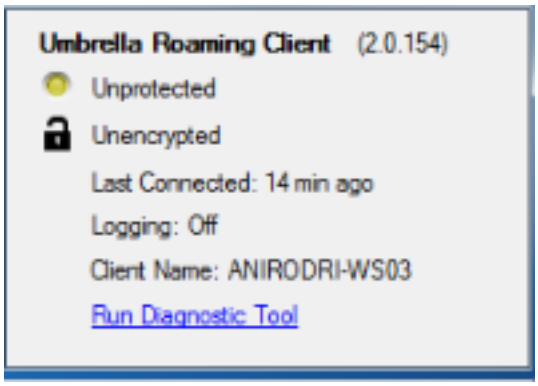
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
Nameserver 192.168.92.2

سيقوم العميل المتجول بتشفير كل حزمة مضبوطة على OpenDNS، ومع ذلك، فإنه لا يبدأ أو يستخدم نفق تشفير إلى 208.67.222.222. يحتوي العميل المتجول على ميزة "فرض طبقة IP" إختيارية والتي ستعمل على فتح اتصال IPSec لأغراض غير DNS لحظر عناوين IP. سيؤدي هذا إلى تعطيله تلقائيا في وجود اتصال AnyConnect نشط. كما أنها ترتبط ب 127.0.0.1:53 لتلقي الاستعلامات التي تم إنشاؤها محليا على الكمبيوتر. عندما تحتاج نقطة النهاية إلى حل اسم، يتم توجيه الاستعلامات المحلية إلى 127.0.0.1 بسبب التجاوز، ثم تقوم عملية وكيل DNSCRYPT الأساسية الخاصة بالعميل المتجول بإعادة توجيهها إلى خوادم OpenDNS العامة عبر القناة المشفرة.

إذا لم يكن DNS مسموحا به التدفق إلى 127.0.0.1:53، فلن يتمكن العميل المتجول من العمل وسيحدث ما يلي. إذا تعذر على العميل الوصول إلى خوادم DNS العامة أو العنوان المرتبط 127.0.0.1:53، فسيتم الانتقال إلى حالة فشل الفتح واستعادة إعدادات DNS على المحولات المحلية. في الخلفية، يستمر في إرسال مستكشفات إلى 208.67.222.222 ويمكن الانتقال إلى الوضع النشط إذا تم إعادة إنشاء الاتصال الآمن.

القيود

بعد الاطلاع على الوظائف عالية المستوى لكلا العملاء، من الواضح أن العميل المتجول يحتاج إلى القدرة على تغيير إعدادات DNS المحلية والربط ب 127.0.0.1:53 لإعادة توجيه الاستعلامات عبر القناة الآمنة. عندما تكون شبكة VPN متصلة، فإن التكوينات الوحيدة التي لا يتداخل فيها AnyConnect مع محلل DNS الأصلي هي Split-include and split-exclude (مع تعطيل جميع DNS الخاص بتقسيم النفق). لذلك، يوصى حاليا باستخدام أحد هذه التكوينات، عندما يكون العميل المتجول قيد الاستخدام أيضا. سيظل العميل المتجول في حالة غير محمية/غير مشفرة إذا تم إستخدام تكوين tunnel-all، أو تم تمكين DNS split-tunnel-all، كما هو موضح في الصورة.



الحل

إذا كانت النية هي حماية الاتصال بين العميل المتجول وخوادم OpenDNS باستخدام نفق VPN، يمكن إستخدام قائمة وصول منفصلة واستثناء وهمية على رأس شبكة VPN. سيكون هذا أقرب شيء إلى تكوين نفق كامل. وفي حالة عدم وجود مثل هذا المتطلب، يمكن إستخدام Split-include حيث لا تتضمن قائمة الوصول خوادم OpenDNS العامة، أو يمكن إستخدام Split-exclude حيث تتضمن قائمة الوصول خوادم OpenDNS العامة.

بالإضافة إلى ذلك، عند إستخدام "العميل المتجول"، لا يمكن إستخدام أوضاع DNS المقسمة لأن ذلك سيؤدي إلى فقد دقة DNS المحلية. يجب أن يبقى أيضا Split-Tunnel-all DNS معطلا؛ ومع ذلك، فهو مدعوم جزئيا ويجب أن يسمح لعميل التجوال بأن يصبح مشفرا بعد تجاوز الفشل.

التكوينات

حركة مرور Tunnel OpenDNS

يستخدم هذا المثال عنوان IP وهميا في قائمة الوصول الخاصة باستبعاد الانقسام. باستخدام هذا التكوين، تحدث جميع الاتصالات مع 208.67.222.222 عبر نفق VPN، ويعمل العميل المتجول في حالة مشفرة ومحمية.

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
wins-server none
dns-server value 1.1.1.1
vpn-tunnel-protocol ssl-client
split-tunnel-policy excludespecified
split-tunnel-network-list value split
default-domain value cisco.com
address-pools value acpool
webvpn
anyconnect profiles value AnyConnect type user
#ciscoasa
```

إستبعاد حركة مرور OpenDNS من نفق VPN

يستخدم هذا المثال عنوان محلل DNS OpenDNS في قائمة الوصول الخاصة باستبعاد الانقسام. مع هذا التكوين، تحدث جميع الاتصالات مع 208.67.222.222 خارج نفق VPN، ويعمل العميل المتجول في حالة مشفرة ومحمية.

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
wins-server none
dns-server value 1.1.1.1
vpn-tunnel-protocol ssl-client
split-tunnel-policy excludespecified
```

```
split-tunnel-network-list value split
      default-domain value cisco.com
          address-pools value acpool
                                webvpn
anyconnect profiles value AnyConnect type user
                               #ciscoasa
```

يوضح هذا المثال تكوين انقسام-يتضمن لشبكة فرعية داخلية 24/192.168.1.0 . باستخدام هذا التكوين، سيظل العميل المتجول يعمل في حالة مشفرة ومحمية نظرا لأنه لا يتم إرسال حركة المرور إلى 208.67.222.222 عبر النفق.

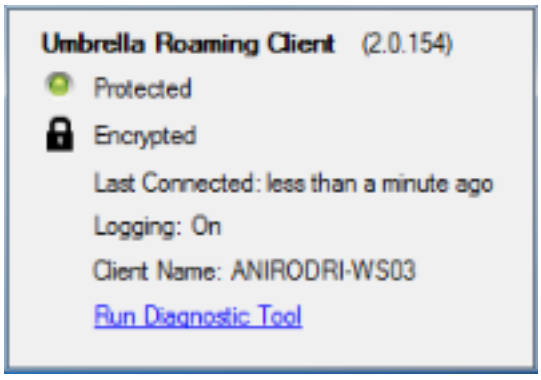
```
                                ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

                                ciscoasa# sh run group-policy
                    group-policy GroupPolicy-OpenDNS internal
                group-policy GroupPolicy-OpenDNS attributes
                                      wins-server none
                                  dns-server value 1.1.1.1
                              vpn-tunnel-protocol ssl-client
                            split-tunnel-policy tunnelspecified
                        split-tunnel-network-list value split
                              default-domain value cisco.com
                                  address-pools value acpool
                                                webvpn
            anyconnect profiles value AnyConnect type user
                                               #ciscoasa
```

Note: Split-tunnel-all-dns must be disabled in all of the scenarios

التحقق من الصحة

عند اتصال شبكة VPN، يجب أن يظهر العميل المتجول محميا ومشفرا كما هو موضح في هذه الصورة:



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).