تكوين Cisco ASA VPN على مثال تكوين عوامل تصفية

المحتويات

المقدمة

يصف هذا المستند عوامل تصفية VPN بالتفصيل ويطبق على شبكة LAN إلى شبكة LAN (L2L)، وعميل Cisco VPN، و Cisco AnyConnect Secure Mobility Client.

تتكون عوامل التصفية من القواعد التي تحدد ما إذا كان سيتم السماح بحزم البيانات المنضدة التي تأتي من خلال جهاز الأمان أو رفضها، وذلك استنادا إلى معايير مثل عنوان المصدر وعنوان الوجهة والبروتوكول. يمكنك تكوين قوائم التحكم في الوصول (ACL) للسماح بأنواع مختلفة من حركة المرور أو رفضها. يمكن تكوين عامل التصفية على نهج المجموعة أو سمات اسم المستخدم أو نهج الوصول الديناميكي (DAP).

يحل DAP محل القيمة التي تم تكوينها ضمن كل من سمات اسم المستخدم ونهج المجموعة. تحل قيمة سمة اسم المستخدم محل قيمة نهج المجموعة في حالة عدم قيام DAP بتعيين أي عامل تصفية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين أنفاق L2L VPN
- تكوين عميل الوصول عن بعد (RA) إلى VPN
- تكوين AnyConnect RA

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) الإصدار 9.1(2) من Cisco 5500-X Series.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يسمح الأمر **sysopt connection allowed-vpn** لجميع حركة مرور البيانات التي تدخل جهاز الأمان من خلال نفق VPN لتجاوز قوائم الوصول إلى الواجهة. لا يزال نهج المجموعة وقوائم الوصول إلى التخويل لكل مستخدم يتم تطبيقها على حركة المرور.

يتم تطبيق عامل تصفية VPN على حركة المرور التي تم فك تشفيرها مسبقا بعد خروجها من نفق وعلى حركة المرور المشفرة مسبقا قبل دخولها إلى نفق. لا يجب أيضا إستخدام قائمة التحكم في الوصول (ACL) المستخدمة لعامل تصفية VPN لمجموعة وصول الواجهة.

عند تطبيق عامل تصفية VPN على سياسة مجموعة تحكم إتصالات عميل Remote Access VPN، يجب تكوين قائمة التحكم في الوصول باستخدام عناوين IP المعينة من قبل العميل في موقع src_ip لقائمة التحكم في الوصول والشبكة المحلية في وضع DEST_IP لقائمة التحكم في الوصول. عند تطبيق عامل تصفية VPN على سياسة مجموعة تحكم اتصال L2L VPN، يجب تكوين قائمة التحكم في الوصول باستخدام الشبكة البعيدة في وضع src_ip لقائمة التحكم في الوصول والشبكة المحلية في وضع dest_ip لقائمة التحكم في الوصول.

التكوين

يجب تكوين عوامل تصفية VPN في الإتجاه الوارد على الرغم من إستمرار تطبيق القواعد بشكل ثنائي الإتجاه. تم فتح التحسينات CSCsf99428 لدعم القواعد الموحدة الإتجاه، ولكن لم يتم جدولتها/الالتزام بتنفيذها بعد.

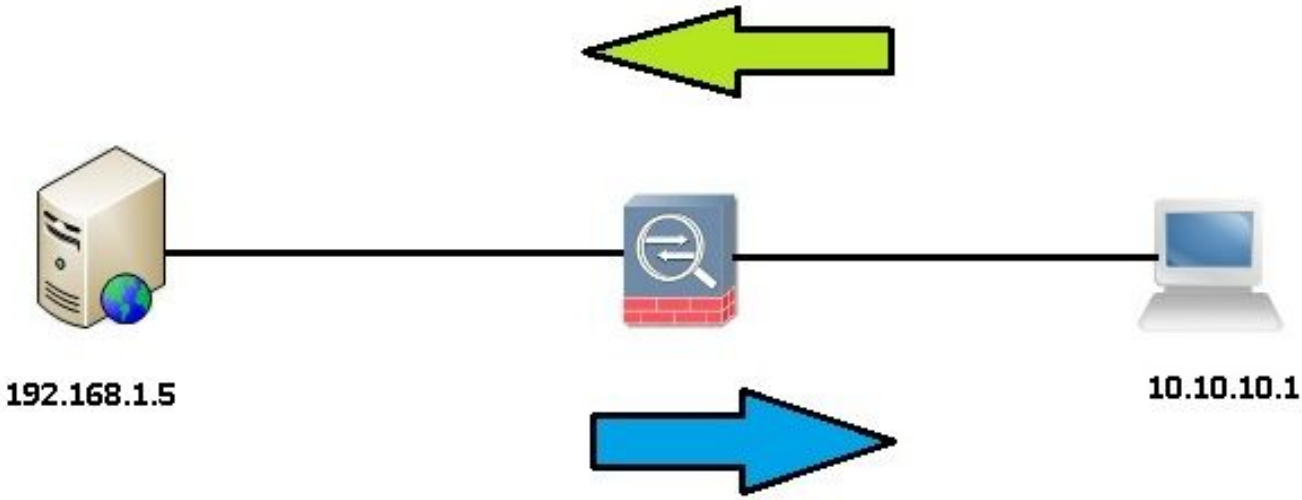
مثال 1. عامل تصفية VPN مع AnyConnect أو VPN Client

بافتراض أن عنوان IP المعين من قبل العميل هو 24/10.10.10.1 والشبكة المحلية هي 24/192.168.1.0.

يتيح إدخال التحكم في الوصول هذا (ACE) لعميل AnyConnect إلى برنامج Telnet للشبكة المحلية:

```
access-list vpnfilt-ra permit tcp
eq 23 192.168.1.0 255.255.255.0 255.255.255.255 10.10.10.1
```

Source IP	Destination IP	Protocol	Source Port	Destination Port	Data
10.10.10.1	192.168.1.5	TCP	1026	23	

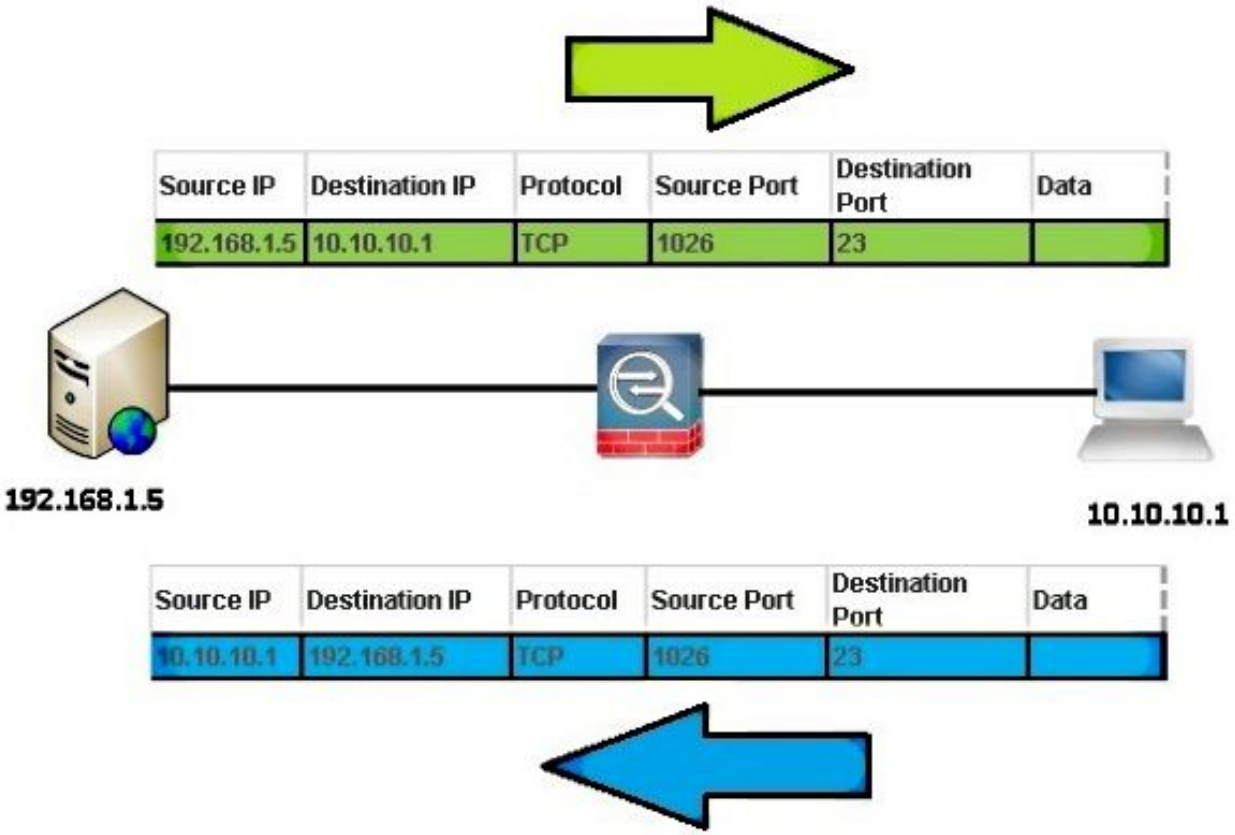


Source IP	Destination IP	Protocol	Source Port	Destination Port	Data
192.168.1.5	10.10.10.1	TCP	23	1026	

ملاحظة: يسمح ACE access-list vpnfilt-ra permit tcp 10.10.1 255.255.255.255.255 192.168.1.0 255.255.255.0 eq 23 أيضا للشبكة المحلية ببدء اتصال بعميل RA على أي منفذ TCP إذا كان يستخدم منفذ مصدر من 23.

يسمح ACE هذا للشبكة المحلية ب Telnet إلى عميل AnyConnect:

```
access-list vpnfilt-ra permit tcp 10.10.10.1 255.255.255.255
                                    eq 23 192.168.1.0 255.255.255.0
```



ملاحظة: يسمح ACE access-list vpnfilt-ra allowed tcp 10.10.1 255.255.255.255.255 eq 23 192.168.1.0 255.255.255.0 أيضا لعميل RA ببدء اتصال بالشبكة المحلية على أي منفذ TCP إذا كان يستخدم منفذ مصدر 23.

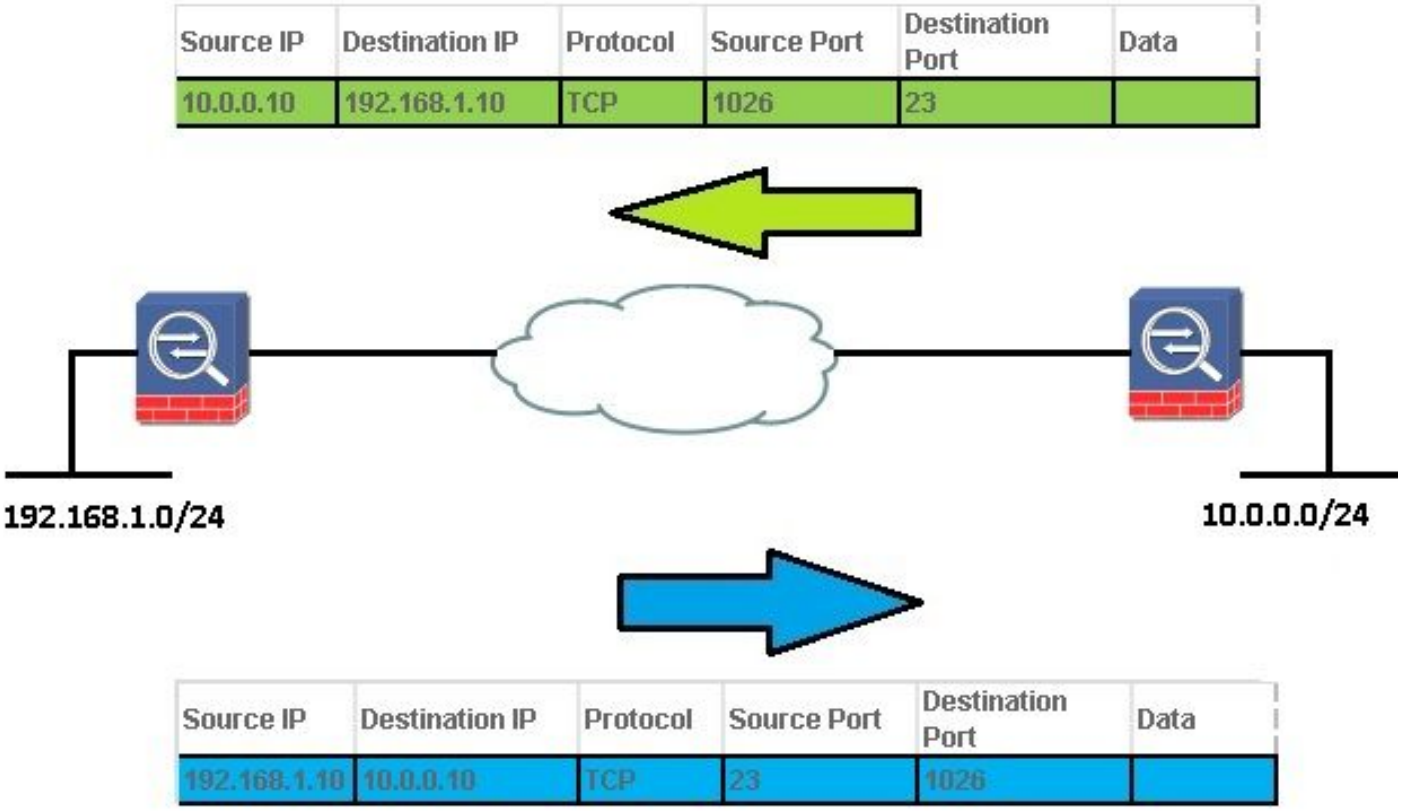
تحذير: تسمح ميزة عامل تصفية الشبكة الخاصة الظاهرية (VPN) بتصفية حركة المرور في الإتجاه الوارد فقط ويتم تحويل القاعدة الصادرة تلقائيا. لذلك، عندما تقوم بإنشاء قائمة وصول لبروتوكول رسائل التحكم بالإنترنت (ICMP)، لا تحدد نوع ICMP في تنسيق قائمة الوصول إذا كنت تريد عوامل تصفية اتجاهية.

مثال 2. VPN-filter مع اتصال L2L VPN

بافتراض أن الشبكة البعيدة هي 24/10.0.0.0 والشبكة المحلية هي 24/192.168.1.0.

يسمح ACE هذا للشبكة البعيدة ب Telnet إلى الشبكة المحلية:

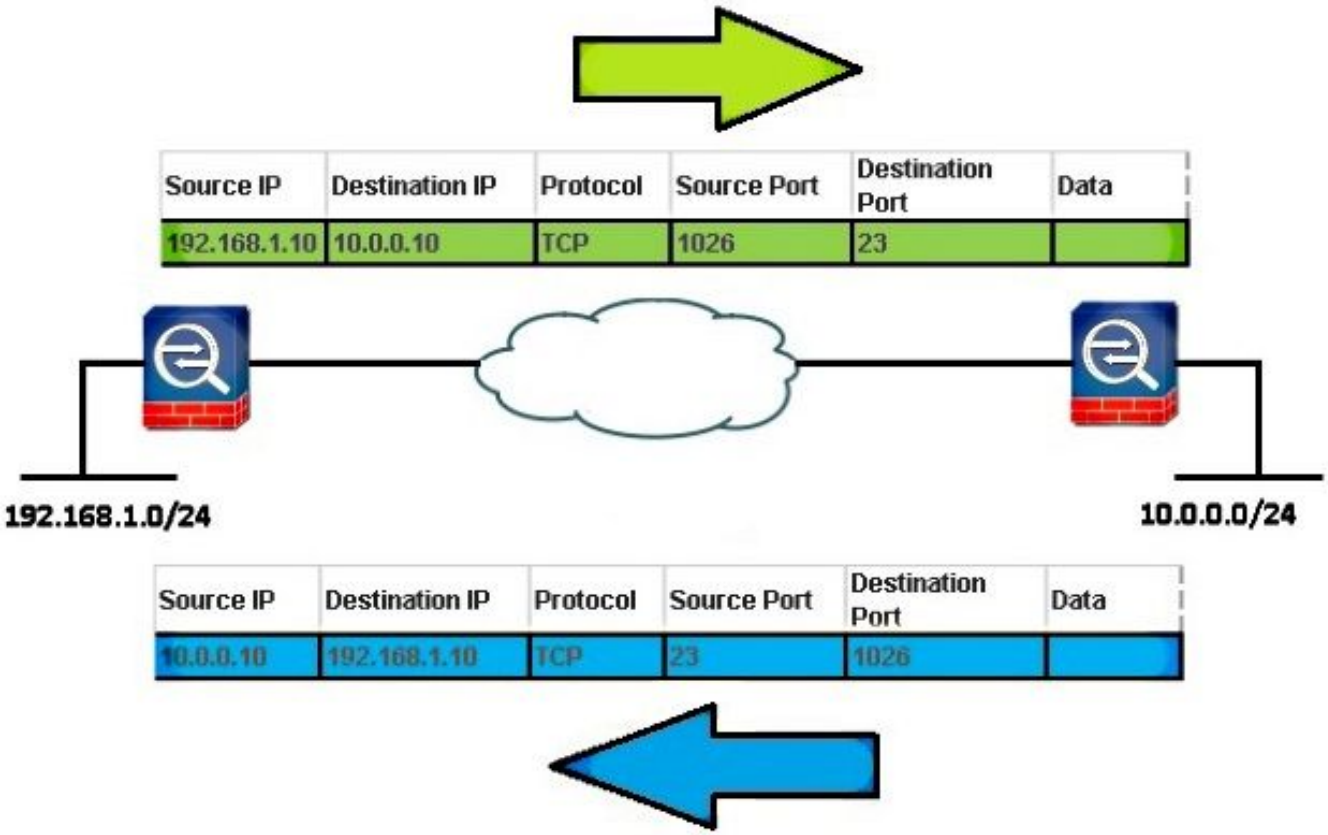
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
eq 23 255.255.255.0
```



ملاحظة: يسمح ACE access-list vpnfilt-l2l ل 192.168.1.0 255.255.255.0 10.0.0.0 TCP 255.255.255.0 eq 23 أيضا للشبكة المحلية ببدء اتصال بالشبكة عن بعد على أي منفذ TCP إذا كان يستخدم منفذ مصدر 23.

يسمح هذا ACE للشبكة المحلية ب Telnet إلى الشبكة البعيدة:

```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23
255.255.255.0 192.168.1.0
```



ملاحظة: يسمح ACE access-list vpnfilt-l2l ل 192.168.1.0 23 eq 255.255.255.0 10.0.0.0 TCP 255.255.255.0 للشبكة البعيدة أيضا ببدء اتصال بالشبكة المحلية على أي منفذ TCP إذا كان يستخدم منفذ مصدر 23.

تحذير: تسمح ميزة عامل تصفية الشبكة الخاصة الظاهرية (VPN) بتصفية حركة المرور في الإتجاه الوارد فقط ويتم تحويل القاعدة الصادرة تلقائيا. لذلك، عندما تقوم بإنشاء قائمة وصول ICMP، لا تقم بتحديد نوع ICMP في تنسيق قائمة الوصول إذا كنت تريد مرشحات اتجاهية.

عوامل تصفية VPN ومجموعات الوصول التي يتجاوز كل مستخدم

لا تتم تصفية حركة مرور VPN بواسطة قوائم التحكم في الوصول (ACLs) للواجهة. يمكن إستخدام الأمر **no sysopt connection allowed-vpn** لتغيير السلوك الافتراضي. في هذه الحالة، إثنان ACLs يستطيع كنت طبقت إلى مستعمل حركة مرور: القارن ACLs فحصت أولا وبعد ذلك ال VPN-filter.

تسمح الكلمة الأساسية **تجاوز كل مستخدم** (لقوائم التحكم في الوصول (ACL) الواردة فقط) بقوائم التحكم في الوصول (ACL) الديناميكية للمستخدم التي يتم تنزيلها لتفويض المستخدم لتخطي قائمة التحكم في الوصول (ACL) التي تم تعيينها للواجهة. على سبيل المثال، إذا رفضت قائمة التحكم في الوصول (ACL) للواجهة جميع حركات المرور من 10.0.0.0، ولكن قائمة التحكم في الوصول (ACL) الديناميكية تسمح بجميع حركات المرور من 10.0.0.0، ثم تتجاوز قائمة التحكم في الوصول (ACL) الديناميكية قائمة التحكم في الوصول للواجهة لذلك المستخدم ويتم السماح بحركة المرور.

الأمثلة (عند **عدم** تكوين **أي اتصال** **sysopt** allowed-vpn):

- لا يوجد تجاوز لكل مستخدم، لا يوجد عامل تصفية VPN - تتم مطابقة حركة المرور مقابل قائمة التحكم في الوصول (ACL) للواجهة

- لا يوجد تجاوز لكل مستخدم، vpn-filter - تتم مطابقة حركة المرور أولا مقابل قائمة التحكم في الوصول (ACL)

للواجهة، ثم مقابل عامل تصفية VPN

- تجاوز كل مستخدم، VPN-filter - تطابق حركة المرور مقابل عامل تصفية VPN فقط

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

يدعم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) (للعملاء المسجلين فقط) أوامر show معينة. استخدم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) لعرض تحليل لمُخرَج الأمر show.

- **إظهار عامل تصفية جدول *acl-name*> ASP [access-list>] [عمليات الاتصال]**

لتصحيح أخطاء جداول تصفية مسار الأمان السريع، أستخدم الأمر **show asp table filter** في وضع EXEC ذي الامتيازات. عند تطبيق عامل تصفية على نفق VPN، يتم تثبيت قواعد التصفية في جدول التصفية. إذا كان النفق يحتوي على عامل تصفية محدد، فإنه يتم التحقق من جدول التصفية قبل التشفير وبعد فك التشفير لتحديد ما إذا كان يجب السماح للحزمة الداخلية أو رفضها.

```
USAGE
show asp table filter [access-list
```

```
<SYNTAX <acl-name>      Show installed filter for access-list <acl-name
hits Show filter rules which have non-zero hits values
```

- **مسح عامل تصفية جدول *acl-name*> ASP [access-list>]**

يقوم هذا الأمر بمسح عدادات الوصول لإدخالات جدول عامل تصفية ASP.

```
USAGE
clear asp table filter [access-list
```

```
SYNTAX
<acl-name> Clear hit counters only for specified access-list <acl-name>
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

يدعم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) (للعملاء المسجلين فقط) أوامر show معينة. استخدم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) لعرض تحليل لمُخرَج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **مرشح تصحيح الأخطاء لقائمة التحكم بالوصول (ACL)**

يمكن هذا الأمر تصحيح أخطاء مرشح VPN. يمكن إستخدامها للمساعدة في أستكشاف أخطاء التثبيت/إزالة عوامل تصفية VPN وإصلاحها في جدول عامل تصفية ASP. على سبيل المثال 1. VPN-filter مع AnyConnect أو VPN Client.

إخراج تصحيح الأخطاء عند اتصال المستخدم1:

```
ACL FILTER INFO: first reference to inbound filter vpnfilt-ra(2): Installing
                                                                .rule into NP
ACL FILTER INFO: first reference to outbound filter vpnfilt-ra(2): Installing
                                                                .rule into NP
```

إخراج تصحيح الأخطاء عند اتصال المستخدم2 (بعد المستخدم 1 ونفس عامل التصفية):

```
ACL FILTER INFO: adding another reference to outbound filter vpnfilt-ra(2): refCnt=2
ACL FILTER INFO: adding another reference to inbound filter vpnfilt-ra(2): refCnt=2
```

إخراج تصحيح الأخطاء عند قطع اتصال المستخدم2:

```
ACL FILTER INFO: removing a reference from inbound filter vpnfilt-ra(2): remaining
                                                                      refCnt=1
ACL FILTER INFO: removing a reference from outbound filter vpnfilt-ra(2): remaining
                                                                      refCnt=1
```

إخراج تصحيح الأخطاء عند قطع اتصال المستخدم1:

```
ACL FILTER INFO: releasing last reference from inbound filter vpnfilt-ra(2): Removing
                                                                .rule into NP
ACL FILTER INFO: releasing last reference from outbound filter vpnfilt-ra(2): Removing
                                                                .rule into NP
```

- **إظهار جدول ASP**

فيما يلي إخراج **عامل تصفية جدول show asp** قبل **اتصال** User1. يتم تثبيت قواعد الرفض الضمني فقط ل IPv4 و IPv6 في كلا الاتجاهين الداخل والخارج.

```
                                                    :Global Filter Table
                                 in id=0xd616ef20, priority=11, domain=vpn-user, deny=true
                hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
                                                 src ip=0.0.0.0, mask=0.0.0.0, port=0
```

```
                                        dst ip=0.0.0.0, mask=0.0.0.0, port=0
                in id=0xd616f420, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
                                                          src ip=::/0, port=0
                                                          dst ip=::/0, port=0
              out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
                                        src ip=0.0.0.0, mask=0.0.0.0, port=0
                                        dst ip=0.0.0.0, mask=0.0.0.0, port=0
              out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
                                                          src ip=::/0, port=0
                                                          dst ip=::/0, port=0
```

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).