حماية طبقتك الأساسية: قوائم التحكم في الوصول لحماية البنية الأساسية

المحتويات

المقدمة

يقدم هذا المستند مبادئ توجيهية وتقنيات نشر موصى بها لقوائم التحكم في الوصول (ACL) لحماية البنية الأساسية. يتم إستخدام قوائم التحكم في الوصول (ACL) الخاصة بالبنية التحتية لتقليل مخاطر وفعالية الهجوم المباشر على البنية التحتية من خلال السماح بشكل صريح لحركة المرور المصرح بها فقط إلى معدات البنية التحتية مع السماح لجميع حركة المرور العابرة الأخرى.

حماية البنية الأساسية

الخلفية

في محاولة لحماية الموجهات من مخاطر متعددة - سواء بشكل عرضي أو ضار - يجب نشر قوائم التحكم في الوصول (ACL) لحماية البنية الأساسية في نقاط الدخول إلى الشبكة. تمنع قوائم التحكم في الوصول (ACL) لبروتوكول IPv4 و IPv6 هذه الوصول من مصادر خارجية إلى جميع عناوين البنية الأساسية، مثل واجهات الموجه. في الوقت نفسه، تسمح قوائم التحكم في الوصول (ACLs) لحركة المرور العابرة الروتينية بالتدفق دون انقطاع وتوفر معيار RFC 1918 وRFC 3330 والتصفية المضادة للانتحال.

يمكن تقسيم البيانات التي يتم استقبالها بواسطة الموجه إلى فئتين عريضتين:

- حركة المرور التي تمر عبر الموجه عبر مسار إعادة التوجيه
- حركة المرور الموجهة للموجه عبر مسار الاستقبال للتعامل مع معالج التوجيه

في العمليات العادية، يتم تدفق الغالبية العظمى من حركة المرور عبر موجه في الطريق إلى وجهته النهائية.

ومع ذلك، يجب أن يعالج معالج التوجيه (RP) أنواع معينة من البيانات مباشرة، وأبرزها بروتوكولات التوجيه والوصول إلى الموجه عن بعد (مثل [SSH] Secure Shell]) وحركة مرور إدارة الشبكة مثل بروتوكول إدارة الشبكة البسيط (SNMP). بالإضافة إلى ذلك، يمكن أن تتطلب البروتوكولات مثل بروتوكول رسائل التحكم في الإنترنت (ICMP) وخيارات IP معالجة مباشرة بواسطة RP. وفي معظم الأحيان، يكون الوصول المباشر لموجه البنية الأساسية مطلوبا فقط من المصادر الداخلية. وتتضمن بعض الاستثناءات البارزة القليلة التجزيئات الخارجية لبروتوكول العبارة الحدودية (BGP)، والبروتوكولات التي يتم إنهاؤها على الموجه الفعلي (مثل تضمين التوجيه العام [GRE] أو IPv6 عبر أنفاق IPv4)، وحزم ICMP المحدودة المحتملة لاختبار الاتصال مثل echo-request أو ICMP الذي يتعذر الوصول إليه والرسائل التي انتهت مدة صلاحيتها (TTL) ل traceroute.

ملاحظة: تذكر أنه غالبا ما يتم إستخدام بروتوكول ICMP لشن هجمات بسيطة على الأشخاص الذين لا يحصلون على الخدمة (DoS)، ولا يجب السماح بذلك إلا من مصادر خارجية إذا لزم الأمر.

تتميز جميع برامج العمل الإقليمية بالأداء الفائق الذي تعمل به. يمكن أن تثقل حركة المرور المفرطة الموجهة إلى RP الموجه. وهذا يتسبب في إستخدام عال لوحدة المعالجة المركزية (CPU) ويؤدي في نهاية المطاف إلى عمليات إسقاط للحزم وبروتوكول التوجيه التي تتسبب في رفض الخدمة. من خلال تصفية الوصول إلى موجهات البنية الأساسية من مصادر خارجية، يتم الحد من العديد من المخاطر الخارجية المرتبطة بهجوم الموجه المباشر. لم تعد الهجمات التي يتم الحصول عليها من مصادر خارجية قادرة على الوصول إلى معدات البنية التحتية. يتم إسقاط الهجوم على واجهات الدخول في النظام الذاتي (AS).

تهدف تقنيات التصفية الموضحة في هذا المستند إلى تصفية البيانات الموجهة لمعدات البنية الأساسية للشبكة. لا تخلط بين تصفية البنية الأساسية والتصفية العامة. يتمثل الغرض المفرد لقائمة التحكم في الوصول (ACL) الخاصة بحماية البنية الأساسية في تقييد البروتوكولات والمصادر التي يمكنها الوصول إلى معدات البنية الأساسية الحيوية على مستوى قابل للتعديل.

تشمل معدات البنية التحتية للشبكة هذه المناطق:

- جميع عناوين إدارة الموجه والمحول، بما في ذلك واجهات الاسترجاع
- جميع عناوين الارتباطات الداخلية: إرتباطات من موجه إلى موجه (وصول من نقطة إلى نقطة والوصول المتعدد)
- الخوادم أو الخدمات الداخلية التي يجب عدم الوصول إليها من مصادر خارجية

في هذا المستند، غالبا ما تتم الإشارة إلى حركة مرور البيانات غير الموجهة للبنية الأساسية باسم حركة مرور النقل.

تقنيات

يمكن تحقيق حماية البنية التحتية من خلال مجموعة متنوعة من التقنيات:

- **إستقبال قوائم التحكم بالوصول (rACLs)**تدعم الأنظمة الأساسية Cisco 12000 و 7500 قوائم التحكم في الوصول (ACLs) التي تعمل على تصفية جميع حركة المرور الموجهة إلى RP ولا تؤثر على حركة مرور النقل. يجب السماح بشكل صريح بحركة المرور المصرح بها ويجب نشر قائمة التحكم في الوصول للبنية الأساسية (rACL) على كل موجه. راجع GSR: إستلام قوائم التحكم في الوصول للحصول على مزيد من المعلومات.
- **قوائم التحكم في الوصول الخاصة بالموجه**يمكن أيضا حماية الموجهات من خلال تحديد قوائم التحكم في الوصول (ACL) التي تسمح فقط بحركة المرور المصرح بها إلى واجهات الموجه، مع رفض جميع البيانات الأخرى باستثناء حركة المرور العابرة، والتي يجب السماح بها بشكل صريح. قائمة التحكم في الوصول (ACL) هذه مماثلة منطقيا لقوائم التحكم في الوصول إلى النقل (rACL) ولكنها تؤثر على حركة مرور النقل، وبالتالي يمكن أن يكون لها تأثير سلبي على معدل إعادة توجيه الموجه.
- **تصفية الحافة عبر قوائم التحكم في الوصول (ACLs) للبنية الأساسية**يمكن تطبيق قوائم التحكم في الوصول (ACL) على حافة الشبكة. في حالة مزود الخدمة (SP)، هذه هي حافة AS. تعمل قائمة التحكم في الوصول (ACL) هذه بشكل صريح على تصفية حركة المرور الموجهة لمساحة عنوان البنية الأساسية. يتطلب نشر قوائم التحكم في الوصول (ACLs) الخاصة بالبنية الأساسية الطرفية تحديد مساحة البنية الأساسية لديك والبروتوكولات المطلوبة/المعتمدة التي تصل إلى هذه المساحة بشكل واضح. يتم تطبيق قائمة التحكم في الوصول (ACL) عند الدخول إلى شبكتك على جميع الاتصالات التي تتم مواجهتها خارجيا، مثل إتصالات نظير واتصالات العملاء وما إلى

ذلك.يركز هذا المستند على تطوير قوائم التحكم في الوصول (ACL) الطرفية لحماية البنية الأساسية ونشرها.

أمثلة على قائمة التحكم في الوصول (ACL)

توفر قوائم الوصول إلى كلا من IPv4 و IPv6 هذه أمثلة بسيطة وواقعية على الإدخالات النموذجية المطلوبة في قائمة التحكم في الوصول (ACL) للحماية. يلزم تخصيص قوائم التحكم في الوصول (ACL) الأساسية هذه باستخدام تفاصيل التكوين الخاصة بالموقع المحلي. وفي بيئات بروتوكولي IPv4 و IPv6، يتم نشر كل من قوائم الوصول.

مثال IPv4

```
Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to ---!
RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-
   list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110
  deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-
  list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your
  AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit
  BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp
      host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses.
      access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic.
                                                  access-list 110 permit ip any any
```

مثال IPv6

يجب تطبيق قائمة وصول IPv6 كقائمة وصول موسعة مسماة.

```
    Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from ---!
    entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !---
Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host
  bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses.
deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6
                                                                                    any any
```

ملاحظة: يمكن إستخدام الكلمة الأساسية **log** لتوفير تفاصيل إضافية حول المصدر والوجهات لبروتوكول معين. على الرغم من أن هذه الكلمة الأساسية توفر رؤية قيمة حول تفاصيل الوصول إلى قائمة التحكم في الوصول (ACL)، إلا أن الوصول المفرط إلى إدخال قائمة التحكم في الوصول الذي يستخدم الكلمة الأساسية **log** يزيد من إستخدام وحدة المعالجة المركزية (CPU). يختلف تأثير الأداء المرتبط بالتسجيل حسب النظام الأساسي. أيضا، إستخدام الكلمة الأساسية السجل يعجز تحويل إعادة التوجيه السريع (Cisco Express Forwarding) CEF للحزم التي تطابق بيان قائمة الوصول. ويتم تبديل هذه الحزم بسرعة بدلا من ذلك.

تطوير قائمة تحكم في الوصول (ACL) للحماية

بشكل عام، تتكون قائمة التحكم في الوصول (ACL) للبنية الأساسية من أربعة أقسام:

- عنوان الاستخدام الخاص والإدخالات المضادة للانتحال التي ترفض المصادر غير الشرعية والحزم ذات عناوين المصدر التي تنتمي إلى AS الخاص بك من إدخال AS من مصدر خارج**ملاحظة:** يحدد RFC 3330 عناوين الاستخدام الخاص ل IPv4 التي قد تتطلب التصفية. يعمل RFC 1918 على تحديد مساحة العنوان المحجوزة للإصدار الرابع من بروتوكول الإنترنت (IP) التي لا تعد عنوان مصدر صالح على الإنترنت. يعمل RFC 3513 على تحديد بنية عنونة بروتوكول IPv6. يوفر RFC 2827 إرشادات لتصفية المدخل.
- حركة مرور البيانات الخارجية المسموح بها بشكل صريح الموجهة إلى عناوين البنية الأساسية
- **رفض** عبارات حركة المرور الأخرى التي تم الحصول عليها من مصادر خارجية إلى عناوين البنية الأساسية

- **عبارات** التصريح لجميع حركات المرور الأخرى لحركة مرور العمود الفقري العادية في الطريق إلى وجهات لا بنية تحتية

يتيح الخط الأخير في قائمة التحكم في الوصول (ACL) للبنية الأساسية بشكل صريح لحركة مرور البيانات العابرة: **السماح للإصدار الرابع** من بروتوكول الإنترنت (IP) **والسماح للإصدار السادس من بروتوكول الإنترنت (IP)** بأي **شيء** للإصدار السادس من بروتوكول الإنترنت (IP). يضمن هذا الإدخال السماح بجميع بروتوكولات IP من خلال الأساسي وأن بإمكان العملاء الاستمرار في تشغيل التطبيقات دون أية مشاكل.

تتمثل الخطوة الأولى عند تطوير قائمة تحكم في الوصول (ACL) لحماية البنية الأساسية في فهم البروتوكولات المطلوبة. على الرغم من أن كل موقع له متطلبات محددة، إلا أنه يتم نشر بروتوكولات معينة بشكل عام ويجب فهمها. على سبيل المثال، يجب السماح بشكل صريح ببروتوكول BGP الخارجي إلى النظراء الخارجيين. كما يجب السماح بشكل صريح بأي بروتوكولات أخرى تتطلب الوصول المباشر إلى موجه البنية الأساسية. على سبيل المثال، إذا قمت بإنهاء نفق GRE على موجه بنية أساسية، فيجب أيضا السماح بشكل صريح بالبروتوكول 47 (GRE). وبالمثل، إذا قمت بإنهاء نفق IPv6 عبر IPv4 على موجه البنية الأساسية الرئيسي، فيجب أيضا السماح بشكل صريح بالبروتوكول 41 (IPv6 عبر IPv4).

يمكن إستخدام قائمة التحكم في الوصول إلى التصنيفات للمساعدة في تحديد البروتوكولات المطلوبة. تتكون قائمة التحكم في الوصول إلى التصنيفات من عبارات **السماح** للبروتوكولات المختلفة التي يمكن توجيهها إلى موجه البنية الأساسية. راجع الملحق الموجود في بروتوكولات IP المدعومة في برنامج Cisco IOS® للحصول على قائمة كاملة. يحدد إستخدام الأمر **show access-list** لعرض عدد من عمليات الوصول إلى إدخال التحكم في الوصول (ACE) البروتوكولات المطلوبة. يجب التحقيق في النتائج المريبة أو المفاجئة وفهمها قبل إنشاء بيانات **سماح** للبروتوكولات غير المتوقعة.

على سبيل المثال، تساعد قائمة التحكم في الوصول (ACL) إلى IPv4 هذه في تحديد ما إذا كان يلزم السماح بنفقي GRE و IPsec (ESP) و IPv6 (بروتوكول IP رقم 41).

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
 access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
The log keyword provides more details !--- about other protocols that are not explicitly ---!
.permitted

access-list 101 permit ip any any

<interface <int
ip access-group 101 in
```

يمكن إستخدام قائمة التحكم في الوصول (ACL) إلى IPv6 هذه لتحديد ما إذا كان يلزم السماح بمعيار GRE و IPsec (ESP).

```
ipv6 access-list determine_protocols
permit GRE any infrastructure_ips_ipv6
permit ESP any infrastructure_ips_ipv6
permit ipv6 any infrastructure_ips_ipv6 log
The log keyword provides more details !--- about other protocols that are not explicitly ---!
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

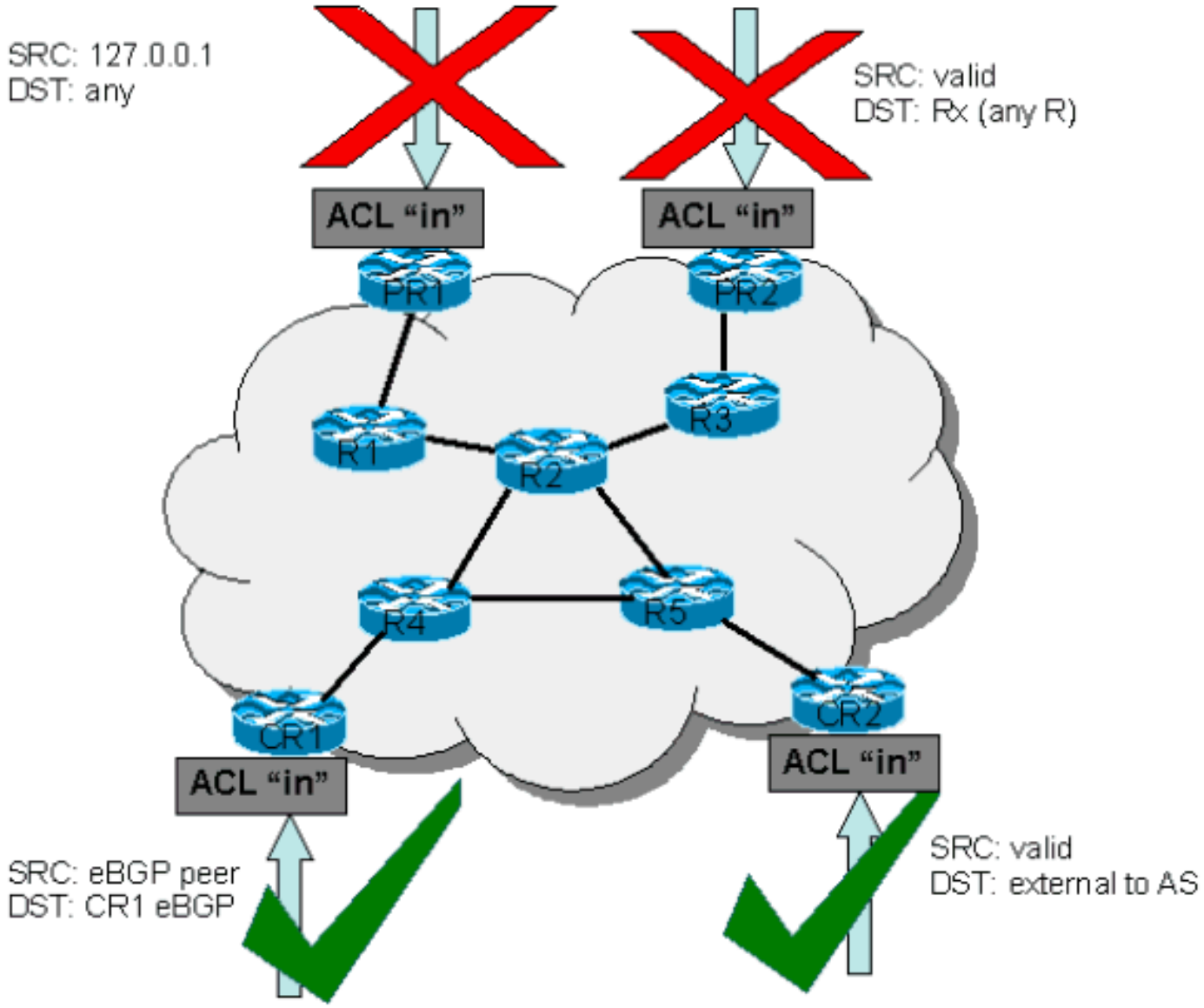
بالإضافة إلى البروتوكولات المطلوبة، يلزم تحديد مساحة عنوان البنية الأساسية نظرا لأنها المساحة التي توفرها قائمة التحكم في الوصول (ACL). تتضمن مساحة عنوان البنية الأساسية أي عناوين يتم إستخدامها للشبكة الداخلية ونادرا ما يتم الوصول إليها من قبل المصادر الخارجية مثل واجهات الموجهات، وعنونة الارتباط من نقطة إلى نقطة، وخدمات البنية الأساسية الحيوية. ونظرا لأنه يتم إستخدام هذه العناوين لجزء الوجهة من قائمة التحكم في الوصول (ACL) للبنية الأساسية، فإن التلخيص أمر بالغ الأهمية. حيثما كان ذلك ممكنا، يجب تجميع هذه العناوين في كتل توجيه المجال التبادلي دون فئات (CIDR).

ومع إستخدام البروتوكولات والعناوين المحددة، يمكن إنشاء قائمة التحكم في الوصول (ACL) للبنية الأساسية للسماح

بالبروتوكولات وحماية العناوين. بالإضافة إلى الحماية المباشرة، توفر قائمة التحكم في الوصول (ACL) أيضا خط دفاع أول ضد أنواع معينة من حركة المرور غير الصالحة على الإنترنت.

- يجب رفض مساحة RFC 1918.
- يجب رفض الحزم ذات عنوان المصدر الذي يقع ضمن مساحة عنوان الاستخدام الخاص، كما هو محدد في RFC 3330.
- يجب تطبيق عوامل التصفية المضادة للانتحال. (يجب ألا تكون مساحة العنوان الخاصة بك مصدر الحزم من خارج AS.)

يجب تطبيق قائمة التحكم في الوصول (ACL) هذه التي تم إنشاؤها حديثا واردة على جميع واجهات الدخول. راجع الأقسام حول إرشادات النشر وأمثلة النشر للحصول على مزيد من التفاصيل.



قوائم التحكم في الوصول والحزم المجزأة

تحتوي قوائم التحكم في الوصول (ACL) على كلمة أساسية **أجزاء** تمكن سلوك معالجة الحزم المجزأة المتخصصة. بدون الكلمة الأساسية **الأجزاء** هذه، تتأثر الأجزاء غير الأولية التي تطابق عبارات الطبقة الثالثة (بغض النظر عن معلومات الطبقة الرابعة) في قائمة التحكم في الوصول (ACL) بجملة السماح أو الرفض الخاصة بالإدخال المتطابق. ومع ذلك، من خلال إضافة الكلمة الأساسية **الأجزاء**، يمكنك فرض قوائم التحكم في الوصول (ACL) على رفض الأجزاء غير الأولية أو السماح بها بمزيد من القابلية. وهذا السلوك هو نفسه لكل من قوائم الوصول إلى IPv4 و IPv6، باستثناء أنه بينما تسمح قوائم التحكم في الوصول إلى IPv4 باستخدام الكلمة الأساسية الأجزاء داخل عبارات الطبقة 3 والطبقة 4، فإن قوائم التحكم في الوصول إلى IPv6 تسمح فقط باستخدام الكلمة الأساسية الأجزاء داخل عبارات

الطبقة 3.

تضيف أجزاء التصفية طبقة إضافية من الحماية ضد هجوم رفض الخدمة (DoS) الذي يستخدم الأجزاء غير الأولية (أي، ما هو > 0). يؤدي إستخدام عبارة **الرفض** الخاصة بالأجزاء غير الأولية في بداية قائمة التحكم في الوصول إلى رفض جميع الأجزاء غير الأولية من الوصول إلى الموجه. في ظروف نادرة، قد تتطلب الجلسة الصالحة التجزئة، وبالتالي تتم تصفيتها إذا وجدت عبارة **رفض الجزء** في قائمة التحكم في الوصول (ACL).

على سبيل المثال، تذكر قائمة التحكم في الوصول (ACL) الجزئية التالية ل IPv4IP:

```
access-list 110 deny tcp any infrastructure_IP fragments
access-list 110 deny udp any infrastructure_IP fragments
access-list 110 deny icmp any infrastructure_IP fragments
<rest of ACL>
```

تؤدي إضافة هذه الإدخالات إلى بداية قائمة التحكم في الوصول (ACL) إلى رفض أي وصول غير أولي إلى الموجهات الأساسية، بينما تقوم الحزم غير المجزأة أو الأجزاء الأولية بالتمرير إلى الأسطر التالية لقائمة التحكم في الوصول (ACL) دون أن تتأثر بجمل **رفض الجزء**. كما يسهل أمر قائمة التحكم في الوصول (ACL) السابقة تصنيف الهجوم نظرا لأن كل بروتوكول - بروتوكول مخطط البيانات العالمي (UDP) و TCP و ICMP - يزيد عدادات منفصلة في قائمة التحكم في الوصول (ACL).

هذا مثال مشابه ل IPv6:

```
ipv6 access-list iacl
deny ipv6 any infrastructure_IP fragments
```

تؤدي إضافة هذا الإدخال إلى بداية قائمة التحكم في الوصول (ACL) إلى IPv6 إلى رفض أي وصول غير أولي إلى الأجزاء إلى الموجهات الأساسية. وكما تمت الإشارة مسبقا، تتيح قوائم الوصول إلى IPv6 إستخدام الكلمة الأساسية الأجزاء داخل عبارات الطبقة الثالثة فقط.

ونظرا لأن العديد من الهجمات تعتمد على غمر موجهات القلب باستخدام الحزم المجزأة، فإن تصفية الأجزاء الواردة إلى البنية الأساسية توفر مقياسا إضافيا للحماية وتساعد على ضمان عدم تمكن الهجوم من حقن الأجزاء عن طريق مطابقة قواعد الطبقة 3 ببساطة في قائمة التحكم في الوصول (ACL) للبنية الأساسية.

ارجع إلى قوائم التحكم في الوصول وأجزاء IP لإجراء مناقشة تفصيلية للخيارات.

تقييم الخطر

ضع في الاعتبار هذين النوعين من المخاطر الرئيسية عند نشر قوائم التحكم في الوصول (ACL) الخاصة بحماية البنية الأساسية:

- التأكد من وجود بيانات **السماح/الرفض** المناسبة. لكي تكون قائمة التحكم في الوصول (ACL) فعالة، يجب السماح بجميع البروتوكولات المطلوبة ويجب حماية مساحة العنوان الصحيحة بواسطة عبارات **الرفض**.
- يختلف أداء قائمة التحكم في الوصول (ACL) من نظام أساسي إلى آخر. راجع خصائص أداء الأجهزة قبل نشر قوائم التحكم في الوصول (ACL).

وكما هو الحال دائما، يوصى باختبار هذا التصميم في المعمل قبل النشر.

الملاحق

بروتوكولات IP المدعومة في برنامج Cisco IOS

يتم دعم بروتوكولات IP هذه من قبل برنامج Cisco IOS software:

- ICMP - 1
- IGMP - 2
- GGP - 3
- IP في تضمين IP - 4
- بروتوكول TCP - 6
- EGP - 8
- بروتوكول العبارة الداخلية (IGRP) - 9
- UDP - 17
- HMP - 20
- بروتوكول RDP - 27
- IPv6 في الاتصال النفقي عبر بروتوكول IPv4 - 41
- RSVP - 46
- GRE - 47
- ESP - 50
- AH - 51
- السحب - 53
- NARP - 54
- إمكانية تنقل IP - 55
- أي شبكة محلية - 63
- Sun ND - 77
- ISO IP - 80
- بروتوكول EIGRP - 88
- OSPF - 89
- Sprite RPC - 90
- LARP - 91
- KA9Q/NOS متوافق مع IP عبر IP - 94
- PIM - 103
- ضغط IP - 108
- بروتوكول VRRP - 112
- PGM - 113
- L2TP - 115
- UTI - 120
- SCTP - 132

إرشادات النشر

توصي Cisco باتباع ممارسات نشر محافظة. من أجل نشر قوائم التحكم في الوصول (ACL) للبنية الأساسية بنجاح، يجب فهم البروتوكولات المطلوبة بشكل جيد، كما يجب تحديد مساحة العنوان وتحديدها بشكل واضح. تصف هذه الإرشادات طريقة محافظة للغاية لنشر قوائم التحكم في الوصول (ACL) للحماية باستخدام نهج متكرر.

1. **تحديد البروتوكولات المستخدمة في الشبكة باستخدام قائمة التحكم في الوصول (ACL) إلى التصنيف.**نشر قائمة تحكم في الوصول (ACL) التي تسمح لجميع البروتوكولات المعروفة التي تصل إلى أجهزة البنية الأساسية. تحتوي قائمة التحكم بالوصول (ACL) الخاصة بهذا الاكتشاف على عنوان مصدر **لأي** وجهة تتضمن مساحة IP للبنية الأساسية. يمكن إستخدام التسجيل لتطوير قائمة عناوين المصدر التي تطابق عبارات **السماح** للبروتوكول.

يلزم إدخال السطر الأخير الذي يسمح **ببروتوكول الإنترنت بأي** (IPv4) أو **بروتوكول IPv6 أي** (IPv6) للسماح بتدفق حركة المرور.والهدف من ذلك هو تحديد البروتوكولات التي تستخدمها الشبكة المحددة. يتم إستخدام التسجيل للتحليل لتحديد أي شيء آخر يمكن أن يكون متصلا مع الموجه.**ملاحظة:** على الرغم من أن الكلمة الأساسية **log** توفر رؤية قيمة حول تفاصيل الوصول إلى قائمة التحكم في الوصول (ACL)، إلا أن عمليات الوصول الزائدة إلى إدخال قائمة التحكم في الوصول (ACL) الذي يستخدم هذه الكلمة الأساسية قد ينتج عنها عدد هائل من إدخالات السجل وربما إستخدام وحدة المعالجة المركزية (CPU) للموجه المرتفع. أيضا، إستخدام الكلمة الأساسية **log** يعجز تحويل Cisco Express Forwarding (CEF) للحزم التي تطابق بيان قائمة الوصول. ويتم تبديل هذه الحزم بسرعة بدلا من ذلك. أستخدم الكلمة الأساسية **log** لفترات زمنية قصيرة وفقط عند الحاجة للمساعدة في تصنيف حركة المرور.

2. **مراجعة الحزم المحددة وبدء تصفية الوصول إلى RP لمعالج التوجيه.**بمجرد تحديد الحزم التي تمت تصفيتها بواسطة قائمة التحكم في الوصول (ACL) في الخطوة 1 ومراجعتها، قم بنشر قائمة تحكم في الوصول (ACL) **والسماح بأي مصدر** إلى عناوين البنية الأساسية للبروتوكولات المسموح بها. كما في الخطوة 1، يمكن أن توفر الكلمة الأساسية **log** مزيد من المعلومات حول الحزم التي تطابق إدخالات **السماح**. يمكن أن يساعد إستخدام **رفض أي** في النهاية في تحديد أي حزم غير متوقعة موجهة إلى الموجهات. يجب أن يكون السطر الأخير من قائمة التحكم في الوصول هذه عبارة **تصريح** IPv4) **ip any**) أو **السماح ل IPv6 بأي** بيان (IPv6) للسماح بتدفق حركة المرور العابرة. توفر قائمة التحكم في الوصول (ACL) هذه الحماية الأساسية وتسمح لمهندسي الشبكة لضمان السماح بجميع حركة المرور المطلوبة.
3. **تقييد عناوين المصدر.**بمجرد حصولك على فهم واضح للبروتوكولات التي يجب السماح بها، يمكن إجراء مزيد من التصفية للسماح بالمصادر المعتمدة فقط لتلك البروتوكولات. على سبيل المثال، يمكنك السماح بشكل صريح لجيران BGP الخارجية أو عناوين نظير GRE معينة.تعمل هذه الخطوة على تقليل المخاطر دون كسر أي خدمات وتسمح لك بتطبيق تحكم دقيق على المصادر التي تصل إلى معدات البنية الأساسية الخاصة بك.
4. **تحديد عناوين الوجهة على قائمة التحكم بالوصول (ACL). *(إختياري)***قد يختار بعض موفري خدمة الإنترنت (ISP) السماح فقط للبروتوكولات المحددة باستخدام عناوين وجهة محددة على الموجه. تهدف هذه المرحلة النهائية إلى تحديد نطاق عناوين الوجهة التي يمكنها قبول حركة مرور البيانات لبروتوكول ما.

أمثلة النشر

مثال IPv4

يوضح مثال IPv4 هذا قائمة تحكم في الوصول (ACL) للبنية الأساسية تحمي موجه استنادا إلى هذه العنونة:

- كتلة عنوان ISP هي 16/169.223.0.0.
- كتلة البنية الأساسية ل ISP هي 22/169.223.252.0.
- الاسترجاع للموجه هو 32/169.223.253.1.
- الموجه هو موجه نظير وينظير مع 169.254.254.1 (للعنوان 169.223.252.1).

يتم تطوير قائمة التحكم في الوصول (ACL) الخاصة بحماية البنية الأساسية المعروضة استنادا إلى المعلومات السابقة. تسمح قائمة التحكم في الوصول (ACL) بدرجات BGP الخارجية إلى النظير الخارجي، وتوفر عوامل تصفية مضادة للانتحال، وتحمي البنية الأساسية من جميع الوصول الخارجي.

```
!
no access-list 110
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !
Phase 1 - Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid ---!
.(source addresses, and spoofs of !--- internal space (space as an external source

!
Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0 ---!
0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list
110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !---
```

See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny our internal space as an external source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0 0.0.255.255 any !!! **!--- Phase 2 – Explicit Permit** !--- - Permit only applications/protocols whose destination !--- address is part of the .infrastructure IP block. !--- The source of the traffic should be known and authorized

!

Note: This template must be tuned to the network's !--- specific source address ---! .environment. Variables in !--- the template need to be changed

Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq ---! bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 ! !! !--- **Phase 3 – Explicit Deny to Protect Infrastructure**

access-list 110 deny ip any 169.223.252.0 0.0.3.255
!
!!!
Phase 4 – Explicit Permit for Transit Traffic ---!

access-list 110 permit ip any any

مثال IPv6

يوضح مثال IPv6 هذا قائمة تحكم في الوصول (ACL) للبنية الأساسية تحمي موجه استنادا إلى هذه العنونة:

- كتلة البادئات الإجمالية المخصصة ل ISP هي 2001:0db8::/32.
- كتلة بادئة IPv6 التي يستخدمها ISP لعناوين البنية الأساسية للشبكة هي 2001:0db8:C18::/48.
- هناك موجه تجميع BGP باستخدام عنوان IPv6 للمصدر في 2001:0DB8:C18:2:1::1 الذي يتوافق مع عنوان IPv6 للوجهة في 2001:0DB8:C19:2:1::F.

يتم تطوير قائمة التحكم في الوصول (ACL) الخاصة بحماية البنية الأساسية المعروضة استنادا إلى المعلومات السابقة. تسمح قائمة التحكم في الوصول (ACL) بدمج بروتوكول BGP الخارجي متعدد البروتوكولات إلى النظير الخارجي، وتوفر عوامل تصفية مضادة للانتحال، وتحمي البنية الأساسية من جميع الوصول الخارجي.

no ipv6 access-list iacl
ipv6 access-list iacl
!!
Phase 1 – Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs ---! of !--- internal space as an external source. !--- Deny fragments to the infrastructure block. deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source. !--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any !! !--- Phase 2 – Explicit Permit !--- Permit only applications/protocols whose destination !--- address is part of the infrastructure IP block. !--- The source of the traffic should be known and authorized. !--- Note: This template must be tuned to the !--- specific source address environment of the network. Variables in !--- the template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host 2001:0DB8:C18:2:1::1 !!! !--- Phase 3 – Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48 !!! !--- Phase 4 – Explicit Permit for Transit Traffic permit ipv6 any any

معلومات ذات صلة

- صفحة دعم قوائم الوصول
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

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).