حماية أمان الشبكة وإتاحة الوصول إلى أطراف ثالثة

المحتويات

المقدمة

أثناء مسار طلب الخدمة هذا، قد تحتاج إلى مهندسي Cisco للوصول إلى شبكة مؤسستك. سيؤدي منح هذا الوصول في أغلب الأحيان إلى السماح بحل طلب الخدمة الخاص بك بسرعة أكبر. في مثل هذه الحالات، يمكن ل Cisco الوصول إلى شبكتك باستخدام إذنك، وسوف تقوم بذلك فقط.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

أحلت cisco في طرف إتفاق لمعلومة على وثيقة إتفاق.

أفضل الممارسات

توصي Cisco باتباع هذه الإرشادات لمساعدتك في حماية أمان شبكتك عند منح الوصول إلى أي مهندس دعم أو شخص خارج شركتك أو مؤسستك.

- أستخدم Cisco Unified MeetingPlace، إن أمكن، لمشاركة المعلومات مع مهندسي الدعم. توصي Cisco باستخدام Cisco Unified MeetingPlace لهذه الأسباب:يستخدم Cisco Unified MeetingPlace بروتوكول طبقة مأخذ التوصيل الآمنة (SSL)، وهو أكثر أمانا من طبقة التوصيل الآمنة (SSH) أو برنامج Telnet في بعض

الحالات.لا يتطلب Cisco Unified MeetingPlace منك توفير كلمات المرور لأي شخص خارج شركتك أو مؤسستك.**ملاحظة:** عند منح الوصول إلى الشبكة إلى أشخاص من خارج شركتك أو مؤسستك، يجب أن تكون أي كلمات مرور تقدمها كلمات مرور مؤقتة تكون صالحة فقط طالما أن الطرف الثالث يتطلب الوصول إلى شبكتك.عادة، لا يتطلب Cisco Unified MeetingPlace منك تغيير سياسة جدار الحماية لديك لأن معظم جدران الحماية الخاصة بالمؤسسات تسمح بالوصول إلى HTTPS الصادر.تفضل بزيارة Cisco Unified MeetingPlace للحصول على مزيد من المعلومات.

- إذا تعذر عليك إستخدام Cisco Unified MeetingPlace وإذا أخترت السماح بوصول الطرف الثالث من خلال تطبيق آخر، مثل SSH، فتأكد من أن كلمة المرور مؤقتة ومتاحة للاستخدام مرة واحدة فقط. بالإضافة إلى ذلك، يجب عليك تغيير كلمة المرور أو إبطالها فورا بعد أن يصبح الوصول إلى جهة خارجية غير ضروري. إذا كنت تستخدم تطبيقا آخر غير Cisco Unified MeetingPlace، فيمكنك اتباع الإجراءات والإرشادات التالية:لإنشاء حساب مؤقت على موجهات Cisco IOS، أستخدم هذا الأمر:

```
#@!Router(config)#username tempaccount secret QWE
```

لإنشاء حساب مؤقت على PIX/ASA، أستخدم هذا الأمر:

```
#@!PIX(config)#username tempaccount password QWE
```

لإزالة الحساب المؤقت، أستخدم هذا الأمر:

```
Router (config)#no username tempaccount
```

قم بإنشاء كلمة المرور المؤقتة بشكل عشوائي. يجب ألا تكون كلمة المرور المؤقتة مرتبطة بطلب الخدمة المعين أو موفر خدمات الدعم. على سبيل المثال، لا تستخدم كلمات مرور مثل *Cisco* أو *Cisco123* أو *CiscoTAC*.لا تعطي اسم المستخدم أو كلمة المرور الخاصة بك.لا تستخدم Telnet عبر الإنترنت. إنه غير آمن.

- إذا كان جهاز Cisco الذي يتطلب الدعم موجودا خلف جدار حماية شركة وكان التغيير في سياسات جدار الحماية مطلوبا لمهندس الدعم إلى SSH في جهاز Cisco، فتأكد من أن تغيير السياسة خاص بمهندس الدعم المعين للمسألة. لا تجعل إستثناء السياسة مفتوحا على الإنترنت بالكامل أو على نطاق أوسع من البيئات المضيفة أكثر من اللازم.لتعديل سياسة جدار حماية على جدار حماية Cisco IOS، أضف هذه الخطوط إلى قائمة الوصول الواردة أسفل واجهة مواجهة الإنترنت:

```
Router(config)#ip access-list ext inbound
Router(config-ext-nacl)#1 permit tcp host
IP address for TAC engineer> host <Cisco device address> eq 22>
```

ملاحظة: في هذا المثال، يتم عرض التكوين Router(config-ext-nacl)#على سطرين لتوفير المساحة. ومع ذلك، عند إضافة هذا الأمر إلى قائمة الوصول الواردة، يجب أن يظهر التكوين على سطر واحد.لتعديل سياسة جدار حماية على جدار حماية Cisco PIX/ASA، أضف هذا السطر إلى مجموعة الوصول الواردة:

```
ASA(config)#access-list inbound line 1 permit tcp host
IP address for TAC engineer> host <Cisco device address> eq 22>
```

ملاحظة: في هذا المثال، يتم عرض تكوين ASA(config)# على سطرين لتوفير المساحة. ومع ذلك، عند إضافة هذا الأمر إلى مجموعة الوصول الواردة، يجب أن يظهر التكوين على سطر واحد.للسماح بوصول SSH على موجهات Cisco IOS، أضف هذا السطر إلى فئة الوصول:

```
<Router(config)#access-list 2 permit host <IP address for TAC engineer
Router(config)#line vty 0 4
Router(config-line)#access-class 2
```

للسماح بوصول SSH على Cisco PIX/ASA، أضف هذا التكوين:

```
ASA(config)#ssh <IP address for TAC engineer> 255.255.255.255 outside
```

إذا كانت لديك أسئلة حول المعلومات الموضحة في هذا المستند أو تتطلب مساعدة إضافية، فاتصل بمركز المساعدة التقنية (TAC) من Cisco.

يقصد من أفضل الممارسات المذكورة أعلاه أن تكون شاملة، ولكنها تقترح لتكميل إجراءات الأمان الحالية للعملاء. تعتمد فعالية أي ممارسة أمنية على الحالة الخاصة بكل عميل، ويشجع العملاء على مراعاة جميع العوامل ذات الصلة عند تحديد الإجراءات الأمنية الأنسب لشبكاتهم.

معلومات ذات صلة

- مجموعة Cisco من Unified MeetingPlace
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- مركز المساعدة التقنية (TAC) من Cisco
- 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).