قوائم التحكم في الوصول على قوائم التحكم في الوصول (WLCs) - القواعد والقيود والأمثلة

المحتويات

المقدمة

يوفر هذا المستند معلومات حول قوائم التحكم في الوصول (ACLs) على وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs). يشرح هذا المستند القيود والقواعد الحالية، ويقدم أمثلة ذات صلة. لا يقصد بهذا المستند أن يكون بديلا لقوائم التحكم في الوصول (ACL) على مثال تكوين وحدة تحكم الشبكة المحلية اللاسلكية، ولكن لتوفير معلومات تكميلية.

ملاحظة: لقوائم التحكم في الوصول (ACL) من الطبقة 2 أو مرونة إضافية في قواعد قائمة التحكم في الوصول (ACL) من الطبقة 3، توصي Cisco بتكوين قوائم التحكم في الوصول (ACL) على موجه الخطوة الأولى المتصل بوحدة التحكم.

يقع الخطأ الأكثر شيوعا عندما يتم تعيين حقل البروتوكول على IP (البروتوكول=4) في سطر قائمة التحكم في الوصول بنية السماح لحزم IP أو رفضها. نظرا لأن هذا الحقل يحدد بالفعل ما يتم تغليفه داخل حزمة IP، مثل TCP وبروتوكول مخطط بيانات المستخدم (UDP) وبروتوكول رسائل التحكم في الإنترنت (ICMP)، فإنه يترجم إلى حظر حزم IP داخل IP أو السماح بها. إذا لم تكن ترغب في حظر حزم IP المحمولة، فيجب عدم تحديد IP في أي خط قائمة تحكم في الوصول (ACL). يقوم معرف تصحيح الأخطاء من CSCsh22975 Cisco (العملاء المسجلون فقط) بتغيير IP إلى IP in-IP.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- معرفة كيفية تكوين نقطة الوصول في الوضع Lightweight (LAP) و WLC للتشغيل الأساسي
- معرفة أساسية ببروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) وطرائق الأمان اللاسلكية

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

فهم قوائم التحكم في الوصول (ACL) على وحدة تحكم في الشبكة المحلية اللاسلكية (WLC)

تتكون قوائم التحكم في الوصول من خط واحد أو أكثر من خطوط قائمة التحكم في الوصول يتبعه "رفض أي" ضمني في نهاية قائمة التحكم في الوصول. يحتوي كل سطر على هذه الحقول:

- رقم تسلسلي
- إتجاه
- عنوان IP وقناع المصدر
- غاية عنوان وقناع
- البروتوكول
- منفذ SRC
- المنفذ الرئيسي
- DSCP
- الإجراء

يصف هذا المستند كل حقل من هذه الحقول:

- **الرقم التسلسلي**— يشير إلى الترتيب الذي تتم معالجة خطوط قائمة التحكم في الوصول مقابل الحزمة. تتم معالجة الحزمة مقابل قائمة التحكم في الوصول (ACL) حتى تطابق سطر قائمة التحكم في الوصول (ACL) الأول. كما يسمح لك بإدراج خطوط قائمة التحكم في الوصول (ACL) في أي مكان في قائمة التحكم في الوصول (ACL) حتى بعد إنشاء قائمة التحكم في الوصول (ACL). على سبيل المثال، إذا كان لديك خط قائمة تحكم في الوصول (ACL) برقم تسلسلي 1، فيمكنك إدراج خط قائمة تحكم في الوصول (ACL) جديد في المقدمة إذا كان ذلك عن طريق وضع رقم تسلسلي 1 في سطر قائمة التحكم في الوصول (ACL) الجديد. يؤدي هذا تلقائيا إلى تحريك الخط الحالي لأسفل في قائمة التحكم في الوصول (ACL).
- **الإتجاه** — يخبر وحدة التحكم في الإتجاه الذي يتم فيه فرض خط قائمة التحكم في الوصول (ACL). هناك ثلاثة أتجاهات: داخلية وخارجية وأي. هذه الاتجاهات مأخوذة من وضع متعلق بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وليس العميل اللاسلكي.يتم فحص حزم IP الواردة التي يتم الحصول عليها من العميل اللاسلكي لمعرفة ما إذا كانت تطابق سطر قائمة التحكم في الوصول (ACL).يتم فحص حزم IP الصادرة الموجهة إلى العميل اللاسلكي لمعرفة ما إذا كانت تطابق سطر قائمة التحكم في الوصول (ACL).يتم فحص حزم IP—Any المستمدة من العميل اللاسلكي والموجهة إلى العميل اللاسلكي لمعرفة ما إذا كانت تطابق سطر قائمة التحكم في الوصول (ACL). يتم تطبيق سطر قائمة التحكم في الوصول (ACL) على كلا الاتجاهين الوارد والصادر.**ملاحظة:** العنوان والقناع الوحيدان اللذان يجب إستخدامهما عند تحديد أي للاتجاه هو 0.0.0.0/0.0.0.0

(أي). يجب عدم تحديد مضيف أو شبكة فرعية معينة باستخدام إتجاه "أي" لأنه سيتم طلب سطر جديد مع العناوين أو الشبكات الفرعية التي يتم تبديلها للسماح بحركة المرور العائدة.يجب إستخدام أي إتجاه فقط في حالات معينة حيث تريد حظر أو السماح ببروتوكول IP معين أو منفذ في كلا الاتجاهين، والانتقال إلى العملاء اللاسلكيين (الصادر) والقادم من العملاء اللاسلكيين (الوارد).عند تحديد عناوين IP أو الشبكات الفرعية، يجب عليك تحديد الإتجاه كالوارد أو الصادر وإنشاء خط قائمة تحكم في الوصول (ACL) جديد ثان لحركة المرور العائدة في الإتجاه المعاكس. إذا تم تطبيق قائمة التحكم في الوصول (ACL) على واجهة ولا تسمح بحركة المرور العائدة العائدة بشكل محدد، يتم رفض حركة المرور العائدة بواسطة "رفض أي" الضمني في نهاية قائمة التحكم في الوصول.

- **عنوان IP المصدر والقناع**— يحدد عناوين IP المصدر من مضيف واحد إلى شبكات فرعية متعددة، والتي تعتمد على القناع. يتم إستخدام القناع بالاقتران مع عنوان IP لتحديد وحدات بت في عنوان IP التي يجب تجاهلها عند مقارنة عنوان IP هذا بعنوان IP في الحزمة.**ملاحظة:** الأقنعة الموجودة في قائمة التحكم بالوصول (ACL) إلى WLC ليست كالأقنعة العكسية أو حرف البدل المستخدمة في قوائم التحكم في الوصول (ACL) من Cisco IOS®. في قوائم التحكم في الوصول (ACL) الخاصة بوحدة التحكم، يعني الرقم 255 مطابقة النظام الثماني في عنوان IP تماما، بينما يمثل الرقم 0 حرف بدل. يتم دمج العنوان والقناع بت بت.يعني البت الخاص بالقناع 1 التحقق من قيمة البت المقابلة. تشير المواصفة 255 في القناع إلى أن النظام الثماني في عنوان IP للحزمة التي يتم فحصها يجب أن يتطابق تماما مع النظام الثماني المقابل في عنوان قائمة التحكم في الوصول.تعني وحدة بت القناع 0 عدم التحقق (تجاهل) من قيمة بت المقابلة. تشير المواصفات من 0 في القناع إلى تجاهل النظام الثماني في عنوان IP للحزمة التي يتم فحصها.0.0.0.0/0.0.0.0 مكافئ لعنوان IP "أي" (0.0.0.0 كعنوان و 0.0.0.0 كالقناع).
- **عنوان IP للوجهة وقناع**— يتبع نفس قواعد القناع مثل عنوان IP المصدر وقناع.
- **البروتوكول**—يحدد حقل البروتوكول في رأس حزمة IP. تتم ترجمة بعض أرقام البروتوكولات لضمان راحة العملاء ويتم تعريفها في القائمة المنسدلة. القيم المختلفة هي:أي (كل أرقام البروتوكولات متطابقة)بروتوكول TCP (بروتوكول IP رقم 6)UDP (بروتوكول IP رقم 17)ICMP (بروتوكول IP رقم 1)ESP (بروتوكول IP رقم 50)AH (بروتوكول IP رقم 51)GRE (بروتوكول IP رقم 47)IP (بروتوكول IP رقم 4 ETH)[CSCsh22975] عبر IP-in-IP (بروتوكول IP رقم 97)OSPF (بروتوكول IP رقم 89)أخرى (تحديد)تطابق أي قيمة أي بروتوكول في رأس IP الخاص بالحزمة. يتم إستخدام هذا لحظر حزم IP بالكامل أو السماح لها من/إلى شبكات فرعية معينة. حدد IP لمطابقة حزم IP داخل IP. التحديدات المشتركة هي UDP و TCP التي توفر إعداد منافذ مصدر ووجهة محددة. إذا قمت بتحديد آخر، فيمكنك تحديد أي من أرقام بروتوكول حزمة IP المعرفة بواسطة ANA .
- **منفذ SRC**—يمكن تحديده فقط لبروتوكول TCP و UDP. 0-65535 مكافئ لأي منفذ.
- **أعلى منفذ** — يمكن تحديده فقط لبروتوكول TCP و UDP. 0-65535 مكافئ لأي منفذ.
- **نقطة كود الخدمات المميزة (DSCP)**—تتيح لك تحديد قيم DSCP معينة لتطابقها في رأس حزمة IP. الخيارات في قائمة السحب لأسفل محددة أو أي. إذا قمت بتكوين محدد، فعليك الإشارة إلى القيمة في حقل DSCP. على سبيل المثال، يمكن إستخدام القيم من 0 إلى 63.
- **العمل** — الحكمان ينفيان أو يسمحان. رفض حظر الحزمة المحددة. السماح بإعادة توجيه الحزمة.

قواعد وقيود قائمة التحكم في الوصول (ACL)

قيود قوائم التحكم في الوصول (ACL) المستندة إلى WLC

هذه هي قيود قوائم التحكم في الوصول (ACL) المستندة إلى WLC:

- لا يمكنك أن ترى ما هي خطوط قائمة التحكم في الوصول التي تم مطابقتها بحزمة (راجع معرف تصحيح الأخطاء من Cisco CSCse36574 (العملاء المسجلون فقط)).
- لا يمكنك تسجيل الحزم التي تطابق سطر قائمة التحكم في الوصول (راجع معرف تصحيح الأخطاء من Cisco CSCse36574 (العملاء المسجلون فقط).
- حزم IP (أي حزمة مع حقل بروتوكول إيثرنت يساوي 0x0800 IP]) هي الحزم الوحيدة التي تم فحصها بواسطة قائمة التحكم في الوصول (ACL). لا يمكن حظر أنواع أخرى من حزم الإيثرنت بواسطة قوائم التحكم في

الوصول (ACLs). على سبيل المثال، لا يمكن حظر حزم ARP (بروتوكول الإيثرنت 0x0806) أو السماح بها بواسطة قائمة التحكم في الوصول (ACL).
- يمكن أن يحتوي جهاز التحكم على ما يصل إلى 64 قائمة تحكم في الوصول (ACL) تم تكوينها، ويمكن أن يكون لكل قائمة تحكم في الوصول (ACL) ما يصل إلى 64 خطا كحد أقصى.
- لا تؤثر قوائم التحكم في الوصول (ACL) على حركة مرور البث والبث المتعدد التي تتم إعادة توجيهها من أو إلى نقاط الوصول (APs) والعملاء اللاسلكي (راجع معرف تصحيح الأخطاء من CSCse65613 Cisco (العملاء المسجلون فقط)).
- قبل WLC الإصدار 4.0، يتم تجاوز قوائم التحكم في الوصول (ACL) على واجهة الإدارة، لذلك لا يمكنك التأثير على حركة المرور الموجهة إلى واجهة الإدارة. بعد WLC الإصدار 4.0، يمكنك إنشاء قوائم التحكم في الوصول (ACL) لوحدة المعالجة المركزية. راجع تكوين قوائم التحكم في الوصول إلى وحدة المعالجة المركزية (CPU) للحصول على مزيد من المعلومات حول كيفية تكوين هذا النوع من قائمة التحكم في الوصول.**ملاحظة:** يتم تجاهل قوائم التحكم في الوصول (ACL) المطبقة على واجهات الإدارة و AP-Manager. تم تصميم قوائم التحكم في الوصول (ACL) على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لحظر حركة مرور البيانات بين الشبكة اللاسلكية والشبكة السلكية، وليس الشبكة السلكية و WLC. لذلك، إذا كنت ترغب في منع نقاط الوصول في الشبكات الفرعية المحددة من الاتصال بمركز التحكم في الشبكة المحلية اللاسلكية (WLC) بالكامل، فأنت بحاجة إلى تطبيق قائمة وصول على المحولات أو الموجه المتقطع لديك. سيؤدي هذا إلى حظر حركة مرور LWAPP من نقاط الوصول (VLANs) هذه إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
- تعتمد قوائم التحكم في الوصول (ACL) على المعالج ويمكن أن تؤثر على أداء وحدة التحكم الواقعة تحت الحمل الثقيل.
- لا يمكن لقوائم التحكم في الوصول (ACL) حظر الوصول إلى عنوان IP الظاهري (1.1.1.1). لذلك، لا يمكن حظر DHCP للعملاء اللاسلكيين.
- لا تؤثر قوائم التحكم في الوصول (ACL) على منفذ الخدمة الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC).

قواعد قوائم التحكم في الوصول (ACL) المستندة إلى WLC

هذه هي قواعد قوائم التحكم في الوصول (ACL) المستندة إلى WLC:

- يمكنك فقط تحديد أرقام البروتوكول في رأس IP (UDP، TCP، ICMP، وما إلى ذلك) في خطوط قائمة التحكم في الوصول، نظرا لأن قوائم التحكم في الوصول مقيدة إلى حزم IP فقط. إذا تم تحديد IP، فإن هذا يشير إلى أنك تريد السماح بحزم IP الموجودة في IP أو رفضها. إذا تم تحديد أي منها، فهذا يشير إلى أنك تريد السماح بالحزم أو رفضها باستخدام أي بروتوكول IP.
- إذا قمت بتحديد أي للاتجاه، يجب أن يكون المصدر والوجهة أي (0.0.0.0/0.0.0.0).
- إذا لم يكن عنوان IP للمصدر أو الوجهة "أي"، فيجب تحديد إتجاه عامل التصفية. كما يجب إنشاء عبارة معكوسة (مع مصدر عنوان IP/منفذ وعنوان IP/منفذ الوجهة التي يتم تبديلها) في الإتجاه المعاكس لحركة المرور العائدة.
- هناك "رفض أي" ضمني في نهاية قائمة التحكم في الوصول (ACL). إذا لم تطابق الحزمة أي خطوط في قائمة التحكم في الوصول، يتم إسقاطها بواسطة وحدة التحكم.

التكوينات

مثال قائمة التحكم في الوصول مع DHCP، و ping، و HTTP، و DNS

في مثال التكوين هذا، يمكن للعملاء فقط:

- استلم عنوان DHCP (لا يمكن حظر DHCP بواسطة قائمة التحكم في الوصول (ACL))
- إختبار الاتصال والضغط (أي نوع رسالة ICMP - لا يمكن تقييده إلى إختبار الاتصال فقط)
- إجراء إتصالات HTTP (الصادرة)

- تحليل نظام اسم المجال (DNS) (الصادر)

لتكوين متطلبات الأمان هذه، يجب أن تحتوي قائمة التحكم في الوصول (ACL) على أسطر للسماح:

- أي رسالة ICMP في أي إتجاه (لا يمكن تقييده إلى إختبار الاتصال فقط)
- أي منفذ UDP إلى DNS الوارد
- DNS إلى أي منفذ UDP صادر (حركة مرور الإرجاع)
- أي منفذ TCP إلى HTTP الوارد
- HTTP إلى أي منفذ TCP صادر (حركة مرور الإرجاع)

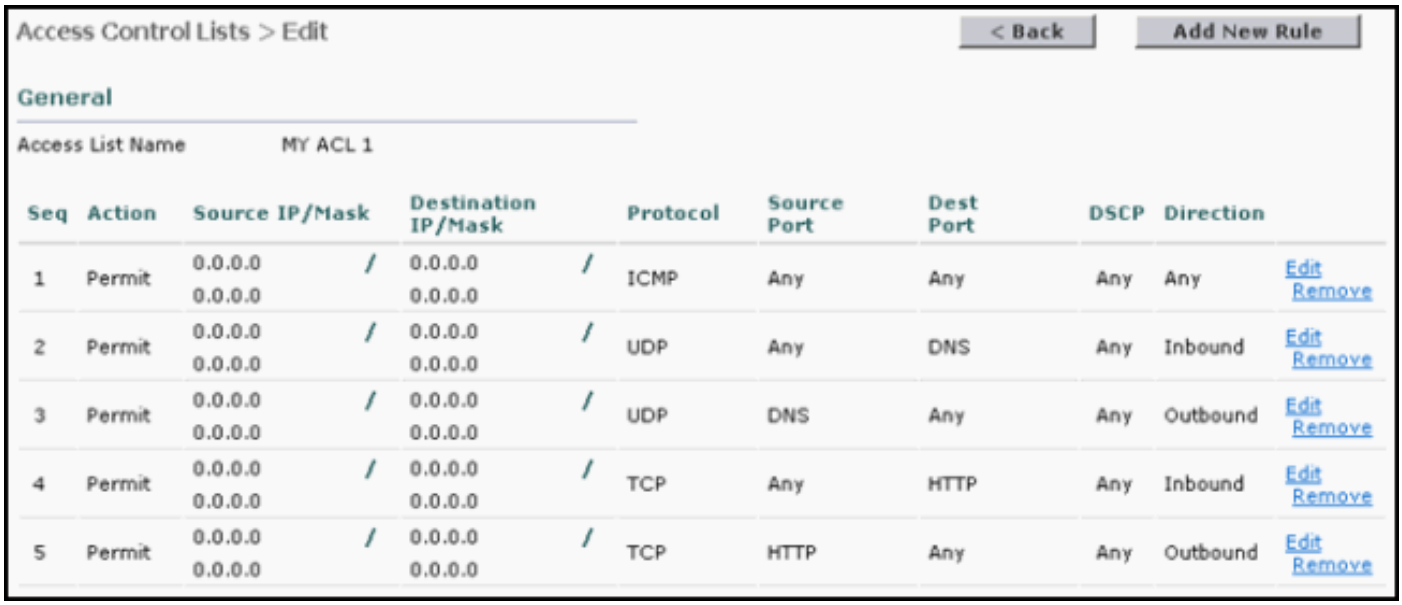
هذا ما تبدو عليه قائمة التحكم في الوصول (ACL) في **إخراج الأمر show acl "قائمة التحكم في الوصول (ACL) التفصيلية** "My ACL 1" (لا تكون علامات الاقتباس ضرورية إلا إذا كان اسم قائمة التحكم في الوصول (ACL) أكثر من كلمة):

```
Seq  Direction  Source IP/Mask   Dest IP/Mask     Protocol  Src Port  Dest Port  DSCP  Action
------  ----  ---------  --------  --------  --------------  --------------  ---------  ---
Any      0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     1      0-65535   0-65535      Any  Permit      1
In       0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     17     0-65535   53-53        Any  Permit      2
Out      0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     17     53-53     0-65535      Any  Permit      3
```

يمكن أن تكون قائمة التحكم في الوصول (ACL) أكثر تقييدا إذا قمت بتحديد الشبكة الفرعية التي يتواجد عليها العملاء اللاسلكيون بدلا من أي عنوان IP في خطوط DNS و HTTP ACL.

ملاحظة: لا يمكن تقييد خطوط قائمة التحكم في الوصول (ACL) إلى DHCP عبر الشبكة الفرعية نظرا لأن العميل يستلم في البداية عنوان IP الخاص به باستخدام 0.0.0.0، ثم يقوم بإعادة تحديث عنوان IP الخاص به عبر عنوان شبكة فرعية.

هذا ما تبدو عليه قائمة التحكم في الوصول (ACL) نفسها في واجهة المستخدم الرسومية:



مثال قائمة التحكم في الوصول مع DHCP، و ping، و HTTP، و SCCP

في مثال التكوين هذا، يمكن لهواتف بروتوكول الإنترنت طراز 7920 فقط ما يلي:

- إستلام عنوان DHCP (لا يمكن حظره بواسطة قائمة التحكم في الوصول (ACL))
- إختبار الاتصال والضغط (أي نوع رسالة ICMP - لا يمكن تقييده إلى إختبار الاتصال فقط)
- السماح بتحليل DNS (الوارد)
- اتصال هاتف IP ب CallManager والعكس (أي إتجاه)

- إتصالات هاتف IP بخادم TFTP (يستخدم CallManager المنفذ الديناميكي بعد اتصال TFTP الأولي بمنفذ UDP 69) (الصادر)
- السماح لهاتف بروتوكول الإنترنت طراز 7920 للاتصال عبر بروتوكول الإنترنت (IP) (أي إتجاه)
- عدم السماح لهاتف IP أو دليل الهاتف (الصادر). يتم القيام بذلك عبر سطر قائمة تحكم في الوصول (ACL) ضمني "رفض أي" في نهاية قائمة التحكم في الوصول (ACL).وهذا سيسمح بالاتصالات الصوتية بين هواتف بروتوكول الإنترنت بالإضافة إلى عمليات التحميل العادية بين هاتف بروتوكول الإنترنت و CallManager.

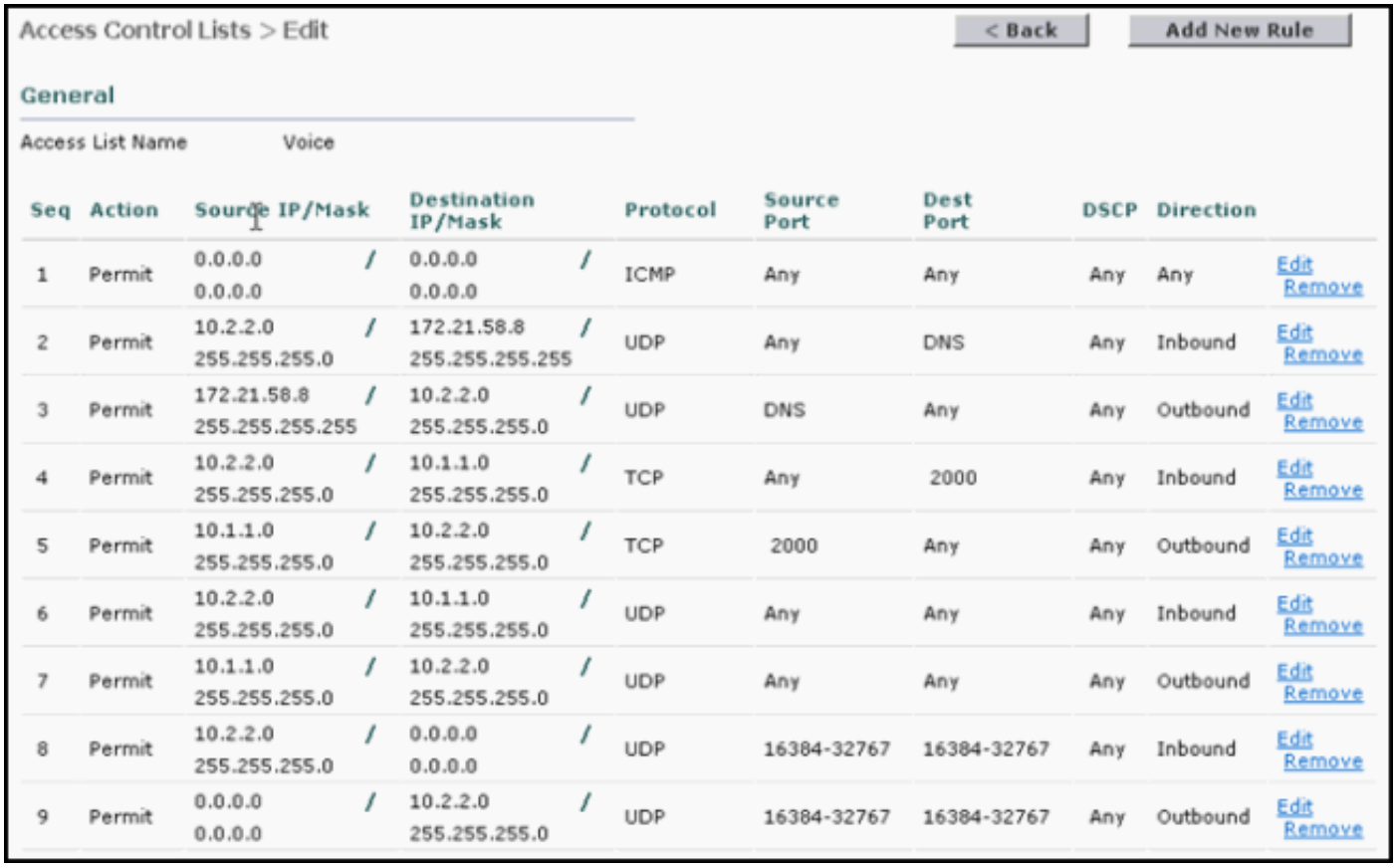
لتكوين متطلبات الأمان هذه، يجب أن تحتوي قائمة التحكم في الوصول (ACL) على أسطر للسماح:

- أي رسالة ICMP (لا يمكن تقييده إلى إختبار الاتصال فقط) (أي إتجاه)
- هاتف IP إلى خادم DNS (منفذ UDP 53) (الوارد)
- خادم DNS إلى هواتف IP (منفذ UDP 53) (الصادر)
- منافذ TCP لهاتف IP إلى منفذ CallManager TCP 2000 (المنفذ الافتراضي) (الوارد)
- منفذ TCP 2000 من CallManager إلى هواتف IP (الصادرة)
- منفذ UDP من هاتف IP إلى خادم TFTP. لا يمكن تقييد هذا بمنفذ TFTP القياسي (69) لأن CallManager يستخدم منفذا ديناميكيا بعد طلب الاتصال الأولي لنقل البيانات.
- منفذ UDP لحركة مرور الصوت RTP بين هواتف IP (منافذ UDP16384-32767) (أي إتجاه)

في هذا المثال، تعد الشبكة الفرعية لهاتف بروتوكول الإنترنت طراز 7920 هي 24/10.2.2.0 والشبكة الفرعية CallManager هي 24/10.1.1.0. خادم DNS هو 172.21.58.8. هذا هو المخرج من الأمر **show acl detail voice**:

```
Seq Direction Source IP/Mask          Dest IP/Mask            Protocol Src Port  Dest Port  DSCP
                                                                                          Action
----  ---------  -------- --------        ---------------        --------------- --------- ---
                                                                                          ------
 Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0           1     0-65535   0-65535    Any     1
                                                                                          Permit
 In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53      Any     2
                                                                                          Permit
 Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535    Any     3
                                                                                          Permit
 In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     6     0-65535   2000-2000  Any     4
                                                                                          Permit
 Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     6     2000-2000 0-65535    Any     5
                                                                                          Permit
 In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     17    0-65535   0-65535    Any     6
                                                                                          Permit
 Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     17    0-65535   0-65535    Any     7
                                                                                          Permit
 In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0           17 16384-32767 16384-32767 Any     8
                                                                                          Permit
 Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0     17 16384-32767 16384-32767 Any     9
                                                                                          Permit
```

هذا ما يبدو عليه في واجهة المستخدم الرسومية:



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name: Voice

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound	Edit Remove
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound	Edit Remove
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound	Edit Remove
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound	Edit Remove
8	Permit	10.2.2.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	16384-32767	16384-32767	Any	Inbound	Edit Remove
9	Permit	0.0.0.0 / 0.0.0.0	10.2.2.0 / 255.255.255.0	UDP	16384-32767	16384-32767	Any	Outbound	Edit Remove

الملحق: منافذ هاتف بروتوكول الإنترنت 7920

هذا هو الوصف الموجز من الميناء ال ip 7920 هاتف أن يتصل مع ال cisco CallManager (CCM) آخر هاتف:

- الهاتف إلى TFTP] CCM] (منفذ UDP 69 في البداية ثم قم بالتغيير إلى منفذ ديناميكي [EPHAMERAL] لنقل البيانات)—بروتوكول نقل الملفات المبسط (TFTP) المستخدم لتنزيل البرامج الثابتة وملفات التكوين.
- الهاتف إلى CCM [خدمات الويب، الدليل] (منفذ TCP 80)—عناوين URL الخاصة بالهاتف لتطبيقات XML والمصادقة والدلائل والخدمات، إلخ. وتكون هذه المنافذ قابلة للتكوين على أساس كل خدمة.
- الهاتف إلى CCM [إرسال الإشارات الصوتية] (منفذ TCP 2000)—بروتوكول التحكم في العميل النحيل (SCCP). هذا المنفذ قابل للتكوين.
- الهاتف إلى CCM [إشارات الصوت الآمنة] (منفذ TCP 2443)—بروتوكول التحكم في عميل Skinny الآمن (SCCPS)
- هاتف إلى CAPF [شهادات] (منفذ TCP 3804)—منفذ الاستماع لوكيل مرجع الشهادة (CAPF) لإصدار الشهادات المهمة محليا (LSCs) إلى هواتف IP.
- حامل الصوت إلى/من الهاتف [المكالمات الهاتفية] (منافذ UDP 16384 - 32768) - بروتوكول الوقت الفعلي (RTP)، بروتوكول الوقت الفعلي الآمن (SRTP). **ملاحظة:** يستخدم CCM منافذ UDP 24576-32768 فقط، ولكن يمكن للأجهزة الأخرى إستخدام النطاق الكامل.
- هاتف IP إلى خادم DNS] DNS] (منفذ UDP 53)—تستخدم الهواتف نظام DNS لحل اسم المضيف الخاص بخوادم TFTP وأجهزة CallManager وأسماء مضيف خادم الويب عند تكوين النظام لاستخدام الأسماء بدلا من عناوين IP.
- هاتف بروتوكول الإنترنت إلى خادم DHCP] DHCP] (منفذ client] UDP 67] و 68 [server])- يستخدم الهاتف بروتوكول DHCP لاسترداد عنوان IP إذا لم يتم تكوينه بشكل ثابت.

يمكن العثور على المنافذ التي يستخدمها CallManager 5.0 للاتصال بها في إستخدام منفذ Cisco Unified CallManager 5.0 TCP و UDP. كما أنه يحتوي على المنافذ المحددة التي يستخدمها للاتصال بهاتف بروتوكول الإنترنت طراز 7920.

يمكن العثور على المنافذ التي يستخدمها CallManager 4.1 للاتصال بها في إستخدام منفذ TCP و UDP الموحد Cisco Unified CallManager 4.1. كما أنه يحتوي على المنافذ المحددة التي يستخدمها للاتصال بهاتف بروتوكول الإنترنت طراز 7920.

معلومات ذات صلة

- مثال على تكوين ACL على وحدة تحكّم الشبكة المحلية اللاسلكية
- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 4.0 من Cisco
- 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).