ACLs auf WLCs - Regeln, Einschränkungen und Beispiele

Inhalt

Einleitung

Dieses Dokument enthält Informationen zu Zugriffskontrolllisten (ACLs) auf Wireless LAN Controllern (WLCs). In diesem Dokument werden die aktuellen Einschränkungen und Regeln erläutert, und es werden relevante Beispiele aufgeführt. Dieses Dokument ist nicht als Ersatz für ACLs am Konfigurationsbeispiel eines Wireless LAN-Controllers gedacht, sondern enthält zusätzliche Informationen.

Hinweis: Für Layer-2-ACLs oder zusätzliche Flexibilität bei Layer-3-ACL-Regeln empfiehlt Cisco, dass Sie ACLs auf dem mit dem Controller verbundenen First-Hop-Router konfigurieren.

Der häufigste Fehler tritt auf, wenn das Protokollfeld in einer ACL-Leitung auf IP (Protokoll=4) gesetzt wird, um IP-Pakete zuzulassen oder zu verweigern. Da in diesem Feld die Kapselung im IP-Paket ausgewählt wird, z. B. TCP, User Datagram Protocol (UDP) und Internet Control Message Protocol (ICMP), werden IP-in-IP-Pakete blockiert bzw. zugelassen. Wenn Sie mobile IP-Pakete nicht blockieren möchten, darf die IP-Adresse nicht in einer ACL-Leitung ausgewählt werden. Cisco Bug-ID CSCsh2975 (nur für registrierte Kunden) ändert IP in IP in IP.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Kenntnisse der Konfiguration des WLC und des Lightweight Access Point (LAP) für den Grundbetrieb
- Grundkenntnisse von LWAPP (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

ACLs auf einem WLC verstehen

ACLs bestehen aus einer oder mehreren ACL-Leitungen, gefolgt von einem impliziten "deny any any" am Ende der ACL. Für jede Zeile gibt es folgende Felder:

- Sequenznummer
- Richtung
- Quell-IP-Adresse und -Maske
- Ziel-IP-Adresse und -Maske
- Protokolle
- SRC-Port
- Zielport
- DSCP
- Aktion

In diesem Dokument werden die folgenden Felder beschrieben:

- **Sequence Number (**Sequenznummer): Gibt die Reihenfolge an, in der ACL-Posten für das Paket verarbeitet werden. Das Paket wird für die ACL verarbeitet, bis es mit der ersten ACL-Leitung übereinstimmt. Sie können ACL-Zeilen auch nach dem Erstellen der ACL an einer beliebigen Stelle in die ACL einfügen. Wenn Sie z. B. eine ACL-Leitung mit der Sequenznummer 1 haben, können Sie eine neue ACL-Leitung davor einfügen, indem Sie die Sequenznummer 1 in die neue ACL-Leitung eingeben. Dadurch wird die aktuelle Zeile in der ACL automatisch nach unten verschoben.
- **Direction (Richtung)**: teilt dem Controller mit, in welche Richtung die ACL-Leitung durchgesetzt werden soll. Es gibt drei Richtungen: Eingehend, Ausgehend und Alle. Diese Richtungen werden von einer Position relativ zum WLC und nicht zum Wireless-Client genommen.Inbound (Eingehend): Vom Wireless-Client stammende IP-Pakete werden auf Übereinstimmung mit der ACL geprüft.Outbound (Ausgehend): An den Wireless-Client gerichtete IP-Pakete werden auf Übereinstimmung mit der ACL-Leitung geprüft.Any (Beliebig): IP-Pakete, die vom Wireless-Client stammen und an den Wireless-Client gerichtet sind, werden überprüft, um festzustellen, ob sie mit der ACL-Leitung übereinstimmen. Die

ACL-Zeile wird sowohl in die ein- als auch in die ausgehende Richtung angewendet.**Hinweis:** Die einzige Adresse und Maske, die verwendet werden soll, wenn Sie Any (Beliebig) für die Richtung auswählen, ist 0.0.0.0/0.0.0.0 (Beliebig). Sie dürfen keinen bestimmten Host oder Subnetz mit der Richtung "Any" (Beliebig) angeben, da eine neue Leitung erforderlich ist, bei der die Adressen oder Subnetze ausgetauscht werden, um den zurückkehrenden Datenverkehr zu ermöglichen.Die "Any"-Richtung sollte nur in bestimmten Situationen verwendet werden, in denen Sie ein bestimmtes IP-Protokoll oder einen bestimmten Port in beide Richtungen blockieren oder zulassen möchten, d. h., wenn Sie zu den Wireless-Clients gehen (ausgehend) und von den Wireless-Clients kommen (eingehend).Wenn Sie IP-Adressen oder Subnetze angeben, müssen Sie die Richtung als ein- oder ausgehend angeben und eine zweite neue ACL-Leitung für den Rückverkehr in die entgegengesetzte Richtung erstellen. Wenn eine ACL auf eine Schnittstelle angewendet wird und keine explizite Rückleitung von Datenverkehr zulässt, wird der zurückgegebene Datenverkehr durch die implizite Option "deny any any" am Ende der ACL-Liste abgelehnt.

- **Source IP Address and Mask** (Quell-IP-Adresse und -Maske): Definiert die Quell-IP-Adressen eines Hosts für mehrere Subnetze, je nach Maske. Die Maske wird in Verbindung mit einer IP-Adresse verwendet, um zu bestimmen, welche Bits in einer IP-Adresse ignoriert werden sollen, wenn diese IP-Adresse mit der IP-Adresse im Paket verglichen wird.**Hinweis:** Masken in einer WLC-ACL ähneln nicht den Platzhaltermasken oder inversen Masken, die in Cisco IOS®-ACLs verwendet werden. Bei Controller-ACLs entspricht 255 genau dem Oktett in der IP-Adresse, während 0 ein Platzhalter ist. Adresse und Maske werden Bit für Bit zusammengefasst.Ein Maskenbit 1 bedeutet, den entsprechenden Bitwert zu überprüfen. Die Angabe von 255 in der Maske gibt an, dass das Oktett in der IP-Adresse des überprüften Pakets genau mit dem entsprechenden Oktett in der ACL-Adresse übereinstimmen muss.Ein Maskenbit 0 bedeutet, dass der entsprechende Bitwert nicht überprüft (ignoriert) wird. Die Angabe von 0 in der Maske gibt an, dass das Oktett in der IP-Adresse des Pakets, das überprüft wird, ignoriert wird.0.0.0.0/0.0.0.0 entspricht "Any" IP Address (0.0.0.0 als Adresse und 0.0.0.0 als Maske).
- **Destination IP Address and Mask** (Ziel-IP-Adresse und -Maske): Es gelten die gleichen Maskenregeln wie die Quell-IP-Adresse und -Maske.
- **Protocol** (Protokoll): Gibt das Protokollfeld im IP-Paket-Header an. Einige der Protokollnummern werden aus Gründen der Benutzerfreundlichkeit übersetzt und im Dropdown-Menü definiert. Die verschiedenen Werte sind:Alle (alle Protokollnummern stimmen überein)TCP (IP-Protokoll 6)UDP (IP-Protokoll 17)ICMP (IP-Protokoll 1)ESP (IP-Protokoll 50)AH (IP-Protokoll 51)GRE (IP-Protokoll 47)IP (IP-Protokoll 4, IP-in-IP [CSCsh22975])Eth Over IP (IP-Protokoll 97)OSPF (IP-Protokoll 89)Andere (bitte angeben)Der Any-Wert entspricht einem beliebigen Protokoll im IP-Header des Pakets. Diese wird verwendet, um IP-Pakete zu/von bestimmten Subnetzen vollständig zu blockieren oder zuzulassen. Wählen Sie IP aus, um IP-in-IP-Pakete abzugleichen. Allgemeine Auswahlmöglichkeiten sind UDP und TCP, die die Einstellung bestimmter Quell- und Ziel-Ports ermöglichen. Wenn Sie Andere auswählen, können Sie eine beliebige IP-Paketprotokollnummer angeben, die von der IANA definiert wurde .
- **Src Port (**Src-Port): Kann nur für das TCP- und UDP-Protokoll angegeben werden. 0-65535 entspricht Any Port (Beliebiger Port).
- **Dest Port (Zielport**): Kann nur für das TCP- und UDP-Protokoll angegeben werden. 0-65535 entspricht Any Port (Beliebiger Port).
- **Differentiated Services Code Point (DSCP)**: Ermöglicht Ihnen, bestimmte DSCP-Werte anzugeben, die im IP-Paket-Header übereinstimmen sollen. Die Optionen im Dropdown-Menü

sind spezifisch oder beliebig. Wenn Sie einen bestimmten Wert konfigurieren, geben Sie diesen im Feld "DSCP" an. Beispielsweise können Werte von 0 bis 63 verwendet werden.
- **Action (Aktion)**: Die beiden Aktionen sind deny (Ablehnen) oder permit. Verweigern blockiert das angegebene Paket. Leiten Sie die Übertragung des Pakets zu.

ACL-Regeln und -Einschränkungen

Einschränkungen WLC-basierter ACLs

Dies sind die Einschränkungen von WLC-basierten ACLs:

- Sie können nicht sehen, welcher ACL-Zeile ein Paket entspricht (siehe Cisco Bug-ID CSCse36574 (nur registrierte Kunden)).
- Pakete, die mit einer bestimmten ACL-Leitung übereinstimmen, können nicht protokolliert werden (siehe Cisco Bug-ID CSCse36574 (nur registrierte Kunden)).
- IP-Pakete (alle Pakete mit einem Ethernet-Protokollfeld gleich IP [0x0800]) sind die einzigen Pakete, die von der ACL geprüft werden. Andere Arten von Ethernet-Paketen können von ACLs nicht blockiert werden. ARP-Pakete (Ethernet-Protokoll 0x0806) können beispielsweise nicht von der ACL blockiert oder zugelassen werden.
- Für einen Controller können bis zu 64 ACLs konfiguriert werden; jede ACL kann bis zu 64 Leitungen haben.
- ACLs haben keine Auswirkungen auf den Multicast- und Broadcast-Datenverkehr, der von oder zu den Access Points (APs) und Wireless Clients weitergeleitet wird (siehe Cisco Bug-ID CSCse65613 (nur für registrierte Kunden)).
- Vor WLC Version 4.0 werden ACLs auf der Verwaltungsschnittstelle umgangen. Sie können daher den Datenverkehr, der an die Verwaltungsschnittstelle gerichtet ist, nicht beeinflussen. Nach WLC Version 4.0 können Sie CPU-ACLs erstellen. Weitere Informationen zum Konfigurieren dieses ACL-Typs finden Sie unter Configure CPU ACLs (CPU-ACLs konfigurieren).**Hinweis:** Auf die Management- und AP-Manager-Schnittstellen angewendete ACLs werden ignoriert. Die ACLs des WLC sind so konzipiert, dass sie den Datenverkehr zwischen dem Wireless- und dem kabelgebundenen Netzwerk blockieren, nicht zwischen dem kabelgebundenen Netzwerk und dem WLC. Wenn Sie also verhindern möchten, dass APs in bestimmten Subnetzen vollständig mit dem WLC kommunizieren, müssen Sie eine Zugriffsliste auf Ihre intermittierenden Switches oder Router anwenden. Dadurch wird der LWAPP-Datenverkehr von diesen APs (VLANs) zum WLC blockiert.
- ACLs sind prozessorabhängig und können die Leistung des Controllers bei hoher Auslastung beeinträchtigen.
- ACLs können den Zugriff auf die virtuelle IP-Adresse (1.1.1.1) nicht blockieren. Daher kann DHCP für Wireless-Clients nicht blockiert werden.
- ACLs haben keine Auswirkungen auf den Service-Port des WLC.

Regeln für WLC-basierte ACLs

Dies sind die Regeln für WLC-basierte ACLs:

- Sie können Protokollnummern nur im IP-Header (UDP, TCP, ICMP usw.) der ACL-Leitungen angeben, da ACLs nur auf IP-Pakete beschränkt sind. Wenn IP ausgewählt ist, bedeutet dies,

dass Sie IP-in-IP-Pakete zulassen oder ablehnen möchten. Wenn Any (Beliebig) ausgewählt ist, bedeutet dies, dass Sie Pakete mit einem beliebigen IP-Protokoll zulassen oder ablehnen möchten.
- Wenn Sie Any (Beliebig) als Richtung auswählen, sollten Quelle und Ziel Any (Beliebig) (0.0.0.0/0.0.0.0) sein.
- Wenn die Quell- oder Ziel-IP-Adresse nicht Any (Beliebig) ist, muss die Richtung des Filters angegeben werden. Außerdem muss für den zurückkehrenden Datenverkehr eine umgekehrte Anweisung (bei Auslagerung von Quell-IP-Adresse/Port und Austausch von Ziel-IP-Adresse/Port) in die entgegengesetzte Richtung erstellt werden.
- Am Ende der ACL wird implizit "deny any any" (Alle verweigern) angezeigt. Wenn ein Paket mit keiner der Leitungen in der ACL übereinstimmt, wird es vom Controller verworfen.

Konfigurationen

Beispiel für ACL mit DHCP, PING, HTTP und DNS

In diesem Konfigurationsbeispiel können Clients nur:

- Empfangen einer DHCP-Adresse (DHCP kann nicht von einer ACL blockiert werden)
- Ping und Ping (jeder ICMP-Nachrichtentyp kann nicht auf Ping beschränkt werden)
- HTTP-Verbindungen herstellen (ausgehend)
- DNS-Auflösung (Domain Name System) (ausgehend)

Um diese Sicherheitsanforderungen zu konfigurieren, muss die ACL über Leitungen verfügen, die Folgendes ermöglichen:

- Jede ICMP-Nachricht in beide Richtungen (kann nicht auf Ping beschränkt werden)
- Beliebiger UDP-Port an eingehenden DNS-Verkehr
- DNS an jeden ausgehenden UDP-Port (Rückverkehr)
- Jeder TCP-Port zu eingehendem HTTP
- HTTP an jeden ausgehenden TCP-Port (Rückverkehr)

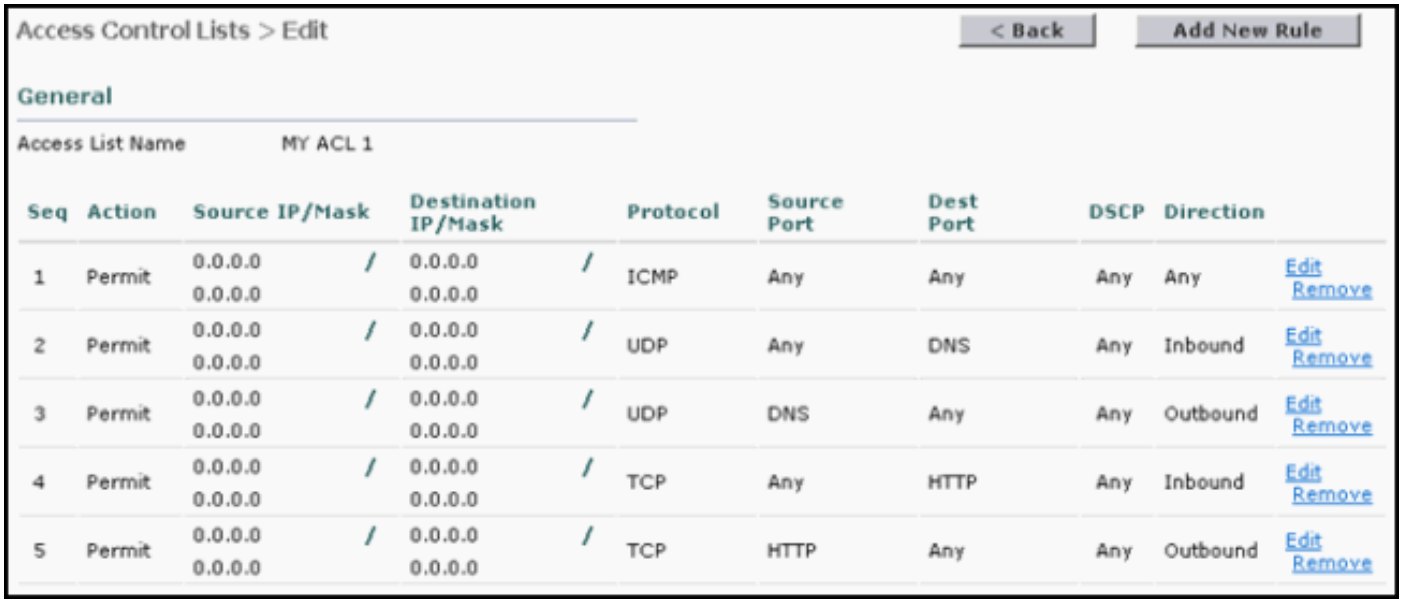
So sieht die ACL in der **Ausgabe** des Befehls **show acl detail "MY ACL 1" aus (**Anführungszeichen sind nur erforderlich, wenn der ACL-Name länger als ein Wort ist):

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

Die ACL kann restriktiver sein, wenn Sie das Subnetz angeben, in dem sich die Wireless-Clients befinden, anstatt Any IP address in den DNS- und HTTP-ACL-Zeilen.

Hinweis: Die DHCP-ACL-Leitungen können nicht auf ein Subnetz beschränkt werden, da der Client zunächst seine IP-Adresse unter Verwendung von 0.0.0.0 erhält und dann seine IP-Adresse über eine Subnetzadresse erneuert.

So sieht die gleiche ACL in der GUI aus:



ACL-Beispiel mit DHCP, PING, HTTP und SCCP

In diesem Konfigurationsbeispiel können 7920 IP-Telefone nur Folgendes ausführen:

- DHCP-Adresse empfangen (kann nicht durch ACL blockiert werden)
- Ping und Ping (jeder ICMP-Nachrichtentyp kann nicht auf Ping beschränkt werden)
- DNS-Auflösung zulassen (eingehend)
- IP-Telefonverbindung zum CallManager und umgekehrt (beliebige Richtung)
- IP-Telefonverbindungen zum TFTP-Server (CallManager verwendet nach der ersten TFTP-Verbindung zum UDP-Port 69 einen dynamischen Port) (Ausgehend)
- IP-Telefon 7920 mit IP-Telefon kommunizieren (in alle Richtungen)
- Deaktivieren Sie das Web- oder Telefonverzeichnis des IP-Telefons (ausgehend). Dies erfolgt über eine implizite "deny any any" ACL-Leitung am Ende der ACL.Dies ermöglicht die Sprachkommunikation zwischen IP-Telefonen sowie normale Boot-Vorgänge zwischen IP-Telefon und CallManager.

Um diese Sicherheitsanforderungen zu konfigurieren, muss die ACL über Leitungen verfügen, die Folgendes ermöglichen:

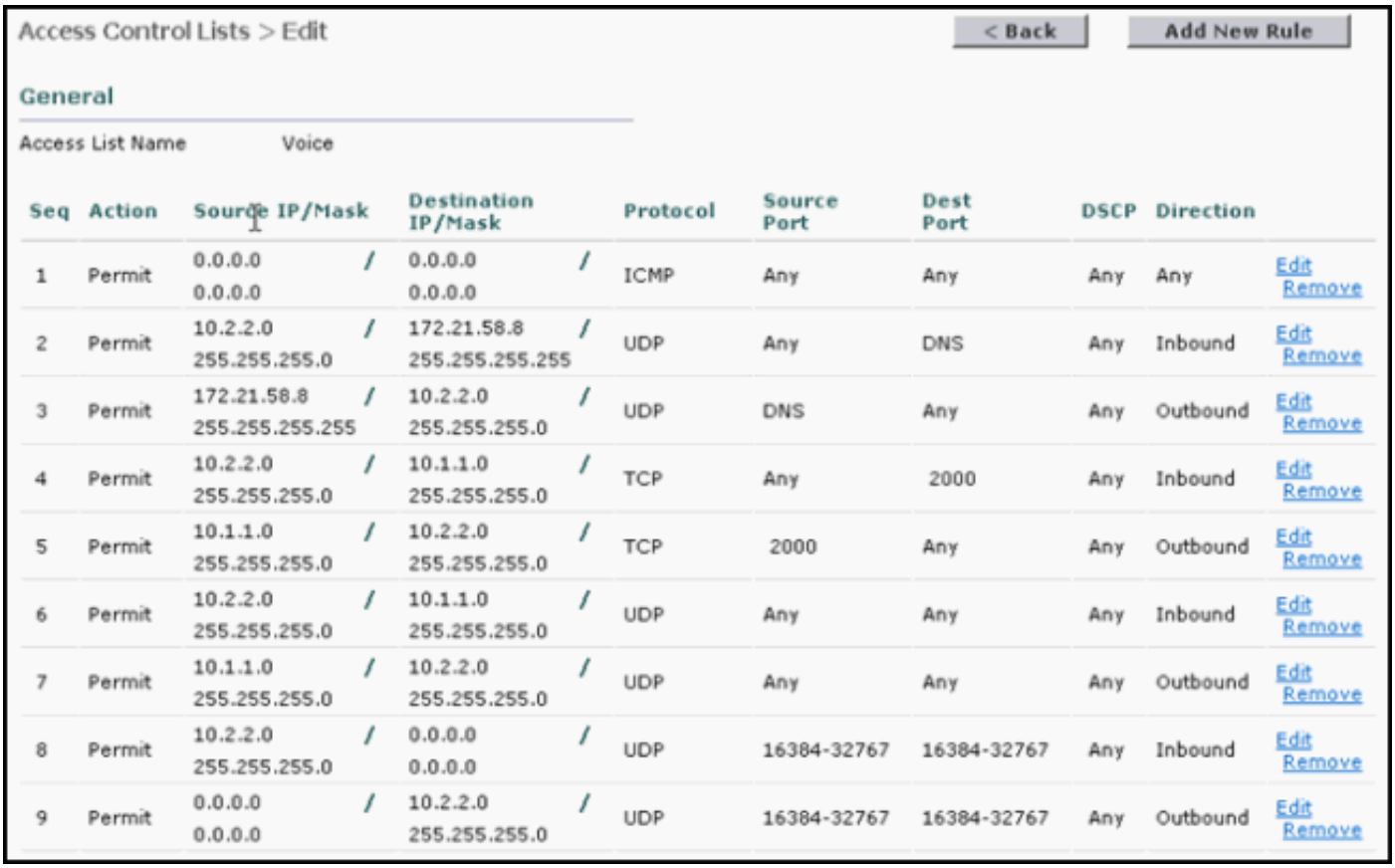
- Beliebige ICMP-Nachricht (kann nicht auf Ping beschränkt werden) (beliebige Richtung)
- IP-Telefon zum DNS-Server (UDP-Port 53) (eingehend)
- DNS-Server an IP-Telefone (UDP-Port 53) (Ausgehend)
- TCP-Ports des IP-Telefons zum CallManager-TCP-Port 2000 (Standard-Port) (eingehend)
- TCP-Port 2000 vom CallManager zu den IP-Telefonen (ausgehend)
- UDP-Port vom IP-Telefon zum TFTP-Server. Dies kann nicht auf den Standard-TFTP-Port (69) beschränkt werden, da der CallManager nach der ersten Verbindungsanforderung für die Datenübertragung einen dynamischen Port verwendet.
- UDP-Port für Audiodatenverkehr RTP zwischen IP-Telefonen (UDP-Ports 16384-32767) (beliebige Richtung)

In diesem Beispiel lautet das Subnetz des IP-Telefons 7920 10.2.2.0/24, und das des CallManager-Subnetzes ist 10.1.1.0/24. Der DNS-Server ist 172.21.58.8. Dies ist die Ausgabe des Befehls **show acl detail Voice**:

```
Seq Direction Source IP/Mask          Dest IP/Mask           Protocol Src Port  Dest Port  DSCP
```

```
Action
--- --------- --------------         --------------         -------- --------  ---------  ----
------
1     Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0            1     0-65535   0-65535    Any
Permit
2     In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53      Any
Permit
3     Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535    Any
Permit
4     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     6     0-65535   2000-2000  Any
Permit
5     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     6     2000-2000 0-65535    Any
Permit
6     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
7     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
8     In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0            17 16384-32767 16384-32767 Any
Permit
9     Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0     17 16384-32767 16384-32767 Any
Permit
```

So sieht es in der GUI aus:



Anhang: 7920 IP-Telefon-Ports

Nachfolgend finden Sie eine zusammenfassende Beschreibung der Ports, die das IP-Telefon 7920 für die Kommunikation mit dem Cisco CallManager (CCM) und anderen IP-Telefonen verwendet:

- Phone to CCM [TFTP] (UDP-Port 69 wird zuerst zum dynamischen Port [Ephemeral] für die Datenübertragung geändert) - Trivial File Transfer Protocol (TFTP) wird zum Herunterladen von Firmware- und Konfigurationsdateien verwendet.

- Phone to CCM [Web Services, Directory] (TCP-Port 80): Telefon-URLs für XML-Anwendungen, Authentifizierung, Verzeichnisse, Services usw. Diese Ports können pro Service konfiguriert werden.
- Telefon an CCM [Voice Signaling] (TCP port 2000) - Skinny Client Control Protocol (SCCP). Dieser Port kann konfiguriert werden.
- Telefon an CCM [Secure Voice Signaling] (TCP-Port 2443) - Secure Skinny Client Control Protocol (SCCPS)
- Von Telefon zu CAPF [Zertifikate] (TCP-Port 3804) - CAPF-Überwachungsport (Certificate Authority Proxy Function) für die Ausgabe von LSCs (Locally Significant Certificates) an IP-Telefone.
- Voice Bearer to/from Phone [Phone Calls] (UDP ports 16384 - 32768) - Real-Time Protocol (RTP), Secure Real Time Protocol (SRTP).**Hinweis:** CCM verwendet nur die UDP-Ports 24576-32768, andere Geräte können jedoch den gesamten Bereich nutzen.
- IP Phone to DNS Server [DNS] (UDP port 53) (IP-Telefon an DNS-Server [DNS] (UDP-Port 53)): Die Telefone verwenden DNS zum Auflösen des Hostnamens von TFTP-Servern, CallManagers und Webserver-Hostnamen, wenn das System für die Verwendung von Namen anstelle von IP-Adressen konfiguriert ist.
- IP Phone to DHCP server [DHCP] (IP-Telefon zu DHCP-Server [DHCP] [UDP-Port 67 [Client] & 68 [Server]): Das Telefon verwendet DHCP, um eine IP-Adresse abzurufen, wenn es nicht statisch konfiguriert ist.

Die Ports, mit denen der CallManager 5.0 kommuniziert, finden Sie unter Cisco Unified CallManager 5.0 TCP und UDP Port Usage. Es verfügt außerdem über die spezifischen Ports, die es für die Kommunikation mit dem IP-Telefon 7920 verwendet.

Die Ports, mit denen der CallManager 4.1 kommuniziert, finden Sie unter Cisco Unified CallManager 4.1 TCP und UDP Port Usage. Es verfügt außerdem über die spezifischen Ports, die es für die Kommunikation mit dem IP-Telefon 7920 verwendet.

Zugehörige Informationen

- Konfigurationsbeispiel für ACLs auf Wireless LAN-Controllern
- Cisco Wireless LAN Controller Configuration Guide, Release 4.0
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.