ACL Best Practices für einen Router der Serie RV34x

Ziel

In diesem Artikel werden Best Practices für die Erstellung von Zugriffskontrolllisten (ACLs) mit dem Router der Serie RV34x beschrieben.

Unterstützte Geräte | Firmware-Version

- RV340 | 1.0.03.20 (zuletzt herunterladen)
- RV340 W | 1.0.03.20 (zuletzt herunterladen)
- RV345 | 1.0.03.20 (zuletzt herunterladen)
- RV345P | 1.0.03.20 (zuletzt herunterladen)

Einführung

Möchten Sie Ihr Netzwerk besser kontrollieren? Möchten Sie zusätzliche Schritte unternehmen, um die Sicherheit Ihres Netzwerks zu gewährleisten? In diesem Fall ist eine Zugriffssteuerungsliste (ACL) genau das, was Sie benötigen.

Eine ACL besteht aus einem oder mehreren ACEs (Access Control Entries), die gemeinsam das Netzwerkverkehrsprofil definieren. Auf dieses Profil kann dann durch Cisco Softwarefunktionen wie Filterung des Datenverkehrs, Priorität oder benutzerdefinierte Warteschlangenverwaltung verwiesen werden. Jede ACL enthält ein Aktionselement (Zulassen oder Verweigern) und ein Filterelement, das auf Kriterien wie Quelladresse, Zieladresse, Protokoll und protokollspezifische Parameter basiert.

Auf Basis der von Ihnen eingegebenen Kriterien können Sie bestimmten Datenverkehr vom Ein- und/oder Verlassen eines Netzwerks steuern. Wenn ein Router ein Paket empfängt, prüft er das Paket, um anhand der Zugriffsliste zu bestimmen, ob das Paket weitergeleitet oder verworfen werden soll.

Die Implementierung dieser Sicherheitsstufe basiert auf verschiedenen Anwendungsfällen, wobei spezielle Netzwerkszenarien und Sicherheitsanforderungen berücksichtigt werden.

Beachten Sie, dass der Router automatisch eine Zugriffsliste erstellen kann, die auf Konfigurationen Ihres Routers basiert. In diesem Fall werden möglicherweise Zugriffslisten angezeigt, die Sie nur löschen können, wenn Sie die Router-Konfigurationen ändern.

Warum Zugriffslisten verwenden?

- In den meisten Fällen verwenden wir ACLs, um eine grundlegende Sicherheitsstufe für

den Zugriff auf unser Netzwerk bereitzustellen. Wenn Sie beispielsweise keine ACLs konfigurieren, können standardmäßig alle Pakete, die den Router durchlaufen, in alle Teile unseres Netzwerks geleitet werden.
- ACLs können einen Host, einen Bereich von IP-Adressen oder Netzwerken zulassen und verhindern, dass ein anderer Host, eine Reihe von IP-Adressen oder Netzwerke auf denselben Bereich (Host oder Netzwerk) zugreifen.
- Mithilfe von ACLs können Sie festlegen, welche Arten von Datenverkehr an den Router-Schnittstellen weitergeleitet oder blockiert werden sollen. Sie können beispielsweise Secure Shell (SSH) File Transfer Protocol (SFTP)-Datenverkehr zulassen und gleichzeitig den gesamten SIP-Datenverkehr (Session Initiation Protocol) blockieren.

Verwendung von Zugriffslisten

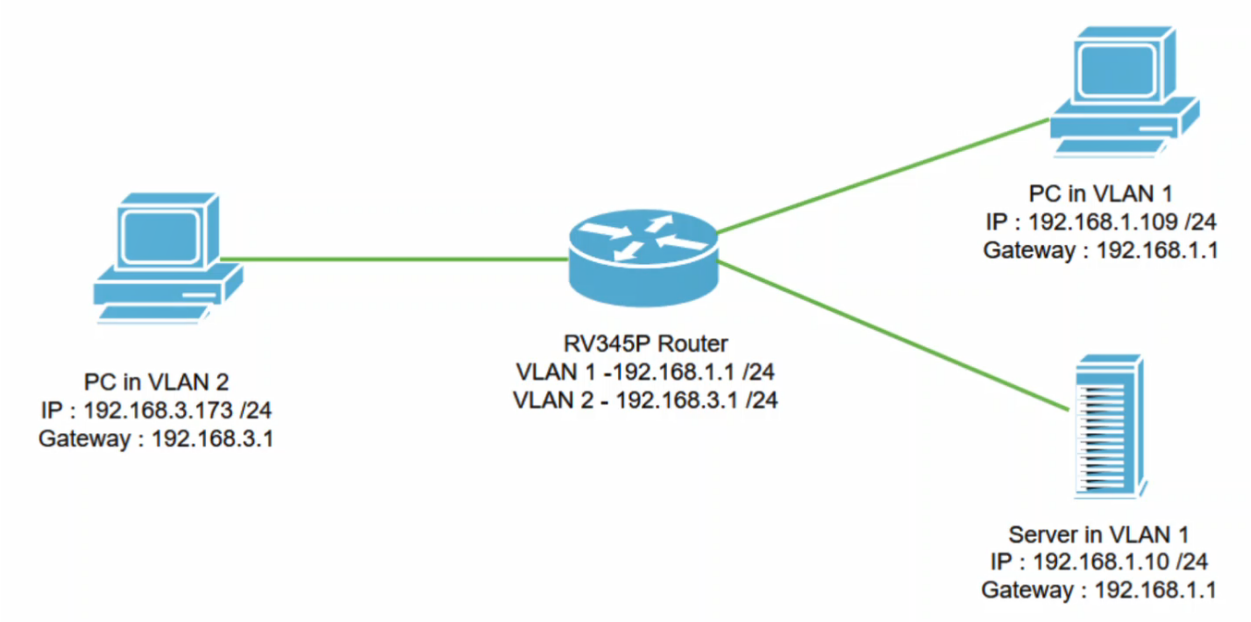
- Sie sollten ACLs in Routern konfigurieren, die zwischen unserem internen Netzwerk und einem externen Netzwerk wie dem Internet positioniert sind.
- Sie können mithilfe von ACLs den ein- und ausgehenden Datenverkehr eines bestimmten Teils unseres internen Netzwerks steuern.
- Wenn Sie eingehenden oder ausgehenden Datenverkehr oder beides auf einer Schnittstelle filtern müssen.
- Sie sollten ACLs für jedes Protokoll definieren, um den Datenverkehr zu steuern.

Best Practices für die Konfiguration grundlegender Sicherheit mit Zugriffslisten

- Implementieren Sie ACLs, die nur Protokolle, Ports und IP-Adressen zulassen, die alles andere verbieten.
- Blockieren eingehender Pakete, die angeblich dieselbe Ziel- und Quelladresse haben (Landangriff auf den Router selbst).
- Aktivieren Sie die Protokollierungsfunktion von ACLs auf einem internen (vertrauenswürdigen) Syslog-Host.
- Wenn Sie SNMP (Simple Network Management Protocol) auf dem Router verwenden, müssen Sie die SNMP-ACL und einen komplexen SNMP Community String konfigurieren.
- Lassen Sie zu, dass nur interne Adressen von den internen Schnittstellen auf den Router zugreifen und nur Datenverkehr, der für interne Adressen bestimmt ist, von außen in den Router geleitet werden darf (externe Schnittstellen).
- Blockieren Sie Multicast, falls nicht verwendet.
- Sperren einiger ICMP-Meldungstypen (Internet Control Message Protocol) (Umleitung, Echo).
- Berücksichtigen Sie immer die Reihenfolge, in der Sie die Zugriffskontrolllisten eingeben. Wenn der Router beispielsweise entscheidet, ob ein Paket weitergeleitet oder blockiert werden soll, testet er das Paket für jede ACL-Anweisung in der Reihenfolge, in der die ACLs erstellt wurden.

Implementierung von Zugriffslisten in Cisco Routern der Serie RV34x

Beispiel für eine Netzwerktopologie



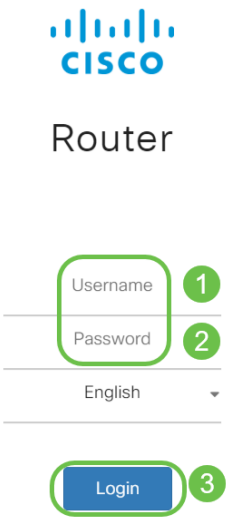
Beispielszenario

In diesem Szenario replizieren wir dieses Netzwerkdiagramm, in dem ein RV345P-Router und zwei verschiedene VLAN-Schnittstellen vorhanden sind. Wir haben einen PC in VLAN 1 und in VLAN2 und einen Server in VLAN 1. VLAN-übergreifendes Routing ist aktiviert, sodass VLAN 1- und VLAN 2-Benutzer miteinander kommunizieren können. Jetzt wenden wir die Zugriffsregel an, um die Kommunikation zwischen dem VLAN 2-Benutzer zu diesem Server in VLAN 1 zu beschränken.

Beispielkonfiguration

Schritt 1

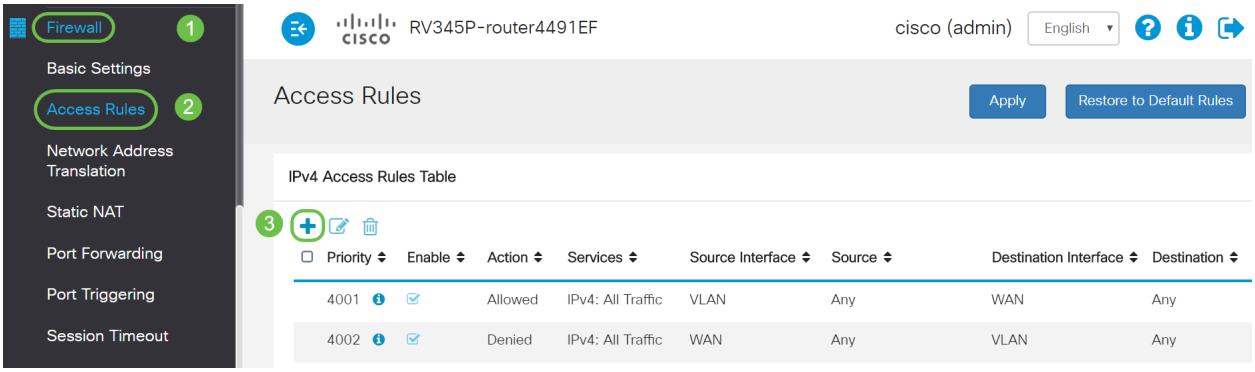
Melden Sie sich mit den von Ihnen konfigurierten Anmeldeinformationen bei der Webbenutzeroberfläche (UI) des Routers an.



Schritt 2

Um die ACL zu konfigurieren, navigieren Sie zu **Firewall > Access Rules** (Firewall > Zugriffsregeln), und klicken Sie auf das **Pluszeichen**, um eine neue Regel

hinzuzufügen.



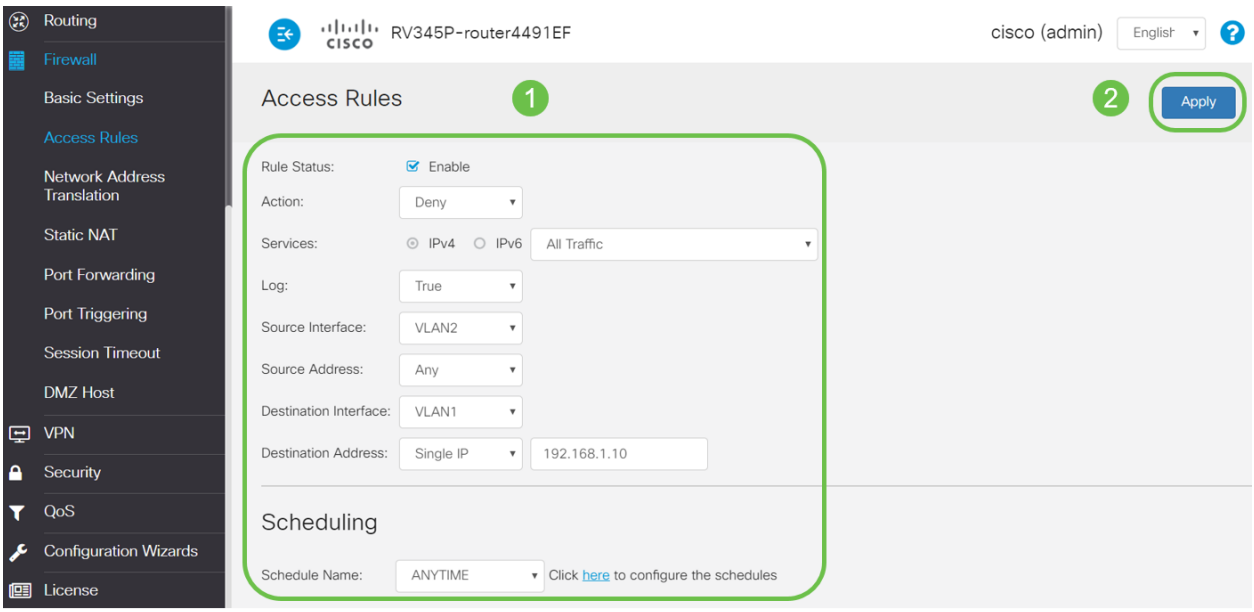
Schritt 3

Konfigurieren Sie die Parameter *für Zugriffsregeln*. ACL anwenden, um den Server einzuschränken (IPv4: 192.168.1.10/24) Zugriff von VLAN2-Benutzern. Für dieses Szenario sind folgende Parameter erforderlich:

- *Regelstatus: Aktivieren*
- *Aktion: Ablehnen*
- *Services: Gesamter Datenverkehr*
- *Protokoll: Richtig*
- *Quellschnittstelle: VLAN2*
- *Quelladresse: Beliebig*
- *Zielschnittstelle: VLAN1*
- *Zieladresse: Eine IP-Adresse 192.168.1.10*
- *Name des Zeitplans: Jederzeit*

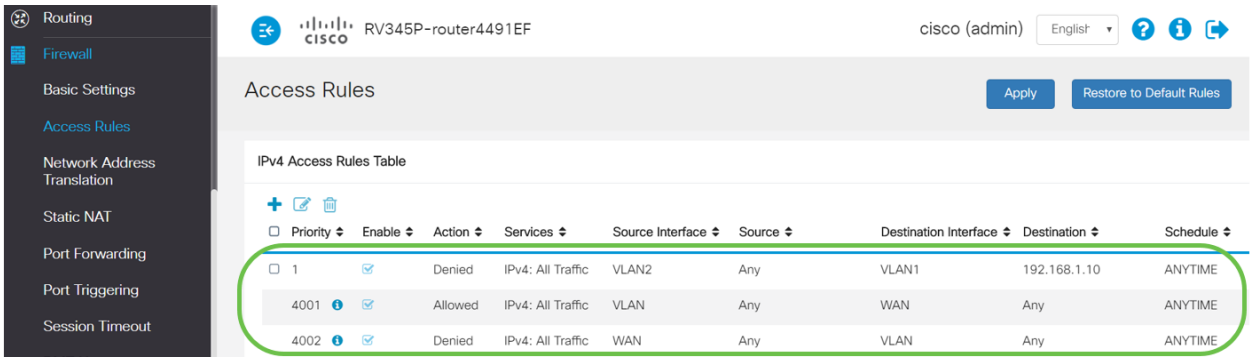
Klicken Sie auf **Apply** (Anwenden).

In diesem Beispiel haben wir den Zugriff von allen Geräten vom VLAN2 auf den Server verweigert und dann den Zugriff auf die anderen Geräte in VLAN1 zugelassen. Ihre Anforderungen können variieren.



Schritt 4

Die Liste der *Zugriffsregeln* wird wie folgt angezeigt:



Überprüfung

Öffnen Sie zum Überprüfen des Dienstes die Eingabeaufforderung. Auf Windows-Plattformen können Sie dies erreichen, indem Sie auf die Windows-Schaltfläche klicken und anschließend **cmd** im unteren linken Suchfeld des Computers eingeben und im Menü die **Eingabeaufforderung** auswählen.

Geben Sie die folgenden Befehle ein:

- Pingen Sie auf dem PC (192.168.3.173) in VLAN2 den Server (IP: 192.168.1.10). Sie erhalten eine *Timeout*-Benachrichtigung für *Anfragen*, was bedeutet, dass eine Kommunikation nicht zulässig ist.
- Pingen Sie auf PC (192.168.3.173) in VLAN2 den anderen PC (192.168.1.109) in VLAN1. Sie erhalten eine erfolgreiche Antwort.

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
```

Fazit

Sie haben die notwendigen Schritte zur Konfiguration der Zugriffsregel auf einem Router der Cisco Serie RV34x gesehen. Sie können diese nun anwenden, um eine Zugriffsregel für Ihr Netzwerk zu erstellen, die Ihren Anforderungen entspricht.