Arbeit - Köppen

Was ist eine ACL?

Eine ACL (Access Control List) ist eine Liste von Regeln, die verwendet wird, um Datenverkehr in einem Netzwerk zu filtern und zu steuern.
ACLs sind ein wichtiger Bestandteil der Netzwerksicherheit und werden verwendet, um den Zugriff auf Netzwerkressourcen, wie z.B. Router, Switche und Server, zu kontrollieren.

Eine ACL besteht aus einer Reihe von Einträgen, die eine Kombination aus Bedingungen und Aktionen enthalten.
Die Bedingungen definieren, welcher Datenverkehr durch die ACL gefiltert wird und können auf Basis von Quell- und Ziel-IP-Adressen, Protokolltypen und Portnummern definiert werden.
Die Aktionen legen fest, ob der Datenverkehr durchgelassen oder blockiert wird.

ACLs können auf verschiedenen Ebenden im Netzwerk angewendet werden, z.B. auf einem Router, um den Datenverkehr zwischen verschiedenen Subnetzen zu steuern oder auf einem Switch, um den Zugriff auf bestimmte Netzwerkressourcen zu beschränken.

Die Funktionsweise von ACLs besteht darin, dass sie den Datenverkehr filtern, indem sie jedes Datenpaket, das durch das Netzwerk fließt, mit den Einträgen in der ACL zu vergleichen.
Wenn das Datenpaket den Bedingungen eines Eintrags in der ACL entspricht, wird die zugehörige Aktion ausgeführt, z.B. das Blockieren des Datenverkehrs oder das Weiterleiten an das Ziel.

ACLs können verwendet werden, um die Netzwerksicherheit zu verbessern, indem sie unerwünschten Datenverkehr blockieren oder den Zugriff auf bestimmte Ressourcen beschränken. Sie können auch verwendet werden, um den Netzwerkverkehr zu priorisieren, z.B. indem sie den Datenverkehr von bestimmten Anwendungen priorisieren oder die Bandbreite für bestimmte Nutzer oder Gruppen begrenzen.

ACL's auf einem Routerinterface sind nur eine Möglichkeit, um Firewalls zu implementieren.
Andere Möglichkeiten:

- Dedizierte Firewall als eigenes Gerät
  Um die Performance zu verbessern, ist es ratsam, eine Firewall als eigenes Gerät zu nutzen, damit ein Router beispielsweise nicht total ausgelastet ist und das ganze Netzwerk langsamer wird.

- Personal Firewall auf einem Endgerät
  Bei Windows wird standardmäßig schon eine Firewall mitgeliefert um bestimmte Dienste zu blockieren und die Sicherheit auf dem Gerät zu verbessern.

> In der Regel ist alles verboten, was nicht benötigt wird, wenn man jetzt bestimmte Software installiert, wird manchmal gefragt, ob die Firewall von Windows umgestellt werden.

Die drei P's:

Pro Protokoll (IPv4, IPv6)
Pro Schnittstelle (fa x|y)
Pro Richtung (ingoing | outgoing)

Pro Interface können 4 ACL's angelegt werden:

- IPv4 on fa 0/1 ingoing
- IPv4 on fa 0/1 outgoing
- IPv6 on fa 0/1 ingoing
- IPv6 on fa 0/1 outgoing

Blacklist vs Whitelist:

Eine Black- und White-list ist eine Art und Weise eine Firewall/Regelwerk zu implementieren.

Blacklist = Ausdrückliches Verbieten
Whitelist = Ausdrückliches Erlauben

Nachteil an einer Blacklist ist, wenn eine Regel vergessen wird, wird eine Sicherheitslücke geschaffen.
Bei einer Whitelist ist das ganze nicht so schlimm, da der Dienst/Netzwerk einfach nicht erreichbar ist.

Unterschied zwischen einer Standard-ACL und einer erweiterten ACL:

1. **Regelumfang:**
   - **Standard-ACLs:**
     Diese ACLs basieren hauptsächlich auf der Quell-IP-Adresse des Datenverkehrs. Sie enthalten Regeln, die den Zugriff basierend auf der IP-Adresse des Absenders einschränken.
   - **Erweiterte ACLs:**
     Im Gegensatz dazu berücksichtigen erweiterte ACLs eine breitere Palette von Kriterien. Sie können den Zugriff basierend auf Quell- und Ziel-IP-Adressen, Protokolltypen, Portnummern und anderen Faktoren regeln. Dies ermöglicht eine genauere Kontrolle über den Datenverkehr.
2. **Flexibilität:**
   - **Standard-ACLs:**
     Sie sind weniger flexibel, da sie hauptsächlich auf der Quell-IP-Adresse basieren. Dies macht sie geeignet, wenn Sie den Zugriff auf Ressourcen nur anhand der Herkunft des Datenverkehrs beschränken müssen.
   - **Erweiterte ACLs:**
     Aufgrund ihrer Vielseitigkeit bieten erweiterte ACLs eine umfassendere Kontrolle über den Datenverkehr. Sie eignen sich besser für komplexe Netzwerkanforderungen, bei denen Sie den Zugriff basierend auf verschiedenen Parametern einschränken müssen.
3. **Anwendungsgebiete:**
   - **Standard-ACLs:**
     Werden häufig in einfachen Netzwerkkonfigurationen verwendet, bei denen die Kontrolle des Zugriffs auf Basis der Quell-IP-Adresse ausreichend ist.
   - **Erweiterte ACLs:**
     Finden Anwendung in komplexeren Netzwerken, in denen eine feinere Steuerung des Datenverkehrs erforderlich ist. Dies kann beispielsweise die Beschränkung des Zugriffs auf bestimmte Dienste, Protokolle oder Anwendungen umfassen.
4. **Nummerierung:**
   - **Standard-ACLs:**
     Werden normalerweise mit niedrigeren Zahlen (1-99) nummeriert.
   - **Erweiterte ACLs:**
     Werden normalerweise mit höheren Zahlen (100-199, 2000-2699) nummeriert.

Insgesamt bieten erweiterte ACLs mehr Funktionalität und Flexibilität, während Standard-ACLs einfacher sind und in weniger komplexen Umgebungen ausreichend sein können. Die Auswahl hängt von den spezifischen Anforderungen des Netzwerks und der gewünschten Kontrolle ab.

Blockieren von Geräten:

Um ein einzelnes Gerät zu blockieren beispielsweise das Gerät "192.168.1.1" wird der folgender Befehl genutzt:

`access-list 101 deny ip 192.168.1.1 any`

Filtern von Paketen:

Um eine ACL zu konfigurieren, um den TCP-Datenverkehr vom Subnetz 192.168.1.0/24 zum Host 192.168.2.1 auf Port 80 zuzulassen:

Router(config)# `access-list 101 deny ip any any`

Router(config)# `access-list 101 permit tcp host 192.168.1.0 0.0.0.255 host 192.168.2.1 eq 80`

- `access-list 101`: Erstellt eine erweiterte ACL mit der Nummer 101. Sie können je nach Bedarf eine andere Nummer verwenden, solange sie innerhalb des Bereichs für erweiterte ACLs liegt (100-199, 2000-2699).
- `permit tcp`: Erlaubt den TCP-Verkehr durch die ACL.
- `192.168.1.0 0.0.0.255`: Gibt das Quellsubnetz an, von dem der Datenverkehr kommen soll. Das Subnetz 192.168.1.0/24 wird hier dargestellt.
- `host 192.168.2.1`: Gibt das Zielhost an, zu dem der Datenverkehr gehen soll. In diesem Fall ist es der Host mit der IP-Adresse 192.168.2.1.
- `eq 80`: Beschränkt den Datenverkehr auf den TCP-Port 80, was dem Standard-HTTP-Port entspricht.

Nachdem Sie diese ACL erstellt haben, müssen Sie sie auf der Schnittstelle anwenden, die den Verkehr überwachen soll. Angenommen, die ACL sollte auf der Eintrittsschnittstelle für das Subnetz 192.168.1.0/24 angewendet werden, lautet der Befehl:

Router(config)# `interface <Schnittstellen-Typ> <Schnittstellen-Nummer>`
Router(config-if)# `ip access-group 101 in`

Durch diesen Befehl wird die ACL auf der eingehenden Seite der Schnittstelle angewendet, um den Datenverkehr gemäß den in der ACL definierten Regeln zu steuern. Bitte passen Sie die Befehle entsprechend Ihrem Netzwerkszenario und dem verwendeten Gerät an.

ACL löschen:

Um eine Access Control List (ACL) mit der Nummer 102 von einem Cisco-Router zu entfernen, müssen Sie den folgenden Befehl verwenden:

Router(config)# `no access-list 102`

Wenn Sie nur eine bestimmte Regel aus der ACL entfernen möchten, können Sie dies durch den Befehl "no" gefolgt von der spezifischen Regel erreichen. Zum Beispiel, wenn Sie die erste Regel in der ACL 102 entfernen möchten, können Sie den folgenden Befehl verwenden:

Router(config)# `no access-list 102 10`

Hier steht "10" für die Nummer der ersten Regel in der ACL 102. Beachten Sie, dass die genaue Syntax von Cisco IOS je nach der Version und Plattform des Routers variieren kann. Es ist immer ratsam, die Dokumentation für Ihre spezifische Router-Version zu überprüfen.

ACL bauen um Geräte pingen zu lassen:

Um das Pingen von Gerät A zu Gerät B zu ermöglichen, müssen Sie sicherstellen, dass ICMP (Internet Control Message Protocol) erlaubt ist. Ping verwendet ICMP, um Echo-Anforderungen und Antworten zu senden.

Router(config)# `access-list 101 permit icmp host 192.168.1.1 host 192.168.1.2 echo`

oder für das ganze Netzwerk

Router(config)# **`access-list 101 permit icmp host 192.168.1.1 host 192.168.1.0 0.0.0.255 echo`**

Stateful und Stateless Firewall:

"Stateful" und "stateless" beziehen sich auf unterschiedliche Arten von Firewalls oder Zugriffskontrollmechanismen, insbesondere auf Access Control Lists (ACLs). Hier sind die Hauptunterschiede zwischen stateful und stateless ACLs:

1. **Stateful ACL (Zustandsbehaftete ACL):**
   - Diese ACLs berücksichtigen den Zustand (Status) des Netzwerkverkehrs. Das bedeutet, dass sie den Zustand der Verbindungen verfolgen können.

- Stateful ACLs können den Datenverkehr basierend auf dem Zustand der Verbindung zulassen oder ablehnen. Zum Beispiel können sie eingehende Pakete zulassen, die zu einer bestehenden, bereits genehmigten Verbindung gehören.
- Solche ACLs sind in der Lage, den Status von Netzwerkverbindungen zu verfolgen, was zu einer effektiveren Kontrolle des Datenverkehrs führen kann.

2. **Stateless ACL (Zustandslose ACL):**
   - Im Gegensatz dazu berücksichtigen stateless ACLs den Verbindungszustand nicht. Jedes Paket wird unabhängig behandelt, ohne Berücksichtigung von vorherigen Paketen oder Verbindungsstatus.
   - Stateless ACLs basieren typischerweise auf festgelegten Regeln, die für jedes einzelne Paket gelten. Diese Regeln können auf Grundlage von Quell- und Zieladressen, Protokolltypen, Portnummern usw. definiert sein.
   - Sie sind einfacher und schneller, da sie den Verbindungsstatus nicht verfolgen müssen. Allerdings können sie in bestimmten Szenarien weniger sicher sein, da sie keine Informationen über den Zustand von Verbindungen berücksichtigen.
3. **Einsatzgebiete:**
   - **Stateful ACLs:** Werden oft in Umgebungen eingesetzt, in denen es wichtig ist, den Zustand von Netzwerkverbindungen zu berücksichtigen, wie z. B. bei der Sicherung von Netzwerkgrenzen und der Kontrolle von eingehendem und ausgehendem Verkehr.
   - **Stateless ACLs:** Finden häufig Anwendung in einfachen Netzwerkkonfigurationen, in denen die Verfolgung des Verbindungszustands nicht erforderlich ist.

Die Wahl zwischen stateful und stateless ACLs hängt von den spezifischen Anforderungen und Sicherheitszielen einer Netzwerkkonfiguration ab. In komplexeren Umgebungen, in denen ein detailliertes Verständnis des Verbindungszustands erforderlich ist, sind stateful ACLs möglicherweise die bevorzugte Wahl. In einfacheren Szenarien können stateless ACLs ausreichend sein.

Revision #30
Created 5 December 2023 00:15:19 by Julian
Updated 8 December 2023 10:09:30 by Julian