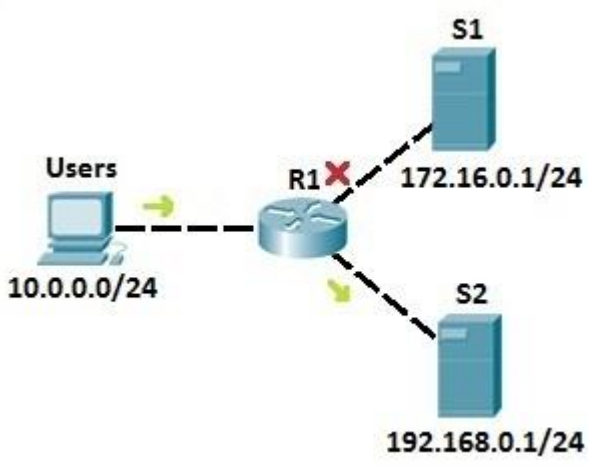
Extended Access Control List



Studiengang:	Medieninformatik WiSe15/16
Modul:	Informationssicherheit - Labor
Laborgruppe:	Gruppe Z (C)
Bericht von:	Arthur Jaks
	Tobias Winkler
	Emel Altmisoglu

Inhaltsangabe

1. Einleitung…… Seite 3
2. Versuchsaufbau…… Seite 4
3. Versuchsdurchführung…….. Seite 5
4. Versuchsergebnisse……..… Seite 7
5. Quellen…… Seite 8

Einleitung

Access control lists (ALCs) sind eine Art Filter für ein Netzwerk. Dabei werden sie von Routern und Switches benutzt um Datenfluss in ein Netzwerk oder aus einem Netzwerk an der Schnittstelle zu erlauben oder zu verbieten.
Es gibt mehrere Gründe warum ACLs eingesetzt werden, der Hauptgrund besteht darin dem Netzwerk ein Mindestmaß an Sicherheit zu gewährleisten.
ACLs sind nicht so komplex oder sicher wie Stateful Firewalls, aber sie bieten Schutz bei Hochgeschwindigkeitsschnittstellen wo die Leitungsgeschwindigkeit wichtig ist und Firewalls restriktiv sein könnten.
Wenn eine ACL an einer Schnittstelle konfiguriert ist, analysiert die Netzwerkgeräte die Daten die durch die Schnittstelle gelangen, vergleicht sie mit den festgelegten ACL Kriterien und entscheidet dann ob der Datenfluss erlaubt oder verboten wird.

In diesem Fall ist das Netzwerkgerät ein Router, der eingehenden Datenfluss analysieren und anhand der definierten Kriterien entscheidet ob der Datenfluss weiter zum Ziel geschickt wird oder nicht.

Versuchsaufbau

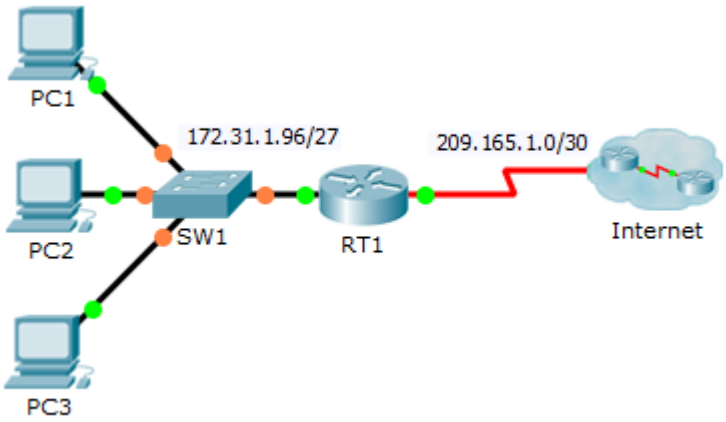


Abbildung 1 - Das fertige Netz für den Versuch

Das Netzwerk besteht aus drei PCs, dabei ist jeder der PCs mit dem Switch „SW1“ über ein Straight-Through Kabel verbunden. Der Switch selber ist dazu noch mit dem Router „RT1“, auch über ein Straight-Through Kabel, verbunden. Router „RT1“ ist mittels Serial mit dem Internet verbunden. Das Internet beinhaltet dabei die beiden Server „Server1“ und „Server2“.
Aufgabe ist nun eine extended ACL auf dem Router „RT1“ zu erstellen die den Datenfluss zwischen den PCs und den Servern regelt.

Versuchsdurchführung

Als erstes wird eine extended ACL mit dem Namen „ACL“ erstellt.
Dazu wechselt man zunächst in den privilegierten Modus mit dem Befehl **enable** und danach in den globalen Konfigurationsmodus mit dem Befehl **configure terminal**.
Zum Erstellen der extended ACL mit dem Namen „ACL“ gibt man nun folgenden Befehl ein **ip access-list extended ACL**. Somit wird die ACL erstellt und man befindet sich direkt in der erstellten ACL und kann diese nun konfigurieren.

Jetzt werden die Kriterien definiert. Im ersten Schritt soll der HTTP und HTTPs Datenfluss von PC1 (172.31.1.101) zu Server1 (64.101.255.254) und Server2 (64.103.255.254) verboten werden.

```
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

Abbildung 2 - HTTP/HTTPs verbot von PC1 zu Server1 und Server2

Wie in der Abbildung zu erkennen ist, wird mit dem Befehl **deny** der Datenfluss verboten. **TCP** ist dabei das Protokoll, **host 172.31.1.101** der PC1, **host 64.101.255.254** der Server1, **eq** steht für gleich (equal) und die Nummern definieren die Anwendung. In diesem Fall steht die **80** für den Port von HTTP und **443** für den Port von HTTPs.

Im zweiten Schritt soll der FTP Datenfluss von PC2 (172.31.1.102) zu Server1 (64.101.255.254) und Server2 (64.103.255.254) verboten werden.

```
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
```

Abbildung 3 - FTP verbot von PC2 zu Server1 und Server2

Dieser Befehl ist ähnlich wie der Befehl in Abbildung 2. Der einzige Unterschied ist die Nummer der Anwendung, in diesem Fall steht die **21** für den Port von FTP.

Im dritten Schritt soll der ICMP Datenfluss von PC3 (172.31.1.103) zu Server1 (64.101.255.254) und Server2 (64.103.255.254) verboten werden.

```
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
```

Abbildung 4 - ICMP verbot von PC3 zu Server1 und Server2

Dieser Befehl ist etwas anders als die Vorigen, denn statt dem TCP wird das **ICMP** verwendet und es wird **keine** Nummer der Anwendung definiert.

Im letzten Schritt der Kriterien werden alle anderen Datenflüsse freigegeben, denn beim Anlegen einer ACL werden standardmäßig alle Datenflüsse blockiert. Dies erreicht man wie folgt.

```
RT1(config-ext-nacl)#permit ip any any
```

Abbildung 5 - Freigabe von allen anderen Datenflüssen

Zu guter Letzt weist man die definierte ACL einer Schnittstelle des Routers zu und legt fest ob diese ACL für einkommende Datenflüsse oder ausgehende Datenflüsse bestimmt ist. Dazu muss man zunächst mit dem Befehl **exit** die Konfiguration der ACL verlassen. Danach wechselt man zu der Schnittstelle an die man die ACL verweisen will, in diesem Fall zu der GigabitEthernet 0/0 Schnittstelle, dazu führt man den Befehl **interface gigabitethernet0/0** aus. Befindet man sich jetzt auf der Schnittstelle, führt man folgenden Befehl aus **ip access-group ACL in**. Damit legt man fest das die IP ACL mit dem Namen „ACL“ für die eingehenden Datenflüsse zuständig ist, **in** steht dabei für die eingehenden und **out** wäre für ausgehende Datenflüsse.

Versuchsergebnisse

Nach erfolgreicher Durchführung diesen Versuchs ist man in der lange eine extended ACL zu erstellen und kennt die Befehle mit samt derer Bedeutung zum Erstellen der einzelnen Kriterien zum Zulassen oder blockieren des Datenflusses. Zudem ist man in der Lage die erstelle ACL einer Schnittstelle am Router zuzuweisen und dieser festzulegen ob die ACL für den einkommenden oder für den ausgehenden Datenfluss zuständig sein soll.
Zum kontrollieren seines Ergebnisses kann man sich die access-list des Routers angucken. Diese ist einsehbar wenn man sich im privilegierten Modus des Routers befindet und den Befehl **show access-list** eingibt. Danach kann man seine erstellte access-list mit der folgenden vergleichen:

```
RT1>enable
RT1#show access-list
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254
    90 permit ip any any
```

Abbildung 6 - Ergebnis der access-list

Ist die ACL aus der Abbildung exakt wie die erstelle ACL, wurde der Versuch erfolgreich durchgeführt.
Zusätzlich kann mein sein Ergebnis testen indem man die zuvor festgelegten Kriterien der ACL austestet. Zum Beispiel könnte man von PC1 versuchen den Webserver von Server1 anzusprechen, oder versuchen sich von PC2 per FTP mit dem Server2 zu verbinden.
Wenn alle definierten Kriterien das richtige Ergebnis liefern, wurde der Versuch ebenso erfolgreich abgeschlossen.

Quellenverzeichnis

ACL Wiki - 05.11.15 - https://de.wikipedia.org/wiki/Access_Control_List

ACL Wiki englisch – 05.11.15 - https://en.wikipedia.org/wiki/Access_control_list

ACL Beschreibung - 05.11.15 - http://kb.netgear.com/app/answers/detail/a_id/21708/~/what-are-access-control-lists-(acls)-and-how-do-they-work-with-my-managed

Cisco IOS Kommandos – 05.11.15 - https://www.aulis.hs-bremen.de/goto.php?target=file_568275_download