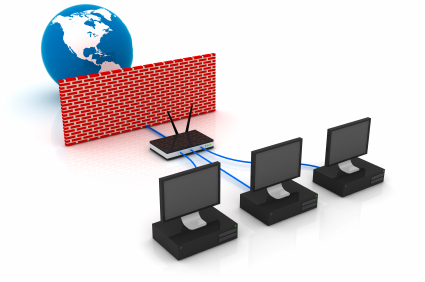
CBAC stateful inspection firewall



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. Quellenverzeichnis……………………………………………………………….. Seite 10
  6. Abbildungsverzeichnis…………………………………………………………… Seite 10

Einleitung

Wer sich mit dem Internet verbindet, geht das Risiko ein Verbindungen von Programmen oder Systemen unbemerkt zu erlauben. Daher werden verschiedenste Sicherheitsvorkehrungen getroffen, welche jeden Nutzer schützen können. Eines davon ist die Firewall. Eine Firewall ist wie eine „Mauer“ zwischen einem Netz und dem Internet. Sie kontrolliert den ein- und ausgehenden Datenfluss. Heut zu Tage ist die Firewall im Router integriert und voreingestellt, welche aber nach persönlichem Nutzen auch umkonfiguriert werden kann. Eine externe Komponente kann auch als Firewall genutzt werden.

Bestandteile einer Firewall sind:

• Paketfilter mit Port- und Protokoll-Filter

• Network Adress Translation (NAT)

• Stateful Inspection

Eine einfache Firewall benutzt einen Paketfilter und prüft nur die Header der Datenpakete.

Dies kann jedoch zu Sicherheitslücken führen, da ein Hacker nur die Header Datei lesen

und ummodifizieren muss, da ein erlaubter Dienst jederzeit eine Antwort zusenden darf,

auch wenn keine Anfrage gestellt wurde. Stateful Inspection hingegen bietet mehr Sicherheit, da hier auch die IP Adresse sowie der Port gemerkt wird und das Paket nicht nur bis zu 4. Schicht ( Transport Schicht) geschickt werden, sondern auch bis zur Applikations Schicht, falls das Packet eine Verbindung aufbauen muss.

Es gibt zwei Arten, wie die Regeln einer Firewall eingestellt werden können:

* Alles erlauben - einzelne Bekannte/Sichere Vorgänge verbieten
  + Diese Methode ist am einfachsten, jedoch ist dieser Weg nur solange sicher, wie alle Gefahren bekannt sind und gesperrt werden.
* Alles sperren - einzelne gewünschte Vorgänge erlauben
  + Diese Methode ist die sicherere, da auch unbekannte Gefahren direkt gesperrt sind. Jedoch bedarf dies Methode mehr Konfigurationszeit, da zunächst alles gewünschte erlaubt werden muss.

Versuchsaufbau

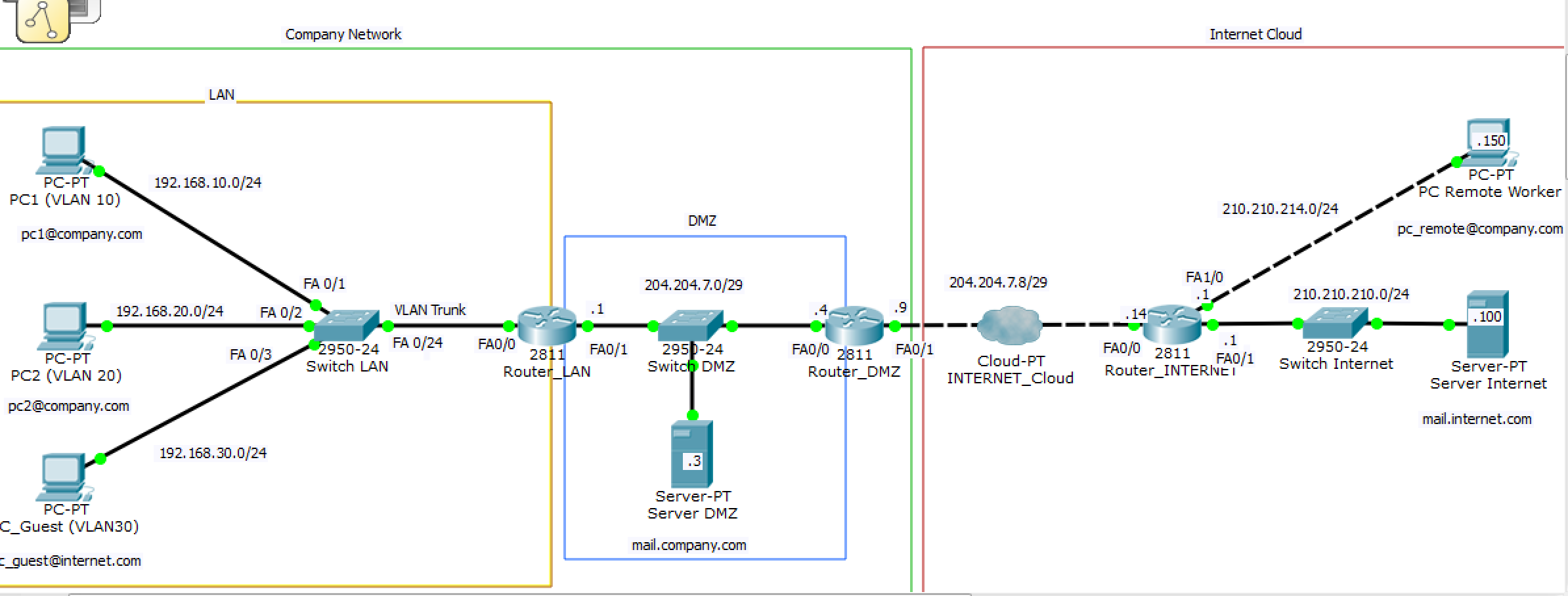
Für den Versuchsaufbau wird ein Netzwerk und eine bestehende Internet Verbindung benötigt.

Abb. 2: Fertiges Netzwerk zur Konfiguration einer Firewall

In diesem Beispiel ist das Netz wie folgt in 3 Bereiche aufgebaut:

LAN, DMZ und Internet Cloud.

Das LAN-Netzwerk ist wie folgt von links nach rechts aufgebaut:

PC1, PC2 so wie PC3 sind via Straight-Through-Kabel mit dem LAN - Switch verbunden.

PC1 hängt an Switch Interface FA 0/1, PC2 an Switch Interface FA 0/2 und PC3 an Switch

Interface FA 0/3.

PC1 gehört zu VLAN 10 mit dem Netzbereich 192.168.10.0 bis 192.168.10.255/24.

PC2 gehört zu VLAN 20 mit dem Netzbereich 192.168.20.0 bis 192.168.20.255/24.

PC3 gehört zu VLAN 30 mit dem Netzbereich 192.168.30.0 bis 192.168.30.255/24.

Vom Interface FA 0/24 ist der Switch via Straight-Through-Kabel an das LAN - Router Interface FA 0/0 angeschlossen. Diese Verbindung ist zeitgleich der VLAN Trunk.

Es folgt der DMZ-Bereich welcher aus drei weiteren Elementen besteht:

Dem DMZ – Switch, DMZ – Server und DMZ – Router.

Der DMZ – Bereich regelt zum einen den Zugriff auf öffentliche Dienste und schützt zeitgleich das interne Netz vor nicht autorisiertem Zugriff von außen.

Über Interface FA 0/1 ist der Switch mit dem LAN - Router , über Interface FA 0/ 3 mit dem

DMZ - Server und über FA 0/2 mit dem DMZ - Router verbunden.

Der DMZ – Router ist außerdem noch über Interface FA 0/1 mit der Internet Cloud via

Ethernetkabel verbunden.

Versuchsdurchführung

Die Firewall wird an den Router\_DMZ konfiguriert, da dieser die Verbindung zum Internet hat. Zunächst kann überprüft werden, ob PC1 Verbindungen zum Internet, z.B Webseiten aufrufe, Ping oder Telnet, aufbauen kann, um diese nach der Firewall Konfiguration vergleichen zu können.

Andersherum kann über den PC Remote Worker Verbindungen zum Router\_DMZ überprüft werden. Folgende Ergebnisse sollten vor der Konfiguration zu verzeichnen:

|  |  |  |  |
| --- | --- | --- | --- |
|  | PC1 |  | Remote Worker |
| Ping Internet Router | Ping statistics for 204.204.7.14:  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) | DMZ Server | Ping statistics for 204.204.7.9:  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) |
| Ping Internet Server | Ping statistics for 210.210.210.100:  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) | http access to the DMZ Server | accessable „Welcome to Company.com Webserver“ |
| Ping Internet Host | Ping statistics for 204.204.7.14:  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) | telnet and ssh to the DMZ Router | accessable, accessable |
| http access to the internet server | accessable „Welcome to Internet Webserver„ |  |  |
| telnet and ssh to the Internet Router | PC>telnet 204.204.7.14  Trying 204.204.7.14 ...Open  User Access Verification  Password:  Router\_INTERNET>  PC>ssh -l hsb 204.204.7.14  Open  Password:  Router\_INTERNET> |  |  |
| mail exchange with PC „Guest“ | successfull |  |  |

Abb. 3: Ergebnisse der Verbindungsüberprüfung

Da Firewall ein- als auch ausgehende Datenströme prüft, muss diese auf beiden Schnittstellen des Routers eingestellt werden. Zunächst werden die ins Internet

versendete Daten kontrolliert. Hierfür wird erst ein extended named ACL mit dem Namen “FILTER\_TRAFFIC\_TO\_INTERNET” angelegt.

>enable

#configure terminal

(config)#ip access-list extended “FILTER\_TRAFFIC\_TO\_INTERNET”

Da alles zu verbieten die sicherere Variante ist, werden zuerst alle erlaubten Verbindungen hinzugefügt und zum Schluss alles verboten, da die Firewall jede Regel der Reihe nach abarbeitet und bei gefunden Regel die restlichen Regeln nicht mehr beachtet, muss das Verbieten aller restlichen Verbindungen zum Schluss aufgelistet werden.

Erlaubt wird nun WWW, SMTP, POP3, SSH und ICMP für alle Hosts. Mit dem permit Befehl werden nun die Netzadresse mit der zugehörigen Wildcard und der jeweilige Dienst hinzugefügt.

(config-ext-nacl)#permit tcp 204.204.7.0 0.0.0.7 any eq 80 —> für WWW

(config-ext-nacl)#permit tcp 204.204.7.0 0.0.0.7 any eq 25 —> für SMPT

(config-ext-nacl)#permit tcp 204.204.7.0 0.0.0.7 any eq 110 —> für POP3

(config-ext-nacl)#permit tcp 204.204.7.0 0.0.0.7 any eq 23 —> für Telnet

(config-ext-nacl)#permit tcp 204.204.7.0 0.0.0.7 any eq 22 —> für SSH

(config-ext-nacl)#permit icmp 204.204.7.0 0.0.0.7 —> für ICMP

Des Weiteren wird dem Server\_DMZ erlaubt, Radius traffic an den Router\_DMZ zu senden.

(config-ext-nacl)#permit udp host 204.204.7.3 any eq 1645

Nun um jeglichen weiteren Traffic zu verbieten der Befehl:

(config-ext-nacl)#deny any any

(config-ext-nacl)#exit

Um statetful inspection einzurichten muss nun eine Regel angelegt werden. Es wird in die jeweilige Schnittstelle Fa0/0 gewechselt und die Regel angelegt sowie die Richtung des Datenstroms. Der Name des ACL wird zur Wiedererkennung des ACLs verwendet um die Regel an dieses zu Binden.

(config)#ip inspect name INSPECT\_TRAFFIC\_TO\_INTERNET tcp

(config)#ip inspect name INSPECT\_TRAFFIC\_TO\_INTERNET icmp

(config-if)#interface fa 0/0

(config-if)#ip access-group FILTER\_TRAFFIC\_TO\_INTERNET in

(config-if)#ip inspect INSPECT\_TRAFFIC\_TO\_INTERNET in

(config-if)#exit

Die Richtung „in“ definiert an der Schnittstelle fa0/0 die eingehenden Datenströme.

D.h. die jenigen Daten die von dem Netz an den Router weitergegeben werden.

Nun die Konfigurationen um die Datenströme aus dem Internet in das Netzt zu kontrollieren.

(config)#ip access-list extended “BLOCK\_TRAFFIC\_FROM\_INTERNET”

(config-ext-nacl)#permit tcp host 204.204.7.3 any eq 80 —> für WWW

(config-ext-nacl)#permit tcp host 204.204.7.3 any eq 25 —> für SMPT

(config-ext-nacl)#permit tcp host 204.204.7.3 any eq 110 —> für POP3

(config-ext-nacl)#permit tcp host 204.204.7.9 any eq 23 —> für Telnet

(config-ext-nacl)#permit tcp host 204.204.7.9 any eq 22 —> für SSH

(config-ext-nacl)#deny any any

(confi-ext-nack)#exit

Nun muss auch hierfür eine Regel angelegt werden und diese an der Schnittstelle fa0/1

dem ACL angebunden werden.

config)#ip inspect name INSPECT\_TRAFFIC\_FROM\_INTERNET tcp

(config-if)#interface fa 0/1

(config-if)#ip access-group BLOCK\_TRAFFIC\_FROM\_INTERNET in

(config-if)#ip inspect INSPECT\_TRAFFIC\_FROM\_INTERNET in

(config-if)#exit

Da die Schnittstelle fa0/1 an das Internet Verbunden ist, wird die Richtung „in“ verwendet, da alles was vom Internet zu dem Router reingekommt, überprüft werden muss.

Versuchsergebnisse

Quellenverzeichnis

Aulis /Informationssicherheit Laboraufgabe IS\_Activity\_Lab4\_Firewall\_20131125 22.11.2015

<http://parachutetechs.com/it-services-importance-of-firewalls/> 22.11.2015

<http://searchnetworking.techtarget.com/definition/stateful-inspection> 22.11.2015

<http://www.elektronik-kompendium.de/sites/net/0803051.htm> 22.11.2015

Abbildungsverzeichnis

Abb. 1 <http://parachutetechs.com/it-services-importance-of-firewalls/> 22.11.2015

Abb. 2 Paket Tracer Labor Aufgabe4 IS\_Activity\_Lab4\_Firewall\_20131125 22.11.2015