IT Sicherachitekturen

Einrichtung einer internen Firewall von Firma-a und Firma-b, sowie LAN-to-LAN-VPN von Firma-a (Server) nach Firma-b(Client)

Paul Drautzburg Georg Mohr

HTWG Konstanz, Sommersemester 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Motivation

Im Zeitalter der Digitalisierung steigt der Grad der Vernetzung immer weiter an. Unternehmen, welche ihre Standorte über die ganze Welt verteilt haben, wollen Wege und Möglichkeiten haben ihre Arbeit sicher und Problemlos zu verrichten. Dafür ist es unerlässlich, dass verschiedene Standorte auf Ressourcen des anderen zugreifen können. Für solche Szenarien gibt es in der Netzwerktechnik und Netzwerkarchitektur verschiedene Lösungsansätze. Jedoch darf dabei ein wichtiger Aspekt nicht vernachlässigt werden, denn jedes Unternehmen hat Betriebsmittel und Informationen, welche es nicht Gefahren von außen aussetzten will. An diesem Punkt kommt der Begriff IT-Sicherheit ins Spiel und genau dieses Umfeld um den Begriff „IT-Sicherheit“ wird im Rahmen des Praktikums zur Lehrveranstaltung „IT-Sicherheitsarchitekturen“ untersucht. In den folgenden Kapiteln wird eine Problemstellung unter Laborbedingungen skizziert, welche ein Szenario wiederspiegelt, mit dem sich Unternehmen täglich konfrontiert sehen. Anschließend wird werden die Laborbedienungen und der Versuchsaufbau beschrieben. Aus der Problemstellung und dem Versuchsaufbau wird eine Lösung auf Grundlage, der damit zu Grunde liegenden Theorie, erarbeitet. Diese Lösung wird abschließend in die Laborumgebung implementiert und auf ihre Akzeptanz gegenüber der Problemstellung untersucht und in einem Fazit bewertet.

2 Problemstellung

In diesem Kapitel wird die Laborumgebung eingeführt und beschrieben, sowie die damit verbundene Aufgaben-/Problemstellung skizziert.

2.1 Laborumgebung und Versuchsaufbau

Im Labor wird die IT-Landschaft zweier Unternehmen „A“ und „B“ simuliert. Jedes Unternehmen besitzt ein lokales LAN, an denen die pot. Mitarbeiter angeschlossen sind, zudem gibt es mehrere Server mit Hilfe derer verschiedene Dienste angeboten werden sollen. Es folgt eine Liste an Diensten welche Angeboten werden sollen: Internetzugang von den Mitarbeiter-Computern. Zugang über HTTPS der Webseiten beider Unternehmen. Eine Virtuelle Kopplung der beiden Unternehmen mit Hilfe einer sog. Site-to-Site Verbindung. Jeder Mitarbeiter der Unternehmen soll die Möglichkeit haben, E-Mails

über einen Mailsserver zu verschicken. Eine weitere wichtige Komponente in dieser IT-Landschaft sind die externen und internen Firewalls, da diese den Grundstein für eine sichere Umgebung legen. In dieser IT-Landschaft gibt es insgesamt 4 Firewalls, jedes Unternehmen hat jeweils eine interne und externe Firewall. Hinter den externen Firewalls beider Unternehmen liegt jeweils die sog. DMZ – Demilitarisierte Zone. In dieser Zone stehen üblicherweise die Unternehmensserver, diese werden nach außen hin von der externen Firewall und nach innen von der internen Firewall geschützt. Jede Firewall läuft auf einem Server, somit besteht die IT-Landschaft insgesamt aus 4 Servern auf welchen die Firewalls laufen, 2 Servern, welche die jeweiligen Unternehmensserver simulieren und einem Server welcher außerhalb der externen Firewall das Internet simulieren soll (vgl. Abb. 1).

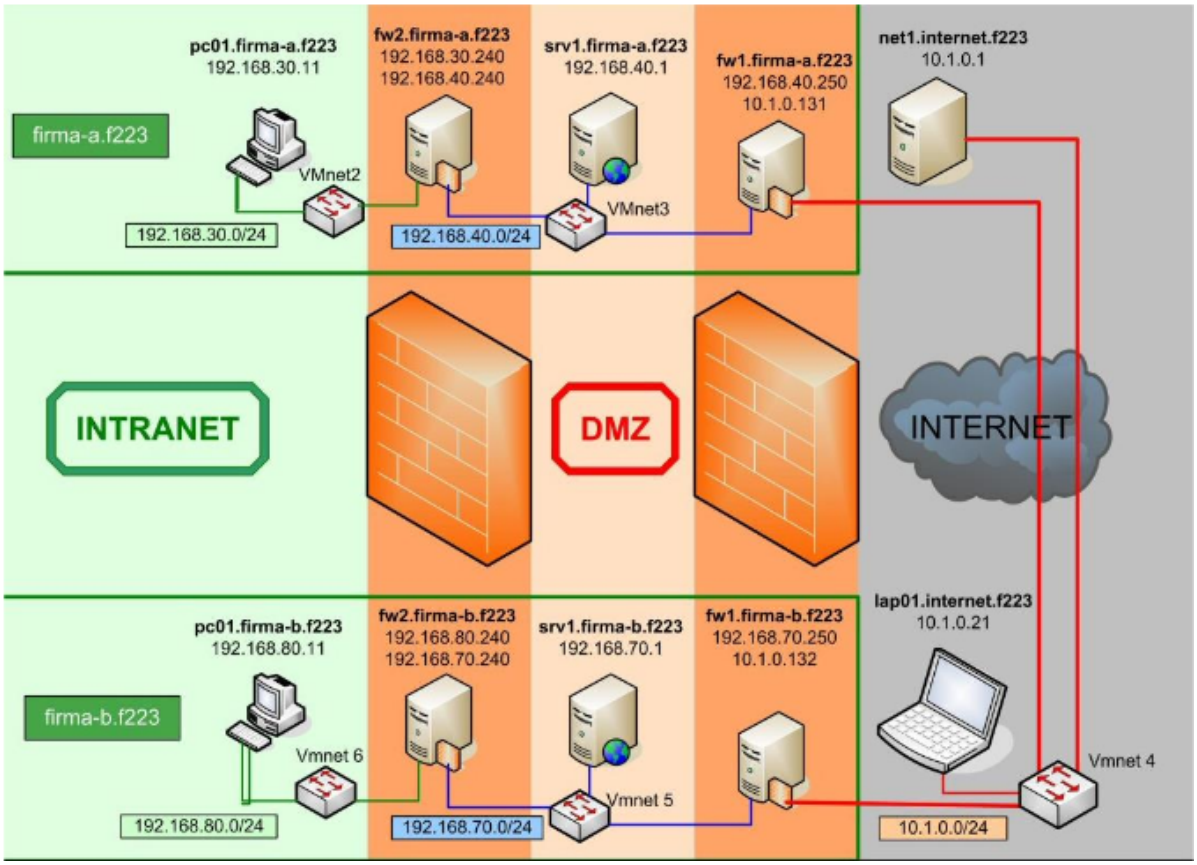

Abbildung 1: Schematischer Aufbau der Laborumgebung im IT-Sicherheitslabor [ND18]

Jede dieser angesprochenen Komponenten muss entsprechen konfiguriert werden, damit

die angesprochenen Dienste fehlerfrei funktionieren können. Technisch gesehen wird jeder dieser Server auf Grundlage einer virtuellen Maschine abgebildet. Jede dieser Maschinen hat Linux als Betriebssystem installiert und vorkonfiguriert, jedoch ohne zusätzliche Pakte, nur die reine Grundinstallation Da die Implementierung und Installation aller dieser Dienste und der damit verbundenen Komponenten den Rahmen dieses Praktikums sprengen würde, werden die Aufgabenstellungen zuvor runtergebrochen. Die detaillierte Aufgabenstellung wird im nächsten Abschnitt eingeführt.

2.2 Aufgabenstellung

Wie schon im vorhergehenden Abschnitt beschrieben, gibt es mehrere Dienste, welche in der IT-Landschaft angeboten werden sollen. In diesem Bericht, wird die Virtuelle Kopplung der Unternehmen „A“ und „B“ durch eine „Site-to-Site-“ oder auch „LAN-to-LAN-“ genannt -Verbindung implementiert. Die Problemstellung gilt als gelöst, wenn es möglich ist, dass Unternehmen A eine gesicherte Verbindung zu Unternehmen B aufbauen kann und die jeweiligen internen Firewalls entsprechend konfiguriert sind. Die Konfiguration der externen Firewalls kann in dieser Aufgabe vernachlässigt werden, hierfür sollen die bereitgestellten internen Firewalls verwendet werden. //TODO Verweis auf Bilder, Begriffe zuordnen.

3 Theoretische Grundlagen

In diesem Kapitel werden die theoretischen Grundlagen eingeführt, welche im Kontext der Aufgabestellung benötigt werden. Dies beschränkt sich auf drei Bereiche, die Netzwerkarchitekturen, Debian GNU Linux 7.11 und IP-Tables. Jede dieser genannten Bereiche wird innerhalb dieses Kapitels eingeführt und in den Aufgabenkontext eingeordnet.

3.1 Netzwerkarchitekturen

Der Bereich Netzwerkarchitekturen ist ein sehr breites Gebiet, deshalb muss zuvor anhand der Anforderungen aus der Aufgabenstellung abgegrenzt werden. Das Netzwerk des Labors besteht netzwerktechnisch grundlegend aus drei Bereichen dem Intranet, der Demilitarisierten Zone und dem Internet. Das Intranet zeichnet sich dadurch aus, dass es hinter einer internen Firewall liegt ...

3.2 Debian GNU Linux 7.11

3.3 IP-Tables

3.4 OpenVPN

4 Lösungsskizze

In diesem Kapitel wird sich mit dem Thema befasst, wie sich eine Side-to-Side VPN Verbindung, die die Firmen A und B wie in Kapitel 2.1 beschrieben verbindet. Dazu waren zu Beginn mehrere Vorüberlegungen zu tätigen. Dies sind zum einen, wie wird das innere Netz der Firmen A und B geschützt, dann welcher VPN Dienst kann für diesen Zweck verwendet werden und welche weiteren Strategien braucht es bei der Umsetzung der Security Policies der Firmen.

4.1 Firewall

Wenn eine Firewall aufgebaut werden soll, muss sich zu beginn überlegt werden, welche allgemeine Strategie mit der Firewall gefahren werden soll. Das heißt sollen alle Verbindungen Standardmäßig freigegeben werden und nur explizit nicht erlaubt Verbindungen geblockt werden (Default-Allow-Strategy), oder sollen alle Verbindungen blockiert werden und nur die die explizit erlaubt wurden, geöffnet werden (Default-Deny-Strategy). Im Standardfall wird in Unternehmen, die Strategie Default-Deny verwendet, weshalb auch im Versuchsaufbau diese Strategie gewählt wurde. Eine Firewall wird mit Hilfe des Userspace-Programmes IPTABLES (siehe Kapitel 3.3) unter Linux realisiert. Dafür wird eine Rules Datei (nachfolgend Skript genannt) angelegt, in dieser werden die Einstellungen und Regeln für die Firewall definiert. Zu Beginn des Skriptes wird der Interpreter für den Code angegeben. Dann wird begonnen die durch die Default Strategie vorgegebenen Default Policies umzusetzen (siehe Auflistung 1). Dabei sagt das -P, dass die Policy angesprochen werden soll, das INPUT, OUTPUT und FORWARD bezieht sich auf die im Kapitel 3.3 vorgestellten Chains. DROP sagt dabei aus, dass die eintreffenden Pakete, wenn keine weiteren Regeln definiert oder zutreffen nicht weitergeleitet und "fallengelassen" werden sollen.

Auflistung 1: Default Policy IPTABLE

```
#Verwenden der Tabelle FILTER
*filter
–P INPUT DROP
–P OUTPUT DROP
–P FORWARD DROP
```

Nach dem die Default Policy erfolgreich eingeführt wurde, werden die feingranulareren Regeln definiert. Dies setzt die Verwendung des Befehles -F voraus. Dieser löscht alle bisherigen Filterregeln, um die nach folgenden neu definierten Regeln einzuführen. Bei Linux ist dabei zu beachten das ein Teil der Interprozesskommunikation über das interne Netzwerk läuft. Dafür ist es nötig diese Kommunikation zuzulassen, dies geschieht wie in der nachfolgenden Auflistung 2 zusehen ist.

Auflistung 2: Interprozesskommunikation zulassen

```
# Interprozesskommunikation Verbindungen erlauben
-A INPUT -i lo -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
```

Dabei sagt das -A an welche Chain diese Regel angehängt werden soll. Das -i ist dabei die Option über welches Netzwerkinterface das Paket eingegangen ist, beziehungsweise -o für das Paket versenden. In diesem Fall das "lo" Netzwerkinterface. Wenn alle Prüfregeln auf das Paket zutreffen wird mit -j entschieden wie mit dem Paket verfahren werden soll, in diesem Beispiel soll es mit ACCEPT akzeptiet werden.

Auflistung 3: Weitere allgemeine Firewallregeln

```
# Erlaube ICMP Befehle
-A INPUT -p icmp -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT

# Erlaube SSH Verbindung
-A INPUT -p tcp --dport 22 -j ACCEPT

# Alle Verbindungen von innen nach aussen zulassen
-A FORWARD -i eth0 -o eth1 -m state --state NEW -j ACCEPT

# Erlaube nur bereits aufgebaute
# Verbindungen von aussen nach innen
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Die in Auflistung 3 dargestellten Regeln sind allgemeine Regeln für die Firewall, diese erlauben das empfangen von Pinganfragen, den Fernzugriff mittels SSH, alle neuen Verbindungen von innen nach außen und alle bereits aufgebauten Verbindungen beziehungsweiße alle Verbindungen die einen Bezug auf eine andere Verbindung besitzen. In

der nachfolgenden Tabelle 1 werden die hier verwendeten Optionen nochmals näher beschrieben. Nach den allgemeine Regeln müssen nun die VPN spezifischen Regeln definiert

Optionen	Beschreibung
-p	Gibt das Protokoll an welches verwendet werden soll hier icmp(Ping), tcp
-dport	Gibt den Destinationport an, auf den zugegriffen werden soll hier 22
eth0,eth1	bezieht sich auf das verwendete Netzwerkinterface
-m state	die entreffenden Pakete sollen auf den Status überprüft werden
–state	Status der eintreffenden Pakete, hier NEW, RELATED,ESTABLISHED

Tabelle 1: IPTABLES Optionen und Beschreibung

werden. Dazu muss man die auf den VPN Ports eintreffenden und ausgehenden Pakete betrachten. Diese Ports sind entweder 1194 oder 1195. In der Auflistung 4 sind VPN Regeln zusehen. Eine Besonderheit bei VPN ist das zum einen alle verbinungen die über das Netzwerkinterface tun0 eintreffenden Pakete ohne Überprüfung an das Inteface eth0 übergeben werden. Des weiteren wird noch die Tabelle NAT benötigt, was das "*nat" angibt. In dieser Tabelle gibt es die Chain POSTROUTING, über diese kann nachträglich der Verkehrsheader eines Paketes verändert werden. MASQUERADE hat dabei die Funktion das wenn ein Paket versendet wird die Source-IP-Adresse so verändert wird das nur noch die IP-Adresse des Firewallservers ersichtlich ist. Dies hat den Grund das von außen nicht ersichtlich wird, was sich für IP-Adressen hinter der Firewall befinden und es so Angreifern erschwert wird diese anzugreifen.

Auflistung 4: Weitere VPN Firewallregeln

```
# Erlaube alle Verbindungen auf den VPN Ports
-A INPUT -i eth1 -p udp --dport 1194 -m state --state NEW -j ACCEPT
-A INPUT -i eth1 -p udp --dport 1195 -m state --state NEW -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i tun0 -j ACCEPT

#Forwarding fuer die VPN Verbindungen
-A FORWARD -i tun0 -o eth0 -m state --state NEW -j ACCEPT
-A FORWARD -i eth0 -o tun0 -m state --state NEW -j ACCEPT
-A FORWARD -i tun0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEP
-A FORWARD -i eth0 -o tun0 -m state --state RELATED,ESTABLISHED -j ACCEP
COMMIT

#Verwenden der Tabelle NAT
*nat
```

```
#Loeschen der vorhandenen Regeln
-F

-A POSTROUTING -o eth1 -j MASQUERADE
COMMIT
```

4.2 VPN

4.2.1 Server Firma A

4.2.2 Client Firma B

5 Auswertung

6 Fazit

Literatur

[ND18] Neuschwander, Jürgen ; Düsterhöft, Sabine: *IT-Sicherheitsarchitekturen Aufgabenstellung zum Praktikum*. March 2018