

Aufgabe 8

Virtual Private Networks

Ziel dieser Aufgabe

Ziel dieser Aufgabe ist es, dass Sie eine Virtual Private Network (VPN) Lösung kennenlernen und einen VPN-Gateway einrichten, der eine sichere Verbindung mit verschlüsselter Kommunikation über IPSec zur Verfügung stellt.

Aufgabe

In der Aufgabe soll ein VPN Gateway wie im Bild 1 gezeigt auf der Basis des StrongSwan Pakets eingerichtet werden. Das Gateway soll das Netzwerk von außen schützen, und Verbindungen nur über IPSec erlauben. Sie müssen dazu IPSec auf Ihrem Gateway und Client einrichten und die nötigen X.509 Zertifikate erstellen.

Der VPN Client soll eine sichere Verbindung über IPSec zum VPN Gateway aufbauen und über die verschlüsselte Verbindung mit dem geschützten Subnetz kommunizieren können. Somit wird in der Aufgabe das klassische 'Roadwarrior'-Szenario simuliert, bei dem ein PC/Laptop von ausserhalb des eigenen Heimnetzes mittels der IPSec-Verbindung gesicherten Zugriff erhält. Das geschützte Subnetz kann ein Firmennetz darstellen und könnte vertrauliche Informationen enthalten.

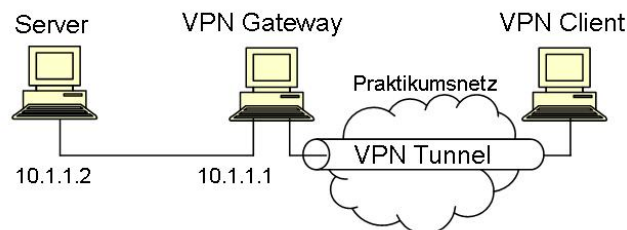


Abbildung 1: VPN Konfiguration

Führen Sie die nächsten Schritte durch, um die IPSec Verbindung zu konfigurieren. Verwenden Sie als Hilfe auch die Manpages, `man ipsec`, `man ipsec.conf`, `man openssl`.

1. Installation des IPSec-Dienstes

Installieren Sie das StrongSwan Paket vom Praktikumsserver:

- Entpacken Sie die Datei `strongswan.tar`
- `make programs`
- `make install`

2. Erstellen von Zertifikaten

Die Zertifikate werden mit dem Tool `openssl` erstellt. Allgemeine Einstellungen für `openssl` können in der Datei `/etc/ssl/openssl.cnf` vorgenommen werden. Die Zertifikate werden standardmäßig im aktuellen Verzeichnis unter `demoCA` erstellt.

Beim Erstellen der Zertifikate geben Sie bitte ein:

- Country: CH
- State: Zurich
- City: Zurich
- Organization: UniZh
- Unit: IFI
- Name: CertAuthority für das CA, Gateway für den VPN Gateway und Client für den VPN Client

Zuerst muss ein Certificate Authority (CA) mit dem folgenden Befehl erstellt werden:

```
/usr/share/ssl/misc/CA.sh -newca
```

Mit dem Befehl werden die zwei Dateien `cakey.pem` und `cacert.pem` generiert. Erstellen Sie auch die Revocation Liste mit dem Befehl

```
openssl ca -gencrl -out crl.pem
```

Danach müssen die Zertifikate für den Client und Gateway erstellt werden. Verwenden Sie dazu die Befehle `CA.sh -newreq` zum Generieren und `CA.sh -sign` zum Signieren der Zertifikate. Benennen Sie die erstellten Dateien `newreq.pem` und `newcert.pem` entsprechend in `gateway.key` bzw. `client.key` und `gateway.pem` bzw. `client.pem` um.

3. Konfiguration der IPSec Verbindung

Konfigurieren Sie die IP Adresse 10.1.1.1 auf dem VPN Gateway und 10.1.1.2 auf dem Rechner im geschützten Subnetz. Richten Sie auf dem Gateway NAT nach außen für alle Pakete ein, die aus dem Subnetz 10.1.1.0/24 und von dem VPN Client kommen, und nach innen für Pakete, die von dem VPN Client kommen. Erlauben Sie Paketforwarding auf dem Gateway.

Wir nehmen als Ordner für Zertifikate und Schlüssel den mit der Installation von IPSec angelegten Ordner `/etc/ipsec.d/`. Schlüssel gehören nach `private`, Zertifikate nach `certs`. Alle generierten Zertifikate müssen in die Unterverzeichnisse von `/etc/ipsec.d` der am VPN teilnehmenden Rechner kopiert werden:

- Root-Zertifikat `cacert.pem` nach `cacerts/`
- Private Schlüssel `gateway.key` bzw. `client.key` nach `private/`
- Zertifikate `gateway.pem` bzw. `client.pem` nach `certs/`
- Revocation List `crl.pem` nach `crls/`

Um eine VPN-Verbindung einzurichten ist es nötig in die folgenden Dateien die gewünschten Konfigurationseinstellungen vorzunehmen:

- `/etc/ipsec.conf` - hier wird die eigentliche Verbindung eingetragen

- `/etc/ipsec.secrets` - enthält das Passwort Ihres privaten Schlüssels

Der wichtigste Konfigurationsteil befindet sich in der `ipsec.conf`. Nehmen Sie die Datei vom Praktikumsserver. In der Datei sind alle benötigten Variablen bereits eingetragen, müssen aber korrekt belegt werden.

Als letztes muss das Passwort des eigenen, privaten Schlüssels noch in die Datei `ipsec.secrets` eingetragen werden.

```
: RSA <Pfad zum Schlüssel *.key> <Passwort>
```

4. Testen der sicheren Verbindung

Nach der Änderung der Konfigurationsdateien starten Sie IPSec auf dem Gateway und auf dem Client. Danach Starten Sie die Verbindung, die Sie in der `ipsec.conf` konfiguriert haben. Benutzen Sie die folgenden Befehle:

- `ipsec setup start` – zum Starten des IPSec-Dienstes
- `ipsec setup stop` – zum Stoppen des IPSec-Dienstes
- `ipsec auto --up <connection name>` – zum Starten einer Verbindung
- `ipsec auto --down <connection name>` – zum Stoppen einer Verbindung
- `ipsec auto --listall` – zum Listen aller aktiven Verbindungen
- `ipsec auto --statusall` – zum Anzeigen von Statusinformationen

Fehler und Warnmeldungen von `ipsec` finden Sie in den Logdateien `/var/log/messages` und `/var/log/warn`. Mit `tail -f /var/log/messages` werden die Meldungen laufend angezeigt.

Da wir sicher gehen wollen, dass die Kommunikation mit unserem Gateway und dem dahinterliegenden Subnetz auch verschlüsselt stattfindet, lassen wir uns mit dem Programm `ethereal` unseren Netzwerktraffic an der Netzwerkkarte mitloggen.

- Beobachten Sie mit `ethereal` die Pakete beim Verbindungsaufbau! Welches Protokoll wird für den Schlüsselaustausch benutzt?
- Stellen Sie in der IPSec-Konfiguration für `leftsubnet` `10.0.0.0/8` ein, und pinggen sie `10.0.0.2` und eine Adresse im Internet (z.B. `www.google.com`). Verfolgen Sie den Paketverlauf mit `Ethereal`? Von wo nach wo werden die Pakete verschlüsselt?

Anschliessend stellen Sie für `leftsubnet` `0.0.0.0/0` ein, und führen Sie die gleichen Schritte aus. Was ist der Unterschied? Welche Pakete werden jetzt verschlüsselt? Vergleichen Sie den Protokollverlauf mit `ethereal`.

- Mittels welcher Pakete findet die Kommunikation bei aktiver IPSec-Verbindung statt? Was kann eine "Dritte Person" aus diesen Paketen für Informationen über unsere Kommunikation erhalten?