CN-Lernmodul 2 - Zusammenfassung

1. Dezember 2012

Inhaltsverzeichnis

1 Einleitung

Ein Virtual Private Network (VPN) ist ein "privates Netzwerk", das über öffentliche Leitungen oder Verbindungen hergestellt wird, indem gewisse Sicherheitsmethoden für den Datentransfer angewendet werden. Dies ermöglicht z.B. Firmen, ihr Netzwerk über öffentliche Netze (wie z.B. das Internet) zu vergrössern und Mitarbeitern einen Remote-Login in das Firmennetz zu ermöglichen.

2 VPN-Typen

Verschiedene VPN-Typen können sich z.B. unterscheiden in Protokoll, abstraction layer, access type usw. VPN's verpacken privat adressierte Pakete in öffentlich adressierten Paketen. Man nennt das „tunneling." Privacy und Authenticity kann durch Verschlüsselungsmechanismen erreicht werden.

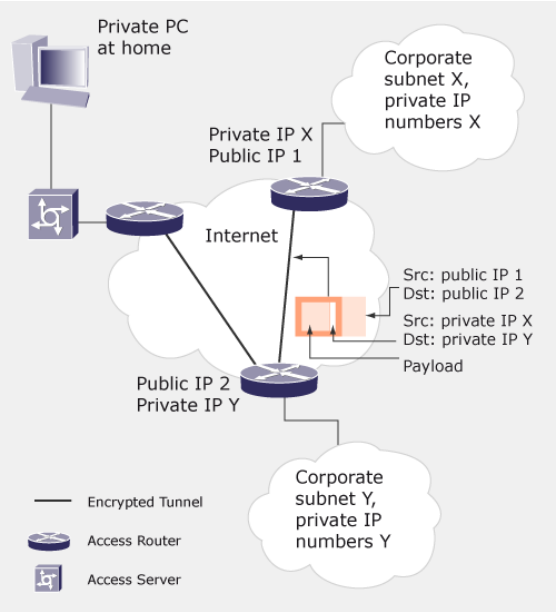


Abbildung 1: vpn-types and tunneling

2.1 Subnet-to-Subnet VPN

Verbindet geographisch getrennte private IP-Subnetzwerke. Der gesamte Datenverkehr, der von einem Subnetzwerk ausgeht und für das andere bestimmt ist, wird durch das öffentliche „getunnelt."

2.2 Access VPN

Ermöglicht Roaming-Usern den Zugriff auf das virtuelle Netzwerk von Home-Computern oder über einen beliebigen Internet-POP (Point of Presence). Auch hier wird das Tunneling benutzt; entweder übernimmt ein Home-Computer die Rolle eine Tunnel-Endpunktes, oder der POP eines Internet Service Providers (ISP).

3 Encapsulation

3.1 Link Layer VPNs (Layer 2)

Beispiele für VPNS auf dieser Ebene sind Integrated Services Digital Network (ISDN), Frame Realy und Asynchronous Transfer Mode. Auch Virtual Local Networks funktionieren auf ähnliche Weise auf dieser Ebene.

Vorteile

- Verbindungsorientiert, Pakete müssen nicht geroutet werden sondern werden über einmal erstellten Link übertragen.
- QoS auf dieser Ebene schon garantiert, muss nicht noch zusätzlich implementiert werden.

Nachteile

- Braucht homogene Netzwerkstruktur
- IP-Ebene muss trotzdem noch verwaltet werden, Mehraufwand auf zwei Ebenen!

3.2 Network Layer VPNs (Layer 3)

IP Pakete werden als Payload in ein anderes IP Paket verpackt(IP in IP, *IPIP*), dann versendet. Dass innere Paket kann dabei verschlüsselt werden und garantiert so Sicherheit, das äussere jedoch nicht. Der VPN Server dient dann als Interface, der den äusseren Header entfernt & das innere Paket entschlüsselt.

Firewalls können eingesetzt werden um verschlüsselte Verbindungen zu erzwingen.

4 Security and the Internet Protocol

Es gibt viele verschiedene Technologien, um die Kommunikation über das Internet sicherer zu machen. Viele davon sind aber an eine bestimmte Anwendung gekoppelt (in diesem Fall werden die Sicherheitsmechanismen auf dem Application Layer bereitgestellt).

Beispiele

- PGP („Pretty Good Privacy“) für die Verschlüsselung von E-Mails und Browser-basierte Authentifizierung
- SSL („Secure Sockets Layer“) für die Verschlüsselung des Datenverkehrt zwischen Web-Browser und Web-Server.

Natürlich ist das für grosse Firmen oder für einen ISP (Internet Service Provider) nicht geeignet, da morgen andere Applikationen über die heutigen Netzwerke laufen könnten.

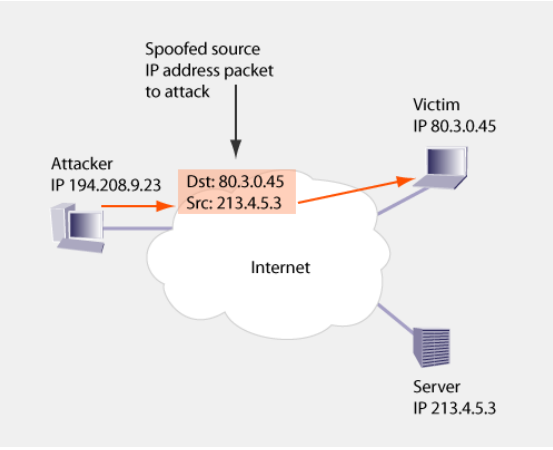
4.1 Possible Threats in the Internet

VPNs müssen mindestens die folgenden drei Anforderungen erfüllen:

- Authentication (Die Person, mit der man kommuniziert, ist die, für die sie sich ausgibt)
- Confidentiality & Privacy (Niemand soll den Datenverkehrt belauschen können)
- Integrity (Daten dürfen während der Übertragung nicht verändert werden können)

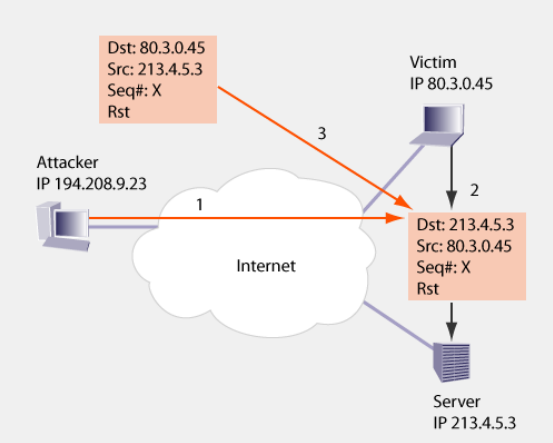
4.1.1 Spoofing

Beim Spoofing gibt sich ein Angreifer als jemand anderes aus, indem er Pakete mit einer entsprechenden IP-Source-Adresse statt der eigenen versieht. Es ist eine allgemeine Tatsache, dass eine IP-Source-Adresse nicht vertrauenswürdig ist.



4.1.2 Session Hijacking / Man in the Middle Attack

Ein Hacker kann sich „in die Mitte eines Kommunikationsweges setzen," und die Kommunikationspartner jeweils glauben lassen, er sei das Gegenüber. Er kann sämtliche Datenpakete filtern und manipulieren. Es reicht daher nicht aus, einen Kommunikationspartner *einmal* zu identifizieren, sondern es sollte jede Datenquelle authentifiziert werden.



4.1.3 Electronic Eavesdropping

Ein grosser Teil der meisten Netzwerke basiert auf Ethernet LANs. Das Abhören solcher Ethernet-Leitungen ist einfach - noch ernster ist die Lage bei Wireless-LANs. In Ethernet-Netzwerken kann jeder angeschlossene Knoten jedes Paket lesen. Es ist eine Konvention, dass jeder Knoten nur die an ihn adressierten Pakete verarbeitet. Natürlich kann ein Gerät einfach konfiguriert werden, dass es alle Pakete „sammmelt," über die Leitung verschickt werden. Physikalisch ist es nicht möglich, an einem anderen Standort im Netzwerk festzustellen, dass ein Gerät alle Pakete verarbeitet.

5 IP Sec: The Security Architecture for the Internet Protocol

Die IP Security Architecture (IPSec) bietet Sicherheits-Features für einzelne Datenpakete. Ursprünglich wurde diese Architektur zur Verwendung in IPv6 konstruiert. Die IPSec-Architektur wurde aber auch in die bisherige IP-Version (IPv4) aufgenommen. IPSec enthält alle Sicherheitsmechanismen, die zur Implementierung von VPNs nötig sind.
Die IPSec-Architektur besteht aus verschiedenen Protokollen, die IP-Header-Erweiterungen beschreiben, die Sicherheitsmechanismen bereitstellen. Die Sicherheitsfunktionen für die einzelnen Pakete werden durch zwei Protokolle bereitgestellt:

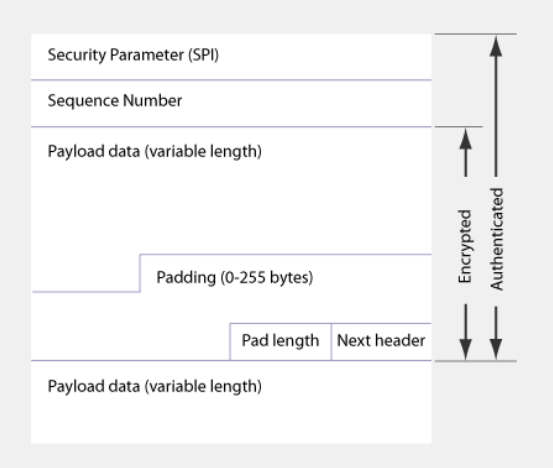
AH Der Authentication Header stellt Datenintegrität und Authentizität sicher.

ESP Das Encapsulating Security Payload-Protokoll sorgt für Privacy mit Hilfe von Verschlüsselungsmechanismen.

AH und ESP sind unabhängige Protokolle, sie separat oder miteinander kombiniert eingesetzt werden können.

5.1 The Encapsulation Security Payload

Das ESP hat die Protokollnummer 50. Die Nutzdaten werden umfasst von einem ESP-Header und einem ESP-Trailer.



5.1.1 ESP header

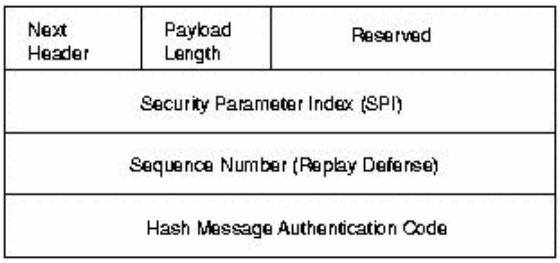
Der ESP-Header befindet sich zwischen IP- und TCP-/UDP-/...-Header. Er enthält einen sogenannten SPI (security parameter index), um die Sicherheits-Assoziation zu identifizieren, und eine Sequenznummer, die für jedes Datenpaket inkrementiert wird (Abwehr von Replay-Attacken).

5.1.2 ESP trailer

Der ESP-Trailer befindet sich hinter den Nutzdaten und ist, wie die Nutzdaten selbst, verschlüsselt. Der Trailer sorgt auch für das Padding (Auffüllen der Datenblöcke), das nötig ist, weil Verschlüsselungs-Algorithmen oft Datenblöcke von einer bestimmten Länge voraussetzen. Der Trailer enthält daher ein Feld, das die Länge des Paddings in Bits enthält (pad length field). Ein weiteres Feld des ESP-Trailers enthält die Protokoll-Nummer des nächsten Protokolls (z.B. IP oder ein ein nächstes IPSec-Protokoll)

5.2 The Authentication Header

Das AH-Protokoll hat die Nummer 51. Es dient dazu, ein Datenpaket zu authentifizieren, so dass das IPSec-Peer des Empfängers sicher sein kann, von wo das erhaltene Paket stammt. Auch die Datenintegrität ist gewährleistet, d.h. die Empfänger-Station kann überprüfen, dass kein Dritter das Paket während der Übertragung manipuliert hat. AH macht das durch das Berechnen von entsprechenden Authentifizierungs-Daten mit einer sicheren one-way Hash-Funktion. Da diese Berechnung mit Hilfe eines geheimen Schlüssels geschieht. Ein Angreifer, der den geheimen Schlüssel nicht kennt, ist nicht in der Lage, ein valides Datenpaket herauszufiltern oder zu authentifizieren.
Der AH-Header enthält ein Feld für den nächsten Header und codiert die Länge der Nutzdaten (nötig, da die Authentifizierungsdaten variabel sind in ihrer Länge). Wie der ESP-Header enthält auch der AH-Header einen SPI (Security Parameter Index) und eine Sequenznummer. Dahinter folgen dann die Authentifizierungsdaten (= der Wert der berechneten Hash-Funktion).



6 Transport and Tunnel Mode

Sowohl bei ESP als auch bei AH gibt es zwei Modi: transport mode und tunnel mode.

6.1 Transport Mode

Beim transport mode werden die Nutzdaten und ein Teil des IP-Headers verschlüsselt. Der IP-Header wird durch das Hinzufügen von neuen Feldern erweitert.
Dieser Modus ermöglicht die Verwendung von IPSec über eine End-zu-End-Verbindung.

6.2 Tunnel Mode

Im tunnel mode wird dem Paket ein komplett neuer IP-Header angefügt. Der Modus ist ideal zum Implementieren eines VPN-Tunnels. Sowohl AH als auch ESP können für einen IP-VPN-Tunnel verwendet werden. Tunneling packt das ursprüngliche IP-Paket ein (ESP) und fügt einen neuen IP-Header hinzu, der die Adresse des IPSec-Gateways enthält. Dieser Modus ermöglichet es, nicht-routbare IP-Adressen (oder andere Protokolle) über ein öffentliches Netzwerk übertragen, da die Adressen im inneren Header versteckt sind. Auch die ursprüngliche Netzwerk-Topologie wird versteckt (Privacy).

7 Security Association (SA) and Security Policy Database (SPD)

Sowohl AH als auch ESP müssen an einem gewissen Punkt im Netzwerk eine Veränderung an IP-Paketen vornehmen. Die involvierten IPSec-Knoten bilden Sender-Empfänger-Paare; der Sender verändert ein IP-Paket, der Empfänger macht die Veränderung rückgängig. Die Beziehung zwischen Sender um Empfänger wir durch eine Security Association (SA) beschrieben.
Eine SA beschreibt also nur genau eine Transformation und die zugehörige Rücktransformation. Beim Einsatz mehrerer Sicherheitsdienste müssen also auch mehrere SA's aufgebaut werden.
Unter IPSec werden durch die SA verschiedene Sachen spezifiziert:

Eine SA wird durch einen Security Parameter Index (SPI, 32 bits), die Ziel-Adresse und einen Security Protocol Identifier (zur Bezeichnung des Übertragungsverfahrens; AH/ESP) festgelegt.
Der Sender schreibt den SPI in das entsprechende Feld der IP-Protokoll-Erweiterung und der Empfänger kann dann mit Hilfe dieser Information die richtige Security Association identifizieren und kann so die zuvor vorgenommene Transformation rückgängig machen und auf das ursprüngliche Paket zugreifen.
Jede kommunizierende Einheit kann in beliebig viele Sicherheitsverbindungen (SA's) involviert sein. Die Spezifikationen der Sicherheitsverfahren sind lokal in jedem IPSec-Knoten lokal in der Security Policy Database (SPD) gespeichert. Die SPD enthält verschiedene Einträge für ein- und ausgehenden Datenverkehr. Durch die SPD wird bestimmt, ob ein Datenstrom verschlüsselt werden muss oder im Klartext übertragen werden kann. Wenn verschlüsselte Daten versendet werden, muss die SPD eine Referenz auf die entsprechende SA haben.