FreeS/WAN für Linux

Markus Mazanec

Was ist FreeS/WAN?

FreeS/WAN ist eine Softwarelösung, welche die Installation von Virtual Private Networks mit Hilfe von Linux-Rechnern als Gateways erlaubt.

Wie der Großteil der für Linux geschriebenen Software, unterliegt FreeS/WAN der GNU Public License und kann somit kostenlos verwendet werden. Die Sourcen können über das Internet bezogen werden (tar.gz-Datei).

FreeS/WAN ist eine (noch unvollständige[1]) IPSEC-Implementierung, wobei die krypthographischen Teile der Software außerhalb der USA programmiert wurden und damit nicht den US-Exportrestriktionen unterliegen.

Schlüsselverwaltung

Zurzeit werden die manuelle Schlüsselverwaltung (dabei werden die Schlüssel direkt in der Konfigurationsdatei gespeichert) und der automatische Schlüsselaustausch über Pluto, einer Implementierung des Internet Key Exchange (IKE)-Protokolls, unterstützt. Nicht unterstützt werden die in IPSEC vorgesehen Methoden Public Key Infrastructure (PKI) oder secure DNS.

Verschlüsselung

Neben den von IPSEC geforderten (aber unsicheren) Algorithmen null encryption transform und DES implementiert FreeS/WAN TripleDES.

Authentifizierung

Die Authentifizierung erfolgt mit den Message Digest Algorithmen Message Digest 5 (MD5) oder Secure Hashing Algorithmus (SHA).

Installation/Integration

Teile des Programms sind Ergänzungen des Kernels, von dem eine eigene Version für FreeS/WAN kompiliert werden muss.

Leider arbeitet FreeS/WAN nicht mit den 2.2.x-Versionen des Linux-Kernels zusammen, unabhängig davon, ob die (experimentelle) IPv6-Unterstützung aktiviert wird oder nicht. Man ist gezwungen. auf die Version 2.0.36 zurückzugreifen. Diese Einschränkung lässt sich allerdings verschmerzen, da es sich dabei um eine ausgesprochen stabile und sichere Kernelversion handelt.

FreeS/WAN wird entpackt und installiert. Nach dem Starten der Kernelkonfiguration findet man folgende Merkmale ausgewählt vor:

```
IP: forwarding/gatewaying
IP: tunneling
Kernel/User network link driver
```

[1] Alle Daten und Fakten beziehen sich auf die FreeS/WAN Version 1.0, April 1999.

Zusätzlich kann man noch `IP: optimize as router not host` aktivieren, falls der Rechner hauptsächlich als Router eingesetzt werden soll.

Als neuer Punkt (verglichen mit einer 2.0.36 Standardauswahl) in der Auswahl erscheint `IP Security Protocol (IPSEC)`, das natürlich aktiviert wird.

Daraufhin wird die Konfiguration gespeichert und ein neuer Kernel übersetzt. Nach einem Neustart stehen die hinzugefügten Merkmale zur Verfügung.

Bevor eine sichere Übertragung erfolgen kann, müssen allerdings noch in der Datei `/etc/ipsec.conf` die Einstel lungen für den zu errichtenden Tunnel konfiguriert werden. Die für die Authentifizierung beim Schlüsselaustausch maßgeblichen Informationen („shared secrets") werden in der Datei `/etc/ipsec.secrets` abgelegt.

ipsec.conf

Ein typischer Eintrag der Konfigurati onsdatei sieht wie folgt aus:

```
conn demo
     type=tunnel
     left=10.0.0.1
     leftnexthop=10.44.55.66
     leftsubnet=172.16.0.0/24
     right=10.12.12.1
     rightnexthop=10.88.77.66
     rightsubnet=192.168.0.0/24
     spibase=0x200
     esp=3des-md5-96
     espenckey=[192 bits]
     espauthkey=[128 bits]
     keyexchange=ike
     keylife=8h
```

Mit `conn` kann der konfigurierten Verbindung ein Name zugewiesen werden.
Die meisten Verbindungsparameter sind paarweise (für jedes Ende des Tunnels) anzugeben.
`left` gibt das Interface des Gateways an, über das die Ver bindung mit dem anderen Gateway hergestellt wird.
`leftnexthop` gibt an, über welchen Router `right` erreicht werden kann. Bei einer direkten Verbindung von `left` mit `right` entfällt dieser Parameter.
`leftsubnet` spezifiziert die IP -Adressen, die von `left` geschü tzt werden.
`leftfirewall=yes` aktiviert die Maskierungsfunktionen des Gateways, für den Fall, dass ein Subnet mit nicht routbaren IP -Adressen angeschlossen ist).
`right...` analog zu `left....`
`spibase` definiert die Basis für die Nummerierung des Security Parameter Index, ohne den mehrere Verbindungen zwischen `left` und `right` nicht unterschieden werden könnten.
`esp` gibt an, welcher Verschlüsselungsalgorithmus verwendet werden soll.

`espenckey` bestimmt die Länge des Schlüssels zur Verschlüsselung.
`espauthkey` bestimmt die Länge des Schlüssels zur Authentifizierung.
Über `keyexchange` kann der Algorithmus ausgewählt werden, der für den Schlüsselaustausch herangezogen wird.
`keylife` ist die Lebensdauer eines Schlüssels.

Anstelle der IP-Adressen können auch Namen verwendet werden. Das verringert allerdings die Sicherheit, da ein Angriff über eine feindliche DNS-Auflösung möglich wird.

ipsec.secrets

In dieser Datei werden die „shared secrets" für die Authentifizierung beim Diffie-Hellman Schlüsselaustausch des IKE Protokolls abgelegt. Jede Zeile enthält dabei eine Gateway-IP-Adresse und das zugehörige „secret". FreeS/WAN enthält ein Tool, mit dessen Hilfe „secrets" erstellt werden können.

Diffie-Hellman Schlüsselaustausch:

$$A \Rightarrow B:\ X = g^x$$
$$B \Rightarrow A:\ Y = g^y$$
$$A:\ K = Y^x = g^{xy}$$
$$B:\ K = X^y = g^{xy}$$

A, B ... Kommunikationspartner
g ... „shared secret" der Kommunikationspartner
x, y ... große Zufallszahl
K ... synchronisierter Schlüssel

Beide Dateien, `ipsec.conf` und `ipsec.secrets`, müssen auf den betroffenen Gateways abgelegt werden (zumindest die Abschnitte der für das jeweilige Gateway relevanten Verbindungen). Es ist darauf zu achten, dass der Transfer dieser Dateien gesichert erfolgt (outband oder verschlüsselt).

Kompatibilität

Linux-FreeS/WAN-Gateways kooperieren nicht nur mit anderen Linux-FreeS/WAN-Gateways, sondern wurden auch mit folgenden Systemen erfolgreich getestet: OpenBSD, Cisco Router, Raptor Firewall/WinNT, Xedia Access Point/QVPN, PGP 6.5 Mac/Windows IPSEC Client

Literatur

[1] Gilmore, J., et al., „FreeS/WAN", http://www.xs4all.nl/~freeswan

[2] Murhammer, M., T. Bourne, T. Gaidosch, Ch. Kunzinger, L. Rademacher, A. Weinfurter, „A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions", http://www.redbooks.ibm.com/

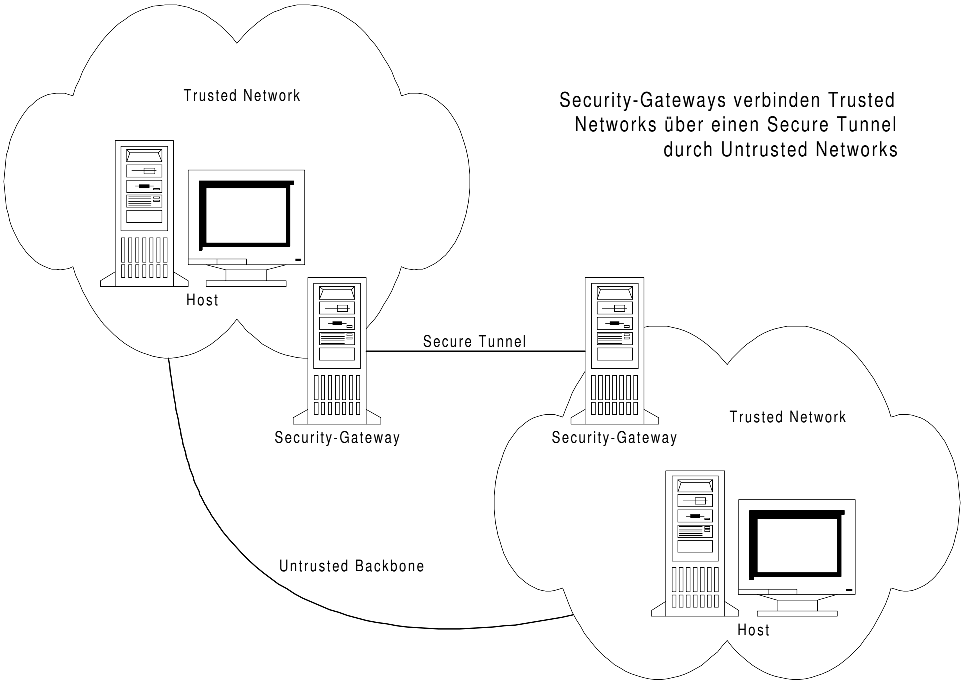
IPSEC

Markus Mazanec

Leistungen

IPSEC stellt Sicherheitsfunktionen auf dem Internet Protocol (IP) -Niveau zur Verfügung. Es übernimmt die Authentifizierung und/oder Verschlüsselung übertragener Pakete. In IPv6 ist IPSEC fester Bestandteil, zu IPv4 kann es optional ergänzt werden.

Struktur



Die Security -Gateways agieren als Kommunikationsgateways, die vertrauenswürdige Netze über unsichere Strecken verbinden und den Rechnern in diesen Netzen die sichere Datenübertragung ermöglichen. Da IPSEC auf IP - Niveau arbeitet, geschieht diese Sicherung völlig transparent für die beteiligten Arbeitsstationen und Server. Alle Security -Gateways besitzen für die Security - Gateways mit denen sie in Verbindung stehen so genannte „Security Associations“ , welche die Parameter für die gesicherte Verbindung enthalten.

Security Associations

Security Associations bilden das fundamentale Konzept von IPSEC. Sie definieren, wie ein Security -Gateway eine Verbindung zu einem anderen Gateway aufbauen und halten sol l. Eine Kombination aus der Zieladresse und dem Security Paramter Index (SPI) identifizieren eine Security Association (SA).

Über die Zieladresse ermittelt das sendende Security Gateway die passende Zieladresse und den zugehörigen SPI. Das empfangende Gat eway ermittelt ebenfalls über diese Daten die zugehörige SA. Es ist zu beachten, dass SAs für eine Richtung definiert werden, d.h. für eine bidirektionale Verbindung zwei SAs erforderlich sind (für jede Richtung ein eigener SPI).

Jede SA enthält folgende Daten:

- Algorithmus, der für die Authentifizierung verwendet wird
- Schlüssel für die Authentifizierung
- Verschlüsselungsalgorithmus
- Schlüssel für die Verschlüsselung
- Daten für die kryptographische Synchronisation
- Sensibilität der übertragenen Daten (ermöglicht die Verwendung unterschiedlicher Sicherheitsstufen)

Authentifizierung

Die Authentifizierung über den Authentication Header (AH) stellt die Integrität und den Ursprung der Daten sicher und schützt vor Replay-Attacken.

Bei der Authentifizierung werden zwei Modi unterschieden: der Transport Mode und der Tunnel Mode. Im Transport Mode entspricht der physische Empfänger dem inhaltlichen Adressaten, im Tunnel Mode wird das Paket vom physischen Empfänger (Gateway) an den inhaltlichen Adressaten weitergeleitet.

Transport Mode:

Original IP-Header	Authentication Header	TCP	Data

Tunnel Mode:

New IP-Header	Authentication Header	Original IP-Header	TCP	Data

In beiden Varianten werden alle Felder authentifiziert. Am häufigsten kommt Message Digest 5 (MD5) als Algorithmus zum Einsatz.

Aufbau des Authentication Headers:

Next Header	Typinformation zum Header in den Nutzdaten
Payload Length	Länge der übertragenen Nutzdaten
Reserved	
SPI	identifiziert die zu verwendende SA
Sequence Number	verhindert Replay-Attacken
Authentication Data	enthält den Integrity Check Value (ICV)

Verschlüsselung

Encapsulating Security Payload (ESP) stellt die Vertrauenswürdigkeit, Integrität und den Ursprung der übertragenen Daten sicher. Zusätzlich schützt es vor Replay-Attacken und verhindert im Tunnel Mode die Verkehrsanalyse. Mittels Padding lässt sich die tatsächliche Menge übertragenen Nutzinformationen verschleiern.

Auch bei der Verschlüsselung wird zwischen einem Transport und Tunnel Mode unterschieden.

Transport Mode:

Original IP -Header	ESP Header	TCP	Data	ESP Trailer	ESP Authentication

Tunnel Mode:

New IP -Header	ESP Header	Original IP -Header	TCP	Data	ESP Trailer	ESP Authentication

$\longleftrightarrow$ Verschlüsselung $\quad$ $\leftarrow - - - \rightarrow$ Authentication

Aufbau des ESP Headers:

SPI	identifiziert die zu verwendende SA
Sequence Number	verhindert Replay -Attacken
Initialization Vector	wird für DES im CBC Mode benötigt

Digital Encryption Standard (DES) im Cipher Block Chaining (CBC) Mode:

$$C_i = E_k(C_{i-1} \oplus P_i)$$
$$C_1 = E_k(IV \oplus P_1)$$

C_i ... i -ter Block des Kryptotexts
E_k ... Verschlüsselung mit Schlüssel k
P_i ... i-ter Block des Klartexts
IV ... Initialisierungsvektor

Aufbau des ESP Trailers:

Padding	Verschleierung der tatsächlichen Nachrichtenlänge
Padding Length	
Next Header	Typinformation zum Header in den Nutzdaten

Aufbau des ESP Authentication Teils:

Authentication Data	enthält den Integrity Check Value (ICV)

Über die Kombination von AH mit ESP kann eine verschlüsselte Übertragung bei gleichzeitiger Authentifizierung jedes gesamten Pakets erreicht werden.

Literatur

[1] Atkinson, R., „Security Architecture for the Internet Protocol", RFC 1825, http://info.internet.isi.edu:80/in -notes/rfc/files/rfc1825.txt

[2] Atkinson, R., „IP Authentication Header", RFC 1826, http://info.internet.isi.edu:80/in -notes/rfc/files/rfc1826.tx t

[3] Atkinson, R., „IP Encapsulating Security Payload", RFC 1827, http://info.internet.isi.edu:80/in -notes/rfc/files/rfc1827.txt

[4] Schneier, B., „Applied Cryptography", Wiley, 1996

[5] Gruska, J., „Foundations of Computing", International Thomson Com puter Press, 1997

[6] Salomaa, A., „Public -key cryptography", Springer -Verlag, 1991