HP-UX IPSec & HP-UX IPFilter

Produkte für die Netzwerksicherheit von HP-UX Systemen

IT-Symposium 2005
P087

6.April 2005
von Winfried Knobloch

HP-UX IPSec & HP-UX IPFilter ☺ Inhalt

Was wollen wir tun ?

- Motivation

- HP-UX IPSec – *Das Produkt*
  – *Konzepte*
- HP-UX IPFilter – *Das Produkt*
  – *Konzepte*
- Diskussion von Einsatzszenarien

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

Das Produkt: **HP-UX IPSec**

„HP-UX IPSec (J4256AA) provides an infrastructure to allow secure communications over IP-based networks between systems and devices that implement the IPsec family of protocol standards.“

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

- die Software gibt es im Internet auf der Seite
  http://www.software.hp.com
  unter Security and manageability

- sie kostet **0 €**

- Dokumentationen und White Papers findet man unter **http://www.docs.hp.com/en/internet.html**

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

Um was geht es dabei ?

- VPN Client Software für HP-UX 11.X Betriebssysteme
- Implementation der „IP security (IPSec) protocol suite“ entsprechend IETF Spezifikation (RFC 2411, RFC 2409 u.a.m)
- sichere und vertrauliche Kommunikation in unsicheren Netzwerken

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

Aufgaben:

1. Sicherstellen der Datenintegrität
   (Data Integrity)
2. Authentifizierung
   (Authentication)
3. Sicherstellen der Vertraulichkeit
   (Confidentiality)
4. Applikationstransparenz
   (Application-transparent Security)

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

Die technische Umsetzung:

- IPSec arbeitet im IP-Layer
- IPSec benutzt eigene IP Protokolle
  (Protokollnummern 50 und 51)
- Es wird der „Internet Key Exchange (IKE)“
  Mechanismus benutzt um die kryptographischen
  Schlüssel zu verwalten.

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

- benutzt entweder **Authentication Header (AH)**
  - dieser sichert „nur“ Datenintegrität und Authentifizierung via kryptographischer Hash-funktion *(Symmetric key hash)* des IP-Paketes

  - nutzbare Hashfunktionen
    HMAC-SHA1
    (Hashed Message Authentication Code-Secure Hash Algorithm 1, 128-bit key)
    HMAC-MD5
    (HMAC-Message Digest 5, 160-bit key)

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

- oder behandelt das Orginalpaket als
  Encapsulating Security Payload (ESP)
  - erlaubt „Verschlüsselung“ oder „Verschlüsselung mit Authentifizierung“
  - nutzbare Algorithmen

DES-CBC
(Data Encryption Standard Cipher Block Chaining Mode, 56-bit key length)
3DES-CBC
(Triple-DES CBC, three encryption iterations, each with a different 56-bit key)
AES128-CBC (Advanced Encryption Standard CBC, 128-bit key length)

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

- der Schlüsselwechsel beim IKE ist konfigurierbar
- für die **primäre IKE Authentifikation** kann man entweder „preshared keys“ oder „digital signatures“ einer PKI benutzen
- aktuell unterstützte PKI Lösungen
  - *VeriSign Managed PKI* (früher *VeriSign OnSite for VPNs*)
  - *Baltimore UniCERT 3.5*

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

Unterstützte Netzwerktopologien

Prinzipiell werden zur Zeit zwei Konfigurationen unterstützt (wenn auch in mehreren Varianten)

- *Host-to-Host*

- *Host-to-Gateway*

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

Was geht nicht ?

- Ein HP-UX System mit „HP-UX IPSec“ Software kann nicht als IPSec Gateway eingesetzt werden !
- Konstuktionsbedingt gibt es Probleme mit NAT.

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

Bemerkungen zur Benutzung

- die Konfiguration via GUI und inzwischen auch via Kommandozeile möglich
- zumindest die Arbeit mit *„preshared keys“* ist intuitiv
- der Einfluß auf die Netzwerk-Performance ist „normalerweise“ <3% (vgl. White paper)

HP-UX IPSec & HP-UX IPFilter ☺ IPSec

- man kann sowohl die Kommunikation zwischen einzelnen Ports als auch den gesamten Netzwerk-verkehr durch IPSec schützen
- HP-UX IPSec ist prinzipiell auch im Serviceguard-umfeld einsetzbar
- HP-UX IPSec arbeitet mit allen „standardkon-formen“ IPSec Implementationen zusammen, d.h. man muß im heterogenen Netzwerk aufpassen

HP-UX IPSec & HP-UX IPFilter ☺ IPFilter

Das Produkt: **HP-UX IPFilter**

„HP-UX IPFilter is a system firewall that filters the IP level packets that travel in or out of a system. The firewall functions as a security defense by cutting down the number of exposure points on a machine.“

HP-UX IPSec & HP-UX IPFilter ☺ IPFilter

→ dieses Produkt ist die HP-UX Portierung der

IP Filter Version 3.5 Alpha 5

Software der „open source community“ (developed by Darren Reed), vgl.

http://coombs.anu.edu.au/~avalon

HP-UX IPSec & HP-UX IPFilter ☺ IPFilter

- diese Software gibt es im Internet auf der Seite
  http://www.software.hp.com
  unter Security and manageability

- sie kostet **0 €**

- Dokumentationen und White Papers findet man unter **http://www.docs.hp.com/en/internet.html**

HP-UX IPSec & HP-UX IPFilter ☺ IPFilter

Um was geht es dabei ?

Es ist eine vollwertige Firewallsoftware mit folgenden Features:

- *statefull packagefilter*
- *NAT – network address translation*
- *Dynamic Connection Allocation* (limits and logging)

HP-UX IPSec & HP-UX IPFilter ☺ IPFilter

Bemerkungen zur Benutzung

- Die Technologie erschließt sich aus den Quellen #;-)!!!
- Die Software arbeitet mit dynamisch ladbaren Kernelmodulen.
- Die Konfiguration erfolgt via Kommandozeile.

HP-UX IPSec & HP-UX IPFilter ☺ Beispiele

Einsatzszenarien

Beispiel 1:

Das Absichern eines Mailservers in der DMZ / beim Provider mit HP-UX IPFilter, vgl.

/etc/opt/ipf/ipf.conf oder `ipfstat -io`

HP-UX IPSec & HP-UX IPFilter ☺ Beispiele

```
## 1)  "die" !!! Default-Regel
block in all

## 2)  es darf auch nichts weggeschickt werden
block out all

## 3) Mailserver Zugriffsregeln; alle dürfen auf
##    den SMTP Port ( == port 25 ) zugreifen
pass in quick proto tcp from any to <local IP>/32 port = 25 keep state
pass in quick proto udp from any to <local IP>/32 port = 25 keep state

## 4)  die Regeln für den eigenen Mailversand
pass out quick proto tcp from <local IP>/32 to any port = 25 keep state
pass out quick proto udp from <local IP>/32 to any port = 25 keep state
```


HP-UX IPSec & HP-UX IPFilter ☺ Beispiele

```
## 5) die Namensauflöung / der DNS Traffic
pass out quick proto udp from <local IP>/32 to any port = 53 keep state

## 6) der Remote-Zugriff der Administratoren
##    via ssh
pass in quick proto tcp from <IP>/32 to <local IP>/32 port = 22 keep state

## 7) HP spezifisch sollte man auch etwas
##    ICMP Kommunikation erlauben
pass out proto icmp from <local IP>/32 to any keep state
```

HP-UX IPSec & HP-UX IPFilter ☺ Beispiele

Beispiel 2: HP-UX IPSec und HP-UX IPFilter

IP-Filter Regeln für IPSec Traffic

```
# IPSec Regel – IKE Kommunikation erlauben
pass in quick proto UDP from <rem.IP> port 500 to <loc.IP> port = 500
pass out quick proto UDP from <loc.IP> port 500 to <rem.IP> port = 500

# encrypted IPSec traffic erlauben
pass in quick proto 50 from <rem.IP> to  <loc.IP>
pass out quick proto 50 from <loc.IP>  to <rem.IP>

pass in quick proto 51 from <rem.IP> to <loc.IP>
pass out quick proto 51 from <loc.IP> to  <rem.IP>
```


HP-UX IPSec & HP-UX IPFilter ☺ Beispiele

Beispiel 3:

Eine sichere NFS Umgebung !