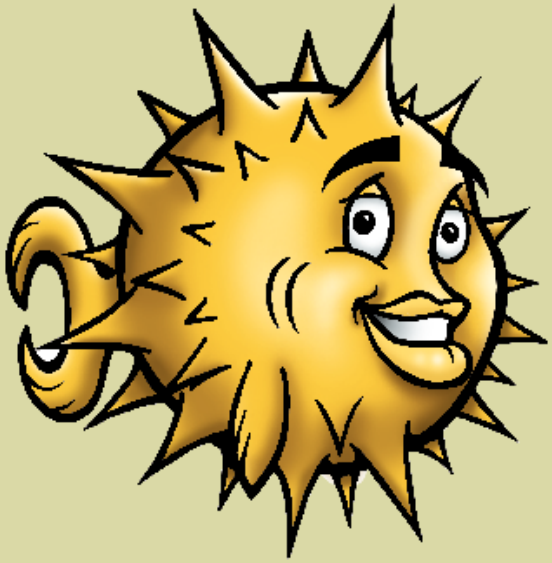
OpenVPN



Chemnitzer Linux-Tage 2010

Felix Kronlage <kronlage@bytemine.net>
@felixkronlage

bytemine GmbH

ich?

- Gründer der bytemine GmbH
  - Seit 2003
- Seit 2006 OpenBSD Entwickler
  - fkr@openbsd.org
- Aktives Mitglied im OpenVPN e.V.

Fahrplan

- Vorstellung VPN
- Vorstellung OpenVPN
- Einsatzzwecke von OpenVPN
- Vorstellung verschiedener Szenarien
- Vorstellung *bytemine-manager*
- Fragen und Antworten

Vorstellung VPN

- Vertraulichkeit
- Integrität
- Echtheit
- Replay protection

Vertraulichkeit

- Sicherstellen, das der Inhalt der Verbindung nur für den Empfänger und den Sender sichtbar ist

- Nicht nur Unternehmensdaten absichern, es wird auch zunehmend im privaten Bereich abgehört!

Echtheit und Integrität

- Echtheit und Integrität gehören zusammen
- **Echtheit**
  - Der Empfänger muss verifizieren können, das die Daten vom Sender stammen
- **Integrität**
  - Eine Modifikation der Daten muss bemerkt werden können

Replay Protection

- Ein Angreifer darf nicht in der Lage sein, Verbindungsdaten aufzuzeichnen und abzuspielen

Anwendungsfälle

- Standortvernetzung
- Anbindung mobiler Nutzer
- Verschlüsselung von Funkanbindungen
- Verbindungen zwischen Client und Server sichern
- Anbindung verschiedener Gebäudeteile
- Schützen der Privatssphäre

VPN Technologien

- IPsec
- L2TP - Layer 2 Tunneling Protocol
- **OpenVPN**
- Mesh'ed VPNs
  - CloudVPN
- SSH based ad-hoc
- pptp – Point-to-Point tunneling protocol

OpenVPN Überblick

- Layer-7
  - *Applicationlayer*
  - SSL-basiert
    - Secure Socket Layer
  - NAT-T fällt weg
- Bietet routed und bridged Modus
- Protokoll gleicht https
  - Funktioniert auch in Proxy-Umgebungen
- Zum Erkennen IDS notwendig

OpenVPN Überblick (2)

- Standard-Port (ab Version 2)
  - 1194
- Ab Version 2.1 Port-Sharing möglich
  - Security by Obscurity?
- Layer-2 Traffic im Bridged-Mode ermöglicht
  - dhcp
  - IPX
  - Microsoft Netzdienste

OpenVPN Überblick (3)

- Free-, Net- und OpenBSD und DragonFly
- Linux
- Solaris / OpenSolaris
- Mac OS X
- Windows ab 2000
- u.a. Bestandteil von IPcop, Zerina

OpenVPN Authentifizierung

- Pre-Shared Key
- Benutzername / Kennwort
  - Benutzerdatenbank
  - s/key
  - Token-basiert
- Zertifikatsbasiert
- Dual-Factor Authentifizierung

OpenVPN Plugins

- PAM
- bsdauth
- LDAP
- Radius
- MySQL
- Sqlite
- Samba

OpenVPN Konfiguration

- Erste Frage: *routed* oder *bridged*
  - *Bridged* ineffizienter
  - IP-Adresskonflikte möglich
  - Schlechtere Beschränkung
  - Broadcast Dienste möglich
- OpenVPN Programm kann sowohl Client- als auch Servermodus
  - Modus wird anhand der Konfiguration entschieden

Die Certificate Authority

- Eine Reise durch die X509 Welt
- Eine der “großen” Hürden beim Einstieg in OpenVPN
- Der schwierige Weg:
  - *easy-rsa*
- Der einfache Weg:
  - tinyCA
  - *bytemine-manager*

Zertifikatsspiele

- Root Certificate Authority
  - ggf. Intermediate
- Server Zertifikat
- Client Zertifikat
- Zertifikatssperrliste (CRL)
- Diffie-hellmann Parameter

easy-rsa

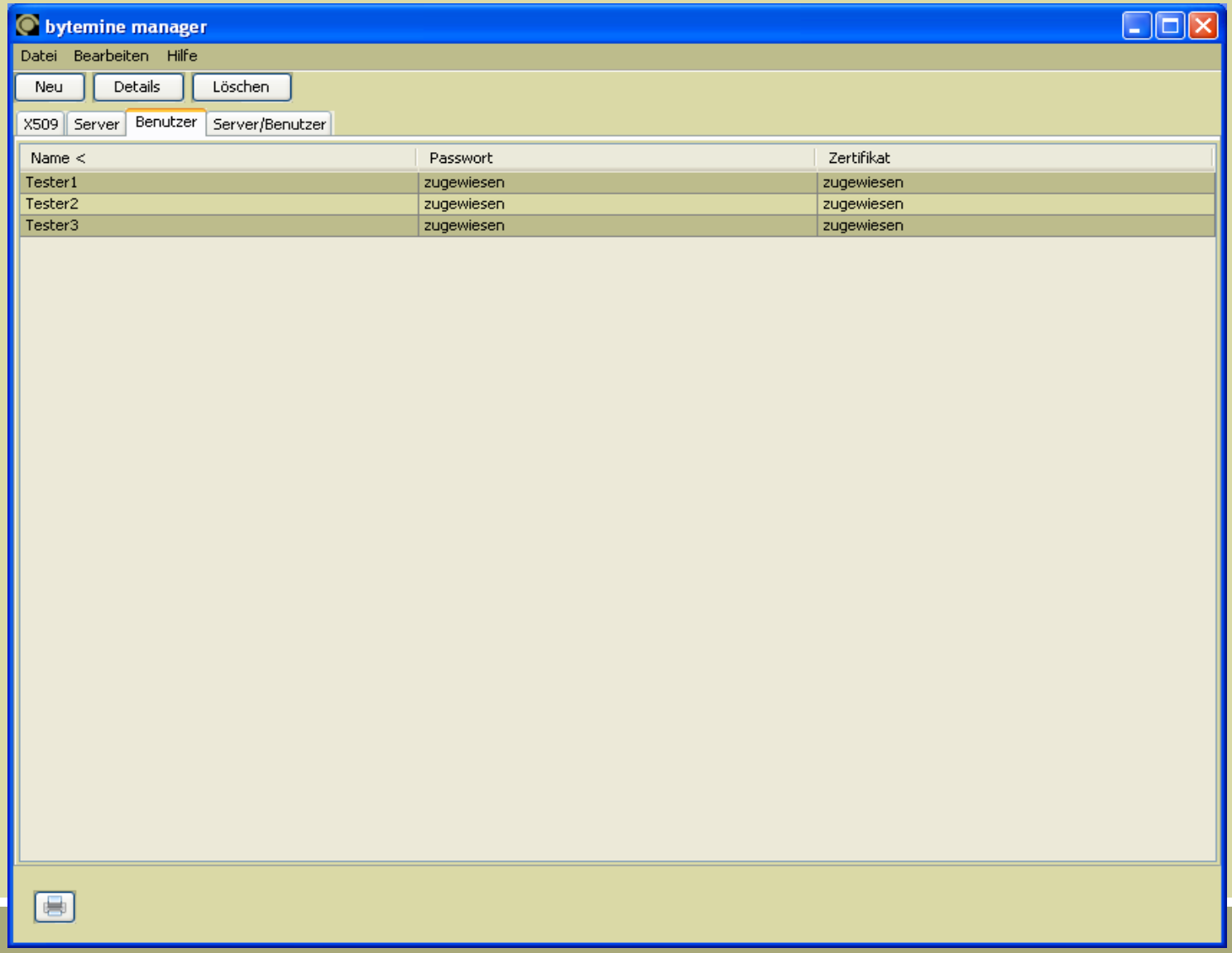
- Skript-Sammlung von openvpn
  - */usr/local/share/examples/openvpn/easy-rsa*
- *Vars* editieren
  - *./build-ca*
  - *./build-key-server*
  - *./build-key client1*
  - *./build-dh*
- Weitere Benutzer via Script

Neue Wege gehen

- *bytemine manager*
- Java-basierte Desktop Software
- Seit CeBIT 2010 unter BSD Lizenz
- Vereint CA und Administration
- Hauptautor Daniel Rauer

bytemine-manager

bytemine-manager (2)



Kommunikation - ut

- Kommunikation zum Konzentrator via ssh
- *Ut* – Socket Wrapper
- Ein einfacher Multiplexer
- Aufruf von *ut* über den SSH Kanal
- Seit OpenVPN 2.1rc13 gibts eine Unix-Domain Socket Schnittstelle
- Ebenfalls BSD-lizensiert

OpenVPN Server config

- */etc/openvpn/*
- ca.crt, server.crt, server.key, crl.pem
- zb. server-udp.conf
- tun / tap Interface

```
01 for _conf in $(find /etc/openvpn -name '*.conf' -maxdepth 1 -type f); do
02             test -r $_conf || continue
03             echo "starting OpenVPN($(basename $_conf))"
04             /usr/local/sbin/openvpn --config $_conf --daemon \
05                     --cd /tmp --script-security 2
06 done
```


OpenVPN Server config (2)

```
01 local 134.106.146.206
02 port 8080
03 proto udp
04 dev tun1
05 ca /etc/openvpn/keys/ca.crt
06 cert /etc/openvpn/keys/server.crt
07 key /etc/openvpn/keys/server.key  # This file should be kept secret
08 dh /etc/openvpn/keys/dh1024.pem
09 server 192.168.4.0 255.255.255.0
10 ifconfig-pool-persist ipp.txt
11 push "route 192.168.1.0 255.255.255.0"
12 push "redirect-gateway"
13 push "dhcp-option DNS 192.168.1.1"
14 keepalive 10 120
15 comp-lzo
16 user nobody
17 group nobody
18 status /var/log/openvpn/openvpn-status.log
19 management /var/run/management-udp unix
20 auth-user-pass-verify /usr/local/sbin/auth.pl via-file
```


OpenVPN Client config

```
01 client
02 dev tun0
03 proto udp
04 remote 134.106.146.206 8080
05 resolv-retry infinite
06 user nobody
07 group daemon
08 persist-key
09 persist-tun
10 ca ca.crt
11 cert fkr_49.crt
12 key fkr_49.key
13 ns-cert-type server
14 comp-lzo
15 auth-user-pass
```


OpenVPN und die Rendunanz

- Redundanz nur in Form von 'Load-balancing' möglich
- carp(4) als Alternative
- Problemstellung Session-Übernahme
  - SSL/TLS Client-Key-Renogiation
  - Man-in-the-middle Attacke

Skalierendes OpenVPN

- Load-balancing Modus
- Client Konfiguration bekommt mehrere Server konfiguriert
- Server-Konfiguration identisch bis auf den Virtual IP address pool

LDAP Anbindung

```
01 <LDAP>
02         URL             ldap://ldap1.office.bytemine.net
03         Timeout         15
04         TLSEnable       no
05         FollowReferrals yes
06         TLSCACertFile   /etc/openvpn/ca.crt
07         TLSCACertDir    /etc/openvpn
08 </LDAP>
09
10 <Authorization>
11         BaseDN          "dc=bytemine,dc=net"
12         SearchFilter    "(|(uid=%u)(mail=%u))"
13         RequireGroup    no
15         <Group>
16                 BaseDN          "dc=bytemine,dc=net"
17                  SearchFilter    "(cn=admins)"
18                  MemberAttribute member
19         </Group>
20 </Authorization>
```


Monitoring von OpenVPN

- Prozessüberwachung mittels Nagios
- TCP-checks sind leicht
- UDP nicht trivial

OpenVPN *Best-Practices*

- *Schlanker* Konzentrator
- Dual-Factor Authentifizierung vewenden
- *tls-auth* und *ns-cert-type* aktivieren
- Unprivilegierte Benutzer einsetzen
  - user/group *nobody*
- *chroot* verwenden
- IP Beschränkung der Nutzer
- Port 443 (https)

Die OpenVPN Community

- Seit 2010 geht openvpn.net neue Wege
  - Samoli als Community Manager
  - Experimental branch
- Der Verein *OpenVPN e.V.*
  - http://www.openvpn.eu/
- Warum ist es wichtig, OpenVPN zu pushen?

OpenVPN Bücher

- *Beginning OpenVPN 2.0.9*
  - Markus Feilner
  - ISBN-10: 184719706X
  - ISBN-13: 978-1847197061
- *OpenVPN – Kurz und Gut*
  - Sven Riedel
  - ISBN-10: 3897215292
  - ISBN-13: 978-3897215290

OpenVPN Kommerziell

- OpenVPN AS
- bytemine GmbH
  - bytemine openbsd appliance
  - ~~bytemine-manager~~
  - OpenVPN Beratung, Konzeption und Support
- SecurePoint GmbH
  - UTM Appliances
  - OpenVPN Client

Ressourcen

- http://www.openvpn.net/
- http://www.openvpn.eu/
- http://www.bytemine.net/
- http://blog.bytemine.net/
- http://github.com/bytemine/

Die berühmte (fast) letzte Seite

- Vielen Dank an die Organisatoren der Chemnitzer Linux-Tage!
- Infos zu OpenVPN und dem OpenVPN e.V. Verein gibts am bytemine Stand

Vielen Dank für die Aufmerksamkeit!

bytemine GmbH

Marie-Curie-Str. 1
26129 Oldenburg

info@bytemine.net
http://www.bytemine.net
http://blog.bytemine.net
+49-441-3091970