OpenVPN

Sicher zwischen Netzen

Vorstellung

- Michael Maier <Michael.Maier@student.tugraz.at>
- Telematik-Student an der TU Graz
- Linux, Open-Source begeistert seit 2004
- ZID der Montanuniversität 2006-2007
- Nebenbei freiberuflich tätig seit 2009

Vorstellung

- Michael Maier <Michael.Maier@student.tugraz.at>
- Telematik-Student an der TU Graz
- Linux, Open-Source begeistert seit 2004
- ZID der Montanuniversität 2006-2007
- Nebenbei freiberuflich tätig seit 2009
- Leite den Grazer OSM-Stammtisch seit May 2011

Struktur von Netzwerken

Bild - Internet (Cloud) - Firewall - Internes Netz (Intranet)

Privates Netz - Öffentliches Netz

Intern biete ich mehr Dienste als von Aussen an

- Fileserver
- VoIP-Server
- Wartungszugänge zu Servern/PCs
- Internen DNS
- Bsp Uni: Zugang zu Bibliotheken auf IP-Adressbasis

Externer Laptop?

Soll ins interne Netz - Warum?
Will außerhalb dieselben Services nutzen können, wie wenn ich daheim wäre

- Zugriff auf Fileserver
- Zugriff auf Intranet-Seiten
- Surfen hinter gesicherter Firewall

Externer Laptop?

Soll ins interne Netz - Warum?
Will außerhalb dieselben Services nutzen können, wie wenn ich daheim wäre

- Zugriff auf Fileserver
- Zugriff auf Intranet-Seiten
- Surfen hinter gesicherter Firewall

Lösung?

- Virtual Private Netzwork!

VPN-Tunnel

„Durchtunnelt" die Firewall

VPN-Tunnel

„Durchtunnelt" die Firewall
Wie sieht das in der Praxis aus

- Bekomme weitere (virtuelle) Netzwerkkarte
- Diese tut so, als wäre ich in meinem Privaten Netz

VPN-Tunnel

„Durchtunnelt" die Firewall
Wie sieht das in der Praxis aus

- Bekomme weitere (virtuelle) Netzwerkkarte
- Diese tut so, als wäre ich in meinem Privaten Netz
- Routing über die virtelle Netzwerkkarte:
  - Entweder nur der Traffic fürs Intranet (192.168.0.*)
  - Oder alles, ich surfe dann über die Firma ins Internet

VPN-Tunnel

„Durchtunnelt" die Firewall
Wie sieht das in der Praxis aus

- Bekomme weitere (virtuelle) Netzwerkkarte
- Diese tut so, als wäre ich in meinem Privaten Netz
- Routing über die virtelle Netzwerkkarte:
  - Entweder nur der Traffic fürs Intranet (192.168.0.*)
  - Oder alles, ich surfe dann über die Firma ins Internet

Sehr praktisch, wenn in meinem WLAN/Hotel/... nicht alle Dienste erlaubt sind!

Weitere Anwendung: Broadcast-Dienste

Broadcast ... 255.255.255.255
Definiert als DIESES Netzwerk - um solche Dienste zu nutzen muß ich in diesem Netzwerk sein!

Weitere Anwendung: Broadcast-Dienste

Broadcast ... 255.255.255.255
Definiert als DIESES Netzwerk - um solche Dienste zu nutzen muß ich in diesem Netzwerk sein!
Schreit förmlich nach VPN!

OpenVPN

- GPL-Lizensierte Software
- Eigenes Protokoll, OpenSSL-basiert
  - Linux, Android, *WRT
  - *BSD
  - MacOS/iOS
  - Solaris/QNX
  - Windows 2K/XP/Vista/7
- Einfache Installation
- „Einfache" Konfiguration ...

OpenVPN

- GPL-Lizensierte Software
- Eigenes Protokoll, OpenSSL-basiert
  - Linux, Android, *WRT
  - *BSD
  - MacOS/iOS
  - Solaris/QNX
  - Windows 2K/XP/Vista/7
- Einfache Installation
- ,,Einfache" Konfiguration ... Simple Config-Files
- Automatisches Failover möglich

OpenVPN Modi

Authentifizierung

- PSK (Pre-Shared Key)
- Benutzername/Passwort
- Zertifikatsbasiert

OpenVPN Modi

Authentifizierung

- PSK (Pre-Shared Key)
- Benutzername/Passwort
- Zertifikatsbasiert

Netzwerkmodi:

- layer-2 based Ethernet (TAP)
- layer-3 based IP tunnel (TUN)

Aus der Praxis: Beispiel zur Nutzung von OpenVPN

Proprietäre Geräte, die nur über Broadcast kommunizieren (Waren für reinen LAN-Betrieb ausgelegt) sollen ins WLAN.

Aus der Praxis: Beispiel zur Nutzung von OpenVPN

Proprietäre Geräte, die nur über Broadcast kommunizieren (Waren für reinen LAN-Betrieb ausgelegt) sollen ins WLAN. Ja und?

Aus der Praxis: Beispiel zur Nutzung von OpenVPN

Proprietäre Geräte, die nur über Broadcast kommunizieren (Waren für reinen LAN-Betrieb ausgelegt) sollen ins WLAN. Ja und?
Broadcast & WLAN: Böse!

- Jedes Paket muß zu jedem Teilnehmer gesendet werden, auch wenn derjenige es garnicht braucht.
- 34 Clients, die miteinander reden wollen ...
- 2 Broadcast-Pakete / Sekunde je 500 B.

Aus der Praxis: Beispiel zur Nutzung von OpenVPN

Proprietäre Geräte, die nur über Broadcast kommunizieren (Waren für reinen LAN-Betrieb ausgelegt) sollen ins WLAN. Ja und? Broadcast & WLAN: Böse!

- Jedes Paket muß zu jedem Teilnehmer gesendet werden, auch wenn derjenige es garnicht braucht.
- 34 Clients, die miteinander reden wollen ...
- 2 Broadcast-Pakete / Sekunde je 500 B.
- Ergibt: 68 Pakete/s auf 33 Zielrechner : 2244 Pakete/sec Worstcase $\Rightarrow$ No-Go!

Aus der Praxis: Beispiel zur Nutzung von OpenVPN

Proprietäre Geräte, die nur über Broadcast kommunizieren (Waren für reinen LAN-Betrieb ausgelegt) sollen ins WLAN. Ja und? Broadcast & WLAN: Böse!

- Jedes Paket muß zu jedem Teilnehmer gesendet werden, auch wenn derjenige es garnicht braucht.
- 34 Clients, die miteinander reden wollen ...
- 2 Broadcast-Pakete / Sekunde je 500 B.
- Ergibt: 68 Pakete/s auf 33 Zielrechner : 2244 Pakete/sec Worstcase $\Rightarrow$ No-Go!
- JEDES Gerät im WLAN wird mit Grundlast von 34 KB/s bombardiert! $\Rightarrow$ bei 20 Geräten am AP 680 KB/s

Lösung: OpenVPN!

Da wir nicht alle anderen Clients im WLAN (Laptops, Handys, Tablets,...) mit unseren Pakete belästigen wollen, spannen wir innerhalb des WLANs ein VPN auf:

Lösung: OpenVPN!

Da wir nicht alle anderen Clients im WLAN (Laptops, Handys, Tablets,...) mit unseren Pakete belästigen wollen, spannen wir innerhalb des WLANs ein VPN auf:

- Ein zentraler OpenVPN-Server
- Broadcast-Pakete in den Tunneln werden nur an unsere Clients gesendet
- Einrichten von Subnetzen mit Firewall-trennung
- Filtern unwichtiger Broadcasts
- Komprimierung der Daten durch OpenVPN

Realisierung:

- Gumstix (r) an den LAN-Clients, die sich ins WLAN einwählen
- OpenVPN-Server in einer VM, ins WLAN-Netz geroutet
- Clients in 3 Subnetze getrennt
  - 3 OpenVPN-Endpunkte am Server
  - Interfaces mit brctl gebridged
  - Filternde Firewall zwischen den Subnetzen
  - Ein Teil der Broadcast-Paket war unnötig, 6/7 gedroppt.

Hilfe

Links

- http://openvpn.net
- Manpage (!): *man 8 openvpn*

Vielen Dank für die Aufmerksamkeit!

Folien zu OpenVPN auf den Grazer Linuxtagen, 20.4.2013.

Folien unter:  .

Erstellt mittels LaTeXBeamer, Quelltext: Github.

Michael Maier
Twitter: @osmgraz