Tinc VPN-Daemon

Alternative zu OpenVPN & Co. für dezentrale Netze

Dominik George

OpenRheinRuhr 2013, Oberhausen

9. November 2013

- Dominik George (Nik, Natureshadow)
- 23 Jahre alt
- Student (Anglistik. Informatik, Elektrotechnik)
- Informatik-Projektlehrer an der Sekundarschule
- Organisation des Kinder- und Jugendprogramms der FrOSCon
- Routinemäßiger Konferenz-Besucher und -Mitmacher

Inhalt

1. Einleitung
   - Begrüßung
   - VPN allgemein
2. Tinc
   - Eigenschaften des Tinc VPN-Daemons
   - Einrichtung eines Beispiel-Netzes
   - Mesh Routing und Erweiterbarkeit
3. Ende
   - Where to go from here...
   - Dank

Was ist VPN?

- Virtual Private Network
- Sichere Verbindungen über unsichere Netzwerke
- Meistens wird entweder IP oder Ethernet getunnelt
- Einsatzzwecke:
  - Authentifizierter Netzzugang zum LAN
  - Sichere Route ins Internet
  - Verbindung von LAN-Segmenten / Standorten

Was ist VPN?

- Virtual Private Network
- Sichere Verbindungen über unsichere Netzwerke
- Meistens wird entweder IP oder Ethernet getunnelt
- Einsatzzwecke:
  - Authentifizierter Netzzugang zum LAN
  - Sichere Route ins Internet
  - Verbindung von LAN-Segmenten / Standorten

Was ist VPN?

- Virtual Private Network
- Sichere Verbindungen über unsichere Netzwerke
- Meistens wird entweder IP oder Ethernet getunnelt
- Einsatzzwecke:
  - Authentifizierter Netzzugang zum LAN
  - Sichere Route ins Internet
  - Verbindung von LAN-Segmenten / Standorten

Was ist VPN?

- Virtual Private Network
- Sichere Verbindungen über unsichere Netzwerke
- Meistens wird entweder IP oder Ethernet getunnelt
- Einsatzzwecke:
  - Authentifizierter Netzzugang zum LAN
  - Sichere Route ins Internet
  - Verbindung von LAN-Segmenten / Standorten

Was ist VPN?

- Virtual Private Network
- Sichere Verbindungen über unsichere Netzwerke
- Meistens wird entweder IP oder Ethernet getunnelt
- Einsatzzwecke:
  - Authentifizierter Netzzugang zum LAN
  - Sichere Route ins Internet
  - Verbindung von LAN-Segmenten / Standorten

Was ist VPN?

- Virtual Private Network
- Sichere Verbindungen über unsichere Netzwerke
- Meistens wird entweder IP oder Ethernet getunnelt
- Einsatzzwecke:
  - Authentifizierter Netzzugang zum LAN
  - Sichere Route ins Internet
  - Verbindung von LAN-Segmenten / Standorten

Was ist VPN?

- Virtual Private Network
- Sichere Verbindungen über unsichere Netzwerke
- Meistens wird entweder IP oder Ethernet getunnelt
- Einsatzzwecke:
  - Authentifizierter Netzzugang zum LAN
  - Sichere Route ins Internet
  - Verbindung von LAN-Segmenten / Standorten

Einige bekannte VPN-Lösungen

- OpenVPN
- IPsec / L2TP
- PPTP / GRE
- Hamachi

Kerneigenschaften von Tinc

- Frei und offen
- Verschlüsselung, Authentifikation und Kompression
- Mesh-Routing
- Leicht erweiterbar / skalierbar
- Switch- (Bridge) und Router-Modus (Layer 2 / 3)
- Portierbar

Kerneigenschaften von Tinc

- Frei und offen
- Verschlüsselung, Authentifikation und Kompression
- Mesh-Routing
- Leicht erweiterbar / skalierbar
- Switch- (Bridge) und Router-Modus (Layer 2 / 3)
- Portierbar

Kerneigenschaften von Tinc

- Frei und offen
- Verschlüsselung, Authentifikation und Kompression
- Mesh-Routing
- Leicht erweiterbar / skalierbar
- Switch- (Bridge) und Router-Modus (Layer 2 / 3)
- Portierbar

Kerneigenschaften von Tinc

- Frei und offen
- Verschlüsselung, Authentifikation und Kompression
- Mesh-Routing
- Leicht erweiterbar / skalierbar
- Switch- (Bridge) und Router-Modus (Layer 2 / 3)
- Portierbar

Kerneigenschaften von Tinc

- Frei und offen
- Verschlüsselung, Authentifikation und Kompression
- Mesh-Routing
- Leicht erweiterbar / skalierbar
- Switch- (Bridge) und Router-Modus (Layer 2 / 3)
- Portierbar

Kerneigenschaften von Tinc

- Frei und offen
- Verschlüsselung, Authentifikation und Kompression
- Mesh-Routing
- Leicht erweiterbar / skalierbar
- Switch- (Bridge) und Router-Modus (Layer 2 / 3)
- Portierbar

Unterschiede zu klassischen VPN-Lösungen

- Kein zentraler Server notwendig
- Keine zentrale Schlüsselverwaltung notwendig
- Sehr einfache, kompakte Konfiguration

Unterschiede zu klassischen VPN-Lösungen

- Kein zentraler Server notwendig
- Keine zentrale Schlüsselverwaltung notwendig
- Sehr einfache, kompakte Konfiguration

Unterschiede zu klassischen VPN-Lösungen

- Kein zentraler Server notwendig
- Keine zentrale Schlüsselverwaltung notwendig
- Sehr einfache, kompakte Konfiguration

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung eines Beispiel-Netzes

- Zweit-einfachstes Netzwerk aus 3 Hosts, mit einer Server-Rolle:
  - sun - Logischer Server
  - pluto - Netzwerkknoten 1
  - merkur - Netzwerkknoten 2
- IP-Adresse des Servers: 10.23.42.123
- IP-Netz des VPNs: 172.16.10.0/24
- VPN-Modus: Layer 2 (Ethernet)
- Netzwerkname: netz

Wichtig: Die Rolle des Servers spielt für Tinc keine Rolle. Wir nutzen sie nur, um einen Host mit einer festen, bekannten Adresse zu haben.
Wir gehen davon aus, dass die IP-Konfiguration der Interfaces schon erledigt ist und auf allen Hosts tinc installiert ist.

Einrichtung auf sun

```
# cat /etc/tinc/netz/tinc.conf
Mode = switch
Name = sun
Interface = tap0

# cat /etc/tinc/netz/hosts/sun
Address = 10.23.42.123
Subnet = 172.16.10.0/24
```

Einrichtung auf pluto

```
# cat /etc/tinc/netz/tinc.conf
Mode = switch
Name = pluto
Interface = tap0
ConnectTo = sun

# cat /etc/tinc/netz/hosts/pluto
Subnet = 172.16.10.0/24
```

Einrichtung auf merkur

```
# cat /etc/tinc/netz/tinc.conf
Mode = switch
Name = merkur
Interface = tap0
ConnectTo = sun

# cat /etc/tinc/netz/hosts/pluto
Subnet = 172.16.10.0/24
```

Erzeugung der Schlüssel

Auf allen Hosts:

```
# tinc -K -n netz
```

Danach /etc/tinc/netz/hosts/* auf allen Hosts synchronisieren.

Fertig!

Funktionalität des Beispiel-Netzes

- Volle Ethernet-Konnektivität
- Authentifikation, Verschlüsselung, Kompression
- Mesh-Routing und mehr

Funktionalität des Beispiel-Netzes

- Volle Ethernet-Konnektivität
- Authentifikation, Verschlüsselung, Kompression
- Mesh-Routing und mehr

Funktionalität des Beispiel-Netzes

- Volle Ethernet-Konnektivität
- Authentifikation, Verschlüsselung, Kompression
- Mesh-Routing und mehr

Mesh-Routing und Erweiterung

- Neue Hosts hinzufügen ist sehr einfach
- Server-Verbindung (ConnectTo) ist nur ein vorgegebener, fixer Kontrollkanal
- Tinc findet automatisch die beste Route durch das eigene Netz von Knoten zu Knoten
  - Wenn öffentliche Adressen von mehreren Knoten bekannt sind, werden redundante Verbindungen aufgebaut und der beste Pfad ermittelt
  - LocalDiscovery (optional) - Tinc ermittelt per (authentifiziertem) Broadcast, ob Knoten im selben darunterliegenden LAN erreichbar sind (Beispiel: Notebooks im selben WLAN) und baut dann automatisch direkte Verbindungen auf.

Mesh-Routing und Erweiterung

- Neue Hosts hinzufügen ist sehr einfach
- Server-Verbindung (ConnectTo) ist nur ein vorgegebener, fixer Kontrollkanal
- Tinc findet automatisch die beste Route durch das eigene Netz von Knoten zu Knoten
  - Wenn öffentliche Adressen von mehreren Knoten bekannt sind, werden redundante Verbindungen aufgebaut und der beste Pfad ermittelt
  - LocalDiscovery (optional) - Tinc ermittelt per (authentifiziertem) Broadcast, ob Knoten im selben darunterliegenden LAN erreichbar sind (Beispiel: Notebooks im selben WLAN) und baut dann automatisch direkte Verbindungen auf.

Mesh-Routing und Erweiterung

- Neue Hosts hinzufügen ist sehr einfach
- Server-Verbindung (ConnectTo) ist nur ein vorgegebener, fixer Kontrollkanal
- Tinc findet automatisch die beste Route durch das eigene Netz von Knoten zu Knoten
  - Wenn öffentliche Adressen von mehreren Knoten bekannt sind, werden redundante Verbindungen aufgebaut und der beste Pfad ermittelt
  - LocalDiscovery (optional) - Tinc ermittelt per (authentifiziertem) Broadcast, ob Knoten im selben darunterliegenden LAN erreichbar sind (Beispiel: Notebooks im selben WLAN) und baut dann automatisch direkte Verbindungen auf.

Mesh-Routing und Erweiterung

- Neue Hosts hinzufügen ist sehr einfach
- Server-Verbindung (ConnectTo) ist nur ein vorgegebener, fixer Kontrollkanal
- Tinc findet automatisch die beste Route durch das eigene Netz von Knoten zu Knoten
  - Wenn öffentliche Adressen von mehreren Knoten bekannt sind, werden redundante Verbindungen aufgebaut und der beste Pfad ermittelt
  - LocalDiscovery (optional) - Tinc ermittelt per (authentifiziertem) Broadcast, ob Knoten im selben darunterliegenden LAN erreichbar sind (Beispiel: Notebooks im selben WLAN) und baut dann automatisch direkte Verbindungen auf.

Mesh-Routing und Erweiterung

- Neue Hosts hinzufügen ist sehr einfach
- Server-Verbindung (ConnectTo) ist nur ein vorgegebener, fixer Kontrollkanal
- Tinc findet automatisch die beste Route durch das eigene Netz von Knoten zu Knoten
  - Wenn öffentliche Adressen von mehreren Knoten bekannt sind, werden redundante Verbindungen aufgebaut und der beste Pfad ermittelt
  - LocalDiscovery (optional) - Tinc ermittelt per (authentifiziertem) Broadcast, ob Knoten im selben darunterliegenden LAN erreichbar sind (Beispiel: Notebooks im selben WLAN) und baut dann automatisch direkte Verbindungen auf.

Weitere Features, die interessant sind

- Einladungen - neue Hosts per E-Mail / URL mit einem Kommando ins VPN einladen
- Local Discovery - Hosts und Pfade im selben Lan finden
- Router-Mode (Layer 3)
- Tunnel-Server - traditionelles, zentralisiertes VPN
- Betrieb mit sslh (z.B. auf Port 443)
- Hook-Scripts (-up, -down, ...)

Weitere Features, die interessant sind

- Einladungen - neue Hosts per E-Mail / URL mit einem Kommando ins VPN einladen
- Local Discovery - Hosts und Pfade im selben Lan finden
- Router-Mode (Layer 3)
- Tunnel-Server - traditionelles, zentralisiertes VPN
- Betrieb mit sslh (z.B. auf Port 443)
- Hook-Scripts (-up, -down, ...)

Weitere Features, die interessant sind

- Einladungen - neue Hosts per E-Mail / URL mit einem Kommando ins VPN einladen
- Local Discovery - Hosts und Pfade im selben Lan finden
- Router-Mode (Layer 3)
- Tunnel-Server - traditionelles, zentralisiertes VPN
- Betrieb mit sslh (z.B. auf Port 443)
- Hook-Scripts (-up, -down, ...)

Weitere Features, die interessant sind

- Einladungen - neue Hosts per E-Mail / URL mit einem Kommando ins VPN einladen
- Local Discovery - Hosts und Pfade im selben Lan finden
- Router-Mode (Layer 3)
- Tunnel-Server - traditionelles, zentralisiertes VPN
- Betrieb mit sslh (z.B. auf Port 443)
- Hook-Scripts (-up, -down, ...)

Weitere Features, die interessant sind

- Einladungen - neue Hosts per E-Mail / URL mit einem Kommando ins VPN einladen
- Local Discovery - Hosts und Pfade im selben Lan finden
- Router-Mode (Layer 3)
- Tunnel-Server - traditionelles, zentralisiertes VPN
- Betrieb mit sslh (z.B. auf Port 443)
- Hook-Scripts (-up, -down, ...)

Weitere Features, die interessant sind

- Einladungen - neue Hosts per E-Mail / URL mit einem Kommando ins VPN einladen
- Local Discovery - Hosts und Pfade im selben Lan finden
- Router-Mode (Layer 3)
- Tunnel-Server - traditionelles, zentralisiertes VPN
- Betrieb mit sslh (z.B. auf Port 443)
- Hook-Scripts (-up, -down, ...)

Vielen Dank für eure Teilnahme!
Für weitere Fragen, Anregungen, etc.:
Website: `http://www.dominik-george.de`
E-Mail / Jabber: nik@naturalnet.de