Fachhochschule Südwestfalen
Hochschule für Technik und Wirtschaft
University of Applied Sciences

citkomm
wir wirken wirklich

IPv6 als Basis für IPSec gestützte native Applikationsabsicherung

Autor: Marcel Vollmer
Tobias Hebmüller

Version:

Projektidee

- IPSec wurde zunächst für IPv6 standardisiert. IPv4-Implementierung ist back-port aus IPv6
- Hypothese: IPSec mit IPv6 bietet höheres Potential durch mehr Funktionen
  - Ziel: Einfache Verschlüsselung von Netzen unter IPv6
- Prüfung im Rahmen von Projektarbeiten in Zusammenarbeit mit Werksstudenten der FH-SWF

Fachhochschule Südwestfalen
Hochschule für Technik und Wirtschaft
University of Applied Sciences

- Prof. Dr. Michael Rübsam

- Martin Krengel
- Gerold Gruber

Agenda

- Gefahren eines unverschlüsselten LAN
- Einblick in IPSec im Transportmodus
- Vorteil - Transportmodus über IPv6
- Erhöhung der Sicherheit durch Zertifikate
- Voruntersuchungen
- Aktuelle Aufgabenstellung
- Möglichkeiten in Windows
- Umsetzung in einem Forest
- Ansätze in Linux

Gefahren eines unverschlüsselten LAN

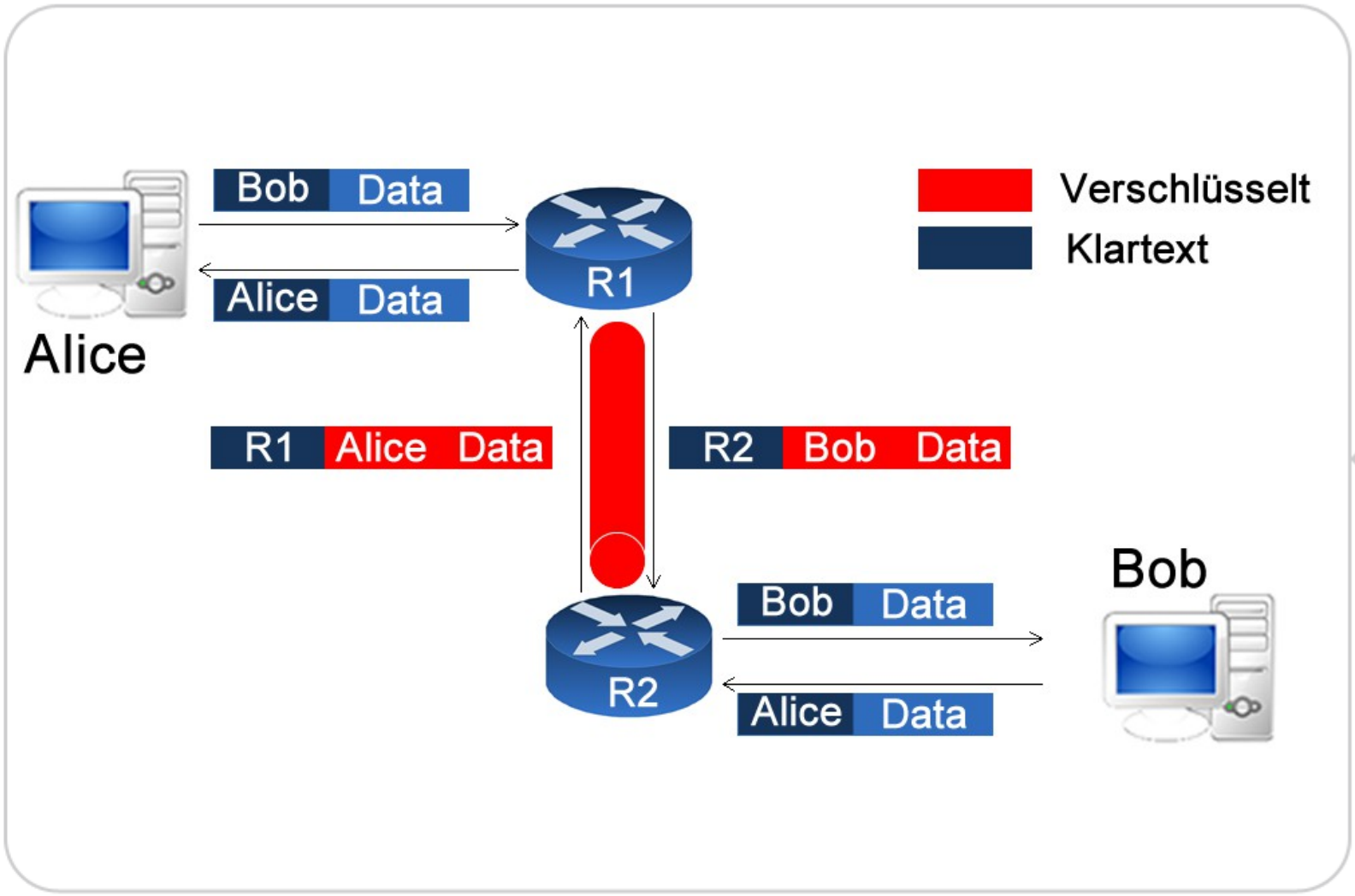
- Daten zwischen zwei Clients im Klartext
- Potential für Man-in-the-Middle Szenarien
- Stören der Netzwerkverbindungen
- Mitlesen von Client-seitig unverschlüsselten E-Mails

Mehr Sicherheit via IP-Sec im Transportm.

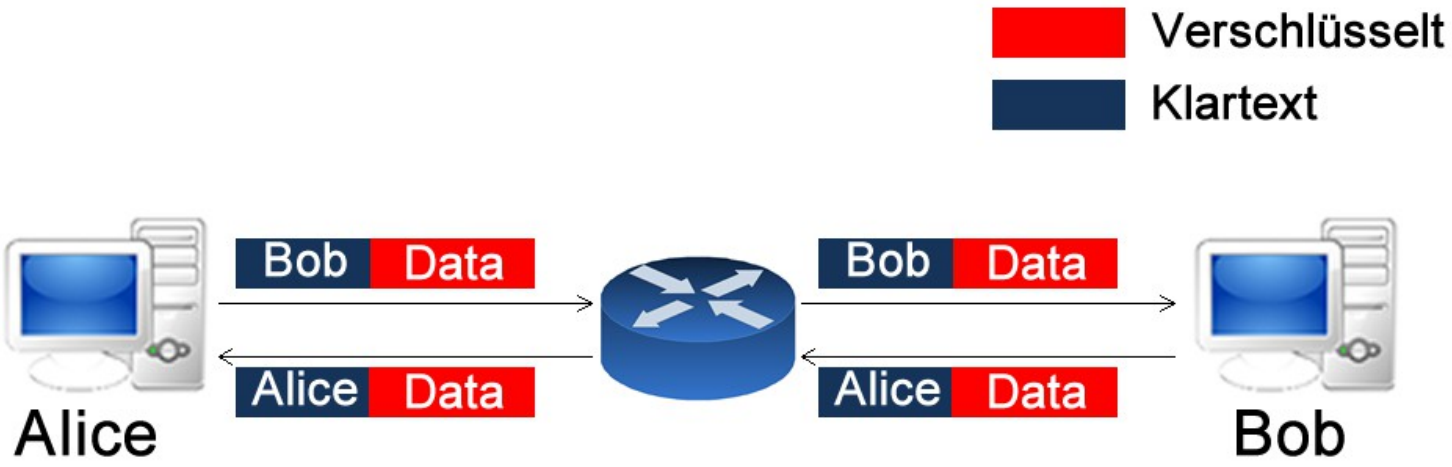
citkomm
wir wirken wirklich

- IPSec bietet Methoden zur Sicherstellung der:
  - Authentizität, Integrität – Authentication Header (AH)
  - Vertraulichkeit – Encapsulated Security Payload (ESP)
- Anwendungen > OSI-Layer 3 kommunizieren verschlüsselt
- Authentifizierung über Pre Shared Key (PSK) oder Zertifikat
- 2 Modi
  - Tunnelmodus
  - Transportmodus

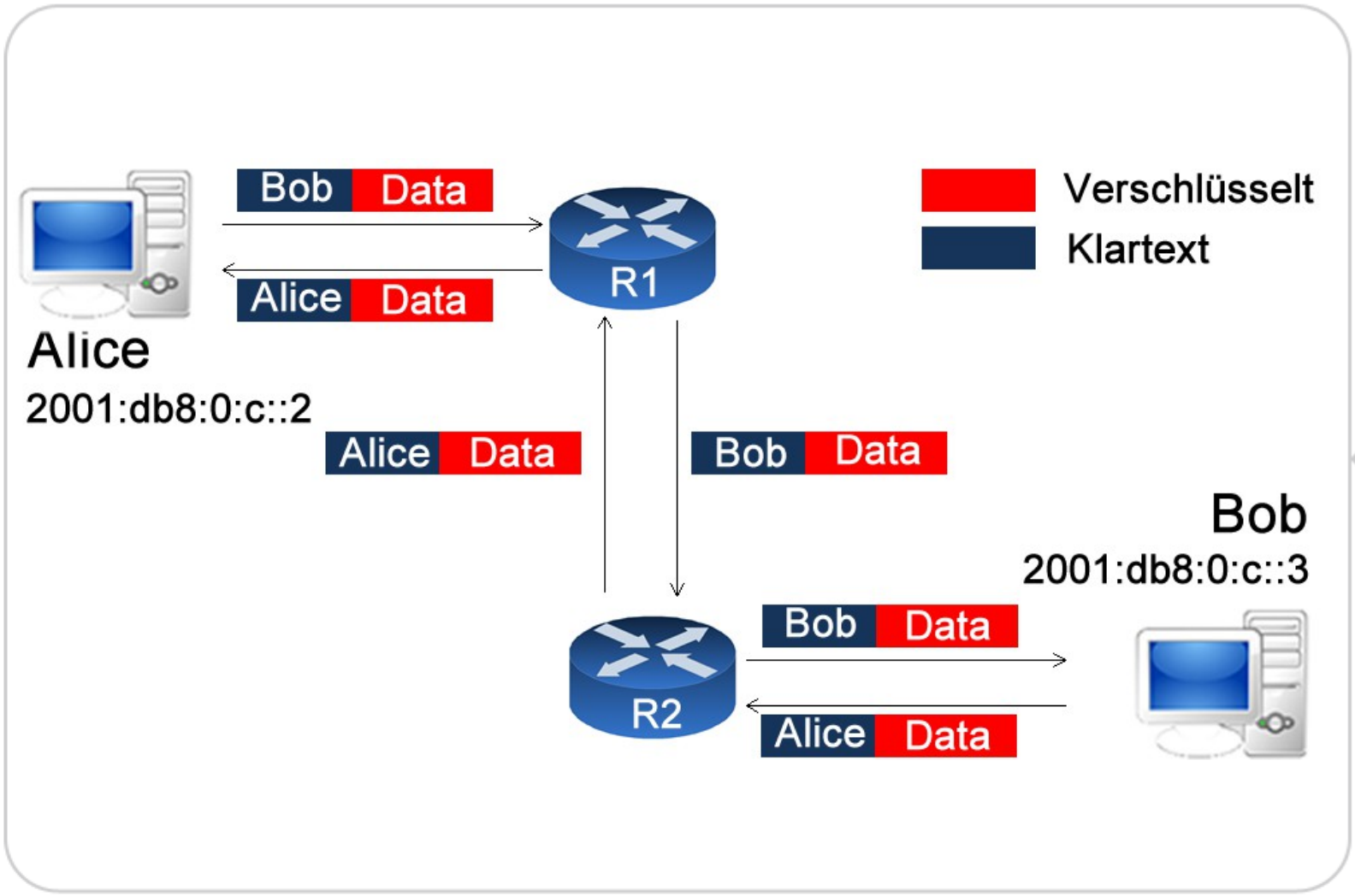
Tunnelmodus



Transportmodus



Vorteil - Transportmodus über IPv6



Vorteile durch X.509 Zertifikate

- Authentizitätsdaten im Gegensatz zum PSK nicht einsehbar.
- Individuelle Identität des Computers
- Durch Verwendung von Computerzertifikaten, benutzerunabhängig.

Projektuntersuchungen

Voruntersuchungen

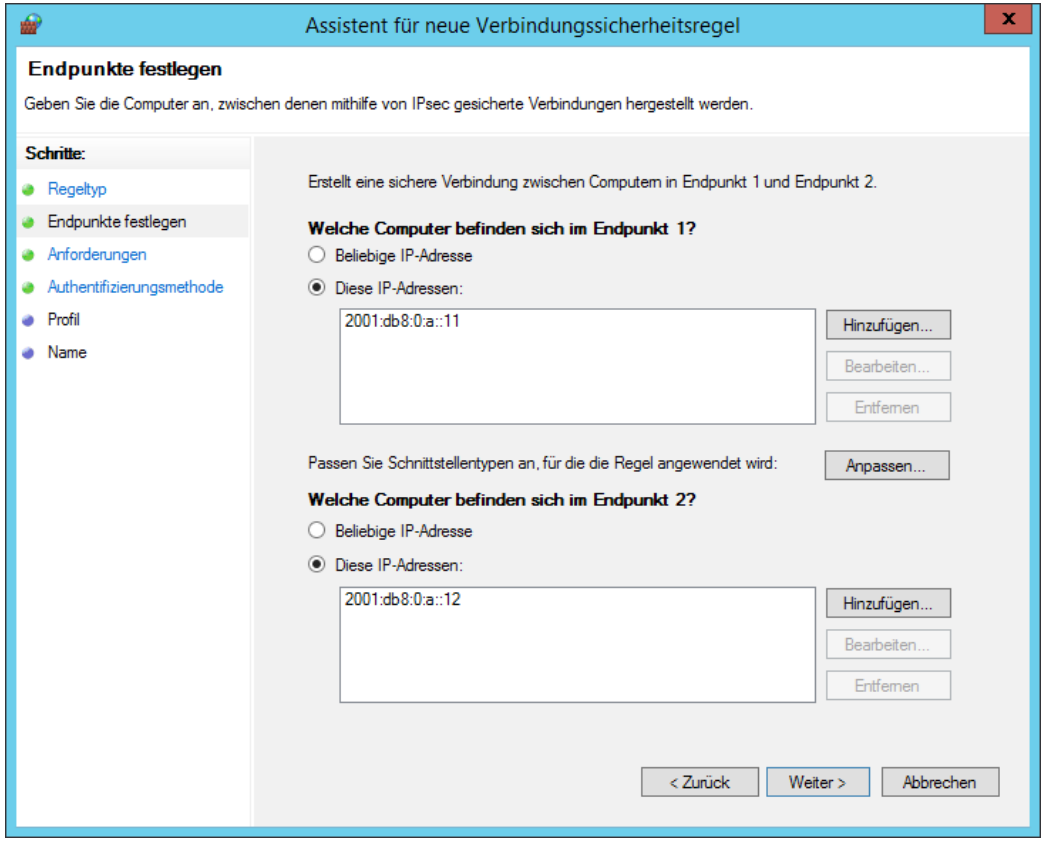
- Erste Untersuchung
  - IPSec im Tunnelmodus weit verbreitet
    - Implementierung für IPv4 und IPv6 einheitlich
  - Implementierung Transportmodus nicht erkennbar
- Folgeuntersuchung
  - IPSec im Transportmodus existiert
    - Kaum dokumentierte Implementierungen
  - IPSec Transportmodus ist für Windows möglich

Aktuelle Aufgabenstellung

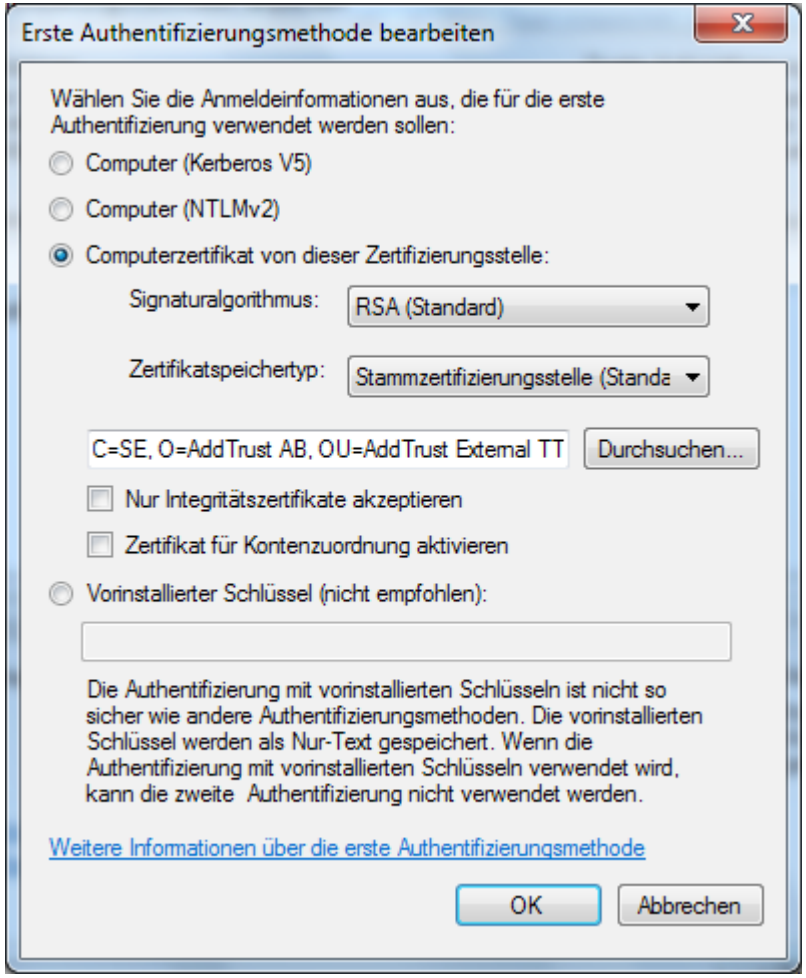
- Ist eine Authentifizierung mittels X.509 Zertifikat möglich?
- Ist eine solche Authentifizierung in einem Windows Forest möglich?
- Ist es möglich, in die Authentifizierung ebenso Linux-Systeme einzubinden?

Möglichkeiten in Windows

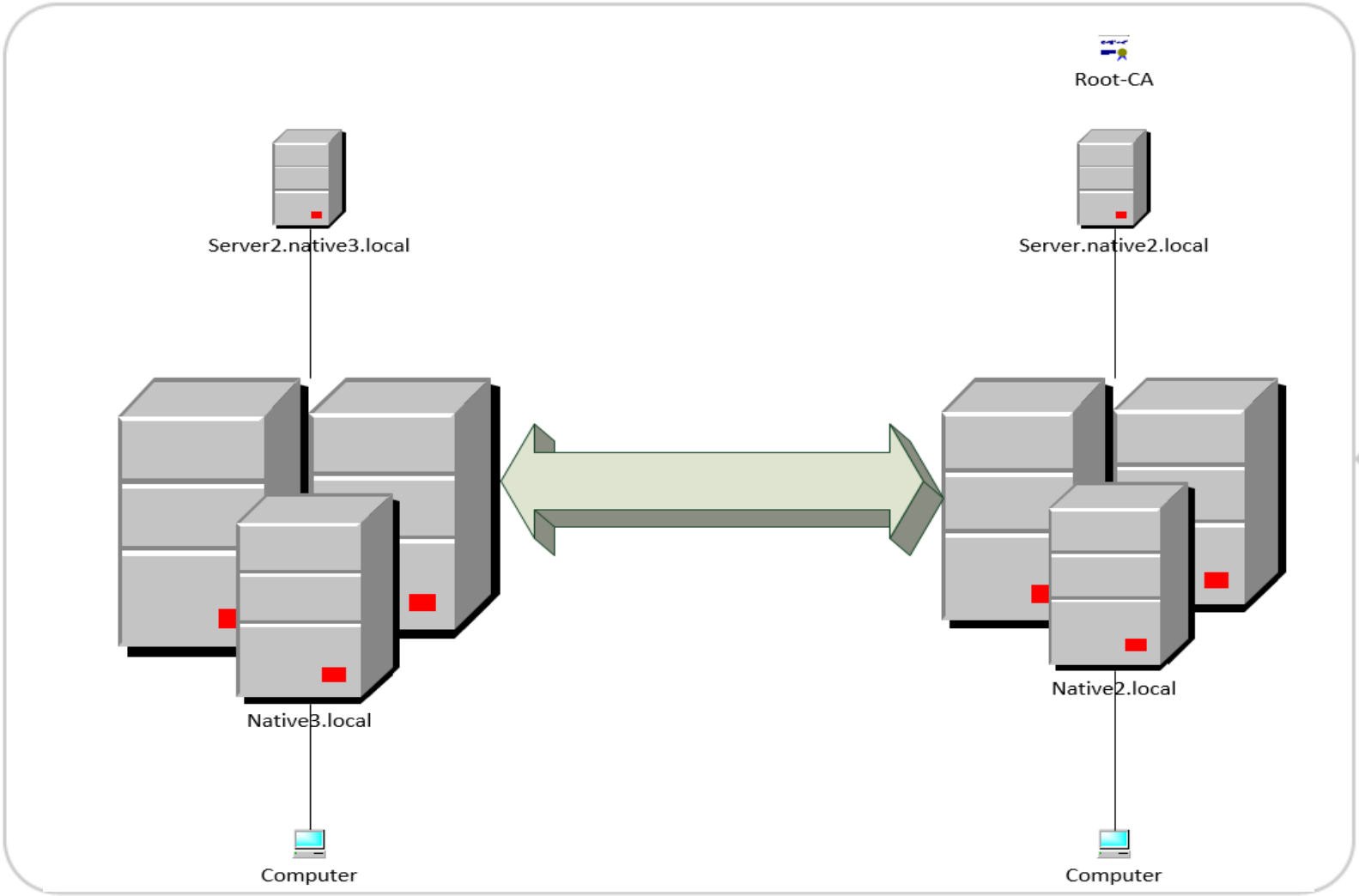
- Durch die Verbindungssicherheitsregeln der FW



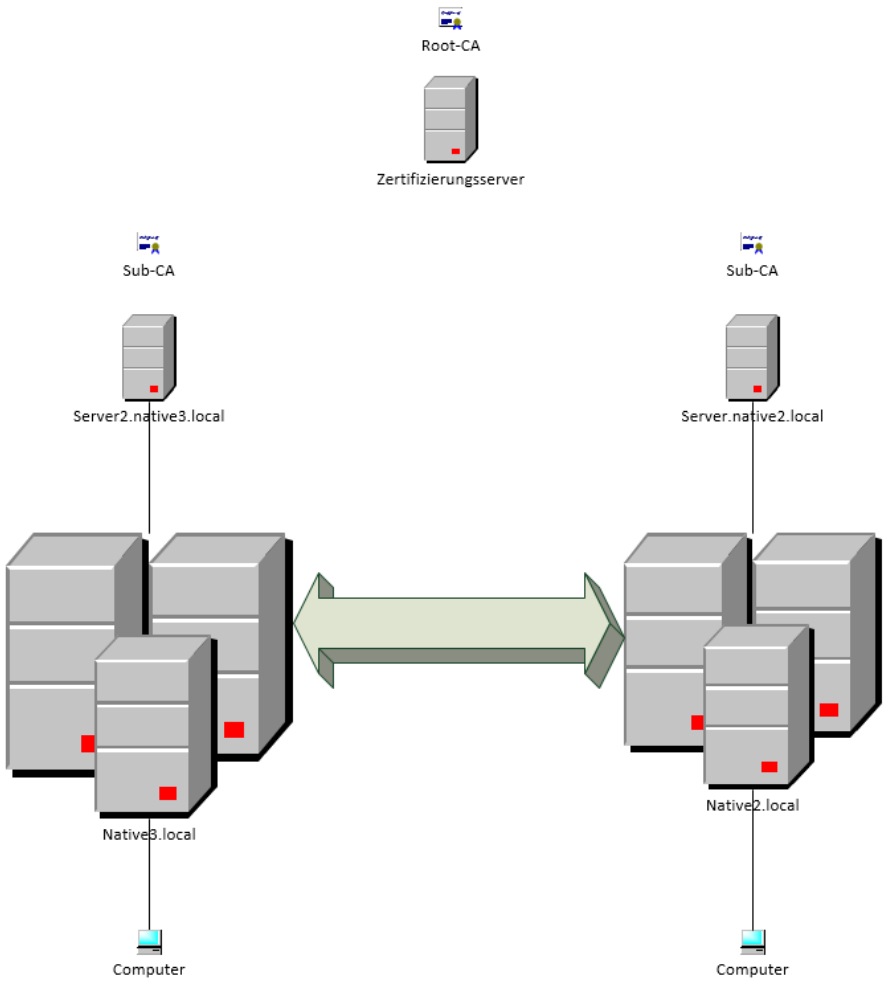
Möglichkeiten in Windows



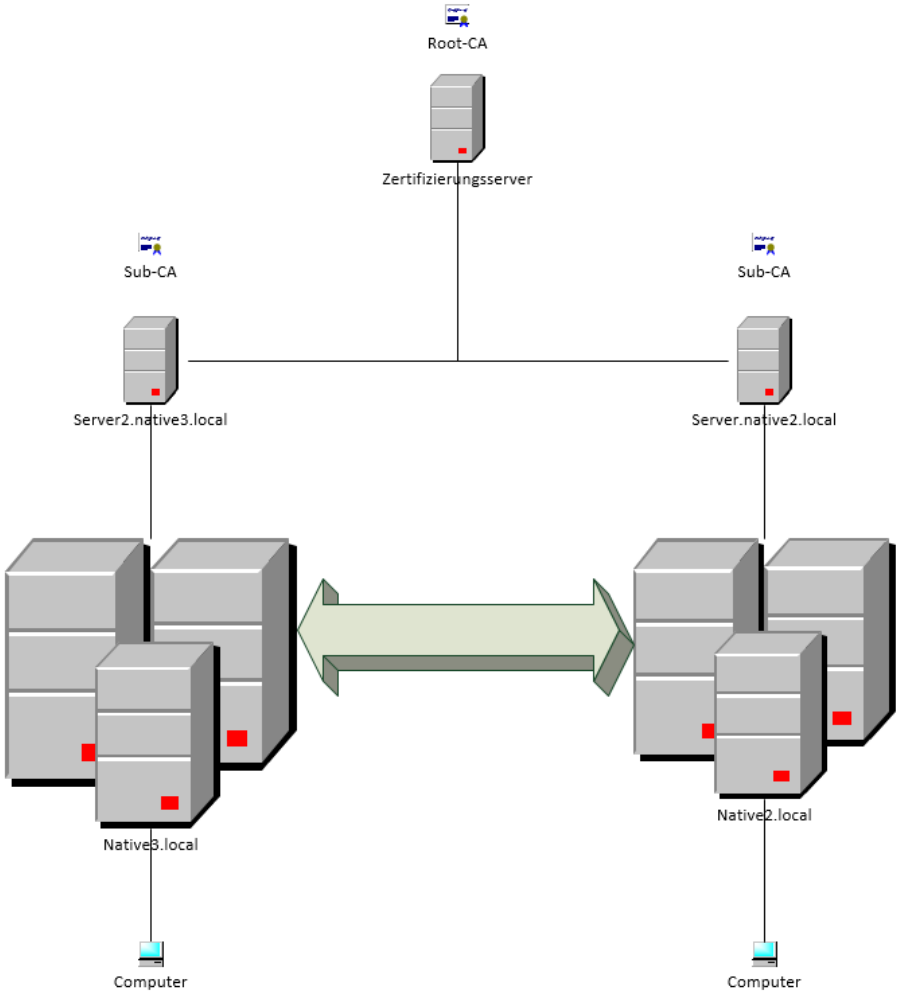
Zwei Domänen mit bidirektionaler Vertrauensstellung, ein AD CS



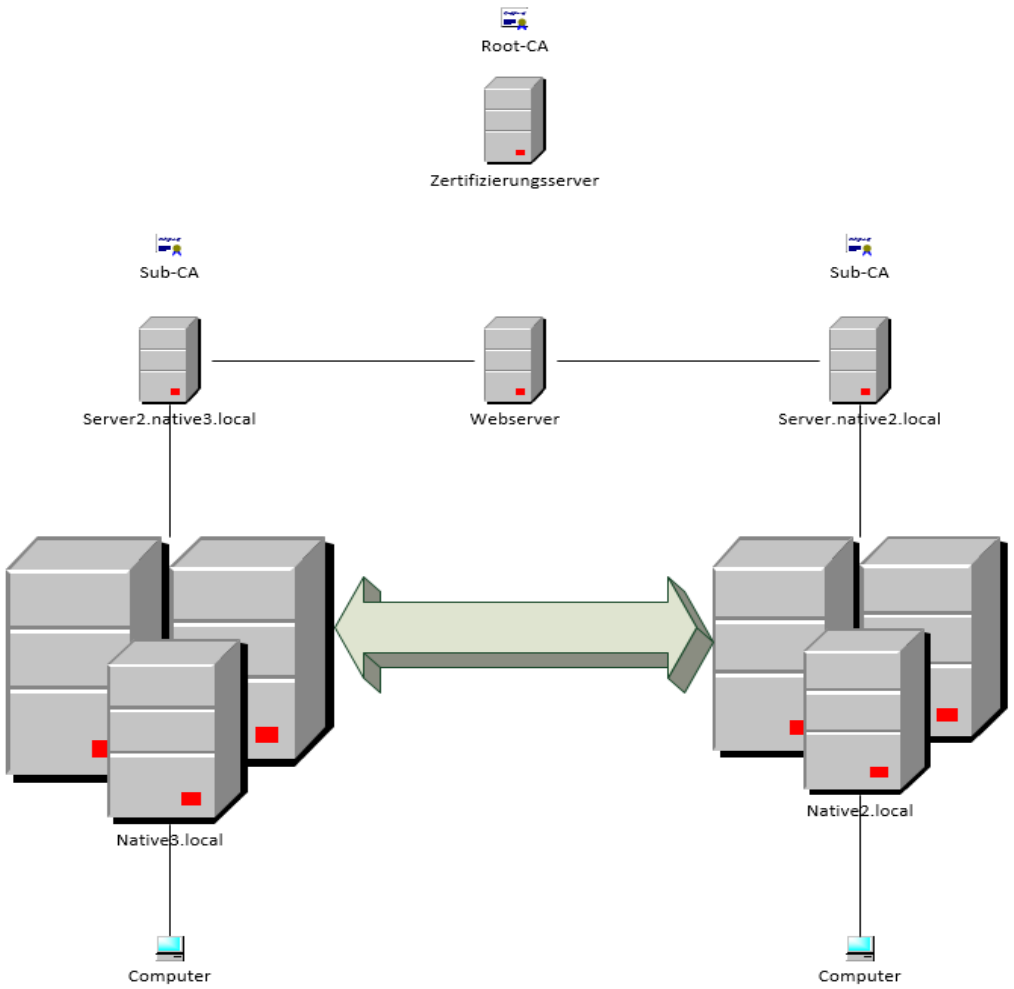
Zwei AD CS in einer Domäne + Offline Stammzertifizierungsstelle



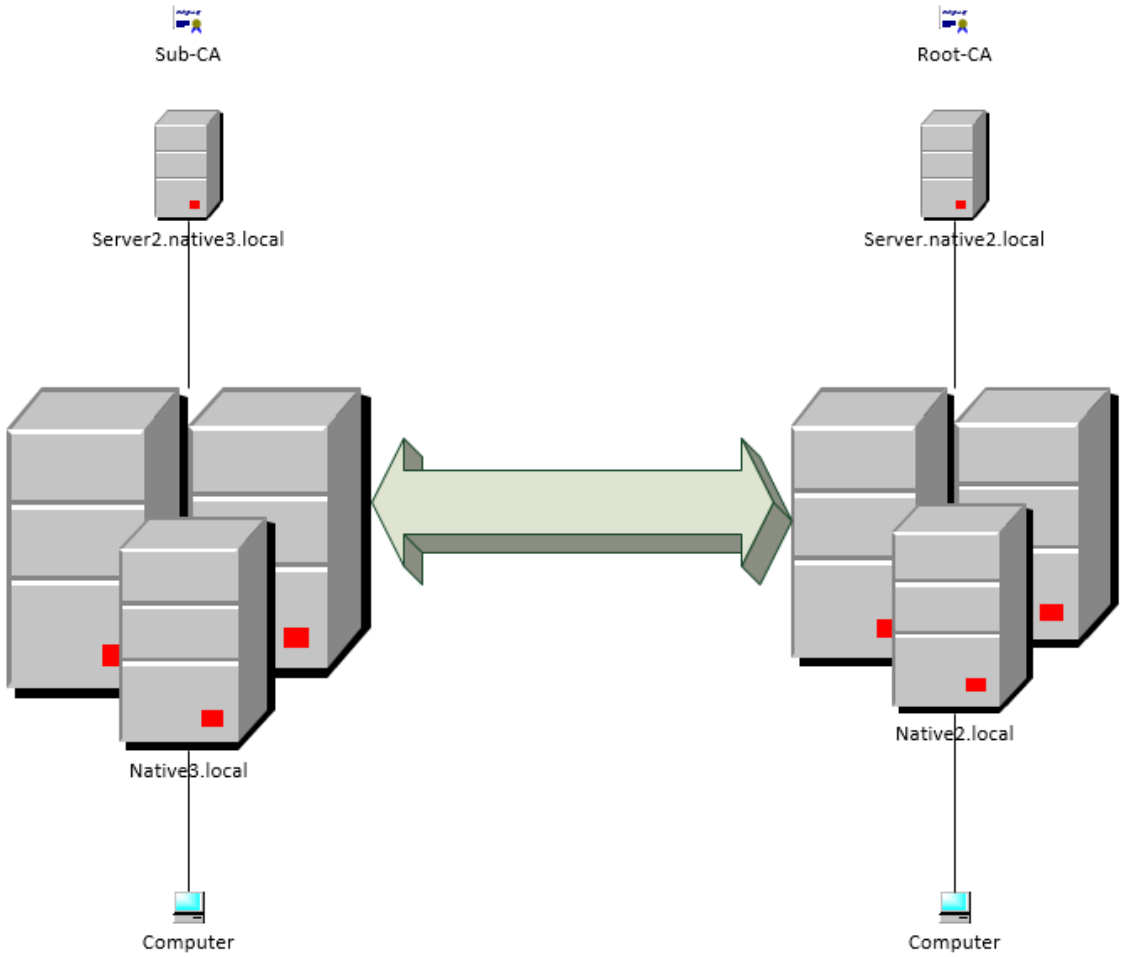
Zwei AD CS in einer Domäne + Online Stammzertifizierungsstelle



Zwei AD CS in Domäne + Offline Stammzertifizierungsstelle + Webserver



Stammzertifizierungsstelle und Unterzertifizierungsstelle im Active Directory



Möglichkeiten in Linux

- Strongswan realisiert die Umsetzung von IPSec
  - Konfiguration über die Dateien ipsec.conf und ipsec.secrets
- TinyCA erzeugt und signiert die Zertifikate
  - Erstellung von Certificate Signing Request (CSR) für Windows AD-CS
- Betrieb von Linux und Windows möglich
  - PSK
  - Zertifikate

Reflexion

- IPSec ist im Transportmodus möglich
- IPSec im Transportmodus bietet in Verbindung mit IPv6 höheres Potential –
  Wegfall der NAT-Problematik
- IPSec ermöglicht die Authentifizierung mittels X.509 Zertifikaten
- Die Funktionalität ist auf einen Forest abbildbar
- Windows und Linux können gegenseitig authentifiziert werden

Vielen Dank für Ihre Aufmerksamkeit

FRAGEN?

Ihr Ansprechpartner:

www.citkomm.de