

4. Netzwerksicherheit

Teil 5: Remote Access Service

Universitatea “Transilvania” din Brasov



Agenda

4.1 Firewall

4.2 Virtual Private Network

4.3 Ipsec

4.4 SSL und TLS

4.5 Remote Access Service

4.5.1 Virtual LAN

4.5.2 Protokoll RADIUS

4.5.3 WLAN



Remote Access und Virtual LAN

- Der Begriff Remote Access Service (RAS) ist eng mit dem Internet verbunden.
- Remote Access Netzwerke stellen die Infrastruktur dar, welche den Zugriff von mobilen Benutzern oder kleineren Firmenniederlassungen auf die Unternehmensressourcen ermöglicht. Es entsteht ein einheitliches virtuelles Firmennetzwerk (VLAN).
- Durch diese VLAN wird das dezentrale Arbeiten durch Ansätze wie Telearbeitsplätze, Heimarbeitsplätze und Home Office ermöglicht, da jeder Mitarbeiter zu allen angebotenen Ressourcen Zugriff hat. Sie können so vollständig in das Unternehmensnetz integriert werden.



Remote Access und Virtual LAN

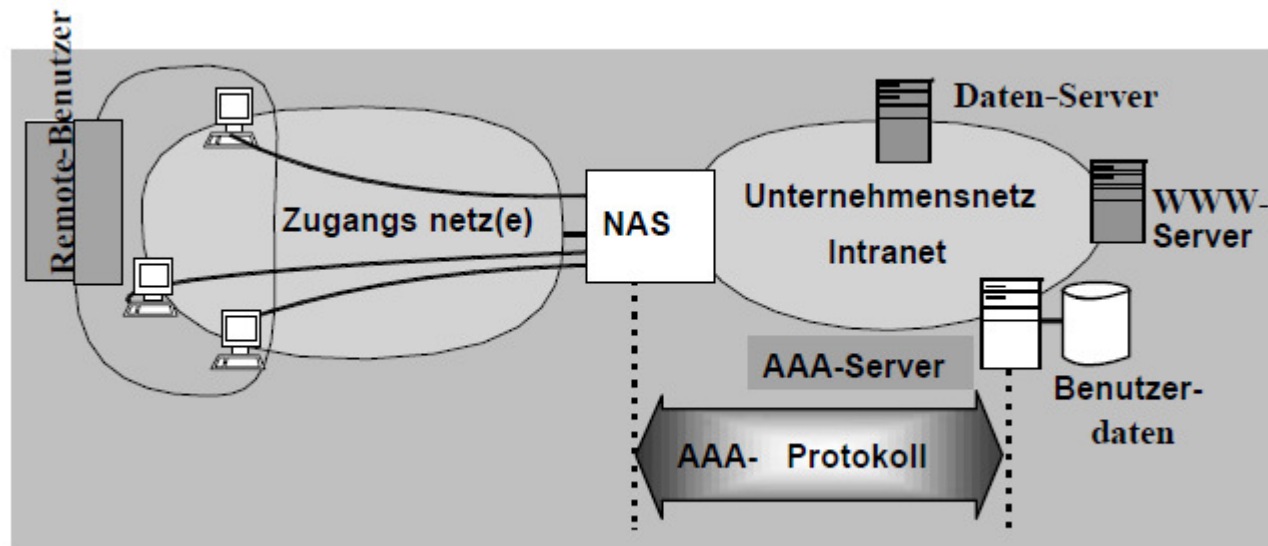
- Mit RAS ist es möglich, ein Unternehmensnetz räumlich uneingeschränkt zu erweitern.
- Man unterscheidet zwei Arten von Remote Access Service:
 - **Dial-In Zugang**, falls der Zugang von einem Remote-Benutzer auf das LAN erfolgt
 - **Dial-Out Zugang**, falls eine Verbindung aus dem LAN zu einem Remote-Benutzer initiiert wird



Remote Access und Virtual LAN

- In großen Unternehmensnetzen ist die Anzahl von Remote-Benutzern so groß, dass es sinnvoll ist, die Funktionen:
 - Authentifizierung (Wer ist das?)
 - Autorisierung (Was darf derjenige?)
 - Accounting (Was hat derjenige genutzt?)zu zentralisieren.
- Eine Trennung von NAS (Network Access Server) ist dabei sinnvoll.
- Dies wird von speziellen dedizierten Servern im Unternehmensnetz übernommen. Ein solcher Server wird oft als AAA-Server bezeichnet. Die nachfolgende Abbildung zeigt den Einsatz eines dedizierten AAA-Servers.

Remote Access und Virtual LAN

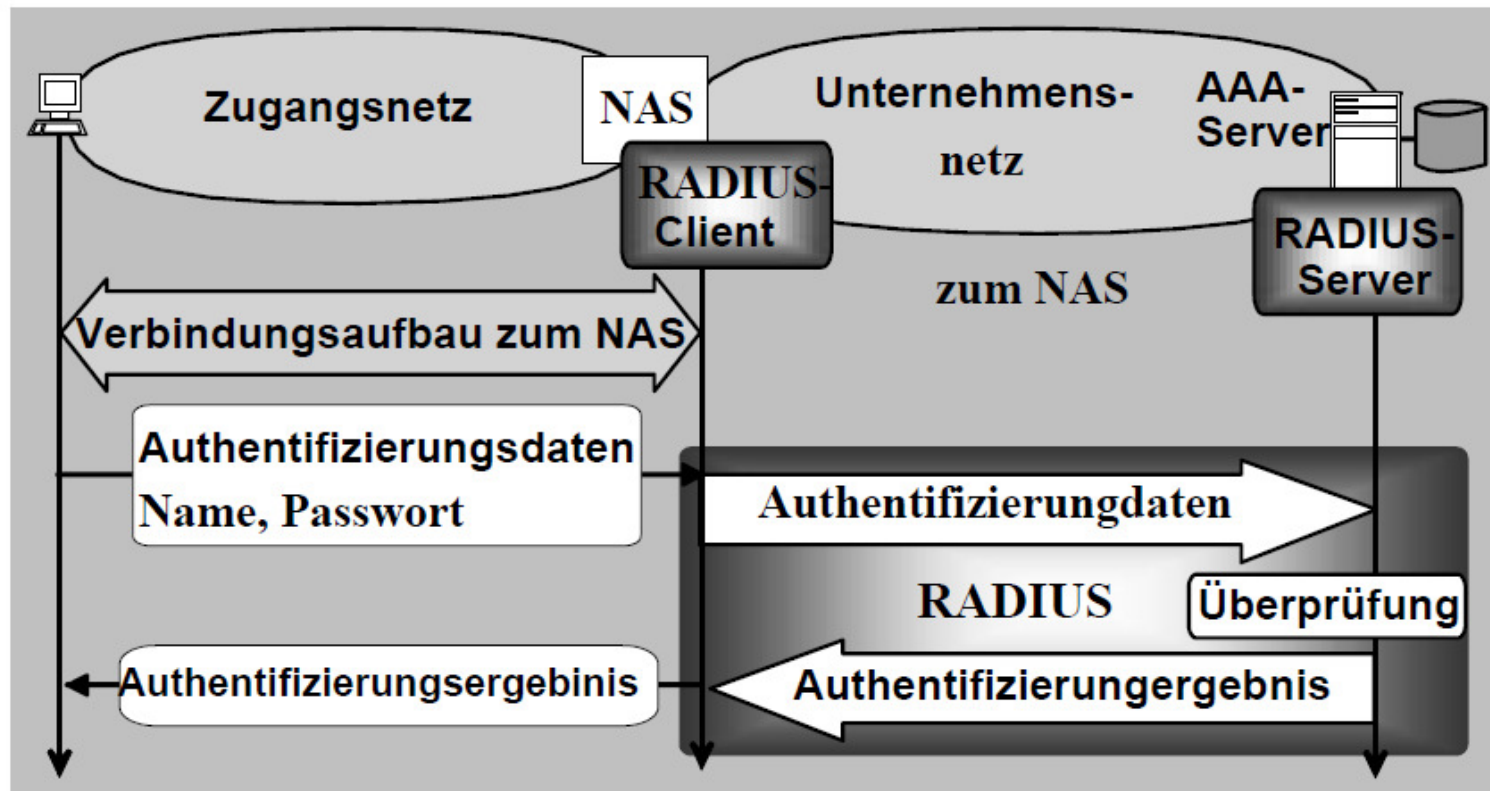




Remote Access Dial-in User Service (RADIUS)

- Das Protokoll RADIUS funktioniert nach dem Client/Server-Konzept und legt die Kooperation zwischen einem NAS und einem AAA-Server fest.
- Der RADIUS-Server kann als ein AAA-Server gesehen werden, in dem sämtliche Informationen über Remote-Benutzer zur Verfügung stehen.
- Der RADIUS-Client stellt ein Funktionsmodul dar, das auf dem NAS installiert wird.

Remote Access Dial-in User Service (RADIUS)



RADIUS unterstützt PAP und CHAP vom Protokoll PPP.
RADIUS ist auch Bestandteil von Windows 2000.



Remote Access Dial-in User Service (RADIUS)

- ❑ Wählt sich ein Remote-Benutzer auf dem NAS ein, muss er dabei seine Kennung und sein Passwort übergeben. Der RADIUS-Client im NAS schickt diese Informationen zum RADIUS-Server, der auf Basis seiner Datenbank die Berechtigungen für diesen Benutzer überprüft.
- ❑ Um die Zugriffe des Benutzers zu steuern, wird ein Profil dieses Benutzers in den NAS geladen.
- ❑ Die Übertragung von Daten zwischen RADIUS-Client und RADIUS-Server erfolgt verschlüsselt durch symmetrische Verschlüsselung.