IPsec als Beispiel für symetrische und asymetrische Verschlüsslungsverfahren

Gliederung

- Einführung eines VPN, Anforderungen und Entscheidung für IPsec
- technische Aspekte von IPsec
- Erweiterungen

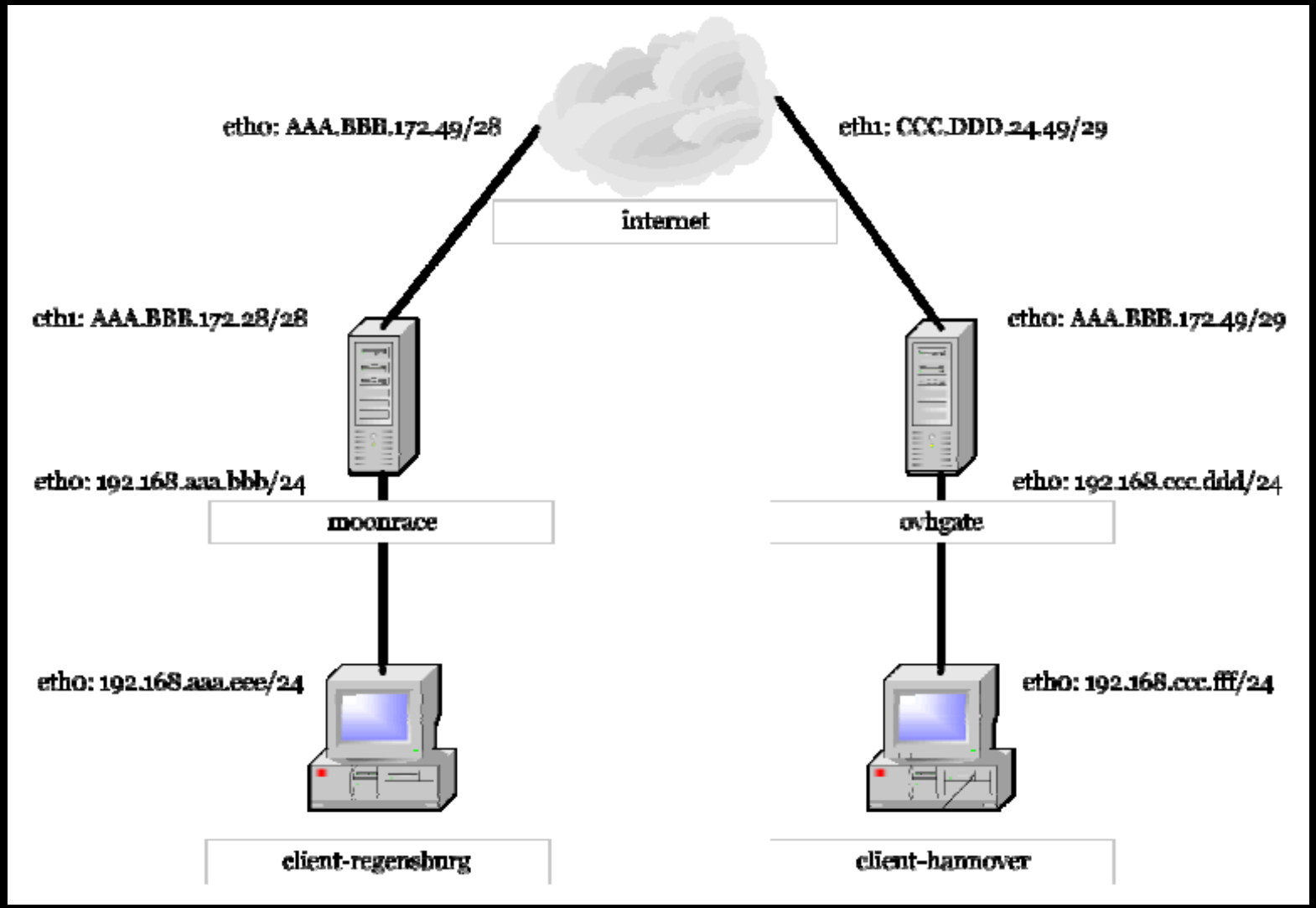
Einführung

- Aussenstellen in aller Welt
- Kommunikation chaotisch
- => Verbindung über ein VPN

Anforderungen

- Diskretion und Integrität der Daten
- Verlässlichkeit
- geringer Overhead
- Wartbarkeit und Einfachkeit
- Flexibilität und Erweiterbarkeit

technische Abläufe



ISAKMP zum Schlüsselaustausch

- asymetrisch, rechenintensiv
- Pre-Shared-Keys, Signaturen oder X.509-Zertifikate möglich
- Triple-DES, u. a. möglich
- Ziel: Aushandeln eines Sitzungsschlüssels für die nächste Phase

Verschlüsseln der Nutzdaten

- symetrisch, weniger rechenintensiv
- ESP oder AH-Betriebsart
- Komprimierung optional

Erweiterungen

- Einbinden von Windows-Rechnern mit X.509-Zertifikaten
- zentrale Administration von Regensburg aus (Single-Sign-On)
- Voice over IP

noch was?

- Fragen!
- weitergehende Informationen:
  - http://www.gerald-able.de
  - http://www.antioffline.com/ipsec/rfc/
- Vielen Dank für die Aufmerksamkeit!