



**secunet Security Networks AG**

# **IPv6 in Hochsicherheitsumgebungen**

## **Probleme und Lösungsansätze**

Potsdam, 15.5.2009

Hans-Markus Krüger, Dr. Kai Martius

---

## Das Unternehmen im Überblick

- Der führende deutsche Spezialist für komplexe IT-Sicherheitslösungen
- Sicherheitspartner der Bundesrepublik Deutschland
- Umfassende Kompetenz – kundennah
  - 4 Geschäftsbereiche
  - 7 Standorte in D, Tochterunternehmen in CH und CZ
  - 260 hoch qualifizierte Mitarbeiter
- secunet Security Networks AG
  - Gegründet 1996, börsennotiert seit 1999
  - Umsatz 2008: ca. 50 Mio. Euro
  - Anteilseigner: G&D 50 % + 1 Aktie, RWTÜV 26,4 %
- Geschäftsbereich Hochsicherheit mit Fokus auf Produkte für Behörden und Militär zugelassen für höchste Sicherheitsanforderungen





## Produktlinie

---

- **SINA Box**  
VPN-Gateway auf Basis IPsec / IKE zur Übertragung klassifizierter Informationen (GEHEIM / SECRET) über offene Netze (bspw. Das Internet)
  
- **SINA Thin Client**  
Client-Arbeitsplatz zur Verarbeitung und Übertragung unterschiedlich klassifizierter Informationen in Terminalserver-Umgebungen (ICA, RDP, X11)
  
- **SINA Virtual Workstation**  
Workstation zur Verarbeitung und Übertragung unterschiedlich klassifizierter Informationen in verschiedenen lokalen Sessions (virtualisierte Windows-® oder Linux-Instanzen)
  
- **SINA Management**  
centralized cryptographic management and configuration station
  
- **SINA L2**  
Layer-2-Verschlüsselungsprodukte (Ethernet, SDH, Fibre Channel) bis 10 GE

## IPv6: Anforderungen / Hindernisse

---

- Zunehmende Kundenforderungen nach IPv6-Tauglichkeit
    - Konkrete Netzplanungen („Netze des Bundes“, „Deutschland Online Infrastruktur“)
  - Tatsächlich sogar Vorreiterrolle unserer Kunden zu erkennen
  - Neue technologische Herausforderung im Hochsicherheitsumfeld
    - „Feature Rich“ ← → Security / minimaler Funktionsumfang
    - Praxistests fehlen
    - Hohe Aufwände für Evaluierung / Zulassung durch Nachweis von Sicherheitseigenschaften bzw. Funktionstrennung
- Neue Systemarchitekturen erforderlich

## IPv6: Sicherheitskriterien (1)

---

### ■ Extension Header

- Schlechtere Filterbarkeit von Headerinformationen
- Alternative: Einschränkung von Funktionalität

### ■ ICMPv6

- Ende-zu-Ende-Nutzung (bspw. PMTU Discovery) erfordert zusätzliche Sicherheitsfunktionalität auf Gateways (Filter / Mapping)
- Starke Abhängigkeit von ICMP für Flusssteuerung (Fehlermeldungen, Adresszuweisung, Discovery-Funktionen)

### ■ Ende-zu-Ende-Adressierung

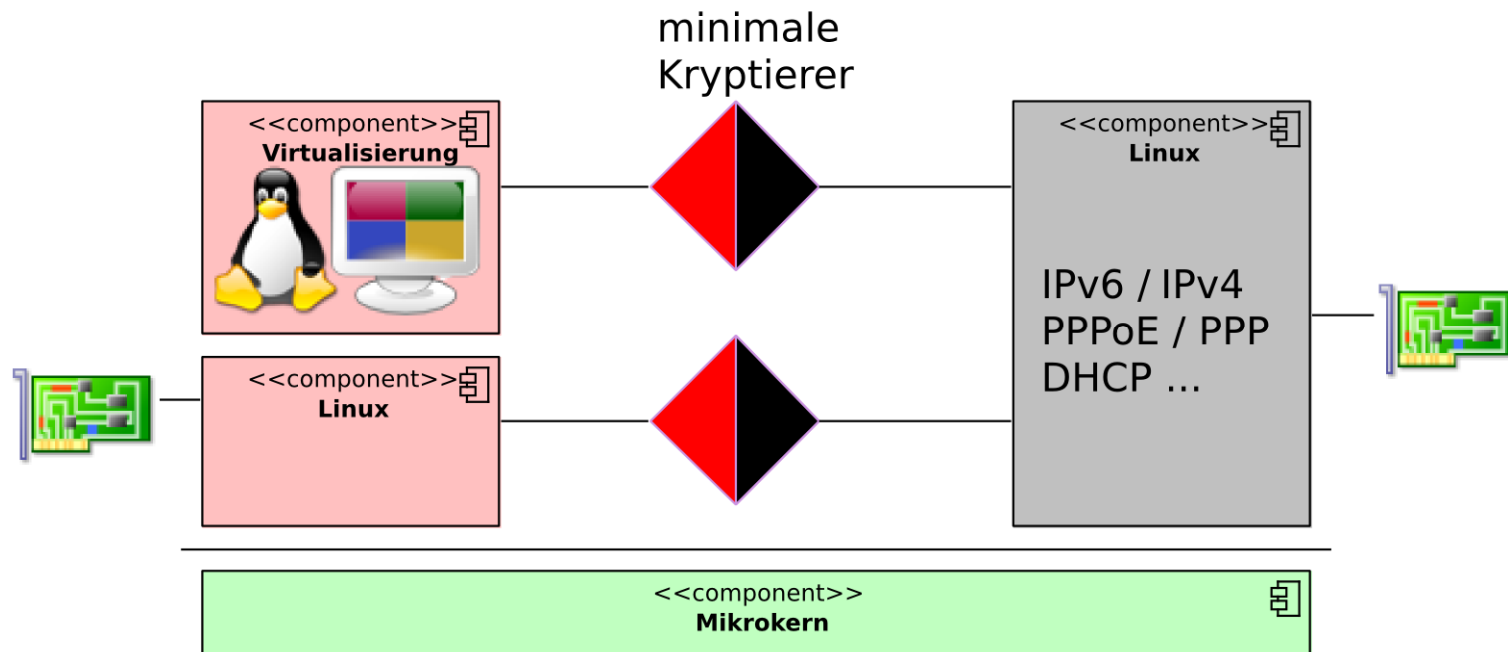
- (vermeintliche) Sicherheit durch NAT und/oder Tunneling geht verloren (Anwendersicht)

## IPv6: Sicherheitskriterien (2)

---

- Breite Einsatzerfahrung im Feld fehlt → Bugs (sehr) wahrscheinlich
  - Erfahrungen selbst mit aktuellsten Linux-Kerneln bestätigen das
  
- Generell wenig Erfahrung bei Nutzern und Administratoren
  - Hohes Fehlbedienungspotential

# Lösungsansätze für Hochsicherheitsanwendungen



## Lösungsansätze für Hochsicherheitsanwendungen

---

- Grundproblem: Hohe Nachweistiefe korrekter Funktionalität vs. Komplexität und Funktionsvielfalt
  
- Lösungsansatz: „Teile und Herrsche“ - Prinzip der sog. Rot-Schwarz-Trennung
  - Aufteilung von Funktionalität in Steuer- und Datenflüsse
  - Notwendige Transfers von Steuerinformationen von Rot nach Schwarz sehr klein und filterbar halten
  - Trennung mit nachweisbar sicheren Barrieren
  - Mikrokern-Betriebssysteme (Prozess- und Speicherschutz)
  - klassische Hardware-Separierung (roter Prozessor + schwarzer Prozessor + Gateway-Funktion)
  
- Keine „out-of-the-box“-Lösung mit Standard-OS!



**Vielen Dank  
für Ihre Aufmerksamkeit.**

Gerne beantworten wir Ihre Fragen.

Hans-Markus Krüger, Dr. Kai Martius

Telefon +49 201 5454 0

[hans.krueger@secunet.com](mailto:hans.krueger@secunet.com)

[kai.martius@secunet.com](mailto:kai.martius@secunet.com)

[www.secunet.com](http://www.secunet.com)