

# Hochgeschwindigkeits-Ethernet-WAN: Bremst Verschlüsselung Ihr Netzwerk aus?

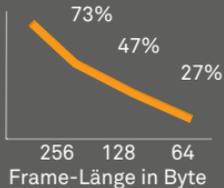


**27%** →

# Fakten zur Verschlüsselung mit IPsec:

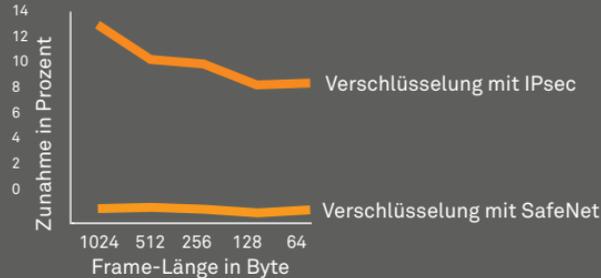
## 27 Prozent Durchsatz

Bei kleinen Frames, wie sie bei Sprach- und Videodaten üblich sind, erreicht die Verschlüsselung nur 27 Prozent des maximalen theoretischen Datendurchsatzes.



## 13-fache Latenzzeit

IPsec erhöht die Latenz um den Faktor 6 bis 13.



## 40 Prozent der Bandbreite

Verschlüsselung mit IPsec kann bis zu 40 Prozent der verfügbaren Bandbreite benötigen.



Quelle: Rochester Institute of Technology,  
„Comparative Performance of Layer 2 and IPsec  
Encryption on Ethernet Networks“

„Tests zeigten den Einfluss auf die Netzwerk-Performance, den sowohl der immanente Bedarf an Rechenleistung von IPsec als auch die begrenzte Leistungsfähigkeit der getesteten IPsec-Hardware haben.“

# Die Layer-2-Netzwerk-Verschlüsselungslösung von SafeNet bietet Ihnen:

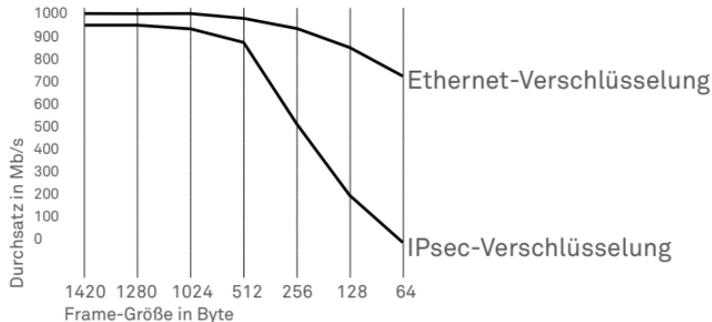
- Maximale Performance
- Größtmöglichen Schutz
- Geringsten administrativen Overhead
- Niedrigste TCO

Nur wenn die Verschlüsselungsstrategie von der Netzwerk-Architektur unabhängig betrachtet wird, kann man ein völlig sicheres, leistungsstarkes Hochgeschwindigkeits-Ethernet-WAN aufbauen.

Die Netzwerk-Verschlüsselungs- und Isolations-Lösung von SafeNet erlaubt eine schnelle Einführung, ohne dass das Netzwerk neu konfiguriert werden muss. Änderungen an den Routing-Tabellen sind unnötig. Und die Lösung hat keine negativen Auswirkungen auf die Leistungsfähigkeit des Netzwerks oder auf die Architektur.

# Maximaler Durchsatz ohne Protokoll-Ballast

## Vergleich des Durchsatzes bei Verschlüsselung



Die Hochgeschwindigkeits-Lösung von SafeNet zur Verschlüsselung auf Layer 2 produziert keinen Protokoll-Ballast. Für die Daten steht das Maximum an Bandbreite zur Verfügung. Damit ist die Lösung um bis zu 50 Prozent effizienter als andere Technologien. Die Lösungen von SafeNet stellen die schnellstmögliche Netzwerk-Verschlüsselung bereit. Und sie arbeiten mit der vollen Leitungsgeschwindigkeit.

Und die Hochgeschwindigkeits-Verschlüsselung von SafeNet hat keine Auswirkungen auf die Latenz. Eine hohe Qualität für Echtzeitanwendungen wie VoIP oder Video-Applikationen mit kleinen Frames ist garantiert. Hochverfügbarkeits-Merkmale unterstützen Architekturen mit einer Uptime von über 99,999 Prozent.



## Der bestmögliche Schutz mit AES-256 und manipulationssicher nach FIPS 140-2 Level 3

Die Hochgeschwindigkeits-Verschlüsselungssysteme von SafeNet nutzen den stärksten Kryptografie-Algorithmus, der öffentlich verfügbar ist – den Advanced Encryption Standard AES-256. Dieser wurde am NIST entwickelt und von der NSA für streng geheime Informationen zugelassen.

Router und Firewalls kämpfen fortlaufend gegen immer neue Sicherheitslücken und Angriffe. Die SafeNet-Devices, die auf Layer 2 arbeiten, benötigen keine ständigen Sicherheits-Patches.

Das physikalische Design der Ethernet-Hochgeschwindigkeits-Verschlüsselungsgeräte von SafeNet ist sicher vor Manipulationen. Es ist nach Common Criteria (ISO/IEC 15408) und FIPS 140-2 Level 3 zertifiziert.



## Minimaler Overhead bei der Administration – geringe Betriebskosten

Ein großer Vorteil der Verschlüsselungslösung von SafeNet ist der geringe Overhead bei der Administration.

Durch den Einsatz des einzigartigen Security Management Centers lassen sich die SafeNet-Verschlüsselungssysteme in wenigen Minuten installieren. Das Netzwerk muss nicht neu konfiguriert und die Routing-Tabellen müssen nicht aktualisiert werden. Alle Updates beim Routing sind für die Verschlüsselung transparent.

Da das Setup und die Installation so einfach sind, sind auch weniger Spezialkenntnisse nötig. Es ist nicht notwendig, von Hand komplexe Adress-Tabellen und Richtlinien anzulegen. Denn die Verschlüsselungsgeräte von SafeNet erkennen alle MAC-Adressen im Netz automatisch. Sind neue Devices im Netzwerk vorhanden, werden deren Keys von ganz alleine erkannt.

Durch die einzigartigen Merkmale der SafeNet-Lösungen integrieren sich die SafeNet Ethernet Encryptors nahtlos als Overlay in jede Netzwerk-Topologie.

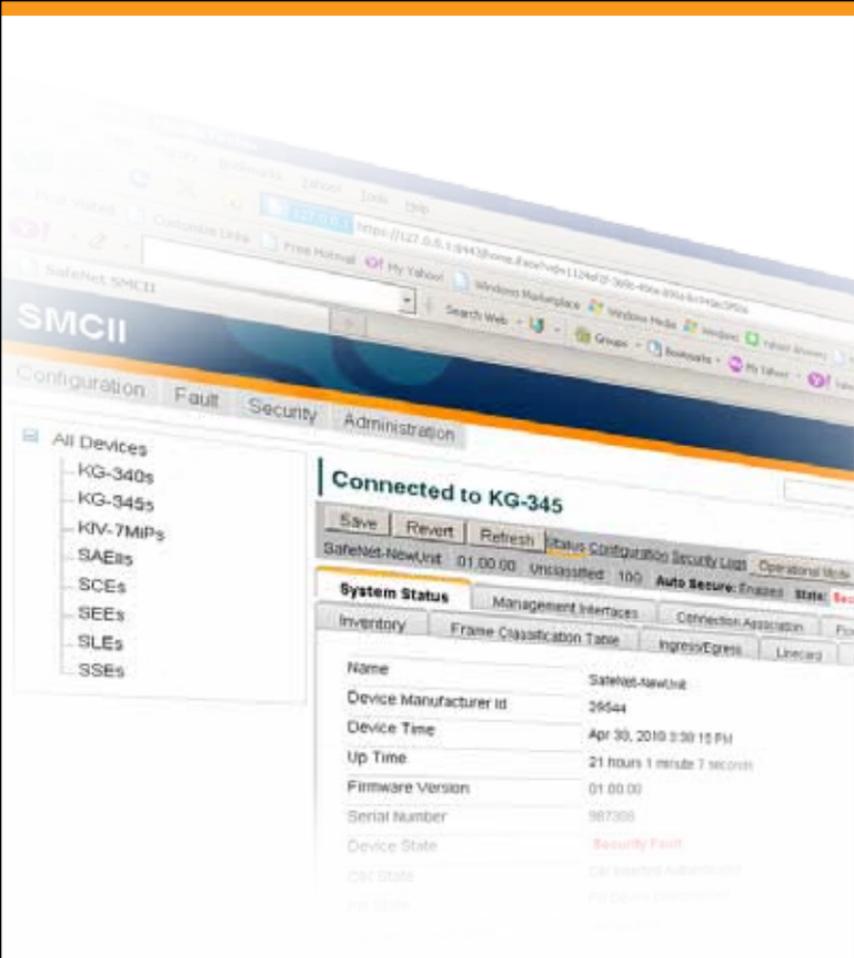


## Geringe Investition

Die Verschlüsselungsgeräte von SafeNet sind die kostengünstigste Lösung, um mehrere Sites oder Hochgeschwindigkeitsnetze zu verbinden. Die SafeNet-Technologie benötigt weniger Devices als vergleichbare Lösungen mit zusätzlichen Routern und Verschlüsselung mit IPsec.

Die einfache Netzwerk-Topologie, die durch die Hochgeschwindigkeits-Verschlüsselungslösung von SafeNet möglich ist, reduziert die Komplexität der Netzwerk-Infrastruktur, der Wartung und der Administration. Sie unterstützt alle Protokolle auf Layer 3 und lässt sich problemlos skalieren.

Und natürlich kann man auch tausende von Euro im Monat sparen, wenn man wieder Herr über seine Bandbreite ist.



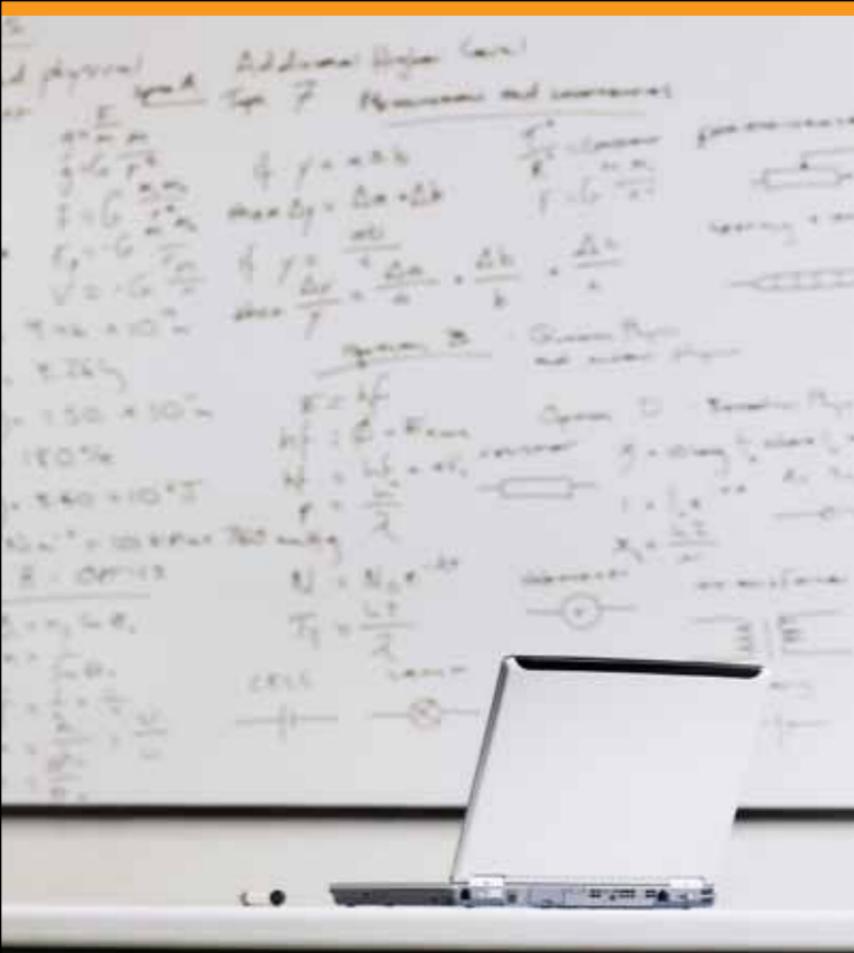
## Unified Security Management

Das Security Management Center von SafeNet stellt eine einzigartige Administrations Schaltstelle dar. Weit mehr als eine Konsole. Es bietet ein einheitliches Management aller Datensicherheitslösungen von SafeNet. Nicht nur für die aktuellen Produkte – auch für kommende Lösungen.

Die einfache Fernadministration erlaubt es, alle Verschlüsselungsgeräte von SafeNet zentral aus der Ferne zu konfigurieren, zu überwachen und auf dem neuesten Stand zu halten.

Die komplett automatisch erstellten Berichte für Sicherheits-Audits senken die Kosten im Bereich der Revision.

Das Security Management Center erlaubt es, über Skripts wiederkehrende Aufgaben zu automatisieren. So werden die Konfiguration und die Administration der Verschlüsselungsgeräte bei vielen Vorgängen erleichtert – etwa beim Ändern der Passwörter, Anlegen neuer Benutzer und Erneuern von Zertifikaten.



# Lösungen zur Netzwerk-Verschlüsselung und -Isolierung von SafeNet

Die Lösungen zur Netzwerk-Verschlüsselung und -Isolierung von SafeNet erleichtern nicht nur die Verwaltung. Sie können durch die automatische Device-Erkennung auch schnell auf tausende von Geräten skalieren.

Durch die dezidierte Verschlüsselung werden Router und andere Geräte im Netzwerk nicht zusätzlich mit dieser Aufgabe belastet. Das gibt dem Netzwerk mehr „Kopffreiheit“, Ausfallsicherheit und Leistungsfähigkeit.

Durch die eingebaute Key-Verwaltung ist ein externes Key-Management überflüssig. Jedes Verschlüsselungsgerät im Netz kann hierbei als führendes System eingerichtet werden und so automatisch die Keys für alle anderen Devices im Netz erstellen.

Durch Multipoint-Unterstützung kann sich ein einziges Verschlüsselungsgerät mit hunderten von Niederlassungen verbinden.

Die Ethernet-Hochgeschwindigkeits-Verschlüsselungslösungen von SafeNet beherrschen von Haus aus VLAN.

# 85 Prozent aller Transfers zwischen Banken werden über Lösungen zur Hochgeschwindigkeits-Ethernet-Verschlüsselung von SafeNet abgewickelt



SafeNet hat das weltweit umfassendste Paket an dezidierten Lösungen für WAN-Verschlüsselung in Hochgeschwindigkeit.

85 Prozent aller Transfers zwischen Banken werden über Lösungen zur Hochgeschwindigkeits-Ethernet-Verschlüsselung von SafeNet abgewickelt. Zudem kommen die Geräte von SafeNet in zahlreichen US-Behörden zum Einsatz.

SafeNet ist ein Security-Unternehmen. Die Verschlüsselungslösungen von SafeNet wurden von Grund auf als Komponenten für die IT-Sicherheit konzipiert und gebaut. Es gibt keine Alternative.

### **Try-and-buy kit:**

... erhalten Sie über die Niederlassung in Ihrer Region. →

<http://safenet-inc.com/contact-us.aspx>

### **Laden Sie unser eBook herunter:**

<http://www.safenet-inc.com/hse-ebook/> →

### **Whitepaper zum Download:**

[www.safenet-inc.com/hseresources](http://www.safenet-inc.com/hseresources) →

### **So funktioniert Fiber-Tapping**

<http://www.safenet-inc.com/fibertapping> →