SpecialInterest

» Layer 2 Verschlüsselung «

Wartungsfreie sichere Netzwerk-Verschlüsselung mit automatischem Schlüsselwechsel.

Der Datenaustausch über den meist genutzten Übertragungsstandard für breitbandige und serviceorientierte Datenübertragungen, dem Ethernet-Protokoll, ist prinzipiell ungeschützt. Die häufig integrierte Layer 3 Verschlüsselung der marktüblichen Hardware lässt viele Lücken zum Mitlesen von Daten. Auch die Gefahr der Manipulation von Integrität (Daten verändern) und Authentizität (Daten wieder einspielen) ist mit einem geringen Maß an Wissen und technischer Ausrüstung allgegenwärtig.

Von 3 auf 2 auf Nummer sicher.

Die wirkungsvollste und effizienteste Maßnahme, um Informationen in Netzwerken zu schützen, bildet die Verschlüsselung. Je tiefer diese Verschlüsselung hierbei auf den Netzwerkebenen des OSI-Modells (Open Systems Interconnection Model, das Referenzmodell für Netz-werkprotokolle als Schichtenarchitektur) implementiert ist, desto umfangreicher sind die Protokolle, die chiffriert werden können. So arbeitet eine Verschlüsselung auf Layer 2 autark zu sämtlichen Applikationen auf der Netzwerkschicht 3. Vereinfacht ausgedrückt: was aus Layer 4 und 3 in der Tiefe immer mehr Platz einnimmt, weil jedes Protokoll einzeln verpackt werden muss, wird im Layer 2 Verfahren sicher und mit entsprechend kleinerem Overhead-Bedarf auf einmal verschlüsselt. Die Vorteile liegen in der enormen Verringerung von Latenzzeiten bei gleichzeitiger Erhöhung der Sicherheit der sich im Netzwerk befindlichen Daten.

Geringerer Overhead.

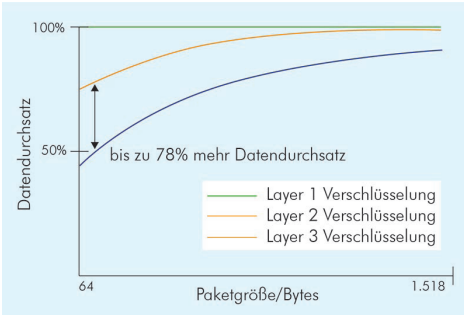
Die Layer 2 Verschlüsselung bietet eine sichere und annähernd verzögerungsfreie Übertragung zeitkritischer Daten (VoIP, Video, etc.) und ist die effizientere Lösung zu klassischen Layer 3 basierenden VPN-Lösungen mit IPSec (Internet Protocol Security) dar. Im Gegensatz zu Layer 3 basierten Verschlüsslungen wird auf der Sicherungsschicht kein Tunneling von Adressinformationen benötigt, was den entsprechenden Overhead signifikant vermindert. So sind Latenzzeiten im Mikrosekundenbereich für Layer 2 Verschlüsselungssysteme charakteristisch.

Höhere Sicherheit.

Die Chiffrierung erfolgt durch das Advanced Encryption Verfahren (AES), auch nach dem Namen seiner Entwickler als Rijndael-Algorithmus bekannt. Die AES-Verschlüsselung nutzt eine Blockgröße von 256 Bits und bietet ein Höchstmaß an Sicherheit. So ist AES-256 zum Beispiel zugelassen für staatliche Dokumente mit höchster Geheimhaltungsstufe.

Autonom und transparent zu anderen Diensten.

Die Layer 2 Verschlüsselung der Pan Dacom Direkt ist einfach und unkompliziert durch das Zwischenschalten in bestehende Netzinfrastrukturen integrierbar. Sowohl für Ende-zu-Ende als auch für Mehrpunkt-zu-Mehrpunkt Verbindungen geeignet, arbeitet sie transparent zu genutzten Diensten wie E-LINE, E-TREE, E-LAN, xWDM, VPLS, MPLS und VLANs. Der weitere Betrieb ist wartungsfrei und beinhaltet einen automatischen Schlüsselwechsel. Dieser erfolgt autonom durch eine Master-Slave Konfigurationen zwischen den im Netzwerk implementierten Geräten. Die so realisierte Verschlüsselung bildet eine dedizierte Trennung zwischen dem öffentlichen Transportnetz und der privaten Infrastruktur mit einer flexiblen Differenzierung von internen Standorten und Zuständigkeiten.



Layer 1, 2 und Layer 3 im Vergleich

» Anwendungsbeispiel

Die Herausforderung:
Verschlüsselte Übertragung von sensiblen Daten mit geringer Latenzzeit für Echtzeitkommunikation im MAN und WAN in Ende-zu-Ende- und Mehrpunktszenarien in Unternehmen sicher zu stellen.

Die Lösung:
Eine Layer 2 Verschlüsselung, umgesetzt mit der Kompetenz des erfahrenen Netzwerkspezialisten Pan Dacom Direkt GmbH, die auch in bestehende Unternehmensnetzwerke implementiert werden kann und über die Richtlinien des BSI (Bundesamt für Sicherheit in der Informationstechnik) hinaus Datenschutz im Netzwerk sicherstellt.

Die Details:
- » Skalierbare Vollduplex-Verschlüsselung
- » Schlüsselaustausch mit Diffie-Hellman Verfahren
- » 1/2/4/8 Gbit/s Fibre Channel
- » 10/40/100 Gbit/s Ethernet
- » manipulationssicheres System-Design (Tamper Proof)

Die Vorteile:
- » integrierbar in bestehende Netzwerke
- » Transparenz zu IPv4, IPv6, xWDM, VPLS, MPLS und VLANs
- » Keine Auswirkungen auf den Quality of Service (QoS)
- » einfaches Zwischenschalten ohne Umbau
- » BSI zugelassene Lösung
- » Deutscher Hersteller

Lösung für Unternehmen: zur einfachen Realisation zuverlässiger Verschlüsselung in bestehenden Netzwerken, abhörsicherer Trennung von internen Abteilungsnetzwerken und gesicherter Verbindungen verschiedener Unternehmensstandorte bei gleichzeitiger Beschleunigung zeitkritischer Anwendungen.