Adva NETWORK SECURITY

genua.

Cyberresiliente Infrastruktur für Netze mit hohen Schutzanforderungen

Hochflexibles Sicherheitselement für Netzübergänge auf Layer 2 und 3

Zwei starke Partner – eine hochsichere Lösung.

Die Anforderungen an ein sicheres Kommunikationsnetz für Behörden und kritische Infrastrukturen (KRITIS) sind hochkomplex und multidimensional. Konkret umfassen diese:

Die Gewährleistung von **digitaler Souveränität** und **Unabhängigkeit** von einzelnen Herstellern, um die Einflussnahme durch externe Akteure zu minimieren.

Die Sicherstellung von **Vertrauenswürdigkeit** und **Verlässlichkeit** der Netzinfrastruktur, um den Schutz und die Integrität der Daten zu gewährleisten.

Die Erfüllung von **Performance-** und **Verfügbarkeitsanforderungen** für die verschiedenen Anwendungen und Dienste, um einen reibungslosen Betrieb zu ermöglichen.

Die Notwendigkeit einer **zukunfts-** und **wandlungsfähigen Netzarchitektur**, um auf veränderte Anforderungen und neue Technologien schnell reagieren zu können.

Die Gewährleistung einer **robusten Lieferkette**, um die Verfügbarkeit und Zuverlässigkeit der Netzkomponenten sicherzustellen.

Management Summary

Um die Anforderungen an eine cyberresiliente Infrastruktur zu erfüllen, müssen Behörden und KRITIS ein sicheres Kommunikationsnetz aufbauen, das die Verwendung öffentlicher Netze ermöglicht, ohne die Sicherheit und Integrität der Daten zu gefährden. Ein wichtiger Aspekt dabei ist die Verschlüsselung von Daten, um sie vor unbefugtem Zugriff zu schützen.

Die genua GmbH ist Hersteller zugelassener und zertifizierter IT-Sicherheitslösungen und bietet eine Lösung an, die es Behörden und KRITIS ermöglicht, ein sicheres Kommunikationsnetz aufzubauen, das die Anforderungen an digitale Souveränität, Vertrauenswürdigkeit und Sicherheit erfüllt.

Die Adva Network Security GmbH bietet optische Übertragungssysteme und Layer-2-Netzzugangstechnologien mit BSI-zugelassener Verschlüsselung an, die sich bereits in vielen einsatzkritischen Anwendungen bewährt haben.

Die hier skizzierte Lösung ermöglicht eine leistungsfähige Ausgestaltung der benötigten Infrastruktur. Mit einer modularen Netzarchitektur, die auf der Verwendung eines hochflexiblen Koppelelements (gemeinsame Lösung mit Layer-2- und Layer-3-Schutz) an allen Netzübergängen setzt, können die verschiedenen Anforderungen effektiv erfüllt werden. Durch die Kombination von verschiedenen Vernetzungstechnologien können breitbandige Layer-2-Ethernet-Verbindungen und IP-geroutete Verbindungen auf Layer 3 für den Datenverkehr zwischen Liegenschaften eines Mandanten sowie die zugelassene IPSec-VPN-Anbindung mobiler User bereitgestellt werden.

Mit kombinierter Layer-2- und Layer-3-Verschlüsselung zu sicheren, skalierbaren und wirtschaftlichen Netzen

Dieser Leitfaden zeigt eine Strategie für den Einsatz von Verschlüsselungstechnik in großflächigen Verbindungsnetzen auf und gibt praktische Empfehlungen für eine wirtschaftliche und flexible Implementierung für den Hochsicherheitsbereich.

Im Folgenden werden zwei unterschiedliche Ebenen beim Einsatz von Kryptografie im Verbindungsnetz verglichen: die Ende-zu-Ende-Verschlüsselung und die Verschlüsselung von aggregiertem Verkehr.

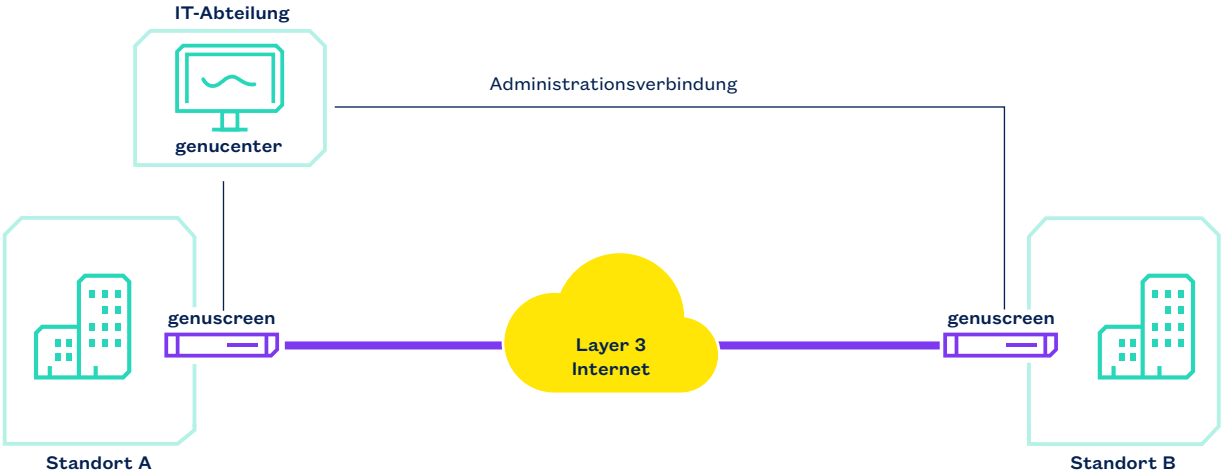
Die Vorteile einer kombinierten Verschlüsselung auf mehreren Ebenen (engl. „Layers") kann zu einer komplexeren Administration führen. Dies lässt sich jedoch durch die Konfiguration mittels eines einheitlichen Management-Systems vermeiden. Damit ist der einfache und wirtschaftliche Betrieb eines umfassend gesicherten Netzes möglich.

Ende-zu-Ende-Verschlüsselung auf Layer 3

Die Übertragung von Daten kann zuverlässig durch die Verschlüsselung aller Ende-zu-Ende-Verbindungen geschützt werden. Das IPSec-Protokoll schützt den Verkehr über potenziell ungesicherte IP-Netze. Der Layer-3-Schutz ist in vielen Endgeräten als Software implementiert und kann leicht eingesetzt werden.

IP-Netze werden über unterschiedliche Infrastrukturen wie Glasfaser, Funk (Mobilfunk, WiFi) oder Kupferkabel realisiert. Ein Anwender hat jederzeit und an jeder beliebigen Stelle Zugang zum IP-Netz.

Es erscheint naheliegend, dass die Sicherheit der Informationen durch den Schutz aller Verbindungen in einem Netz gewährleistet werden kann. Dabei ist es jedoch wichtig, einige Randbedingungen zu berücksichtigen.



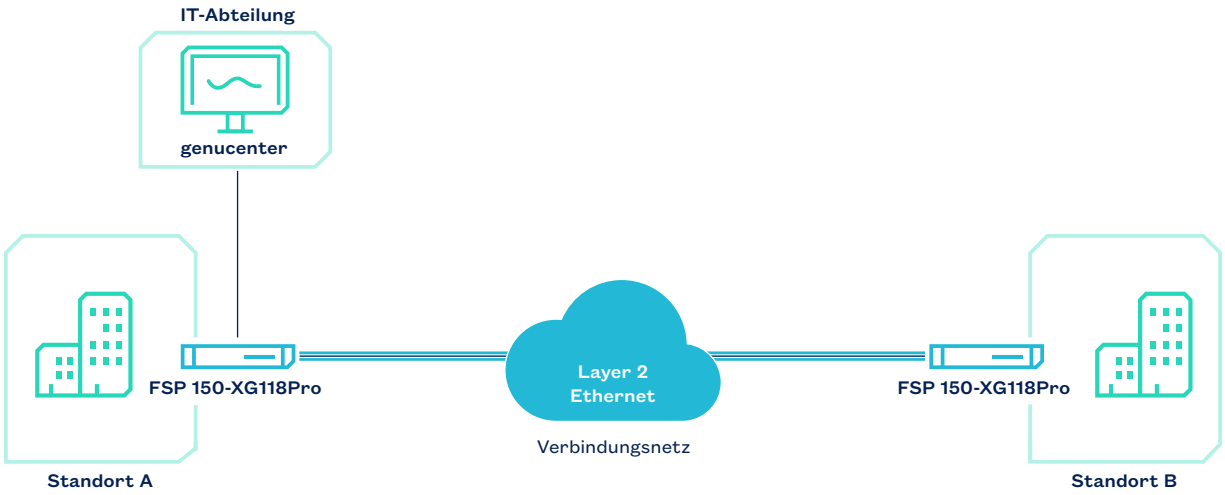
Sicheres Layer-3-Netz mit genuscreen von genua, mehrmandantenfähig

Die Sicherheit einer Verschlüsselung ist in erster Linie vom Schutz der privaten Schlüssel abhängig. Jeder Endpunkt im Netz muss in der Lage sein, Schlüssel sicher aufzubewahren und sie mit anderen Teilnehmern auszutauschen. Diese Anforderung ist nicht trivial und kann von einfachen Endpunkten wie z. B. IoT-Geräten nicht ohne Weiteres erfüllt werden.

Die globale Erreichbarkeit von Anwendungen, die mit dem Internet verbunden sind, führt zu einer großen Angriffsfläche, da Angreifer global auf den Anschlusspunkt zugreifen können. IP/VPNs isolieren den Verkehr unterschiedlicher Mandanten und reduzieren dadurch die Erreichbarkeit der angeschlossenen Geräte aus dem Internet.

Bei einer Verschlüsselung aller Verbindungen wird die Implementierung von Systemen zur Erkennung von Angriffen durch Deep Packet Inspection erschwert, da Schadcode im Verkehr nicht mehr erkannt wird. Dies gilt auch dann, wenn der Verkehr auf höheren Netzebenen wie zum Beispiel TLS oder HTTPS verschlüsselt wird. Es gibt also Gründe, den Verkehr zumindest in lokalen, physisch gesicherten Bereichen unverschlüsselt zu übertragen.

Im Folgenden werden alternative Verschlüsselungsarchitekturen beschrieben, die den oben genannten Beschränkungen einer reinen IP-Verschlüsselung Rechnung tragen und in einigen Anwendungsfällen eine attraktive Lösung darstellen.



Sicheres Layer-2-Netz mit FSP 150-XG118Pro von Adva, mehrmandantenfähig

Sichere Standort-Anbindung mit Layer-2-Ethernet

Ethernet-Bandbreitendienste werden als provisionierte Festverbindungen angeboten. Sie sind für Anwendungen mit langen Standzeiten von einigen Stunden bis zu mehreren Jahren ausgelegt. Diese geringe Dynamik entspricht den Anforderungen für die Verbindung von Rechenzentren oder die Anbindung von Standorten bzw. Liegenschaften.

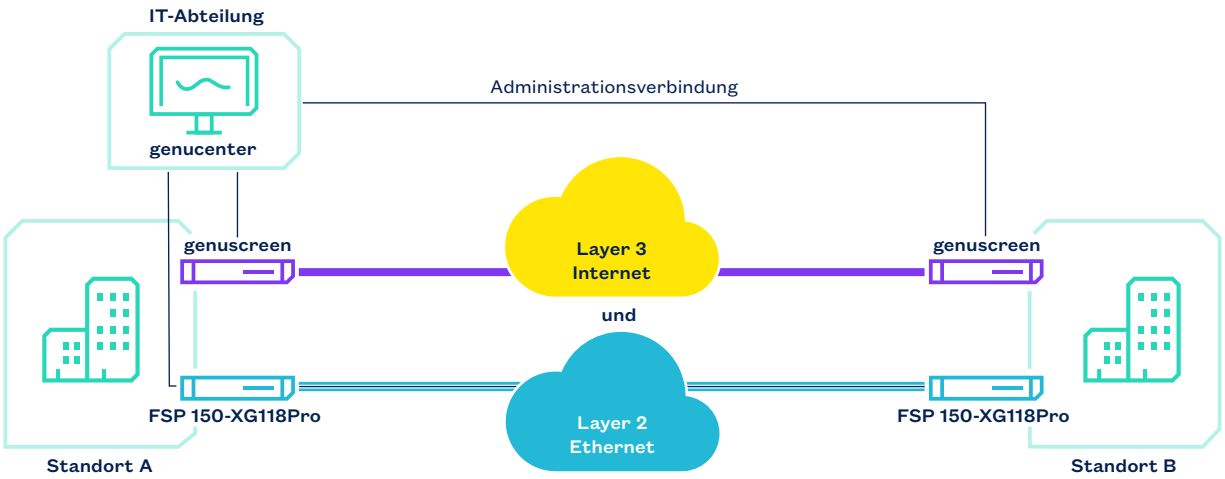
Über Layer-2-Verbindungen werden die Protokolle höherer Netzebenen transparent übertragen. Die IP-Adressen müssen nicht ausgewertet werden, was den Konfigurationsaufwand minimiert und eine schnelle Weiterleitung der Daten begünstigt.

Eine Verschlüsselung der Ethernet-Verbindung schützt den gesamten Verkehr zuverlässig vor Angriffen auf dem Verbindungsweg. Gegenüber der Verschlüsselung einzelner Verbindungen hat der Schutz des aggregierten Verkehrs einige Vorteile.

- Einzelne Verbindungen werden häufig auf höheren Netzebenen mit Software verschlüsselt, während eine schnelle Ethernet-Verschlüsselung mit dedizierter Hardware realisiert wird. Darüber hinaus begünstigt die höhere Geschwindigkeit des aggregierten Verkehrs eine geringe Latenz.

- Die gemeinsame Verschlüsselung des aggregierten Verkehrs ist kostengünstiger und verbraucht weniger Energie als die individuelle Verschlüsselung einzelner Verbindungen.

- Verkehrsbeziehungen auf höheren Netzschichten werden verschleiert, da die gesamten Daten der höheren Netzschichten inklusive beispielsweise von IP-Adressen verschlüsselt werden.



Layer-2- / Layer-3-Netz, mehrmandantenfähig

Die Verschlüsselung von Layer-2-Verbindungen bietet einen wirksamen Schutz vor Angriffen auf dem Verbindungsweg. Allerdings sind die Nutzer am Standort nicht vor kompromittierten Geräten oder Angriffen, die über höhere Layer ins lokale Netz gelangen, geschützt. Für einen umfassenden Schutz sollte die Kombination von Verschlüsselung auf mehreren Netzschichten in Betracht gezogen werden.

Vorteile einer Kombination von Layer-2- und Layer-3-Verschlüsselung

Die Betreiber von Kommunikationsnetzen werden ihre Nutzer und Standorte mit unterschiedlichen Technologien untereinander verbinden.

- Kleine Standorte, Heimarbeitsplätze oder mobiles Arbeiten werden die Vorteile einer Layer-3-Anbindung mit dem IP-Protokoll und dem Schutz durch IPSec nutzen.

- Breitband-Datenströme sollten bevorzugt auf den unteren Netzschichten geschützt werden. Layer-2-Ethernet ist eine hochperformante und wirtschaftliche Lösung für die Anbindung mittlerer und großer Standorte.

- Für die sehr hohen Bandbreiten zwischen Datenzentren ist eine direkte Verschlüsselung des optischen Kanals auf Layer 1 empfehlenswert.

Um die Resilienz zu erhöhen, können Standorte gleichzeitig über verschlüsselte Layer-2- und Layer-3-Verbindungen angebunden werden.

Eine Partnerschaft ebnet den Weg zu wirtschaftlichen und sicheren Netzen

Die Verschlüsselung wird in großen Netzen auf unterschiedlichen Layern eingesetzt, um einen kosteneffizienten, hochperformanten und sicheren Betrieb zu gewährleisten. Der verbesserte Schutz hat jedoch eine höhere betriebliche Komplexität zur Folge.

Abhilfe schafft ein einheitliches Management des Netzes und der auf mehreren Netzschichten eingesetzten Sicherheitstechnik. Die neue Partnerschaft zwischen genua und Adva Network Security ermöglicht dies. Die Kombination der sicheren Layer-3-Lösungen von genua und der geschützten Layer-2-Technik von Adva Network Security erlaubt es Kunden, ihr Netz einfach zu betreiben, ohne dabei Kompromisse bei Sicherheit und Wirtschaftlichkeit einzugehen. An einigen Standorten werden zwei Netzschutzgeräte für Layer 2 und Layer 3 eingesetzt.

Durch Virtualisierungstechnologien lassen sich die Schutzmaßnahmen um weitere Bausteine ergänzen. Diese können direkt auf dem Adva-System betrieben werden, da dieses durch Ergänzung um Server-Komponenten als Edge Cloud eingesetzt werden können.

Zusammenfassung und Ausblick

Die beiden deutschen IT-Sicherheitsexperten genua und Adva Network Security haben eine Netzarchitektur entwickelt, um Kommunikationsnetze für einsatzkritische und hoheitliche Anwendungen sicherer, schneller und wirtschaftlicher zu machen. Die Integration unter ein gemeinsames Managementsystem bietet operative Einfachheit für eine sichere Netzlösung, die ein umfassendes Spektrum an Anwendungen und Use Cases mit bewährter Technik adressiert. Zukünftig werden weitere Komponenten des Lösungsportfolios von genua und Adva Network Security die gemeinsame Lösung ergänzen, um Netze noch umfassender und einfacher zu schützen.

Die Lösungen von genua und Adva Network Security sind vom BSI für den Transfer von klassifizierten Daten zugelassen. Die kombinierte Lösung der beiden deutschen Unternehmen wird für viele Kunden aus dem Hochsicherheitsbereich eine bedeutende Rolle beim Ausbau ihrer Netze spielen.

Über genua

Die genua GmbH sichert sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert das Unternehmen auf den umfassenden Schutz von Netzwerken, Kommunikation und interner Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls und Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security bis hin zu Remote-Access-Lösungen für mobile Mitarbeiter und Homeoffices.

Die genua GmbH ist eine Tochtergesellschaft der Bundesdruckerei-Gruppe. Mit mehr als 400 Mitarbeitenden entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung in 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

genua.

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
+49(0) 89 991950-0, info@genua.de, www.genua.de

Über Adva Network Security

Adva Network Security hat sich auf den Schutz von Datennetzen mit hohem Sicherheitsbedarf spezialisiert. Mit der ConnectGuard™ Sicherheitstechnik sind Unternehmen, Behörden und kritische Infrastrukturen schon heute in der Lage, zukünftige Cyberangriffe durch Quantencomputer abzuwehren. Die Verschlüsselungslösungen zeichnen sich durch eine sehr geringe Latenzzeit aus und bieten Glasfasernetzen einen umfassenden Schutz auf mehreren Netzebenen. Anerkannte Sicherheitsexperten haben das Unternehmen in Deutschland gegründet, um Organisationen und Behörden beim Schutz ihrer Netze zu unterstützen und damit Cyberbedrohungen ihrer kritischen Anwendungen abzuwenden. Die Entwicklungs- und Fertigungsprozesse sowie die Verschlüsselungslösungen wurden von führenden staatlichen Sicherheitsbehörden zertifiziert und zugelassen.

Adva
NETWORK SECURITY

Adva Network Security GmbH, Hermann-Dorner-Allee 91, 12489 Berlin
+49 (0) 30 2636969-0, info@advasecurity.com, www.advasecurity.com

102024.01.DE