Adva NETWORK SECURITY

genua.

Cyber-Resilient Infrastructure for Networks with High Protection Requirements

Highly Flexible Security Element for Network Transitions on Layer 2 and 3

Strong Partnership for a Highly Secure Solution.

The requirements placed on a secure communication network for public authorities and critical infrastructures are highly complex and multidimensional. In concrete terms, they include the following:

Guaranteeing **digital sovereignty** and **independence** from individual manufacturers in order to minimize the influence of external actors.

Safeguarding the **trustworthiness** and **reliability** of the network infrastructure in order to ensure the protection and integrity of the data.

Meeting **performance** and **availability requirements** for the various applications and services in order to enable trouble-free operation.

Need for a **future-proof** and **versatile network architecture** to be able to react fast to changed requirements and new technologies.

Guaranteeing a **robust supply chain** to safeguard availability and reliability of the network components.

Management Summary

In order to meet the requirements on a cyber-resilient infrastructure, public authorities and critical infrastructures need to set up a secure communication network which enables the use of public networks without jeopardizing the security and integrity of the data. A key aspect here is the encryption of data in order to protect it from unauthorized access.

genua GmbH is a manufacturer of approved and certified IT security solutions and offers a solution that enables public authorities and critical infrastructures to set up a secure communication network which meets the requirements regarding digital sovereignty, trustworthiness, and security.

Adva Network Security GmbH provides optical transmission systems and layer 2 network access technologies with BSI-approved encryption which have already been tried and tested in numerous mission-critical applications.

The solution outlined here enables an efficient design and configuration of the required infrastructure. Its modular network architecture, which uses a highly flexible coupling element (combined solution with layer 2 and layer 3 protection) at all network transitions, allows the various requirements to be met effectively. By combining various networking technologies, broadband layer 2 Ethernet connections and IP-routed connections on layer 3 can be provided for data traffic between the properties of a client as well as for the approved IPSec VPN connection of mobile users.

Combined Layer 2 and Layer 3 Encryption for Secure, Scalable, and Cost-Efficient Networks

This white paper describes a strategy for using encryption technology in large-scale networks and provides practical recommendations for cost-efficient and flexible implementation in high-security applications.

Below is a comparison of two different layers of cryptography used in the network: end-to-end encryption and the encryption of aggregated traffic.

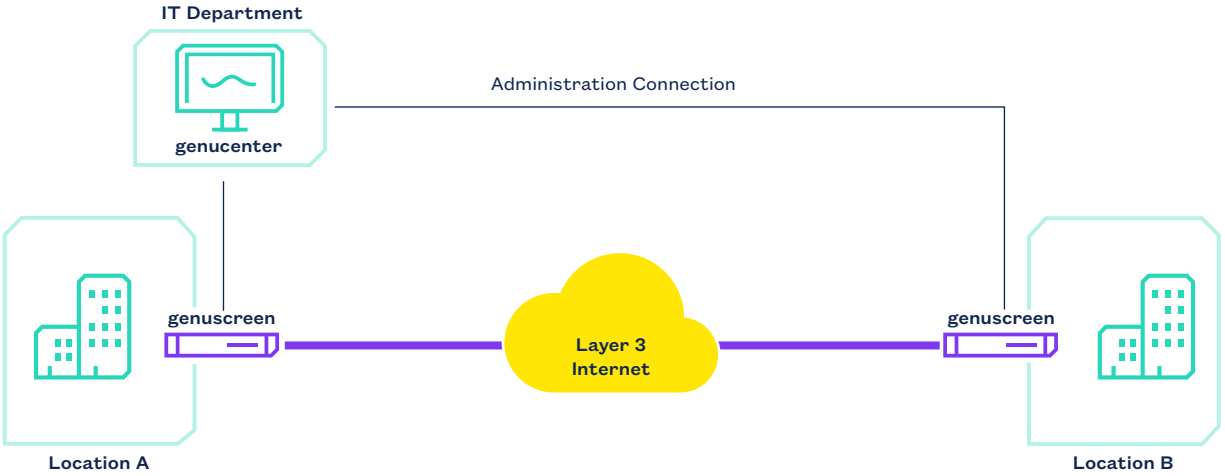
The advantages of combined encryption on multiple layers can result in a more complex administration. However, this can be avoided by means of configuration using a uniform management system. This enables simple and cost-efficient operation of a fully secured network.

End-to-End Encryption on Layer 3

The transfer of data can be reliably protected through the encryption of all end-to-end connections. The IPSec protocol protects the traffic on potentially non-secure IP networks. In many end devices, layer 3 protection is implemented as software and is easy to deploy.

IP networks are realized using different infrastructures such as fiber optics, wireless technology (mobile telephony, WiFi) or copper cables. A user has access to the IP network at all times and at any location.

It is obvious that the information security can be guaranteed by protecting all connections in a network. Here, however, it is important to take into account a number of boundary conditions.



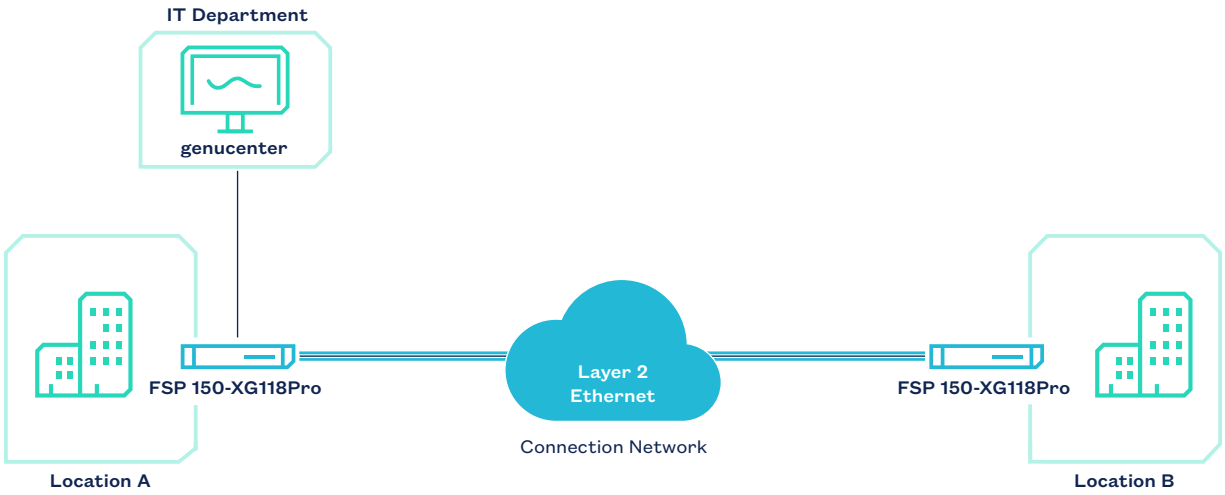
Secure layer 3 network with genuscreen from genua, multi-client capable

The security of an encryption primarily depends on the protection of the private keys. Each end point in the network must be capable of keeping keys safe and exchanging them with other users. This requirement is far from trivial and cannot easily be fulfilled by simple end points such as IoT devices.

The global accessibility of applications that are connected to the Internet constitutes a major avenue of attack because attackers can access the connection point from anywhere in the world. IP/VPNs isolate the traffic of different clients, thereby reducing accessibility to the connected devices from the Internet.

Encrypting all connections makes it difficult to implement systems for detecting attacks by means of deep packet inspection, because malicious code in the traffic is no longer detected. This is also the case if the traffic on higher network layers, e.g., TLS or HTTPS, is encrypted. There are therefore reasons to transfer the traffic without encryption, at least in local, physically secured areas.

Alternative encryption architectures that take into account the above-mentioned limitations of pure IP encryption and, in some cases, present an attractive solution are described below.



Secure layer 2 network with FSP 150-XG118Pro from Adva, multi-client capable

Secure Location Connectivity with Layer 2 Ethernet

Ethernet broadband services are offered as provisioned fixed connections. They are designed for applications with long service durations of a few hours up to several years. This low dynamic meets the requirements for linking data centers or connecting locations and premises.

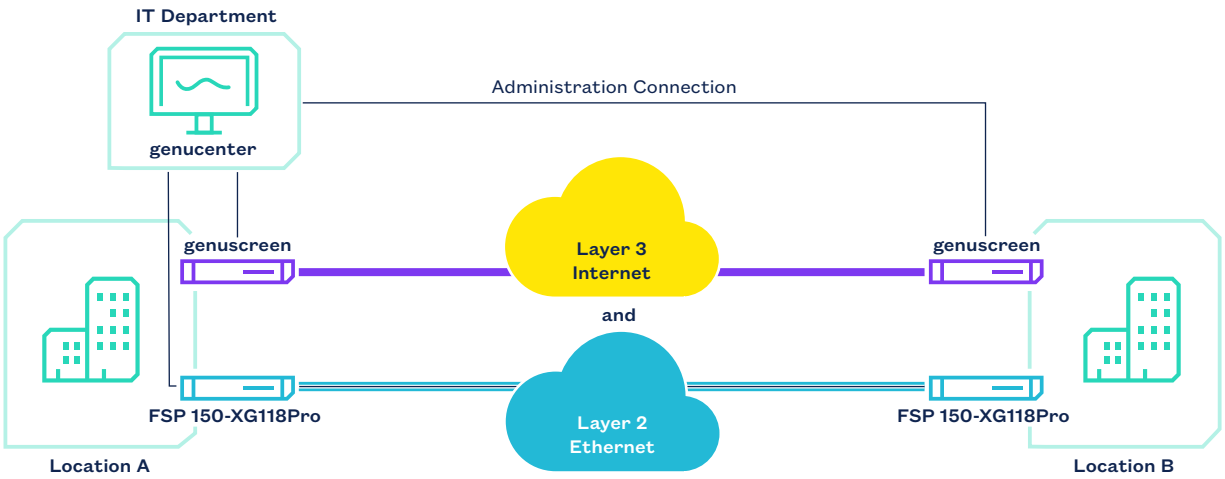
Via layer 2 connections, the protocols of higher network layers are transferred transparently. The IP addresses do not need to be evaluated, which minimizes configuration effort and facilitates fast forwarding of the data.

Encryption of the Ethernet connection reliably protects all traffic against attacks along the connection path. Protection of the aggregated traffic has a number of advantages over the encryption of individual connections.

- Individual connections are frequently encrypted on higher network layers using software, whereas fast Ethernet encryption is achieved using dedicated hardware. Moreover, the higher speed of the aggregated traffic also helps reduce latency.

- Collective encryption of the aggregated traffic is more cost-efficient and uses less energy than the individual encryption of single connections.

- Traffic correlations on higher network layers are concealed because all of the data on the higher network layers including, e.g., IP addresses is encrypted.



Layer 2/layer 3 network, multi-client capable

The encryption of layer 2 connections provides effective protection against attacks along the connection path. However, the users at the location are not protected against compromised devices or attacks that penetrate into the local network from higher layers. To ensure comprehensive protection, the combination of encryption on multiple network layers should be considered.

Advantages of Combined Layer 2 and Layer 3 Encryption

The operators of communication networks connect their users and locations using different technologies.

- Small locations, working from home or mobile work utilize the advantages of a layer 3 connection with IP protocol and protection through IPSec.
- Preferably, broadband data streams should be protected on the lower network layers. Layer 2 Ethernet is a high-performance and cost-effective solution for connecting medium-sized and large locations.
- For the extremely high bandwidths between data centers, direct encryption of the optical channel on layer 1 is recommended.

To increase resilience, locations can be connected via encrypted layer 2 and layer 3 connections simultaneously.

A Partnership Paves the Way to Cost-Efficient and Secure Networks

In large networks, encryption is implemented on different layers in order to ensure cost-efficient, high-performance and secure operation. However, the improved protection increases operational complexity.

Uniform management of the network and of the security technology deployed on multiple network layers provides a remedy. The new partnership between genua and Adva Network Security makes this possible. The combination of secure layer 3 solutions from genua and protected layer 2 technology from Adva Network Security allows customers to operate their network simply without comprising on security and economic efficiency. At some locations, two network protection devices are deployed for layer 2 and layer 3.

Using virtualization technologies, further modules can be added to the protective measures. They can be operated directly on the Adva system, because adding server components allows it to be used as an edge cloud.

Summary and Outlook

The two German IT security experts genua and Adva Network Security have developed a network architecture to make communication networks for critical and sovereign applications more secure, faster and more efficient. Integration under a common management system offers operational simplicity for a secure network solution which addresses a broad range of applications and use cases with tried-and-tested technology. Further components of the solution portfolio from genua and Adva Network Security will be added to the joint solution in future so that networks can be protected even more comprehensively and simply.

The solutions from genua and Adva Network Security are BSI-approved for the transfer of classified data. For many customers in the high-security sector, the combined solution from the two German companies will play a central role in the expansion of their networks.

About genua

genua GmbH secures sensitive IT networks in the public and enterprise sectors, at KRITIS organizations and in the classified industry with highly secure and scalable cyber security solutions. The company focuses on comprehensive network protection and internal network security for IT and OT. The range of solutions includes firewalls and gateways, VPNs, remote maintenance systems, internal network security, and cloud security through to remote access solutions for mobile working.

genua GmbH is a company of the Bundesdruckerei Group. With more than 400 employees, it develops and produces IT security solutions exclusively in Germany. Since the founding of the company in 1992, regular certifications and approvals from the German Federal Office for Information Security (BSI) provide proof of the high security and quality standards of the products. Customers include, among others, Arvato Systems, BMW, the German Armed Services, THW as well as the Würth Group.

genua.

genua GmbH, Domagkstrasse 7, 85551 Kirchheim near Munich
+49(0) 89 991950-0, info@genua.eu, www.genua.eu

About Adva Network Security

Adva Network Security specializes in the protection of data networks with high security requirements. With the ConnectGuard™ security technology, companies, public authorities and critical infrastructures are today already capable of fending off tomorrow‘s cyberattacks by quantum computers. The encryption solutions are characterized by an extremely short latency time and provide fiber-optic networks with comprehensive protection on multiple network layers. Recognized security experts founded the company in Germany to help organizations and public authorities protect their networks and thus prevent cyber threats to their critical applications. The development and production processes as well as the encryption solutions have been certified and approved by leading national security agencies.

Adva
NETWORK SECURITY

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

062025.01.EN