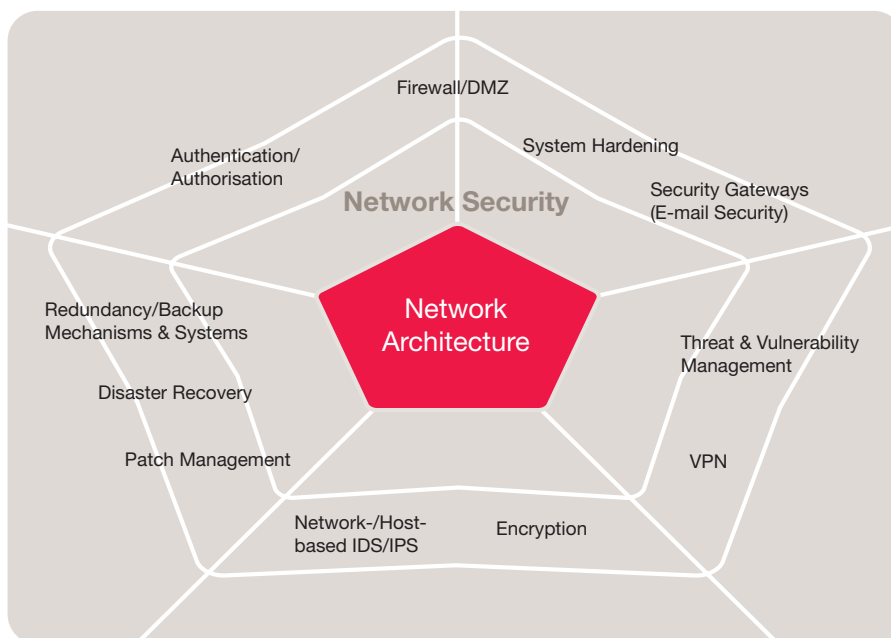


secunet

Network Security

The core of your company needs end-to-end protection



Today's corporations are very diverse. So are their IT landscapes. IT networks have to be assessed not only in terms of size and design, but also in terms of business-critical processes. Finding and implementing the correct degree of security and the appropriate security technologies requires vendor-independent expertise of many years in two main areas: security and network technology.

Why network security?

Security presupposes a holistic approach. Incomplete solutions only offer incomplete protection. Therefore, it is key to consider all elements of your IT network which together guarantee the security of your company. secunet supports you in building a network that is optimised to meet your specific security demands. It begins with risk and threat analyses, covers the definition of protection measures and reaches all the way to the implementation by means of IT systems.

End-to-end, holistic protection of your IT landscape means:

- **Cost-effectiveness:**
Optimisation and extension of existing security components
- **Consistent implementation:** Addressing of all security-relevant aspects
- **Integration:** Intelligent interaction of all the individual security components
- **Central management:**
Reduction of complexity and administration effort
- **Flexibility and scalability**
within the scope of the defined security level

On the basis of the security requirements determined, for instance, by our analyses and audits, secunet checks the existing security mechanisms in your company. The objective is to optimise existing structures to the maximum extent possible and to extend them with required security mechanisms in an appropriate scope.

Firewall architecture

Whenever a network is opened, e.g. to the Internet or to partner networks, security requirements are a crucial issue. Firewall architectures provide effective protection against unauthorised access to the corporate network and its sensitive data. In addition, they enable connection monitoring and controlling via logging and full evaluation of the Internet use all the way to cost allocation. This way, they comprise various security zones which may differ to a considerable degree in terms of authorisations, threats and controllability. In order to reliably regiment these security zones, firewall systems are used. secunet knows the current threats to and weaknesses of IT systems and considers them in selecting the firewall architecture suitable for your specific requirements.

Intrusion Detection and Intrusion Prevention Systems

The dramatic increase of attacks on IT systems shows that networks and servers may have weak points in spite of protection through firewalls and virus scanners. Many companies lack an instrument allowing for detection, verification, tracking and prevention of attacks on an ongoing basis. In this context, Intrusion Detection or Prevention Systems (IDS and IPS) complement your firewalls, VPN gateways and security scanners. Audit and log functions as well as network monitors serve as the basis for the detection of attacks. They document who initiated IT-security-relevant activities when and where. While an IDS works "passively", i.e. triggers an alarm or logs an

attack, an IPS intervenes actively. Attacks are automatically and immediately blocked before damage can be done. However, in order to ensure that only dangerous activities are blocked and legitimate traffic remains unobstructed, systems and requirements-specific settings must be extremely accurate.

Virtual private networks

A virtual private network (VPN) protects the transmitted information from unauthorised access by creating "tunnels" through insecure networks (Internet, WAN, internal networks, etc.) that are protected by strong cryptographic mechanisms. VPNs can be used to network sites (gateway-to-gateway) or to enable secure access from the notebook of a mobile user to the corporate network via the Internet (client-to-gateway). secunet implements suitable VPN components that fully protect your applications and efficiently counteract threats. secunet knows the possible application scenarios. We configure VPNs for your specific requirements, implement the solutions and support you in operating the VPNs.

Why secunet?

secunet is a supplier of products and services specialised in IT security. Since IT security requirements and measures greatly differ from company to company, we do not simply sell solutions out of the box. Instead, we identify each customer's specific requirements to provide customised, maximum security. On this basis, we develop an adequate, scalable and effective security concept specially designed for your corporate network. We take care of implementation and operation on a sustained basis. We are backed by a vendor-independent approach and a number of selected network security partnerships for all conceivable application scenarios.

secunet Security Networks AG

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 230 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

Editor:

secunet

secunet Security Networks AG
Kronprinzenstraße 30,
45128 Essen, Germany
Phone: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 123
E-mail: info@secunet.com
www.secunet.com