Network Security

Are you perfectly protected already?

Are you confident that you could resist a DDoS attacks? That you will be able to detect ransomware or other malware before it attacks your internal information systems? That sensitive data is not leaking outside your organization? That no one can take control over your servers or technology systems? That you will pass any security audit with no major findings? And that your company, while ensuring this, is not facing any major constraints preventing it from regular routine work?

If not, there is still some room left for improving your information security, and network security in particular.

www.aec.cz

What can we help you with?

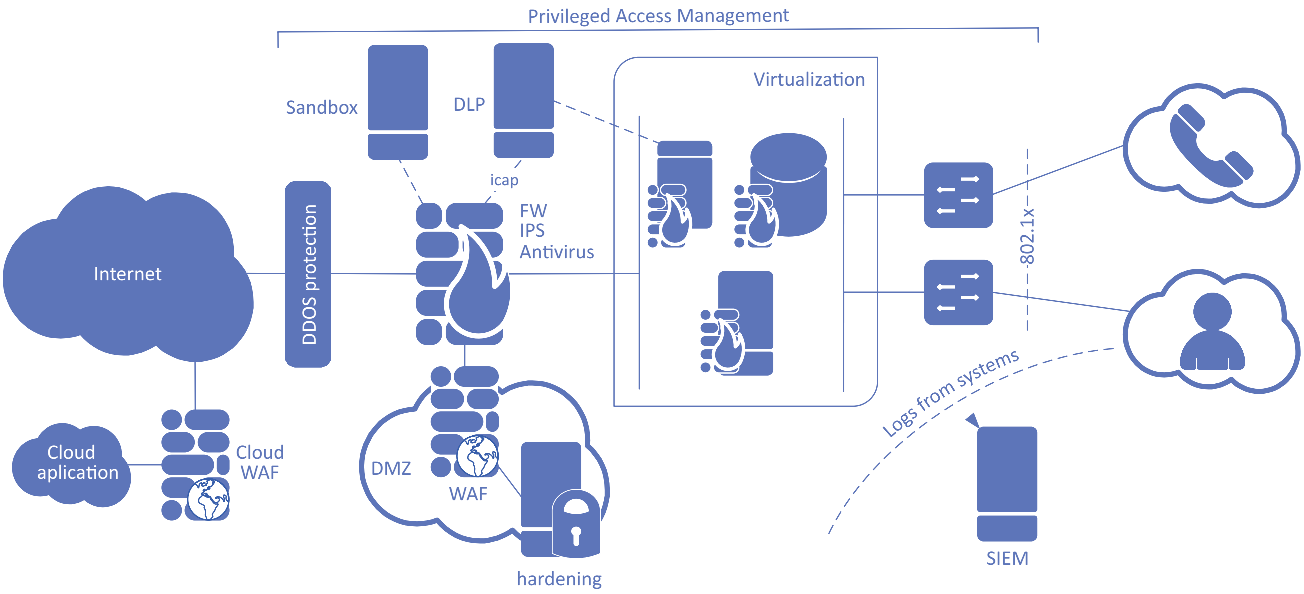
- with network security design,
- with design of appropriate technical measures,
- with their implementation,
- with subsequent maintenance and support,
- with architecture and technology audits,
- with answering your questions and other requirements.

AEC added value

- We are developing our own tools assisting us and our customers with technology management.
- We are testing various combinations of technologies and possibilities of their integration.
- We are using our internal best-practices based on our actual experience from different environments.
- We advise our customers to the best of our ability. We are not trying to promote any specific products.
- We are a long-term partner. We do not engage in half-baked sales of technologies ill-suited for our customers.
- We collaborate with other security teams, thus ensuring continuity regarding other technologies, penetration testing results, and already executed analyses.

Network Security

AEC



Example of network security technology chart.

Technologies we can assist with

Firewall and IPS/IDS

Basic elements of a network infrastructure. We have experience with their implementation and management, including advanced configuration and IPS/IDS protection finetuning.

Application and web firewalls

These technologies are an important part of the network, especially when publishing a service to the Internet. We have experience with their implementation as well as detailed configuration.

Firewall rules management

We implement and integrate tools for firewall policies management and workflow approval. We interconnect technology with business requirements.

Data Loss Prevention

In collaboration with our analytics team, we implement solutions in a meaningful and efficient way not only at the DLP network level but to the endpoint as well.

Log Management and SIEM

Security incident monitoring is an important element of cyber security. Without it, you may find out about your network issue only after it has been published in the media. We have experts specializing in SIEM solutions implementation and management, as well as in subsequent analysis of any incidents detected.

Network monitoring

Network visibility is the key. We will help you to obtain an overview of what your network looks like and the way it is used. You can identify changes that may indicate a security incident by analysing its behaviour.

Vulnerability management a hardening

By continuously monitoring vulnerabilities, we can help you with a timely and efficient configuration of your other technologies, in order to patch the detected weaknesses before there is a fix available.

Centralized Privileged Access Management

This technology makes it possible to track the administrators' actions while providing easier access to the managed systems and secure login.

DDoS protection, proxy etc.

We are also able to help you with DDoS protection, web gateways and many other technologies not making it to this particular list.

Network antivirus software

Malware protection is mostly being moved to the endpoint. However, it is pertinent to have a layered security. Network antiviruses are one of the necessary add-ons to the network security.

Sandboxing

New malware modifications are created all the time. Reputation-based detection is no longer enough. We need to focus on the behaviour. Sandbox can create an environment suitable for malware activation and its subsequent detection.

Cloud technologies

The abovementioned technologies usually come in a cloud variant as well. Our experience includes cloud implementations and architecture designs, with all their specifics.