Network Security Architecture

By Mariusz Stawowski – ISSA member, Poland Chapter

Secure networks are crucial for IT systems and their proper operation. Essential to their design is the security architecture describing the network segmentation and security layers.

Secure networks are crucial for IT systems and their proper operations as most applications work in the networking environment and closely depend on its performance, reliability, and security. Improper network design can be very expensive for a company (i.e., loss of business continuity, security incidents, costs of network rebuilding, etc.). Essential to network design is the security architecture that describes the network segmentation (i.e., security zones) and security layers (i.e., access control, intrusion prevention, content inspection, etc.). An appropriate design of the architecture provides many advantages (e.g., isolation of low trust systems, limitation of a security breach's scope, costs savings).

During network design in order to avoid errors and achieve project cost-effectiveness, recognized principles should be taken into account: compartmentalization, defense in depth, adequate protection, etc. However, there is not one standard network security architecture. Different IT systems have specific and differing requirements that their individual architectures should fulfill. The article provides guidelines for designing the network security architectures and an overview of the architectures of IT systems with high security requirements such as e-commerce and data centers.

An appropriate design of the network security architecture provides many advantages:

- Isolation of low-trust network areas, which can be potentially used to launch attacks against strategic IT system resources
- Limitation of the security breach scope to one system or network segment as well as limiting the incident spreading to other systems
- Accurate network access control to IT system resources as well as monitoring and auditing resource usage and management
- Quick identification of IT systems security incidents based on the events detected in the network areas, where these events should not occur
- Cost optimization by an appropriate IT resource location and segmentation, and deployment of adequate safeguards for requirement compliance (e.g., IT resources requiring expensive safeguards according to PCI DSS, SOX, or other standards are located in separate security zone)

In practical implementations the security zone is a network segment connected to a physical interface or sub-interface (801.2q VLAN) of an access control device (e.g., network firewall) that separates it from the rest of the network. The network communication between different zones is strictly controlled. The security layers are implemented on the network devices (i.e., dedicated safeguards, security modules on the routers and switches). In the design of network security architecture, the safeguards are named as security layers because the protection scope covers an entire zone (i.e., IT resources located in the network segments).

The concept of security layers was adopted by approved guidelines and standards (e.g., ISO/IEC 18028-2:2006). The security layers identify where protection must be addressed in products and solutions by providing a sequential perspective of network security. Mapping of the safeguards to security layers allows determining how the elements in one layer can rely on protection provided by other layers.

Design principles

In practice, deployment of the security products does not always improve the safety of IT system resources. Due to design or configuration errors, the safeguards may not perform their tasks properly, causing an illusive sense of security. Designing an appropriate network security architecture is not an easy task, mainly because in the network there are many different protections, often integrated one with another, such as access control, intrusion prevention, encryption, user authentication, content inspection, etc. The network protections operations depend on the IT system environment, i.e., the safeguards do not create an autonomous system but rather a protection layer complementing and ensuring operating system, application, and database security.

Principles Useful for the Design of Network Security Architectures

Fundamental IT systems security principle	Other rules expanding fundamental principles that are applied in specific conditions
Compartmentalization – IT system resources of different sensitivity should be located in different security zones (also known as Segmentation).	**Choke Point** – Access to IT system resources in the network should be provided through controlled, limited number of communication channels.
Defense in Depth – Protection of IT system resources is based on many security layers which complement and ensure one another (known also as Layered Protections).	**Defense in Multiple Places** – Security elements are distributed in different places of IT system. **Defense through Diversification** – Safety of IT system resources should be based on the protection layers consisting of different kinds of safeguards (also known as **Diversity of Defense**).
Adequate Protection – Protections should be relevant to the threats and values of the resources being protected (i.e., risk analysis results), compliant with law and other regulations, and properly cooperative with other IT system elements.	**Simplicity** – The design and safeguards configuration should be simple and clear, and if technically possible, based on widely approved standards. **Due Diligence** – Ensuring IT system safety requires continual activities that test that the protection mechanisms are operational and that security incidents are being detected and resolved.
Least Privilege – Subjects should have minimal privileges to IT resources which are necessary to perform company's business tasks.	**Information Hiding** – The IT system makes available only the information that is necessary for the company's business operations (also known as **Security through Obscurity**). In the designs of intrusion prevention systems the principle is known as **Attack Surface Reduction**. **Need To Know** – IT system users and administrators should have access to the information relevant to their position and performed duties.
Weakest Link in the Chain – Security level of IT system depends on the least secured element of the system.	**Single Point of Failure** – Protection against failures is achieved by using redundant elements, so called High-Availability (HA). **Fail-Safe Stance** – Access to IT system resources should be denied automatically in case of the safeguards failure (important for data-sensitive assets). **Fail-Open Stance** – Network communication is passed through without control in case of the safeguards failure (important for mission-critical assets).

Recognized principles should be adhered to when designing a network security architecture in order to avoid errors and achieve project cost-effectiveness. The design should apply the following guidelines:

1. The security zones in the network should be planned according to the compartmentalization principle: IT system resources of different sensitivity levels (i.e., different confidentiality class, value, and threat susceptibility) should be located in different network segments, guarded by appropriate protections. Prior to designing the zones, a risk analysis should be performed. IT resources that require special protections according to law, standards, or other regulations should be located in dedicated zones

2. The security layers in the network should be planned according to the *adequate protection* and *defense-in-depth* principles:

   - **Adequate protection** – IT system resources protection should be relevant to the threats and values of the resources being protected (i.e., risk analysis results) as well as compliant with law and other regulations. The principle helps ensure that protections are deployed in a cost-effective way.

   - **Defense in depth** – network security protections should be designed and deployed in such a way that they effectively ensure and complement other layers, i.e., protection means in the operating systems, applications, and databases. In the case of improper operation of one layer (e.g., configuration error, software error, security operation disruptions), the protection of other layers should not allow for an easy attack of the IT resources and should enable quick identification and elimination of the abnormalities/threats.

In medium- and large-scale networks the *simplicity principle* plays an important role, stating that security design and safeguard configuration should be simple, clear, and if technically possible based on widely approved standards. Complicating the security design undoubtedly makes its recognition and subsequent attack possibility more difficult for the intruders. However, from the IT systems resources safety perspective, it is more important that the safeguards are properly designed, configured, and managed. An error in the design or in the security system configuration usually creates a potential vulnerability to breach the IT system resources security.

There are other principles useful in the network security designs. Table 1 summarizes these principles. Deeper explanation can be found in "The Principles of Network Security Design," published in October 2007 edition of *The ISSA Journal.*

E-commerce architecture

E-commerce systems provide IT services in an open networking environment and should be ready to handle Internet threats (i.e., hackers, malicious code, DoS attacks). They deploy a multi-tier network security architecture consisting of Web, application, and database server zones and appropriate security layers. Today the Internet provides standard access for most e-commerce applications, e-banking, and data centers. It is convenient and cost-effective because geographically distributed users do not need to install, configure, and upgrade any client application.

Figure 1 shows an e-commerce network security architecture. The zones construction is relevant to the functional elements of e-commerce systems, i.e., the Web servers are responsible for interaction with the users, the application servers perform data processing, and the database servers provide data storage. The servers of the same type (e.g., Web servers) that provide different e-commerce services should be separated and located in different zones. A dedicated security zone is also created for the management systems.

The security layers are divided into at least two groups – perimeter and internal. Perimeter security layers usually consist of edge routers providing first line of DoS protection and dedicated security devices (i.e., network firewall, data encryption-VPN, intrusion prevention system-IPS, web application firewall-WAF) as well as server-acceleration devices (i.e., load balancing, SSL offload). For effective attack prevention, it is important to perform SSL offload before IPS and WAF inspection (i.e., HTTPS traffic should be decrypted). Internal security layers consist of the firewall and IPS devices that control internal zones and optionally the load balancers for the application and database servers. Other security and acceleration solutions are used if required.

Security concerns in e-commerce systems place restrictions on network communication. Internet users should not have direct access to the application and database servers. The application servers are accessible *only* to the Web servers. The database servers are accessible *only* to the application servers. In simple applications Web servers can directly access the database servers, however, it is not recommended. In properly designed network, for the cybercriminal to gain full access to the e-commerce system, he must first hack the Web servers, then the application servers, and then launch an attack on the database servers. The network security architecture of e-commerce systems is designed in a way to stop hacking attacks in Web server zones.

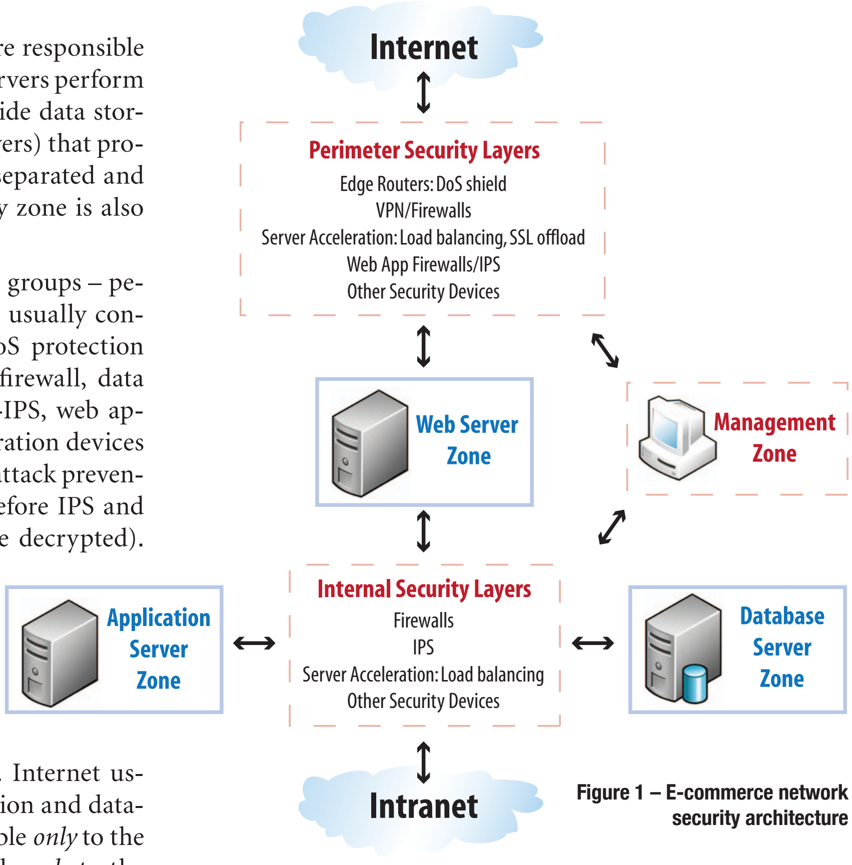
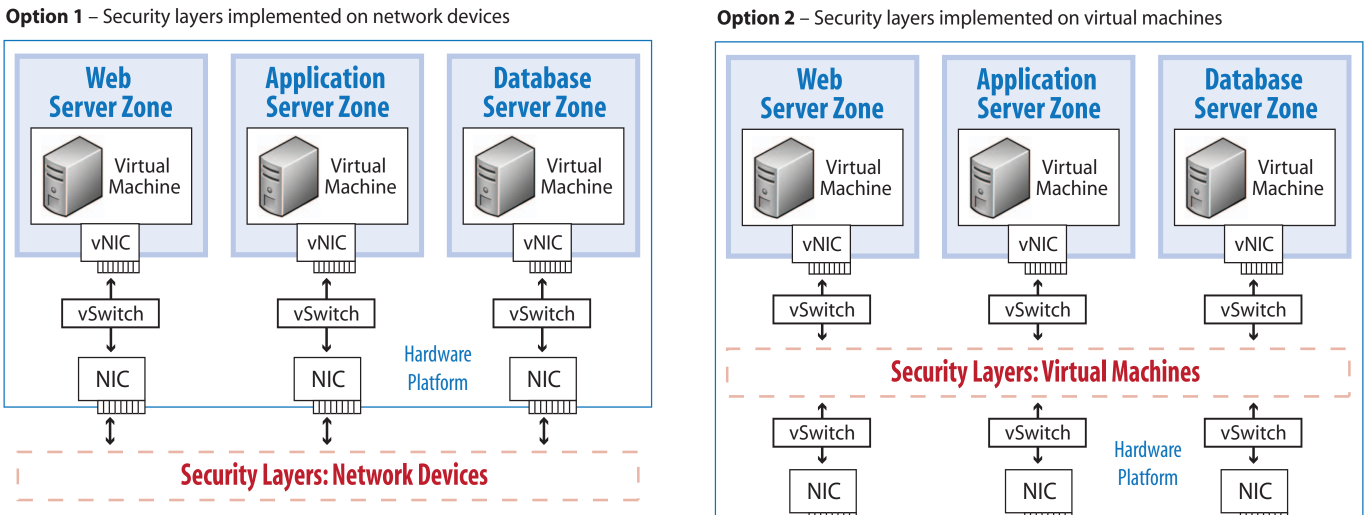


Figure 1 – E-commerce network security architecture

Virtual server protection

Virtual servers are commonly used in IT systems and e-commerce. Consolidation of many servers on one hardware platform provides a cost savings. However, it is important to note that servers in virtualized environment like VMware ESX are vulnerable to the same threats as physical servers (i.e., hacking, malicious code, DoS). E-commerce systems that utilize virtual servers also require appropriate network security architecture, i.e., the security zones and layers. Additionally the safeguards should be ready to handle the attacks specific for the virtualized environment (e.g., vmkernel). See Figure 2.

Virtual servers of different security zones can be separated on dedicated virtual switches (vSwitch) and network interfaces (NIC), or share the same vSwitches and NICs and be separated using VLANs (802.1q). The security zones are created in


Option 1 – Security layers implemented on network devices

Option 2 – Security layers implemented on virtual machines

Figure 2 – Concepts of network security architectures in virtualized environment

similar ways as in physical networks. The security layers can be implemented in two ways, i.e., using the network security devices or the safeguards deployed as virtual machines. Figure 2 presents the concepts of network security architectures implemented in the virtualized environment.

Data center architecture

From the network security perspective, the data center is a centralized IT system consisting of the servers and data repositories, the network and security infrastructure, and the management systems located in the network operation center (NOC).[1] The network security architecture of the data center consists of the same main components as e-commerce system, i.e., Web, application, and database servers security zones with appropriate security layers. However, the implementation is different according to specific data center requirements. The network security architecture implemented in the data center should provide very high throughput and virtualization of switching and routing services to efficiently add new security zones and layers and adjust the network and security infrastructure according to the changes in IT systems.

High security requirements result mostly from the following factors:

- The data center stores IT resources of many different customers (sometimes different departments of one corporation). Consolidation in a single location of IT resources of many companies significantly increases the likelihood of the attacks, especially DDoS.
- The data center operates in open, hostile network environments (Internet, WAN) and provides IT services for large number of users from different companies that have different privileges and trust levels.
- The data center does not manage and control the end users' computers. When these privileged computers are not properly protected they can be used by the intruders and malicious applications to launch attacks at data center resources.
- The data center's servers, security, and network infrastructure can be overloaded as a result of large levels of user activity as well as network attacks.
- Security incidents in the data center can cause huge losses for many companies (i.e., customers of the data center).

There are two main approaches to the design of data center network security architecture. The first recommends building the network based on services switches, i.e., switches with hardware modules that perform additional functions like firewall, intrusion detection, load balancing, etc. The second approach is based on the core routers/switches[2] that at high speed manage and forward the network traffic between the data center network segments. In this model dedicated devices provide security, acceleration, and other required services. This approach is more flexible and scalable and is most often implemented.

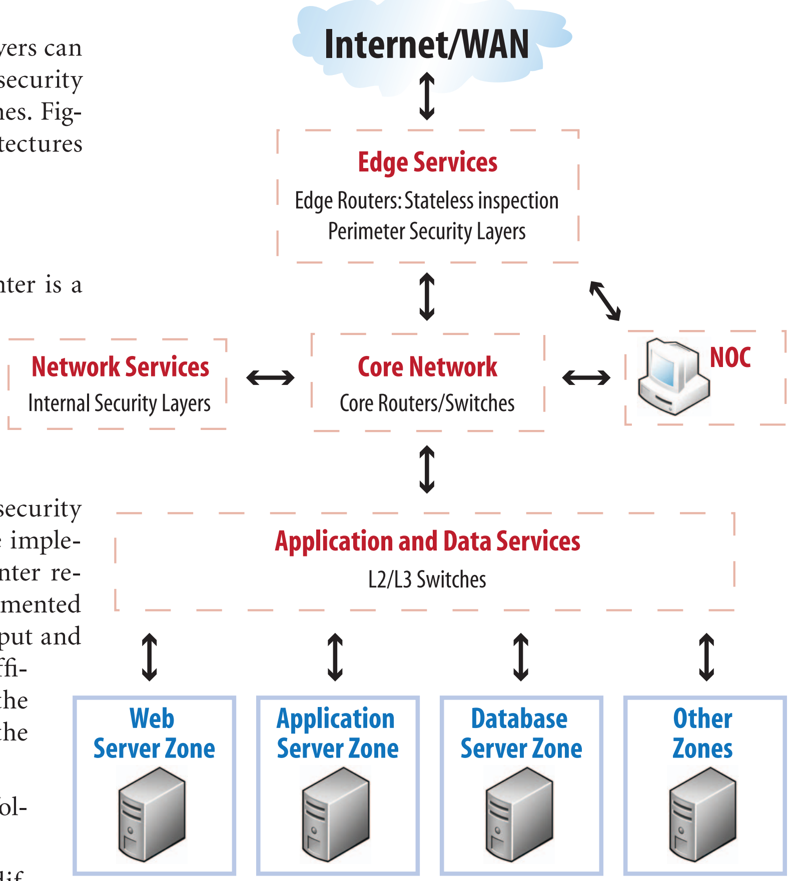


Figure 3 – Data center network security architecture

Figure 3 shows the data center network security architecture based on the core routers/switches. It consists of the following tiers:

- **Edge services**: Edge routers provide network access to the data center from the Internet and WAN, manage traffic with dynamic routing protocols, and implement the first defense layer against network attacks with firewall stateless inspection. Dedicated security devices provide stateful firewall, VPN termination, and other functions. The devices can be located inline or the traffic can be redirected to them by core routers/switches. In this layer also WAN acceleration can be performed.
- **Core network**: Core routers/switches provide network access to all tiers of the data center and perform virtualization of switching, routing, and security services as well as the network analysis.
- **Network services**: Dedicated security devices provide firewall and IPS protection for data center resources and secure remote access for the users (SSL VPN is recom-

[1] Sometimes called Security Operations Center (SOC).

[2] Core network devices provide both advanced L2 and L3 services, and they can be named as a switch or router.

mended) as well as other services like load balancing and SSL acceleration. The devices can work inline or the traffic can be redirected by core routers/switches.

- **Application and data services**: L2/L3 switches provide network connectivity for data center servers and the network storage.

There is also the backbone network that provides connectivity between primary and backup data center facilities.

Ensuring high availability of the data center's services requires IT systems deployment in fault-tolerant, redundant configurations. Additionally IT systems should be geographically distributed in primary and backup locations to be ready for any kind of disaster recovery. Data center protection against massive DoS network attacks can be implemented on the edge routers. They are the first defense layer against external attacks. The routers can provide the traffic inspection in a different way than the network firewalls, i.e., stateless inspection. They can drop unwanted traffic types based on many criteria (e.g., protocol type, flags settings). Carrier-class routers can filter the traffic at high speed in the hardware modules. What is important is that the stateless inspection on the routers allows for the filtering of traffic asymmetrically. This means that traffic does not need to follow a specific path for ingress and egress traffic (as required by stateful inspection firewalls). This flexibility is needed in places like data center access to the Internet and WAN where there is no guarantee of routing symmetry.

Security virtualization

Usually data centers store IT assets and provide services for many different companies. The companies have their own security polices and may require access to logs, alerts, and reports related to their IT assets. The protected assets and the security means of one customer must not be visible to other customers. A conventional way to fulfill these requirements has the provider deploy a large number of network and security devices (i.e., separate devices for each customer), which translates to very high costs. A better solution is security virtualization, i.e., one security device is divided into many parts – so called virtual systems – designated for the protection of different IT resources. Virtual systems are isolated from one another and have their own autonomy (i.e., individual security policy, routing table, network interfaces).

Virtualization can also be utilized in the security management field. Data center customers may require some administrative access to their part of the security system. Deployment of a separate management server for each customer is not efficient. The solution defines management domains in one management server (i.e., management virtualization). Each management domain contains its own configuration and logs as well as separate administrator accounts. Although it is one physical system, the administrators of one management domain do not see other domains.

The virtualization of the security devices and management systems allows for cost-effective data center deployments. However, specific threats related to virtualization should be taken into account early in the design phase. The main risk of virtualization results from the fact that overloading one of the virtual systems can disrupt operations of other virtual systems that share the same hardware platform and as a result disrupt operations of other customers' IT systems. Virtual systems should be properly controlled in respect of shared hardware resources usage (i.e., CPU, RAM, network bandwidth, etc.).

Summary

Secure networks are important for proper operation of IT systems as most applications work in the networking environment. An essential part of the network design is the security architecture that describes security zones and layers. An appropriate design of the network security architecture provides many advantages (e.g., isolation of low-trust systems, limitation of the security breach's scope, cost savings). When designing the architecture to avoid the errors and achieve project cost-effectiveness, recognized principles should be taken into account (i.e., compartmentalization, defense in depth, adequate protection, etc.). There is not one standard architecture. Different IT systems have specific requirements that the network security architecture should fulfill.

References

—Daswani. N., Kern C., Kesavan. A. 2007. *Foundations of Security*, Apress.

—*ESX Server Security Technical Implementation Guide*. 2008 DISA.

—*Government Data Center Network Reference Architecture*. 2008 Juniper Networks.

—*ISO/IEC 18028-2 (ITU X.805) Network security architecture*. 2006 ISO/IEC.

About the Author

Mariusz Stawowski, Ph.D., is Director of Professional Services of CLICO, a security technologies distributor and service provider located in Poland. For more than 10 years he has been responsible for management of security projects. He holds CISSP and PRINCE2 certificates. His doctoral dissertation was elaborated at the Military University of Technology in the special field of IT systems security auditing and network protections designing. Mariusz can be contacted at mariusz.stawowski@clico.pl.