

# **ISi-LANA - A Secure Basic Architecture for Networks Connected to the Internet**

Thomas Haeberlen

Federal Office for Information Security (BSI), Godesberger  
Allee 185-189, 53175 Bonn, Germany

## **Abstract**

This P-A-Per gives a brief summary of a study compiled for the German Federal Office for Information Security (BSI). The study will be published as part of a new series of documents on Internet security later this year.

A basic architecture to support secure operation of a network connected to the internet is proposed. By implementing this basic architecture, the risks associated with connecting a network to the internet, can be greatly reduced. The basic architecture and recommendations cover the robust design of the network, the selection and configuration of network equipment, as well as aspects of network operations. The view is mostly on security aspects of the lower layers of the TCP/IP reference model; application specific aspects of internet security will be subject of additional studies scheduled to appear later in 2007 and in 2008.

## **Introduction**

When a network is connected to the Internet, the IT systems and the information processing are exposed to a great number of threats and attacks that don't exist in a disconnected environment. It is therefore necessary to modify the structure of a network to provide for adequate protection.

In the basic architecture proposed by the ISi-LANA study, both using and providing the most popular services Web and E-Mail are supported. The concept can be adapted to the size and complexity of the network infrastructure, the number and types of services to support and the individual security requirements of applications. The study provides a number of variations covering on one hand small and non-critical IT infrastructures and on the other hand supporting high security requirements by supplementary measures or modular extensions.

The underlying principles of the proposed architecture can be summarised as follows:

- *Defence in depth*: There exist several independent layers of defence. There must be no single point of failure that would allow an attacker to gain access to the internal network after overcoming just one line of defence.
- *Separation of functionality*: Independent functions should be implemented independently („one service – one server“). This holds especially for security-related functionality. This serves to reduce the complexity of the configuration of security components, servers and services, thereby minimising the „contact surface“ and the load of the individual components.
- *Minimality*: All components - especially those of the security gateway itself and of the Internet-facing servers – should be configured in a minimal way. Unnecessary software should be deinstalled, unnecessary functionality should be deactivated.
- *Need-to-Know*: System components, applications and services may only disclose such information on the network and its users, that are essential for the functioning and the use of the IT infrastructure. Available information should be protected according to a role and permissions scheme.
- *Whitelisting*: All filter rules should be such that only explicitly allowed packets or connections are allowed and everything else is blocked („default deny“).
- *Currentness*: Operating systems and applications should always be kept up to date. Available patches should be applied as soon as possible.

## **Basic Architecture**

The core principle of the basic architecture is controlling the data flow between the Internet and the local network by a three-stage security gate-

way in „P-A-P“ setup, i.e. consisting of an outer **P**acket filter, an **A**pplication level gateway and an inner **P**acket filter. No connection should be initiated from the „outside“ with any computer on the internal network. Moreover, the internal network is divided into several security zones separated by packet filters.

For all network zones, private IP address ranges such as 192.168.0.0/16 should be used; the necessary network address translation will be done on the packet filter *PF1*. Ingress / egress filtering and antispoofing rules should be implemented on the perimeter router.

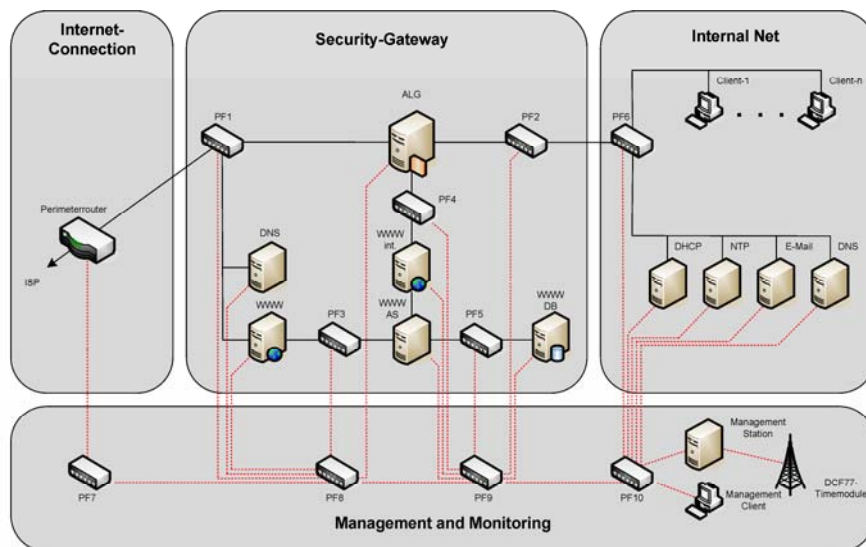


Figure 1: Basic Architecture including management and monitoring network

Regarding the connection to the Internet, the two modes of using and providing Internet services have to be distinguished. While in the first case the communication goes straight over the three steps of the P-A-P security gateway, external requests for any services provided have to be dealt with on a server located in a separate demilitarised zone (DMZ) of the security gateway. These servers can revert to other servers located in downstream security zones of the DMZ.

### Using Internet Services

The P-A-P gateway for using Internet services like WWW and E-Mail consists of the outer packet filter *PF1*, the application level gateway (ALG) containing proxy servers for protocols such as HTTP and SMTP, and the

inner packet filter *PF2*. These two packet filters should support stateful filtering.

The security gateway must not be circumvented. All traffic between the internal network and the Internet has to pass through this gateway, with the gateway using a strict whitelist policy, i.e. allowing only the explicitly permitted protocols. Furthermore, the *ALG* needs filtering capabilities for all supported protocols, notably an E-mail virus (or rather: malware) scanner and a filtering module for the Web proxy. The latter should be configured to filter out most, if not all, Active Content in Web pages. In some cases, JavaScript and other types of Active Content may be required for certain Web sites. Generally, Active Content should only be allowed on a case by case basis for selected sites on a whitelist.

To allow complete control, there can, in general, be no encrypted traffic through the security gateway. Checking this type of traffic requires proxy functionalities on the application level gateway (*ALG*) which allow the decryption and re-encryption of protocols like HTTPS. End-to-end encryption will only be permitted on a case by case basis for selected partners and trustworthy Web sites. While this has some drawbacks, it is a necessary trade-off providing an acceptable security level at the expense of some functionality. As an example, certificate checks for SSL-protected Web sites will not be possible for the end users and will have to be made by the SSL proxy component of the *ALG*. This is, however, the only way to keep malware from directly reaching the internal network through encrypted tunnels.

### **Providing Internet Services**

In the basic architecture, the Internet-facing services *DNS* and *WWW* are covered. A separate server for the administration and an internal web server (*WWW int*), as well as a web application server (*WWW AS*) capable of serving dynamically-generated pages, are foreseen. The *WWW int* server is available as a frontend for the administration of the web services provided, and for providing dedicated web services for users from the internal network. Requests from the internal network to the *WWW int* server have to pass through the *ALG* and the servers are separated from the *ALG* by a packet filter, hence there is a P-A-P gateway between them and the clients on the internal network.

As a backend for the web service, a database server (*WWW DB*) is included in a separate security zone. The communication between this server and the *WWW AS* application server is controlled by a packet filter, limiting the traffic to the necessary protocols, e.g. ODBC, JDBC or a vendor-

specific proprietary protocol. If the database server has to be synchronised with an internal database server, this can be implemented over the management network.

The Internet-facing *WWW* and *DNS* servers are located in a forward security zone of the Security Gateway, separated from the Internet only by the packet filter *PF1*. Therefore, they have to be separated from the downstream servers by the packet filter *PF3*. There is no implicit trust relationship between the *WWW* server and the clients in the internal network. If clients from the internal network want to use the „external“ Web service, the requests are routed through the P-A-P gateway in the same manner as they would be for an external Web server. That way, an intruder who might have captured the *WWW* server, can not use this server as a starting point for attacking computers in the internal network e.g. by placing malicious JavaScript code in the served pages, because malicious code will be filtered out by the application level gateway component.

### **Administration and Monitoring**

Administration and monitoring of all servers and security components in the Security Gateway zone are done „out-of-band“ over a separate management network.

In the management network, log and monitoring data are collected from the individual devices e.g. via remote syslog or SNMP and are stored on one or several management servers (in figure 1, only one server is shown). This allows for central evaluation and correlation of events, giving the administrators the opportunity to quickly detect and react to problems.

In the same way, data from host- or network-based intrusion detection sensors can be collected and processed. If properly implemented, this can give the network early-warning capabilities.

A time server, connected to a high precision time source such as GPS or DCF-77 is placed in the inner zone of the management network. This server is used to synchronise the system clocks of all components of the management and security gateway zones, as well as for the internal NTP server, which provides a network time source for the computers on the internal network.

The management network is divided in several zones by the packet filters *PF7 – PF10*.

### **Implementation and Operations**

As the network architecture alone can not guarantee the security of the network, in the ISi-LANA study the basic architecture is complemented by

extensive advice concerning implementation and network operations. Included are

- basic requirements for all network and server components,
- more specific requirements for switches, packet filters, application level gateway components and servers,
- general configuration advice for the network devices, application level gateway components and servers,

as well as some points concerning operations. For more details concerning procedures and security management, the reader is referred to standards such as the BSI Grundschrift Manual (GSHB).

## **Discussion**

### **Overall Structure**

The overall structure was developed during extensive discussions. Requirements from various sources such as the BSI Grundschrift Manual (GSHB) and the E-Government Manual (EGov) were collected and combined. The resulting structure derives naturally from the requirements and the basic principles mentioned above.

The (ISi-LANA 2007) study provides an extensive list of well-known network-related threats on the lower layers of the OSI reference model. Examples include

- MAC- or ARP-spoofing,
- attacks on the network infrastructure through inter-switch protocols (e.g. STP or VLAN-related protocols) or routing protocols,
- attacks via basic properties of the IP protocol suite (e.g. related to ICMP, fragmentation or broadcast mechanisms),
- TCP- or UDP-related attacks (such as TCP connection hijacking), and
- attacks on DNS and other „service“ protocols.

It was assumed that the network has normal protection requirements. The network structure should provide an adequate level of protection against these threats, while keeping complexity and cost at a reasonable level.

When making trade-offs between security and functionality, security was given precedence over functionality or cost in most cases. In real life, things may not always work out that way. For organisations with a higher risk acceptance, or budget constraints, it is possible to simplify the structure in several places. In (ISi-LANA 2007), a number of variants are dis-

cussed, describing the possible benefits and the associated risks. On the other hand, variants providing better protection for networks with higher protection requirements are also described.

Two examples can serve to illustrate the way the network architecture was developed:

- Out-of-band management is a result of the following requirements: firstly, no connections should be made from outside the security gateway to the inside network. Secondly, on one hand no encrypted tunnels should be permitted, but on the other hand insecure and outdated protocols like telnet and SNMPv1 should not be used on the „main“ network because the data transported over these protocols can be of rather sensitive nature. The separate management network solves this apparent conflict in a natural way.
- The place of the network address translation was chosen to be the packet filter *PFI* for simplicity. Translation further downstream is not necessary due to the requirement that all outbound requests and transmissions should pass through the application level gateway *ALG*, which will terminate the connection coming from the internal network and initiate a new connection on its own external interface. Therefore, the address of the *ALG* is the only address that will show up on *PFI*. Nevertheless, the *ALG* should not get a „public“ IP address because the NAT will protect its TCP/IP stack from direct attacks.

### **Structure of the Security Gateway**

The security gateway is structured in a way that implements different security zones even inside the security gateway itself. Some reasons for this were already discussed above.

The separate internal web server *WWW int* helps to secure the administration interface of the web application server *WWW AS*. Often, web applications have their administration and „members only“ sections reachable more or less directly from the front page. That way, all that is between an attacker and the administration interface is a password and a piece of software that often is not implemented very securely. By separating the management and the internal web service from the outward facing server (assuming that the application server and web content management system support this), this potential problem is eliminated.

Routing all requests even from the clients on the internal network through the application level gateway provides an additional line of defence against attacks on the application layer.

Using separate packet filters *PF3 - PF5* instead of just putting all servers on different interfaces of a larger packet filter was chosen to keep the complexity of the filtering rules down. Using only one packet filter may be possible, but as the complexity of the filtering rules grows very quickly with the size of the communication matrix, the administration of such a central hub device would be quite tricky and the risk for configuration errors would be high.

### **Structure of the Management Network**

While using four packet filters in the Management Network zone may seem like overkill at first, it is a necessary precaution in order to implement the defence in depth principle. If, for example, only *PF7* was used as a single packet filter, this would constitute a single point of failure that, if captured, would allow an attacker to completely circumvent the security gateway and reach the internal network in only one step. In the proposed setup, an attacker will still find himself completely outside the security gateway even after capturing *PF7* and will need to compromise several other security devices before finally reaching the internal network.

Unlike the „main“ packet filters *PF1* and *PF2* in the security gateway zone, *PF7 - PF10* need not necessarily support stateful filtering. Also, the bandwidth requirements of the management network will usually be lower than those of the main internet connection. Therefore the packet filters in the management network can be built with cheaper hardware.

### **Structure of the Internal Network**

The proposed structure of the internal network is not overly sophisticated: the servers are separated from the clients by a packet filter, which should support stateful filtering. Network security inside the internal network consists mainly of configuration options on the switches to limit the impact of attacks on the lower layers of the ISO model, such as ARP or ICMP spoofing.

One more recommendation should be noted at this point: using the VLAN functionality of switches should not be considered a security measure. VLANs can be used to keep broadcast domains small, but they should not be used to separate security zones.

(ISi-LANA 2007) also discusses variants for higher security requirements, such as segmentation of the client network or using a more sophisticated security gateway to protect the server zone.

## **Conclusion and Outlook**

The basic architecture proposed by ISi-LANA provides a good level of protection against threats on the network level and also limits the options of an inside attacker. Due to its modular and extensible design, the architecture can be adapted to different requirements and thus provide a starting point for the design of secure networks in most scenarios.

The study also presents variants for organisations with higher security requirements.

It has to be noted that the implementation of the network structure needs to be complemented by appropriate security measures on the clients in the internal network, ranging from secure configuration to an up to date malware protection. These and other aspects of the security of networks connected to the Internet will be covered in separate modules of the ISi series. The upcoming modules “ISi-Mail” and “ISi-Web” will provide a more in-depth coverage of the most used services in internet-connected networks.

## **References**

- Federal Office for Information Security (2007) “Sichere Anbindung von lokalen Netzen an das Internet” (ISi-LANA)
- Federal Office for Information Security (2006) IT-Grundschutz Manual. <http://www.bsi.bund.de/english/gshb/index.htm>
- Federal Office for Information Security (2006) E-Government Manual. [http://www.bsi.bund.de/english/topics/egov/3\\_en.htm](http://www.bsi.bund.de/english/topics/egov/3_en.htm)