

Guideline   
Separation of networks

Information security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Directive Separation of networks | |  |
| Number | [Number] | |
| Issued on | 14.01.2025 | |
| Through | Information Security Officer | |
| Entry into force | 01.09.2022 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | Information security policy Network connections | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last review | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Table of contents

[1 Principles 4](#_Toc110851925)

[2 Objectives 4](#_Toc110851926)

[3 Controls 4](#_Toc110851927)

[3.1 Connectivity to internal networks 4](#_Toc110851928)

[3.2 Separation of nets 4](#_Toc110851929)

[3.2.1 Gateways between internal networks with low trustworthiness difference 5](#_Toc110851930)

[3.2.2 Gateways between internal networks with a higher trustworthiness difference 5](#_Toc110851931)

[3.2.3 Gateways between office IT and internal server networks 5](#_Toc110851932)

[3.2.4 Gateways between internal live and test networks 5](#_Toc110851933)

[3.2.5 Network connections to external networks 5](#_Toc110851934)

[3.2.6 Wide area networks operated by or on behalf of SÜDVERS 6](#_Toc110851935)

[3.2.7 External access to SÜDVERS internal networks 6](#_Toc110851936)

[3.2.8 SÜDVERS access to the Internet 7](#_Toc110851937)

[3.2.9 Wireless guest networks 8](#_Toc110851938)

# Principles

All connections between networks and between IT systems, ICS/OT systems and security systems located on different networks must be individually identified, verified, documented and approved by the IT system owners or the network owner, and the corresponding communication between these networks must be routed through a well-configured secure network gateway before access to networks is allowed or before leaving networks.

# Objectives

To prevent unauthorized users or unauthorized network traffic from gaining access to IT systems, IT networks or leaving internal systems and networks.

# Controls

## Connectivity to internal networks

All systems connected to internal networks[[1]](#footnote-1) must be authorized before being granted access to any internal resource other than the network transport medium itself. If authorization is not successful, the connectivity of such devices must be restricted to Internet access for systems in end-user networks and to no access for all other systems.

## Separation of nets

Networks that represent different security zones must be separated from each other.

Networks containing systems that are fully managed by 3rd (i.e. the 3rd party has full access to the operating system level) must be separated from each other and from networks managed by SÜDVERS. Similarly, SÜDVERS systems hosted/housed by 3rd must be segregated from other 3rd Party networks.

Network connections between networks in different security zones must undergo an information risk assessment and be signed off by a responsible company representative (e.g. the owner of the network) before they are implemented.

The schematic network zone model and the technical network security controls required to secure the zones and segments against each other are outlined in the Excel table below (click to read):



### Gateways between internal networks with low trustworthiness difference

The gateway functionality between internal networks of the same trust level can be provided by switches, routers or firewalls.

### Gateways between internal networks with a higher trustworthiness difference

The gateway between networks with a higher trustworthiness difference must be at least a stateful inspection firewall with IPS functionality.

### Gateways between office IT and internal server networks

Networks used for office IT and internal IT server environments must be kept separate.

All applicable controls described in the chapter "Gateways between internal networks with a higher trustworthiness difference" apply.

### Gateways between internal live and test networks

Networks that are used for live or test environments (infrastructure) or sandbox environments (IT solutions) must be separated from each other.

All applicable controls described in the chapter "Gateways between internal networks with a higher trustworthiness difference" apply.

### Network connections to external networks

All applicable controls as described in the chapter "Gateways between internal networks with a higher trustworthiness difference" also apply to external network connections.

Network interconnections with external networks with a high difference in trustworthiness (such as the Internet) that are used for incoming communication must be additionally secured by

* Two-stage firewall design[[2]](#footnote-2)
* Network-based intrusion prevention systems (IPS) that run in mixed mode in order to
  + Block known attack patterns
  + detect other suspicious traffic and log corresponding events
* Antivirus scan for incoming and outgoing data traffic
* URL filtering

Networks accessible via external connections must be designed to use an agreed set of security controls for information formats and communication protocols.

Networks that are accessible via external connections must:

* Restrict external network traffic to certain parts of IT systems and networks
* Restrict connections to certain access points (e.g. certain network gateways, terminal servers)
* Check the source of external connections (e.g. by checking the source IP address or the certificate)
* Log security-related activities (e.g. unsuccessful login attempts to firewalls by authorized users and unsuccessful changes to access rights for applications and resources)
* Document details of the external connections established (e.g. Internet, ISDN, site-to-side VPN and dial-up VPN).

### Wide area networks operated by or on behalf of SÜDVERS

Network connections via the SÜDVERS WAN must be secured by access control mechanisms (such as ACLs, VPLS configurations...) to ensure that only valid internal systems and networks can communicate with each other via the WAN backbone.

Depending on the difference in trustworthiness, encryption of the WAN traffic should be considered.[[3]](#footnote-3)

### External access to SÜDVERS internal networks

External access to internal networks (e.g. via Internet connections) must be restricted by:

* Establishment of "demilitarized zones" (DMZ) between internal and untrusted external networks
* Two-stage firewall design[[4]](#footnote-4)
* Forwarding of network traffic through firewalls (e.g. stateful inspection firewalls (typically at the edge of a network) or proxy firewalls (typically between internal networks))
* Forwarding of data traffic through network-based systems to prevent intrusion
* Granting access only to certain business applications, IT systems or certain parts of the network (e.g. domains).

Network-based IPS systems must be configured in such a way that they

* Check all connections (regardless of whether they come from outside or not)
* Automatically take appropriate action based on threat level and vulnerability status

Unauthorized external connections must be identified (e.g. for investigation or possible removal) by:

* carrying out checks of the installed network components and documentation to identify discrepancies with records of known external connections
* the use of computer and network management and diagnostic tools

### SÜDVERS access to the Internet

Internal systems that access external networks must be secured by

* Restrict connections to authorized services, devices or users
* Performing virus and malware checks on the Internet gateway or at proxy level
* Blocking Internet connections for unauthorized types of communication
* Avoid connections to websites that offer undesirable content (e.g. known attack sites, sites with illegal content, ....)
* Direct, uncontrolled connections from internal systems to the Internet must be prevented and secured by centrally managed systems.

### Wireless guest networks

* Guest networks may not be used by SÜDVERS employees for business purposes.
* Guest networks must be separated from all other internal networks and treated at the same security level as the Internet.
* Users connected to guest networks must be authenticated with a temporary user name and password.
* Systems that are connected to guest networks may only have an Internet connection.
* Internet access from systems in the guest network must be routed through web proxies to ensure that the requirements of the "Web filtering" policy are met.
* The bandwidth allocated to guest networks must be managed in such a way that communication from/to such a network segment has no negative impact on other internal network segments or external connections used for business purposes.

1. An internal network is any network that is operated by or on behalf of SÜDVERS. The only exceptions are guest networks that are not connected to networks other than the Internet. Guest networks are treated as an external, completely uncontrolled and unmanaged network. [↑](#footnote-ref-1)
2. Please note that VPN gateways must not bypass the firewall and IPS requirements (simply passing SSL through an IPS does not fulfill the requirement of a two-tier design). All traffic from VPN connections terminating at the gateway must be routed through an IPS (can be operated on the VPN gateway) and an additional firewall. [↑](#footnote-ref-2)
3. If confidentiality and risk management are covered in the service agreement with the WAN provider, the use of encryption should be considered very carefully due to the significant design and cost implications. If there are no regulatory or legal requirements for the encryption of data over controlled WAN connections, the use of ACL on the WAN routers may also be considered sufficient. [↑](#footnote-ref-3)
4. Please note that VPN gateways must not bypass the firewall and IPS requirements (simply passing SSL through an IPS does not fulfill the requirement of a two-tier design). All traffic from VPN connections terminating at the gateway must be routed through an IPS (can be operated on the VPN gateway) and an additional firewall. [↑](#footnote-ref-4)