-



Security Policy   
Network components

Information security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Network components | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | CInformation Security Officer | |
| Entry into force | 04.07.2022 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG, its majority-owned subsidiaries, and SÜDVERS International GmbH | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last | 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 Configuration of network devices 4](#_Toc108074830)

[1.1 Principle 4](#_Toc108074831)

[1.2 Objective 4](#_Toc108074832)

[1.3 Controls 4](#_Toc108074833)

[2 Management of the physical network 7](#_Toc108074834)

[2.1 Principle 7](#_Toc108074835)

[2.2 Objective 7](#_Toc108074836)

[2.3 Controls 7](#_Toc108074837)

[3 Firewalls 9](#_Toc108074838)

[3.1 Principle 9](#_Toc108074839)

[3.2 Objective 9](#_Toc108074840)

[3.3 Controls 9](#_Toc108074841)

# Configuration of network devices

## Principle

The network devices must be configured in such a way that they function as desired and that unauthorized or incorrect updates are prevented.

## Objective

Ensure that the configuration of network devices is correct and does not jeopardize the security of the network.

## Controls

There must be documented standards/procedures for the configuration of network devices (such as routers, firewalls, switches and wireless access points) that cover the following

* Principles of the security architecture
* Standard procedure for security management
* Device configuration
* Restricting access to network devices
* Vulnerability and patch management
* Changes to routing tables and settings in network devices
* Regularly check the configuration and setup of network devices.

Network devices must be configured so that they:

* enforce the separation between networks that have been assigned different security zones/levels (e.g. the separation of dedicated, classified networks from the corporate network)
* Protection from untrusted environments (e.g. external networks, company networks or the internet)
* Separation of networks managed by the company from networks that are not controlled by SÜDVERS (e.g. networks operated by a supplier or business partner on site)
* Restrict malicious activity if one or more network zones are compromised.

The security controls for network devices must take into account the principles of the security architecture (e.g. "Secure by Design", "Defense in Depth", "Secure by Default", "Default Deny", "Fail Secure", "Secure in Deployment" and "Usability and Manageability").

Standardized security management procedures must apply to network devices, which include the following

* Restricting physical access to network devices to authorized personnel (e.g. by placing them in protected data centers or special, locked storage rooms or computer cabinets)
* Hardening the operating systems that support them (e.g. by patching all known vulnerabilities, disabling unnecessary services, removing unnecessary scripts, drivers, functions and subsystems and changing insecure default parameters provided by the manufacturer such as passwords and SNMP community strings)
* Use of a comprehensive set of management tools (e.g. maintenance utilities, remote support and enterprise management tools)
* keeping the network devices up to date (e.g. by applying change management and patch management)
* Monitoring of network devices (e.g. with SNMP) so that events such as hardware failures and external attacks can be detected and responded to effectively

As far as technically possible, the network devices must be configured (usually on the basis of a secure standard setup) in such a way that:

* To emphasize overload or exceptional conditions when they occur
* log specified security-relevant events in a verifiable form and store them on a separate system
* copy control information (e.g. event logs and tables) to authorized portable storage media
* Integration with access control mechanisms in other devices (e.g. for strong authentication)
* Use of a predefined secure setup when booting
* ensure that passwords are not sent in plain text
* Deactivation of source routing (to retain control within the packet forwarding device).

Access to network devices must be restricted to a limited number of authorized administrators, using access controls that support individual accountability, and devices must be protected from unauthorized access.

IT must have a process for dealing with vulnerabilities in network devices that includes the following:

* Monitoring for known vulnerabilities (e.g. by monitoring security vendor websites, following CERT advisories, subscribing to vulnerability notification services, utilizing intelligence services or using vulnerability scanning software)
* Issue instructions to network specialists on what to do if a network device fails
* Regulations for compliance with the "Vulnerability and patch management" guideline
* In which cases and how network traffic is automatically redirected to an alternative network device

Network devices that perform routing (e.g. routers and switches) must be configured to prevent unauthorized or incorrect updates by

* Checking the source of routing updates (e.g. by using techniques such as Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Enhanced Interior Gateway Routing Protocol (EIGRP) or Border Gateway Protocol (BGP))
* Checking the destination of routing updates (e.g. by only sending updates to certain routers)
* Protection of the exchange of routing information (e.g. through the use of passwords/passphrases) where possible
* Encryption of the routing information exchanged, where possible.

Network devices must be checked regularly (e.g. using NMS systems) to verify configuration settings, assess the strength of passwords and, if necessary, assess the activities carried out on the network device (e.g. by inspecting logs).

# Management of the physical network

## Principle

Networks (including voice networks) must be protected by physical controls and supported by accurate, up-to-date documentation and labeling of key components.

## Objective

Ensure that networks (including voice networks) are configured accurately and securely, and that there are documented guidelines on what security requirements must be met.

## Controls

The internal infrastructure of telecommunication cables (e.g. network and telephone cables) must comply with ISO/IEC 11801.

Internal telecommunication cables (e.g. network and telephone cables) must be protected by:

* Attaching identification labels to communication devices and cables
* Locking the inspection and end points (e.g. in a locked cabinet or locked room)
* Provide alternative feeds or relocations
* Avoid routes through publicly accessible areas.

Network access points (e.g. ports on switches, routers, etc.) must be protected by:

* they are stored in secure environments (e.g. in locked rooms or cupboards)
* they are deactivated on the network device (e.g. a network switch) until they are needed.

The networks must be supported by documentation that includes the following

* Diagrams of the network configuration showing nodes and connections
* a list of communication devices, software, connections and services provided by external parties
* one or more diagrams of the internal cable routes for each physical location
* Configurations and settings for internal switchboards
* Details of the telephones and the associated lines/cables.

Network documentation (e.g. labels, diagrams, inventories and schedules) must clearly identify critical environments and data flows that, if compromised, could have a significant impact on business operations or regulatory compliance. Corresponding information must be included in the respective criticality analyses of the systems that use the respective communication networks.

The network documentation (e.g. diagrams, inventories and schedules) must:

* be kept up to date
* be easily accessible to authorized persons
* are regularly checked by network specialists
* electronically with the help of software tools.

The cabling and the devices must:

* Regular physical inspection, where feasible
* Comparison with the network documentation
* be investigated in cases of suspected or actual abuse.

# Firewalls

## Principle

Network traffic must be routed through a firewall configured to best-practice standards before access to networks is allowed or before it leaves networks.

## Objective

Prevent unauthorized network traffic from gaining access to or leaving networks.

## Controls

The networks must be protected by one or more firewalls against malicious data traffic in other networks or sub-networks (internal or external).

There must be documented standards/procedures for the management of firewalls (or similar devices capable of filtering network traffic, such as switches and routers) that include the following:

* Filtering of certain types or sources of network traffic (e.g. IP addresses, TCP ports or information about the status of communication and users)
* Blocking or otherwise restricting certain types or sources of network traffic
* Development of predefined rules (or tables) for filtering network traffic
* Protection of firewalls against attacks or failures (e.g. by restricting access to authorized persons)
* Limiting the disclosure of information about networks and network devices
* Application of the principles of the security architecture during configuration
* Documentation and regular review of firewall rules (e.g. monthly).

Firewalls must filter network traffic on the basis of:

* Source and destination addresses (e.g. IP addresses) and ports (e.g. TCP ports)
* Information about the status of the associated communication (e.g. saving the outgoing port command of an FTP session so that an associated incoming FTP communication can be compared with it)
* Information about the status of users (e.g. permission to access users only if they have been authenticated in a previous communication)
* the validity of a network service (e.g. by using an application proxy firewall).

The firewall configuration must take into account the principles of the security architecture (e.g. "Secure by Design", "Defense in Depth", "Secure by Default", "Default Deny", "Fail Secure", "Secure in Deployment" and "Usability and Manageability").

Firewalls must be configured in such a way that they:

* protect communication protocols that are vulnerable to abuse (such as HTTP, HTTPS, SSH, FTP, SMTP, Telnet and UUCP)
* Block network packets that are typically used for denial-of-service attacks (e.g. ICMP echo, UDP and TCP echo, batch and discard)
* Denial of incoming data traffic if the source address is known to be forged (e.g. if the source address pretends to originate from the destination network)
* Denial of outgoing data traffic if the source address is known to be forged (e.g. if the source address does not correspond to the network from which it originates)
* restrict the disclosure of information about networks at network level through IP masquerading (such as Network Address Translation (NAT) or Port Address Translation (PAT)).

Firewalls must be configured to block or otherwise restrict communication based on specific sources/destinations:

* Addresses (e.g. a specific IP address)
* ports (e.g. ports 20 and 21 for FTP and port 23 for Telnet).

The filtering of network traffic must be based on predefined rules (or tables) that:

* have been defined by trusted persons and approved by the respective specialist department as part of change management
* explicitly enforce the principle of "default denial" (e.g. by including a DENY-ALL rule (or equivalent) that applies after all other rules have been processed)
* Use clear, consistent naming conventions (such as host name, IP address or network area)
* are grouped together (e.g. 20 rules) to make it easier to manage and understand long rule sections
* are documented (with version control) and kept up to date
* take into account the information security policy, network standards/procedures and user requirements.

Before new or modified rules are applied to firewalls, their strength and correctness must be tested, checked and signed off by the network owner.

Firewalls must be protected against attacks by:

* Restrict administrator access to a limited number of authorized, qualified persons, e.g. firewall administrators (e.g. through strict access control mechanisms and strong authentication)
* Restrict administrator access to special accounts that are only used for firewall management
* Encryption of administrator access (e.g. by using secure administration consoles, secure remote login shells such as SSH or encrypted connections with TLS, IPsec or equivalent methods)
* Restriction of administrator access to a central point (e.g. in a Network Operations Center (NOC) using a minimum number of firewall management consoles)
* Preventing information about the firewall (e.g. manufacturer and model of the firewall, version numbers of the operating system and security software) from being passed on in the network.

Firewall configurations must be documented (e.g. in a configuration management database (CMDB) or an equivalent database) and contain a justification for:

* Standard services, protocols and ports that are allowed to pass through the firewall (e.g. HTTP (80), HTTPS (443) and SSH (22))
* Services, protocols and ports that are inherently vulnerable to abuse (e.g. SQL Server (1433), FTP (21), NetBIOS (139), RPC (593), Telnet (23), POP3 (110), IMAP (143), PPTP (1723) and SNMP (161)).

The firewall configurations must be checked regularly (e.g. quarterly) to ensure that:

* each firewall rule is approved and signed off by the relevant head of department
* expired or unnecessary rules are removed
* contradictory rules are resolved
* unused/duplicated objects (such as networks or information systems) are removed
* the system administrators responsible for firewall management are informed about the current configurations, security policies and operating procedures.