Security requirement

# Architecture of the access and transport network

Deutsche Telekom Group

| | |
|---|---|
| Version | 2.1 |
| Date | Dec 1, 2019 |
| Status | Released |

# Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

| File name | Document number | Document type |
|---|---|---|
| | 3.57 | Security requirement |

| Version | State | Status |
|---|---|---|
| 2.1 | Dec 1, 2019 | Released |

| Contact | Validity | Released by |
|---|---|---|
| Telekom Security<br>psa.telekom.de | Dec 1, 2019 - Nov 30, 2024 | Stefan Pütz, Leiter SEC-NIS |

Summary
This document sets out the specific technical security requirements that must be implemented to protect IP-based access and transport networks.

# Table of Contents

# 1. Introduction

This security document has been prepared based on the general security policies of the group.

The security requirement is used as a basis for an approval in the PSA process, among other things. It also serves as an implementation standard for units which do not participate in the PSA process. These requirements shall be taken into account from the very beginning, including during the planning and decision-making processes. When implementing these security requirements, the precedence of national, international and supranational law shall be observed.

# 2. General

| Req 1 | The operational network and its systems must be entirely separate from the test and development systems. |
|---|---|

The operational network and its systems must be entirely separate from the test and development systems. Physical separation would be preferable. Logical separation is only permitted if the logical separation of both system types cannot be avoided. Furthermore, it must be ensured that production security will not be affected by activities on the test and development systems.

Any communication required between the operational systems and the test/development systems must be via a secure connection. This means that communication between the systems must take place via a separate system such as a firewall or a router with access control list, which is necessary to ensure implementation of the most restrictive rules possible for communication.

*Motivation: A sufficiently secure system status cannot be assumed in the case of test and development systems because these systems are typically subject to permanent changes. If operational systems or networks are used for test and development activities, and if communication between the various system types is not secure, the operational environment may be accessed by an unauthorized party from the test/development environment or the stability and availability of this environment may be impaired. Another benefit of a complete separation of the operational environment from the test and development systems is that the latter can then be permanently used for acceptance tests. This ensures, for example, that security updates can be tested and made available more quickly even during critical phases (or "frozen zones").*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability

ID: 3.57-1/2.1

| Req 2 | The IPv4 and IPv6 infrastructure address space of the transport network must not be accessible from customer lines and connected networks. |
|---|---|

The infrastructure address space of the transport network is used for accessibility within the network. These addresses are, for example, used to transmit the control plane traffic. These addresses must not be accessible, or only to a very limited extent, from the outside, i.e., from customer lines or connected networks such as the Internet. Accessibility must therefore be restricted. There are various possible approaches to achieve this. One of them is, for example, to use access control lists on routers to protect the infrastructure address space (iACL).

*Motivation: If the infrastructure address space of the transport network is accessible without restrictions, this can be used by attackers to carry out denial-of-service attacks against individual systems or the entire network. Furthermore, services (routing and other control plane protocols) in the network can also be accessed as a result. This makes it possible for third parties to directly manipulate the infrastructure.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.57-2/2.1

## 2.1. System management

| Req 3 | A reliable transfer of control and management traffic must be ensured. |
|---|---|

Data packets used to exchange control plane information and to manage different systems in a network must be transferred with the highest priority. To do this, relevant packets must, for example, be transported in a sufficiently prioritized quality-of-service class.

*Motivation: If control, management and user traffic in a network was handled in the same way, this could mean that in extreme situations the necessary control information could no longer be exchanged and access to management services would no longer be possible. It would also mean that the affected systems could no longer be accessed in order to perform maintenance and troubleshooting tasks. Such a situation could lead to the network becoming unstable or even availability being impaired. An attacker could exploit this in order to cause network outage by means of denial-of-service attacks.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.57-3/2.1

| | |
|---|---|
| Req 4 | If data needs to be exchanged between management plane and planes for user and control traffic, this communication must be protected. |

Management traffic must generally be separated from control and user plane traffic. It may, however, be necessary to exchange data between the different planes. If this is required, the exchange may only take place via secure connections. The bidirectional restriction of the permissible communication relationships to necessary sender and recipient is required here for protection purposes. Any communication relationships that are not necessary must be prevented.

*Motivation: If unprotected communication between different network planes is possible, an attacker can exploit this situation to attack system management services. If such an attack is successful, the result is generally that the relevant system is fully compromised.*

For this requirement the following threats are relevant:
- Unauthorized access to the system

ID: 3.57-4/2.1

| | |
|---|---|
| Req 5 | After a successfull authentication on a network device it must not possible to access other network devices or systems without anew authentication. |

Following successful authentication to a network device, it shall not be possible to gain access to the management of another network device or system without renewed authentication. Renewed authentication shall therefore be enforced for login to another network device.

*Motivation: This measure prevents an attacker using a compromised network device to gain access to other network devices or systems without renewed authentication.*

For this requirement the following threats are relevant:
- Unauthorized access to the system

ID: 3.57-5/2.1

## 2.2. Control plane protocols

| | |
|---|---|
| Req 6 | Mutual authentication must be used for internal signalling protocols through which path information is exchanged. |

For signalling protocols, such as routing protocols (IBGP, OSPF, IS-IS, etc.) and other protocols, via which path information is distributed (LDP, RSVP, etc.), mutual authentication of the communication partners must be used. The data used for authentication must be protected against viewing and tampering by means of a cryptographic procedure. As secure a procedure as possible must be selected here.

*Motivation: An attacker can interfere with signalling protocols in order to tamper with path decisions in the network, to divert traffic or to disrupt communication. Signalling protocols and the services open for them on a network device also bring the risk of denial-of-service attacks. These attacks can also be prevented by the use of authentication of the involved communication parties for the relevant signalling protocols.*

For this requirement the following threats are relevant:
- Unauthorized access to the system

- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability

ID: 3.57-6/2.1

| Req 7 | Routing protocols must be disabled on interfaces where routing updates need not be sent or received. |
|---|---|

Routing protocols, and thus the sending of routing updates, may only be enabled on interfaces to other network elements where there is a neighborhood relationship in place within the framework of the relevant routing protocol. On all other interfaces, the routing protocol must be disabled.

*Motivation: An attacker could glean information from recorded routing updates that contains details about the network architecture. This information could be used to plan and implement further attacks.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.57-7/2.1

| Req 8 | TTL security must be used for EBGP. |
|---|---|

EBGP packets (External Border Gateway Protocol) are sent with a TTL value of 1 in order to ensure that they are not transferred beyond a router. The TTL security function means that EBGP packets are sent with the highest possible TTL value. The TTL value is calculated using the following formula: "255 – [maximum number of necessary hops]." On the BGP neighbor, the function must be enabled with the same TTL value. This is the only way to ensure that BGP packets with a value that is smaller than the predefined one are discarded. The TTL security function is not supported by all manufacturers.

*Motivation: An unprotected BGP service can be taken over by an attacker. It is also possible for denial-of-service attacks to be carried out on accessible BGP ports and thus on the relevant router. By implementing this measure, attacks using fake BGP packets from external networks can largely be prevented.*

For this requirement the following threats are relevant:
- Unauthorized modification of data
- Disruption of availability

ID: 3.57-8/2.1

| Req 9 | If prefixes are exchanged with a customer via a routing protocol, the maximum number of prefixes must be limited. |
|---|---|

When a router is informed about new routes via routing updates, it enters them in its routing table. The size of the routing table has a direct influence on the memory and CPU usage of the router. This is why the maximum number of learnable routes should be limited depending on the hardware used.

*Motivation: A routing table that is too large can lead to critical utilization levels for system resources such as RAM and CPU. An attacker can exploit this specifically to compromise the availability of a network element or even entire sections of the network by means of faked routes.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.57-9/2.1

# 3. Access network

| Req 10 | A standardized authentication procedure must be used in order to ensure the authenticity of a customer device. |
|---|---|

It may be necessary to verify the authenticity of devices connected to the access network via authentication. By this means it can be ensured that only known and thus trustworthy systems can be connected to the network. This is mainly useful for systems and network elements that are operated in environments that cannot be monitored, or for customer systems. Possible solutions include IKE/IPSec as well as IEEE 802.1X (with EAP) for port-based network access control (PNAC).

*Motivation: Network elements that are operated in non-secure environments (e.g., multi-functional street cabinets, CPE) are subject to an increased risk of manipulation or unauthorized exchange of devices. Appropriate device authentication means that only trustworthy systems can be connected to the network.*

For this requirement the following threats are relevant:
- Unauthorized access to the system

ID: 3.57-10/2.1

| Req 11 | If addresses are assigned dynamically, they must be protected against manipulation. |
|---|---|

If a dynamic assignment of IPv4 or IPv6 addresses such as DHCP is used, relevant systems must be protected against the following scenarios:

- Manipulation of address assignment using fake response packets.
- Using up the available address pool.

In the case of DHCP, protection against fake response packets and/or against a fake DHCP server must be set up via the DHCP snooping function. Protection against the manipulative allocation of the available address space may involve, for example, limiting the maximum number of addresses that can be accessed per line, and/or the MAC address. However, this requires the implementation of a further measure that stops the fake MAC addresses on a line.

*Motivation: The automated assignment of addresses can be manipulated by an attacker. One possible way of doing this is to redirect traffic using fake response packets in order to record data in need of protection. Another attack scenario would be using up the available address pool, whereby no more addresses are available for other systems and the functionality of the systems is impaired.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability

ID: 3.57-11/2.1

| Req 12 | if control plane protocols are exchanged with customers a rate limit must set. |
|---|---|

Control plane protocols are an important control mechanism in the network and are also exchanged with customers, e.g., in order to exchange routing and authentication data. This results in a risk as insufficient protection can compromise the transport platform. For this reason, a rate limit must be configured for control plane protocols that are exchanged with customers. Dimensioning depends on the available performance of the network elements used.

*Motivation: The resources (e.g., CPU, memory) of a system are limited. This can be deliberately exploited or, via targeted attacks, also impair system availability. In this case, mass-generated control plane protocol packets are used to generate a high load on the system affected.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.57-12/2.1

| Req 13 | With Ethernet-based customer lines, the maximum number of MAC addresses that can be learned on the network side must be limited. |
|---|---|

If it is necessary for MAC addresses of customer devices to be learned on the network side, the maximum number of addresses per customer must be limited. Lines on which MAC addresses must be learned include, for example, Ethernet-based and VPLS/Layer 2 VPN customer lines. The maximum number of MAC addresses to be learned depends on each individual case and on the hardware used and cannot therefore be specified authoritatively.

*Motivation: An attacker can use fake packets with a high number of different MAC addresses to overbook existing resources so that the functionality, and thus, availability of systems is impaired.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.57-13/2.1

| Req 14 | VLAN tags that originate from customer lines or external networks must not be used to control traffic. |
|---|---|

VLAN tags can be freely manipulated and are thus classified as not trustworthy if they are assigned on the customer side. VLAN tags must therefore be handled appropriately at the network boundary. Depending on the usage model, the following methods can be used:

- With a Layer 2 VPN service, the customer sends packets with a VLAN tag (C-tag). This C-tag must not be analyzed within the network; instead, the traffic must be transparently routed to another customer location. This means that within the network the traffic must be encapsulated. This can, for example, be achieved using an additional provider tag (P-tag) assigned at the network boundary.
- If no traffic with VLAN tags is expected from a customer, packets with VLAN tags must be rejected.

If, in deviation from this requirement, VLAN tags from the customer are used for network-internal traffic control, a check must be carried out at the network entry point to determine whether the VLAN tag is correct for this customer and that there is no multiple tagging (Q-in-Q).

*Motivation: Using manipulated VLAN tags, an attacker may break out from his permitted communication channel in order to access other systems in the network or systems of other customers.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability

ID: 3.57-14/2.1

| Req 15 | QoS values in packets that originate from customer lines or external networks must not be trusted. |
|---|---|

Quality-of-service (QoS) is used in the network to prioritize traffic flows. This is used within the network for the prioritized transfer of control and management traffic. Furthermore, different traffic classes for customers are implemented using this technology. It is therefore necessary for the parameters used for this to be assigned in packets (TOS-bits) or frames (p-bits) in trustworthy systems. This means that relevant values, in packets or frames, which originate from customer lines or from connected third-party networks, must not be trusted. On network elements at network edges, these values must be overwritten and changed to in-house values.

*Motivation: If an attacker can manipulate the QoS class of packets, it may be possible to upgrade traffic and thus to use services that do not comply with his contract or to influence the transport of other customers' data and the transport platform.*

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability

ID: 3.57-15/2.1

## 3.1. Protection against spoofing

| Req 16 | Spoofed ARP packets must be identified and rejected. |
|---|---|

Protection must be provided on a network element or on a separate system in the network through which the spoofed ARP packets are identified. The preferred measure for this is to use ARP inspection to monitor the ARP cache and traffic and thus to identify ARP spoofing attacks. Other, and in some cases, additional measures include deactivating proxy ARP and gratuitous ARP as well as using static ARP entries.

*Motivation: An attacker can use ARP spoofing attacks to prepare, e.g., man-in-the-middle attacks on systems located in the same network as the attacker. To do this, he sends spoofed ARP packets to systems in the network, whereby any traffic that is to be sent to the originating system is redirected via the attacker's system.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability

ID: 3.57-16/2.1

| Req 17 | Frames of customer lines with the same MAC sender and destination address must be rejected. |
|---|---|

Identifying and filtering frames with fake MAC addresses is time-consuming and only possible to a limited extent. For this reason, at least those frames that contain an invalid MAC sender and destination address combination must be identified and rejected. These are frames whose MAC sender and destination address are identical. A network element must identify these frames as invalid and reject them. Further processing is not permitted.

*Motivation: An attacker can use manipulated frames with the same MAC sender and destination address to impair the availability of vulnerable systems.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.57-17/2.1

| Req 18 | Frames with the same MAC sender address for different customer lines on the same network element must be rejected. |
|---|---|

Network elements save the MAC source addresses of frames forwarded for the first time in a table so that subsequent frames can be processed more quickly. If a MAC address on a customer line has been identified and saved in the MAC address table of the network element, frames with the same MAC source address from another customer line must be rejected.

*Motivation: An attacker can send a frame with a MAC source address of the victim that has been faked. A network element that does not notice this overwrites the existing MAC address in the MAC address table with the port number of the attacker's line. For as long as the victim does not send a new frame, the attacker will receive the victim's data.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability

ID: 3.57-18/2.1

| Req 19 | Packets with spoofed IPv4 or v6 source addresses must be identified and rejected. |
|---|---|

Protection against packets with spoofed IPv4 or v6 source addresses must be provided on routers at network boundaries, i.e., at gateways to external networks and network elements to customer lines, in order to identify and reject the relevant packets. Possible solutions include:

- Activating the Unicast RPF (Unicast Reverse Path) function.
- Access control list via which packets that originate from an external network and have an IP source address

from the internal network are identified and rejected.

On routers used for peering only spoofed packets adressed to the infrastructue addresses of the backbone must be filtered. this means transit traffice shall not be filtered.

There is no need to implement this measure on the router where a firewall providing IP spoofing protection is used for the network gateways.

*Motivation: An attacker can use packets with a spoofed IP source address to hide his actual IP source address during attacks and to access systems for which his IP source address has been blocked.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability

ID: 3.57-19/2.1

# 4. Multi Protocol Label Switching (MPLS)

| Req 20 | The internal structure of the MPLS transport network must not be visible from the outside. |
|---|---|

The internal structure of the MPLS transport network must not be visible from the outside. This means that the label switch router (LSR) of the transport network must not appear as a hop on a trace route from a customer line or from external networks. The transport network thus only appears in the path as two hops (ingress and egress LER). This can be done by configuring the relevant routers accordingly. This suppresses the propagation of the TTL field of the IP packet into the preceding MPLS label.

*Motivation: Implementing this measure makes it more difficult for an attacker to obtain information.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.57-20/2.1

## 4.1. MPLS layer 2 and 3 VPNs

| Req 21 | A separate connection must be used to connect a customer router to the MPLS edge router. |
|---|---|

To ensure the separation of VPNs, a separate connection must be used every time a customer router (CE) is connected to a label edge router (LER). The connection can either be physically or logically separated. If, in the case of logical separation, a switch is used, make sure that a separate VLAN is used for each CE/LER connection.

*Motivation: If multiple customer routers share the same Layer 2 infrastructure for the LER connection, fake packets may be imported by a VPN customer in order to gain access to a VPN of another customer on the same LER.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.57-21/2.1

| Req 22 | Customer VPNs must be entirely separate from one another and from the underlying transport network. |
|---|---|

Virtual networks can be implemented for customers on an MPLS-based transport network using Layer 2 and Layer 3 VPNs. In this way, every customer can use its own IP address structure without influencing other customers. Where such VPN solutions are implemented, it must be ensured that the traffic and the IP address structure of the various customers are separated from one another and from the transport platform used.

*Motivation: It must be ensured that customers cannot break out from their VPN. If it is possible to overcome the VPN boundaries, an attacker can potentially feed packets into external customer VPNs or access systems in the transport network.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.57-22/2.1

| Req 23 | If the customer uses its own routing in a customer VPN, this must be entirely separate from the routing for other VPNs and the transport platform. |
|---|---|

Since every VPN customer can use its own IP address space within its VPN, it is possible for several customers to be using identical IP addresses. For this reason, in addition to a strict separation of the VPN traffic, an independent routing entity per customer VPN is also required.

The separation of the routing for a VPN is typically achieved via the configuration of "route targets" for VRF (Virtual Routing and Forwarding). Route targets are used to define which routes on an LER are imported or exported to a VRF for a customer VPN.

*Motivation: The routing entities in the various customer VPNs must be entirely separate from each other as otherwise unauthorized accessibility of systems between customer VPNs would be possible. The greatest threat to the separation of VPNs is therefore posed by misconfiguring network elements.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.57-23/2.1

| Req 24 | The components of the MPLS transport network must not be accessible from customer VPNs. |
|---|---|

The MPLS transport network provides data transport services for the connected customers. For a customer, the MPLS transport network to which the CEs of its locations are connected is not visible. To utilize the transport service, no more than the IP addresses between the CE and LER need to be visible to connect the VPN to the MPLS transport network. There is no need for the IP addresses of the core network to be accessible.

*Motivation: Direct accessibility of the MPLS transport network from a customer VPN increases the risk of attack.*

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability

ID: 3.57-24/2.1

| Req 25 | Layer 2 and 3 control plane traffic from customers must not affect the transport network. |
|---|---|

One service feature of Layer 2 and Layer 3 VPNs is the exchange of control plane protocols with the customer. This is used to distribute routing information between customer locations or to exchange route decisions for transport in the VPN. Make sure that the control plane protocols used do not have any influence on the transport network.

*Motivation: An attacker can specifically exploit an interpretation of the control plane protocols by the transport platform to impair the platform's availability or to influence traffic.*

For this requirement the following threats are relevant:
- Disruption of availability

ID: 3.57-25/2.1

| Req 26 | It must be ensured that targeted LDP packets are only accepted by trustworthy sender systems. |
|---|---|

Targeted LDP packets (LDP = Label Distribution Protocol) are exchanged between routers that are not directly connected to each other in order to establish layer 2 VPNs, for example. Since such packets can be sent across several hops, it must be ensured that they are only accepted by trustworthy senders.

One option here is to limit the acceptance of targeted LDP packets to configured neighbors. However, this approach is only supported by some router manufacturers. Another option is to use filter lists so that only targeted LDP packets from authorized IP sender addresses are permitted.

*Motivation: Accepting all targeted LDP requests on a destination system allows an attacker to send false information to a destination system, thus potentially compromising the stability of individual VPNs and/or the platform.*

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability

ID: 3.57-26/2.1