ETSI TS 103 931 V1.1.1 (2024-01)

Cyber Security (CYBER);
Network Router Security Requirements

Reference
DTS/CYBER-0081

Keywords
cybersecurity, router

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines security requirements for the network routers to mitigate the threats analysed in ETSI TR 103 869 [i.1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 869: "Cybersecurity; Network Router Security Threat Analysis".

[i.2] IETF RFC 4272: "BGP Security Vulnerabilities Analysis".

[i.3] IETF RFC 6518: "Keying and Authentication for Routing Protocols Design Guidelines".

[i.4] IETF RFC 8210: "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1".

[i.5] IETF RFC 8572: "Secure Zero Touch Provisioning (SZTP)".

[i.6] ISO/IEC 9899: "Information technology - Programming languages - C".

[i.7] ETSI TS 103 848 (V1.1.1): "Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things".

[i.8] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.9] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.10] IEEE 802.1AE™: "Media Access Control (MAC) Security".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

administrator: entity with the valid identity for operation and maintenance of the network router through the login to the device

lawful interception: action (based on the law), performed by a communications service provider, of making available certain information and providing that information to a law enforcement monitoring facility

NOTE: This term is referenced from ETSI TS 101 331 [i.9].

least privilege: granting an authenticated administrator the minimum set of execution and access rights to the network router resources to perform the essential operation the administrator is authorized for

user: entity external to the network which utilizes connections through the network for communication, e.g. the customer of the IP network operator

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
CAR	Committed Access Rate
CFI	Control Flow Integrity
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
HG	Home Gateway
ICMP	Internet Control Message Protocol
ID	IDentifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol security
ISO	International Organization for Standardization
ISP	Internet Service Provider
L3VPN	Layer 3 Virtual Private Network
MAC	Media Access Control
MACsec	Media Access Control security
ND	Neighbour Discovery
NMS	Network Management System
NX	No eXecute
OS	Operating System
PE	Provider Edge router
PIE	Position Independent Executables
QoS	Quality of Service

RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
SSH	Secure SHell
SZTP	Secure Zero Touch Provisioning
TLS	Transport Layer Security
UPE	User-end Provider Edge router
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

4 Network router introduction

In the Internet model, constituent networks are connected by IP datagram forwarders which are called routers or IP routers.

There are many types of routers. The home and small office routers, which simply forward IP packets between the home computers and the Internet, are out of the scope of the present document. The present document only discusses the network routers that are enterprise routers or ISP routers. The following two examples briefly show how network routers are used, and clause 4 of ETSI TR 103 869 [i.1] provides more detailed introductions about the network router.

In the IP Backbone network scenario as shown in Figure 1, the network routers are the Provider Router and Provider Edge Router.

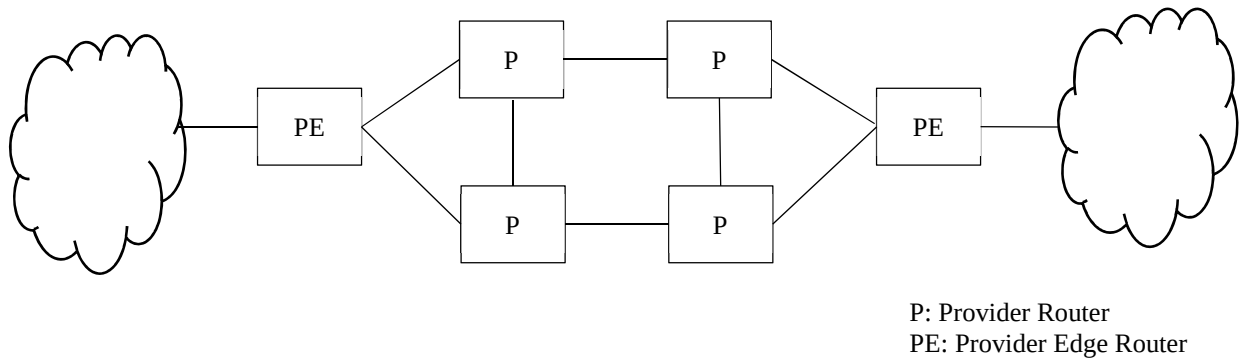

Figure 1: Topology of IP Backbone Network

In the IP Metro network scenario as shown in Figure 2, the network routers are the User-end Provider Edge Router and Broadband Network Gateway.

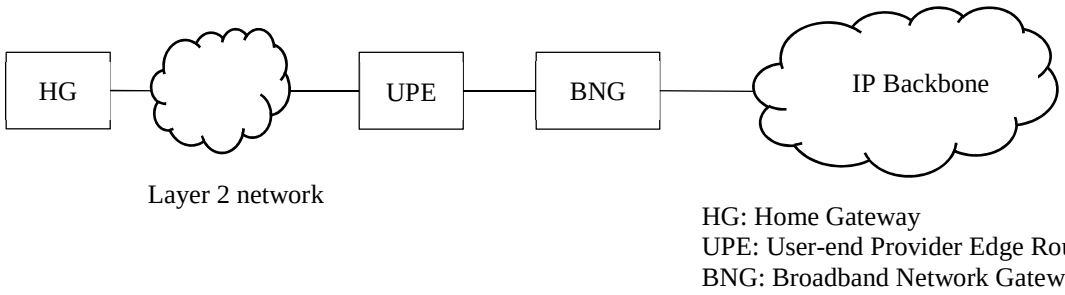

Figure 2: Topology of IP Metro Network

The logical architecture of a network router consists of three planes: data plane, control plane, and management plane, as shown in Figure 3.

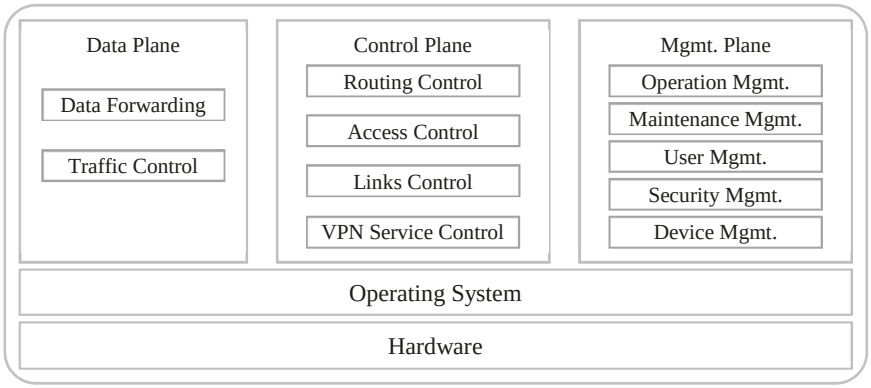

Figure 3: Logical architecture of a network router

5 Security objectives for threat mitigation

As described in clause 5.1 of ETSI TR 103 869 [i.1], the security objectives for threat mitigation include eight dimensions: Access control, Authenticity, Non-repudiation, Data confidentiality, Communication security, Data integrity, Availability/Resilience, and Privacy. The mitigations should include mechanisms of different security objectives to counter different threats, which are described below.

To counter the threats of **unauthorized interception**, it is necessary to prevent the attackers from accessing data and obtaining original information:

- To prevent the attackers from accessing data, the mitigations should include **Access control** and **Authenticity** mechanisms.
- To prevent the attackers from obtaining original information, the mitigations should include **Data confidentiality**, **Communication security**, and **Privacy** mechanisms.
- To ensure the correct security configuration of the system, the mitigations should include **Availability/Resilience** mechanisms.

To counter the threats of **unauthorized access**, it is necessary to protect system permissions and prevent tampering with critical data:

- To protect system permissions, the mitigations should include **Access control** and **Authenticity** mechanisms.
- To prevent the tampering of critical data, the mitigations should include **Data confidentiality**, **Communication security**, and **Data integrity** mechanisms.
- To provide isolation mechanisms to prevent the spread of intrusion attacks, the mitigations should include **Availability/Resilience** mechanisms.

To counter the threats of **masquerade**, it is necessary to protect system permissions and communication data:

- To protect system permissions, the mitigations should include **Access control** and **Authenticity** mechanisms.
- To protect communication data, the mitigations should include **Data confidentiality** and **Communication security** mechanisms.

To counter the threats of **forgery**, it is necessary to prevent the attackers from accessing communication data and enhance communication data security mechanisms:

- To prevent the attackers from accessing communication data, the mitigations should include **Access control** mechanisms.
- To enhance communication data security, the mitigations should include **Communication security** and **Data integrity** mechanisms.

- To provide system security detection and recovery mechanisms to cut down the impact of attacks, the mitigations should include **Availability/Resilience** mechanisms.

To counter the threats of **loss or corruption of information**, it is necessary to protect the network router system account and enhance the data security mechanisms:

- To protect the network router system account, the mitigations should include **Authenticity** mechanisms.
- To enhance the data security, the mitigations should include **Data confidentiality, Communication security** and **Privacy** mechanisms.
- To provide system security detection mechanisms to cut down the impact of attacks, the mitigations should include **Availability/Resilience** mechanisms.

To counter the threats of **repudiation**, it is necessary to protect the network router system account and record security-related activities. The mitigations should include **Authenticity** and **Non-repudiation** mechanisms.

To counter the threats of **denial of service**, it is necessary to provide system security policy and limit DDoS attack traffic.

- To provide system security policy, the mitigations should include **Access control** and **Authenticity** mechanisms.
- To limit DDoS attack traffic, the mitigations should include **Availability/Resilience** mechanisms.

6 Network router security requirements

6.1 Objectives

The objectives of this clause are to identify a possible common set of measures which are able to mitigate the threats faced by the network router, which have been identified in clause 5 of ETSI TR 103 869 [i.1], and to provide guidance for designing a robust security framework of products.

6.2 Prerequisites

The mitigation measures defined in the present document adhere to the following prerequisites:

- The mitigation measures defined in the present document are security requirements for the network router itself and are based on the network router architecture introduced in clause 4.2 of ETSI TR 103 869 [i.1]. The present document does not provide security requirements for other entities, such as network operators. For example, to mitigate physical attacks that cause damage to the device hardware, such as tearing network wires off or smashing it with a hammer, the network operator should provide physical protection mechanisms such as enclosed equipment rooms and professional security teams, and the network router should provide the necessary functions such as logging and alarming to meet the record and audit requirements. The mitigation measures defined in the present document cover only the latter type.
- The measures to mitigate the impacts to the network caused by the device failure of the network router are out of the scope of the present document. These impacts can be mitigated by network resilience design including commensurate redundancies.
- The network operator designs patching programs to ensure that became known vulnerabilities of network routers are fixed on short term. Since a vulnerability mitigation might require development time, the network operator should immediately take protective measures to repel the exploitation of the known vulnerability.

6.3 Access control

Requirement.AC.001: The network router shall control the access to the OS by following the principle of least privilege when granting an administrator the permission to access the OS resources.

NOTE: Embedded devices, including the network router, usually use closed systems built upon the Unix-like system, such as Linux. Commonly, the network router uses the account management function provided by the manufacturer and configured by the administrator rather than the OS default. If so, the network router disables the OS (Linux) account to prevent the threat agent from bypassing the account management function.

Requirement.AC.002: The provided network router features shall be specified in the product documentation.

Requirement.AC.003: The network router shall have control mechanisms for the authorized administrator to activate or deactivate the critical functions like lawful interception.

EXAMPLE: Before activating or deactivating the critical functions like lawful interception, the network router can authenticate whether the administrator is authorized to perform the operation and provide the administrator with a second confirmation. The network router can also record this operation for auditing.

Requirement.AC.004: The network router shall have password authentication or stronger security control mechanisms for the management ports, such as the console port.

EXAMPLE: The console port is an operating channel for connecting to a device. When the administrator connects via the console port, the network router authenticates the administrator by verification of the entered password. If the default password is used when connecting for the first time, the network router requires the administrator to set a new password and cease to allow the default password.

Requirement.AC.005: The service ports, such as the line card port, shall be disabled by default.

EXAMPLE: The line card ports of the network router are shut down by default. The service connection is supported only after the administrator configures the certain configuration.

Requirement.AC.006: The network router shall have authentication and control mechanisms for access requests to the management service received by the service ports.

NOTE: Besides the management ports, the service ports can often be used to connect to the management service as well. Therefore, the authentication and control mechanisms need to be performed when establishing such connections.

Requirement.AC.007: The network router shall support restricting the function of allowing access to the management service through specific service ports.

EXAMPLE: The service ports can be configured to accept or discard the access requests to the management service. Furthermore, they can also be configured to accept or discard specific protocol types, for example, only to accept SSHv2.

Requirement.AC.008: The network router should provide the account management function accessible to a dedicated administrator role to manage accounts and authentication credentials.

NOTE: Password-based authentication is acceptable for local physical login, or when the network router is initially installed or as long the network router is disconnected and the NMS is out of work. To ensure that the passwords have sufficient complexity and are changed periodically, the network router can provide quality checking mechanisms.

EXAMPLE: For example, the network router can force the administrator to set a new password on the first login with the factory-set default password.

Requirement.AC.009: The network router should support Secure Zero Touch Provisioning (SZTP) function when accessing the network for the first time.

NOTE: The SZTP defined by IETF RFC 8572 [i.5] presents a security technique to provide authentication to a networking device when booting in a default state.

Requirement.AC.010: The network router shall identify and filter packets based on their header information.

EXAMPLE: Filtering the incoming packets deemed for or traversing the network router, where the filtering is based on an Access Control List (ACL), is a functionality that is in mature use.

6.4 Authenticity

Requirement.AU.001: The network router shall authenticate and authorize assigned access rights to each administrator when they login to the network router.

EXAMPLE: AAA is a technology which provides authentication, authorization, and accounting functions. The AAA server receives connection requests, completes authentication, and returns the result to the network router. The network router usually provides AAA functionality to authenticate and authorize the administrator to a certain role.

NOTE: Various protocols support the communication between the network router and an AAA server, such as RADIUS. The network router needs to provide the security mechanism to ensure the security of these protocol communications, such as the DTLS tunnel.

Requirement.AU.002: The network router shall support authentication of protocol session peers.

NOTE: The network router uses various protocols to discover, learn information from, and distribute information to its neighbours. Authenticating the peer can prevent establishing sessions with the spoofed peers, thus to avoid learning incorrect information and leaking information.

6.5 Data confidentiality

Requirement.DC.001: The network router shall use best practice cryptography when the packets, files, or data need to be cryptographically operated, such as encryption/decryption, signature/signature-verification, and so on.

NOTE 1: The meaning of best practice cryptography is defined in ETSI EN 303 645 [i.8].

NOTE 2: The cryptographic algorithms supported by the network router are supposed to comply with the local laws and regulations.

Requirement.DC.002: The software package used by the network router should be protected to prevent attackers from using de-compilation to obtain the firmware and software information that can facilitate the attacker to launch the attacks.

EXAMPLE: By de-compiling the software package, the attackers can analyse the files contained to understand the architecture of the product as well as to identify security vulnerabilities. The best common practice is to encrypt the important files or the whole software package, or use a technique like code obfuscation.

Requirement.DC.003: The network router shall be able to establish security tunnels to protect the forwarding paths between network routers, such as IPsec tunnels or MACsec tunnels, and route the according traffic to the corresponding security tunnels.

EXAMPLE: The MAC Security Protocol (MACsec) defined by IEEE 802.1AE standard [i.10] could establish a secure channel between two devices, provide integrity and confidentiality protection for the data forwarding between devices, and prevent it from being eavesdropped or tampered with.

Requirement.DC.004: The network router shall protect the critical security parameters from being compromised, such as secret keys, passwords, etc.

NOTE: The meaning of critical security parameters is defined in ETSI EN 303 645 [i.8].

6.6 Communication security

Requirement.CS.001: The network router shall support best practice security protocols, including SSHv2 or TLS1.2/TLS1.3, to protect the management plane operations, such as remote login, file transfer, and log transfer.

Requirement.CS.002: The network router shall support best practice security mechanisms, such as limiting the rate and type of ICMP packets processed, to protect the device from ICMP-based attacks, including ICMP-based DDoS attacks.

EXAMPLE 1: The network router can use Committed Access Rate (CAR) or other mechanisms to prevent ICMP-based DDoS attacks from interrupting the running services on network routers.

EXAMPLE 2: The network router can disable certain ICMP functions, for example, not sending or responding to ICMP packets with certain ICMP types. This can prevent attackers from obtaining network topology and address information or launching certain attacks.

Requirement.CS.003: The network router shall support best practice security mechanisms, such as limiting the rate of ARP packets processed, to protect the device from ARP/ND-based attacks, including ARP/ND-based DDoS attacks and scanning attacks.

EXAMPLE: The network router can suppress ARP packets sent to one port to repel ARP scanning attacks.

Requirement.CS.004: When the network router supports routing protocols for forwarding services, security mechanisms required by these protocols shall be supported based on threat scenarios.

EXAMPLE 1: IETF RFC 6518 [i.3] describes the requirements of routing protocol authentication.

EXAMPLE 2: IETF RFC 4272 [i.2] describes the vulnerabilities and attack scenarios of BGP.

EXAMPLE 3: IETF RFC 8210 [i.4] proposes a public key authentication framework to repel the BGP route hijacking attack.

Requirement.CS.005: If the network router comprises multiple line cards that internally communicate with each other, the communication channels should encrypt the sensitive data transmitted to protect it from unauthorized disclosure.

6.7 Data integrity

Requirement.DI.001: The network router shall support best practice security mechanisms, such as Address Space Layout Randomization (ASLR) mechanism and Control Flow Integrity (CFI) mechanism, to protect the system against attacks on known vulnerabilities.

EXAMPLE 1: The network router can support the Address Space Layout Randomization (ASLR) mechanism. ASLR is a technique that randomizes the memory address space. It increases the difficulty for attackers to predict target addresses, protects from simple memory readout of concatenated data, and reduces the risk of successfully invading the processes.

EXAMPLE 2: The network router can support the Control Flow Integrity (CFI) mechanism. CFI is a security mechanism that does not allow deviations from the specified control flow of compiled binaries, making it extremely difficult to perform such attacks.

Requirement.DI.002: The network router should verify all software loaded during the booting phase using secure boot mechanisms to avoid loading maliciously modified software.

EXAMPLE: The network router can also support the remote attestation function to ensure that the software is not tampered with. Remote attestation is used to determine the trusted status of the network router, which can include the comparison of the data digest of software running on the network router with the data digest saved on the remote attestation server. For more details, see ETSI TS 103 848 [i.7].

Requirement.DI.003: The network router shall verify all patches loaded to avoid unauthorized patch modification.

Requirement.DI.004: The network router should support integrity verification of running software during the network router runtime to discover software tampering.

6.8 Availability/Resilience

Requirement.AR.001: The network router shall monitor the operational status of its own systems, detect service failures and provide either automatic recovery mechanisms or alerting.

EXAMPLE: Some attacks, such as tampering with the packets, can cause system exceptions on the network router, such as high CPU usage or port link congestion. The network router needs to support detecting and handling these exceptions.

Requirement.AR.002: The network router should cooperate with the NMS to enable central administrated service monitoring, failure detection, and reaction.

EXAMPLE: The network router may also support sampling functions such as NetStream when cooperating with the NMS to detect attacks in a timely fashion.

Requirement.AR.003: The network router shall use secure coding rules that comply with industry standards to protect the device from attacks due to code vulnerabilities, such as stack overflow attacks. The basic practices are setting appropriate secure compilation options and using secure compilation tools and procedures.

EXAMPLE 1: The network router can use secure functions defined in C/C++ programming standards, such as ISO/IEC 9899 [i.6].

EXAMPLE 2: Setting appropriate compilation options improves the difficulty of attacking software: Setting Position Independent Executables (PIE) randomizes the addresses and protects against stack overflow attacks, while setting No eXecute (NX) renders the stack to a non-executable condition and protects by that from malicious code execution.

Requirement.AR.004: The network router may support advanced security functions to improve its anti-attack capabilities, such as intrusion detection and prevention mechanisms to handle the intrusions quickly.

Requirement.AR.005: The network router should support automatic recovery to a minimum available state that the network router is still able to be logged in and managed in this state when severe attacks happen.

NOTE: The minimum available state can reduce the time a network router is out of management, and therefore help reduce the time of service interruption or downtime. This is essential for large networks.

Requirement.AR.006: The network router shall support security isolation mechanisms to prevent attacks from spreading across the device.

EXAMPLE 1: The isolation mechanisms include data plane isolation, such as VPN and VLAN. For example, the L3VPN function creates a specific logical network topology and ensures IP packets are forwarded among a limited range of addresses. The services in different L3VPNs are independent to prevent impact with each other.

EXAMPLE 2: The isolation mechanisms may also include process isolation, container isolation, and sandbox isolation.

Requirement.AR.007: The network router should monitor the allocated computing resources and trigger an alert if the resources used by a process or task exceed the pre-set normal range.

NOTE: It is common practice to trigger an alert when resource usage is detected above a default or administrator-set threshold. For example, when the administrator sets the threshold of CPU usage to 75 %, an alert is triggered to notify the administrator if the CPU usage exceeds 75 %.

Requirement.AR.008: The network router shall support the Quality of Service (QoS) to minimize the impact on the forwarding quality of high-priority packets when the data channel is congested.

NOTE: The network router can have the capability of scheduling queues with different priorities and the non-blocking switching to ensure that the metrics of delay, jitter, and packet loss ratio of forwarded packets with different priorities are within the specified range.

6.9 Privacy

Requirement.PR.001: The network router shall not trace, parse, forward, or store the payload of user packets unless the critical functions like lawful interception is enabled by the authorized administrator.

6.10 Non-repudiation

Requirement.NR.001: The network router shall generate records of all security-related events, such as administrator login, modification of account and authentication credentials, and the information of detected or suspected attacks.

EXAMPLE: The abnormal increase of CPU-usage or other resources can be an indication for an attack.

Requirement.NR.002: The details of the event records shall enable the support of retrospective auditing, which consequently requires the presence of appropriate event data.

EXAMPLE: Necessary event data comprise timestamp, account ID, event type, and result, which is non-exhaustive.

Requirement.NR.003: The network router shall support the remote and secure transmission of event record files with the protection of authentication of the entities, confidentiality, and integrity to the auditing server.

Requirement.NR.004: Record files integrity protection shall be provided to prevent event record files from modification, even by the administrators that conduct the retrospective audit.

NOTE: Records are an important means of anti-repudiation. In addition to the integrity protection of the records, appropriate access controls are important to protect the records also from complete deletion.

7 Rationales

The threats faced by the network router is analysed in ETSI TR 103 869 [i.1]. It defines in detail the threat scenarios numbers and vulnerability numbers that are used below.

Table 1: Mitigation Requirement Rationales

Threat Type	Threat	Threat Scenario No.	Vulnerability No.	Mitigation Requirement No.
Unauthorized interception (eavesdropping)	Eavesdropping protocol packets	Threat.Inter-device.01	VUL.HW.0006	Requirement.AC.004
				Requirement.AC.005
				Requirement.AC.006
				Requirement.AC.007
			VUL.PO.0006	Requirement.DC.001
	Eavesdropping data packets	Threat.Inter-device.02	VUL.HW.0001	Requirement.DC.003
			VUL.HW.0006	Requirement.AC.004
				Requirement.AC.005
				Requirement.AC.006
				Requirement.AC.007
			VUL.DA.0001	Requirement.PR.001
	Eavesdropping encrypted data	Threat.Inter-device.03	VUL.HW.0001	Requirement.DC.003
			VUL.HW.0006	Requirement.AC.004
				Requirement.AC.005
				Requirement.AC.006
				Requirement.AC.007
			VUL.DA.0003	Requirement.AC.001
			VUL.PO.0005	Requirement.CS.001
			VUL.PO.0006	Requirement.DC.001
	Abuse of the lawful interception management function	Threat.OM.01	VUL.SW.0004	Requirement.AU.001
			VUL.SW.0005	Requirement.AU.001
			VUL.SW.0007	Requirement.AC.001
			VUL.SW.0013	Requirement.AC.002
				Requirement.AC.003
	De-compilation software package	Threat.SC.01	VUL.SW.0006	Requirement.DC.002
			VUL.HW.0001	Requirement.DC.002

Threat Type	Threat	Threat Scenario No.	Vulnerability No.	Mitigation Requirement No.
Unauthorized access	Scan of router address	Threat.Access.01 Threat.Inter-device.04 Threat.OM.02	VUL.SW.0015	Requirement.AR.006
			VUL.PO.0005	Requirement.CS.002
			VUL.PO.0007	Requirement.CS.002
	Scan of router ports	Threat.Access.02 Threat.Inter-device.05 Threat.OM.03	VUL.SW.0015	Requirement.AR.006
			VUL.PO.0005	Requirement.CS.002
			VUL.PO.0007	Requirement.CS.002
	Cracking router accounts	Threat.Access.03 Threat.Inter-device.06 Threat.OM.04	VUL.SW.0003	Requirement.AC.008
			VUL.SW.0004	Requirement.AU.001
			VUL.SW.0007	Requirement.AC.008
			VUL.SW.0008	Requirement.AR.003
			VUL.SW.0009	Requirement.AC.008
			VUL.SW.0013	Requirement.AU.001
			VUL.SW.0014	Requirement.AU.001
			VUL.SW.0016	Requirement.DI.001
			VUL.DA.0002	Requirement.DC.001
			VUL.DA.0003	Requirement.AC.008
	Exploiting vulnerability	Threat.Access.04 Threat.Inter-device.07 Threat.OM.05	VUL.SW.0003	Requirement.AC.008
			VUL.SW.0004	Requirement.AU.001
			VUL.SW.0015	Requirement.AR.006
			VUL.SW.0016	Requirement.DI.001
			VUL.SW.0017	Requirement.AR.004
			VUL.SW.0018	Requirement.AR.005
	Physical damage or degradation	Threat.Physical.02	VUL.DA.0004	Requirement.NR.001
				Requirement.NR.002
				Requirement.NR.003
				Requirement.NR.004
Masquerade	Spoofing address	Threat.Access.05	VUL.SW.0001	Requirement.CS.003
			VUL.PO.0004	Requirement.AC.008
			VUL.PO.0005	Requirement.CS.001
			VUL.PO.0007	Requirement.AC.010
	Spoofing user	Threat.Access.06 Threat.Inter-device.08	VUL.SW.0005	Requirement.AU.001
			VUL.SW.0006	Requirement.DC.001
	Spoofing sessions	Threat.Inter-device.09 Threat.OM.06	VUL.SW.0001	Requirement.AU.002
			VUL.PO.0002	Requirement.AU.002
			VUL.PO.0004	Requirement.AU.002
			VUL.PO.0006	Requirement.DC.001
	Spoofing router accessed to network	Threat.SC.02	VUL.SW.0005	Requirement.AC.009
			VUL.SW.0006	Requirement.AC.009
			VUL.PO.0004	Requirement.AC.009
			VUL.PO.0007	Requirement.AC.009
Forgery	Forgery of data packets	Threat.Access.07	VUL.SW.0015	Requirement.AR.006
			VUL.DA.0001	Requirement.AR.001
				Requirement.AR.002
	Forgery of protocol packets	Threat.Inter-device.10 Threat.OM.07	VUL.SW.0001	Requirement.CS.001
			VUL.HW.0005	Requirement.CS.001
			VUL.PO.0001	Requirement.CS.001
			VUL.PO.0005	Requirement.CS.001
			VUL.PO.0009	Requirement.AR.005
	Send error data	Threat.Inter-device.11	VUL.SW.0001	Requirement.CS.004
			VUL.PO.0001	Requirement.CS.004
			VUL.PO.0006	Requirement.CS.004
	Tamper with software	Threat.SC.03	VUL.SW.0011	Requirement.DI.004
			VUL.SW.0012	Requirement.DI.002
			VUL.SW.0017	Requirement.AR.004
			VUL.SW.0018	Requirement.AR.005
	Use of incorrect version of software	Threat.SC.04	VUL.SW.0006	Requirement.DI.002
			VUL.SW.0012	Requirement.DI.003
			VUL.SW.0016	Requirement.DI.001

Threat Type	Threat	Threat Scenario No.	Vulnerability No.	Mitigation Requirement No.
Loss or corruption of information	Modification or deletion of system files	Threat.Access.08	VUL.SW.0004	Requirement.AU.001
			VUL.SW.0009	Requirement.AU.001
			VUL.SW.0013	Requirement.AU.001
			VUL.SW.0014	Requirement.AU.001
			VUL.SW.0017	Requirement.AR.004
	Corruption of protocol session data	Threat.Inter-device.12	VUL.PO.0005	Requirement.CS.004
			VUL.PO.0006	Requirement.CS.004
	Corruption of user traffic data	Threat.Inter-device.13	VUL.SW.0006	Requirement.DC.003
			VUL.DA.0001	Requirement.AR.001
				Requirement.AR.002
	Disclosure of key data, such as passwords	Threat.OM.08	VUL.SW.0004	Requirement.AU.001
			VUL.SW.0009	Requirement.AU.001
			VUL.HW.0003	Requirement.CS.005
			VUL.HW.0008	Requirement.CS.005
			VUL.HW.0009	Requirement.CS.005
			VUL.HW.0010	Requirement.CS.005
			VUL.DA.0002	Requirement.DC.004
			VUL.DA.0003	Requirement.AU.001
Repudiation	Modification or deletion of data files such as logs	Threat.Access.09 Threat.Inter-device.14 Threat.OM.09	VUL.SW.0004	Requirement.NR.001
				Requirement.NR.002
				Requirement.NR.003
				Requirement.NR.004
			VUL.SW.0009	Requirement.AU.001
			VUL.DA.0004	Requirement.AU.001
			VUL.PO.0003	Requirement.NR.001
				Requirement.NR.002
				Requirement.NR.003
				Requirement.NR.004
Denial of service	Send user data packet as traffic DDoS	Threat.Access.10 Threat.Inter-device.15	VUL.SW.0001	Requirement.AU.001
			VUL.HW.0002	Requirement.AR.008
			VUL.DA.0001	Requirement.AR.001
				Requirement.AR.002
	Send protocol packet as protocol DDoS	Threat.Access.11 Threat.Inter-device.16 Threat.OM.10	VUL.SW.0002	Requirement.AR.007
			VUL.SW.0008	Requirement.AR.007
			VUL.SW.0010	Requirement.AR.007
			VUL.SW.0018	Requirement.AR.005
			VUL.HW.0004	Requirement.AR.008
			VUL.PO.0007	Requirement.AC.010
			VUL.PO.0008	Requirement.AR.008
			VUL.PO.0009	Requirement.AR.005

History

Document history		
V1.1.1	January 2024	Publication