RAS/IPL/SIG Security Guide 4.13

This documentation is also available in web version at
doc.etictelecom.com

TABLE OF CONTENTS

1. REFERENCES

1. **ANSSI**. [Guide ANSSI-PA-022 v3.0] - Mai 2021 - Recommandations relatives à l'administration sécurisée des systèmes d'information.
2. **ANSSI**. [Guide ANSSI-PG-078 v2.0] - Octobre 2021 - Recommandations relatives à l'authentification multifacteur et aux mots de passe.
3. **ANSSI**. [DAT-NT-003/ANSSI/SDE/NP] - Août 2015 - Recommandations de sécurité relatives à IPsec pour la protection des flux réseau.
4. **ANSSI**. [SDE-NT-35/ANSSI/SDE/NP] - Mars 2020 - Recommandations de sécurité relatives à TLS.
5. **ANSSI**. [ANSSI-RGS-2] - Février 2014 - Annexe B1 au Référentiel général de sécurité (Version 2.0) : Choix et dimensionnement des mécanismes cryptographiques.
6. **ANSSI**. [ANSSI-RGS-2] - Juin 2012 - Annexe B2 au Référentiel général de sécurité (Version 2.0) : Gestion des clés utilisées dans les mécanismes cryptographiques.

2. NOTATION CONVENTIONS

2.1. Recommendations

Rx	Recommendation	Px
Motivation for setting (applying this setting reinforces XX)		
Application	How to implement the recommendation in router configuration.	

- **Rx** : Recommendation ID for reference
- **Recommendation**: Title of the configuration recommendation
- **Px**: Priority of the setting (from x=1 "Highest priority" to x=3 "Least priority")

The recommendations are grouped into 5 categories:

- **Ax**: **A**dministration interfaces
- **Ux**: **U**ser Management
- **Rx**: Network Security
- **Vx**: **V**PN
- **Ox**: **O**perational management

3. SECURING THE CONFIGURATION

This section contains all the recommendations for securing the configuration of routers in a production environment.

3.1. Administration interfaces

NOTE	This section does not address the issue of a secure administration architecture. The rules cited here are a summary of the rules considered fundamental for a secure administration of equipment. For a more global approach, refer to the specific ANSSI guide (ANSSI-PA-022).

Secure access to the administration interface

Enable authentication

A1	Enable authentication	P1
In the absence of a password, any local access to the equipment gives administration rights. In order to prevent illegitimate access and restrict changes to the equipment configuration, equipment administration must imperatively require a password. To ensure that the password cannot be recovered in the event of compromise of the equipment or its configuration extracts, passwords must be recorded in hash form using a state-of-the-art algorithm (Annex B1 of the RGS).		
Application	On the page ***Configuration*** > ***Security*** > ***Administration rights*** : Parameter **Password protect the configuration interface** : • Enable protection	

HTTPs protocol

A2	HTTPs protocol	P1
Unencrypted flows can be "listened" to at many points in the network, and information (such as the administrator password) is then accessible. So that a third party cannot listen to the exchanges and retrieve sensitive information (identifiers, etc.), the equipment must be administered using secure and encrypted protocols (SSH, HTTPS, etc.). In order to ensure server authentication, the associated certificate must be valid and issued by a recognized CA; in particular, the first connection to the administration console must not raise an alert. Administration interfaces are a prime target for an attacker. The concept of defense in depth involves protecting these interfaces in successive layers. One of the first actions is to change the administration ports defined by default by the manufacturer, which will slow down their discovery by an attacker.		

Application	On the page ***Configuration > Security > Administration rights*** : Parameter **Protocols to use for configuration** : • Select `HTTPS only` Parameter **HTTPS port for administration (4433)** : • Choose a port other than the default 4433 Parameter **Port TCP 80 redirects to Administration Area** : • Disable the option Parameter **Use the factory self-signed certificate** : • Disable the option Parameter **Choose a custom certificate** : • Select the certificate added to the device. Refer to Certificate Management to configure a certificate in the equipment.

Restricted access to the administration console

Disable access to administration by M2Me

A3	Disable access to administration by M2Me	P1
If the router allows M2Me access, this channel can be used to access the administration console.		
Application	On the page ***Configuration > Security > Administration rights*** : Parameter **Enable access via EticNet (HTTPS only)** : • Disable the option	

Disable WAN admin access

A4	Disable WAN administration access	P1
Since the WAN interface is by definition accessible from an external network, it is necessary to disable access to administration via this means.		
Application	On the page ***Configuration > Security > Administration rights*** : Parameter **Enable access from the WAN (HTTPS only)** : • Disable the option	

Disable SSH server

A5	Disable SSH Server	P1
SSH servers can be easily detected by port scanning, and in the absence of anti-brute force protection, the SSH interface is highly exposed to these attacks. In order to limit the exposure of the equipment, if the SSH protocol is not used regularly, it must be disabled and can be temporarily re-enabled if an operation justifies it.		
Application	On the page ***Configuration > Security > Administration rights*** : Parameter **Enable SSH server** : • Disable the option	

Access management

A6	Access management	P1
Administrators do not all have the same uses. It is necessary to have distinct users with the associated administrator role corresponding to their usage needs. Reducing the scope of an administrator helps minimize unwanted configuration changes, malicious or not. Compromising an administrator account that does not have maximum rights does not allow the attacker to do everything on the product. *Restricting the scope of administrators to the strict minimum by choosing the appropriate role improves the security of the product.*		
Application	For user management, see section User Management On the page ***Configuration > Security > Administration rights > Add/Edit an administrator***: Parameter **Role**: • Select the administrator role Parameter **User**: • Select the user to whom the role is assigned	

Temporary return to factory configuration

Disable temporary factory reset

A7	Disable temporary factory reset	P1
The temporary factory reset allows you to take control of the equipment, by applying the default factory configuration. An attacker could then gain access to the equipment, view the entire configuration and edit it. *In order to restrict access to the firmware and therefore preserve the integrity of the equipment, it is recommended to prevent the temporary factory reset by pressing the rear panel push button.*		

Application	On the page ***Configuration > Security > Administration rights*** : Parameter **Disable rear button for recovery (temporarily factory settings)** : • Enable the option

Hotline access

Hotline access configuration

A8	Hotline Access Configuration	P2
*Access for the Hotline service requires knowledge of two passwords, the password generated on the product at the request of an administrator. And the unique password of the product held by **Etic Telecom**.* *The password generated on the product must be stored securely*		
Application	On the ***Configuration > Security > Administration rights*** page: **Generate new hotline password** button: • Click on the `Generate` button, then store it securely.	

Disable remote access by push button

A9	Disable remote access by push button	P2
*The front button of the product allows the **Etic Telecom** customer service to connect to the product without the password generated on the product. This password bypass is valid for a period of one hour.* *Restricting this option does not allow the password generated by the product to be bypassed.*		
Application	On the page ***Configuration > Security > Administration rights*** : Parameter **Disable push button for Etic Telecom hotline remote access** : • Enable the option	

3.2. User Management

Usernames and passwords

User identifiers

U1	User identifiers	P1

The use of generic accounts does not allow actions and connections to be attributed or rights to be segregated. *In order to guarantee finer rights management and better traceability, user identifiers (administrators, operators, etc.) must be nominative.*
Application On the page ***Configuration > Security > Users Add/Modify a user*** : Parameter **Username** : • This is the user's login. Give an explicit name, because this is the information that will appear in the logs as well. Parameter **Password** : • Choose a strong password. The user can change his password himself later if he has access to the administration page.

Password Construction

U2	Password Construction	P1
A password that is too simple can be easily found during a brute force or dictionary attack. *In order to protect against such an attack, a strong password policy must be applied to administrator accounts. It will have a minimum of 16 characters, with at least 3 character classes and will not be easily guessable (no dictionary words). It will be unique to each device.*		
Application On the page ***Configuration > Security > Users Add/Modify a user*** : Parameter **Password** : • Change a user's password. The user can change his password himself if he has access to the administration page.		

3.3. Network Security

Network connectivity

Configure DNS manually

R1	Configure DNS manually	P2
By manipulating DNS records, it is possible to affect operations that rely on them (such as potentially establishing VPN tunnels or obtaining updates). If DNS servers are defined by DHCP, it is no longer possible to guarantee DNS information. In order to limit the risk associated with manipulating DNS records, the DNS servers used by the equipment must be trusted servers. It is recommended to use static and determined trusted DNS servers (ideally internal or those of the ISP).		

Application	In the menu: ***Home > Setup > WAN Interface*** It is recommended to use internal DNS servers to avoid disclosures of internal domain names on external DNS. • Uncheck the box **Obtain DNS servers addresses automatically** • Add a primary DNS server • Add a secondary DNS server

Disable DHCP server

R2	Disable DHCP Server	P1
DHCP address allocation without additional controls (e.g. NAC) allows an exogenous machine to be integrated into the network, provided that it has physical access. To limit unauthorized access to the network, it is recommended not to activate DHCP server features on "remote" routers. However, if DHCP must be activated for field constraints, it is necessary to control the terminals that connect to the network.		
Application	In the menu: ***Home > Setup > LAN Interface > DHCP Server*** Uncheck the parameter ***Enable DHCP server*** However, if DHCP must be activated for field constraints, it is possible to associate the IPs allocated in DHCP by MAC address. Be sure to enter an IP address range consistent with the number of assets managed by DHCP.	

Reduce the exposure area

Disable the application server

R3	Disable Application Server	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automated scans. In order to limit the equipment's exposure, it must be disabled.		
Application	In the menu: ***Home > Setup > Remote access > Remote access servers*** Uncheck the parameter **Enable HTTPS application server**	

Disable SNMP agent

R4	Disable SNMP agent	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automatic scans. *If SNMP monitoring is not implemented, it is recommended to disable the SNMP agent.*		

Application	In the menu: ***Home > Setup > System > SNMP*** Uncheck the parameter **Enable**

Disable NTP server

R5	Disable NTP server	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automated scans. In order to limit the equipment's exposure, it must be disabled.		
Application	In the menu: ***Home > Setup > System > Date and time settings > NTP*** Uncheck the parameter **Enable NTP service**	

Disable EticFinder

R6	Disable EticFinder	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automated scans. In order to limit the equipment's exposure, it must be disabled.		
Application	In the menu: ***Home > Setup > Security > Administration rights*** Uncheck the parameter **Enable EticFinder tool**	

Disable the WEB portal

R7	Disable WEB portal	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automated scans. In order to limit the equipment's exposure, it must be disabled.		
Application	In the menu: ***Home > Setup > LAN interface > WEB portal*** Uncheck the parameters **Show Web portal** and **Show portal on home page**	

Disable M2Me_Connect

R8	Disable M2Me_Connect	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automated scans. In order to limit the equipment's exposure, it must be disabled.		
Application	In the menu: ***Home > Setup > Remote access > M2Me_Connect*** Uncheck the parameter **Enabled**	

Disable Modbus TCP server

R9	Disable Modbus TCP Server	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automated scans. In order to limit the equipment's exposure, it must be disabled.		

Application	In the menu: ***Home*** > ***Setup*** > ***System*** > ***Modbus Server*** Uncheck the parameter **Enable**

Disable the OPC-UA server

R10	Disable OPC-UA Server	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automated scans. In order to limit the equipment's exposure, it must be disabled.		
Application	In the menu: ***Home*** > ***Setup*** > ***System*** > ***OPC UA Server*** Uncheck the parameter **Enabled**	

Block unused ports

R11	Block unused ports	P3
Physical access to equipment can sometimes be compromised, so it is advisable to physically block unused ports so that a malicious person with physical access to the equipment cannot use these ports.		
Application	Use physical port locks to block unused RJ45 or USB ports.	

Disable unused interfaces

R12	Disable unused interfaces	P3
Physical access to the equipment can sometimes be compromised, so it is advisable to disable unused interfaces so that a malicious person with physical access to the equipment cannot use these interfaces.		
Application	In the menu: > ***Home*** > ***Setup*** > ***LAN Interface*** > ***Ethernet and IP*** In the "Advanced Settings" section, each LAN port has its own configuration: **Port 1/2/3/4 configuration**, Set this parameter to `Disabled` to disable unused ports. In the menu: > ***Home*** > ***Setup*** > ***WAN Interfaces*** > ***Ethernet***, For the **Connection Type** parameter, set the value to `Unused` if it is unused. In the menu: > ***Home*** > ***Setup*** > ***WAN Interfaces*** > ***Wi-Fi***, uncheck the **Enable Wi-Fi WAN** parameter if it is unused. In the menu: > ***Home*** > ***Setup*** > ***WAN Interfaces*** > ***Cellular***, uncheck the **Enabled** parameter if it is unused.	

Firewall: fix firewall rules for VPN

Blocking WAN to LAN inbound flows

R13	Blocking incoming WAN to LAN flows	P1
Any service exposed on the Internet is likely to be the target of an attack, whether targeted or generic, opportunistic or automated. Incoming flows from a public network (Internet/WAN) should be limited as much as possible. In the context of site-to-site VPN without direct access to remote sites, no direct WAN to LAN flows should be allowed.		
Application	In the menu: ***Home*** > ***Setup*** > ***Security*** > ***Firewall*** Block incoming WAN to LAN flows by default: **WAN→LAN Default policy** to `Deny`	

Blocking LAN to WAN outgoing flows

R14	Blocking LAN to WAN outgoing flows	P1
Uncontrolled Internet access can be a source of network threats or data exfiltration. In the context of site-to-site VPN without direct access to remote sites, no direct flow from the local network (LAN) of these sites to the Internet (WAN) must be allowed.		
Application	In the menu: ***Home*** > ***Setup*** > ***Security*** > ***Firewall*** Block LAN to WAN incoming flows by default: **LAN→WAN Default policy** to `Deny`	

Blocking VPN inbound flows to LAN

R15	Blocking VPN to LAN inbound streams	P1
The flows coming from the VPN to the LAN must also be secured, because the zone of origin is not necessarily a trusted zone. It is advisable to control all flows to the LAN in order to avoid any attempted attack from a compromised asset outside the LAN. Communication needs between LAN equipment and those of the central infrastructure may be necessary (supervision, backup, etc.). It is therefore essential to list them, enter them in a repository, and then implement them clearly and precisely. Any rule that is too permissive lowers the overall security level of the IS.		
Application	In the menu: ***Home*** > ***Setup*** > ***Security*** > ***Firewall*** Block incoming VPN to LAN flows by default: **VPN→LAN Default policy** to `Deny`	

Blocking LAN to VPN outgoing flows

R16	Blocking LAN to VPN outgoing flows	P1
The flows from the LAN to the VPN must be precise and not open without restriction. In the event of a compromise, precise flows can slow down the propagation of an attacker through the IS. A significant amount of work must be done upstream to identify the flows in order to avoid any interruption of service due to rules that are too strict or an oversight. It is necessary to list the communications between the LAN and the remote networks, to enter them in a repository, and then to implement them clearly and precisely. Any rule that is too permissive lowers the overall security level of the IS.		

Application	In the menu: ***Home > Setup > Security > Firewall*** Block incoming VPN to LAN flows by default: **LAN→VPN Default policy** to `Deny`

Enable the anti-Denial of Service filter

R17	Enable the Denial of Service filter	P1
Excessive packet forwarding to the admin port can result in a potential denial of service (DoS), resulting in the web page being unavailable. *Therefore, it is necessary to be able to identify and block malicious packets.*		
Application	In the menu: ***Home > Setup > Security > Firewall*** Check the parameter **Enable Deny of Services filter (DoS)**	

Disable conntrack helpers

R18	Disable conntrack helpers	P1
A problem of bypassing the iptables rules set by user can occur with the use of firewall rules RELATED,ESTABLISH too generic and the loading of service helpers not present or not used on the machine (for example active FTP, SIP, IRC ...). *It is therefore recommended to disable the conntrack helpers.*		
Application	In the menu: ***Home > Setup > Security > Firewall*** Uncheck the parameter **Enable conntrack helpers (Not recommended)**	

Certificate Management

Usage of a trusted PKI

R19	Using a trusted PKI	P1
Equipment identification and VPN authentication rely on certificates. A compromise of the PKI can therefore jeopardize the entire chain of trust. *Certificate management must be carried out by a PKI controlled by the company or recognized as trusted. This allows for a fine definition of the use and format of certificates. Certificates must also be created with state-of-the-art encryption algorithms, in order to avoid the weaknesses of obsolete algorithms (breaking, etc.) (SDE-NT-35/ANSSI/SDE/NP).*		

Application	In the menu: ***Home > Setup > Security > Certificate Store*** Adding and removing Certificates, private keys and CA certificates is possible in the different tables. See the "Router firmware / Certificate Store" section of the configuration guide for more information. We recommend: a hash function used for signing certificates must be of the SHA-2 family and the certificate signing key must be at least 3072 bits for RSA and 256 for ECC. For fine-grained management of a PKI, refer to appendices B of the RGS (Annexes B1 and B2 of the RGS).

Equipment certificates

R20	Equipment Certificates	P1
Reusing a certificate for multiple clients prevents identifying the user, increases the certificate's exposure, and in case of compromise, the revocation/reissuance of the certificate impacts multiple clients. Certificates must be unique and individual per machine for better traceability and to allow revocation without side effects if necessary. Used for HTTPS communications, they must have a validity period of 13 months maximum.		
Application	In the menu: ***Home > Setup > Security > Certificate Store*** Adding and removing Certificates, private keys and CA certificates are possible in the different tables. See the "Router firmware / Certificate Store" section of the configuration guide for more information. All services requiring a router certificate will retrieve them from the certificate store.	

Revocation of certificates

R21	Revocation of certificates	P1
A certificate that is no longer used is potentially less protected, and therefore represents a source of risk as long as it is valid. Certificates whose purpose is no longer relevant must be revoked. The goal is to maintain control over your certificate fleet.		
Application	In the menu: ***Home > Setup > Security > Certificate Store***: CRL List tab We recommend that you update the list of certificates assigned to users and keep a history of revoked certificates. Some typical use cases where certificates must be revoked: • Equipment removed from the IT park, workstations returned to stock, etc. • Decommissioned users: staff movement (internal or partner), end of contract with an external company, etc. • The most exhaustive list possible must be established, and the revocation of certificates must be included in the various related procedures.	

3.4. VPN

Site-to-site VPN

Using Certificates

V1	Use of certificates	P1
Reusing a certificate for multiple clients prevents identifying the user, increases the certificate's exposure, and in case of compromise, the revocation/reissuance of the certificate impacts multiple clients. *It is recommended to use unique and individual certificates per machine for better traceability and to allow revocation without side effects if necessary.* *Signing digital certificates generated from private keys deemed obsolete (e.g. RSA 1024) is deprecated for security reasons. It is therefore necessary to prevent the use of these certificates.*		
Application	In the menus: • ***Home > Setup > Network > VPN Connections > IPSec > IPsec Connection*** • ***Home > Setup > Network > VPN Connections > OpenVPN > OpenVPN Server*** • ***Home > Setup > Network > VPN Connections > OpenVPN > Outgoing OpenVPN Connections*** Once the certificate is installed, uncheck **Use the factory certificate**, and in the context menu **Choose a custom certificate**, choose the newly added certificate. Avoid using the default certificate that is not validated by a recognized certification authority. Refer to the Certificate Management section to generate state-of-the-art client and server certificates.	

Encryption and authentication algorithms

V2	Encryption and Authentication Algorithms	P1
New vulnerabilities in protocols and algorithms are regularly discovered, calling into question their level of protection. *The various protocols and algorithms inherent to the use of VPNs must be configured to the state of the art, in order to avoid the weaknesses of obsolete algorithms (breaking, etc.) (Annexes B1 du RGS).*		

Application	In the menus: • ***Home > Setup > Network > VPN Connections > IPSec > IPsec Connection*** • ***Home > Setup > Network > VPN Connections > OpenVPN > OpenVPN Server*** • ***Home > Setup > Network > VPN Connections > OpenVPN > Outgoing OpenVPN Connections*** Choose the following values for these parameters: • **Encryption Algorithm** / **Encryption**: `AES-256-CBC` or `AES-256-GCM` • **Authentication Algorithm** / **Authentication**: `SHA-256`, `SHA-384` or `SHA-512`

Disallow traffic between VPNs

V3	Prohibit traffic between VPNs	P1
Flows from the VPN to other VPNs must be secured, because the zone of origin is not necessarily a trusted zone. *All flows to VPNs must be controlled in order to avoid any attempted attack.*		
Application	In the menu: ***Home > Setup > Security > Firewall*** • Uncheck the box **Accept traffic between VPN**	

OpenVPN: Authentication Management

V4	OpenVPN: Authentication Management	P1
Password authentication presents several risks: password leakage (replacing it then requires action on each device concerned), its lack of renewal, and its robustness. Using an individual certificate for authentication makes it possible to block access by revoking the certificate. The lifetime of certificates is also fixed, which requires the rotation of secrets within a defined time window. Finally, a certificate is generally a more robust secret than a password. As such, it is the authentication method recommended by ANSSI. *It is recommended to manage the authentication of OpenVPN peers by certificate.*		

Application	Setting up a VPN tunnel is a two-part process. First, a VPN server must be configured, then to accept client connections, an incoming connection per client must be configured. • Server-side authentication ◦ In the menu: ***Home > Setup > Network > VPN Connections > OpenVPN > OpenVPN Connection*** ◦ Set a strong password. This password will also be used by the client router initiating the connection ◦ Enter the "Common Name" of the client router certificate that you previously generated and add to the client router initiating the connection. Refer to the section Certificate Management to see how to add a certificate in a router. • Client-side authentication ◦ In the menu: ***Home > Setup > Network > VPN connections > OpenVPN > Outgoing OpenVPN connections*** ◦ Enter the strong password shared between the server and the client

OpenVPN: Choice of Diffie-Hellman

V5	OpenVPN: Choosing Diffie-Hellman	P1
New vulnerabilities in protocols and algorithms are regularly discovered, calling into question their level of protection. *The various protocols and algorithms inherent to the use of TLS must be configured to the state of the art, in order to avoid the weaknesses of obsolete algorithms (breaking, etc.) (SDE-NT-35/ANSSI/SDE/NP).*		
Application	In the menu: ***Home > Setup > Network > VPN Connections > OpenVPN > OpenVPN Server*** For the parameter **Diffie Hellman**, choose the value `4096 bits (Recommended)`	

OpenVPN: Using tls-crypt v2

V6	OpenVPN: Using tls-crypt v2	P1
The first exchanges for establishing the TLS connection between the client and the OpenVPN server are done in clear text. This exchange of keys done in clear text can induce a Man-in-the-Middle vulnerability. *To prevent this type of attack, it is recommended to enter a tls-crypt pre-shared key to also encrypt the TLS channel establishment frames.*		

Application	In the menu: ***Home*** > ***Configuration*** > ***Network*** > ***VPN Connections*** > ***OpenVPN*** > ***OpenVPN Server*** • Check the box **Enable tls-crypt-v2** and enter the tls-crypt-v2 key In the menu: ***Home*** > ***Configuration*** > ***Network*** > ***VPN Connections*** > ***OpenVPN*** > ***Outgoing OpenVPN Connections*** • Check the box **Enable tls-crypt-v2** and enter the tls-crypt-v2 key

OpenVPN: Disable LZO compression

V7	OpenVPN: Disable LZO compression	P1
Using LZO compression is not recommended, because the compression ratio leaks information about the clear compressed data. *It is therefore recommended to disable LZO compression.*		
Application	In the menu: ***Home*** > ***Setup*** > ***Network*** > ***VPN Connections*** > ***OpenVPN*** > ***OpenVPN Server*** • Check the box **Disable compression** In the menu: ***Home*** > ***Setup*** > ***Network*** > ***VPN Connections*** > ***OpenVPN*** > ***Outgoing OpenVPN Connections*** • Check the box **Disable compression**	

IPsec: Authentication Management

V8	IPsec: Authentication Management	P1
Password authentication presents several risks: password leakage (replacing it then requires action on each device concerned), its lack of renewal, and its robustness. The use of an individual certificate for authentication makes it possible to block access by revoking the certificate. The lifetime of certificates is also fixed, which requires the rotation of secrets within a defined time window. Finally, a certificate generally constitutes a more robust secret than a password. As such, it is the authentication method recommended by ANSSI. *It is recommended to use authentication by certificates and not by pre-shared key (DAT-NT-003/ANSSI/SDE/NP).*		

Application	In the menu: ***Home > Setup > Network > VPN Connections > IPSec > IPSec Connection*** • Configure authentication by certificates ◦ In the **Authentication by** field, select `Client certificate` ◦ In the IKE authentication section, uncheck **Use the factory certificate** ◦ Choose your server certificate or client certificate ◦ Choose a **Certificate revocation policy** `strict` • Configure authentication by PSK ◦ In the **Authentication by** field, select `Pre-shared key` ◦ Enter the PSK value in the **Key value** field. A PSK should have a minimum entropy greater than or equal to 100 bits

IPsec: Diffie-Hellman Group

V9	IPsec: Diffie-Hellman Group	P1
New vulnerabilities in protocols and algorithms are regularly discovered, calling into question their level of protection. *The various protocols and algorithms inherent to the use of IPsec must be configured to the state of the art, in order to avoid the weaknesses of obsolete algorithms (breaking, etc.) (DAT-NT-003/ANSSI/SDE/NP).*		
Application	In the menu: ***Home > Setup > Network > VPN Connections > IPSec > IPSec Connection*** Check the box **Show advanced parameters**, for the parameter **DH Group** choose from these values: `Group 14`, `Group 16`, `Group 18`	

Peer-to-Site VPN

Disable PPTP

V10	Disable PPTP	P1
The more exposed the equipment, the more possible sources of illegitimate access, including automatic scans. PPTP is now considered an obsolete protocol in terms of security, in order to limit the exposure of the equipment, it must be disabled.		
Application	In the menu: ***Home > Setup > Remote access > Remote access servers*** Uncheck the box **Enable PPTP**	

Disable L2TP/IPSec

V11	Disable L2TP/IPSec	P1

The more exposed the equipment, the more possible sources of illegitimate access, including automatic scans. *It is recommended to disable the L2TP/IPSec server to limit the exposure of the equipment.*	
Application	In the menu: ***Home > Setup > Remote access > Remote access servers*** Uncheck the box **Enable L2TP/IPSec**

User certificates

V12	User Certificates	P1
Reuse of a certificate for multiple users prevents identification of the user, increases the exposure of the certificate, and in case of compromise of the certificate, the revocation-reissue of the certificate impacts multiple users. *User certificates must be nominative for traceability and allow their revocation if necessary. We recommend a maximum validity of 1 year.*		
Application	In the menu: ***Home > Setup > Security > Users*** The CN, i.e. Common Name, is expected as a means of identifying the certificate. Enter the CN of the user certificate in the **CN of the user certificate** field. We recommend following the following procedure: • Issue one certificate per user, i.e. with a unique CN, and distribute it only to the user concerned • Maintain a list of certificates assigned to users, which makes it easier to revoke them if necessary • Set a maximum certificate validity of one year • Use a server certificate on the router for peer-to-site VPNs Refer to the Certificate Management section for best practices for generating certificates	

Two-factor authentication

V13	Two-factor authentication	P1
Since users' mobile devices are exposed, a single authentication factor can leak. User authentication should be two-factor.		
Application	In the menu: ***Home > Setup > Remote access > Remote access servers***, tabs **OpenVPN Properties** and **OpenVPN Properties (SmartPhone Access)** For the parameter **User authentication**, choose `Login / Password + Certificate`	

Encryption and authentication algorithms

V14	Encryption and Authentication Algorithms	P1

New vulnerabilities in protocols and algorithms are regularly discovered, calling into question their level of protection. *The different algorithms inherent in the use of TLS for establishing a peer-to-site VPN must be configured to the state of the art in order to avoid the weaknesses of obsolete algorithms (SDE-NT-35/ANSSI/SDE/NP).*
Application In the menu: ***Home > Setup > Remote access > Remote access servers***, tabs **OpenVPN Properties** and **OpenVPN Properties (SmartPhone Access)** Choose the following values for these parameters: • **Encryption algorithm**: `AES-256-CBC` or `AES-256-GCM` • **Message digest algorithm**: `SHA-256`, `SHA-384` or `SHA-512`

Only one remote connection at a time

V15	Only one remote connection at a time	P1
By changing the IP address of the "OpenVPN remote access" client to an IP address of another "OpenVPN remote access" client already connected to the remote access server, an attacker obtains the firewall rights of the impersonated user. *It is therefore recommended to allow only one remote connection at a time, in this way, the firewall rights cannot be impersonated.*		
Application	In the menu: ***Home > Setup > Remote access > Remote access servers***, tabs **OpenVPN Properties** and **OpenVPN Properties (SmartPhone Access)** Check the box **Allow only one remote connection at a time**	

Disable LZO compression

V16	Disable LZO compression	P1
Using LZO compression is not recommended, because the compression ratio leaks information about the clear compressed data. *It is therefore recommended to disable LZO compression.*		
Application	In the menu: ***Home > Setup > Remote access > Remote access servers***, tabs **OpenVPN Properties** and **OpenVPN Properties (SmartPhone Access)** Check the box **Disable compression**	

3.5. Operational management

Updates

Keep equipment up to date

O1	Equipment maintenance	P1

Security flaws in the firmware of the equipment can allow to bypass the security measures and take control of the equipment. In order to protect against flaws corrected by the publisher, the equipment must be regularly updated.	
Application	Router firmware version updates are published on the Etic Telecom website. Vulnerabilities concerning router firmware versions are published on a dedicated page. **To update the router firmware:** On the > ***Home*** > ***Maintenance*** > ***Firmware update*** page: **Update using an update file** parameter: 1. Choose the update file 2. Click on the `Update` button

Configuration backups

Regular configuration backups

O2	Regular configuration backups	P3
A mishandling, correction or equipment failure may occur, leading to the need to restore the configuration for continuity of service, on this equipment or new equipment. *In order to allow a rapid return to an operating state if necessary, a backup of the equipment configuration must be performed regularly.*		
Application	On the > ***Home*** > ***Maintenance*** > ***Configuration Management*** page: **Save the current configuration:** Parameter **Configuration name**: 1. Name the configuration 2. Click on the `Save` button **Download the configuration to the local PC:** Table **User configurations**: 1. Select the configuration 2. Click on the `Export to PC` button 3. Enter a secret encryption key	

Backup Security

O3	Backup Security	P3

Backups are used to restore the configuration of a device, so the availability of backups affects the availability of the device. Backups also contain sensitive information such as network configuration or credentials, the disclosure of which would impact the security of the devices and the network as a whole. *In order to ensure the confidentiality, integrity and availability of backups, they must be stored securely in accordance with the company's backup policy.*	
Application	When exporting the configuration to a PC, it is important to choose a secret encryption key with a sufficient level of security (more than 15 characters). When a key is entered, secrets that cannot be stored hashed are exported encrypted in the resulting configuration file. Backups should be stored and archived only on storage spaces whose availability and confidentiality are ensured, with strict control over access rights. They should ideally be centralized, and should not be stored outside an encrypted container (encrypted Zip, Zed, etc.), on removable media or unencrypted mobile devices.

Outsourcing Backups

O4	Outsourcing backups	P3
In the event of an incident on site, backups may be destroyed along with the equipment, impacting the subsequent reconstruction of the equipment. To ensure their availability, backups should be outsourced, in compliance with the business continuity activities.		
Application	To ensure the availability of backups, it is recommended to outsource them, like any critical infrastructure backup. The outsourcing site must provide the necessary guarantees in terms of confidentiality.	

Restore Backups

O5	Restore Backups	P3
To ensure the integrity of backups, validate and regularly practice procedures, the restoration of backups must be documented and tested at least annually, in compliance with the company's backup policies.		
Application	On the page > ***Home*** > ***Maintenance*** > ***Configurations management***: Restore a configuration backup: 1. Choose the name that will be given to the configuration 2. Choose the configuration file on the PC 3. Enter the configuration decryption key if necessary 4. Load the imported configuration file	

Logging

Time synchronization

O6	Time Synchronization	P2
When analyzing logs, if the equipment does not have a consistent time source, the timestamp of the logs may be inconsistent and the analysis inaccurate. *To standardize the IS and allow a global study if necessary, the equipment must be synchronized on a time server known to be reliable and consistent with the other equipment in the IS. If the equipment's logging is exported to another machine, the latter must be synchronized with the same time source.*		
Application	On the page > ***Home*** > ***Setup*** > ***System*** > ***Date and time settings*** > ***NTP*** : Parameter **Sync the clock using timeservers** : • Enable the option Parameter **NTP Servers** : • List the IP addresses or domain names of the time servers separated by a comma.	

Outsourcing Logs

O7	Log Outsourcing	P2
In the event of a malfunction or attack, the reliability of the logs on the device can no longer be guaranteed. The retention of the logs on the device cannot be guaranteed. *To ensure their availability and allow for global analysis, the logs must be outsourced to a third-party log server.*		
Application	To ensure log reliability, a third-party log server should be set up to securely store logs. Log outsourcing configuration is configured on the router on the > ***Home*** > ***Setup*** > ***System*** > ***Syslog*** page: **Enabled** parameter: • Enable the option **Transfer mode** parameter: • Choose `Mutual authentication` parameter: **Server hostname** parameter: • Enter the server name. This must be the same name that is in the "Common name" field of the syslog server certificate Parameter **Certificate**: • Select the router certificate	

Analyze logs

O8	Analyze logs	P3

Tracing events allows for a posteriori investigation in the event of an incident, but detecting ongoing incidents requires proactive analysis of the logs. *In order to detect illegitimate access attempts or malfunctions, it is recommended to implement regular (or real-time) analysis of the logs.*	
Application	Log analysis cannot be done automatically by Etic Telecom devices. A manual log analysis task must be planned, or controls implemented on the log server or on the SIEM.

Supervision by SNMP (v3)

O9	SNMP (v3) supervision	P3
In order to anticipate risks related to the availability and abnormal behavior of the equipment, it is recommended to supervise the equipment by SNMP. *SNMP v1 and v2 are not secure by nature, only the community allows to "restrict" access. Versions 1 and 2 of the protocol are also affected by many vulnerabilities.* *If this supervision is implemented, version 3 of the protocol must be used. Furthermore, it is recommended not to use the default community "public".*		
Application	The SNMP server configuration on the router is done on the page > ***Home*** > ***Setup*** > ***System*** > ***SNMP*** • Parameter **SNMP protocol version**: `SNMP version 3` • Parameter **Authentication algorithm**: `SHA-256`, `SHA-384` or `SHA-512` • Parameter **Cipher algorithm**: `AES-256-CBC`	

Monitored Keypoints

O10	Monitored indicators	P3
Overconsumption of resources can lead to equipment unavailability. *To prevent equipment unavailability, it is recommended to monitor the CPU, RAM and disk space usage of the equipment, as well as the number of simultaneous VPN connections.*		
Application	Indicators can be queried by SNMP using the OIDs provided in the MIB-2 standard.	

Long term monitoring

O11	Long term monitoring	P3
Depending on usage, equipment may be at the limit/exceeding capacity in given periods (information consolidation phases, attacks, etc.) *To identify abnormal equipment behavior, it is recommended to set up a history of the monitored indicators and to follow their evolution over time.*		
Application	Monitoring scenarios will need to be implemented at the monitoring solution level.	

Network traffic analysis with ERSPAN

O12	Network traffic analysis with ERSPAN	P3
Analyzing network traffic is a preventative security measure that helps troubleshoot the network, detect anomalies or malicious traffic. *Port mirroring with ERSPAN is a technique for analyzing the network. It allows you to send a copy of the monitored traffic to a remote device that can analyze the packets.*		
Application	A server will need to be set up to receive the mirrored traffic and handle packet analysis. ERSPAN mirroring configuration on the router is done on the page ***Setup*** > ***Network*** > ***ERSPAN***.	

Authentification

Password Policy

O13	Password Policy	P2
Compromised user passwords can lead to illegitimate access to the IS. A password that is too simple can be easily found during a brute force attack, by dictionary or hash cracking. *In order to protect against such an attack, it is important to define a password policy at the organizational level in accordance with the document (ANSSI-PG-078).*		
Application	Set a password policy at the organization level. We recommend passwords that contain: • 16 characters minimum • At least one uppercase letter, one lowercase letter, and one number • At least one special character `&$%[]{}=?!-_*+~#@`	

Use a centralized authentication system

O14	Use a centralized authentication system	P2
When you have a fleet of routers, managing local user lists on the routers quickly becomes tedious to manage. Maintaining the same user list duplicated on several routers can lead to errors and omissions on one of the routers. *To avoid these security problems, it is advisable to manage the fleet of routers centrally.*		
Application	A centralized authentication server such as Active Directory or another LDAP server must be set up to manage user authentication on the fleet. The authentication delegation configuration is done on the > ***Home*** > ***Setup*** > ***Security*** > ***Authentication*** page.	

Disable LDAP caching

O15	Disable LDAP caching	P1

The centralized authentication system allows the caching of authentication credentials for a configurable period. If an account were to be blocked, change groups, or have its password changed, authentication, with the old credentials, would still be possible during the caching time if the server is not reachable. *To avoid authorizing an access request that has been disabled on the LDAP server, it is advisable to disable the caching of credentials.* *Warning, in the event of a lack of communication between the router and the centralized directory, authentication will no longer be possible.*	
Application	On the page > ***Home*** > ***Setup*** > ***Security*** > ***Authentication***: Uncheck the parameter **Cache credentials**

Use LDAPS only

O16	Use LDAPS only	P1
The RADIUS and TACACS+ protocols are not providing a sufficient level of security. In addition, it has some limitations since it does not allow to define roles for administrators. *In order to improve the security of the centralized authentication system, it is necessary to use the secure and encrypted LDAPs protocol.*		
Application	On the page > ***Home*** > ***Setup*** > ***Security*** > ***Authentication*** : • **Authentication type** : `LDAP` • Check the parameter **LDAP over TLS**	

Enable authentication protection

O17	Enable authentication protection	P1
Brute force attack is a method of trying all possible password combinations in order to find a user's credentials, and thus impersonate them and gain access to an escalation of privileges. *In order to improve the security of the authentication system, it is necessary to protect authentication from brute force attacks.*		
Application	On the > ***Home*** > ***Setup*** > ***Security*** > ***Authentication*** page, in the 'Authentication protection' section: • Check the **Enabled** parameter	

Authentication warning

O18	Authentication warning	P3
Displaying a system usage notification message before authenticating serves as a deterrent to anyone attempting to access the product illegally. *This allows for criminal prosecution of offenders and demonstration of intentional violation.*		
Application	On the > ***Home*** > ***Setup*** > ***Security*** > ***Authentication*** page, in the 'Authentication warning' section, specify a message to be displayed on all authentication interfaces in the parameter **Warning message before authentication** * Check the **Enabled** parameter	

4. FOLLOW-UP ON RECOMMENDATIONS

A1: Enable authentication	**P1**	
A2: HTTPs protocol	**P1**	
A3: Disable access to administration by M2Me	**P1**	
A4: Disable WAN administration access	**P1**	
A5: Disable SSH Server	**P1**	
A6: Access management	**P1**	
A7: Disable temporary factory reset	**P1**	
A8: Hotline Access Configuration	**P2**	
A9: Disable remote access by push button	**P2**	
O1: Keep equipment up to date	**P1**	
O2: Regular configuration backups	**P3**	
O3: Backup Security	**P3**	
O4: Outsourcing backups	**P3**	
O5: Restore Backups	**P3**	
O6: Time Synchronization	**P2**	
O7: Outsourcing Logs	**P2**	
O8: Analyze logs	**P3**	
O9: SNMP (v3) supervision	**P3**	
O10: Monitored indicators	**P3**	
O11: Long term monitoring	**P3**	
O12: Network traffic analysis with ERSPAN	**P3**	
O13: Password Policy	**P2**	
O14: Use a centralized authentication system	**P2**	
O15: Disable LDAP caching	**P1**	
O16: Use LDAPS only	**P1**	
O17: Enable authentication protection	**P1**	
R1: Configure DNS manually	**P2**	
R2: Disable DHCP Server	**P1**	
R3: Disable Application Server	**P1**	
R4: Disable SNMP agent	**P1**	
R5: Disable NTP server	**P1**	
R6: Disable EticFinder	**P1**	

4. Follow-up on recommendations

R7: Disable WEB portal	**P1**	
R8: Disable M2Me_Connect	**P1**	
R9: Disable Modbus TCP Server	**P1**	
R10: Disable OPC-UA Server	**P1**	
R11: Block unused ports	**P3**	
R12: Disable unused interfaces	**P3**	
R13: Blocking incoming WAN to LAN flows	**P1**	
R14: Blocking LAN to WAN outgoing flows	**P1**	
R15: Blocking VPN to LAN inbound streams	**P1**	
R16: Blocking LAN to VPN outgoing flows	**P1**	
R17: Enable the anti-Denial of Service filter	**P1**	
R18: Disable conntrack helpers	**P1**	
R19: Using a trusted PKI	**P1**	
R20: Equipment Certificates	**P1**	
R21: Revocation of certificates	**P1**	
U1: User identifiers	**P1**	
U2: Password Construction	**P1**	
V1: Use of certificates	**P1**	
V2: Encryption and authentication algorithms	**P1**	
V3: Prohibit traffic between VPNs	**P1**	
V4: OpenVPN: Authentication Management	**P1**	
V5: OpenVPN: Choosing Diffie-Hellman	**P1**	
V6: OpenVPN: Using tls-crypt v2	**P1**	
V7: OpenVPN: Disable LZO compression	**P1**	
V8: IPsec: Authentication Management	**P1**	
V9: IPsec: Diffie-Hellman Group	**P1**	
V10: Disable PPTP	**P1**	
V11: Disable L2TP/IPSec	**P1**	
V12: User Certificates	**P1**	
V13: Two-factor authentication	**P1**	
V14: Encryption and authentication algorithms	**P1**	
V15: Only one remote connection at a time	**P1**	
V16: Disable LZO compression	**P1**	

5. DISPOSAL

The disposal procedure allows the product to be returned to its initial factory configuration, as well as deleting all user data from the product (secrets, passwords, configurations, certificates, private keys, ...).

NOTE	This data is lost and cannot be recovered with data mining software.

On the back of the product there is a hole to press a button; obtain a rod in order to press this button.

5.1. Procedure

1. Turn off the product
2. Press the back button
3. Power on the product while pressing the button on the back for 30 to 40 seconds.
4. The LED will blink in red/green
5. The product will revert to its factory settings, while deleting all user data.