# RAS/IPL/SIG Guide de sécurisation 4.13

*Cette documentation est également disponible en version web sur doc.etictelecom.com*

# TABLE OF CONTENTS

# 1. RÉFÉRENCES


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. CONVENTIONS DE NOTATION

## 2.1. Recommandations

| Rx | Recommandation | Px |
|---|---|---|
| *Motivation du paramétrage (l'application de ce paramètre renforce XX)* | | |
| **Application** | Comment mettre en pratique la recommandation dans la configuration du routeur. | |

- **Rx** : Identifiant de la recommandation pour référence
- **Recommandation** : Titre de la recommandation de configuration
- **Px** : Priorité du paramétrage (de x=1 "Le plus prioritaire" à x=3 "Le moins prioritaire")

Les recommandations sont groupées en 5 catégories:

- **Ax**: Interfaces d'**A**dministration
- **Ux**: Gestion des **U**tilisateurs
- **Rx**: Sécurité **R**éseau
- **Vx**: **V**PN
- **Ox**: Gestion **O**pérationnelle

# 3. SÉCURISATION DE LA CONFIGURATION

Cette section contient toutes les recommandations permettant de sécuriser la configuration des routeurs dans un environnement de production.

## 3.1. Interfaces d'administration

| | |
|---|---|
| **NOTE** | Cette partie n'aborde pas la problématique d'une architecture sécurisée d'administration. Les règles ici citées sont une synthèse des règles jugées fondamentales pour une administration sécurisée d'un équipement. Pour une approche plus globale, se référer au guide spécifique de l'ANSSI (ANSSI-PA-022). |

### Accès sécurisé à l'interface d'administration

#### Activer l'authentification

| A1 | Activer l'authentification | P1 |
|---|---|---|
| *En absence de mot de passe, tout accès local à l'équipement donne les droits d'administration. Afin de prévenir les accès illégitimes et de restreindre les modifications de la configuration des équipements, l'administration de l'équipement doit impérativement nécessiter un mot de passe. Pour que le mot de passe ne soit pas récupérable en cas de compromission de l'équipement ou de ses extraits de configuration, les mots de passe doivent être enregistrés sous forme de hash selon un algorithme à l'état de l'art (Annexe B1 du RGS).* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Paramètre **Protéger l'accès à la configuration par mot de passe** :<br><br>• Activer la protection | |

#### Protocole HTTPs

| A2 | Protocole HTTPs | P1 |
|---|---|---|

| | |
|---|---|
| *Les flux non chiffrés peuvent être « écoutés » à de nombreux points du réseau, et les informations (telles que le mot de passe administrateur) sont alors accessibles. Afin qu'une tierce partie ne puisse pas écouter les échanges et récupérer des informations sensibles (identifiants…), l'administration de l'équipement doit se faire par des protocoles sécurisés et chiffrés (SSH, HTTPS…). Afin d'assurer l'authentification du serveur, le certificat associé doit être valide et issu d'une CA reconnue, en particulier la première connexion à la console d'administration ne doit pas lever d'alerte. Les interfaces d'administration sont une cible privilégiée pour un attaquant. Le concept de défense en profondeur implique de protéger par couches successives ces interfaces. L'une des premières actions est de changer les ports d'administrations définis par défaut par le constructeur, ce qui ralentira leur découverte par un attaquant.* | |
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Paramètre **Protocoles à utiliser pour la configuration** :<br><br>• Sélectionner `HTTPS seulement`<br><br>Paramètre **Port HTTPS d'administration (4433)** :<br><br>• Choisir un autre port que le port 4433 par défaut<br><br>Paramètre **Le port TCP 80 redirige vers la Zone Administration** :<br><br>• Désactiver l'option<br><br>Paramètre **Utiliser le certificat usine auto-signé** :<br><br>• Désactiver l'option<br><br>Paramètre **Choisir un certificat personnalisé** :<br><br>• Sélectionner le certificat ajouté dans l'équipement. Se référer au point Gestion des certificats pour configurer un certificat dans l'équipement. |

## Accès restreint à la console d'administration

### Désactiver l'accès à l'administration par M2Me

| A3 | Désactiver l'accès à l'administration par M2Me | P1 |
|---|---|---|
| *Si le routeur autorise l'accès par M2Me, ce canal peut être utilisé pour accéder à la console d'administration.* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Paramètre **Activer l'accès par M2Me (HTTPS seulement)** :<br><br>• Désactiver l'option | |

### Désactiver l'accès à l'administration par le WAN

| A4 | Désactiver l'accès à l'administration par le WAN | P1 |
|---|---|---|
| *L'interface WAN étant par définition accessible depuis un réseau externe, il est nécessaire de désactiver l'accès à l'administration par ce biais.* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Paramètre **Activer l'accès par le WAN (HTTPS seulement)** :<br><br>• Désactiver l'option | |

### Désactiver le serveur SSH

| A5 | Désactiver le serveur SSH | P1 |
|---|---|---|
| *Les serveurs SSH peuvent être facilement détectés par scan de port, et en absence de protection anti-brute force, l'interface SSH est fortement exposée à ces attaques. Afin de restreindre l'exposition de l'équipement, si le protocole SSH n'est pas utilisé régulièrement, il doit être désactivé et pourra être réactivé temporairement si une opération le justifie.* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Paramètre **Activer le serveur SSH** :<br><br>• Désactiver l'option | |

### Gestion des accès

| A6 | Gestion des accès | P1 |
|---|---|---|
| *Les administrateurs n'ont pas tous les mêmes usages. Il est nécessaire d'avoir des utilisateurs distincts avec le rôle d'administrateur associé correspondant à leur besoin d'utilisation. Réduire le champ d'action d'un administrateur permet de minimiser les changements de configuration non désirés, malveillants ou non. La compromission d'un compte administrateur n'ayant pas les droits maximums ne permet pas à l'attaquant de tout faire sur le produit.*<br>*Restreindre le champ d'action des administrateurs au strict nécessaire en choisissant le rôle adéquat améliore la sécurité du produit.* | | |
| **Application** | Pour la gestion des utilisateurs, voir la section Gestion des utilisateurs<br><br>Sur la page ***Configuration > Sécurité > Droits d'administration > Ajouter/Éditer un administrateur*** :<br><br>Paramètre **Role** :<br><br>• Sélectionner le rôle d'administrateur<br><br>Paramètre **Utilisateur** :<br><br>• Sélectionner l'utilisateur à qui attribuer le rôle | |

## Retour temporaire à la configuration usine

### Désactiver retour configuration usine temporaire

| A7 | Désactiver retour configuration usine temporaire | P1 |
|---|---|---|
| *Le retour à la configuration d'usine temporaire permet de prendre la main sur l'équipement, en appliquant la configuration usine par défaut. Un attaquant pourrait alors obtenir un accès à l'équipement, visualiser l'ensemble de la configuration et l'éditer.*<br>*Afin de restreindre l'accès au firmware et donc préserver l'intégrité de l'équipement, il est recommandé d'empêcher le retour à la configuration d'usine temporaire par un appui sur le bouton poussoir de face arrière.* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Paramètre **Désactiver le bouton poussoir arrière de retour en configuration usine temporaire** :<br><br>• Activer l'option | |

## Accès hotline

### Configuration de l'accès hotline

| A8 | Configuration de l'accès hotline | P2 |
|---|---|---|
| *L'accès pour le SAV nécessite la connaissance de deux mots de passe, le mot de passe généré sur le produit à la demande d'un administrateur. Et le mot de passe unique du produit détenu par **Etic Telecom**.*<br>*Le mot de passe généré sur le produit doit être stocké de manière sécurisée* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Bouton **Générer un nouveau mot de passe pour le SAV** :<br><br>• Cliquer sur le bouton `Générer`, puis stockez-le de manière sécurisée. | |

### Désactiver accès distant par bouton poussoir

| A9 | Désactiver accès distant par bouton poussoir | P2 |
|---|---|---|
| *Le bouton face avant du produit permet au SAV d'**Etic Telecom** de se connecter au produit sans le mot de passe généré sur le produit. Ce contournement du mot de passe est valide sur une période d'une heure.*<br>*Restreindre cette option ne permet pas de contourner le mot de passe généré par le produit.* | | |

| | |
|---|---|
| **Application** | Sur la page ***Configuration > Sécurité > Droits d'administration*** :<br><br>Paramètre **Désactiver le bouton poussoir autorisant l'accès distant au SAV Etic Telecom** :<br><br>• Activer l'option |

## 3.2. Gestion des utilisateurs

### Identifiants et mots de passe

#### Identifiants des utilisateurs

| U1 | Identifiants des utilisateurs | P1 |
|---|---|---|
| *L'usage de comptes générique ne permet pas d'imputer les actions et connexions ni de ségréguer les droits.*<br>*Afin de garantir une gestion plus fine des droits et une meilleure traçabilité, les identifiants des utilisateurs (administrateurs, opérateur, ...) doivent être nominatifs.* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Utilisateurs Ajouter/Modifier un utilisateur*** :<br><br>Paramètre **Nom d'utilisateur** :<br><br>• Il s'agit du login de l'utilisateur. Donner un nom explicite, car c'est cette information qui apparaîtra dans les journaux également.<br><br>Paramètre **Mot de passe** :<br><br>• Choisissez un mot de passe robuste. L'utilisateur peut aller changer lui-même son mot de passe par la suite s'il a accès à la page d'administration. | |

#### Construction du mot de passe

| U2 | Construction du mot de passe | P1 |
|---|---|---|
| *Un mot de passe trop simple pourra être facilement trouvé lors d'une attaque de type brute force ou par dictionnaire.*<br>*Afin de se prémunir contre une telle attaque, une politique de mots de passe forte doit être appliquée sur les comptes administrateurs. Celui-ci comportera un minimum de 16 caractères, avec au moins 3 classes de caractères et ne sera pas facilement devinable (pas de mot du dictionnaire). Il sera unique à chaque équipement.* | | |
| **Application** | Sur la page ***Configuration > Sécurité > Utilisateurs Ajouter/Modifier un utilisateur*** :<br><br>Paramètre **Mot de passe** :<br><br>• Changer le mot de passe d'un utilisateur. L'utilisateur peut aller changer lui-même son mot de passe s'il a accès à la page d'administration. | |

# 3.3. Sécurité réseau

## Connectivité réseau

### Configurer le DNS manuellement

| R1 | Configurer le DNS manuellement | P2 |
|---|---|---|
| *En manipulant les entrées DNS, il est possible d'affecter les opérations qui s'appuient dessus (tel que potentiellement l'établissement des tunnels VPN ou l'obtention des mises à jour). Si les serveurs DNS sont définis par DHCP, il n'est plus possible de garantir les informations DNS. Afin de restreindre le risque lié à la manipulation d'enregistrements DNS, les serveurs DNS utilisés par les équipements doivent être des serveurs de confiance. Il est recommandé d'utiliser des serveurs DNS statiques et déterminés de confiance (idéalement internes ou ceux du FAI).* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Interface WAN***<br><br>Il est recommandé d'utiliser des serveurs DNS internes afin d'éviter les divulgations de noms de domaines internes sur des DNS externes.<br><br>• Décocher la case **Obtenir les adresses des serveurs DNS automatiquement**<br>• Ajouter un serveur DNS primaire<br>• Ajouter un serveur DNS secondaire | |

### Désactiver le serveur DHCP

| R2 | Désactiver le serveur DHCP | P1 |
|---|---|---|
| *L'allocation d'adresses par DHCP sans contrôles complémentaires (par exemple NAC) permet d'intégrer une machine exogène au réseau, sous seule condition de disposer d'un accès physique. Pour limiter les accès non autorisés au réseau, il est recommandé de ne pas activer les fonctionnalités de serveur DHCP sur les routeurs « distants ». Si toutefois le DHCP doit être activé pour des contraintes terrain, il est nécessaire de contrôler les terminaux qui se connectent sur le réseau.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Interface LAN > Serveur DHCP***<br><br>Décocher la paramètre ***Activer le serveur***<br><br>Si toutefois le DHCP doit être activé pour des contraintes terrain, il est possible d'associer les IP allouées en DHCP par adresse MAC. Veillez à entrer une plage d'adresse IP cohérente avec le nombre d'actifs gérés par le DHCP. | |

## Réduire la surface d'exposition

### Désactiver le serveur d'application

| R3 | Désactiver le serveur d'application | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Accès distant > Moyens d'accès***<br><br>Décocher le paramètre **Activer le serveur d'applications HTTPS** | |

### Désactiver l'agent SNMP

| R4 | Désactiver l'agent SNMP | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques.*<br>*Si la supervision SNMP n'est pas mise en place, il est recommandé de désactiver l'agent SNMP.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Système > SNMP***<br><br>Décocher le paramètre **Activer** | |

### Désactiver le serveur NTP

| R5 | Désactiver le serveur NTP | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Système > Réglage date et heure > NTP***<br><br>Décocher le paramètre **Activer le service NTP** | |

### Désactiver EticFinder

| R6 | Désactiver EticFinder | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Droits d'administration***<br><br>Décocher le paramètre **Activer EticFinder** | |

### Désactiver le portail WEB

| R7 | Désactiver le portail WEB | P1 |
|---|---|---|

| | |
|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | |
| **Application** | Dans le menu : ***Accueil > Configuration > Interface LAN > Portail WEB***<br><br>Décocher les paramètres **Afficher le portail web** et **Afficher le portail sur la page d'accueil** |

### Désactiver M2Me_Connect

| R8 | Désactiver M2Me_Connect | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Accès distant > M2Me_Connect***<br><br>Décocher le paramètre **Actif** | |

### Désactiver le serveur Modbus TCP

| R9 | Désactiver le serveur Modbus TCP | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Système > Serveur Modbus***<br><br>Décocher le paramètre **Activer** | |

### Désactiver le serveur OPC-UA

| R10 | Désactiver le serveur OPC-UA | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Système > Serveur OPC UA***<br><br>Décocher le paramètre **Actif** | |

### Bloquer les ports non utilisés

| R11 | Bloquer les ports non utilisés | P3 |
|---|---|---|
| *L'accès physique à l'équipement peut parfois être compromis, il convient alors de bloquer les ports inutilisés physiquement, afin qu'une personne mal intentionnée ayant un accès physique à l'équipement ne puisse pas utiliser ces ports.* | | |

| | |
|---|---|
| **Application** | Utiliser des verrous de ports physiques afin de bloquer les ports RJ45 ou USB non utilisés. |

#### Désactiver les interfaces non utilisées

| R12 | Désactiver les interfaces non utilisées | P3 |
|---|---|---|
| *L'accès physique à l'équipement peut parfois être compromis, il convient alors de désactiver les interfaces inutilisées, afin qu'une personne mal intentionnée ayant un accès physique à l'équipement ne puisse pas utiliser ces interfaces.* | | |
| **Application** | Dans le menu : > ***Accueil*** > ***Configuration*** > ***Interface LAN*** > ***Ethernet et IP***<br><br>Dans la partie "Paramètres avancés", chaque port LAN à sa configuration : **Configuration port 1/2/3/4**, Mettre la valeur de ce paramètre à `Désactivé` pour désactiver les ports inutilisés.<br><br>Dans le menu : > ***Accueil*** > ***Configuration*** > ***Interfaces WAN*** > ***Ethernet***, pour le paramètre **Type de connexion** mettre la valeur `Désactivée` si c'est inutilisé.<br><br>Dans le menu : > ***Accueil*** > ***Configuration*** > ***Interfaces WAN*** > ***Wi-Fi***, décocher le paramètre **Activer le WAN Wi-Fi** si c'est inutilisé.<br><br>Dans le menu : > ***Accueil*** > ***Configuration*** > ***Interfaces WAN*** > ***Cellulaire***, décocher le paramètre **Actif** si c'est inutilisé. | |

## Firewall

#### Blocage des flux entrants WAN vers LAN

| R13 | Blocage des flux entrants WAN vers LAN | P1 |
|---|---|---|
| *Tout service exposé sur internet est susceptible d'être la cible d'une attaque, qu'elle soit ciblée ou générique, opportuniste ou automatisée. Les flux entrants depuis un réseau public (Internet/WAN) devraient être limités au maximum. Dans le contexte de VPN site à site sans accès direct sur les sites distants, aucun flux direct WAN vers LAN ne doit être autorisé.* | | |
| **Application** | Dans le menu : ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Pare-feu***<br><br>Bloquer par défaut les flux entrants WAN vers LAN : **Politique par défaut WAN→LAN** à `Interdire` | |

#### Blocage des flux sortants LAN vers WAN

| R14 | Blocage des flux sortants LAN vers WAN | P1 |
|---|---|---|
| *Les accès Internet non contrôlés peuvent être source de menaces sur le réseau ou d'exfiltration de données. Dans le contexte de VPN site à site sans accès direct sur les sites distants, aucun flux direct depuis le réseau local (LAN) de ces sites vers Internet (WAN) ne doit être autorisé.* | | |

| | |
|---|---|
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Pare-feu***<br><br>Bloquer par défaut les flux entrants LAN vers WAN : **Politique par défaut LAN→WAN** à `Interdire` |

### Blocage des flux entrants VPN vers LAN

| R15 | Blocage des flux entrants VPN vers LAN | P1 |
|---|---|---|
| *Les flux provenant du VPN à destination du LAN sont également à sécuriser, car la zone d'origine n'est pas forcément une zone de confiance. Il convient de maîtriser tous les flux à destination du LAN afin d'éviter toute tentative d'attaque provenant d'un actif compromis hors LAN. Des besoins de communications entre les équipements du LAN et ceux de l'infrastructure centrale peuvent être nécessaires (supervision, sauvegarde, etc). Il est donc primordial de les lister, de les renseigner dans un référentiel, puis de les implémenter de manière claire et précise. Toute règle trop permissive abaisse le niveau de sécurité globale du SI.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Pare-feu***<br><br>Bloquer par défaut les flux entrants VPN vers LAN : **Politique par défaut VPN→LAN** à `Interdire` | |

### Blocage des flux sortants LAN vers VPN

| R16 | Blocage des flux sortants LAN vers VPN | P1 |
|---|---|---|
| *Les flux provenant du LAN à destination du VPN doivent être précis et non pas ouverts sans restriction. En cas de compromission, des flux précis permettent de ralentir la propagation d'un attaquant au travers du SI. Un important travail d'identification des flux est à faire en amont afin d'éviter toute interruption de service dû à des règles trop strictes ou à un oubli. Il est nécessaire de lister les communications entre le LAN et les réseaux distants, de les renseigner dans un référentiel, puis de les implémenter de manière claire et précise. Toute règle trop permissive abaisse le niveau de sécurité globale du SI.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Pare-feu***<br><br>Bloquer par défaut les flux entrants VPN vers LAN : **Politique par défaut LAN→VPN** à `Interdire` | |

### Activer le filtre anti Déni de Service

| R17 | Activer le filtre anti Déni de Service | P1 |
|---|---|---|
| *L'acheminement excessif de paquets vers le port d'administration peut entraîner un potentiel déni de service (DoS), entraînant ainsi une indisponibilité de la page web.*<br>*Il faut donc pouvoir identifier et bloquer les paquets malicieux.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Pare-feu***<br><br>Cocher le paramètre **Activer le filtre anti Déni de Service (DoS)** | |

### Désactiver les conntrack helpers

| R18 | Désactiver les conntrack helpers | P1 |
|---|---|---|
| *Un problème de contournement des règles iptables fixées par utilisateur peut survenir avec l'utilisation de règles firewall RELATED,ESTABLISH trop génériques et le chargement de helper de service non présent ou non utilisé sur la machine (par exemple FTP actif, SIP, IRC ...).*<br>*Il est donc recommandé de désactiver les conntrack helpers.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Pare-feu***<br><br>Décocher le paramètre **Activer les 'conntrack helpers' (Non recommandé)** | |

## Gestion des certificats

### Usage d'une PKI de confiance

| R19 | Usage d'une PKI de confiance | P1 |
|---|---|---|
| *L'identification des équipements et les authentifications VPN s'appuient sur les certificats. Une compromission de la PKI peut donc remettre en cause la totalité de la chaîne de confiance.*<br><br>*La gestion des certificats doit être effectuée par une PKI maîtrisée par l'entreprise ou reconnue de confiance. Cela permet une définition fine de l'usage et du format des certificats. Les certificats doivent de plus être créés avec des algorithmes de chiffrement à l'état de l'art, afin d'éviter les faiblesses des algorithmes obsolètes (cassage...) (SDE-NT-35/ANSSI/SDE/NP).* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Magasin de certificats***<br><br>L'ajout et la suppression de Certificats, de clés privées et de certificats d'autorité de certification sont possibles dans les différents tableaux. Voir la partie « Router firmware / Certificate Store » du guide de configuration pour de plus amples informations.<br><br>Nous recommandons : une fonction de hachage utilisée pour la signature des certificats doit être de la famille SHA-2 et la clé de signature des certificats doit être au moins de 3072 bits pour RSA et de 256 pour ECC.<br><br>Pour une gestion fine d'une PKI, se reporter aux annexes B du RGS (Annexes B1 et B2 du RGS). | |

### Certificats des équipements

| R20 | Certificats des équipements | P1 |
|---|---|---|
| *La réutilisation d'un certificat pour plusieurs clients empêche d'identifier celui qui l'utilise, augmente l'exposition du certificat, et en cas de compromission de celui-ci, la révocation/réémission du certificat impacte plusieurs clients. Les certificats doivent être uniques et individuels par machine pour une meilleure traçabilité et permettre la révocation sans effets de bords en cas de besoin. Utilisés pour les communications HTTPS, ils doivent avoir une durée de validité de 13 mois maximum.* | | |

| | |
|---|---|
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Magasin de certificats***<br><br>L'ajout et la suppression de Certificats, de clés privées et de certificats d'autorité de certification sont possibles dans les différents tableaux. Voir la partie « Router firmware / Certificate Store » du guide de configuration pour de plus amples informations.<br><br>L'ensemble des services nécessitant un certificat du routeur viendront les récupérer dans le magasin de certificats. |

**Révocation des certificats**

| R21 | Révocation des certificats | P1 |
|---|---|---|
| *Un certificat qui n'est plus utilisé est potentiellement moins protégé, et représente donc une source de risque tant qu'il est valide. Les certificats dont l'objet n'a plus lieu d'être doivent être révoqués. L'objectif est de garder le contrôle sur son parc de certificat.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Magasin de certificats*** : Onglet Liste des CRL<br><br>Nous recommandons, de votre côté, de mettre à jour la liste des certificats attribués aux utilisateurs et de garder un historique des certificats révoqués. Quelques cas d'usages classiques où les certificats doivent être révoqués :<br>• Des équipements sortis du parc informatique, postes remis en stock…<br>• Utilisateurs décommissionnés : mouvement de personnel (interne ou partenaire), fin de contrat avec une entreprise externe…<br>• Une liste la plus exhaustive possible doit être établie, et la révocation des certificats doit être incluse dans les différentes procédures liées. | |

## 3.4. VPN

### VPN site à site

**Utilisation des certificats**

| V1 | Utilisation des certificats | P1 |
|---|---|---|
| *La réutilisation d'un certificat pour plusieurs clients empêche d'identifier celui qui l'utilise, augmente l'exposition du certificat, et en cas de compromission de celui-ci, la révocation/réémission du certificat impacte plusieurs clients.*<br>*Il est recommandé d'utiliser des certificats uniques et individuels par machine pour une meilleure traçabilité et permettre la révocation sans effets de bords en cas de besoin.*<br>*La signature de certificats numériques générés à partir de clés privées jugées obsolètes (ex: RSA 1024) est déprécié pour des raisons de sécurité. Il faut donc empêcher l'utilisation de ces certificats.* | | |

| | |
|---|---|
| **Application** | Dans les menus :<br>• ***Accueil > Configuration > Réseau > Connexions VPN > IPSec > Connexion IPsec***<br>• ***Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Serveur OpenVPN***<br>• ***Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexions OpenVPN sortantes***<br><br>Une fois le certificat installé, décocher **Utiliser le certificat usine**, et dans le menu contextuel **Choisir un certificat personnalisé**, choisir le certificat nouvellement ajouté. Éviter l'utilisation du certificat par défaut qui n'est pas validé par une autorité de certification reconnue.<br><br>Se référer à la section Gestion des certificats pour générer des certificats clients et serveurs à l'état de l'art. |

### Algorithmes de chiffrement et d'authentification

| V2 | Algorithmes de chiffrement et d'authentification | P1 |
|---|---|---|
| *De nouvelles vulnérabilités sur les protocoles et algorithmes sont régulièrement découvertes, remettant en cause leur niveau de protection.*<br>*Les différents protocoles et algorithmes inhérents à l'usage des VPN doivent être configurés à l'état de l'art, afin d'éviter les faiblesses des algorithmes obsolètes (cassage...) (Annexes B1 du RGS).* | | |
| **Application** | Dans les menus :<br>• ***Accueil > Configuration > Réseau > Connexions VPN > IPSec > Connexion IPsec***<br>• ***Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Serveur OpenVPN***<br>• ***Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexions OpenVPN sortantes***<br><br>Choisir les valeurs suivantes pour ces paramètres :<br>• **Algorithme de chiffrement** / **Chiffrement**: `AES-256-CBC` ou `AES-256-GCM`<br>• **Algorithme d'authentification** / **Authentification**: `SHA-256`, `SHA-384` ou `SHA-512` | |

### Interdire le trafic entre VPN

| V3 | Interdire le trafic entre VPN | P1 |
|---|---|---|
| *Les flux provenant du VPN à destination des autres VPN sont à sécuriser, car la zone d'origine n'est pas forcément une zone de confiance.*<br>*Il convient de maîtriser tous les flux à destination des VPN afin d'éviter toute tentative d'attaque.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Pare-feu***<br>• Décocher la case **Autoriser le trafic entre VPN** | |

### OpenVPN : Gestion de l'authentification

| V4 | OpenVPN : Gestion de l'authentification | P1 |
|---|---|---|
| *L'authentification par mot de passe présente plusieurs risques : la fuite du mot de passe (son remplacement nécessite alors d'intervenir sur chaque équipement concerné), son manque de renouvellement, et sa robustesse. L'usage d'un certificat individuel pour l'authentification permet de bloquer les accès par révocation du certificat. La durée de vie des certificats est également fixée, ce qui impose la rotation des secrets dans une fenêtre de temps définie. Enfin, un certificat constitue généralement un secret plus robuste qu'un mot de passe. À ce titre, c'est le mode d'authentification préconisé par l'ANSSI.*<br>*Il est recommandé de gérer l'authentification des pairs OpenVPN par certificat.* | | |
| **Application** | La configuration d'un tunnel VPN se fait en deux parties. Tout d'abord, un serveur VPN doit être configuré, puis pour accepter les connexions des clients, une connexion entrante par client doit être configurée.<br>• Authentification côté serveur<br>◦ Dans le menu : ***Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexion OpenVPN***<br>◦ Définir un mot de passe fort. Ce mot de passe sera également utilisé par le routeur client initiant la connexion<br>◦ Entrer le "Common Name" du certificat du routeur client que vous aurez préalablement généré et ajouter au routeur client initiant la connexion. Se référer à la section Gestion des certificats pour voir comment ajouter un certificat dans un routeur.<br>• Authentification côté client<br>◦ Dans le menu : ***Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Connexions OpenVPN sortantes***<br>◦ Entrer le mot de passe fort partagé entre le serveur et le client | |

### OpenVPN : Choix du Diffie-Hellman

| V5 | OpenVPN : Choix du Diffie-Hellman | P1 |
|---|---|---|
| *De nouvelles vulnérabilités sur les protocoles et algorithmes sont régulièrement découvertes, remettant en cause leur niveau de protection.*<br>*Les différents protocoles et algorithmes inhérents à l'usage de TLS doivent être configurés à l'état de l'art, afin d'éviter les faiblesses des algorithmes obsolètes (cassage...) (SDE-NT-35/ANSSI/SDE/NP).* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Réseau > Connexions VPN > OpenVPN > Serveur OpenVPN***<br><br>Pour le paramètre **Diffie Hellman**, choisir la valeur `4096 bits (Recommandé)` | |

### OpenVPN : Utilisation de tls-crypt v2

| V6 | OpenVPN : Utilisation de tls-crypt v2 | P1 |
|---|---|---|

| | |
|---|---|
| *Les premiers échanges pour l'établissement de la connexion TLS entre le client et le serveur OpenVPN sont fait en clair. Cet échange de clés fait en clair peut induire une vulnérabilité de type Man-in-the-Middle.*<br>*Pour parer ce type d'attaques, il est recommandé de renseigner une clé pré-partagée tls-crypt permettant de chiffrer aussi les trames d'établissement du canal TLS.* | |
| **Application** | Dans le menu : ***Accueil*** > ***Configuration*** > ***Réseau*** > ***Connexions VPN*** > ***OpenVPN*** > ***Serveur OpenVPN***<br>• Cocher la case **Activer tls-crypt-v2** et renseigner la clé tls-crypt-v2<br>Dans le menu : ***Accueil*** > ***Configuration*** > ***Réseau*** > ***Connexions VPN*** > ***OpenVPN*** > ***Connexions OpenVPN sortantes***<br>• Cocher la case **Activer tls-crypt-v2** et renseigner la clé tls-crypt-v2 |

**OpenVPN : Désactiver la compression LZO**

| V7 | OpenVPN : Désactiver la compression LZO | P1 |
|---|---|---|
| *L'utilisation de la compression LZO est déconseillée, car le ratio de compression laisse fuiter de l'information sur les données compressées claires.*<br>*Il est donc recommandé de désactiver la compression LZO.* | | |
| **Application** | Dans le menu : ***Accueil*** > ***Configuration*** > ***Réseau*** > ***Connexions VPN*** > ***OpenVPN*** > ***Serveur OpenVPN***<br>• Cocher la case **Désactiver la compression**<br>Dans le menu : ***Accueil*** > ***Configuration*** > ***Réseau*** > ***Connexions VPN*** > ***OpenVPN*** > ***Connexions OpenVPN sortantes***<br>• Cocher la case **Désactiver la compression** | |

**IPsec : Gestion de l'authentification**

| V8 | IPsec : Gestion de l'authentification | P1 |
|---|---|---|
| *L'authentification par mot de passe présente plusieurs risques : la fuite du mot de passe (son remplacement nécessite alors d'intervenir sur chaque équipement concerné), son manque de renouvellement, et sa robustesse. L'usage d'un certificat individuel pour l'authentification permet de bloquer les accès par révocation du certificat. La durée de vie des certificats est également fixée, ce qui impose la rotation des secrets dans une fenêtre de temps définie. Enfin, un certificat constitue généralement un secret plus robuste qu'un mot de passe. À ce titre, c'est le mode d'authentification préconisé par l'ANSSI.*<br>*Il est recommandé d'utiliser une authentification par certificats et non par clé pré-partagée (DAT-NT-003/ANSSI/SDE/NP).* | | |

| | |
|---|---|
| **Application** | Dans le menu : ***Accueil*** > ***Configuration*** > ***Réseau*** > ***Connexions VPN*** > ***IPSec*** > ***Connexion IPSec***<br>• Configurer l'authentification par certificats<br>◦ Dans le champ **Authentification par**, sélectionner `Certificat client`<br>◦ Dans la partie IKE authentification, décocher **Utiliser le certificat usine**<br>◦ Choisir votre certificat serveur ou certificat client<br>◦ Choisir une **Politique de révocation de certificat** `strict`<br>• Configurer l'authentification par PSK<br>◦ Dans le champ **Authentification par**, sélectionner `Clé pré partagée`<br>◦ Entrer la valeur de la PSK dans le champ **Valeur clé**. Une PSK devrait avoir une entropie minimale supérieure ou égale à 100 bits |

#### IPsec : Groupe Diffie-Hellman

| V9 | IPsec : Groupe Diffie-Hellman | P1 |
|---|---|---|
| *De nouvelles vulnérabilités sur les protocoles et algorithmes sont régulièrement découvertes, remettant en cause leur niveau de protection.*<br>*Les différents protocoles et algorithmes inhérents à l'usage d'IPsec doivent être configurés à l'état de l'art, afin d'éviter les faiblesses des algorithmes obsolètes (cassage...) (DAT-NT-003/ANSSI/SDE/NP).* | | |
| **Application** | Dans le menu : ***Accueil*** > ***Configuration*** > ***Réseau*** > ***Connexions VPN*** > ***IPSec*** > ***Connexion IPSec***<br>Cocher la case **Paramètres avancés**, pour le paramètre **Groupe DH** choisir parmi ces valeurs : `Groupe 14`, `Groupe 16`, `Groupe 18` | |

## VPN poste à site

#### Désactiver PPTP

| V10 | Désactiver PPTP | P1 |
|---|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques. Le protocole PPTP est maintenant considéré comme un protocole obsolète niveau sécurité, afin de restreindre l'exposition de l'équipement, il doit être désactivé.* | | |
| **Application** | Dans le menu : ***Accueil*** > ***Configuration*** > ***Accès distant*** > ***Moyens d'accès***<br>Décocher la case **Activer PPTP** | |

#### Désactiver L2TP/IPSec

| V11 | Désactiver L2TP/IPSec | P1 |
|---|---|---|

| | |
|---|---|
| *Plus l'équipement est exposé, plus les sources possibles d'accès illégitimes sont nombreuses, et notamment les scans automatiques.*<br>*Il est conseillé de désactiver le serveur L2TP/IPSec afin de restreindre l'exposition de l'équipement.* | |
| **Application** | Dans le menu : ***Accueil > Configuration > Accès distant > Moyens d'accès***<br><br>Décocher la case **Activer L2TP/IPSec** |

#### Certificats utilisateurs

| V12 | Certificats utilisateurs | P1 |
|---|---|---|
| *La réutilisation d'un certificat pour plusieurs utilisateurs empêche d'identifier celui qui l'utilise, augmente l'exposition du certificat, et en cas de compromission de celui-ci, la révocation-réémission du certificat impacte plusieurs utilisateurs.*<br>*Les certificats utilisateurs doivent être nominatifs pour la traçabilité et permettre leur révocation en cas de besoin. Nous recommandons une validité maximum de 1 an.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Sécurité > Utilisateurs***<br><br>Il est attendu le CN, i.e. Common Name, comme moyen d'identification du certificat. Renseigner le CN du certificat utilisateur dans le champ **CN du certificat utilisateur**. Nous recommandons de suivre la démarche suivante :<br><br>• Délivrer un certificat par utilisateur, c'est-à-dire avec un CN unique, et ne le distribuer qu'à l'utilisateur concerné<br>• Maintenir une liste des certificats attribués aux utilisateurs, ce qui facilite notamment leur révocation en cas de besoin<br>• Définir une validité maximale de certificat d'un an<br>• Utiliser un certificat serveur sur le routeur pour les VPN poste à site<br><br>Se référer à la section Gestion des certificats pour les bonnes pratiques de génération de certificats | |

#### Authentification deux facteurs

| V13 | Authentification deux facteurs | P1 |
|---|---|---|
| *Les postes mobiles des utilisateurs étant exposés, un facteur d'authentification simple peut fuiter.*<br>*L'authentification des utilisateurs doit être à deux facteurs.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Accès distant > Moyens d'accès***, onglets **Propriétés OpenVPN** et **Propriétés OpenVPN (Accès SmartPhone)**<br><br>Pour le paramètre **Authentification des utilisateurs**, choisir `Login / Mot de passe + Certificat` | |

#### Algorithmes de chiffrement et d'authentification

| V14 | Algorithmes de chiffrement et d'authentification | P1 |
|---|---|---|

| | |
|---|---|
| *De nouvelles vulnérabilités sur les protocoles et algorithmes sont régulièrement découvertes, remettant en cause leur niveau de protection.*<br>*Les différents algorithmes inhérents à l'usage de TLS pour l'établissement d'un VPN poste à site doivent être configurés à l'état de l'art afin d'éviter les faiblesses des algorithmes obsolètes (SDE-NT-35/ANSSI/SDE/NP).* | |
| **Application** | Dans le menu : ***Accueil > Configuration > Accès distant > Moyens d'accès***, onglets **Propriétés OpenVPN** et **Propriétés OpenVPN (Accès SmartPhone)**<br><br>Choisir les valeurs suivantes pour ces paramètres :<br><br>• **Algorithme de chiffrement** : `AES-256-CBC` ou `AES-256-GCM`<br>• **Algorithme de hachage** : `SHA-256`, `SHA-384` ou `SHA-512` |

**Une seule connexion distante à la fois**

| V15 | Une seule connexion distante à la fois | P1 |
|---|---|---|
| *En changeant l'adresse IP du client "OpenVPN accès distant" pour une adresse IP d'un autre client "OpenVPN accès distant" déjà connecté au serveur d'accès distant, un attaquant obtient les droits de firewall de l'utilisateur usurpé.*<br>*Il est donc recommandé de n'autoriser qu'une seule connexion distante à la fois, de cette manière, les droits de firewall ne peuvent pas être usurpés.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Accès distant > Moyens d'accès***, onglets **Propriétés OpenVPN** et **Propriétés OpenVPN (Accès SmartPhone)**<br><br>Cocher la case **N'autoriser qu'une seule connexion distante à la fois** | |

**Désactiver la compression LZO**

| V16 | Désactiver la compression LZO | P1 |
|---|---|---|
| *L'utilisation de la compression LZO est déconseillée, car le ratio de compression laisse fuiter de l'information sur les données compressées claires.*<br>*Il est donc recommandé de désactiver la compression LZO.* | | |
| **Application** | Dans le menu : ***Accueil > Configuration > Accès distant > Moyens d'accès***, onglets **Propriétés OpenVPN** et **Propriétés OpenVPN (Accès SmartPhone)**<br><br>Cocher la case **Désactiver la compression** | |

## 3.5. Gestion opérationnelle

### Mises à jour

**Maintien à jour de l'équipement**

| O1 | Maintien à jour de l'équipement | P1 |
|---|---|---|

| | |
|---|---|
| *Des failles de sécurités dans le firmware de l'équipement peuvent permettre de contourner les mesures de sécurité et de prendre le contrôle de l'équipement. Afin de se prémunir des failles corrigées par l'éditeur, l'équipement doit être régulièrement mis à jour.* | |
| **Application** | Les mises à jour des versions du firmware routeur sont publiées sur le site internet d'Etic Telecom.<br><br>Les vulnérabilités concernant les versions du firmware des routeurs sont publiées sur une page dédiée.<br><br>**Pour mettre à jour le firmware du routeur :**<br><br>Sur la page > ***Accueil*** > ***Maintenance*** > ***Mises à jour du logiciel*** :<br><br>Paramètre **Mettre à jour en utilisant un fichier de mise à jour** :<br><br>1. Choisir le fichier de mise à jour<br>2. Cliquer sur le bouton `Mettre à jour` |

## Sauvegardes de la configuration

### Sauvegardes régulières de la configuration

| O2 | Sauvegardes régulières de la configuration | P3 |
|---|---|---|
| *Une fausse manipulation, une correction ou la panne d'un équipement peuvent survenir, entraînant le besoin de rétablir la configuration pour la continuité de service, sur cet équipement ou un équipement neuf.*<br>*Afin de permettre un retour rapide à un état de fonctionnement en cas de besoin, une sauvegarde de la configuration de l'équipement doit être effectuée régulièrement.* | | |
| **Application** | Sur la page > ***Accueil*** > ***Maintenance*** > ***Gestion des configurations*** :<br><br>**Sauvegarder la configuration actuelle :**<br><br>Paramètre **Nom de la configuration** :<br><br>1. Nommer la configuration<br>2. Cliquer sur le bouton `Enregistrer`<br><br>**Télécharger la configuration sur le PC local :**<br><br>Tableau **Configurations utilisateur** :<br><br>1. Sélectionner la configuration<br>2. Cliquer sur le bouton `Exporter vers le PC`<br>3. Saisir une clé de chiffrement des secrets | |

### Sécurité des sauvegardes

| O3 | Sécurité des sauvegardes | P3 |
|---|---|---|
| *Les sauvegardes permettent de rétablir la configuration d'un équipement, la disponibilité des sauvegardes influe donc sur la disponibilité de l'équipement. Les sauvegardes contiennent également des informations sensibles telles que la configuration réseau ou les identifiants, dont la divulgation impacterait la sécurité des équipements et du réseau dans son ensemble.*<br>*Afin de garantir la confidentialité, l'intégrité et la disponibilité des sauvegardes, celles-ci doivent être stockées de façon sécurisée en conformité avec la politique de sauvegarde de l'entreprise.* | | |
| **Application** | Lors de l'export de la configuration sur un PC, il est important de choisir une clé de chiffrement des secrets présentant un niveau de sécurité suffisant (+ de 15 caractères). Lorsqu'une clé est entrée, les secrets ne pouvant être stockés hachés sont exportés chiffrés dans le fichier de configuration obtenu.<br><br>Les sauvegardes doivent être conservées et archivées uniquement sur des espaces de stockages dont la disponibilité et la confidentialité sont assurées, avec un contrôle strict sur les droits d'accès. Elles seront idéalement centralisées, et ne devraient pas être conservées en dehors d'un conteneur chiffré (Zip chiffré, Zed, etc.), sur des médias amovibles ou des appareils mobiles non chiffrés. | |

### Externalisation des sauvegardes

| O4 | Externalisation des sauvegardes | P3 |
|---|---|---|
| *En cas d'incident sur le site, les sauvegardes risquent d'être détruites en même temps que l'équipement, impactant la reconstruction ultérieure de l'équipement. Pour garantir leur disponibilité, les sauvegardes devraient être externalisées, en conformité avec les PCA/PRA.* | | |
| **Application** | Pour garantir la disponibilité des sauvegardes, il est recommandé de les externaliser, comme toute sauvegarde critique de l'infrastructure. Le site d'externalisation devra présenter les garanties nécessaires en termes de confidentialité. | |

### Restauration des sauvegardes

| O5 | Restauration des sauvegardes | P3 |
|---|---|---|
| *Pour s'assurer de l'intégrité des sauvegardes, valider et pratiquer régulièrement les procédures, la restauration des sauvegardes doit être documentée et testée a minima annuellement, en conformité avec les politiques de sauvegarde de l'entreprise.* | | |
| **Application** | Sur la page > ***Accueil*** > ***Maintenance*** > ***Gestion des configurations*** :<br><br>Restaurer une sauvegarde de configuration :<br><br>1. Choisir le nom qui sera donné à la configuration<br>2. Choisir le fichier de configuration sur le PC<br>3. Saisir la clé de déchiffrement de la configuration si nécessaire<br>4. Charger le fichier de configuration importé | |

## Journalisation

### Synchronisation temporelle

| O6 | Synchronisation temporelle | P2 |
|---|---|---|
| *Lors d'une analyse des journaux, si les équipements ne disposent pas d'une source de temps cohérente, l'horodatage des journaux risque d'être incohérent et l'analyse inexacte.*<br>*Pour uniformiser le SI et permettre une étude globale en cas de besoin, l'équipement doit être synchronisé sur un serveur de temps réputé fiable et cohérent avec les autres équipements du SI. Si la journalisation de l'équipement est exportée sur une autre machine, cette dernière doit être synchronisée avec la même source de temps.* | | |
| **Application** | Sur la page ***> Accueil > Configuration > Système > Réglage date et heure > NTP*** :<br><br>Paramètre **Synchroniser l'horloge en utilisant un serveur de temps** :<br><br>• Activer l'option<br><br>Paramètre **Serveurs NTP** :<br><br>• Lister les adresses IPs ou noms de domaine des serveurs de temps séparés par une virgule. | |

### Externalisation des journaux

| O7 | Externalisation des journaux | P2 |
|---|---|---|
| *En cas de dysfonctionnement ou d'attaque, la fiabilité des journaux sur l'équipement ne peut plus être garantie. La rétention des journaux sur l'équipement ne peut par ailleurs pas être garantie.*<br>*Pour garantir leur disponibilité et permettre une analyse globale, les journaux doivent être externalisés sur un serveur de journaux tiers.* | | |

| | |
|---|---|
| **Application** | Pour assurer la fiabilité des journaux, il convient de mettre en place un serveur de journaux tiers permettant le stockage sécurisé des journaux.<br>La configuration de l'externalisation des journaux se configure sur le routeur sur la page ***> Accueil > Configuration > Système > Syslog*** :<br><br>Paramètre **Actif** :<br><br>• Activer l'option<br><br>Paramètre **Mode de transfert** :<br><br>• Choisir `Authentification mutuelle`<br><br>Paramètre **Nom d'hôte du serveur** :<br><br>• Entrer le nom du serveur. Ce doit être le même nom qui se trouve dans le champ "Common name" du certificat du serveur syslog<br><br>Paramètre **Certificat** :<br><br>• Sélectionner le certificat du routeur |

### Analyser les journaux

| O8 | Analyser les journaux | P3 |
|---|---|---|
| *Tracer les évènements permet de mener une investigation a posteriori en cas d'incident, mais la détection d'incidents en cours nécessite une analyse proactive des journaux.*<br>*Afin de détecter les tentatives d'accès non légitimes, ou les dysfonctionnements, il est recommandé de mettre en œuvre une analyse régulière (ou temps réel) des journaux.* | | |
| **Application** | L'analyse des journaux ne peut être faite automatiquement par les équipements ETIC. Il faut prévoir une tache d'analyse manuelle des journaux, ou implémenter des contrôles sur le serveur de journaux ou sur le SIEM. | |

### Supervision par SNMP (v3)

| O9 | Supervision par SNMP (v3) | P3 |
|---|---|---|
| *Afin d'anticiper les risques liés à la disponibilité et les comportements anormaux de l'équipement, il est recommandé de superviser l'équipement par SNMP.*<br>*SNMP v1 et v2 ne sont par nature pas sécurisés, seule la communauté permettant de "restreindre" l'accès. Les versions 1 et 2 du protocole sont par ailleurs concernées par de nombreuses failles.*<br>*Si cette supervision est mise en place, la version 3 du protocole devra être utilisée. Par ailleurs, il est recommandé de ne pas utiliser la communauté par défaut "public".* | | |

| | |
|---|---|
| **Application** | La configuration du serveur SNMP sur le routeur se fait sur la page > ***Accueil*** > ***Configuration*** > ***Système*** > ***SNMP***<br>• Paramètre **Version de protocole SNMP** : `SNMP version 3`<br>• Paramètre **Algorithme d'authentification** : `SHA-256`, `SHA-384` ou `SHA-512`<br>• Paramètre **Algorithme de chiffrement** : `AES-256-CBC` |

#### Indicateurs surveillés

| O10 | Indicateurs surveillés | P3 |
|---|---|---|
| *Une surconsommation des ressources peut conduire à une indisponibilité des équipements.*<br>*Pour prévenir une indisponibilité des équipements, il est recommandé de surveiller l'occupation CPU, RAM et espace disque de l'équipement, ainsi que le nombre de connexions VPN simultanées.* | | |
| **Application** | Les indicateurs peuvent être interrogés par SNMP en utilisant les OIDs fournis dans la MIB-2 standard. | |

#### Monitoring long terme

| O11 | Monitoring long terme | P3 |
|---|---|---|
| *Selon les usages, les équipements peuvent se trouver en limite/dépassement capacitaire dans des périodes données (phases de consolidations d'informations, attaques ...)*<br>*Pour repérer les comportements anormaux des équipements, il est recommandé de mettre en place un historique des indicateurs surveillés et de suivre leur évolution dans le temps.* | | |
| **Application** | Les scénarios de surveillance devront être mis en place au niveau de la solution de supervision. | |

#### Analyse de trafic réseau avec ERSPAN

| O12 | Analyse de trafic réseau avec ERSPAN | P3 |
|---|---|---|
| *Analyser le trafic réseau est une mesure de sécurité préventive, elle permet de dépanner le réseau, de détecter des anomalies ou du trafic malveillant.*<br>*Le port mirroring avec ERSPAN est une technique pour analyser le réseau, celle-ci permet d'envoyer une copie du trafic monitoré à un équipement distant qui pourra analyser les paquets.* | | |
| **Application** | Un serveur devra être mis en place pour recevoir le trafic mirroré et gérer l'analyse de paquets.<br>La configuration du mirroring ERSPAN sur le routeur se fait sur la page ***Configuration*** > ***Réseau*** > ***ERSPAN***. | |

## Authentification

#### Politique de mot de passe

| O13 | Politique de mot de passe | P2 |
|---|---|---|

| |
|---|
| *La compromission de mot de passe utilisateur peut conduire à un accès illégitime au SI. Un mot de passe trop simple pourra être facilement trouvé lors d'une attaque de type brute force, par dictionnaire ou cassage de hash.*<br>*Afin de se prémunir contre une telle attaque, il est important de définir une politique de mot de passe au niveau organisationnel conformément au document (ANSSI-PG-078).* |
| **Application** : Définir une politique de mot de passe au niveau de l'organisation. Nous recommandons des mots de passes qui contiennent :<br>• 16 caractères minimum<br>• Au moins une majuscule, une minuscule et un chiffre<br>• Au moins un caractère spécial `&$%[]{}=?!-_*+~#@` |

### Utiliser un système d'authentification centralisé

| O14 | Utiliser un système d'authentification centralisé | P2 |
|---|---|---|
| *Lorsqu'on a une flotte de routeur, la gestion des listes d'utilisateurs locale sur les routeurs devient vite fastidieuse à gérer. Le maintien d'une même liste d'utilisateurs dupliquée sur plusieurs routeurs peut mener à des erreurs et des oublis sur un des routeurs.*<br>*Pour éviter ces problèmes de sécurité, il convient de gérer la flotte de routeurs de manière centralisée.* | | |
| **Application** | Un serveur d'authentification centralisée de type Active directory ou autre serveur LDAP devra être mis en place pour gérer l'authentification des utilisateurs sur la flotte.<br>La configuration de la délégation d'authentification se fait sur la page > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Authentification***. | |

### Désactiver la mise en cache LDAP

| O15 | Désactiver la mise en cache LDAP | P1 |
|---|---|---|
| *Le système d'authentification centralisé permet la mise en cache des identifiants d'authentification pendant une durée configurable. Si un compte venait à être bloqué, changeait de groupe, ou voyait son mot de passe changé, l'authentification, avec les anciens identifiants, serait toujours possible durant le temps de mise en cache si le serveur n'est pas joignable.*<br>*Pour éviter d'autoriser une demande d'accès qui aurait été désactivée sur le serveur LDAP, il convient de désactiver la mise en cache des identifiants.*<br>*Attention, en cas d'absence de communication entre le routeur et l'annuaire centralisé, l'authentification ne sera plus possible.* | | |
| **Application** | Sur la page > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Authentification*** :<br><br>Décocher le paramètre **Mettre en cache les identifiants** | |

### Utiliser LDAPS uniquement

| O16 | Utiliser LDAPS uniquement | P1 |
|---|---|---|

| | |
|---|---|
| *Les protocoles RADIUS et TACACS+ ne présentent pas un niveau de sécurité suffisant. Par ailleurs, il présente certaines limitations puisqu'il ne permet pas de définir des rôles pour les administrateurs. Afin d'améliorer la sécurité du système d'authentification centralisé, il est nécessaire d'utiliser le protocole sécurisé et chiffré LDAPs.* | |
| **Application** | Sur la page > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Authentification*** :<br>• **Type d'authentification** : `LDAP`<br>• Cocher le paramètre **LDAP sur TLS** |

### Activer la protection de l'authentification

| O17 | Activer la protection de l'authentification | P1 |
|---|---|---|
| *L'attaque par force brute est une méthode consistant à essayer toutes les combinaisons de mot de passe possibles afin de trouver les identifiants d'un utilisateur, et ainsi usurper son identité et accéder à une augmentation de privilèges.*<br>*Afin d'améliorer la sécurité du système d'authentification, il est nécessaire de protéger l'authentification des attaques par force brute.* | | |
| **Application** | Sur la page > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Authentification***, dans la section 'Protection de l'authentification' :<br>• Cocher le paramètre **Actif** | |

### Avertissement à l'authentification

| O18 | Avertissement à l'authentification | P3 |
|---|---|---|
| *L'affichage d'un message de notification d'utilisation du système avant de procéder à l'authentification est un élément de dissuasion pour toute personne voulant s'introduire illégalement dans le produit.*<br>*Cela permet la poursuite pénale des contrevenants et la démonstration d'une violation intentionnelle.* | | |
| **Application** | Sur la page > ***Accueil*** > ***Configuration*** > ***Sécurité*** > ***Authentification***, dans la section 'Avertissement à l'authentification', renseigner un message à afficher sur toutes les interfaces d'authentification dans le paramètre **Message d'avertissement avant l'authentification** | |

# 4. SUIVI DES RECOMMANDATIONS

| | | |
|---|---|---|
| **A1**: Activer l'authentification | **P1** | |
| **A2**: Protocole HTTPs | **P1** | |
| **A3**: Désactiver l'accès à l'administration par M2Me | **P1** | |
| **A4**: Désactiver l'accès à l'administration par le WAN | **P1** | |
| **A5**: Désactiver le serveur SSH | **P1** | |
| **A6**: Gestion des accès | **P1** | |
| **A7**: Désactiver retour configuration usine temporaire | **P1** | |
| **A8**: Configuration de l'accès hotline | **P2** | |
| **A9**: Désactiver accès distant par bouton poussoir | **P2** | |
| **O1**: Maintien à jour de l'équipement | **P1** | |
| **O2**: Sauvegardes régulières de la configuration | **P3** | |
| **O3**: Sécurité des sauvegardes | **P3** | |
| **O4**: Externalisation des sauvegardes | **P3** | |
| **O5**: Restauration des sauvegardes | **P3** | |
| **O6**: Synchronisation temporelle | **P2** | |
| **O7**: Externalisation des journaux | **P2** | |
| **O8**: Analyser les journaux | **P3** | |
| **O9**: Supervision par SNMP (v3) | **P3** | |
| **O10**: Indicateurs surveillés | **P3** | |
| **O11**: Monitoring long terme | **P3** | |
| **O12**: Analyse de trafic réseau avec ERSPAN | **P3** | |
| **O13**: Politique de mot de passe | **P2** | |
| **O14**: Utiliser un système d'authentification centralisé | **P2** | |
| **O15**: Désactiver la mise en cache LDAP | **P1** | |
| **O16**: Utiliser LDAPS uniquement | **P1** | |
| **O17**: Activer la protection de l'authentification | **P1** | |
| **R1**: Configurer le DNS manuellement | **P2** | |
| **R2**: Désactiver le serveur DHCP | **P1** | |
| **R3**: Désactiver le serveur d'application | **P1** | |
| **R4**: Désactiver l'agent SNMP | **P1** | |
| **R5**: Désactiver le serveur NTP | **P1** | |
| **R6**: Désactiver EticFinder | **P1** | |

| | | |
|---|---|---|
| **R7**: Désactiver le portail WEB | **P1** | |
| **R8**: Désactiver M2Me_Connect | **P1** | |
| **R9**: Désactiver le serveur Modbus TCP | **P1** | |
| **R10**: Désactiver le serveur OPC-UA | **P1** | |
| **R11**: Bloquer les ports non utilisés | **P3** | |
| **R12**: Désactiver les interfaces non utilisées | **P3** | |
| **R13**: Blocage des flux entrants WAN vers LAN | **P1** | |
| **R14**: Blocage des flux sortants LAN vers WAN | **P1** | |
| **R15**: Blocage des flux entrants VPN vers LAN | **P1** | |
| **R16**: Blocage des flux sortants LAN vers VPN | **P1** | |
| **R17**: Activer le filtre anti Déni de Service | **P1** | |
| **R18**: Désactiver les conntrack helpers | **P1** | |
| **R19**: Usage d'une PKI de confiance | **P1** | |
| **R20**: Certificats des équipements | **P1** | |
| **R21**: Révocation des certificats | **P1** | |
| **U1**: Identifiants des utilisateurs | **P1** | |
| **U2**: Construction du mot de passe | **P1** | |
| **V1**: Utilisation des certificats | **P1** | |
| **V2**: Algorithmes de chiffrement et d'authentification | **P1** | |
| **V3**: Interdire le trafic entre VPN | **P1** | |
| **V4**: OpenVPN : Gestion de l'authentification | **P1** | |
| **V5**: OpenVPN : Choix du Diffie-Hellman | **P1** | |
| **V6**: OpenVPN : Utilisation de tls-crypt v2 | **P1** | |
| **V7**: OpenVPN : Désactiver la compression LZO | **P1** | |
| **V8**: IPsec : Gestion de l'authentification | **P1** | |
| **V9**: IPsec : Groupe Diffie-Hellman | **P1** | |
| **V10**: Désactiver PPTP | **P1** | |
| **V11**: Désactiver L2TP/IPSec | **P1** | |
| **V12**: Certificats utilisateurs | **P1** | |
| **V13**: Authentification deux facteurs | **P1** | |
| **V14**: Algorithmes de chiffrement et d'authentification | **P1** | |
| **V15**: Une seule connexion distante à la fois | **P1** | |
| **V16**: Désactiver la compression LZO | **P1** | |

# 5. MISE AU REBUT

La procédure de mise au rebut permet de remettre le produit dans sa configuration usine initiale, ainsi que de supprimer toutes les données utilisateurs du produit (secrets, mots de passe, configurations, certificats, clés privées, ...).

| | |
|---|---|
| **NOTE** | Ces données sont perdues et ne peuvent pas être récupérées à l'aide de logiciels d'exploration de données. |

Sur la façade arrière du produit se trouve un trou pour appuyer sur un bouton, procurez-vous une tige afin de pouvoir appuyer sur ce bouton.

## 5.1. Déroulement de la procédure

1. Éteindre le produit
2. Appuyer sur le bouton arrière
3. Alimenter le produit tout en appuyant sur le bouton face arrière pendant 30 à 40 secondes
4. La LED  va clignoter en rouge/vert
5. Le produit reprendra sa configuration usine, tout en supprimant toutes les données utilisateur