
 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 1 sur 10

Table des matières

1	Remarques générales	2
1.1	Objectif	2
1.2	Application	2
1.3	Limitations	2
1.4	Principes	2
1.5	Termes et sigles	3
1.5.1	Réseaux	3
1.5.2	Passerelles réseau	3
1.5.3	Sigles	4
2	Concept	5
2.1	Architecture	5
3	Exigences générales	6
3.1	Services	6
3.2	Matériel informatique	8
4	Exigences spécifiques	8
4.1	Accès de télémaintenance	9
4.2	VDV	9
4.3	Réseau IP EES Backbone de la confédération (zone de migration backbone)	9
4.4	Agrégats	9
5	Annexe	10
5.1	Normes et prescriptions	10

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 2 sur 10

1 Remarques générales

1.1 Objectif

La présente fiche technique contient les consignes techniques de l'OFROU concernant le matériel informatique et les logiciels pare-feu des réseaux IP existants des unités territoriales (réseaux IP des UT).

La fiche technique définit un standard minimal à respecter pour tous les réseaux IP de l'UT. Elle met en application les prescriptions générales de la directive 13030 Sécurité IT des systèmes de gestion et de commande des EES.

Les pare-feu des unités territoriales forment un élément important du concept « Defense in Depth » selon la norme IEC 62443. Ils ont pour objectif de réduire le risque pour la sécurité.

1.2 Application

La présente fiche technique doit être utilisée :

- lors de la planification, l'étude de projet, la réalisation et l'exploitation de pare-feu
- lors d'adaptations et d'extensions des réseaux IP des UT
- pour les passerelles réseaux supplémentaires et les adaptations réalisées sur des passerelles réseaux existantes

Cette fiche technique doit être utilisée par les unités territoriales, les planificateurs et les entrepreneurs.

Elle doit également être appliquée en cas d'installations nouvelles et existantes, indépendamment des directives selon lesquelles les EES sont ou ont été construits.

La fiche technique doit être appliquée également pour les nouvelles installations qui n'ont pas été autorisées sur la présente base. La directive 13030 Sécurité IT des systèmes de gestion et de commande des EES sur laquelle repose la présente fiche technique et qui définit les exigences de protection est en vigueur depuis 2016.

1.3 Limitations

La présente fiche technique contient uniquement des directives qui sont à appliquer aux infrastructures de réseau existantes.

En ce qui concerne la migration en cours des réseaux IP des UT vers les réseaux IP EES UT, la transition entre les deux réseaux peut être fluide. Il n'est possible de déroger à la présente fiche technique que si d'autres exigences prescrivant le même niveau ou un niveau supérieur de sécurité sont appliquées.


Elle n'est pas à appliquer aux exigences futures liées aux réseaux IP EES UT. Une fiche technique séparée sera établie à cet effet.

La transition réseau vers le backbone de la Confédération n'est pas traitée dans la présente fiche technique, mais dans une fiche technique à part.

1.4 Principes

La présente fiche technique repose sur les bases suivantes :

- Stratégie nationale de protection de la Suisse contre les cyberrisques, (SNPC) 2018-2022 Unité de pilotage informatique de la Confédération (UPIC), avril 2018
- Mesures de protection pour les systèmes de contrôle industriels (SCI), Melani, avril 2013
- Directive OFROU 13030 Sécurité IT des systèmes de gestion et de commande des équipements d'exploitation et de sécurité, édition 2016, version 1.21

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 3 sur 10

- « Norme minimale pour améliorer la résilience informatique », Office fédéral pour l'approvisionnement économique du pays OFAE, Berne 2018

1.5 Termes et sigles

1.5.1 Réseaux

Réseau IP des UT : les réseaux existants et actuellement en fonction sont appelés réseaux IP des UT. Ils ont été établis selon les directives des cantons, des unités territoriales ou de fiches techniques OFROU qui ne sont actuellement plus en vigueur.

Réseau IP EES : les nouveaux réseaux établis selon les directives de l'OFROU, notamment la directive 13040, sont désignés sous le terme de réseau IP EES. Le réseau IP EES est sous-divisé en un réseau IP EES backbone de la Confédération, un réseau IP EES xy (UT), un réseau IP EES VMZ-CH (VMZ) et un réseau IP EES services de base (BD). La présente fiche technique ne traite pas de ces réseaux.

Autres réseaux : on entend sous « Autres réseaux » des réseaux qui ne font partie ni des réseaux IP des UT ni des réseaux IP des EES (backbone Confédération / UT / VMZ / BD). Il s'agit, par exemple, des réseaux administratifs des cantons, des réseaux opérationnels des services d'urgence, etc., qui ne sont ni la propriété ni sous la responsabilité de l'OFROU.

1.5.2 Passerelles réseau


Backbone Confédération : la dorsale n'est pas traitée dans le présent document (voir également VDV).

Connexion Internet : accès à la connexion de services basés sur Internet. Les applications suivantes (énumération non exhaustive) utilisent des connexions Internet :

- téléphonie IP (appels d'urgence VoIP)
- mises à jour (antivirus/malware, systèmes d'exploitation, micrologiciel, mises à jour OS, mises à jour gén., etc.)
- connexions redondantes pour les installations de sécurité (TUSnet)
- publication d'images vidéo pour les pages de projet de l'OFROU, etc.
- services météo (par ex. MétéoSuisse)
- données de trafic
- notification de statut (avis de dysfonctionnement / commande de pièces de rechange, en particulier serveur)
- accès de télémaintenance

Accès à une connexion mobile : en font partie tous les agrégats / modems / routeurs, etc. qui sont reliés au réseau de l'unité territoriale par une connexion mobile. Il s'agit par exemple de caméras, de systèmes de détection précoce du verglas, de postes de comptage du trafic, etc. Ne sont pas visés les agrégats non sollicités directement via les réseaux IP des UT et qui ne terminent donc pas dans les réseaux IP des UT (par ex. les postes de comptage du trafic directement connectés à l'OFROU Ittigen / à des tiers et qui communiquent via BIT M2M).

Connexion

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 4 sur 10

cantons/communes : en font partie les passerelles vers les réseaux des autorités cantonales et communales ainsi que les services d'urgence, par ex. pour les images vidéo, les données de trafic, les installations de signaux lumineux, les appels d'urgence


Connexion de télémaintenance : accès à distance pour le personnel d'exploitation et les entreprises autorisées à effectuer la maintenance et à supprimer les dérangements.

VDV Centre de données sur les transports (VerkehrsDatenVerbund). Cette connexion est intégrée à la connexion backbone Confédération. La passerelle réseau est utilisée par exemple pour mettre à disposition des images vidéo, des données de trafic, des accès aux systèmes de gestion pour d'autres UT, la VMZ-CH ou des tiers.

UT-UT Passerelle entre les deux réseaux IP des unités territoriales

1.5.3 Sigles

FTP	File Transfer Protocol
GS-X	Mesure de protection de base X de la directive 13030
HTTPS	Hypertext Transfer Protocol Secure
M2M	Service Machine-to-Machine
NDR	Network Device Requirements
NT	Téléphonie d'urgence
OT	Operational Technology
SIP	Session Initiation Protocol
TUS	Communauté d'intérêts Télécommunication et Sécurité (Securiton, Siemens)
VDV	Centre de données sur les transports
VPN	Virtual Private Network
TVT	Observation à distance du trafic
WAN	Wide Area Network

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 5 sur 10

2 Concept

2.1 Architecture

Toutes les connexions qui partent du réseau IP des UT vers un autre réseau doivent passer par un pare-feu. Ces passerelles réseau doivent être surveillées et gérées par l'unité territoriale. Les autres accès ne sont pas autorisés.

Toutes les passerelles réseau, y compris les connexions de transit, par exemple via le réseau mobile ou d'autres UT, doivent être représentées de manière claire dans un graphique (Layer 4 document) avec la technologie et les services. Dans ce contexte, voir la figure suivante (exemple).

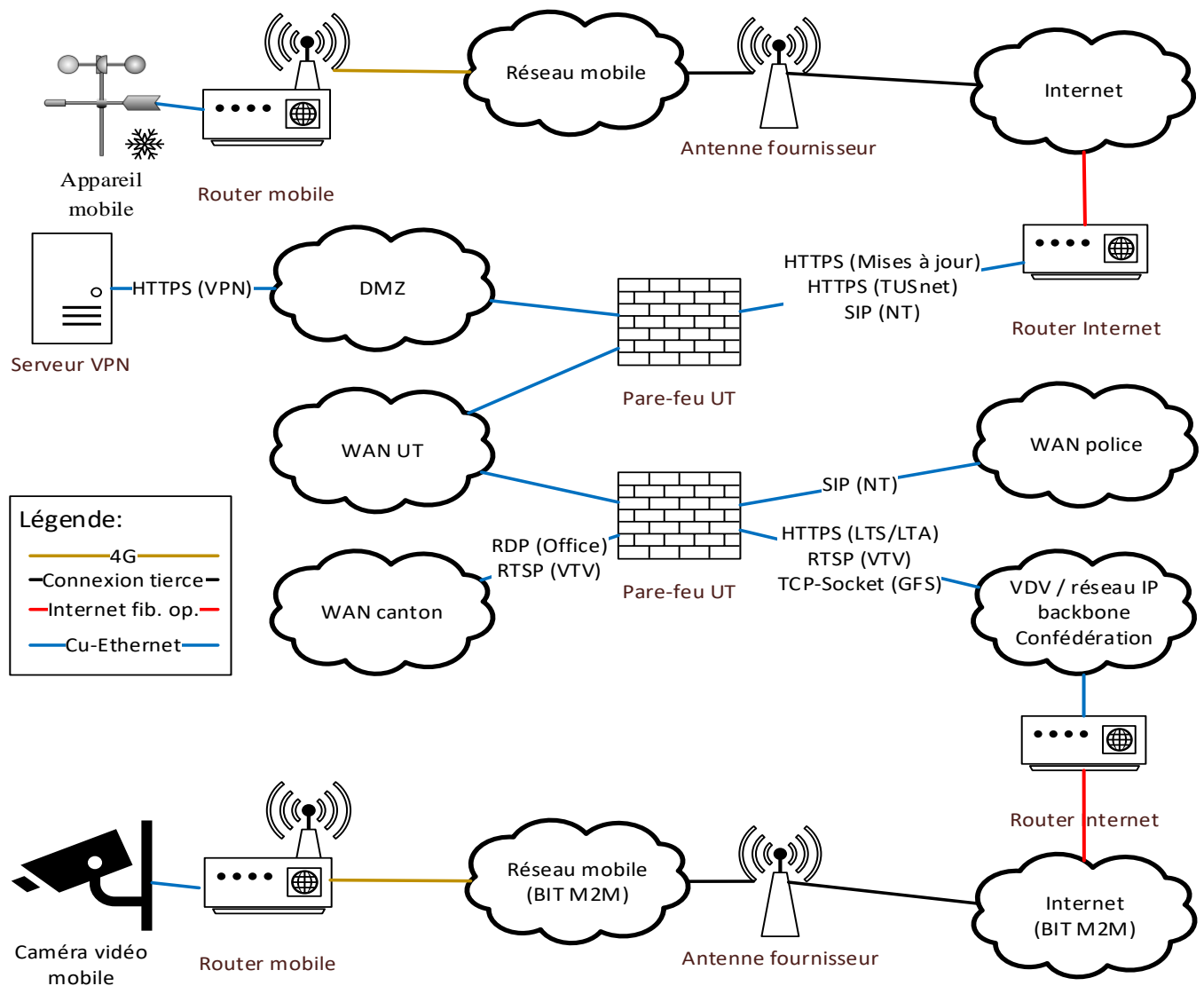



Figure 1 : exemple d'architecture

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 6 sur 10

Les connexions via Internet doivent être réduites au minimum. Dans la mesure du possible, il convient de mettre en place des solutions sans connexions directes au réseau IP des UT, par exemple pour la consultation d'images vidéo ou de données du trafic.

Un inventaire des passerelles réseau doit être établi pour chaque réseau IP des UT. Il faut documenter les mesures de protection de chaque passerelle.

3 Exigences générales

3.1 Services

La réalisation prévoit différentes solutions (voir FiFigure 2 et Figure 3.

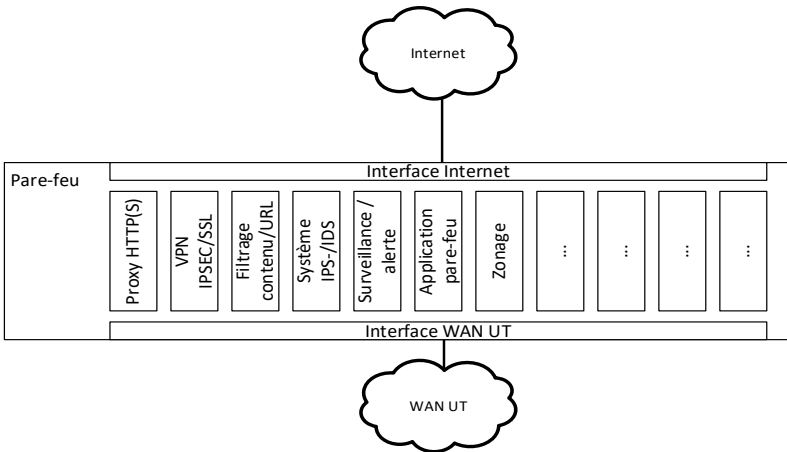


Figure 2 : Exemple de solution tout-en-un

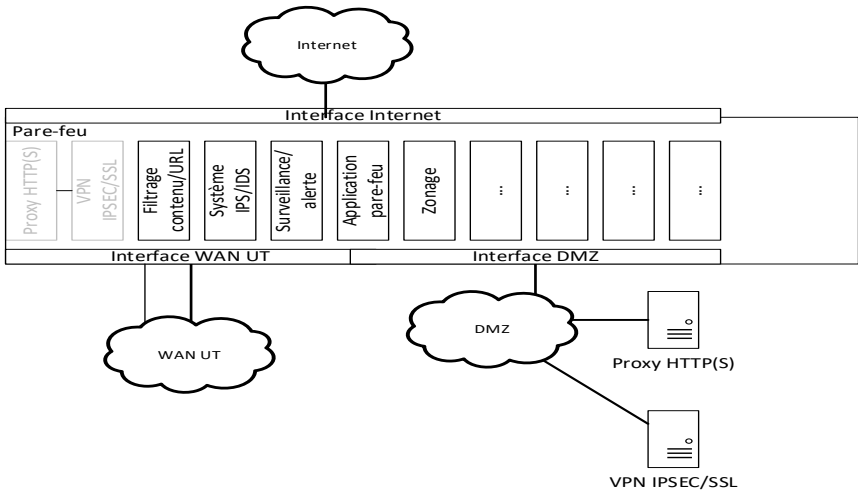




Figure 3 : Exemple de solution services dédiés

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 7 sur 10

Les présentes exigences minimales doivent être remplies. Ci-après la fonctionnalité ¹⁾ des pare-feu :

- ALG :** l'application-Level Gateway (ALG) contrôle les accès aux services qui utilisent des ports dynamiques au lieu des ports statiques (par exemple FTP et SIP) et connaît l'état (statefull) de chaque communication de données.
- Filtre de paquets :** toutes les données sont contrôlées à travers un filtre de paquets. Les communications de données sont soumises à des règles qui n'autorisent que ce qui est nécessaire et rejettent les paquets non conformes, quel que soit leur état (stateless). Ces règles doivent être définies dans le concept de sécurité IT/OT.
- Protection contre les virus :** la protection contre les virus contrôle les données entrantes et sortantes à la recherche de virus et de malware.
- Filtre URL / contenu :** Ce filtre vérifie les URL appelées et leur contenu. Il est ainsi possible d'interdire l'accès à certaines URL (filtre URL). Il est, par exemple, possible d'autoriser l'accès à une application web via VPN, mais de refuser l'accès au site web administrateur du même ordinateur. De même, le contenu (filtre de contenu) peut être limité à certaines images/configurations d'images, par exemple.
- Monitoring :** l'ensemble du trafic doit pouvoir être journalisé et enregistré.
- Journalisation :** toutes les modifications de configuration doivent être journalisées.
- Reporting :** toutes les informations collectées à partir du monitoring ou de la journalisation doivent pouvoir être évaluées automatiquement au moyen de rapports séparés. De même, ces rapports doivent pouvoir être distribués automatiquement par classement ou par e-mail.
- Connexion :** une connexion au pare-feu peut uniquement être effectuée depuis l'interface réseau interne, de préférence depuis un réseau de gestion dédié. Il faut faire cesser toute connexion directe via une interface réseau externe (par ex. Internet, réseaux cantonaux).
- Gestion des utilisateurs :** les utilisateurs personnels employés sur le pare-feu doivent être gérés par la gestion centralisée des utilisateurs. Les utilisateurs locaux ne sont autorisés que comme solution de repli ou pour la configuration initiale.
- IPS / IDS :** les systèmes de prévention des intrusions / systèmes de détection des intrusions sont des systèmes qui peuvent détecter (IDS) ou empêcher (IPS) des irrégularités, par exemple dans les activités du réseau. Dans le sens d'une protection avancée contre les maliciels.
- Proxy :** pour le forwarding / reverse proxy, il faut par exemple utiliser ftp, http(s) et smtp. Pour d'autres services, dans la mesure où cela est d'usage.
- Protection contre les maliciels :** une protection contre les virus et les maliciels est à activer sur le pare-feu. Celle-ci complète les mesures de prévention des maliciels mises en place sur les clients et offre, en plus de l'antivirus, une protection contre les botnets, contre les IP/domaines compromettants et contre la propagation locale via le réseau.
- Filtre botnet :** des mesures appropriées doivent être prises pour empêcher les botnets.
- Filtre Géo-IP :** son accès doit être limité. Les accès doivent être définis dans le concept de sécurité IT/OT selon 26010- 04002.
- Sauvegarde des données :** le pare-feu doit supporter une sauvegarde automatique et périodique des logs et des configurations sur une mémoire externe.

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 8 sur 10

Redondance : si une connexion redondante à d'autres réseaux est réalisée, elle doit être exécutée en tant que cluster.

Journal d'audit : toutes les connexions au pare-feu doivent être, en outre, transmises à un journal de serveur externe.

1) Pour une meilleure compréhension, il est possible d'utiliser le guide « Integration und IT-Revision von Netzwerkübergängen » de l'Office fédéral pour la sécurité en matière de technologies de l'information (BSI, Allemagne), Bonn 2006, version 1.0 (chapitre 2« Integration und IT-Revision von Netzwerkübergängen »).

3.2 Matériel informatique

Le matériel doit répondre aux exigences suivantes :

- il faut utiliser des produits actuels et éprouvés, pour lesquels le fournisseur doit justifier de références obtenues dans un environnement et pour une taille comparables.
- Il n'est pas admissible d'installer des équipements sur des sites qui n'ont pas été explicitement définis par les UT. En particulier, tous les composants nécessaires à l'exploitation doivent être installés exclusivement sur les sites des UT.
- Les équipements doivent pouvoir être montés directement dans un rack 19" (482,6 mm) avec accès frontal couramment commercialisé.
- Les équipements doivent être construits conformément à une norme. Tous les équipements doivent respecter les normes légales (p. ex. NIBT, OIBT, prescriptions cantonales, etc.) en matière de sécurité physique et de protection des personnes.
- Extensible de manière modulaire, avec un système de logement et de marquage distinctif
- Durée de fonctionnement : fonctionnement continu 24 heures sur 24
- Disponibilité des pare-feu / redondance
- Disponibilité du produit : > 5 ans (End-of-Support)
- Durée de vie : > 6 ans
- Conditions ambiantes : zone 30 (conformément à la fiche technique 23 001-12210)
- Type de protection : IP 20
- Tension : 230 VAC, $\pm 10\%$
- Fréquence : 50 Hz, $\pm 5\%$
- Bloc d'alimentation : redondant avec surveillance


La capacité du pare-feu dépend de la taille du réseau et du trafic de données. Il faut qu'elle soit déterminée en fonction de l'objet.

Le matériel doit satisfaire aux homologations et normes suivantes :

- CE (marque de conformité)
- SN EN 61000 (compatibilité CEM)
- SN EN 55022(caractéristiques des perturbations radioélectriques)
- IEC 62443 (sécurité informatique, principalement exigences NDR conformément à la norme IEC 62443-4-2) ou adéquate

4 Exigences spécifiques

Les chapitres suivants traitent des exigences spécifiques aux différentes catégories de passerelles réseau. Les besoins de protection des différentes catégories de passerelles réseau peuvent varier en fonction des données transmises et du niveau de protection des réseaux connectés. Les différentes catégories de passerelles réseau peuvent être protégées par le même pare-feu.

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 9 sur 10

4.1 Accès de télémaintenance

La directive OFROU 13030 Sécurité informatique des systèmes de commande et de gestion des équipements d'exploitation et de sécurité règle l'accès. Un accès de télémaintenance doit garantir l'intégrité et la confidentialité des données ainsi que l'authentification des partenaires de communication. Un accès de télémaintenance doit répondre aux exigences de la norme IEC62443-3-3 SR 2.6.

L'accès via Internet au réseau interne de l'unité territoriale peut se faire uniquement par VPN (VPN SSL ou IPSec). Une authentification personnelle à deux facteurs doit être mise en place.

L'accès doit toujours être réduit au strict nécessaire (privilège minimal) et être limité dans le temps. Les directives correspondantes doivent être définies dans le concept de sécurité IT/OT.

4.2 VDV

Cette passerelle réseau est intégrée en liaison avec le backbone de la confédération.

4.3 Réseau IP EES Backbone de la confédération (zone de migration backbone)

Cette passerelle réseau doit désormais déjà être mise en place afin d'assurer la transition vers le nouveau backbone national. Une fois la migration VDV terminée, tout le trafic de l'ancienne passerelle réseau VDV passera par ce point (jusqu'au moment de la migration du réseau IP EES dans toute la Suisse).


4.4 Agrégats

Ce chapitre couvre tous les équipements pouvant être mis en réseau, tels que les caméras, les capteurs, les dispositifs de communication, etc. Ils doivent faire l'objet de mesures de protection appropriées contre les attaques informatiques.

Les agrégats connectés sans fil doivent passer par un pare-feu. Le trafic de données doit être crypté de manière appropriée (VPN IPSec/SSL, protocoles sécurisés, etc.).

La connexion ne doit se faire qu'avec une unité d'évaluation / commande dédiée, par exemple par communication M2M. Les connexions à Internet ne sont pas admises.

L'exigence GS-3 de la directive 13030 s'applique.

 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Manuel technique EES (équipements d'exploitation et de sécurité) Fiche technique composants Communication & systèmes de gestion	23 001-11615
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC Office fédéral des routes OFROU	Pare-feu (réseaux existants)	V1.01 01.01.2023
Division Infrastructure routière I		Page 10 sur 10

5 Annexe

5.1 Normes et prescriptions

Il faut particulièrement veiller aux normes et prescriptions suivantes lors de l'étude et de l'exécution :

- OFROU 13030 Sécurité IT des systèmes de gestion et de commande des équipements d'exploitation et de sécurité ; édition 2016 version 1.21
- IEC 62443 Industrial communication networks – Network and system security
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements