

Plan d'adressage réseau

Une adresse IP permet d'identifier chaque hôte connecté à un réseau informatique utilisant le protocole IP. Un ordinateur, une imprimante, un smartphone, un routeur, etc... tout périphérique connecté à un réseau et qui veut communiquer avec les autres hôtes du réseau doit disposer d'une adresse IP.

Les adresses IP privées ne peuvent pas être utilisées sur internet car elles ne peuvent pas être routées sur internet. Les hôtes qui les utilisent sont donc visibles uniquement dans le réseau local. Pour ces raisons, ces adresses seront à privilégier pour les S2I :

- Les adresses privées de la classe A : **10.0.0.0 à 10.255.255.255**
- Les adresses privées de la classe B : **172.16.0.0 à 172.31.255.255**
- Les adresses privées de la classe C : **192.168.0.0 à 192.168.255.255**

Routeurs et WI-FI

Les routeurs et les éléments actifs du réseau sont des composants clés de l'infrastructure réseau, et leur configuration incorrecte peut entraîner des vulnérabilités de sécurité qui peuvent être exploitées par des attaquants pour accéder au réseau et compromettre la sécurité des systèmes informatiques.

La mise en place de mesures de configuration des routeurs ou des éléments actifs d'un réseau est essentielle pour assurer la sécurisation du système dans son ensemble.

Mesures de sécurisation du routeur :

- mettre à jour le routeur avec le dernier micro-logiciel recommandé par le fournisseur :
 - o lors de la mise en place ;
 - o lors de la MCS ;
 - o lors d'une vulnérabilité critique ;
 - créer des comptes nominatifs ou fonctionnels avec des privilèges limités en fonction des responsabilités de la ou des personne(s) ;
 - désactiver ou renommer tous les comptes par défaut ;
 - désactiver les interfaces réseau non utilisées ;
 - désactiver tous les services non utilisés ;
 - désactiver le WPS ;
 - désactiver l'IPv6 ;
 - ne pas utiliser les plages d'adresses IP par défaut (exemple : 192.168.1.0/24) ;
 - utiliser le HTTPS pour l'interface d'administration du routeur et désactiver l'interface une fois le routeur configuré ;
 - dédier une interface physique à son administration ;
 - conserver une sauvegarde sécurisée de la configuration du routeur en cas de panne ;
 - utiliser les services IPS/IDS pour une meilleure protection, journalisation et gestion des alertes.
- Pour la journalisation, garder les journaux pendant maximum 1 ans.

Mesures de sécurisation du WI-FI:

- désactiver le wifi s'il n'est pas utilisé. Si celui-ci est utilisé¹, le mot de passe par défaut doit être modifié par un mot de passe fort, utiliser le WPA3 et changer le SSID par défaut :
 - o longueur minimale des mots de passe de 14 caractères ;
 - o complexité des mots de passe avec l'utilisation de 3 types de caractères différents majuscules, minuscules, chiffres et caractères spéciaux ;
- désactiver l'accès à l'interface d'administration du routeur du réseau Wi-Fi (Accès seulement en filaire) ;
- s'assurer de la couverture d'un réseau Wi-Fi limitée au besoin :
 - o l'usage d'antennes directionnelles ou le réglage de la puissance des antennes permettent de contrôler la zone de couverture.

Pare-feu

Un pare-feu est un élément clé de la sécurité réseau qui permet de protéger les systèmes et les réseaux contre les menaces de sécurité venant de l'extérieur et notamment d'internet telles que les attaques par déni de service, les intrusions et les logiciels malveillants. Cependant, pour qu'un pare-feu soit efficace, il doit être correctement configuré en fonction des besoins spécifiques des systèmes qu'il protège.

Mesures de sécurisation du pare-feu (Matériel) :

- mettre à jour le pare-feu avec le dernier micro-logiciel recommandé par le fournisseur (Système → Active Update) :
 - o Lors de la mise en place ;
 - o Lors de la MCS ;
 - o Lors d'une vulnérabilité critique ;
- créer des comptes nominatifs ou fonctionnels avec des privilèges limités en fonction des responsabilités de là ou des personne(s) ;
- créer des mots de passe complexes et sécurisés ;
- désactiver ou renommer tous les comptes par défaut
- désactiver les interfaces d'administration de pare-feu de l'accès extérieur et public. (Système → Configuration → Administration du Firewall) ;
- dédier une interface Ethernet à l'administration ;
- désactiver l'interface WEB d'administration. Elle peut être réactivée uniquement pendant la configuration et modifications du pare-feu ;
- compléter les règles d'antispoofing ;
- désactiver les interfaces réseau non utilisées (Réseau → Interfaces) ;
- synchroniser au serveur NTP existant, s'il n'y a pas de serveur NTP configuré, utiliser celui du pare-feu qui lui sera synchronisé au serveur NTP sur internet :
 - o Serveur : 0.fr.pool.ntp.org
 - o Serveur : 1.fr.pool.ntp.org
 - o Serveur : 2.fr.pool.ntp.org
 - o Serveur : 3.fr.pool.ntp.org
- modifier le certificat par défaut de l'interface web d'administration en utilisant l'IGC du pare-feu comme StormShield ou autre si existant ;

¹ L'utilisation est assujettie à une autorisation de la personne publique.

- utiliser les certificats pour la connexion au VPN géré par l'IGC (les certificats par défaut sont interdits. Utiliser des certificats auto signés par l'éditeur du VPN);
- utiliser SNMPv3 si besoin de supervision à distance du pare-feu.

Les zones de pare-feu (Matériel) :

- isoler dans un réseau dédiée les équipements qui ont un service exposé sur le réseau extérieur (DMZ).

Les règles de pare-feu :

- désactiver les règles implicites par défaut ;
- ajouter une règle explicite qui bloque tout le trafic entrant et sortant de chaque interface, puis autoriser les flux souhaités ;
- les règles de pare-feu doivent être rendues aussi spécifiques que possible aux adresses IP source et/ou de destination et aux numéros de port exacts chaque fois que possible ;
- faire des tests de ce qui ne devrait pas être autorisé et vérifier que les services autorisés fonctionnent correctement.

Autres services de pare-feu (Matériel et logiciel) :

- utiliser les services IPS/IDS pour une meilleure protection, journalisation et gestion des alertes. Pour la journalisation, garder les journaux pendant maximum 1 ans ;
- certains pare-feu proposent des services supplémentaires comme DHCP, DNS, etc. Désactiver tous les services que vous n'avez pas l'intention d'utiliser.

Autres (Matériel et logiciel) :

- conserver une sauvegarde sécurisée de la configuration du pare-feu en cas de panne ;
- maintenir le micro-logiciel / logiciel à jour avec des tests de non régression (Effectuer une sauvegarde avant la mise à jour).

Commutateur (switch)

Les commutateurs sont des équipements de transit pour une quantité importante d'informations. Il convient donc de porter une attention particulière à leur niveau de robustesse face à des attaques venant du réseau.

- dédier une interface physique du commutateur à son administration ;
- mettre en place une séparation physique ou un cloisonnement logique utilisant des VLAN pour appliquer cette séparation entre les réseaux d'administration et les réseaux métier ;
- ne pas désactiver le port console des commutateurs ;
- utiliser le protocole SSH en version 2 pour l'administration à distance des commutateurs ;
- désactiver le serveur web de gestion du commutateur, que ce soit en version sécurisée (HTTPS) ou non (HTTP) ;
- supprimer les certificats créés par défaut sur le commutateur ;
- ne pas utiliser le protocole Telnet pour l'administration à distance des commutateurs lorsque des protocoles plus sécurisés sont supportés par l'équipement. Si Telnet doit être utilisé du fait de l'absence de protocoles sécurisés, mettre en place les moyens adéquats de sécurisation du réseau sur lequel vont transiter ces flux ;
- un commutateur ne doit disposer que d'une seule adresse IP dédiée à son administration ;

- prendre les mesures nécessaires au sein du SI afin de n'autoriser l'accès à l'interface d'administration des commutateurs qu'aux administrateurs, notamment par l'utilisation de filtrage au niveau des pare-feu. Si cela n'est pas possible, la mise en place des ACL sur le commutateur peut être envisagée en tant que mesure palliative ;
- activer la journalisation des authentifications et tentatives d'authentification ;
- mettre en place des contre-mesures pour protéger le commutateur des attaques de type brute force. (Exemple commande CISCO : login block - for 300 attempts 3 within 120 / login delay 2) ;
- protéger les fichiers de configuration contenant des mots de passe, ceux-ci étant soit stockés en clair, soit retrouvables facilement par une personne malveillante. Supprimer les mots de passe des fichiers de configuration en cas de partage de ces fichiers avec d'autres personnes ou entités ;
- supprimer les comptes par défaut - au minimum, les désactiver - tout en veillant à conserver au moins un compte administrateur local « de secours » ;
- la politique de sécurité des mots de passe des comptes utilisateurs doit respecter la PSSI en vigueur ;
- désactiver les services de configuration automatique des VLAN, VTP, MVRP ou GVRP selon les commutateurs ;
- interdire la configuration automatique des ports (en mode trunk ou access) et configurer ceux-ci de façon sécurisée, notamment :
 - Dans le cas des ports en mode access : ne configurer que le VLAN nécessaire sur un port donné ;
 - dans le cas des ports en mode trunk : n'autoriser que les VLAN devant effectivement circuler sur le port trunk.
- tous les ports qui sont censés être inutilisés doivent être associés au VLAN de quarantaine. Les ports placés dans ce VLAN ne doivent donner accès à aucune ressource du système d'information et doivent interdire les communications avec toute autre machine, y compris les machines placées dans ce VLAN. Ces ports doivent aussi être désactivés, de même que le VLAN de quarantaine et l'interface associée ;
- le VLAN par défaut ne doit jamais être utilisé ;
- le VLAN natif :
 - Doit être configuré afin d'être différent du VLAN par défaut ;
 - ne doit être attribué à aucun port en mode access (il ne doit pas être utilisé pour faire circuler du trafic métier ou d'administration ;
 - doit être le même sur tous les commutateurs du même domaine de diffusion (et de préférence dans tout le système d'information par principe d'homogénéité) afin d'éviter les comportements inadéquats.
- le routage interVLAN doit être assuré par des équipements de niveau 3. Celui-ci doit donc être désactivé sur les commutateurs d'accès ;
- désactiver la fonctionnalité de Source routing ;
- activer les fonctions de DHCP snooping et d'IP Source Guard afin de pallier les faiblesses de sécurité du protocole DHCP ;
- activer les fonctions d'inspection ARP ;
- activer des protections contre la propagation des trames Spanning Tree sur les ports d'accès ;

- activer le mode portfast ou edge port (selon le constructeur) sur les ports connectés à des machines clientes. Ne pas activer ce mode sur les interfaces connectées à d'autres commutateurs ;
- synchroniser l'heure des commutateurs de son système d'information de manière automatisée afin de garantir une cohérence de l'heure de ses équipements. Utiliser si possible plusieurs sources de temps situées au sein du système d'information ;
- régler le niveau de journalisation des commutateurs pour l'adapter aux besoins de journalisation du SI et si possible activer l'envoi des journaux vers un serveur de collecte (exemple : syslog) ;
- dans le cadre de la centralisation des journaux du commutateur, faire remonter les événements par le réseau d'administration afin d'éviter la fuite d'informations sensibles ;
- activer la journalisation des commandes entrées par les administrateurs ;
- utiliser SNMP en version 3 AuthPriv, si cela n'est pas possible techniquement, utiliser à défaut la version 2c. Ne pas utiliser le protocole SNMP en mode set pour administrer les commutateurs ;
- afin d'augmenter la bande passante ou d'assurer une redondance sur les liens réseau entre les commutateurs de desserte et de distribution, il est recommandé de mettre en place l'agrégation de lien (aussi appelée EtherChannel ou Bridge Aggregation) ;
- homogénéiser les configurations matérielles et logicielles des commutateurs de son système d'information afin de faciliter leur MCO/MCS ;
- mettre à jour régulièrement le système d'exploitation des commutateurs afin de les protéger contre les failles de sécurité corrigées par ces mises à jour ;
- centraliser l'administration des commutateurs au sein du système d'information.
- mettre en place une procédure de sauvegarde, restauration de la configuration des commutateurs. Tester les procédures de façon régulière ;
- activer le chiffrement des mots de passe contenus dans le fichier de configuration.

Automates

Les postes de supervision et des équipements de terrain (automates) ne devront pas avoir d'accès possible à Internet. L'accès aux ports Ethernet et USB du système, ainsi que les connexions sans fil (Wi-Fi, Bluetooth, NFC, etc.), seront bloqués si ces derniers ne sont pas utilisés.

Les équipements autorisés à se connecter aux installations dans le cadre des interventions devront être clairement identifiés et validés (PC dédiés validés par le bureau cyber du SID Sud-Ouest) ; ils devront être marqués par le bureau cyber du SID Sud-Ouest. Une attestation de contrôle cyber de l'équipement devra être en permanence présentable à l'Administration et présente avec l'équipement

Lors de la mise en place ou d'un remplacement, les mots de passe par défaut de sortie d'usine devront être modifiables et modifiés.

Les mots de passe devront être transmis à l'Administration (RSSI-A) sous enveloppe scellée et datée/signée par le POC Cyber. Elle sera stockée dans un lieu sûr. Chaque modification du mot de passe devra être tracée dans un registre tenu par l'Administration.

La longueur et la complexité des mots de passe doivent être adaptées à chaque composant. Ces exigences seront transmises durant la période préparatoire au titulaire.

Postes informatiques

Durcissement

Les systèmes d'exploitation sont la base de tous les systèmes informatiques. Ils gèrent les ressources matérielles et logicielles des ordinateurs, assurent la communication entre les différents composants du système et fournissent un environnement d'exécution pour les applications. Cependant, ces systèmes présentent également des vulnérabilités qui peuvent être exploitées par des attaquants pour compromettre la sécurité du système dans son ensemble.

Pour cette raison, il est essentiel de prendre des mesures pour sécuriser et durcir les systèmes d'exploitation, tels que Microsoft Windows et Linux. Le durcissement consiste à éliminer ou à limiter les fonctionnalités inutiles ou dangereuses des systèmes d'exploitation, à configurer les paramètres de sécurité de manière appropriée et à installer les mises à jour de sécurité régulièrement.

En renforçant la sécurité des systèmes d'exploitation, il est possible de minimiser les risques de cyberattaques et de protéger les actifs numériques de l'entreprise ou du particulier. Cela permet également de garantir la confidentialité, l'intégrité et la disponibilité des données, qui sont essentielles pour la continuité des activités et la réputation de l'organisation.

Les mesures à appliquer sont :

- désactiver tous les services non utilisés ;
- désactiver le service du spooler d'impression ;
- désactiver le service Windows update ;
- activer le pare-feu Windows ;
- désactiver toutes les règles de pare-feu non utilisées, ne laisser que les flux utiles ;
- désactiver l'exécution automatique pour tous les médias et pour tous les comptes ;
- supprimer les tâches planifiées non utilisées par le système ;
- désinstaller toutes les applications non essentielles au système (jeux, Xbox, météo etc..) et pour tous les comptes ;
- installer un antivirus sur tous les postes et serveurs et le maintenir à jour ;
- désactiver les protocoles LLMNR, NetBIOS, Wins ;
- désactiver IP V6 ;
- mettre un mot de passe d'accès au BIOS pour interdire une modification du BIOS non autorisée (nommage donné par le bureau cyber) ;
- interdire la séquence de démarrage sur un autre média que la partition d'amorçage du disque dur ;
- mettre la synchronisation du temps (NTP) en cas d'absence d'un active-directory ;
- désactiver le wifi et/ou le Bluetooth via le BIOS si possible sinon dans le système d'exploitation ;
- désactiver les ports Ethernet non utilisés ;
- privilégier les comptes nominatifs et à faibles privilèges ;
- dans le cas de comptes fonctionnels, le RSSI-A s'assurera de la traçabilité des connexions (mise en place d'un cahier, PV d'intervention,..) ;
- créer un compte RSSI-A avec un profil administrateur pour ouvrir une session ;
- créer un compte RSSI-A avec un profil administrateur pour ouvrir une session sur le logiciel de supervision.
- limiter les droits utilisateurs au strict nécessaire ;

- mettre en place une politique de mots de passe :
 - 9 caractères minimum ;
 - 14 pour les comptes d'administration ;
 - Utilisation de 3 types de caractères différents sur les 4 possibles (Majuscule, minuscule, chiffre et caractères spéciaux) ;
- mettre en place une politique USB en autorisant techniquement que les supports identifiés (principe de white list) ;
- mettre en place une sauvegarde régulière, stockée sur un équipement déconnecté et dédié au système ;
- pour tout nouveau système, mettre à jour l'OS et logiciel(s) métier(s) avant la réception ;
- tous les comptes accompagnés des mots de passe seront donnés au RSSI-A de l'USID ;
- Si la limitation d'accès à l'Internet ne peut pas intégrer les mises à jour (anti-virus et de sécurité), le maintenancier doit prévoir une procédure en mode hors connexion ;
- dans le cas de systèmes d'exploitation Microsoft, la version est Windows 10 pro ou entreprise au minimum avec la dernière version soutenue par Microsoft .

Configuration de l'anti-virus

La mise en place de mesures de configuration d'un antivirus est essentielle pour assurer une protection efficace contre les menaces informatiques telles que les virus, les vers, les chevaux de Troie et les ransomwares.

Les paramètres suivants sont à respecter pour les agents antivirus déployés :

- analyser tous les fichiers scannables² ;
- programmer la planification de l'analyse hebdomadairement ; de préférence tous les dimanches à 12h ;
- configurer le niveau d'utilisation de l'UC à moyen, de manière à ne pas gêner l'utilisation du système ;
- analyser les fichiers compressés sur 3 couches ;
- analyser la zone d'amorçage ;
- activer l'IntelliTrap ou un outil similaire s'il existe ;
- activer l'antispyware/grayware ;
- exclure de l'analyse les répertoires d'installation de l'antivirus ;
- configurer les actions à réaliser dans le cadre d'une détection de programmes malveillants :
 - 1ère action : Nettoyer ;
 - 2ème action : Quarantaine ;
 - 3ème action : Supprimer ;
- exclure les flux vidéos et les enregistrement vidéos de l'analyse en temps réel pour les serveurs vidéos.

² Option dans l'anti-virus.

Attestation Cybersécurité PC de maintenance

Ce certificat est obligatoire pour toute intervention sur un équipement du Ministère. L'intervenant doit pouvoir le présenter à tout instant. Il doit donc accompagner le PC.

Marché

Nom du marché : _____
Numéro du marché : _____
Nom de l'entreprise : _____

POC cyber entreprise

Nom Prénom : _____
Téléphone : _____
@mail : _____

Détenteur

Nom Prénom : _____
Téléphone : _____
@mail : _____
Entreprise/unité : _____

Caractéristique du PC

Marque : _____
Modèle : _____
Num. de série : _____
Adresse MAC : _____
BIOS (Num. de version) : _____

Système d'exploitation

Nom OS : _____
Version OS : _____
Date MAJ : _____

Logiciels métiers

Nom	Version	Date MAJ
_____	_____	_____
_____	_____	_____
_____	_____	_____

Antivirus

Nom : _____
Version moteur : _____
Version signatures : _____
Date MAJ Moteur : _____
Date MAJ signatures : _____

Systèmes indus concernés

Nom

Nature des contrôles

Vérification de l'OS (MAJ) : _____
Vérification de l'AV (MAJ) : _____
Durcissement du PC (logiciels inutiles, BIOS...): _____
Chiffrement du disque (CRYHOD/BitLocker) : _____
Vérification des logiciels métiers (MAJ) : _____
Scan antivirus complet : _____
Sensibilisation par le RSSI-P ou A: _____
Signature IM2004 : _____

Signature responsable

Date : _____

Cachet,
Signature : _____

Commentaires

