ROYAUME DU MAROC

ADMINISTRATION DE LA DÉFENSE NATIONALE

DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

GUIDE TECHNIQUE

RELATIF À LA SÉCURITÉ DES RÉSEAUX

INFORMATIONS

AVERTISSEMENT
Destiné à vous assister dans l'adoption d'une démarche cohérente et homogène pour la mise en conformité de la sécurité de vos systèmes d'information avec les règles de sécurité édictées par la Directive Nationale de la Sécurité des Systèmes d'information (DNSSI), ce guide élaboré par la DGSSI traite la démarche de sécurisation des réseaux informatiques. Il est destiné à évoluer avec les usages, mais aussi avec vos contributions et retours d'expérience. Les recommandations citées dans ce guide sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, la DGSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par la DGSSI doit être soumise, au préalable, à la validation du Responsable de la Sécurité des Systèmes d'Information (RSSI) et de l'administrateur du système concerné.

ÉVOLUTION DU DOCUMENT :

Version	Date	Nature des modifications
1.0	12/12/2014	Version initiale

PUBLIC CONCERNÉ PAR CE DOCUMENT :

Direction SI
RSSI
Administrateur systèmes et réseaux

POUR TOUTE REMARQUE :

Contact	Email
DGSSI	contact@dgssi.gov.ma

Table des matières

1 Introduction

L'accroissement de l'utilisation des technologies de l'information, le développement de l'Internet et des réseaux de communication ont conféré aux systèmes d'information une importance capitale dans nos sociétés. Cet accroissement et ce développement se sont accompagnés par une recrudescence des cybermenaces et donc par d'importants investissements de la part des organismes pour la mise en place des règles et mesures de sécurité afin de garantir un niveau adéquat de maturité en matière de sécurité. Les réseaux de communication occupent une place de choix dans les investissements relatifs à la sécurité. En effet, un réseau sécurisé doit être protégé contre toutes attaques malveillantes et devrait répondre aux besoins de l'organisme en termes de confidentialité, d'intégrité et de disponibilité.

C'est dans cette optique que le présent document propose des recommandations et bonnes pratiques liées à la sécurité des réseaux basées sur l'état de l'art. L'objectif de ce document est de fournir des recommandations pour la conception et la configuration du réseau pour qu'il soit le moins vulnérable possible.

Le processus de la sécurité n'étant pas statique, ce document ne couvre pas tous les domaines de la sécurité du réseau. Toutefois, le risque peut être remarquablement réduit grâce à la mise en place d'une configuration sécurisée et par l'amélioration des fonctions de la sécurité selon les menaces et la criticité du système cible.
Ce guide comporte huit parties :

La première partie a pour but de présenter les différents risques qui peuvent menacer une infrastructure réseau.

La deuxième partie présente les recommandations pour l'implémentation d'une architecture sécurisée. Ceci à travers des règles de conception d'un réseau depuis le cloisonnement jusqu'à la centralisation et le partage de charge.

La troisième partie concerne le contrôle des accès et présente quelques règles relatives à la sécurisation des accès locaux et distants.

La quatrième partie traite le contrôle de flux et les recommandations pour un filtrage optimisé du trafic, et fournit les bonnes pratiques pour l'implémentation des systèmes de détection et de prévention contre les intrusions.

La cinquième partie se focalise sur la gestion de la journalisation des événements et la synchronisation du temps.

La sixième partie traite l'aspect de la gestion de la sauvegarde et de la restauration de la configuration.

La septième partie concerne la supervision et le management de la sécurité.

La huitième partie présente une vue globale sur l'audit de la sécurité du réseau et propose un ensemble d'outils permettant la réalisation de cet audit.

2 Risques de sécurité associés aux réseaux

L'importance croissante des actifs immatériels, l'augmentation des débits, l'interconnexion des systèmes d'information et l'ouverture à l'Internet, ont conduit à une évolution sans précédent des risques auxquels sont exposés les systèmes d'information à travers les réseaux qui les composent.

Par ailleurs, l'information est produite, traitée, transportée et exploitée par des systèmes et sur des réseaux qui peuvent présenter des vulnérabilités. Ces vulnérabilités concerneraient tous les composants du réseau qui comprennent les routeurs, les commutateurs, les ordinateurs de bureau, les serveurs et même les dispositifs de sécurité.

Les réseaux constituent à cet effet une cible privilégiée des menaces qui sont généralement dues à l'un des facteurs suivants :

- Le manque d'une politique de la gestion de la sécurité de l'information ;
- Le manque de la sécurité physique des équipements ;
- Le manque d'une politique de la gestion des correctifs et des mises à jour ;
- L'absence d'une analyse des risques avec des mesures de sécurité définies ;
- La conception aléatoire des réseaux sans aucune mesure de sécurité ;
- Le manque des méthodes et des procédures de gestion des accès ;
- Le manque des mécanismes de cryptographie ;
- L'administration et la supervision du réseau sans une maitrise des pratiques de la sécurité ;
- La mauvaise configuration des équipements réseaux.

Il convient donc de réaliser une identification et une analyse des risques afin de les classer en fonction de leur criticité et des objectifs fixés par l'organisme. Les résultats de cette analyse permettront de définir les actions prioritaires à mettre en place et les mesures convenables pour la protection contre les risques identifiés. A noter par ailleurs que le processus d'évaluation du risque devra être itératif pour garantir une optimisation des actions et des mesures de sécurité à adopter.

3 Conception d'une architecture réseau sécurisée

3.1 Considérations générales

La phase de la conception des réseaux est un processus complexe. Une conception appropriée ne doit pas se baser seulement sur les besoins fonctionnels du réseau, elle doit tenir compte aussi des considérations de sécurité conformément à la politique de sécurité de l'organisme. En effet, un réseau bien équipé et correctement configuré mais ne respectant pas une approche sécurisée dans sa conception pourrait présenter des vulnérabilités critiques et un risque de dysfonctionnement menaçant la sécurité du système d'information de l'organisme..

La conception d'un réseau ne doit pas tenir compte seulement des principes fondamentaux relatifs au respect de la fonctionnalité, l'évolutivité, l'adaptabilité et la facilité de gestion, mais elle doit tenir compte en plus des objectifs de la sécurité, notamment des éléments ci-après :

- **La confidentialité :** consiste à assurer que seuls les sujets (les personnes, les machines ou les logiciels) autorisés aient accès aux ressources et aux informations auxquelles ils ont droit ;
- **L'intégrité :** consiste à assurer que les ressources et les informations ne soient pas corrompues, altérées ou détruites par des utilisateurs ou des ressources non autorisés ;
- **La disponibilité :** vise à assurer un fonctionnement sans faille, et garantir l'accès aux services et ressources installés avec le temps de réponse attendu ;
- **La traçabilité :** consiste à gérer toute modification ou changement dans le système afin d'assurer la possibilité d'un contrôle systématique, et/ou d'apporter des preuves à posteriori.

R 1	Inclure les contraintes et les exigences de sécurité dès la phase de la conception du réseau.

3.2 Cloisonnement du réseau

Le cloisonnement consiste en la séparation du réseau en domaines physiques et logiques protégés chacun par un périmètre de sécurité bien défini. Il convient à cet effet de placer les postes de travail, les périphériques et les serveurs ayant différentes exigences et autorisations dans des zones de sécurité (domaines) différentes afin d'en optimiser la gestion et le niveau de sécurité.

Cela permet de restreindre les connexions autorisées en différenciant, à titre d'exemple, un réseau interne pour lequel aucune connexion venant d'Internet

n'est autorisée d'un réseau dit DMZ (zone démilitarisée) accessible depuis Internet. La mise en œuvre d'une telle DMZ nécessite l'installation de passerelles sécurisées (pare-feu) entre les réseaux à cloisonner afin de contrôler les flux d'information entrants et sortants.

Pour renforcer la sécurité de ces domaines, il faut créer une zone dédiée à l'administration des équipements du réseau. Cette zone d'administration permet de gérer et de vérifier le bon fonctionnement de tous les composants d'un périmètre de sécurité donné. Cette zone est par nature particulièrement sensible et doit être protégée de manière adéquate.

Il convient aussi de séparer le trafic de gestion du reste du trafic de production afin d'éliminer la possibilité qu'il puisse être intercepté durant le transit. Le cas échéant, le trafic de gestion doit être véhiculé via un protocole sécurisé.

R 2	Procéder à une analyse des risques pour identifier les différentes exigences en matière de sécurité pour chaque domaine.

R 3	Subdiviser le réseau en fonction de la criticité des informations véhiculées sur le réseau.

R 4	Subdiviser le réseau en tenant compte des niveaux de sécurité des accès : DMZ, réseaux internes, réseaux critiques, etc.

R 5	Dédier une zone d'administration pour le réseau, au minimum prévoir un réseau logiquement séparé de celui des autres réseaux.

R 6	Tenir compte des besoins de cloisonnement dans toute nouvelle extension du réseau.

3.3 Cloisonnement par VLAN

Les VLANs (Virtual LANs 802.1Q) permettent de créer des réseaux virtuels connectés à un équipement physique (commutateur) selon des critères (ex. port, adresse MAC, protocole), dans le but de séparer les trafics entre les différents réseaux ainsi constitués. Les machines d'un VLAN ne pourront pas communiquer avec celles appartenant à un autre VLAN. Pour permettre cette communication, il faut interconnecter les VLANs à l'aide d'un routeur ou d'un commutateur de niveau 3.

A noter qu'un lien « trunk » permet de transporter le trafic de plusieurs VLANs sur le même lien en se basant sur la norme 802.1Q qui consiste à insérer un champ à l'entête de la trame Ethernet à la fois pour gérer les VLANs et pour gérer les classes de service 802.1P. Toutefois ce type de lien doit être utilisé avec précaution et doit être configuré manuellement en cas de nécessité.

Ainsi, les VLAN offrent un meilleur contrôle de la diffusion, améliorent les performances et offrent une flexibilité et une évolutivité dans la gestion du réseau. Mais, ils ne fournissent aucun mécanisme de sécurité à proprement parler. En effet, les VLAN sont vulnérables à certaines attaques de couche 2 (le saut des VLANs « VLAN hopping ») qui consiste à détourner la segmentation logique et faire passer le trafic d'un VLAN à un autre.

R 7	Limiter le nombre de VLANs au strict nécessaire.

R 8	Mettre en place des mécanismes de protection contre les attaques sur les VLANs, notamment : – Limiter le nombre d'adresses MAC par port. – Configurer les ports comme ports d'accès et configurer les ports trunk manuellement si nécessaire. – Désactiver les ports non utilisés.

La séparation physique doit être préconisée dans le cas d'une différence importante dans les niveaux de sécurité et de criticité des informations véhiculées par les différentes zones des réseaux concernés.

3.4 Défense en profondeur

La défense en profondeur consiste à déterminer les barrières à mettre en place en fonction des menaces et des biens à protéger. Cela consiste à multiplier les niveaux de protection suivant une approche en couche afin de permettre aux autres couches de réagir si une couche de sécurité de niveau inférieur est franchie.

Il convient donc de déterminer, sur la base d'une analyse des risques, les mécanismes et les solutions à mettre en place selon la criticité et l'importance des biens à protéger. Plus le système à protéger est critique, plus le nombre des barrières de sécurité doit être important. On peut citer dans ce cadre :

- La sécurité physique ;
- Les pare-feu ;
- Les IDS/IPS ;
- Les VPNs ;
- Les solutions de journalisation, de supervision ;
- Les solutions antivirales ;

R 9	Implémenter une défense en profondeur pour assurer un niveau de sécurité adéquat du réseau selon l'importance des biens à protéger.

3.5 Centralisation de la gestion du réseau

La gestion centralisée du réseau permet une exploitation efficiente de l'infrastructure réseau. Cela se traduit par une supervision efficace et une intervention rapide en cas d'incident pour assurer une haute disponibilité des services. La solution de gestion centralisée doit être compatible avec les équipements du réseau de l'organisme tout en assurant une gestion facile et efficiente de l'infrastructure réseau.

R 10	Mettre en place une plateforme centralisée de gestion de l'infrastructure réseau.

R 11	Implémenter la solution de gestion du réseau dans la zone d'administration.

3.6 Disponibilité

L'indisponibilité des services offerts par le réseau représente une menace au bon fonctionnement du système d'information. Cette menace peut provenir de plusieurs sources telles que la défaillance des équipements, la saturation du réseau ou les attaques par déni de service, etc.

La conception d'un réseau doit tenir compte de l'aspect haute disponibilité et de partage de charge des services offerts. Cela consiste à assurer une redondance et une distribution de charge de façon intelligente pour améliorer le temps de réponse des services, renforcer la capacité à pallier la défaillance d'un ou plusieurs équipements du réseau et l'ajout de nouveaux équipements sans interruption du service.

Il se traduit en général par la mise en œuvre de solutions qui permettent la redondance de l'alimentation, des équipements, des liens, des passerelles, des accès Internet, voire même l'utilisation des protocoles de redondance des passerelles (ex. VRRP « Virtual Router Redundancy Protocol ») et les protocoles de routage dynamique (ex. OSPF « Open Short Path First »).

R 12	Assurer une haute disponibilité des éléments clés du réseau en tenant compte de l'impact de la défaillance de ces éléments sur la disponibilité du réseau.

3.7 Les réseaux sans fil

Si l'utilisation des réseaux sans fil (Wireless LAN) s'impose dans certains cas, il convient de les séparer du réseau local par l'utilisation de dispositifs de segmentation. Cela fournit une sécurité supplémentaire et un point de passage obligé

entre le réseau sans fil et le réseau local filaire.

La sécurité physique des points d'accès (Access Point « AP ») et des infrastructures connexes devrait également être considérée comme faisant partie de l'infrastructure. Il convient donc de mettre en place les contrôles appropriés visant à protéger physiquement le matériel, tels que l'installation des points d'accès dans des armoires sécurisées ou le montage des points d'accès dans des zones fermées.

La conception d'un réseau sans fil doit également prendre en considération les mécanismes d'authentification et de cryptage à utiliser. En effet, il est recommandé de mettre en place un niveau élevé d'authentification, des techniques cryptographiques appropriées et de réaliser un contrôle fin des utilisateurs qui ont accès aux réseaux sans fil.

D'une manière générale, il faut éviter le déploiement de réseaux sans fil sur des systèmes d'information manipulant des données sensibles, à défaut, mettre en œuvre de mesures spécifiques.

R 13	Séparer les réseaux sans fil du reste du réseau global.

R 14	Renforcer la sécurité des points d'accès, notamment : – Changer la configuration par défaut des points d'accès : les mots de passe d'administration, le SSID par défaut, etc. – Désactiver les interfaces de management et les services non utilisées. – Désactiver la diffusion du SSID. – Mettre en place un filtrage par adresse MAC. – Activer la journalisation de l'activité des points d'accès.

R 15	Mettre en place des techniques cryptographiques efficaces : – Éviter l'utilisation des protocoles vulnérables comme le WEP. – Utiliser un chiffrement robuste.

R 16	Mettre en place une solution d'authentification centralisée (exemple : le standard IEEE 802.1X / EAP "Extensible Authentication Protocol").

4 Contrôle d'accès

Le contrôle d'accès aux ressources est un élément capital dans la sécurité des réseaux. Ce contrôle permet en effet de protéger le réseau contre tout accès non autorisé aux ressources.

Ce type de contrôle doit faire l'objet d'une politique documentée et doit s'appuyer sur des logiciels, des technologies, et des composants physiques appropriés.

4.1 Contrôle d'accès au réseau

4.1.1 Politique de contrôle d'accès

Le contrôle d'accès devrait être à la fois logique et physique. Avant de mettre en place des mécanismes de contrôle d'accès, il est recommandé de définir une politique de contrôle d'accès qui définit les autorisations et les droits d'accès à un périmètre de sécurité défini.

R 17	Définir et séparer les rôles et les responsabilités pour les accès aux ressources du réseau.

R 18	Établir des règles d'accès fondées sur le principe «tout est généralement interdit sauf autorisation expresse» plutôt que sur la règle, moins fiable, selon laquelle «tout est généralement autorisé sauf interdiction expresse».

R 19	Attribuer des autorisations et des droits d'accès adaptés au niveau de sécurité souhaité.

R 20	Assurer une traçabilité des modifications des droits d'accès.

4.1.2 Gestion des accès physiques

La sécurité physique d'un réseau est l'un des facteurs clés de la réussite d'une politique de contrôle d'accès. Il doit reposer sur la définition d'un périmètre de sécurité approprié et sur la restriction des accès aux seules personnes autorisées.

R 21	Définir les périmètres physiques à accès restreint, et mettre en place des dispositifs de contrôle d'accès.

R 22	Placer les ressources critiques (les pare-feu, les routeurs, les switchs, etc.) dans des périmètres sécurisés.

R 23	Identifier, documenter et valider toute modification physique de l'infrastructure réseau.

4.1.3 Gestion des accès logiques

Afin d'empêcher tout accès non autorisé au réseau, il convient d'utiliser des mécanismes d'authentification pour les utilisateurs et les équipements. Ces mécanismes sont à la fois de nature organisationnelle (des procédures de gestion des accès) et technique (des mécanismes d'authentification et d'autorisation), permettant de minimiser les accès non autorisés aux ressources et par conséquent diminuer l'impact en cas d'action malveillante.

R 24	Mettre en place une procédure de gestion des accès des utilisateurs aux ressources réseaux.

R 25	Mettre à la disposition des utilisateurs des comptes nominatifs et uniques et attribuer les droits d'accès selon le principe du moindre privilège.

R 26	Mettre à la disposition des administrateurs des comptes nominatifs et uniques et attribuer les privilèges selon leurs rôles et leurs responsabilités.

R 27	Mettre en place des mécanismes d'authentification des équipements autorisés sur le réseau (ex. le standard IEEE 802.1X).

R 28	Générer des traces des accès et des commandes exécutées à des fins d'investigation de sécurité.

4.1.4 Authentification et autorisation d'accès

L'accès des dispositifs et des utilisateurs aux ressources réseaux doit être préalablement authentifié et autorisé. Le processus d'authentification et d'autorisation doit suivre une approche respectant le modèle AAA (Authentification « Authentication », Autorisation « Authorization » et Journalisation « Accounting »). L'utilisation de ce modèle permet de confirmer l'identification du propriétaire du compte avant d'autoriser l'accès, de lui décrire les droits à exercer et de garder un enregistrement et un suivi de ses actions.

Compte tenu de l'évolution de la taille, la nature et la complexité des réseaux, la gestion des bases de données d'authentification peut s'avérer difficile. Il convient donc de mettre en place des solutions centralisées assurant une authentification unique (SSO) pour bénéficier des services offerts par le réseau. Cela

permet aussi d'assurer l'identification et la résolution des problèmes d'accès dans des délais raisonnables sans entraver la continuité des activités.

R 29	Implémenter une politique d'authentification et d'autorisation selon le modèle AAA.

R 30	Renforcer l'authentification par la mise en place d'une authentification forte (exemple : Tokens, certificats, empreinte digitale, etc.).

R 31	Mettre en place une solution centralisée d'authentification et d'autorisation des accès aux ressources réseaux.

R 32	Placer les périphériques et les utilisateurs authentifiés dans des zones de sécurité qui correspondent à leurs profils et privilèges.

R 33	Bloquer l'accès des périphériques et des utilisateurs non authentifiés ou les placer dans des zone dédiées qui permettent un accès restreint aux services du réseau.

R 34	Mettre en place des techniques de protection contre les tentatives de connexion infructueuses (ex. limiter le nombre de tentatives de connexion avant de bloquer l'accès).

R 35	Déconnecter les sessions de connexion après une période d'inactivité.

4.1.5 Gestion des mots de passe

Le mot de passe constitue un des moyens d'identification d'un utilisateur pour l'accès à une ressource réseau. Il convient donc de respecter les bonnes pratiques de sécurité lors du choix d'un mot de passe, notamment :

- Le mot de passe doit contenir au moins 12 caractères (composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux) ;
- Le mot de passe ne doit pas être composé d'une suite consécutive de caractères identiques totalement numériques ou totalement alphabétiques ;
- Le mot de passe ne doit pas être attaché à une information personnelle facile à deviner ou à obtenir, et il doit être non vulnérable à une attaque par dictionnaire.

Il convient aussi de protéger l'enregistrement et la sauvegarde des mots de passe par l'implémentation des mécanismes cryptographique assurant la confidentialité et l'intégrité des fichiers de configuration et des fichiers de backup.

R 36	Choisir un mot de passe fort.

R 37	Ne pas partager le mot de passe.

R 38	Ne pas garder un enregistrement du mot de passe en clair (sous format papier ou fichier électronique).

R 39	Eviter d'utiliser les mots de passe par défaut.

R 40	Changer les mots de passe à intervalles réguliers (entre 60 et 90 jours) et ne pas réutiliser d'anciens mots de passe.

R 41	Protéger les fichiers de configuration des équipements réseaux contre les divulgations non autorisées, et prendre les mesures nécessaires afin d'éviter que les mots de passe apparaissent en claire.


Pour une meilleure application des recommandations citées ci-dessus, il convient de mettre en place une politique de gestion des mots de passe au niveau de la solution centralisée d'authentification.

4.2 Exploitation et administration

4.2.1 Administration des équipements réseaux

L'administration et la gestion des équipements réseau est un aspect sensible qui doit être géré d'une manière adéquate pour empêcher toute connexion non autorisée. Il est recommandé de dédier une zone d'administration sécurisée avec un plan d'adressage spécifique. Cette zone d'administration doit être protégée par filtrage strict, et doit favoriser l'utilisation des protocoles sécurisés.

R 42	Disposer d'un inventaire de l'infrastructure réseau avec l'emplacement, le rôle, la version du système, l'adresse IP de management de chaque composant.

R 43	Mettre en place une procédure de nomination des équipements réseaux et des câbles pour faciliter la maintenance.

R 44	Renforcer la sécurité des équipements, notamment : – Changer les comptes et les mots de passe d'administration fournis par défaut. – Désactiver tous les services non utilisés. – Désactiver les interfaces non utilisées. – Restreindre l'accès physique aux équipements aux seules personnes autorisées. – Restreindre l'accès aux interfaces de management des équipements aux seules personnes autorisées.

R 45	Utiliser des protocoles sécurisés (SSHv2, TLS v1.1+, etc.).

R 46	Veiller à la mise à jour des logiciels et des systèmes d'exploitation (OS) des éléments de l'infrastructure réseau.

4.2.2 Gestion des accès à distance

Les solutions d'accès à distance permettent aux utilisateurs d'accéder à des fonctionnalités internes du système d'information à partir de l'extérieur. Il est par conséquent nécessaire d'appliquer au minimum le même niveau de sécurité que les mécanismes utilisés pour contrôler l'accès local aux ressources réseaux.
La sécurité d'accès à distance repose sur une combinaison de la sécurité des éléments suivants :

- Le client (le système d'exploitation client, pare-feu client, le logiciel client d'accès à distance, etc.) ;
- Le réseau (le point d'accès à distance, la segmentation réseau, les droits associés aux comptes d'accès à distance, etc.) ;
- Les exigences cryptographiques.

R 47	S'assurer que tous les accès distants sont authentifiés et chiffrés (IKE/IPsec).

R 48	Isoler les accès distants dans un segment d'adresse IP déterminée afin de faciliter le filtrage ultérieur par d'autres équipements de sécurité.

R 49	Limiter les services offerts pour les accès distants aux seuls besoins identifiés.

R 50	Sécuriser les ordinateurs utilisés pour les accès distants par l'implémentation d'un logiciel antivirus ainsi qu'un pare-feu local.

R 51	Auditer périodiquement la base de données des utilisateurs autorisés à accéder à distance afin d'éliminer les comptes non utilisés.

5 Contrôle des flux

5.1 Considérations générales

Un contrôle des flux efficace repose sur l'établissement d'une politique de contrôle des trafics échangés entre les différentes zones de sécurité. Ce contrôle permet de disposer d'une vision globale des échanges effectués sur le réseau à travers l'identification du rôle de chaque dispositif de sécurité et l'établissement d'une matrice des flux et des services autorisés.

De plus, il convient de disposer d'une procédure de gestion des changements permettant de formaliser et de tracer toute modification apportée à l'architecture réseau ou à la matrice des flux échangés.

R 52	Définir une politique de contrôle des flux selon les besoins de l'organisme.

R 53	Documenter la topologie du réseau et élaborer une matrice des flux.

R 54	Etablir des procédures formelles pour le processus de gestion des changements et le traçage des modifications apportées sur l'architecture réseau.

R 55	Mettre en place des mécanismes de filtrage, des proxies de services et des dispositifs de prévention et détection d'intrusion pour séparer, protéger et superviser le réseau.

5.2 Filtrage de paquets

La fonction de filtrage de paquets n'est pas réservée exclusivement aux pare-feu. D'autres dispositifs tels que les routeurs et les commutateurs de la couche 3 permettent aussi de réaliser du filtrage de paquets par l'implémentation des filtres spécifiques. Le filtrage de paquets se base essentiellement sur l'analyse des paquets échangés, les adresses IP 'source' et 'destination', les types de paquets et le service ou le port demandé.

La mise en place des mécanismes de filtrage tels que le filtrage statique « stateless », le filtrage à état « stateful » et le filtrage applicatif, permet d'assurer une protection adéquate du réseau conformément à la politique de contrôle d'accès tout en évitant de trop limiter les fonctionnalités de l'utilisateur (équilibre entre sécurité et fonctionnalité).

R 56	Définir les règles de filtrage sur la base de "tout ce qui n'est pas explicitement autorisé est interdi".

R 57	Mettre en place des règles de filtrage sur la base des interfaces (interne, externe, DMZ, etc.), de la direction des connexions (trafic entrant et trafic sortant), de l'adresses IP source et destination, des ports sources et destination.

R 58	Mettre à jour les règles de filtrage en fonction des exploits et vulnérabilités récents et de l'évolution de l'architecture du réseau.

R 59	Protéger contre le IP Spoofing, en bloquant toute connexion provenant de l'Internet ayant comme adresse source : une adresse du réseau interne, les adresses locales « 127.0.0.0-127.255.255.255 », une adresse privée « 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 » ou une adresse de multicast « 224.0.0.0/4 ».

R 60	Autoriser seulement les connexions sortantes ayant comme adresse source l'adressage du réseau interne.

R 61	Activer l'envoi de logs pour les règles de filtrage qui bloquent l'accès à une ressource système ou réseau.

R 62	Filtrer les messages ICMP "destination unreachable" et "redirect".

R 63	Protéger le réseau interne contre le "traceroute" provenant des réseaux externes.

5.3 Protocoles de routage

Le terme routage désigne le mécanisme par lequel les données d'un équipement expéditeur sont acheminées jusqu'à leur destinataire, même si aucun des deux ne connaît le chemin complet que les données devront suivre. Les protocoles de routage permettent la diffusion des informations de routage aux autres systèmes du réseau afin de transmettre les modifications des tables de routage. Ces informations de routage sont utilisées lors de l'acheminement des paquets d'un réseau IP à l'autre en fonction de leur adresse IP de destination.

Ces protocoles nécessitent d'être protégés afin d'éviter tout impact sur les tables de routage du réseau. En effet, ils peuvent être cibles d'attaques, notamment :

- Attaques par injection de routes, qui consistent à injecter un nombre important de fausses routes ou de routes dupliquées afin de rendre instable le processus de routage du réseau ;
- Attaques permettant de générer une instabilité des routes, qui consistent à injecter des mises à jour importantes, par exemple sur une route légitime, afin d'impacter le processus de routage ou de bloquer certaines routes.

R 64	Définir des règles de configuration des protocoles de routage internes et externes permettant d'assurer un périmètre de sécurité précis du processus de routage.

R 65	Sécuriser les échanges des informations de routage par l'utilisation d'un mot de passe de type message digest.

5.4 Systèmes de détection et de prévention contre les intrusions

Les systèmes de détection et de prévention contre les intrusions permettent de surveiller le trafic réseau afin de repérer les activités anormales et suspectes. Les systèmes de détection d'intrusion « IDS » sont des systèmes software ou hardware conçus pour analyser le trafic circulant dans un périmètre réseau bien définit. Ils fonctionnent en mode passif en envoyant des logs en cas de détection d'une intrusion. Par contre, les systèmes de prévention d'intrusion « IPS » fonctionnent en mode actif, et ils permettent, en plus de l'envoi des logs, d'autoriser ou de bloquer le trafic en cas de détection des activités malveillantes.

La détection d'intrusions se base sur les signatures stockées dans des bases de connaissances des IDS/IPS. Ces signatures nécessitent des mises à jour régulières en fonction des nouvelles attaques et vulnérabilités détectées.

De manière générale, l'utilisation de ces solutions dépend des besoins de l'organisme, mais il est conseillé de placer l'IDS/IPS après le Firewall (coté réseau interne).

R 66	Choisir un emplacement adéquat de l'IDS/IPS qui répond aux besoins de sécurité de l'organisme.

R 67	Mettre à jour régulièrement les bases des signatures des IDS/IPS.

R 68	Veiller à réduire le taux des faux positifs qui peut engendrer un arrêt du trafic dans le réseau.

R 69	Sécuriser et limiter l'accès aux interfaces de management des IDS/IPS et journaliser toute tentative de connexion.

R 70	Journaliser les alertes détectées par l'IDS/IPS.

R 71	Etablir une procédure de traitement d'incidents dans le cas d'une détection d'intrusion.

6 Journalisation des évènements et synchronisation du temps

6.1 Journalisation des évènements

La journalisation est un mécanisme de contrôle de la sécurité d'information qui permet de surveiller le réseau et de garder une traçabilité sur les journaux d'activités (logs). Elle représente un moyen d'investigation et d'analyse en cas d'incident.

De manière générale, il est recommandé d'utiliser des équipements disposant nativement d'une fonctionnalité de journalisation, de synchroniser ces équipements sur plusieurs sources de temps (utiliser le NTP), de définir la granularité de la journalisation en fonction du rôle de l'équipement et du besoin de l'organisme et de privilégier en cas de besoin un transfert en temps réel des journaux sur des serveurs centraux.

R 72	Établir des procédures formelles permettant la gestion des journaux d'activités, leur examen périodique et leur sauvegarde.

R 73	Déterminer le niveau de journalisation requis pour chaque équipement par le biais d'une appréciation du risque.

R 74	Centraliser et consolider les journaux d'activités sur une solution centrale (serveur de logs), et veiller à ce que cette solution soit redondée afin d'assurer une haute disponibilité du service de collecte des logs.

R 75	Envoyer les journaux d'activités vers un réseau de gestion sécurisé et dédié, et s'appuyer de préférences sur des mécanismes cryptographiques lors du transfert des logs (mettre en place un VPN sécurisé si le réseau est distant.)

R 76	Etablir une estimation de l'espace de stockage nécessaire à la conservation des journaux d'activités.

R 77	Restreindre l'accès aux logs aux seules personnes autorisées.

6.2 Synchronisation et serveur NTP

Pour pouvoir analyser convenablement les journaux d'évènements collectés, il est recommandé de disposer d'équipements synchronisés sur la même base de temps.

Le protocole NTP (Network Time Protocol) permet de synchroniser automatiquement les équipements réseau et système sur une ou plusieurs sources de temps. Il convient d'établir une architecture NTP qui prend en compte des serveurs NTP internes sur lesquels se synchronise l'ensemble des équipements du réseau de l'organisme.

R 78	Synchroniser l'horloge principale des serveurs NTP locaux sur une référence reconnue, par exemple sur le Temps Universel Coordonné (UTC) ou des serveurs externes approuvés.

R 79	Envisager l'utilisation d'un serveur NTP redondant à mettre en place dans la zone d'administration.

R 80	S'assurer que tous les équipements réseaux sont synchronisés sur les serveurs NTP locaux.

R 81	S'assurer que les équipements réseaux sont synchronisés sur les serveurs NTP autorisés (utiliser par exemple l'authentification NTP et le filtrage par des règles de sécurité).

7 Sauvegarde et restauration

L'opération de sauvegarde consiste à réaliser des copies périodiques des fichiers de configuration des éléments réseau. Celle-ci peut être utile lors de la restauration en cas d'incident. Cette opération peut se faire manuellement ou automatiquement en utilisant des outils appropriés.

Pour ce faire, il convient de mettre en place une procédure de gestion de la sauvegarde et de la restauration afin de formaliser ce processus en définissant les rôles, les responsabilités et les mécanismes mis en place pour la réalisation des opérations de sauvegarde et de restauration.

R 82	Etablir une procédure de gestion de la sauvegarde et de la restauration de la configuration réseau.

R 83	Placer les sauvegardes dans un lieu sûr distinct du site source.

R 84	Protéger les sauvegardes réalisées par un chiffrement approprié.

R 85	Automatiser les sauvegardes pour faciliter le processus de sauvegarde et de restauration.

R 86	Soumettre régulièrement à essai les supports de sauvegarde pour s'assurer de leur fiabilité.

R 87	Mettre en place un suivi approprié à l'aide des outils de supervision du processus de sauvegarde

8 Supervision et management de la sécurité

8.1 Solution de management de la sécurité "SIEM"

Les solutions de management de la sécurité de l'information et des événements fonctionnent en temps réel pour sécuriser le réseau d'une manière ponctuelle et proactive. Elles permettent de surveiller les alertes de sécurité générées par diverses solutions de sécurité logicielles ou matérielles.

Les solutions SIEM permettent de recueillir des données pertinentes de sécurité à partir de différentes sources (à savoir les routeurs, les IDS/IPS, les pare-feu, les serveurs, etc.), de les normaliser, de les corréler, et de fournir une réponse automatique pour réduire le temps de réaction à une attaque. Elles permettent ainsi de relier plusieurs évènements de sécurité à une même cause.

R 88	Procéder à un déploiement progressif de la solution. Commencer le déploiement sur un périmètre limité avant de l'étendre à l'ensemble du SI de l'organisme.

R 89	Séparer le trafic du SIEM du reste du trafic réseau, et favoriser l'utilisation des protocoles de transfert des évènements collectés qui s'appuient sur des mécanismes cryptographiques (par exemple mettre en place un VPN sécurisé si le réseau est distant).

R 90	Veiller à réduire le taux des faux positifs générés par le SIEM, notamment lors de la première mise en œuvre de la solution.

R 91	Conserver et gérer les données historiques pour une analyse ultérieure.

8.2 Supervision du réseau

Les solutions de supervision permettent notamment de détecter l'état des liens et de mesurer les performances en termes de bande passante et de charge (CPU et mémoire) des équipements réseau. Cela permet de détecter tout changement dans le réseau afin de permettre aux administrateurs de réagir en temps opportun pour empêcher tout dysfonctionnement éventuel.

La centralisation de la supervision permet une surveillance facile et efficace du réseau par la centralisation et la consolidation des informations collectées depuis les éléments supervisés (routeurs, commutateurs, pare-feu, IDS/IPS, serveurs, etc.).

R 92	Mettre en place une solution de supervision centralisée.

R 93	Définir le périmètre de supervision souhaité et le niveau de suivi des activités.

R 94	Placer la solution de supervision dans une zone de management dédiée et sécurisée.

R 95	Restreindre l'accès à ces solutions de supervision aux seules personnes autorisées.

R 96	Implémenter les options de sécurité offertes par les protocoles de supervision.

R 97	Protéger les échanges entre les serveurs de supervision et les équipements supervisés (mettre en place un VPN sécurisé si le réseau est distant).

9 Audit de la sécurité du réseau

L'audit de la sécurité du réseau est un examen méthodique et périodique de la situation de l'infrastructure réseau en vue de vérifier sa conformité à des bonnes pratiques, à des règles ou à des normes.

L'audit de la sécurité des réseaux peut être effectué en utilisant une combinaison d'outils de scan des réseaux et de détection des vulnérabilités (ex. HPing, Nmap, Ethereal, OpenVAS, Aircrack-ng, etc.). Il est important aussi d'utiliser des outils de test d'intrusion et des techniques d'évasion tel que le Framework des tests d'intrusion Metasploit. En plus, il convient d'utiliser des outils d'audit et de validation de la configuration des équipements réseaux (ex. NCAT 'Network Config Audit Tool').

R 98	Réaliser périodiquement des contrôles et des audits de sécurité de l'infrastructure réseau.

R 99	Utiliser des outils de tests d'intrusion pour évaluer la capacité du réseau à résister à des attaques extérieures.

R 100	Auditer et examiner la configuration des équipements réseau (Routeur, firewall, Switches, IDS/IPS, etc.).

R 101	Etablir un rapport d'audit détaillé qui résume la situation actuelle du réseau et propose des recommandations pour en améliorer la sécurité.

Afin d'éviter des conséquences liées aux éventuels dysfonctionnements sur un environnement de production, il est préférable de réaliser les tests d'intrusion sur un environnement de test ou pré-production.

Références

[1] Norwegian National Security Authority, *"Network Security Guidance N-01"*, 20-08-2012.

[2] Norwegian National Security Authority,*Security guidance for switches and routers*,29-09-2012.

[3] National Security Agency (NSA), *"Hardening Network Infrastructure"*, MIT-003FS-2013, May 2013.

[4] Keith Barker & Scott Morris, *"CCNA Security, 640-554 Official cert guide"*,2013 Pearson Education.

[5] John Swartz & Todd Lammle,*"Cisco Certified Internetwork Expert (CCEI) Study Guide"*.

[6] SANS Institute InfoSec Reading Room, *"Virtual LAN Security : weaknesses and countermeasures"*.

[7] Thomas Akin, *"Hardening Cisco Routers"*, February 2002.