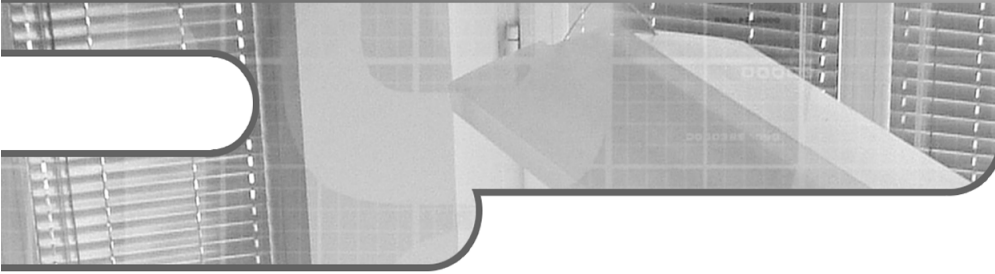


Chapitre 4
Principes de sécurité sur un réseau local

1. Sécurité au niveau des commutateurs

1.1 Les faiblesses du protocole ARP

Le protocole ARP (*Address Resolution Protocol*) est indispensable au fonctionnement d'un réseau internet IPv4. Il assure en effet, la correspondance entre adresses IP des machines et adresses MAC. Ce protocole a été créé dès 1982, dans un contexte où la sécurité n'était pas encore une priorité.

ARP repose sur des broadcast, dans lesquels une machine voulant obtenir une résolution envoie une trame « ARP request » à l'ensemble du segment réseau. La machine concernée renvoie une requête « ARP Reply » où elle indique alors son adresse MAC. À partir de là, la machine émettrice peut constituer son paquet IP et envoyer la trame à son destinataire connaissant désormais son adresse physique.

Afin de s'annoncer sur le réseau et également détecter d'éventuels conflits d'adresses IP, une machine se connectant physiquement sur le réseau émet une requête ARP appelée « ARP gratuit » dans laquelle elle s'annonce à tous les membres du segment réseau (`filtre wireshark : arp.isgratuitous == 1`). Ces derniers mettent alors à jour leur cache ARP dans lequel ils vont stocker l'adresse IP et l'adresse MAC correspondante, même s'ils n'ont jamais émis d'« ARP request » pour connaître la machine en question. Pour les communications futures, une machine du réseau consulte en premier lieu son cache ARP à la recherche d'une correspondance. Si et seulement si la correspondance n'existe pas, la machine émet une requête « ARP request ». On peut également placer statiquement des entrées permanentes dans le cache ARP (que l'on appelle table ARP) qui ne sont pas modifiables par le protocole.

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.17134.590]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\WINDOWS\system32>arp -a

Interface : 192.168.88.1 --- 0x21
  Adresse Internet      Adresse physique      Type
  192.168.88.255        ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  229.111.112.12        01-00-5e-6f-70-0c     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique

Interface : 192.168.1.56 --- 0x3c
  Adresse Internet      Adresse physique      Type
  172.31.141.122        00-ae-8c-79-1e-2d     dynamique
  192.168.1.76          f4-ca-e5-6b-ee-ac     dynamique
  192.168.1.89          08-2e-5f-f1-02-d8     dynamique
  192.168.1.90          3c-bd-3e-c4-4d-22     dynamique
  192.168.1.240         24-5e-be-0f-fe-e3     dynamique
  192.168.1.254         14-0c-76-95-c2-9a     dynamique
  192.168.1.255         ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  226.178.217.5         01-00-5e-32-d9-05     statique
  229.111.112.12        01-00-5e-6f-70-0c     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

Affichage de la table ARP sur une machine Windows 10

Partant du fait que n'importe quelle machine peut émettre des requêtes ARP sans vérification d'identité, il est tout à fait envisageable pour un attaquant d'émettre des requêtes ARP en usurpant une adresse IP. Concrètement, rien n'empêche d'annoncer à tout le segment réseau que l'adresse IP d'un poste, d'un serveur, de la passerelle par défaut par exemple, correspond à sa propre adresse MAC. Cela permet alors à l'attaquant d'intercepter du trafic qui ne lui est pas destiné.

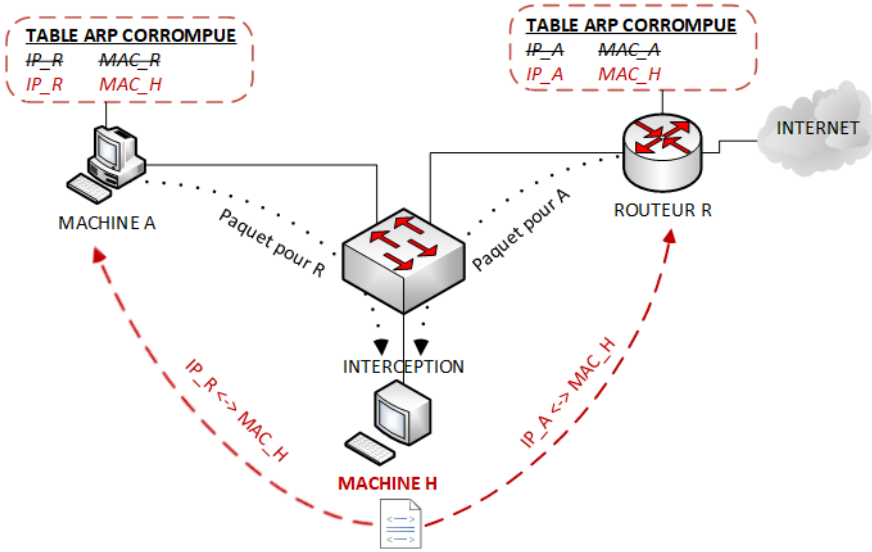
Voici en détail comment mettre en place ce type d'interception pour mieux comprendre le mécanisme d'attaque appelé « homme du milieu » ou « Man-in-the-Middle » :

Soit une machine A sur le réseau, naviguant sur Internet par l'intermédiaire du routeur passerelle par défaut R. H est un attaquant, il est connecté sur le même segment réseau qu'A et R. Son but est d'intercepter l'intégralité du trafic, entrant et sortant, entre A et R et donc l'intégralité de la navigation internet de la machine A.

La machine attaquante va dans un premier temps générer un paquet ARP dans lequel elle va annoncer que l'adresse IP du routeur « IP_R » correspond à son adresse MAC « MAC_H » (on parle d'« ARP poisoning »). La machine A va donc physiquement envoyer les trames à destination de l'IP de R sur l'adresse MAC de H. H recevra alors les paquets à destination de R contenant le trafic à destination d'Internet.

L'attaque ne peut s'arrêter là : dans un second temps, afin d'obtenir les paquets de réponse correspondant à la requête initialement interceptée, l'attaquant doit faire en sorte d'usurper l'identité de A par rapport au routeur. Il va annoncer alors avec une requête ARP, que l'adresse MAC correspondant à l'adresse IP de la machine A « IP_A » est la sienne : « MAC_H ». Le routeur enverra désormais toutes les réponses concernant logiquement la machine A à l'adresse physique de l'attaquant « MAC_H ». H se trouve donc en situation complète de MiM (Man In the Middle) et est capable d'intercepter le trafic dans les deux sens. Il ne lui reste plus qu'à transmettre les paquets sortants ou entrants aux deux intéressés pour ne pas interrompre la communication.

L'attaquant n'a cependant pas la possibilité d'empêcher A ou R d'envoyer leurs trames ARP sur le réseau. Ainsi, il est obligé d'envoyer des requêtes falsifiées à intervalles de temps régulier pour maintenir l'interception.

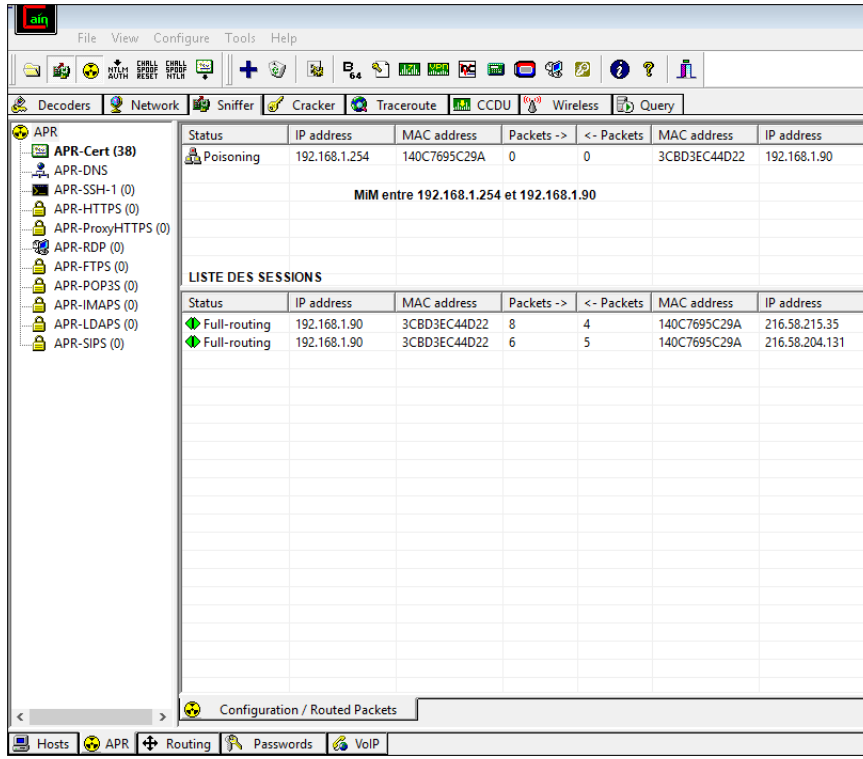


Attaque MiM ARP, la machine attaquante H émet des ARP request falsifiée et intercepte alors le trafic entre la machine A et le routeur R, et indirectement le trafic Internet

Il existe un certain nombre de programmes permettant de réaliser ce type d'attaque (en laboratoire uniquement) afin de mieux comprendre ces mécanismes. Il y a, par exemple, Cain&Abel sous Windows et ETTERCAP sous Linux pour les plus connus :

– http://www.oxid.it/

– https://www.ettercap-project.org/



Attaque MiM ARP via le logiciel Cain & Abel - interception de trafic entre 192.168.1.90 et le routeur 192.168.1.254

Le fichier C4_1_AttaqueARP_capture.pcapng est disponible en téléchargement sur le site des Éditions ENI.

La machine cible A peut-elle s'apercevoir que sa communication Internet est interceptée? Si le protocole de niveau applicatif n'a pas prévu une procédure d'authentification et de chiffrement, concrètement si la famille de protocoles SSL/TLS n'est pas utilisée, alors l'attaque reste imperceptible. Dans le cas de l'utilisation d'un protocole d'authentification comme SSH et dans notre cas présent HTTPS pour de la navigation web, la machine affichera un message d'avertissement de son application cliente (le navigateur), lui indiquant que la communication avec le serveur distant n'est pas sûre.

Pour améliorer l'attaque et la rendre plus discrète, l'attaquant devrait dans ce cas usurper le certificat du serveur de destination, en faisant en sorte qu'il soit reconnu par une autorité de certification (une CA), ce qui demande d'être en possession de la clé privée du serveur web de destination, ou d'avoir manipulé le navigateur web de la victime avant l'attaque, ce qui reste plus complexe, mais réalisable.

Une alternative plus simple consisterait à forcer l'utilisation par l'application cliente, d'un protocole non sécurisé, c'est-à-dire HTTP au lieu de HTTPS pour un navigateur, quitte ensuite à réencapsuler les requêtes en HTTPS pour la communication entre l'attaquant et le serveur web.

Les éditeurs de navigateurs, et en particulier Google avec son navigateur Chrome, ont été parmi les premiers à mettre en place une parade interdisant la consultation d'un site en HTTP, s'il existe une version HTTPS. C'est ce que propose le mécanisme HSTS (*HTTP Strict Transport Security*) dans la RFC 6797 imposant au navigateur l'utilisation du HTTPS.

Remarque

Dans une optique de mise en place de portail captif ou d'inspection de trafic web par un firewall, l'HSTS pose énormément de problèmes, car ces mécanismes reposent justement sur l'interception du trafic entre le client et le site web. Le renforcement de la sécurité sur les navigateurs, le durcissement des contraintes dans la génération d'un certificat TLS et les améliorations récentes autour du HSTS, deviennent alors contre-productives dans ces cas précis, et sont à l'origine de problèmes techniques rendant la navigation web impossible.

1.2 Mécanisme de sécurité de port ou port-security

Dans la section précédente était évoquée une attaque MiM sur un réseau local à partir d'une machine malveillante connectée sur le même segment réseau. Pourquoi ne pas endiguer une potentielle attaque en amont, en contrôlant les machines autorisées à se connecter sur un réseau local et donc un commutateur donné?

Une machine étant identifiée auprès d'un commutateur par son adresse MAC, il est en théorie possible de mettre en place un contrôle de l'adresse MAC source des en-têtes Ethernet des trames émises : c'est ce que l'on appelle un mécanisme de « sécurité de port » ou « port-security ».

La configuration du port-security nécessite que le commutateur de rattachement propose la fonctionnalité, sachant qu'il n'y a pas de normalisation et donc que l'implémentation est libre.

La fonction port-security est capable d'analyser les adresses MAC des machines connectées sur un port spécifique, d'autoriser ou non le raccordement d'une machine sur un port autre que celui sur lequel son adresse MAC a été préalablement déclarée, d'interdire des communications au-delà d'un certain nombre d'adresses MAC recensées sur un port donné. Enfin, le port-security peut lutter contre l'usurpation d'adresse MAC en interdisant la présence d'une même adresse MAC, sur des ports différents du commutateur à un instant T. L'application du port-security sur un commutateur suffit à empêcher l'attaque MiM évoquée précédemment.

Si les conditions imposées par le port-security pour un port donné sont violées (Cisco utilise le terme « violation de sécurité »), l'administrateur réseau est libre de choisir un comportement à adopter qui peut aller de la simple émission d'un message de journal (« message de log ») jusqu'à la désactivation totale du port.

Si le port-security permet d'autoriser une ou plusieurs adresses MAC spécifiques sur un port donné, il paraît relativement contraignant pour l'administrateur de configurer manuellement l'ensemble des adresses MAC des machines du réseau… Il est souvent possible de placer le switch dans un mode d'apprentissage dynamique où il va recenser l'ensemble des adresses MAC observées sur chaque port. L'administrateur décide alors de mettre fin à l'apprentissage au bout d'un certain temps, après une semaine de mise en production par exemple, tout en conservant les associations apprises dynamiquement. Cette fonction est référencée en tant que « sticky mode » sur Cisco et « auto-learn » chez HPe Aruba.

Exemple de configuration du port-security sur un commutateur Cisco :

```
! Mise en place de l'apprentissage automatique
Switch(config)#interface GigabitEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky

! Mise en place d'une restriction : 2 adresses Mac différentes
!peuvent se connecter. Désactivation du port en cas de violation
Switch(config)#interface GigabitEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security violation shutdown
```

1.3 Sécurité autour des mécanismes d'adressage IP

1.3.1 Adressage statique ou dynamique via DHCP

À partir d'un certain nombre d'actifs recensés sur un même réseau, la mise en place d'un adressage dynamique via un serveur DHCP paraît indispensable sous peine d'effectuer chaque configuration manuellement sur chaque actif et poste du réseau. Cependant, l'approche statique paraît indispensable pour des équipements tels que les serveurs, les routeurs, les commutateurs et finalement tous les équipements sur lesquels on est amené à se connecter explicitement. Le service DHCP est donc plutôt à déployer dans un contexte d'adressage de postes utilisateurs.

Certains administrateurs considèrent que la mise en place d'un adressage statique apporte une certaine sécurité, car il nécessite une configuration manuelle sur le poste de travail, configuration contrôlée et mise en place par l'administrateur réseau, là où un serveur DHCP aurait permis à la machine connectée d'obtenir une connectivité au réseau sans intervention de l'administrateur, et sans qu'il soit forcément averti.

Objectivement, cette approche devient faillible lorsque l'on prend en considération qu'il est relativement facile de récupérer les informations de connexion à un réseau, via une capture de trames par exemple, à partir de n'importe quel poste utilisateur raccordé à ce dernier (DHCP repose sur du broadcast). Rien n'empêche en effet, l'utilisateur, de configurer lui-même ces paramètres statiquement. C'est pour cela qu'un adressage IP statique généralisé dans un réseau ne peut être vu comme une mesure de sécurité, mais de commodité.

Outre la distribution des paramètres minimums obligatoires pour communiquer : adresse IP, masque, passerelle par défaut et serveurs DNS, l'utilisation d'un serveur DHCP se révèle fort utile pour assigner des paramètres précis à un type de machine spécifique. Un bail DHCP peut fournir jusqu'à 256 informations/options pour une machine donnée.

Dans le domaine de la TOIP, il est presque indispensable d'avoir recours à un serveur DHCP afin d'indiquer au téléphone son VLAN, son serveur de configuration ou de mise à jour et son IPBX de rattachement.

Dans un contexte d'infrastructure sans fil reposant sur des bornes Wi-Fi contrôlées, le DHCP est capable de leur indiquer au démarrage le contrôleur sur lequel elles doivent se rattacher.

Remarque

On trouve généralement le numéro d'option à définir pour une fonctionnalité donnée, ainsi que son formalisme (chaîne de caractères en ASCII ou en hexadécimal) dans la documentation du constructeur de l'équipement.

1.3.2 DHCP Snooping

L'intérêt du déploiement d'un ou plusieurs serveurs DHCP n'est plus à démontrer. Par contre, il faut prendre en compte le fait qu'il est tout à fait possible pour une machine connectée au réseau d'usurper le rôle du DHCP en distribuant des baux selon les paramètres de son choix. La documentation anglaise utilise le terme de « rogue DHCP server ».

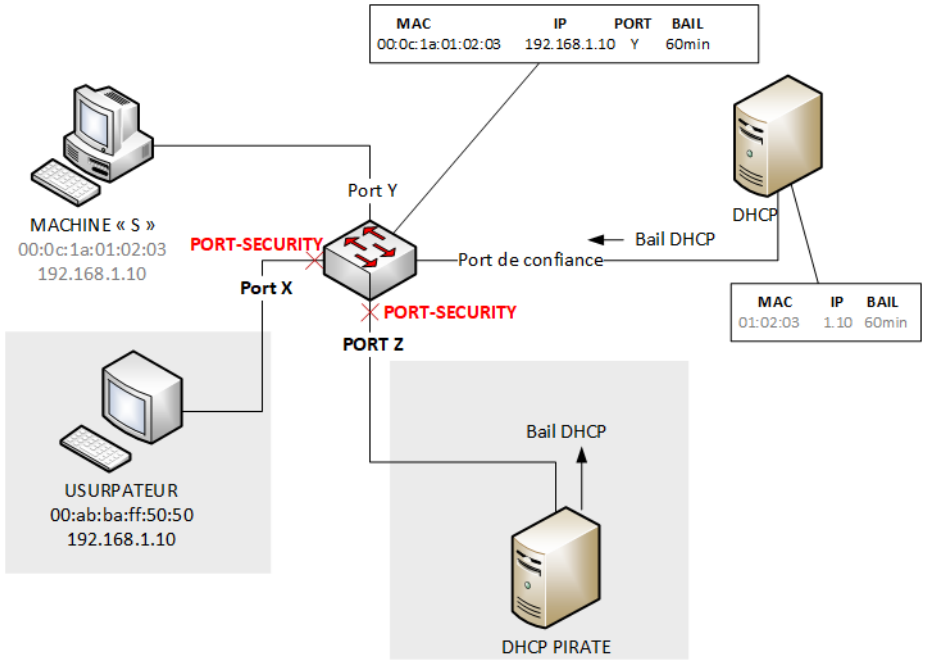
La facilité à configurer un serveur DHCP pirate et de le placer sur un réseau doit interpeller l'administrateur réseau. Ce dernier devrait impérativement mettre en place des mécanismes permettant de détecter ces équipements pirates et d'endiguer la distribution de baux falsifiés qui pourraient contenir par exemple, un serveur DNS ou un routeur contrôlé par le pirate dans le but d'intercepter les communications et/ou les rediriger vers des serveurs malicieux.

C'est pour cela qu'existe le « DHCP snooping », disponible directement sur les commutateurs. Il permet de détecter les serveurs pirates et de prémunir le réseau des paquets DHCP malicieux ou malformés.

Sa mise en place consiste à déclarer explicitement les serveurs DHCP dits de confiance en indiquant les ports du commutateur sur lesquels ils sont rattachés. Le commutateur construit alors une base de données sous la forme d'un fichier brut contenant les correspondances entre adresse IP assignée par le serveur DHCP de confiance et adresse MAC de la machine adressée. Sont enregistrés également la durée du bail, le VLAN de raccordement et le port de connexion. Le commutateur consulte la base et vérifie la conformité du contenu de chaque paquet DHCP circulant sur le réseau. Au besoin, il bloque certaines requêtes et désactive les ports sur lesquels il a détecté un serveur pirate, ou en tout cas, une machine émettant des requêtes qui ne correspondent pas à la logique du protocole par rapport aux entrées enregistrées dans la base.

Cette base peut être parallèlement utilisée également pour renforcer les mécanismes de sécurité déjà mis en place. On parle d'inspection ARP lorsqu'un commutateur analyse les requêtes ARP qui transitent. L'analyse du contenu des trames ARP, conjuguée aux informations contenues dans la base construite par le procédé de DHCP snooping, peut alors déclencher l'activation du port-security (cf. section sur le port-security).

Si le commutateur inspecte une trame ARP dont le contenu de l'en-tête Ethernet contient l'adresse MAC source : « MAC_S » émise à partir d'un port X, alors qu'un bail DHCP a été attribué à cette machine S par l'émission d'une trame sur le port Y et non X, alors le commutateur interprète cela comme une tentative d'usurpation d'adresse MAC.



Couplage de DHCP snooping avec inspection ARP sur un commutateur. Le switch bloque le port Z, car du trafic DHCP est détecté sur un port qui n'est pas de confiance. Le port X est bloqué, car le triplet adresse MAC/adresse IP/Port concerne déjà le port Y, l'usurpation d'adresse IP est empêchée.

Enfin, le DHCP snooping s'assure également que les machines utilisent bien l'adresse IP précédemment assignée via DHCP.

1.4 Politiques d'accès au réseau

1.4.1 Principe du NAC : Network Access Control

Les mécanismes permettant de contrôler les accès au réseau dès le niveau 2 Ethernet sont désignés génériquement comme procédés de contrôle d'accès au réseau ou NAC pour « *Network Access Control* ».

Le contrôle d'accès peut être effectué par :

- **une authentification basée naturellement sur l'adresse MAC** de la machine connectée s'appuyant sur les mécanismes explorés ci-dessus ;
- **une authentification effectuée via un portail web**, appelé portail captif. À la connexion, et une fois l'adresse IP assignée à la machine statiquement ou dynamiquement, l'utilisateur est invité par l'intermédiaire d'une page web à s'authentifier explicitement. Classiquement, l'authentification nécessite la vérification d'un couple login/mot de passe, mais on peut envisager d'autres mécanismes en supplément, comme la vérification de certificats TLS, ou un système de TOTP (*Time-based One Time Password*) par exemple, comme le propose l'application gratuite Google Authenticator : https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=fr
- **une authentification basée sur le standard ouvert 802.1X** qui représente la solution conseillée en termes de sécurité, mais également la plus lourde à gérer et à configurer. Cela suppose que le système d'exploitation de la machine cliente gère ce mécanisme (ce qui est le cas pour les systèmes Windows/Mac et Linux dans la majorité des versions), que le commutateur soit compatible et qu'un serveur contenant la base des utilisateurs existe.

1.4.2 Authentification 802.1x sur port de commutateur

802.1x désigne un modèle d'implémentation de mécanismes d'authentification sécurisés utilisés principalement dans le cadre d'un accès réseau par port de commutateur ou via une connexion sans-fil.

Le modèle identifie en détail les fonctions et le rôle de chaque entité logicielle et/ou matérielle qui vont intervenir dans le processus d'authentification, ainsi que les protocoles utilisés ou compatibles.

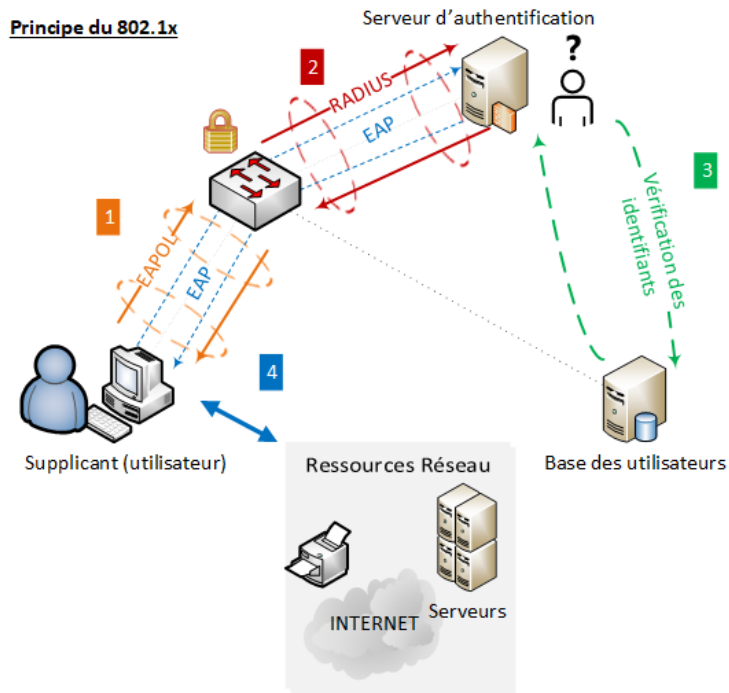
La machine à identifier est désignée comme le « supplicant ». Elle fournit ses identifiants à l'« authenticator » qui désigne l'équipement réseau d'accès comme le commutateur ou la borne Wi-Fi. L'authenticator joue le rôle d'intermédiaire entre le supplicant et le serveur d'authentification. Ce dernier utilise le protocole Radius, mais il existe des variantes comme le protocole propriétaire TACACS+. Le supplicant est vu comme client radius par le serveur d'authentification désigné aussi comme serveur.

Le serveur Radius peut se baser aussi bien sur un fichier texte, que sur une base de données déportée sur un autre serveur, voire même un serveur LDAP ou Active Directory. Il n'est pas rare également, que le serveur Radius soit directement intégré sur le supplicant.

– RFCs par rapport à 802.1x : https://1.ieee802.org/security/802-1x/

Le protocole utilisé pour assurer la communication entre les différents acteurs est EAP (*Extensible Authentification Protocol*), protocole de niveau 2. Il définit les champs de la trame EAP pour structurer les échanges et est capable ensuite de s'adapter à une multitude de méthodes d'authentification : il est donc extensible.

Le fichier C4_1_IdentificationEAP_capture.pcapng est disponible en téléchargement sur le site des Éditions ENI.



Accès au réseau via 802.1x et EAPOL. 1. Le client (supplicant) fournit ses informations d'authentification au commutateur (authenticator) 2&3. Ce dernier les transmet au serveur d'authentification (en général Radius). 4. Un tunnel EAP est alors monté, le client peut accéder aux ressources du réseau.

Remarque

De nombreuses variantes d'EAP ont vu le jour afin de s'adapter à des mécanismes spécifiques comme une authentification par carte SIM (EAP-SIM) dans le domaine de la téléphonie mobile. EAP peut être couplé à n'importe quel protocole de niveaux 1 et 2 comme PPP dans le cadre d'une authentification d'un abonné xDSL par son opérateur, par exemple.

802.1X offre de nombreux avantages comme la possibilité d'autoriser ou d'interdire une machine à émettre des trames sur un port donné. Après l'authentification, le périphérique utilisateur peut être placé dynamiquement dans un VLAN spécifique, permettant d'éviter une configuration classique de VLAN par port. Il est également possible de placer d'office le périphérique sur un

VLAN restreint « invité » avant authentification ou en cas d'échec d'authentification. Enfin, on peut utiliser 802.1x pour définir un ensemble de privilèges d'accès à un équipement ou à un service réseau en sus de l'étape d'authentification tout en journalisant ces accès.

Par exemple, on peut autoriser l'accès au management d'un équipement réseau via SSH tout en contrôlant les commandes qui pourront ensuite être exécutées sur l'équipement une fois connecté.

Remarque

L'ensemble des protocoles utilisés dans 802.1x permettent d'assurer trois fonctions de NAC désignées par le trio AAA : « Authentication, Authorization, Accounting », littéralement authentification, gestion des privilèges et traçabilité.

Configuration AAA sur Cisco 3750 :

```
SW_CISCO(config)# Aaa new-model
SW_CISCO(config)# Dot1x system-auth-control
# on définit une authentification basée sur radius
SW_CISCO(config)# Aaa authentication dot1x default group radius
SW_CISCO(config)# Radius-server host 10.1.10.10
SW_CISCO(config)# Radius-server key cle_radius
SW_CISCO(config)# Interface-range gi0/1/24
SW_CISCO(config-if)# Switchport mode access
SW_CISCO(config-if)# Dot1x port-control auto
```

Configuration AAA sur HP Procurve :

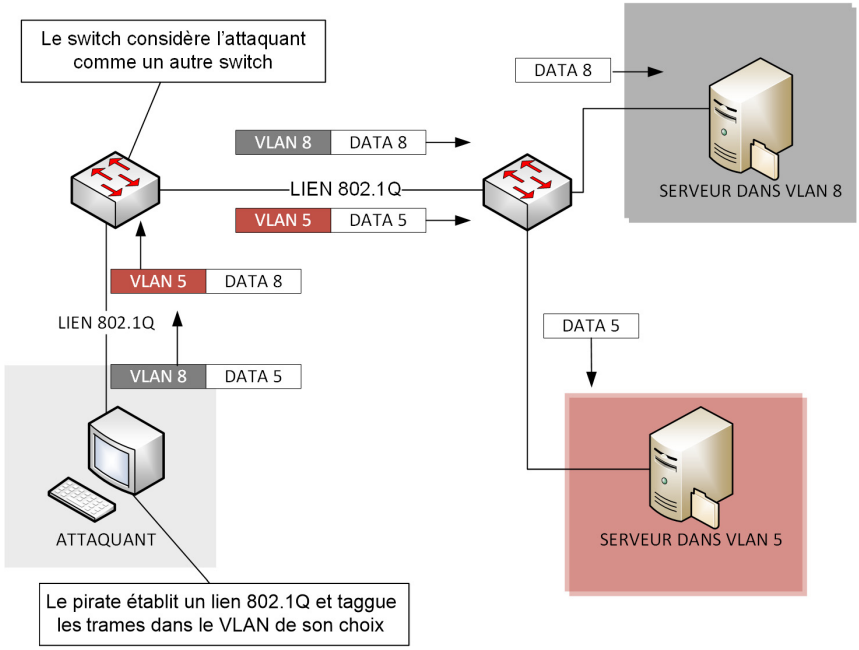
```
SW_HP(config)# radius-server host 10.1.10.10 key cle_radius
SW_HP(config)# aaa authentication port-access eap-radius
SW_HP(config)# aaa port-access authenticator A1-A24
SW_HP(config)# aaa port-access authenticator active
```

1.5 Saut de VLANs : hopping

On met généralement en place des VLANs dans un réseau local pour des raisons de sécurité. Cela permet d'isoler et de contrôler les communications entre les différents segments réseau correspondant aux VLANs (cf. chapitre Conception d'un réseau local - Segmentation réseau par la mise en place de VLANs).

Cependant, il faut prendre en compte qu'une mauvaise configuration peut permettre à un attaquant de contacter une machine, un serveur ou tout autre équipement actif situé dans un VLAN différent. Cette brèche porte le nom de « saut de vlan » ou « vlan hopping ».

Une première méthode consiste pour la machine attaquante à essayer de se faire passer pour un commutateur. Si un protocole de négociation automatique de lien 802.1Q comme DTP (*Dynamic Trunking Protocol*) est activé sur le switch de rattachement, l'attaquant peut être considéré comme un commutateur et monter un lien 802.1Q de son côté. Dans ce cas, il suffit alors à l'usurpateur de marquer les trames du VLAN de son choix pour pouvoir communiquer avec une machine appartenant à ce VLAN.



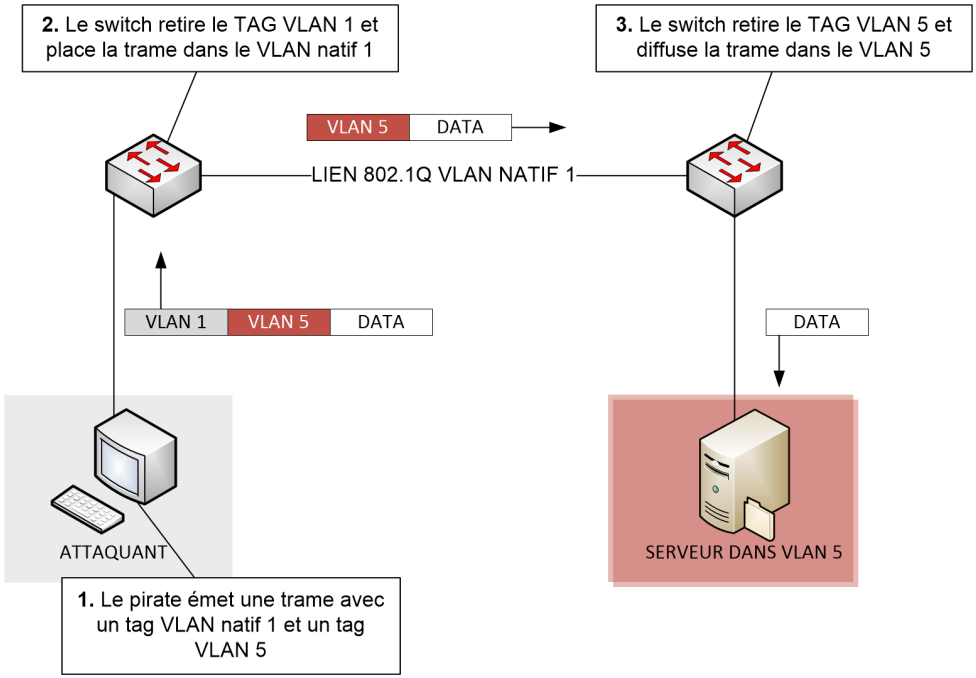
Saut de VLANs par usurpation de commutateur, l'attaquant peut communiquer avec tous les VLANs

Une deuxième technique est la méthode du « double tagging » reposant sur la notion de VLAN natif. Elle est possible si l'attaquant se trouve raccordé dans le VLAN natif qui est très souvent, rappelons-le, le VLAN par défaut. La seconde condition est que la machine avec laquelle il veut communiquer se trouve sur un autre commutateur lié par un lien 802.1Q avec le commutateur de rattachement.

Il est possible de marquer une trame Ethernet avec deux tags de VLANs selon le principe du QinQ (cf. chapitre Conception d'un réseau local - Conception avancée de réseau à partir de VLANs - La norme QuinQ ou 802.3ad). L'attaque consiste alors à générer des trames contenant un tag correspondant au VLAN natif dans lequel il se trouve (très souvent le VLAN 1) ainsi qu'un second tag désignant le VLAN avec lequel il souhaite communiquer.

Le comportement du commutateur de raccordement est alors le suivant : il enlève le premier tag, car le VLAN par défaut ne doit pas être balisé, ne le remplace donc pas et fait suivre la trame telle quelle, sur le lien 802.1Q avec le second commutateur. Ce dernier examine la trame entrante, constate qu'elle est marquée dans le VLAN ciblé (2e tag) et la diffuse alors dans le VLAN correspondant.

Notons cependant que l'attaquant ne recevra pas de réponse de la part de la machine visée, cette faille ne peut servir qu'à émettre des requêtes en broadcast.



Saut de VLANs par double tagging, l'attaquant arrive à envoyer des trames dans le VLAN 5 en étant connecté dans le VLAN 1

2. Les firewalls

2.1 Caractéristiques d'un firewall

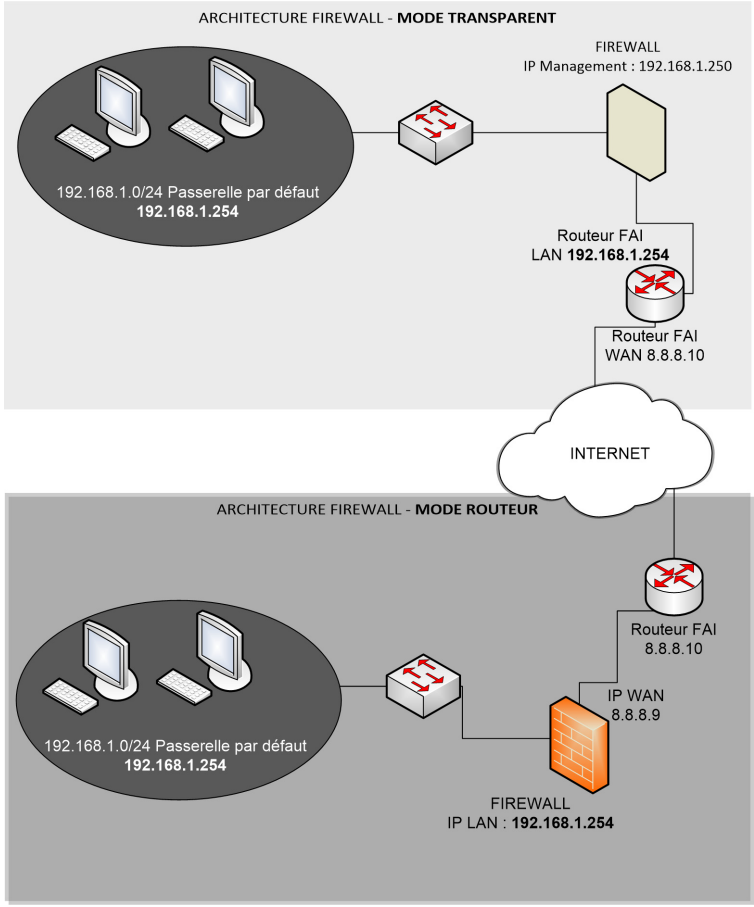
2.1.1 Fonction et positionnement dans un réseau

Un firewall ou pare-feu peut être logiciel ou matériel. Il désigne un actif dont le but est de contrôler les communications entre différents réseaux, ou, pour un firewall logiciel, contrôler les communications entre le système d'exploitation d'une machine et les autres équipements du réseau.

Le firewall logiciel est un programme installé sur un poste client, parfois intégré directement au sein du système d'exploitation d'une machine donnée. Il permet de mettre en place un premier niveau de sécurité en traitant l'ensemble des flux entrants et sortants sur la (ou les) carte réseau de la machine. Il est bien sûr possible de paramétrer finement les droits d'accès afin de n'autoriser que certains protocoles bien particuliers. On peut citer l'application Netfilter (commandes iptables) sous Linux ou sous Windows 10, le firewall du centre de sécurité : Windows Defender. Il existe bien sûr d'autres solutions commerciales où la fonction de firewall est intégrée à une solution d'antivirus.

Mais lorsqu'on utilise le terme firewall dans le domaine de l'administration réseau, on fait plutôt référence à un équipement dédié à la fonction, placé à un endroit stratégique du réseau, très souvent en lieu et place de la passerelle par défaut. En fait, un firewall est avant tout un routeur, car pour contrôler les flux et les communications entre tous les réseaux de la société et l'Internet, il faut forcément que ces flux transitent par ce dernier. C'est pourquoi la fonction de firewall est rarement dissociée de celle de routeur.

Dans certaines configurations spécifiques, il est possible de placer le firewall « en coupure » entre le commutateur et le routeur par défaut du réseau : on parle de mode transparent. Le firewall devient totalement passif en termes de routage, il n'est là que pour analyser les flux circulants, mais cela implique dans tous les cas que les flux à surveiller transitent par son biais.



Deux architectures pour un même réseau LAN avec un firewall en mode transparent puis en mode routeur

La gestion d'un firewall repose sur la définition de règles entre réseaux s'appliquant lorsqu'un flux qui transite correspond à une règle donnée. Sauf cas exceptionnels, toute communication ne correspondant pas à une règle est interdite d'accès. L'administrateur réseau, s'il veut être efficace, devrait raisonner dans une optique d'élaboration de règles devant cibler les flux à autoriser et non pas les flux à interdire.

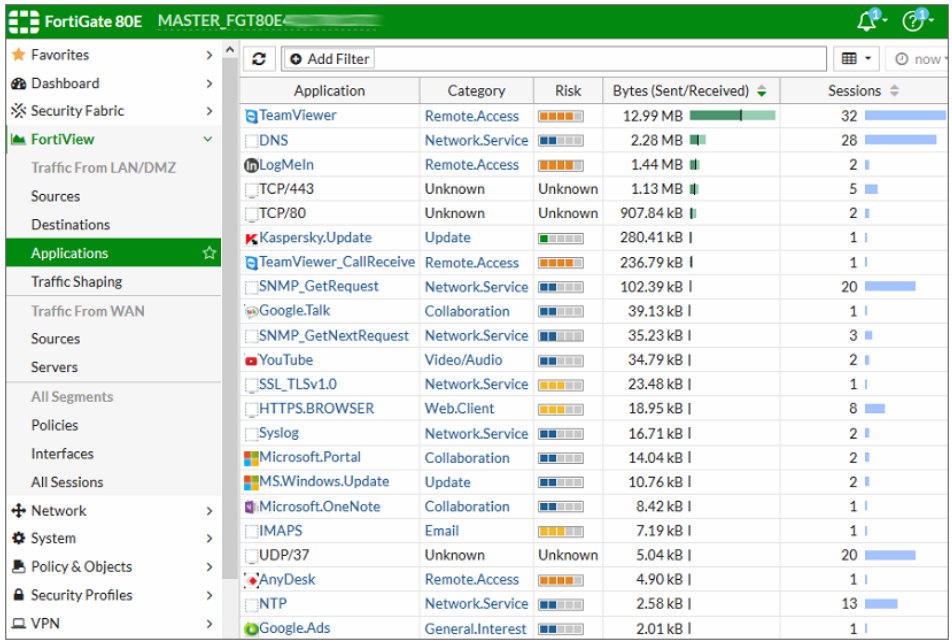
L'ordre des règles dans un firewall est aussi très important, car sa non-compréhension peut amener à des erreurs de configuration et donc des brèches de sécurité. Par rapport à un flux donné, les règles vont s'appliquer de haut en bas, sachant que la dernière est la règle générique d'interdiction s'appliquant dans tous les cas si aucune règle située en amont n'a été déclenchée. Autre élément important, une fois qu'une règle est déclenchée, les autres règles ne s'appliquent plus au flux. Les règles les plus spécifiques et restrictives sont généralement spécifiées en premier, les moins contraignantes en dernier : on autorise l'adresse IP 192.168.1.10 à sortir sur Internet (règle 1), **puis** on interdit le réseau 192.168.1.0/24 de communiquer avec l'extérieur (règle 2) et non l'inverse.

Le mécanisme décrit ici s'applique pour la majorité des constructeurs et éditeurs, mais il peut être adapté, modifié selon la propre décision de l'administrateur.

La fonction principale d'un firewall est d'analyser les paquets qui transitent. Cette analyse peut concerner seulement une partie des en-têtes du paquet : au minimum ceux de la couche réseau et transport. D'autres firewalls sont capables de remonter jusqu'à la couche applicative, voire même jusqu'aux données elles-mêmes pour une analyse beaucoup plus précise et une sécurité grandement renforcée, c'est d'ailleurs ce qui va influer dans le choix d'une solution de firewall et sur le coût du matériel en lui-même.

Pour schématiser, la majorité des solutions libres ou des solutions gratuites proposent un filtrage standard basé sur l'en-tête IP et l'en-tête au niveau transport. Il sera, par exemple, possible de filtrer une communication entre deux réseaux, LAN et Internet, et un autre réseau comme Internet, sur un port de destination particulier comme le port 80 HTTP.

Des solutions plus élaborées, souvent payantes, proposent ainsi un filtrage au niveau applicatif, permettant de détecter l'utilisation d'un protocole non habituel et/ou potentiellement malveillant. Pour revenir à l'exemple précédent, grâce à l'analyse applicative, nous pourrions filtrer une communication web qui contiendrait un script reconnu comme malveillant. Dans le contexte de sécurité actuel avec une cyberdélinquance qui s'est professionnalisée, et avec des menaces de plus en plus critiques et nombreuses, il est implicitement conseillé d'opter pour ce type de solution de pare-feu applicatif.



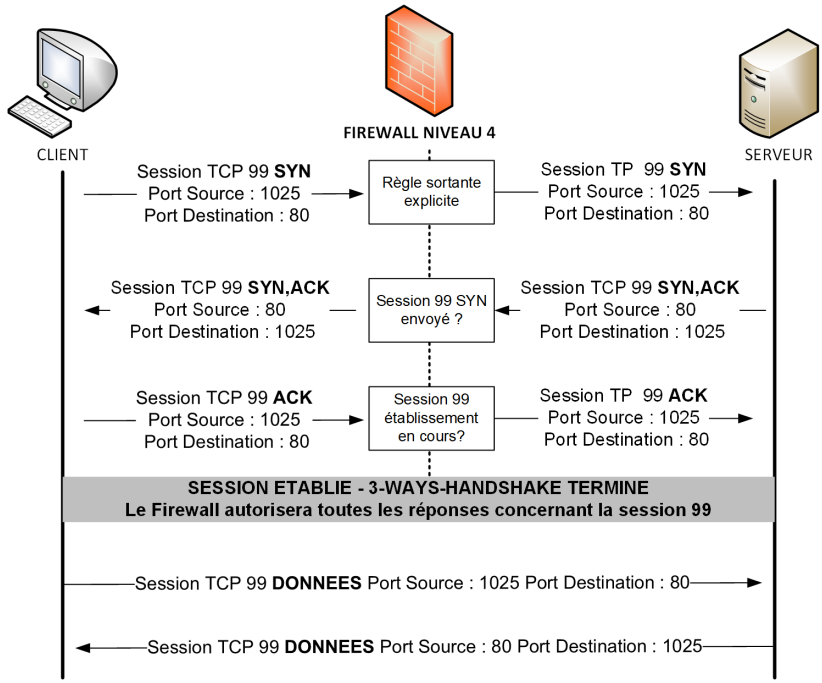
Reconnaissance applicative sur un firewall Fortigate 80E sous licences

2.1.2 Analyse jusqu'à la couche transport

Pour comprendre le fonctionnement d'un firewall, il est nécessaire de maîtriser le fonctionnement des protocoles de niveau transport UDP et TCP. Le but n'est pas ici d'être exhaustif dans la description de leur fonctionnement, mais de présenter les concepts qui permettent de mieux implémenter les règles.

L'élément le plus important à comprendre est qu'un firewall de niveau 4 agit véritablement au moment de la mise en place de la communication. Si celle-ci utilise le protocole TCP, ce qui sera le cas dans 95 % des cas, le firewall va analyser l'établissement de la communication en observant la séquence de « TCP 3-ways-handshake » (poignée de main en trois étapes).

En effet, le protocole TCP définit que pour s'échanger des données, deux participants doivent établir en premier lieu un canal de communication, donc une session. Les échanges correspondant à l'établissement de ce canal sont normalisés : l'émetteur envoie un paquet TCP avec un champ FLAG contenant la valeur « SYN », le destinataire à réception devra acquitter ce segment TCP en envoyant une réponse qui contiendra un champ FLAG « ACK » ainsi qu'une demande de synchronisation « SYN ». L'émetteur devra acquitter également la demande de synchronisation et ainsi commencera à envoyer les données. Cette séquence est appelée « 3-ways-TCP Handshake ». C'est sur cette dernière que le firewall agit, particulièrement dès le premier échange « SYN » : s'il veut interdire la communication, il lui suffit de bloquer ces segments TCP contenant le flag « SYN » pour un port de destination donné. Par exemple, si on veut bloquer la navigation internet via HTTP, le firewall interdira tous les paquets TCP SYN dont le port de destination est 80.



Séquence TCP-3 WAYS-HANDSHAKE avec firewall niveau 4 sans analyse applicative

À partir du moment où les segments d'établissement de session sont autorisés, le firewall autorisera alors tous les autres paquets de données sans avoir forcément besoin de les analyser. Ainsi, les règles de firewalls sont à définir selon le sens dans lequel est établie la communication : est-ce une communication établie de l'intérieur du réseau vers l'extérieur ou l'inverse? Selon le cas, ce ne seront pas les mêmes règles qui seront appliquées, et surtout, une règle permettant le 3-ways-handshake (SYN, SYN-ACK, ACK) pour un paquet sortant, autorisera implicitement tous les paquets entrants se référant à la même session sans qu'il ne soit donc nécessaire de mettre en place une autre règle supplémentaire qui autoriserait les flux retours. C'est l'erreur qui est commise par de nombreux administrateurs débutant dans l'administration de firewall.

Remarque

Le mécanisme décrit ci-dessus s'applique pour un firewall dit « stateful », c'est-à-dire capable d'examiner et de comprendre le mécanisme d'établissement de session. Il paraît nécessaire cependant de préciser qu'un firewall peut agir par défaut sans prendre en compte les sessions, il est ainsi classifié comme « stateless ». C'est le cas, par défaut, du très célèbre netfilter/conntrack, dont l'une des premières commandes « iptables » de configuration consiste en fait à lui faire adopter un comportement stateful…

Commande permettant de rendre un firewall Linux stateful :

```
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

Les firewalls modernes possèdent tous la capacité d'analyser des sessions TCP. La difficulté réside maintenant dans le traitement des protocoles sans état dit « connection-less » comme UDP ou ICMP. Pour traiter ce type de communication, le firewall est obligé de s'intéresser au numéro de session. Si un premier segment UDP a été émis et autorisé initialement, le firewall maintient une table où le numéro de la session est enregistré. Il doit cependant analyser tous les segments UDP reçus et consulter cette table pour être en mesure de déterminer si le segment est une réponse à une communication autorisée ou non.

Pour ICMP, dans le cas d'une réponse reçue à la suite d'une commande PING générée par une machine du réseau local vers un serveur situé sur Internet, le firewall va consulter sa table, à la recherche d'une entrée faisant référence à la requête ICMP Echo-request d'origine qui conditionnera l'autorisation de la réponse associée (ICMP Echo-reply).

Si cette table n'existait pas, il faudrait alors, pour une communication donnée, placer une règle dans le sens sortant puis une autre règle inversée dans le sens entrant. Le firewall perdrait également sa capacité à raisonner à l'échelle d'une session complète et traiterait les paquets de façon individuelle sans prendre en compte le contexte de la session complète.

2.1.3 Analyse jusqu'à la couche applicative

Un firewall peut agir jusqu'au niveau applicatif, c'est-à-dire qu'il va aller au-delà d'une simple analyse de l'en-tête IP et du numéro de port au niveau de la couche transport. Un firewall applicatif analyse le contenu des paquets dans leur intégralité et permet alors d'être beaucoup plus fin dans les autorisations.

Les protocoles applicatifs sont tous normalisés dans les documents officiels RFC. Une requête doit respecter un certain formalisme, contenir des champs avec des valeurs définies pour un protocole donné. Les réponses sont elles aussi normalisées de la même façon. Le firewall est capable d'interdire des paquets où les protocoles sont mal employés ou utilisés de façon frauduleuse. Par exemple, on pourra interdire dynamiquement une machine envoyant un nombre trop important de requêtes HTTP GET (demande d'une page web à un serveur) sur un laps de temps donné.

Pour aller plus loin, les éditeurs intègrent souvent un ensemble de signatures, un peu à la manière des éditeurs d'antivirus, qui définissent un contenu frauduleux pour une requête donnée. Ces signatures sont mises à jour régulièrement et permettent d'empêcher des attaques qui ont déjà été observées précédemment sur d'autres firewalls. On s'approche ici du concept d'outils de prévention et de détection d'intrusions : IPS et IDS qui fournissent justement ce type de capacité. La fonction IDS a pour rôle de comparer le contenu d'un paquet applicatif à une base de signatures et ainsi de bloquer le paquet selon le résultat de la comparaison. L'efficacité de l'analyse applicative dépend alors de la présence de signatures à jour, définissant les dernières attaques observées pour un protocole donné.

Comment sont définies les signatures utilisées par les systèmes d'IDS des firewalls ?

La majorité des systèmes se basent sur la définition d'expressions régulières correspondant à une chaîne de caractères spécifique, inhabituelle, unique, permettant de conclure à un type d'attaque préalablement observée. Il faut donc que l'attaque ait déjà eu lieu et qu'elle ait été capturée et analysée. Les éditeurs de firewall se basent souvent sur les bases CVE (*Common Vulnerabilities and Exposures*) publiques. Dans ces bases de données sont recensées les failles de sécurité observées sur des applications ou des protocoles précis et sont décrits le mode d'attaque utilisé, le contenu ou le code de la requête utilisée pour l'attaque (on parle d'exploit) et la criticité en cas d'exploitation.

– http://cve.mitre.org

La signature devra donc capturer le contenu du paquet qui contiendrait la requête frauduleuse ou même le code de l'exploit recensé. Les bases CVE sont publiques, mais les éditeurs constituent également leur propre base de signatures.

– https://fortiguard.com/updates/ips

Remarque

Certains systèmes de détection d'intrusions possèdent la capacité d'analyse probabiliste et statistique, en supplément de l'analyse statique basée sur des signatures.

2.2 Les solutions du marché et comment faire son choix

2.2.1 Solutions commerciales NGFW (Next Generation Firewall)

Le marché de la sécurité est en pleine expansion depuis une dizaine d'années. Les firewalls matériels sont vendus sous la forme de boîtiers appelés appliances de sécurité UTM (*Unified Threat Management)*.

Le terme UTM désigne en fait des fonctions supplémentaires, notamment l'analyse applicative (« deep packet inspection »), que n'assuraient pas les pare-feux traditionnels.

Le cabinet américain Gartner utilise maintenant le terme de NGFW pour désigner des firewalls de nouvelle génération.

– https://www.gartner.com

En fait, un NGFW comporte des fonctions supplémentaires avancées comme un IDS, un IPS, la possibilité de faire du filtrage d'URL, de l'analyse antivirale et antispam, voire même de l'inspection avancée dédiée aux protocoles du Web (on parle alors de WAF : *Web Application Firewall*).

Précisons que ces fonctionnalités étaient disponibles sur de nombreux firewalls bien avant que le terme NGFW, qui reste un terme commercial au final, n'ait été choisi.

– https://www.esecurityplanet.com/products/top-ngfw-vendors.html#features

Le marché du firewall a connu une croissance à deux chiffres en 2017/2018, les prévisions pour 2022 sont de l'ordre d'une hausse des ventes allant en volume jusqu'à 20 %. Ce marché est fortement concurrentiel, mais quelques acteurs se détachent par l'efficacité de leurs produits et leur facilité de gestion.

– https://www.statista.com/statistics/235347/global-security-appliance-revenue-market-share-by-vendors/

Selon le cabinet Gartner, les acteurs proposant les solutions les plus intéressantes en termes d'innovation et de maturité sont Fortinet, Checkpoint, Cisco et Palo Alto. Checkpoint et Palo Alto ont fondé leur réputation notamment par rapport à leur expertise dans l'analyse applicative.

Sur le marché français, dans le milieu de gamme on rencontre souvent l'américain Fortinet très bien implanté ainsi que Stormshield, née de la fusion des sociétés françaises Netasq et Arkoon rachetées en 2013 par Airbus, qui s'impose comme leader européen. Cisco avec sa gamme ASA est bien sûr présent, mais positionné davantage sur du haut de gamme.

L'objectif de cet ouvrage n'est pas de prendre parti pour un constructeur, mais d'aider au choix d'une solution efficace et surtout adaptée à un besoin précis. Tous ces constructeurs assurent un niveau de sécurité satisfaisant lorsque leurs modèles sont bien configurés et surtout adaptés au réseau sur lequel ils sont déployés. La différence se fera majoritairement en termes de coût logiciel et matériel, de reporting, ainsi que de facilité de gestion au quotidien, notamment en ce qui concerne le dépannage. C'est d'ailleurs sur ce dernier point que Fortinet a fondé sa réputation initiale, au point d'être considéré comme le leader par le cabinet Gartner.

Date/Time	Source	Destination	Application Name
19:18:45	user0020 90:b9:31:c	208.91.112.53 (fortinet-public-dns-53.fortinet.com)	Fortinet-FortiGuard
19:17:51	user0028 fc:c2:de:4	31.13.67.11 (edge-mqtt.facebook.com)	Facebook-Web
19:16:32	192.168.2.55	8.8.8.8 (google-public-dns-a.google.com)	Google-DNS
19:13:46	user0037 iPhonedsalaulu	208.91.112.53 (fortinet-public-dns-53.fortinet.com)	Fortinet-FortiGuard
19:13:45	user0037 iPhonedsaroulou	208.91.112.53 (fortinet-public-dns-53.fortinet.com)	Fortinet-FortiGuard
19:13:15	user0020 90:b9:31:	208.91.112.53 (fortinet-public-dns-53.fortinet.com)	Fortinet-FortiGuard
19:10:52	user0028 fc:c2:de:	35.190.35.114 (api.infomobi.me)	Google-Google.Cloud
19:10:48	user0028 fc:c2:de:	35.190.35.114 (api.infomobi.me)	Google-Google.Cloud
19:09:20	user0028 fc:c2:de:	88.221.83.33 (dm16.byteoversea.com)	HTTPS
19:09:19	user0028 fc:c2:de:	184.50.88.73 (dm16.byteoversea.com)	Splunk-Web
19:09:18	user0028 fc:c2:de:	88.221.83.33 (dm16.byteoversea.com)	HTTP
19:09:18	user0028 fc:c2:de:	184.50.88.73 (dm16.byteoversea.com)	Splunk-Web
19:08:52	user0028 fc:c2:de:	172.217.6.238 (plus.l.google.com)	Google-Gmail
19:08:32	user0028 fc:c2:de:	172.217.3.106 (oauthaccountmanager.googleapis.com)	Google-Gmail
19:08:20	user0028 fc:c2:de:	172.217.18.206 (clients.l.google.com)	Google-Gmail
19:08:20	user0028 fc:c2:de:	172.217.18.206 (clients.l.google.com)	Google-Gmail
19:08:16	user0028 fc:c2:de:	172.217.18.206 (clients.l.google.com)	Google-Gmail
19:08:05	user0028 fc:c2:de:	13.32.158.157 (d2k03kvdk5cku0.cloudfront.net)	Amazon-Web
19:08:05	user0028 fc:c2:de:	13.32.158.157 (d2k03kvdk5cku0.cloudfront.net)	Amazon-Web
19:07:00	user0029 34:de:1a:6	208.91.112.53 (fortinet-public-dns-53.fortinet.com)	Fortinet-FortiGuard
19:07:00	user0029 34:de:1a:6	8.8.8.8 (google-public-dns-a.google.com)	Google-DNS
19:06:59	PC-QUINTERNET	8.8.8.8 (google-public-dns-a.google.com)	Google-DNS
19:06:59	PC-QUINTERNET	208.91.112.53 (fortinet-public-dns-53.fortinet.com)	Fortinet-FortiGuard
19:06:00	user0028 fc:c2:de:	99.84.181.46 (xlog.byteoversea.com)	LogMeIn-GoTo.Suite

Monitoring live de sessions d'un pare-feu fortigate concernant un accès Wi-Fi invité (authentification préalable sur un portail captif)

– https://www.fortinet.com/

– https://www.stormshield.com/

Ces firewalls sont administrables via une interface web couplée à un accès console SSH pour l'activation de fonctions très avancées.

2.2.2 Solutions libres

Dans le monde du libre, on retrouve le paquet « Netfilter/Conntrack/iptables » qui a été développé pour un système basé sur un noyau Linux. La distribution FreeBSD propose, quant à elle, le paquet « Packet Filter » qui est optimisé pour une approche de matériel embarqué.

Ainsi, Netfilter peut s'employer en tant que pare-feu logiciel installé sur une machine Linux spécifique à protéger. Son concurrent direct, Packet Filter, a été packagé au sein de la solution PfSense, relativement connue, qui propose un fonctionnement plus proche de celui des NGFW destinés à protéger l'intégralité du réseau. La distribution PfSense est portée par la société Netgate qui commercialise du support sur le produit, du service de déploiement dans le cloud et propose désormais des fonctions additionnelles, parfois payantes, comme de l'IDS/IPS ou du filtrage d'URL.

– https://www.pfsense.org/

On retrouve aujourd'hui dans les solutions libres les fonctions de base d'un firewall qui se cantonne globalement à une analyse des paquets jusqu'au niveau transport parfois au niveau applicatif pour certains protocoles (Filtrage d'URL, par exemple).

Cependant, les capacités d'un pare-feu à mettre à jour en temps quasi réel sa base antivirale et sa base de signatures applicatives, le haut niveau d'expertise des chercheurs en sécurité notamment dans la définition des signatures applicatives et dans la reconnaissance non plus d'un protocole isolé, mais d'une infinité d'entre eux, n'existent pas dans le monde du libre.

Quand on opte pour une solution commerciale, le choix du produit ne se fait plus tellement sur les fonctionnalités traditionnelles d'un firewall, mais sur l'expertise et également la réputation du centre de recherches en sécurité du constructeur. La vision traditionnelle originale du firewall, qui consistait à la mise en place d'un équipement utilisé dans le but d'autoriser ou bloquer des ports, est largement dépassée et surtout insuffisante. D'ailleurs, le modèle économique des constructeurs d'appliance n'est pas de vendre du matériel, mais de vendre les licences associées, permettant d'accéder à toutes les fonctionnalités supplémentaires qui en font des NGFW, équipements indispensables aujourd'hui.

2.2.3 Critères de choix et métriques

Le processus d'avant-vente d'une solution de firewall devrait commencer par une évaluation du nombre de personnes qui utilisent le réseau de la société, soit pour accéder à Internet, soit pour accéder à d'autres réseaux ou VLANs dans la société.

Si possible, des statistiques ou des graphiques relatant les débits enregistrés sur les interfaces de l'équipement à remplacer (routeur existant) ou sur le routeur d'accès au WAN (routeur FAI) peuvent donner une idée précise des caractéristiques que doit posséder impérativement le nouvel équipement (cf. chapitre Métrologie et mesure de performances, section Mesure de débit et optimisation).

Finalement, il s'agit d'évaluer le débit et si possible le nombre de sessions simultanées (à mettre en corrélation avec le nombre d'utilisateurs potentiels) que devra traiter le futur firewall.

Les documentations techniques des constructeurs comportent un certain nombre de métriques. Voici un tableau énumérant celles qui permettent d'évaluer et de comparer différents modèles :

MÉTRIQUE	UNITÉ	COMMENTAIRE
Bande passante globale du firewall	Mégabits par seconde ou nombre de paquets par secondes	Exprime la capacité de routage du firewall sans fonctions de filtrage.
Latence induite par le firewall	Millisecondes	Temps supplémentaire induit par le traitement du paquet.
Nombre de sessions simultanées		Dépend du nombre d'applicatifs différents utilisés et du nombre d'utilisateurs.
Nombre de nouvelles sessions par seconde		Variable à considérer lors de mises à jour, de sauvegardes ou d'événements ponctuels nécessitant un besoin soudain en ressources.

MÉTRIQUE	UNITÉ	COMMENTAIRE
Bande passante VPN IPsec ou SSL maximum	Mégabits par seconde	Bande passante maximum atteignable pour une connexion VPN site à site ou nomade.
Bande passante avec fonctions NGFW	Mégabits par seconde ou nombre de paquets par secondes	Capacités de traitement du firewall lorsque les fonctions avancées sont activées dont l'inspection de paquets, l'analyse applicative et les fonctions antivirus.
Capacité de clustering		Capacité de load-balancing et de haute disponibilité au niveau de l'équipement et au niveau des interfaces réseau, dont les accès WAN.
Interface de monitoring et de configuration		Connexion HTTP/HTTPS de management, accès console, compatibilité avec les protocoles de supervision, tableau de bord des sessions en temps réel.
Gestion des logs		Déportation des logs sur un serveur externe, génération de rapports automatisée, conservation des fichiers localement.

Même s'il est parfois difficile de comparer les valeurs indiquées sans disposer de valeurs références, ce tableau permettra au minimum de comparer une appliance par rapport à une autre.

Pour finir, voici quelques conseils ou précisions :

- Il n'est pas obligatoire d'activer les fonctions de NGFW pour tous les flux à surveiller : cela sera le cas pour les échanges avec Internet, mais très rarement entre des VLANs.
- Le filtrage d'URL est assez consommateur en ressources et très contraignant en administration, il paraît évident de ne l'activer que pour des postes de travail navigant sur le Web (pas forcément pour des serveurs).
- L'analyse de contenu SSL nécessite une interception des flux par le firewall le plaçant alors dans une position de Man-in-the-Middle. Cette position amène à des problématiques au niveau du navigateur client (cf. section Les faiblesses du protocole ARP de ce chapitre).
- Dans une optique de firewall permettant principalement l'accès à Internet, il est raisonnable de penser que le débit à router n'atteindra rarement plus de 1 Gb/s. En effet, on est dans tous les cas limité par le débit de l'accès internet proposé par le FAI. Si le firewall est cependant utilisé pour du routage inter-VLANs, on se référera au débit maximum apporté par les commutateurs de notre réseau local : attention notamment aux interfaces 10 Gbits/s.
- Le nombre de sessions étant difficile à évaluer, il est impératif de raisonner en termes d'utilisateurs simultanés, en prenant également les autres actifs tels que les serveurs ou tout autre périphérique n'entrant pas dans la catégorie des postes de travail notamment les périphériques mobiles comme les tablettes.
- Le débit étant variable au cours du temps, il est préférable de faire ses calculs sur des périodes d'activité intense ; attention à la récupération des e-mails le matin, aux mises à jour des systèmes d'exploitation, à la consultation des médias de divertissement très consommateurs lors des pauses.

Remarque

Le filtrage d'URL et de contenu, et plus largement l'ensemble des journaux de connexions récoltés sur l'équipement, sont considérés à juste titre comme un traitement de données personnelles, entrant dans le cadre du RGPD (cf. chapitre Autres protocoles de supervision réseau, section Enjeux de la journalisation des événements).

2.2.4 Firewall matériel ou virtuel?

Pour des raisons qui dépassent de plus en plus le cadre technique et qui peuvent être justifiées parfois à tort par une politique de baisse des coûts ou pire par un effet de mode, des sociétés considèrent que la fonction informatique doit être déportée dans le cloud. Par rapport à ce besoin, les constructeurs ont travaillé sur du matériel pouvant s'adapter facilement aux contextes des fournisseurs de cloud et autres sociétés de gestion des datacenters.

Il est rapidement devenu évident de porter le système d'exploitation fonctionnant sur les appliances, sur des architectures x86 sous la forme de machines virtuelles. La maturité des hyperviseurs, les progrès dans la gestion du réseau ont renforcé cette tendance (cf. chapitre Une nouvelle approche du réseau SDN et NFV, section Virtualisation du réseau). Ainsi, la majorité des constructeurs d'appliances de sécurité proposent également leur produit sous la forme de machine virtuelle à exécuter au sein d'une infrastructure virtuelle hébergée en datacenter ou localement.

Certains constructeurs poussent leurs clients à adopter ce type de solution en les orientant vers un hébergement à l'extérieur, opéré par leur soin, et facturé alors mensuellement comme un service. Si le client possède déjà une infrastructure virtuelle, il paraît intéressant d'opter pour ce type de solution (hébergée localement ou à l'extérieur).

D'autres constructeurs possèdent dans leur catalogue ce type de solution, mais préfèrent mettre en avant leur gamme matérielle pour des raisons de performances. En effet, les processeurs embarqués dans les appliances sont conçus et dédiés à réaliser un certain type de tâches spécifiques, en l'occurrence ici le routage, la commutation et l'analyse des paquets. On parle d'ASIC pour « *Application-Specific Integrated Circuits* ». Ces puces sont beaucoup plus adaptées pour traiter de nombreux paquets simultanément.

La limite ne se situe pas au niveau de la cadence du processeur, mais plutôt au nombre d'événements, plus précisément d'interruptions, que peut gérer le processeur par seconde. Un processeur x86 classique est plus adapté pour exécuter une centaine de processus différents nécessitant des calculs complexes, que pour traiter une centaine de petits processus, relativement basiques, mais devant être traités simultanément et générant alors énormément d'interruptions. Les interruptions représentent ici des accès constants au matériel et précisément aux cartes réseau. Pendant un temps, le goulot d'étranglement s'est même situé directement au niveau du débit du bus de la carte mère.

Pour ces raisons, l'industrie travaille plutôt sur des processeurs ASIC ou des processeurs développés spécifiquement pour des opérations très précises et répétitives. On retrouve notamment ces considérations dans le monde de la commutation (cf. chapitre Gestion des actifs et haute disponibilité, section Capacités de commutation d'un commutateur).

On peut prendre comme exemple la société Fortinet qui conçoit ses appliances en utilisant plusieurs circuits dédiés, séparés et spécifiquement développés selon les fonctions de traitement des paquets, de gestion des règles, et d'inspection de contenu.

– https://www.fortinet.com/products/fortigate/fortiasic.html

Mais les progrès dans le développement, l'ouverture des APIs, l'émergence de la virtualisation et des réseaux virtuels SDN (*Software Defined Network*) (cf. chapitre Une nouvelle approche du réseau : SDN et NFV, section Approche du SDN) entraînent forcément une dynamique vers la généralisation des architectures x86 pour du matériel réseau.

Certains constructeurs repensent leur modèle économique notamment lorsqu'ils prennent en compte les avantages de gérer des grandes quantités de mémoire fournies par les serveurs x86 actuels. En effet, le point faible des architectures embarquées, en tout cas pour ce qui concerne les équipements réseau, réside dans les coûts de fabrication de leur mémoire spécifique. De plus, ils pourraient bénéficier des économies d'échelles engendrées par la généralisation des processeurs x86 dans le monde de l'informatique ; un circuit dédié revient cher à produire, lorsque l'on considère les coûts de recherche nécessaires au développement du composant.

2.3 Tester son firewall

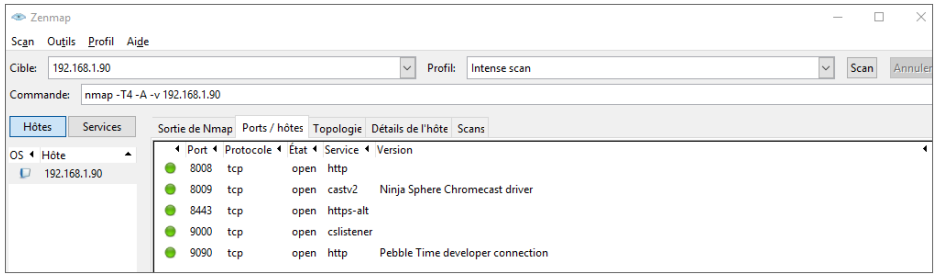
Tester une configuration de firewall en se mettant dans les conditions d'une machine dans le réseau à protéger semble intéressant pour s'assurer de la logique et du bon ordonnancement des règles de sécurité mises en place.

Avant toute chose, il est relativement difficile de tester l'analyse applicative d'un firewall et ces tests ne pourront de toute façon pas être exhaustifs au vu de leur envergure. Pour les réaliser, on devra s'appuyer sur des outils permettant de générer des types d'attaques connus : les scanners de vulnérabilités. Cependant, la probité des tests reste bien trop dépendante de la qualité du logiciel utilisé et on est amené à fabriquer son propre outil de génération de paquet. On peut citer l'outil open source OpenVAS successeur du très célèbre Nessus v2 qui est maintenant un outil propriétaire de la société Tenable. Citons également des outils efficaces orientés vulnérabilités web comme Acunetix et toute la gamme proposée par la société Qualys.

– https://www.qualys.com
– https://www.acunetix.com
– https://www.tenable.com/products/nessus/nessus-professional
– http://www.openvas.org/

Par contre, il est beaucoup plus facile de tester les fonctions basiques comme le potentiel blocage des communications sur un port donné, c'est-à-dire les fonctions de niveau 3 et 4 du modèle OSI. Pour cela, on utilise des scanners de ports dont le principe est relativement simple : générer une demande de synchronisation TCP-SYN et observer la réponse du correspondant. En général, un firewall bloquant la session, renverra alors lui-même une réponse TCP-RST (reset de la connexion), voire rien du tout et la session expirera. Les outils de scan de ports reposent sur ce principe. Inutile d'investir dans des solutions commerciales pour des tests de ce niveau, l'outil libre reconnu par la communauté comme étant le plus efficace est nmap et sa version graphique Windows ZenMap.

Le fichier C4_2_SCAN_TCP_capture.pcapng est disponible en téléchargement sur le site des Éditions ENI.

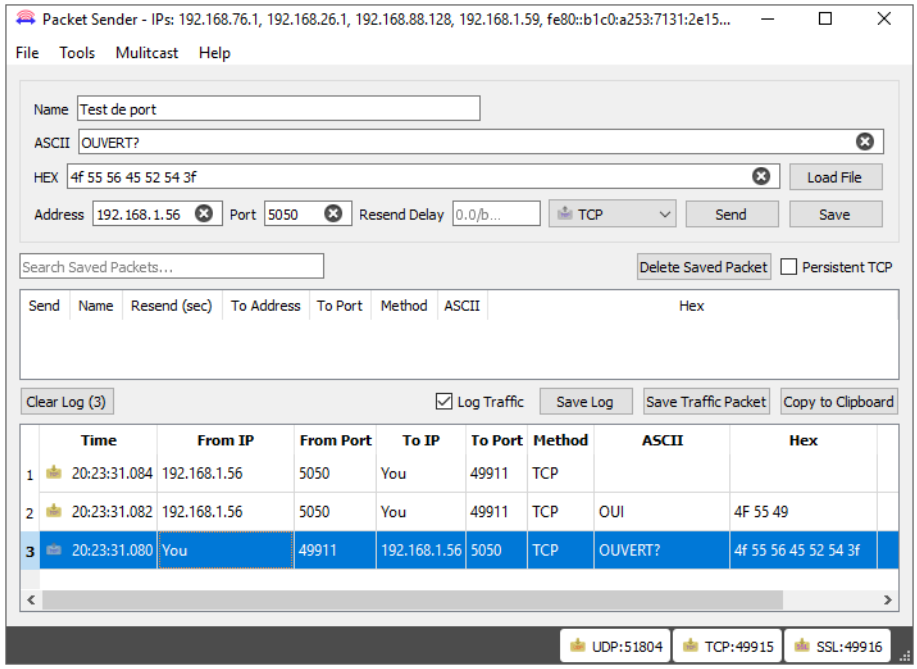


Scan d'une box TV Android avec Zenmap

– https://nmap.org/

Enfin, il existe des outils permettant de générer des paquets avec le contenu de notre choix tout en choisissant ports et protocoles. Packet Sender est une application gratuite permettant ce type de tests, multiplateforme et plutôt simple à prendre en main. De plus, elle peut fonctionner en mode client/serveur : en la plaçant, d'un côté, en écoute sur un port précis et en paramétrant un message de retour selon ce que l'application cliente envoie, et de l'autre, en se substituant à l'application cliente en forgeant la requête de notre choix. Le principe est d'installer client et serveurs dans un contexte où les flux transitent forcément via le firewall pour tester ce dernier.

– https://packetsender.com



Application Packet Sender - envoi d'une chaîne de caractères à destination de l'IP 192.168.1.56 sur le port TCP/5050, une réponse est bien reçue, le port est donc ouvert

3. Les attaques de déni de service

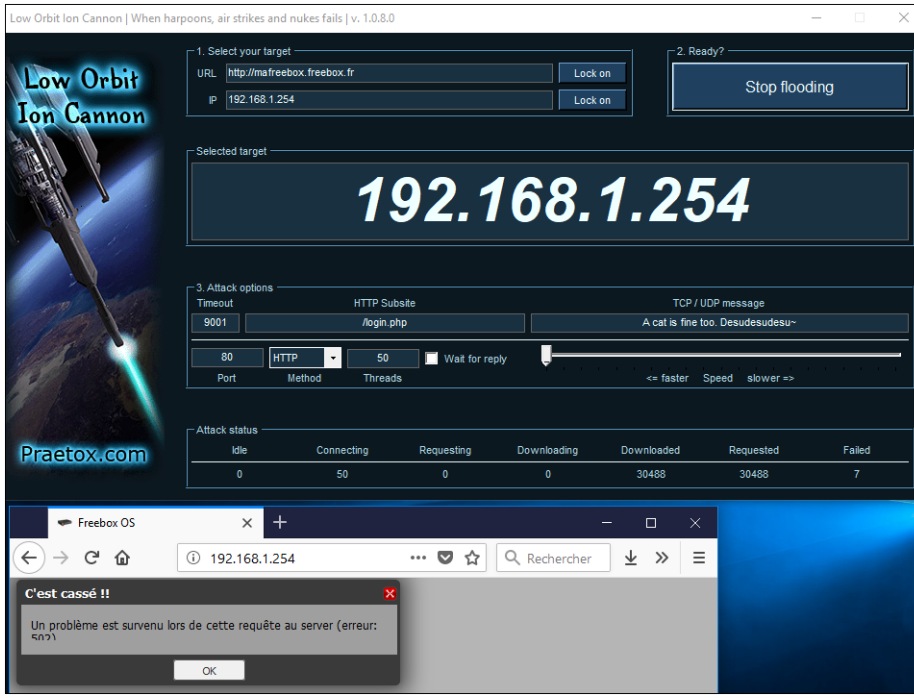
3.1 Principe de l'attaque

Un déni de service est caractérisé par le fait de remplir une zone de stockage ou un canal de communication jusqu'à arriver à une utilisation dégradée ou impossible du service. L'attaque de déni de service est en principe ciblée et consiste le plus souvent à transmettre des requêtes que la cible ne peut pas traiter. Dans ce cas, la cible ne peut pas non plus répondre aux requêtes légitimes, le service assuré habituellement devient alors indisponible.

L'attaque peut se concevoir par l'envoi de requêtes complexes suffisamment nombreuses pour saturer le processeur de la victime. On peut également faire en sorte de saturer la mémoire RAM de la cible lorsque l'on multiplie le nombre de requêtes même très simples, mais qui utiliseront chacune un fragment de RAM réservé. Enfin, l'attaque peut porter directement sur la saturation du lien réseau permettant l'accès à la cible. Dans ce cas-là, on peut cibler un réseau entier.

Dans les années 1990, il était possible de saturer un serveur tout simplement par un envoi massif de requêtes « ping ». Désormais, on ciblera un service particulier, une application spécifique, plutôt que le serveur dans sa globalité. Au niveau réseau, une attaque classique consiste à saturer la pile TCP/IP du système d'exploitation de la machine ciblée par l'envoi de nombreuses demandes de synchronisation TCP-SYN. À réception de ces requêtes, la cible crée un processus pour traiter l'envoi de données qui devrait suivre au niveau de l'application ou du service visé et ouvre un « socket », c'est-à-dire un processus en attente de données sur le port ciblé. Cette attaque porte le nom de « SYN-Flooding ».

Ce type d'attaque est à la portée de n'importe qui puisqu'il existe des utilitaires en libre téléchargement permettant de les réaliser. Le groupe anonymous est à l'origine du développement du logiciel LOIC qu'il a distribué massivement à tous ses membres : il suffit de paramétrer l'adresse IP de la cible et de cliquer sur un bouton pour lancer le « flooding ».



Attaque de déni de service HTTP sur une Freebox avec le logiciel LOIC - La page d'administration web ne répond plus pendant l'attaque

Il existe d'autres outils ciblant précisément des applications ou des services spécifiques qui peuvent être utilisés pour une attaque, mais aussi pour des tests de montées en charge sur des applications ou des serveurs. La commande `ab` sur Linux pour « Apache Benchmark » permet par exemple de générer des requêtes web HTTP sur un serveur afin d'évaluer le nombre maximum de requêtes qu'il peut traiter. Évidemment, il convient à l'administrateur réseau de choisir les requêtes les plus consommatrices en termes de ressources pour effectuer ces tests : formulaires de recherche de mots clés afin de générer de nombreuses requêtes en base de données, affichage de pages hébergeant du contenu multimédia fort consommateur de bande passante, etc.

Remarque

Toute attaque (ou test) de déni de service perpétrée sans autorisation explicite du propriétaire du service est formellement punie par la loi.

3.2 Dénis de services distribués

Une attaque par déni de service a peu de chances de réussir si elle est à l'origine d'une machine unique. De plus, elle est très facilement repérable et donc aisément maîtrisable. L'idée est donc d'une part d'utiliser plusieurs machines attaquantes pour multiplier le nombre de requêtes envoyées sur la cible et d'autre part, brouiller plus facilement les cartes : en effet, il est facile de bloquer du trafic entrant en provenance d'une source unique (une seule adresse IP), que de bloquer des milliers de connexions simultanées en provenance d'adresses IP et de lieux différents… Faire la distinction entre trafic légitime et trafic correspondant à l'attaque devient très difficile, voire impossible.

Ce type d'attaques appelé « DDos » (*Distributed Denial of Service*) semble aujourd'hui incontestablement représenter une menace critique, car elles nécessitent la mise en place de matériels et de logiciels très spécifiques, notamment en termes d'intelligence artificielle, que seuls les gros hébergeurs et opérateurs peuvent et doivent financièrement se permettre.

À ce jour, l'attaque la plus importante en termes de débit mesuré a été enregistrée sur les serveurs de GitHub le 29 février 2018 avec un débit de plus de 1.35 Tbits/s ! Pour arriver à un tel flot de données, les attaquants ont dans un premier temps utilisé environ 5 500 serveurs memcached (serveurs de cache de contenu web) à qui ils ont envoyé des requêtes de taille très modeste, en falsifiant les adresses IP sources par celles des serveurs cibles de GitHub. En y répondant, les serveurs memcached ont envoyé des requêtes en réponse d'une taille 50 000 fois supérieure, et à destination des serveurs GitHub, ce qui paralysa complètement les serveurs pendant cinq minutes.

– https://githubengineering.com/ddos-incident-report/

En septembre 2016, l'hébergeur français OVH (leader du marché européen d'hébergement) a connu une attaque de l'ordre de 1 Tbits/s. À l'origine, il s'agissait d'un trafic généré entre autres par 150000 caméras IP vérolées qui étaient sous contrôle discret d'une organisation criminelle. Selon l'enquête, OVH a été ciblé, car la société avait contribué à la fermeture du site VDOS qui proposait moyennant finance, la possibilité de lancer des attaques DDos à partir de machines vérolées, pilotables via un compte en ligne : c'est-à-dire du « DDOS-as-a-service ».

– https://www.ovh.com/fr/blog/rapport-attaques-ddos-observees-par-ovh-en-2017/

3.3 Moyens de protection

Les attaques de déni de service, surtout lorsqu'elles sont distribuées, sont très difficilement atténuables et parables. Dans ce cas-là, l'administrateur réseau peut contacter son opérateur ou transitaire, afin que ce dernier déporte le trafic sur une infrastructure permettant d'atténuer les requêtes grâce à des équipements dédiés et des liens au débit suffisant pour encaisser les débits générés par l'attaque.

Des sociétés comme Cloudflare proposent ce genre de services (cf. chapitre Gestion des actifs et haute disponibilité, section Redondance et clustering de niveau 3 - Redondance de liens opérateurs). Les hébergeurs mettent désormais en avant commercialement l'efficacité de leur système antiDDos, cependant, peu d'entre eux communiquent vraiment sur le fonctionnement technique de leur système. OVH, en revanche, joue la transparence et n'hésite pas à mettre en ligne l'explication et les détails techniques de son infrastructure anti-DDos.

– https://www.ovh.com/fr/anti-ddos/technologie-anti-ddos.xml

À une échelle plus petite, nombreux sont les firewalls capables de bloquer une communication lorsque cette dernière utilise trop de sessions ou de bande passante. Certains se basent également sur des listes d'adresses IP publiques possédant une mauvaise réputation évaluée, par exemple, d'après le calcul d'un score qui dépend du pays d'origine, du taux d'émission de spams, de potentiel trafic réseau généré à la suite d'une contamination par un malware…

– https://www.talosintelligence.com/reputation_center

Enfin, on peut citer l'outil Linux Fail2-ban, très facilement configurable et libre, qui permet de placer en liste noire (« blacklister ») des adresses IP apparaissant dans les logs d'un serveur, en temps réel selon des critères précis comme le nombre de requêtes par seconde ou le nombre de tentatives d'authentification manquées pour un service donné. Cependant, cette solution n'est à envisager que pour protéger un serveur spécifique et non l'intégralité d'un réseau en ce qui concerne l'outil cité.

4. Gestion des accès distants

4.1 Connexion à distance sécurisée : VPN nomade

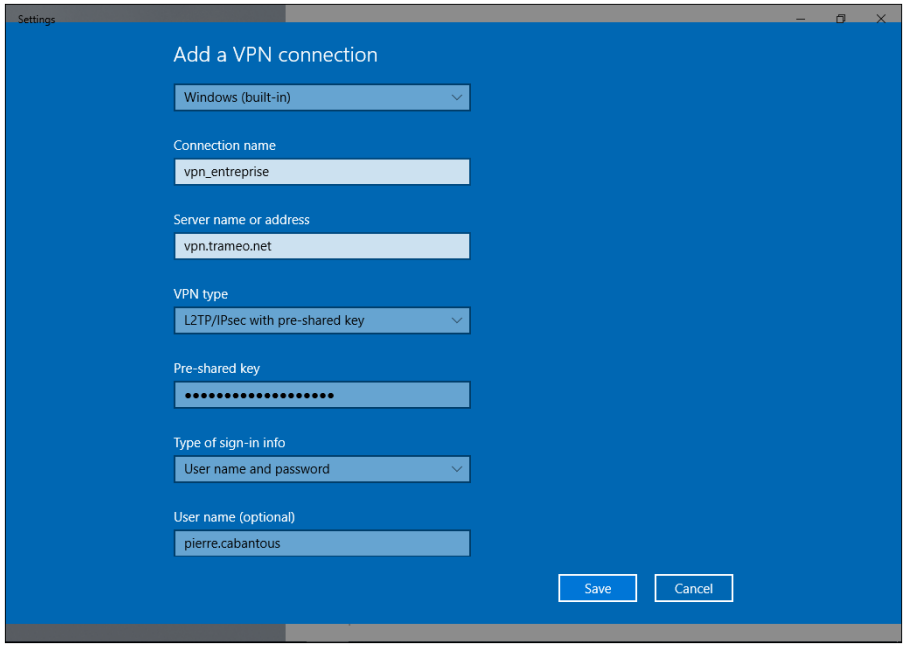
4.1.1 Principe

L'augmentation des débits des connexions internet, notamment avec le déploiement de la fibre optique et des réseaux 4G, et bientôt 5G, rendent maintenant possible techniquement le travail à distance. Il est tout à fait envisageable qu'un employé d'une société puisse accéder à partir de n'importe quel accès internet, y compris domestique, aux ressources internes de la société dans des conditions réellement optimales.

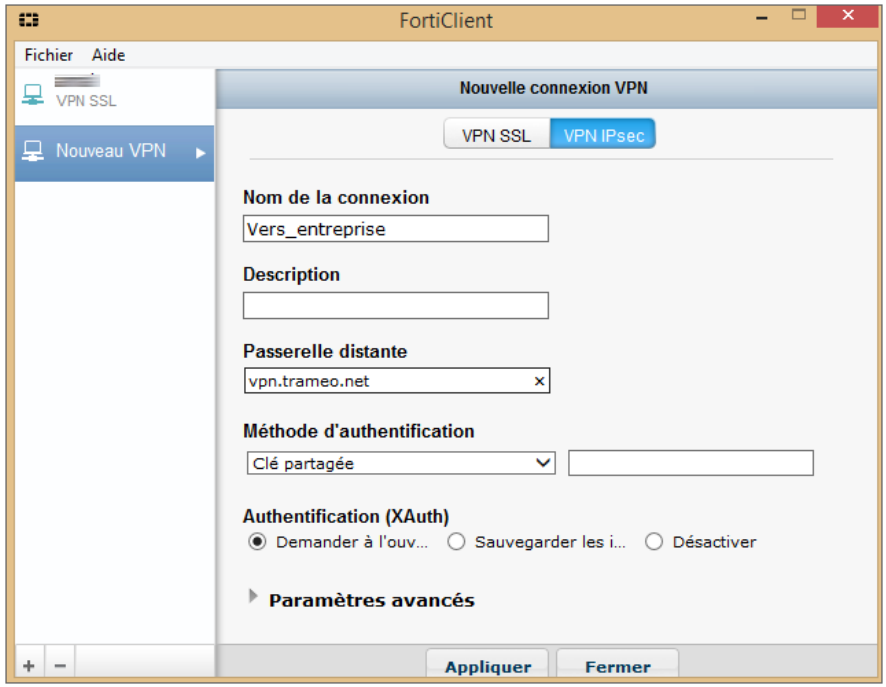
Les travailleurs nomades ont donc la possibilité d'accéder à leurs ressources, quelle que soit leur situation géographique, on utilise alors le terme de « poste nomade ». Même si fonctionnellement, le nomade doit pouvoir accéder aux mêmes ressources réseau que lorsqu'il est connecté directement sur le LAN de sa société, l'administrateur réseau commettrait une erreur en la considérant comme une connexion interne standard. Il est préférable de placer toute connexion nomade dans un réseau particulier, afin de lui soumettre des règles de sécurité plus restrictives. On définit alors facilement les règles d'accès aux ressources situées dans les autres segments réseau de la société (dont le LAN). À partir du moment où le poste nomade s'authentifie explicitement pour mettre en place la connexion, les firewalls permettent de gérer l'utilisateur spécifiquement et mettre en place les restrictions adéquates, quelle que soit d'ailleurs sa provenance.

La connexion nomade se configure de plusieurs manières. À l'origine, elle nécessitait l'utilisation d'une application cliente dédiée, souvent propriétaire, qui initiait une connexion vers la société avec des protocoles comme L2TP, PPTP, SSTP sur Windows et surtout IPSEC. Cette configuration classique nécessite le paramètrage des deux côtés de la connexion. Les protocoles de sécurité en ce qui concerne l'authentification, l'intégrité et le chiffrement des échanges ont beaucoup évolué, ont été renforcés et font de ce type de solutions la meilleure alternative en termes de sécurité et de confidentialité.

Techniquement, elle consiste tout d'abord à mettre en place un tunnel sécurisé entre le poste nomade et une passerelle VPN (un firewall compatible dans 90 % des cas). Une fois ce tunnel monté, tous les échanges concernant la société sont encapsulés à travers le protocole choisi. Il est certain que le protocole le plus sécurisé reste encore IPSEC par rapport aux nombreuses alternatives existantes. Cependant, la mise en place du tunnel et la sécurité des échanges peuvent s'envisager avec des protocoles différents, c'est le cas de L2TP, développé par Microsoft et Cisco dans une optique de créer un tunnel puis d'y ajouter une couche IPSEC pour sécuriser les échanges. Ces protocoles utilisés sont définis dans des RFC, normalisés et donc implémentables par n'importe quel éditeur ou constructeur. Ils sont parfois intégrés directement dans le système d'exploitation, ils peuvent également se présenter sous la forme de « plug-in » ou encore être spécifiquement développés par un éditeur qui le mettra à disposition gratuitement ou sous licence.



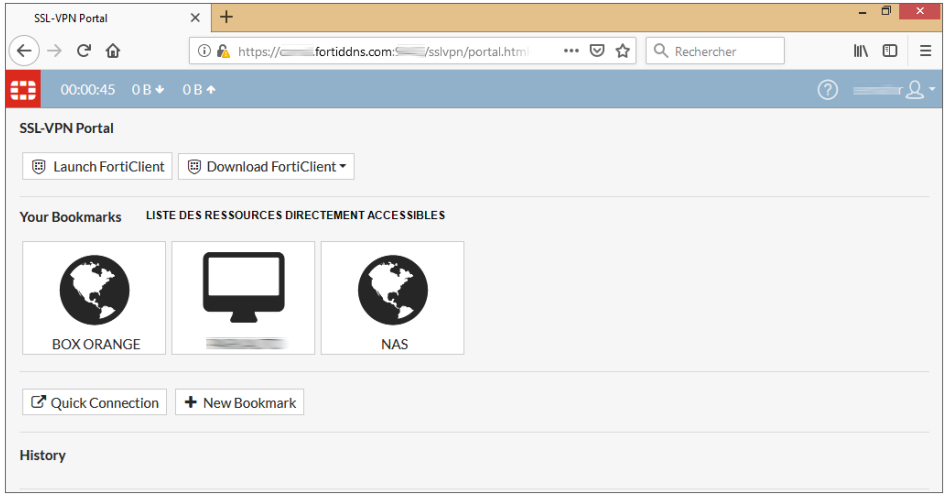
Configuration d'une connexion VPN nomade via l'outil intégré de Windows 10



Application lourde FortiClient permettant un accès VPN IPSEC nomade via une passerelle Fortigate

Il existe un type de VPN très spécifique, mais largement déployé : le VPN SSL nomade. Le principe est ici de configurer une passerelle VPN SSL (dans 80 % des cas, on utilisera un firewall), sous la forme d'une plateforme web accessible par n'importe quel navigateur. L'utilisateur nomade, se connecte au portail, s'identifie par l'intermédiaire d'un formulaire et accède alors à une page contenant des liens sécurisés vers une liste de ressources préalablement définies : accès Intranet, accès bureau à distance, accès à un partage de fichiers, etc. La connexion au portail et donc aux ressources est sécurisée, car utilisant le protocole SSL/TLS sur le protocole HTTP, c'est-à-dire HTTPS. C'est exactement le même type de processus de chiffrement utilisé lors de la navigation sur un site internet HTTPS classique.

L'avantage est qu'il n'y a pas besoin de configurer et d'installer une application cliente spécifique sur le poste nomade puisque seul un navigateur suffit. De plus, les clients VPN SSL évitent nativement de par leur conception, l'accès à la totalité du réseau (bien que ce soit possible moyennant configuration spécifique), car l'utilisateur ne peut utiliser que les applications ou protocoles qui sont définis dans son espace sur le portail SSL. En termes de sécurité, le protocole TLS/SSL est totalement valable, bien que ce soit uniquement les données qui sont chiffrées alors qu'avec une solution type IPSEC, le chiffrement descend jusqu'à la couche réseau.



Connexion à un VPN-SSL via un navigateur - trois ressources sont à disposition

Les solutions de VPN SSL ont beaucoup évolué et reposent en fait sur la capacité du navigateur à exécuter des scripts Java qui se comportent comme une application cliente indépendante, apportant des applications similaires à un VPN nomade avec client lourd. Avec la généralisation du langage HTML5, certaines fonctions peuvent être assurées nativement sans plug-in.

Cela explique la forte popularité des VPN SSL, mais ne doit pas cacher le fait que leur utilisation génère au quotidien davantage de maintenance. En effet, une simple mise à jour de navigateur ou du framework Java, notamment en termes de fonctions de sécurité, peut avoir une influence sur le fonctionnement du VPN SSL.

Cela est supportable lorsque l'éditeur ou le constructeur de la passerelle SSL est réactif et propose régulièrement des mises à jour logicielles de la plateforme.

Dans la réalité, les constructeurs assurent uniquement le support par rapport à des versions spécifiques de navigateur et de framework Java, ce qui oblige parfois à empêcher les mises à jour des navigateurs sur les postes clients afin de maintenir le service aux nomades, raison plutôt discutable en termes de sécurité.

Remarque

Certains constructeurs comme Fortinet ou SonicWall ont choisi de rendre compatible leur client lourd, initialement prévu pour du VPN IPSEC, avec SSL. L'utilisation ne nécessite pas de connexion préalable via un navigateur, mais c'est bien HTTPS qui est utilisé pour encapsuler et protéger les données.

4.1.2 Solutions nomades libres

Dans le monde libre, outre l'utilisation possible des protocoles énoncés précédemment, la communauté a développé d'autres protocoles réputés comme par exemple OpenVPN (très largement implémenté) ou SoftEtherVPN (plus discret).

Ces solutions nécessitent l'installation et la configuration d'un client lourd installé sur le poste nomade. Elles utilisent une couche SSL/TLS qui assure les fonctions de sécurité, mais au niveau applicatif les protocoles sont différents et spécifiques à chaque solution.

OpenVPN est à l'initiative d'une société américaine, mais distribué sous licence open source. La première version a vu le jour début 2002, le but était alors de s'affranchir de l'utilisation de protocoles plus bas niveau comme L2TP ou IPSEC ainsi que de viser de meilleures performances en ce qui concerne le débit. La solution est très populaire, elle est même intégrée sur les box des accès internet domestiques de l'opérateur Free. Elle est également multiplateforme et simple à mettre en place et à configurer.

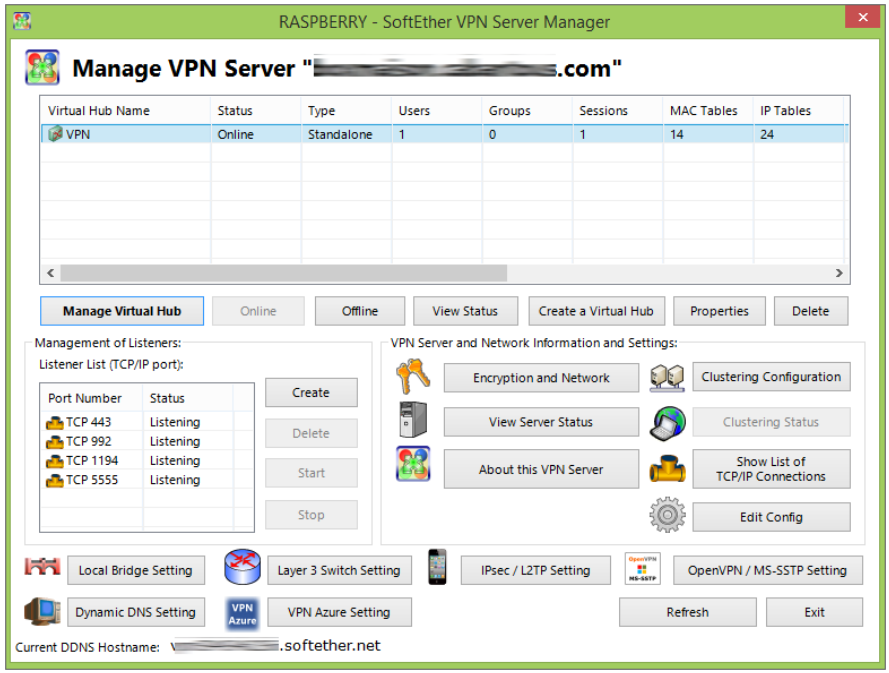
– https://openvpn.net

De plus, OpenVPN a acquis une première notoriété grâce au fait que le protocole passait relativement bien les firewalls, car en effet, le port utilisé par OpenVPN est configurable (par défaut le port est le 1194). Partant du constat qu'un accès à Internet nécessite l'ouverture en sortie sur les ports HTTP/80, HTTPS/443 et DNS/53, l'utilisation d'un de ces ports pour la mise en écoute de la partie serveur suffisait à outrepasser d'éventuels blocages de la communication client OpenVPN vers le serveur OpenVPN.

Comme évoqué dans ce chapitre, à la section Solutions commerciales NGFW, les firewalls ont évolué et sont maintenant capables grâce à l'analyse applicative d'identifier le protocole OpenVPN, quel que soit le port utilisé et ainsi de le bloquer. Ainsi, un utilisateur nomade ne sera pas en mesure de se connecter au serveur VPN sur l'intégralité des accès à Internet dont il disposera potentiellement. Cela dit, ce problème apparaît également avec IPSEC, dont on ne peut d'ailleurs pas choisir le port spécifique puisque le protocole n'utilise pas de couche transport dans l'échange des paquets (bien qu'un fonctionnement en mode transport ait été développé par la suite avec la fonction de NAT-Traversal pour contourner le problème, cf. section Connexion site à site VPN IPSEC).

SoftEtherVPN est une solution qui a été développée dans le but d'améliorer les performances de débit et surtout qui permet d'outrepasser le blocage applicatif réalisé par les firewalls de nouvelle génération. En fait, le protocole SoftEther, développé en 2014 par le japonais Daiyuu Nobori sous licence GPL, est capable d'encapsuler le trafic de l'utilisateur dans un autre protocole applicatif connu comme HTTPS, DNS et même ICMP! La stabilité du produit, la gestion des systèmes d'exploitation mobiles, les performances et la facilité de configuration en ligne de commande ou via une interface graphique en font une solution convaincante et maintenant mature pour l'usage en production. Il paraissait évident d'y faire référence dans cet ouvrage.

– https://www.softether.org/



Application Windows de configuration d'un serveur SoftEther VPN installé sur un Raspberry pi

Remarque

Il existe un débat sur la comparaison des niveaux de sécurité entre IPSEC et les protocoles à base de SSL. Les puristes affirmeront qu'IPSEC est plus sécurisé. Pourtant, les algorithmes utilisés sont très souvent les mêmes et la facilité de configuration des solutions SSL par rapport à l'IPSEC ne fait plus débat. La difficulté de configuration de ce dernier entraîne même les administrateurs à utiliser des paramètres de sécurité ou des méthodes d'authentification trop faibles pour configurer le tunnel (notamment l'utilisation d'une clé prépartagée au lieu de certificats).

4.2 Connexion site à site : VPN IPSEC

4.2.1 Le principe

À partir du moment où l'on veut relier deux réseaux distants en permanence, une connexion VPN nomade ne suffit plus. C'est d'ailleurs la raison initiale qui a poussé à la recherche sur les VPN. Pour une architecture de ce type, appelée alors « site à site », la mise en place d'un tunnel VPN IPSEC est parfaitement adaptée.

Un tunnel IPSEC est construit dans l'objectif de relier deux réseaux distants, séparés par un WAN, c'est-à-dire Internet. L'accès aux ressources du site distant est alors totalement transparent pour les utilisateurs, ces ressources sont d'ailleurs atteignables via le plan d'adressage privé du réseau distant en question. Virtuellement, cela revient à une architecture où deux segments réseau seraient reliés directement par un unique routeur au sein du même réseau de l'entreprise. Le premier protocole de tunnel site à site a été développé par Cisco avec le protocole GRE. Ce dernier n'assure pas nativement de sécurité des échanges, IPSEC a donc par la suite été développé par rapport à ce besoin de sécurité.

L'objectif de ce chapitre n'est pas de décrire de manière exhaustive IPSEC (un ouvrage pourrait y être consacré…), mais simplement de mettre en avant les étapes de configuration et quelques principes qui permettront à l'administrateur réseau de le configurer, quel que soit le matériel ou le logiciel utilisé. On essaiera également d'énumérer l'ensemble des problèmes qui peuvent se poser ou les éléments techniques à anticiper avant la mise en place du tunnel.

IPSEC assure les quatre principes fondamentaux de sécurité suivants :

– **L'authentification** : on s'assure que l'émetteur ou le récepteur soit bien celui qu'il prétend être.
– **L'antirejeu** : le but est de veiller à ce qu'un message chiffré ne puisse pas être généré ou réémis par un tiers.
– **La confidentialité** : le secret du message doit être conservé.
– **L'intégrité** : le contenu du message envoyé doit être identique au message reçu.

Afin de remplir ces quatre objectifs, les VPN IPSEC utilisent de nombreux protocoles et algorithmes qu'il est nécessaire de configurer spécifiquement, et ce, à chaque extrémité du tunnel. C'est en cela que la configuration peut s'avérer parfois complexe, qui plus est dans le cas où les passerelles de chaque extrémité (dans 90 % des cas, ce sont des routeurs/firewall) sont de marque différente.

Remarque

Pour faciliter les configurations, les constructeurs proposent souvent des assistants (« wizard ») permettant de configurer un tunnel VPN en quelques clics, à condition que les deux extrémités soient de la même marque, voire de la même version.

4.2.2 Les phases et la négociation d'un tunnel VPN IPSEC

Afin de résoudre un problème de connexion sur un tunnel VPN, il est primordial de comprendre le fonctionnement global de la mise en place du tunnel ainsi que les différents protocoles, et ils sont nombreux, qui participent à la création du tunnel et à son fonctionnement.

Un tunnel VPN est monté en deux phases bien distinctes qui ont chacune un rôle bien défini. Pour simplifier, on dira que la phase 1 permet la mise en place d'un premier canal de communication entre les deux passerelles VPN définissant la manière dont vont s'échanger différents paramètres de chiffrement qui seront utilisés dans la phase 2. La phase 2 définit véritablement les modalités d'échanges et de chiffrement des paquets de données entre les deux réseaux privés utilisés sur le VPN.

La configuration d'un tunnel VPN IPsec consiste donc à la définition des protocoles et des algorithmes utilisés pour monter la phase 1, puis la phase 2. Ce découpage est défini au sein d'un framework appelé ISAKMP (*Internet Security Association and Key Management*), que l'on confond souvent comme étant un protocole. En fait, ISAKMP définit un cadre à la négociation du tunnel, notamment par le découpage en deux phases. Le protocole utilisé lors de la négociation des phases est le protocole IKE actuellement en version 2 (*Internet Key Exchange*) qui fonctionne sur le port UDP/500. Du point de vue de la passerelle VPN, ce sont les premiers paquets qui vont être envoyés pour monter cette première phase.

Spécificités de la phase 1

Dans la phase 1, les passerelles s'envoient des informations d'identification réciproques qui sont des certificats ou une clé commune appelée clé prépartagée. Chacune d'elles fournit un identificateur qui peut être une adresse IP par exemple. Ainsi, une passerelle donnée possède un identifiant spécifique et connaît l'identifiant de l'autre passerelle : le « Peer ID».

C'est au niveau de la phase 1 qu'il est important de définir le mode de fonctionnement : normal ou agressif. Concrètement, à partir du moment où l'un des sites distants ne dispose pas d'une IP publique statique, c'est le mode agressif qu'il faut sélectionner. Dans ce dernier, on ne garantit pas l'identité de son voisin.

D'autres options vont se présenter à l'administrateur réseau comme la détection automatique de la perte de connectivité avec l'autre pair (DPD : *Dead Peer Detection*) et l'utilisation du NAT-Traversal (cf. section suivante Les problématiques de NAT).

Enfin, les deux entités s'accordent sur les paramètres de « transformation » de la phase 1 : ce sont un ensemble de paramètres qui définissent les algorithmes utilisés pour garantir l'authentification, le chiffrement de l'échange des clés et l'intégrité. La phase 1 aboutit à la mise en place de ce que l'on appelle une association de sécurité ISAKMP (ISAKMP SA). Une fois établie, on passe à la négociation concernant les algorithmes utilisés pour ce qui concerne les données c'est-à-dire à la phase 2.

Spécificités de la phase 2

La phase 2 ne peut se monter qu'après l'exécution d'une phase 1. À noter qu'il peut y avoir une phase 1 permettant l'établissement de plusieurs phases 2. La phase 2 permet de définir des paramètres pour l'échange de données entre deux réseaux privés. La sécurité des échanges de la négociation de la phase 2 est assurée par les algorithmes définis en phase 1.

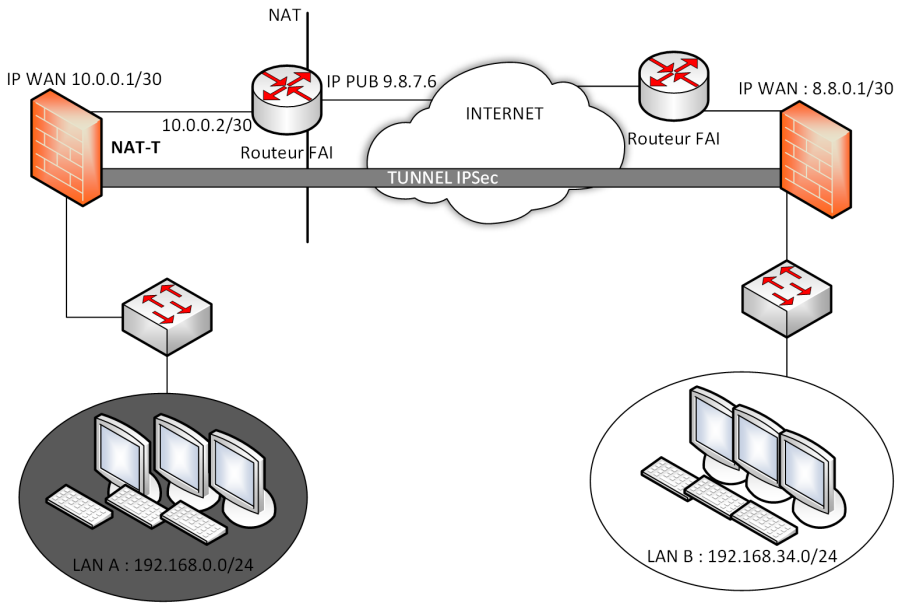
Chaque réseau distant à router possède un identifiant de phase 2. Les deux entités vont s'accorder alors sur un ensemble de paramètres constituant une association de phase 2 appelée couramment IPSEC SA. On utilise le même type d'algorithme que lors de la phase 1 pour garantir authentification, intégrité et chiffrement, excepté qu'il s'agit ici de la sécurité des données, non plus de la sécurité des échanges de clés effectués en phase 1.

L'association de sécurité de phase 2 possède un paramètre définissant la durée de validité avant renouvellement des clés de sécurité, elle peut donc expirer. Il est possible de forcer le renouvellement des clés de la phase 1 lorsque la phase 2 expire, pour durcir le niveau de sécurité, grâce à l'option PFS (*Perfect Forward Secrecy*). Cela s'accompagne du choix d'un algorithme spécifique basé sur des groupes appelés DH, pour « Diffie Helmann » que nous ne détaillerons pas en détail, l'important étant de comprendre qu'il faut choisir le même numéro de groupe DH pour une phase 2 sur les deux passerelles.

Une fois l'association de sécurité IPSEC établie, IKE n'est plus utilisé, les paquets de données se voient accoler un en-tête ESP (*Encapsulating Security Payload*) ou AH (*Authentification Header*). Ce dernier n'étant plus utilisé maintenant, car il n'assure pas le chiffrement des données, mais seulement l'authentification. ESP est un protocole de niveau 3 qui encapsulera les échanges sans utiliser de protocole de transport supplémentaire. Une IPSEC SA est identifiée par un identificateur de sécurité appelé SPI (*Security Parameter Index*).

4.2.3 Les problématiques de NAT

La première difficulté dans la mise en place d'un tunnel IPsec est le fait que les données échangées utilisent le protocole ESP de niveau 3. Dans une situation de NAT où l'une des passerelles VPN ne porterait pas l'IP publique, cela pose de sérieux problèmes puisqu'un protocole de niveau 3 n'est par définition pas « natable » car il ne repose sur aucun port. On retrouve ce cas de figure relativement souvent, dans le cas où le routeur fourni par le FAI ou la « box » porte l'IP publique de l'accès à Internet et que l'opérateur n'a pas prévu de seconde IP pour un autre équipement comme ici la passerelle VPN.



Architecture nécessitant de configurer du NAT-T pour le tunnel IPSEC au vu du réseau privé utilisé sur le site A pour relier la passerelle VPN au routeur FAI portant l'unique IP publique

Pour pallier cette situation a été développé un principe permettant d'encapsuler les paquets ESP dans un protocole supplémentaire de niveau transport : c'est ce que l'on appelle le « NAT-Traversal » ou « NAT-T » utilisant le port UDP 4500. NAT-T encapsule également les échanges IKE.

4.2.4 Problématiques d'adressage IP

L'établissement d'un tunnel VPN lorsqu'au moins une des passerelles possède une adresse IP dynamique peut s'avérer problématique. Pour cela, l'administrateur doit utiliser le mode agressif de la phase 1 de chaque côté du tunnel. La passerelle possédant une IP dynamique est alors désignée par un FQDN au lieu d'une adresse IP.

Autre point à prendre en considération, spécifique notamment aux accès type 3G/4G, est le fait que les opérateurs peuvent affecter une adresse IP publique (voire même privée) à un ensemble de clients. Ils utilisent pour cela un mécanisme de NAT appelé « CGN » pour « *Carrier-Grade NAT* ». Du point de vue de l'extérieur, l'ensemble des clients est vu comme une unique source, la différenciation des communications entre un client A et un client B se fait par l'intermédiaire d'une plage de ports dynamiquement attribués à l'identique du NAT traditionnel. Autrement dit, même en utilisant le NAT-Traversal, on ne peut pas garantir que le paquet à destination de l'IP publique de la passerelle de notre client A connectée via un accès 4G, arrive au client B. Dans cette situation, le tunnel peut monter uniquement dans le cas où l'une des extrémités possède une adresse IP fixe et non partagée via CGN.

Enfin, il n'est pas possible que le plan d'adressage IP privé des réseaux à router soit le même des deux côtés. Dans cette situation, on définit au niveau de la phase 2, un nouveau plan d'adressage virtuel privé pour le site distant. La passerelle effectue alors du NAT entre adresse IP virtuelle et adresse IP réelle, cela veut dire que le site 1 devra communiquer avec le site 2 uniquement grâce à ce plan d'adressage virtuel. L'obligation de mettre en place ce mécanisme réside dans le fait qu'une machine voulant communiquer avec un homologue dans le même plan d'adressage, et donc dans le même réseau logique, utilise directement le protocole ARP et ne fait pas appel au processus de routage : les paquets ne sont pas acheminés via la passerelle VPN du réseau.

4.2.5 Guide pour une configuration IPSEC site à site rapide et simple

Afin de cerner les points essentiels pour la mise en place d'un tunnel IPSEC, l'administrateur peut utiliser le diagramme suivant :

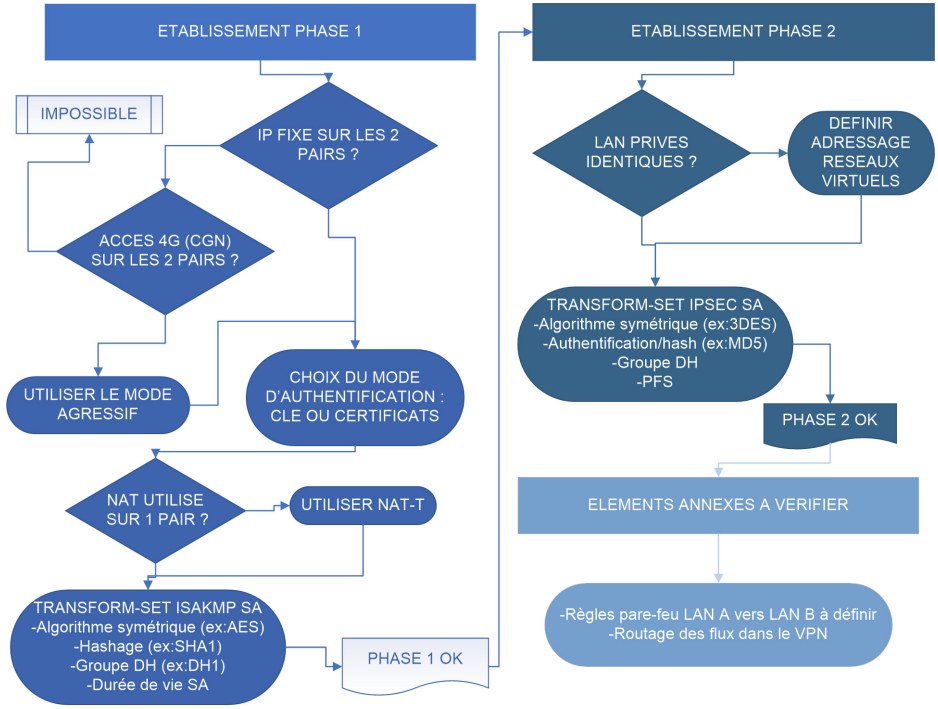


Diagramme décisionnel pour configurer un tunnel VPN IPSEC

4.3 Autres types de VPN

Il existe d'autres moyens pour interconnecter plusieurs sites distants à partir du moment où les accès internet de l'ensemble des sites sont gérés par le même opérateur. D'un point de vue opérateur, cela consiste à mettre en œuvre un simple routage accompagné de la mise en place d'une technologie appelée MPLS. Pour vulgariser, l'utilisation du MPLS dans l'optique d'un VPN permet de gérer une table de routage virtuelle (une VRF pour *Virtual Routing and Forwarding*) pour l'ensemble des sites raccordés d'un client donné. L'opérateur différencie ses clients en attribuant une VRF par client (pour une interconnexion donnée).

Ce qu'il faut retenir des VPN MPLS c'est qu'ils n'assurent en aucune façon le chiffrement et plus globalement la sécurité des échanges de données qui transitent de site à site. Libre au client, qui ignore souvent cet aspect-là malheureusement, de mettre en place une couche IPSEC supplémentaire. L'inconvénient majeur de ce type de solutions est son coût. En effet, la mise en place et la maintenance d'une interconnexion VPN MPLS sont facturées de façon récurrente par l'opérateur à son client.

Un des arguments principaux tendant au choix d'une architecture VPN MPLS repose sur le fait que le FAI est en mesure techniquement d'assurer une qualité de service et une garantie de débit sur l'interconnexion, car c'est lui qui maîtrise l'infrastructure réseau de bout en bout. Les paquets ne transitent effectivement pas par d'autres opérateurs et MPLS a été prévu pour une implémentation poussée de QOS.

Chapitre 4
Supervision temps réel

1. Hôtes et services dans tous leurs états : définition

1.1 Type d'état et statut

Chaque élément supervisé par Centreon possède un type d'état et un statut.

Le statut traduit une disponibilité pour les hôtes et une performance pour les services. Le type d'état quant à lui définit le degré de confiance dans le statut de l'hôte ou du service.

À noter : les mots « état » ou « statut » sont souvent utilisés pour la même notion dans Centreon.

Traditionnellement, Centreon reprend les statuts historiques de Nagios, mais il existe des statuts propres à Centreon Engine, par exemple le statut `PENDING` (ou `EN ATTENTE`) qui signifie que l'objet (hôte ou service) n'a pas encore été vérifié.

1.2 Hôte et objets associés

1.2.1 Hôte

Un hôte est une entité IP, aussi appelé *nœud* ou *ressource*.

Un serveur physique ou virtuel est un hôte au sens Centreon mais également un switch, un routeur, une imprimante réseau ou encore une caméra IP. De manière générale, tout ce qui possède une IP sur le réseau peut être configuré comme un hôte dans Centreon.

Centreon contrôle la *disponibilité* d'un hôte. Le statut d'un hôte peut avoir les valeurs suivantes :

- `UP` : l'hôte est disponible.
- `DOWN` : l'hôte est indisponible.
- `UNREACHABLE` : l'hôte est injoignable, à cause de l'indisponibilité d'un hôte dont il dépend (souvent un switch ou un routeur).

Remarque

La vérification de la disponibilité d'un hôte se fera souvent via un simple `ping`. Centreon laisse toutefois la liberté dans la commande utilisée. Il est possible de vérifier l'accès à une page web pour superviser la disponibilité d'un serveur web, par exemple.

Remarque

Si une sonde retourne un code de statut inconnu pour un hôte, Centreon conserve le dernier statut connu.

1.2.2 Groupe d'hôtes

Centreon permet de regrouper les hôtes dans un ou plusieurs groupes d'hôtes. Ces groupes peuvent avoir des sémantiques différentes : technique (ex : *Serveurs Linux*), géographique (ex : *Site Nord*) ou encore applicative ou métier (ex : *Système d'Information RH*).

Ces groupes peuvent être utilisés dans la gestion des droits, des escalades de notifications ou simplement en tant que filtre dans les différents écrans de supervision.

Catégories d'hôtes

Centreon permet également de regrouper des hôtes au sein de catégories. À partir de Centreon Web 2.5, il est possible d'associer des criticités aux catégories afin de rendre un hôte plus ou moins critique par rapport à un autre.

Les catégories d'hôtes sont utilisées notamment pour :

– Définir des droits spécifiques sur certaines ressources
– Filtrer plus efficacement par criticité dans les vues d'incidents
– Ajuster les rapports Centreon MBI

Remarque

D'une manière générale, il est préférable d'utiliser les groupes d'hôtes pour la gestion des droits et de préférer les catégories pour définir les notions de criticité ou pour la génération de vos rapports Centreon MBI.

1.3 Service et objets associés

1.3.1 Service

Un service est un point de contrôle rattaché à un hôte. Un service est aussi souvent appelé *mesure* ou *indicateur*. Un service peut se situer sur les couches matérielle, système, logiciel, applicative ou encore métier ou processus.

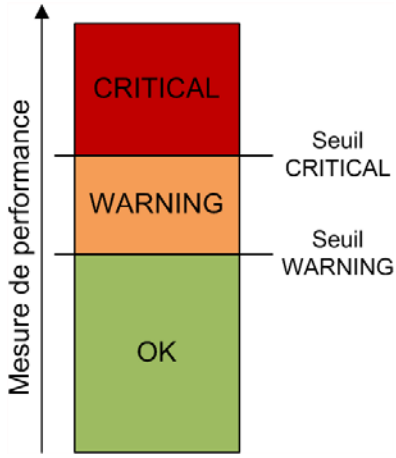
Quelques exemples de services : latence d'un `ping`, occupation d'un espace disque, utilisation d'un processeur, niveau d'une cartouche d'encre, température d'une salle serveur, vitesse de rotation d'un ventilateur, état d'un RAID, connexion à une base de données, latence d'une page web, nombre de commandes bloquées dans un logiciel, état du processus de mise à jour de prix, etc.

Centreon contrôle la *performance* d'un service. Pour ce faire, il se base sur deux seuils (`WARNING` et `CRITICAL`) qui lui permettent de qualifier la performance du service. Les statuts possibles d'un service sont :

– `OK` : le service fonctionne de manière nominale.
– `WARNING` : le service est dégradé, il est au-dessus du seuil `WARNING` mais en dessous du seuil `CRITICAL`.

– `CRITICAL` : le service est dans un statut critique qui nécessite une intervention immédiate, la valeur de performance calculée dépasse le seuil `CRITICAL`.

– `UNKNOWN` : le statut du service est inconnu, il n'a pas pu être vérifié à cause d'un incident extérieur (erreur dans la sonde, agent SNMP désactivé ou mal configuré, etc.).



1.3.2 Groupe de services

Comme les groupes d'hôtes, les groupes de services servent à regrouper plusieurs services ayant un lien sémantique. Par exemple, un groupe de service *Supervision du SGBD Oracle* peut servir à regrouper certains services clés de la supervision de l'infrastructure Oracle.

Les groupes de services peuvent être utilisés dans la configuration des droits d'accès et la configuration des escalades de notification. En pratique, ils sont surtout utiles pour afficher rapidement les graphiques de plusieurs services dans les écrans d'analyse ou encore des statistiques agrégées dans les écrans de rapports.

Les catégories de services

Comme pour les catégories d'hôtes, les catégories de services sont surtout utilisées pour ajouter de la lisibilité à votre écran de supervision (via la notion de criticité) et pour la génération de rapports Centreon MBI.

Remarque

Les services sont associés aux catégories de services via leur modèle. Cette notion est abordée dans le chapitre Configuration des ressources.

1.3.3 Métaservice

Un métaservice est un service dont les données de performance sont construites par agrégation des données d'autres services à l'aide d'opérations mathématiques : somme, moyenne, minimum ou maximum.

Les métaservices sont soumis au mécanisme des notifications et possèdent un graphique de performance.

Le métaservice est un concept introduit par Centreon, qui n'existe pas dans Nagios.

Exemples de métaservices

Les métaservices peuvent être utilisés pour sommer plusieurs bandes passantes afin d'afficher un graphique agrégé pour une liaison redondée par exemple. Ils peuvent être encore utiles pour sommer le nombre de connexions sur un cluster web ou en calculer une moyenne, etc.

Remarque

Lors de la définition d'un métaservice, attention aux unités : les opérations mathématiques doivent se faire sur des données de performance similaires.

1.4 Types d'états SOFT et HARD

Lorsqu'un statut d'erreur survient (`DOWN`, `WARNING`, `CRITICAL` ou `UNKNOWN`), Centreon le confirme à l'aide de plusieurs contrôles successifs avant de notifier les contacts.

Le type d'état est utilisé pour différencier les statuts d'erreurs confirmés de ceux non confirmés :

- `SOFT` : l'état n'est pas confirmé, les contacts ne sont pas notifiés.
- `HARD` : l'état est confirmé, les contacts peuvent être notifiés.

L'objectif est de réduire le nombre de fausses alertes et de notifications.

Remarque

Les statuts UP et OK sont automatiquement confirmés par Centreon.

Configuration

Le nombre de vérifications avant confirmation de l'état, ainsi que l'intervalle entre chaque vérification pendant une confirmation, sont configurables au niveau des hôtes et services.