Sécurité des accès extérieurs

Si la surveillance des sources de danger sur un réseau est un travail à temps plein, l'installation des outils de protection limitera le temps consacré à cette surveillance aux seules situations non prévues dans le système. Nous nous appliquerons à traiter de la sécurisation des accès distants à travers les outils suivants : Proxy, Routeur filtrant et Firewall.

Nous évoquerons aussi la zone démilitarisée qui ouvre l'espace de l'entreprise tout en protégeant le système interne. Enfin, nous présenterons un bref aperçu des techniques de détection et protection contre les intrusions (IDS et IPS). Un autre support fera l'objet de la sécurisation des échanges en dehors de l'entreprise (VPN).

I Les outils de protection

1.1 Translation d’adresses

C’est la technique la plus simple de toutes les sécurisations, réalisée par les routeurs courants et les serveurs proxy. Le NAT (Network Address Translation) repose sur :

- un adressage interne, en général privé (10.x.x.x, 172.16.x.x à 172.31.x.x ou 192.168.x.x)
- une adresse publique (utilisable sur internet) ou plusieurs
- un matériel ou logiciel prenant en son nom les requêtes vers l’extérieur (il remplace l’adresse de l’émetteur par la sienne et retransmet la réponse au bon destinataire)

Le NAT existe dans sa version transparente ou dynamique, et dans une version paramétrable manuellement, souvent complétée par la translation de port.

Translation Dynamique

Aucune configuration spécifique n'est nécessaire sur le poste client. Il faudra activer la fonction de translation d'adresse sur l'outil assurant le routage.

En masquant les adresses internes dans ses communications avec l'extérieur, la translation permet d'éviter l'usurpation d'adresse (IP spoofing).

Illustration : modification de l'adressage avec la translation d'adresse

A mettre en forme Trame émise par le poste Trame niveau 2 IP em : 10.0.0.25 IP dest xxxxx

```
Trame expédiée par le routeur
```

Trame niveau 2 IP em : 202.20.0.4 IP dest xxxxx Le routeur retient en mémoire la demande du poste jusqu'à réception de la réponse du destinataire

```
                    Réponse reçue par le
routeur
```

Trame niveau 2 IP em xxxxx IP dest : 202.20.0.4

```
Réponse réexpédiée au poste
```

Trame niveau 2 IP em xxxxx IP dest : 10.0.0.2

NAT Statique et translation de port (PAT)

Si le NAT transparent est une fonction naturelle des routeurs et des proxys, on peut utiliser cette technique pour décider de la façon dont des accès extérieurs doivent être renvoyés vers les éléments de la DMZ et/ou du réseau local.

NAT statique

Un serveur accessible aux utilisateurs extérieurs pourra être masqué par le routeur qui restera le seul visible aux internautes. Le routeur recevant une demande destinée à son adresse publique, il étudiera sa table de translation pour savoir vers quelle adresse interne il destinera effectivement le paquet. Le poste externe ne saura pas qu'il a contacté un équipement interne.

PAT

En complément de ce NAT statique, qui permet de renvoyer une demande adressée à un équipement (routeur en général) vers un autre (serveur), on peut affiner le fonctionnement par le recours à la translation de port (PAT) qui travaillera en outre sur le service sollicité depuis l'extérieur et pourra renvoyer distinctement sur plusieurs équipements, chacun jouant un rôle particulier.

Cette option autorisera aussi à masquer une fonction existante (on met un numéro de port non standard) soit sur le routeur (voir illustration sur port 8080), soit sur le serveur interne.

Illustration : NAT seul

image à coller

Illustration : NAT et PAT

image à coller

1.2 Le cache Internet et la surveillance du trafic

Cache

Le cache consiste à sauvegarder sur une machine de l'entreprise, les données d'un site internet (pages, images, ...).

Le cache est utile si le site à télécharger :

- est statique : le contenu est décrit dans des pages fixes qui ne sont pas construites à partir des données d'une base (sinon le téléchargement est impossible et sans intérêt)
- est stable : les informations qu'il présente ne doivent pas être modifiées trop souvent
- est sans droits d'auteur : en effet, la notion de cache implique la recopie intégrale en interne d'un site, et des réglementations visent à en limiter l'utilisation
- est souvent accédé : il n'est pas utile de rapatrier des informations demandées par un seul utilisateur, même si le cache ne sait pas faire le tri et télécharge systématiquement les pages consultées.

La sécurité apportée par le cache des Proxy et des firewall est évidente : une seule demande est véhiculée vers l'extérieur, à la suite de quoi toutes les navigations se font en interne. En plus de cette sécurisation, le cache diminue les coûts (pas de communication, mais c'est moins pertinent avec les accès DSL forfaitaires) et augmente la rapidité d'utilisation d'internet : le réseau interne assure un débit en Mbits/s ou Gbits/s, tandis qu'on se contente de Kbits/s ou Mbits/s pour internet actuellement.

Proxy

La fonction proxy assure un partage de connexion unique entre plusieurs postes, et permet la surveillance du trafic. En enregistrant dans des fichiers de log (journalisation) l'ensemble des requêtes émises, il permet de connaître qui a utilisé quoi à quelle heure, voire ce qui a été échangé.

Pour utiliser cette fonction, il sera nécessaire de se prémunir juridiquement en prévenant les utilisateurs que l'usage qu'ils feront d'internet donnera lieu à une surveillance.

Le client du proxy est un navigateur internet qui adresse toutes ses demandes au service proxy. Cela est différent de la passerelle IP qui est transparente pour la machine : les demandes sont directement adressées au site distant à travers un routeur ou un firewall, alors qu'elles sont adressées uniquement au Proxy si celui-ci est activé.

1.3 Le filtrage

Le filtrage consiste à déterminer les machines autorisées à communiquer, ce que l'on peut laisser actif, ce que l'on veut voir entrer ou sortir. Le filtrage est la technique mise en place sous l'appellation Firewall ou Pare-feu.

A Règles et filtrage

Il faut bien distinguer :

- l'étape de constitution des règles, qui définit a priori les éléments (IP, ports, mots clés, URL, etc) interdits ou autorisés
- le moment du filtrage qui s'applique à étudier les éléments d'une trame circulant du réseau interne vers l'extérieur (ou l'inverse) pour appliquer l'une des règles

Règles

Le principe de la définition d'une règle de filtrage est le suivant :

- chercher les informations techniques qui peuvent être étudiées : adresse (ou plage) IP, ports, informations de niveau 7 ou mots clés, etc. Ces informations doivent pouvoir être valorisées dans la règle : on doit être certain des valeurs que l'on veut autoriser ou interdire
- déterminer le sens de l'échange à filtrer : les informations d'adressage ou de port sont elles à préciser pour la source et/ou pour la destination, par quelle interface du filtre parviendront les trames correspondant à cette règle → il est parfois nécessaire d'écrire deux règles (une pour l'envoi, une pour la réception) pour garantir l'efficacité d'un filtrage
- éventuellement, préciser l'état d'un échange dans le cadre du filtrage : on peut laisser entrer un trafic si la demande à été initiée depuis le réseau local (accès Web par exemple)
- placer la règle dans l'ordre

Une règle se présente sous la forme

N°	Interface	IP Source	IP Destinataire	Port Source	Port Destinataire	Etat*

Filtrage

L'application du filtrage pour une trame parvenant sur un filtre se déroule selon les étapes suivantes :

- on cherche la première règle pour laquelle les champs connus sont présents dans la trame et on effectue l'action correspondante
- si aucune règle ne correspond, on applique la politique par défaut du filtre (tout autoriser ou tout interdire).

Le filtrage est une démarche fastidieuse pour laquelle des outils pré-configurés ou des listes prêtes à l'emploi sont disponibles. Il peut porter sur tout ou partie des éléments du modèle OSI.

B Filtrage par adresse

Première sécurité réelle, le filtrage IP repose sur les adresses de niveau 3, en en autorisant l'entrée où la sortie. Il est ainsi possible :

- de limiter les seules adresses IP autorisées en sortie : dans le cadre d'un Extranet, seules les communications entre partenaires sont possibles. Ce filtrage IP permet aussi d'éviter que des attaques soient lancées depuis le réseau de l'entreprise en passant par des sites anonymant
- de limiter les seules adresses IP autorisées en entrée : par exemple lorsque le site interne ne doit être autorisé qu'à des télétravailleurs
- de limiter, pour une machine les adresses IP en sortie : pour éviter la fuite d'information
- d'interdire un certain nombre d'adresses en sortie : si le site interne offre un portail (orientant vers une sélection de sites), on peut interdire les adresses des moteurs de recherche, ou encore de sites reconnus comme distrayants dans un cadre professionnel
- d'interdire un certain nombre d'adresses en entrée : pour éviter que des internautes passant par les sites anonymant ne pénètrent le réseau de l'entreprise

Cette partie est très fastidieuse à mettre en place. Il faut en effet travailler sur les adresses IP, ce qui demande de bien maîtriser son réseau interne, mais aussi de connaître les IP de l'extérieur. Un administrateur n'aurait pas le temps d'étudier, par le biais des Ping et des fonctions DNS, une stratégie suffisamment permissive et sécurisée sur son firewall. Toutefois, on peut envisager une mise en place progressive, partant d'une restriction maximale et s'ouvrant au fur et à mesure ou, à

l'inverse, initialement très ouverte et se fermant progressivement.

Il sera donc plus facile de travailler directement sur les fonctions réseau de la couche application.

C Le filtrage par port

Cette sécurisation monte au niveau 4. Le protocole TCP (ainsi que son équivalent sans contrôle UDP) associe à chaque service de la couche Application un port d'écoute standardisé (FTP → 21, HTTP → 80,…).

Il va alors être possible d'autoriser ou d'interdire, pour le réseau ou par machine l'utilisation de ces fonctionnalités. Les Firewall autorisent ce filtrage, ainsi que les options avancées de configuration des cartes réseau sous les OS Windows (onglet sécurité).

On pourra :

- limiter les services autorisés en entrée : si le serveur assure la fonction FTP et Web, on pourra n'autoriser que ces fonctions, en interdisant par exemple le Telnet ou le mail
- limiter les services autorisés en sortie : si l'on ne souhaite pas que les employés passent leur temps à naviguer sur le net, mais qu'ils puissent utiliser la messagerie, par exemple
- interdire des services en entrée ou sortie : à l'opposé des restrictions ci-dessus, on autorise tout, mais on interdit des fonctions que l'on considère inutiles

On trouvera, sous Windows, la liste des ports standards dans le fichier services présent dans winnt\system32\drivers\ et dans ce même fichier quelque part sous Linux.

D Le filtrage utilisateur

Il s'agit d'effectuer les restrictions vues ci-avant, non plus à partir des adresses mais directement à partir de l'identification de l'utilisateur (soit définie auprès du Firewall, soit auprès du système d'exploitation de l'entreprise). On pourra limiter les plages horaires d'accès aux différents services.

E Le filtrage par mots-clé

Cette dernière restriction est sans doute la plus simple d'utilisation, mais pas forcément la plus sécurisée. Il s'agit d'autoriser la circulation des messages contenant tel mot, ou au contraire de les interdire. Dans un bureau de recherche et développement, tous les mots spécifiques au domaine de l'entreprise pourront ainsi être contenus dans les murs de la société, pour éviter toute fuite par le réseau. Dans une autre entreprise, on interdira les recherches sur le sexe, le racisme, les jeux, la télévision, la météo, les voyages…

Alors que cette technique semble simple, on se rend rapidement compte que faire la liste exhaustive de tous les mots que l'on souhaite interdire devient un travail titanesque, d'autant que les effets peuvent être inattendus lorsque le vocabulaire utilisé peut entraîner des contre-sens.

II La zone démilitarisée (DMZ)

La seule manière d'assurer la sécurité pour un réseau, ce serait de l'isoler dans une salle coupée du reste du monde. Et encore...

Pour ne pas en venir à ces extrémités, il est possible d'ouvrir un espace intermédiaire entre l'interne et l'externe, en assurant un filtrage sur chacun des accès possible.

Ce sas de communication offre ainsi des services en direction de l'extérieur (Serveurs Web, accès des employés mobiles et distants, extranet...) et laisse aux utilisateurs du réseau local une possibilité d'accès à la fois aux informations de cet espace (pour l'extranet, pour l'échange avec les clients mobiles...) et à internet. On parle d'une DeMilitarized Zone (DMZ) ou zone démilitarisée.

Il existe différentes mises en œuvre pour réaliser une DMZ, basée sur un unique filtre, ou créant une véritable zone contenue entre deux filtres.

DMZ et Honey Pot

En ouvrant un espace sur l'extérieur, l'entreprise expose une partie de son intelligence aux attaques venant d'internet. Cette seule présence est susceptible d'attirer l'attention des utilisateurs malveillants. C'est pourquoi la DMZ peut être complétée par une nouvelle zone nommé Pot de miel ou Honey pot qui appâtera ces pirates et les laissera s'attaquer à une zone fictive dans laquelle ils viendront s'engluer en vain.

III IDS et IPS

À l'image des antivirus qui bloquent des objets connus ou des comportements identifiables, les réseaux informatiques peuvent être équipés de systèmes ayant pour vocation de repérer des comportements suspects (trafic massif et inhabituel, tentative répétée de connexion) qui cherchent à nuire à l'activité de l'entreprise. Ils travaillent à la fois comme un analyseur de trame qui étudie le trafic du réseau, et comme des consoles SNMP capables d'interroger certains paramètres des équipements.

Ces systèmes sont dits IDS (Intrusion Detection System). Ils fonctionnent de manière analogue aux antivirus, en étudiant la signature habituelle des attaques classiques, ou bien d'une façon proche de la sécurisation de type anti-spam en observant les situations de confiance et en en déduisant celles qui sont douteuses.

En cas de détection d'une intrusion, ils doivent pouvoir avertir qui de droit par divers moyens (SMS, mail, etc.). Leur activité de supervision ne doit pas encombrer le réseau ou les équipements de trafic et sollicitations inutiles. Identification des signatures

Première approche dans la détection d'intrusion, l'identification des signatures d'attaques consiste à analyser sur les différents systèmes participant au fonctionnement du réseau des installations de services ou des comportements typiques d'une attaque connue. Ainsi, l'introduction de SYN Flood, attaque de déni de service identifiable par la présence de trames TCP de synchronisation portant sur un même numéro de paquet peut être détectée sur un routeur d'entrée. De même, on pourra repérer une montée d'activité de l'intérieur vers l'extérieur qui pourra être le symptôme d'une attaque par ping distribué depuis le réseau interne (à partir de chevaux de Troie). Ou encore, l'augmentation

subite du trafic SMTP pourra annoncer l'infection des postes par un ver.

Pour alimenter les IDS en signature, des bases de données sont mises à disposition des administrateurs par les éditeurs, ou bien celles-ci peuvent être complétées par une veille technologique ou l'expérimentation d'une situation vécue.

L'efficacité d'un tel système dépend évidemment de la pertinence de la base de signature, de sa richesse et de sa fiabilité, au même titre que les signatures de virus utilisées par les antivirus. En outre, un tel système ne peut être fiable face à une attaque inédite (attaque d'une faille nouvelle) puisque la signature d'attaque n'existe pas encore.

Identification des fonctionnements normaux

En complément de la première approche (qui présente tout de même l'avantage de limiter les risques face à des dangers connus et donc parables), les IDS peuvent aussi tenter de repérer le mode de fonctionnement normal des différents services et équipements : on pourra ainsi leur définir le nombre moyen de message expédiés par jour ou par heure, la quantité de trame erronées habituellement présentes sur le réseau, la proportion de connexions TCP, la répartition des protocoles applicatifs (http, ftp, telnet, smtp, dns) utilisés, le temps habituel de réponse d'un serveur, etc. Dès qu'un comportement irrationnel est perçu par l'IDS, une alerte est levée.

De l'IDS à l'IPS

Presque vus comme les sauveteurs de la sécurité au moment de leur apparition, les IDS ont vite montré leurs limites : faux-vrais (des alertes pour des dangers détectés qui ne sont pas des dangers) et faux-faux (ne pas prévenir pour des attaques réelles), multiplication des alertes, difficulté d'adaptation aux nouvelles techniques d'intrusion pour certains, encombrement du trafic ou alourdissement des serveurs.

En outre, l'analyse devient de plus en plus difficile sur des réseaux commutés puisque la vision du trafic n'est possible que sur le domaine de collision sur lequel l'IDS est présent, ou éventuellement sur le trafic passant par l'ensemble des ports si le commutateur permet la mise en mode écoute généralisée d'un port (mode promiscuous). Avec les VLAN, la tâche se complique et l'on doit multiplier les IDS sur les segments réseau.

La grande critique qui leur est surtout adressée est leur incapacité à pallier une attaque. C'est pourquoi, riches de l'expérience des méthodes de gestion de la sécurité et des bonnes pratiques sur la sécurité, des outils plus précis ont vu le jour : les IPS (Intrusion Protection System) qui ajoutent des parades aux attaques, sont capable de mettre en action des honey-pots (pots de miel) pour détourner une attaque malveillante, mettre à jour une table de filtrage pour interdire une IP reconnue comme suspecte, modifier les droits d'accès aux ressources, etc.

Ces outils ne sont pas encore largement répandus, mais comme leurs prédécesseurs, ils nécessiteront une surveillance proactive, des paramétrages toujours plus subtils et des compétences toujours plus poussées.

Conclusion

Si la sécurité est le thème de prédilection des administrateurs, il ne doit pas devenir une obsession démesurée empêchant une activité relativement autonome des utilisateurs. En effet, plus ce dernier

est bloqué dans son travail, moins il aura envie de s'investir. Il s'agit donc de mettre en place le bon dosage, susceptible de sécuriser au maximum le réseau sans pénaliser les utilisateurs.

Une fois la sécurisation d'un réseau mise en place, l'administrateur ne pourra pas se reposer sur ses lauriers. En effet, les formes d'attaques toujours renouvelées, les tentatives d'intrusions se diversifiant, etc, il est nécessaire de s'abonner à des listes de diffusion et à faire la veille technologique attendue d'un responsable. Une attention devra enfin être portée à la légalité des actions menées. En effet, un réseau d'entreprise véhicule des données professionnelles, mais aussi des échanges privés dont on ne peut exploiter le contenu autrement que par des moyens automatisés ne gardant pas trace du contenu étudié, modifié, ou supprimé.

Les outils déjà évoqués que sont les IDS et IPS fourniront des compléments permettant d'inventorier les attaques et, éventuellement, d'automatiser le reparamétrage des outils de sécurité (notamment les règles de filtrage).