Le firewall identitaire - innover par le retour aux sources

"Quelles sont les autorisations pour ces personnes ?" C'est la question qui vient naturellement en tête lorsque l'on parle de politique de sécurité. Réflexe naturel puisque la sécurité, qu'elle soit physique ou logicielle, consiste effectivement à gérer l'accès aux ressources selon les personnes.
Et pourtant ! Dès qu'il s'agit de mettre en place la règle de sécurité sur un firewall, la question se transforme immédiatement pour devenir "Quelles adresses IP doivent être autorisées ?"

Il est vrai qu'historiquement l'adresse IP - identifiant de la machine sur le réseau - a joué un rôle déterminant dans la politique de sécurité. Dans le schéma de sécurité traditionnel, le réseau est découpé en différents sous-réseaux IP cloisonnés. Chaque personne et chaque machine sont à leur place - fixe et statique - dans un sous-réseau donné, et leurs droits sont ceux du sous-réseau auquel elles appartiennent.

Cette vision traditionnelle est aujourd'hui remise en question.

L'adresse IP, critère de filtrage coûteux... et dépassé ?

Les topologies réseau évoluent rapidement au gré de la vie des sociétés : changements technologiques, fusions, ouvertures de nouvelles filiales, interconnexions avec de nouveaux partenaires... Le modèle de sécurité étant directement lié au découpage technique du réseau, chacune des évolutions de celui-ci implique également de revoir la politique de sécurité. Les coûts liés au changement s'en retrouvent donc démultipliés, ainsi que les risques d'erreurs.

Pour maîtriser ces coûts et ces risques, il devient donc nécessaire de décorréler la gestion de la topologie réseau et la gestion de la politique de sécurité. Les perspectives futures, quant à la multitude de changements et d'incertitudes que provoquera la transition vers IPv6 dans le monde du réseau, renforcent d'autant plus ce constat !

Le temps où les personnes dans l'entreprise disposaient d'un ordinateur de bureau fixe est également révolu. Sans même sortir physiquement des locaux, les utilisateurs se connectent au réseau par différents points d'accès : le câble réseau de leur bureau, le Wifi interne, la salle de réunion... Sans compter que la plupart d'entre eux disposent également d'un Smartphone, voire d'une tablette, et demain peut-être encore de nouveaux outils introduits par le BYOD ! La démultiplication des points d'accès et des outils de travail connectés pour chaque collaborateur augmente ainsi d'autant la difficulté et les coûts pour établir une politique de sécurité fiable.

Pour répondre à cette prolifération des outils et de leurs moyens d'accès au

Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com

réseau, et à la complexité qu'elle entraîne dans la gestion de la politique de sécurité, il est aujourd'hui indispensable de définir cette politique autour d'un nouveau critère.

Revenir à la conception intuitive de la sécurité : quelles sont les autorisations pour ces utilisateurs ?

Devant cette complexité croissante a émergé la notion de "firewall identitaire", dont la philosophie est de remettre la notion d'utilisateur au centre de la politique de sécurité.

En effet, la vraie question que doit poser la règle de sécurité ne doit pas être l'identification de son outil de travail, mais plutôt l'identification de l'utilisateur lui-même. L'outil de travail peut changer d'emplacement sur le réseau, ou l'outil lui-même peut changer ; l'identité de l'utilisateur, elle, ne change pas : la politique de sécurité reste fiable dans le temps, ce qui réduit les coûts d'administration. La traçabilité est également plus simple à établir pour les besoins légaux, puisque les traces d'audit indiquent sans équivoque l'activité d'un utilisateur donné sur le réseau.

Concernant la méthode, les techniques d'authentification ne manquent pas : de l'authentification SSO ne nécessitant aucun déploiement sur le poste-client et totalement transparente pour l'utilisateur, jusqu'aux mécanismes impliquant une administration plus conséquente, mais également une sécurité renforcée.

Dans tous les cas, les solutions doivent proposer différents mécanismes d'authentification en fonction des besoins. Les mécanismes les plus sécurisés doivent, en outre, être reconnus formellement comme tels, par exemple via une qualification ou une certification par un organisme tiers.

Reste le cas plus spécifique des utilisateurs mobiles se connectant au réseau d'entreprise par l'intermédiaire d'un VPN, et qui ne pourront sans doute pas utiliser ces mécanismes d'authentification internes. Une solution peu coûteuse pourrait alors consister à réutiliser l'authentification déjà fournie pour établir la connexion VPN. Réutiliser ce vecteur d'authentification offre un gain en temps et en simplicité - et donc en coûts - considérable, sans compter que la sécurité des authentifications VPN n'a plus besoin de faire ses preuves.

Bien entendu, la politique de sécurité ne devrait pas être définie pour chaque utilisateur unitairement - trop lourd, trop statique ! Il convient de définir les autorisations pour chaque profil de personne, et de bâtir la politique autour de ces profils.
Les solutions de sécurité doivent alors s'interfacer avec un annuaire de type Active Directory, où se fera l'association entre les utilisateurs et les profils auxquels ils appartiennent. Les turnovers et les évolutions des personnes dans la société sont ainsi gérés de façon centralisée au niveau de l'annuaire, et la politique de société qui leur est appliquée

Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com

évolue automatiquement en conséquence, sans aucune intervention d'administration. Dans leur définition de « Next Generation Firewalls », les analystes de Gartner précisent d'ailleurs que ceux-ci se doivent de présenter une « *intelligence en dehors du firewall* », à savoir l'utilisation de sources externes pour affiner la politique de filtrage ; un des exemples donnés mentionne justement l'intégration avec un annuaire afin de lier l'action de filtrage à l'identité de l'utilisateur.

Ne négligeons cependant pas toutes les technologies construites en chemin !

Au cours des dernières années, de nombreux éditeurs se sont positionnés sur le segment du firewall identitaire et en font un argument majeur de différenciation. Il faut toutefois garder à l'esprit que cette brique à elle seule ne suffit pas : elle doit être intégrée de façon cohérente à une solution de confiance reconnue pour ses qualités en termes de sécurité, d'administration et de performances.

Car identifier l'utilisateur n'est que le début de la chaîne de filtrage...

Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com