16.2.2 - Atténuation des attaques du réseau

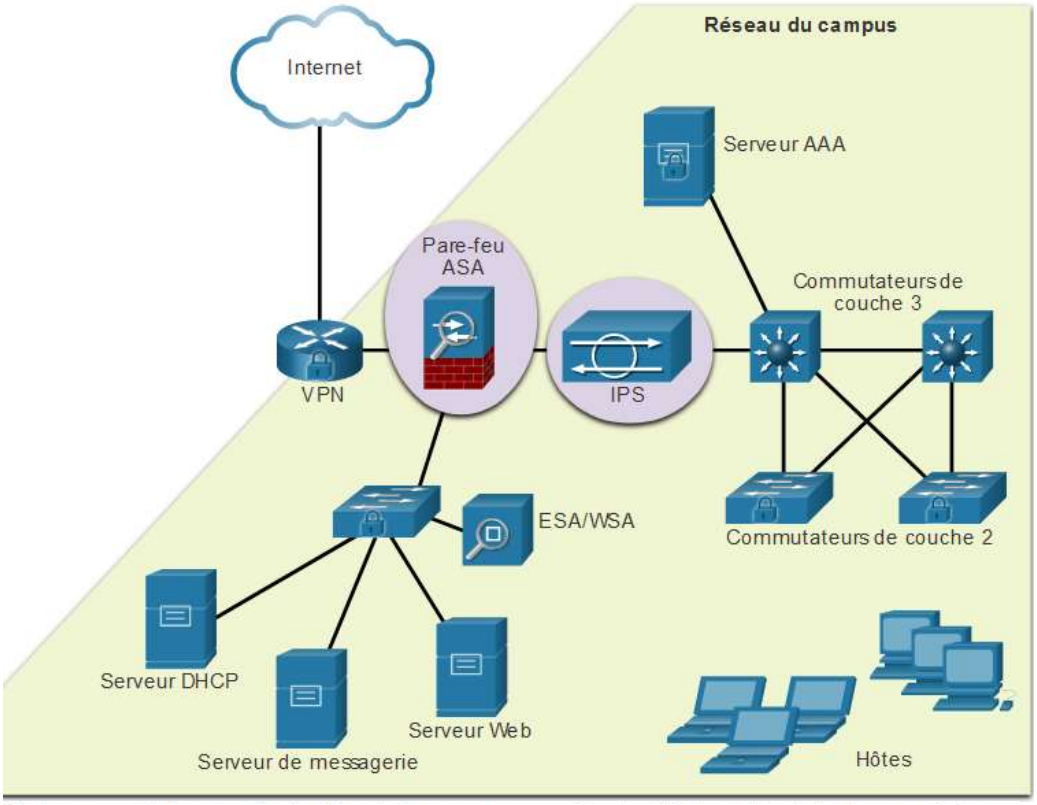
L'Approche de Défense en Profondeur

Maintenant que vous en savez plus sur la façon dont les acteurs de menace peuvent pénétrer les réseaux, vous devez comprendre ce qu'il faut faire pour empêcher cet accès non autorisé. Cette rubrique détaille plusieurs actions que vous pouvez entreprendre pour rendre votre réseau plus sécurisé.

Pour atténuer les attaques réseau, vous devez d'abord sécuriser les périphériques, y compris les routeurs, les commutateurs, les serveurs et les hôtes. La pluPartie des organisations utilisent une approche de défense en profondeur (également connue sous le nom d'approche par couches) de la sécurité. Pour cela, divers appareils réseau et services doivent fonctionner en tandem.

Prenons l'exemple du réseau de la figure. Plusieurs périphériques et services de sécurité sont mis en œuvre pour protéger les utilisateurs et les ressources contre les menaces TCP/IP.

Tous les périphériques réseau, y compris le routeur et les commutateurs, sont également renforcés, comme l'indiquent les verrous combinés sur leurs icônes respectives. Cela signifie qu'ils ont été sécurisés pour empêcher les acteurs de menace d'accéder et de falsifier les périphériques.



Plusieurs appareils et services de sécurité sont mis en œuvre pour protéger les utilisateurs et les atouts d'une organisation contre les menaces TCP / IP.

- **VPN** - Un routeur est utilisé pour fournir des services VPN sécurisés avec des sites d'entreprise et un support d'accès à distance pour les utilisateurs distants à l'aide de tunnels cryptés sécurisés.
- **Pare-feu ASA** - Cet appareil dédié fournit des services de pare-feu avec état. Il garantit que le trafic interne peut sortir et revenir, mais le trafic externe ne peut pas établir de connexions avec des hôtes internes.
- **IPS** - Un système de prévention des intrusions (IPS) surveille le trafic entrant et sortant à la recherche de logiciels malveillants, de signatures d'attaques réseau, etc. S'il détecte une menace, il peut immédiatement l'arrêter.
- **ESA/WSA** - L'appliance de sécurité de messagerie (ESA) filtre les spams et les e-mails suspects. L'appliance de sécurisation du web filtre (WSA) les sites de malwares Internet connus et suspects.
- **Serveur AAA** - Ce serveur contient une base de données sécurisée de qui est autorisé à accéder et à gérer les périphériques réseau. Les périphériques réseau authentifient les utilisateurs administratifs à l'aide de cette base de données.

Conserver les sauvegardes

La sauvegarde des données est l'un des moyens de protection les plus efficaces contre la perte de données. Une sauvegarde de données stocke une copie des informations de l'ordinateur sur un support amovible qui peut être conservé en lieu sûr. Les périphériques d'infrastructure doivent avoir des sauvegardes de fichiers de configuration et d'images IOS sur un serveur FTP ou similaire. Si l'ordinateur ou un matériel de routeur échoue, les données ou la configuration peuvent être restaurées à l'aide de la copie de sauvegarde.

La sauvegarde des données doit donc être effectuée régulièrement. Elle doit faire partie de la politique de sécurité. Les sauvegardes sont généralement stockées en dehors des installations, afin de protéger le support de sauvegarde en cas de sinistre dans le bâtiment principal. Les hôtes Windows disposent d'un utilitaire de sauvegarde et de restauration. Cet utilitaire permet aux utilisateurs de sauvegarder leurs données sur un autre lecteur ou sur stockage basé sur le cloud.

Le tableau présente les considérations relatives à la sauvegarde et leurs descriptions.

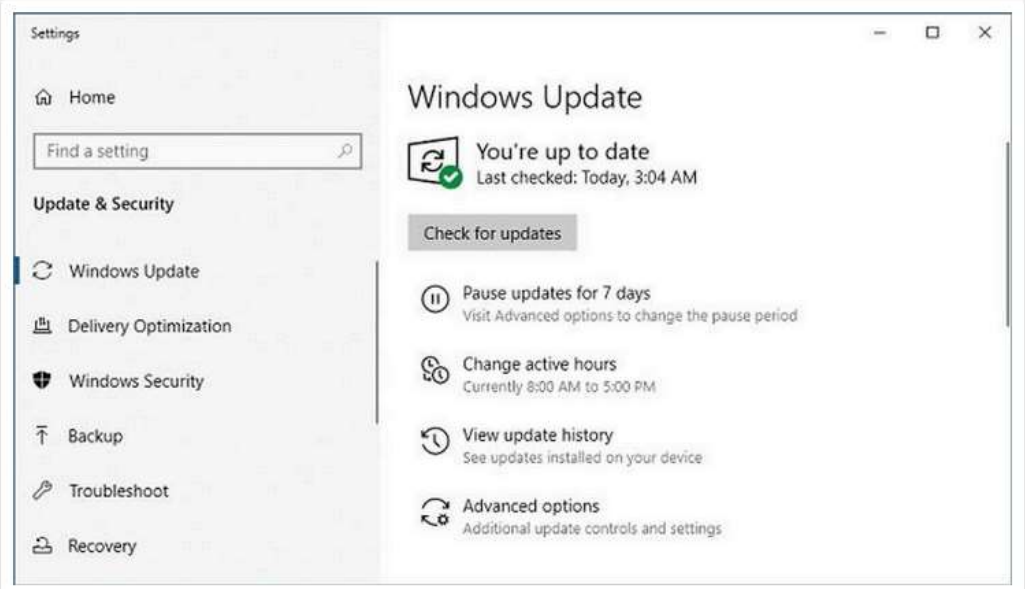
Considération	Description
Fréquence	• Sauvegardez régulièrement les données conformément à la politique de sécurité. • Les sauvegardes complètes peuvent prendre du temps, c'est pourquoi elles doivent être effectuées mensuellement ou hebdomadaires avec des sauvegardes partielles fréquentes des fichiers modifiés.
Stockage	• Validez toujours les sauvegardes afin de garantir l'intégrité des données et de valider les procédures de restauration des fichiers.
Sécurité	• Les sauvegardes doivent être transportées vers un stockage hors site approuvé au cours d'une rotation quotidienne, hebdomadaire ou mensuelle, comme l'exige de la politique de sécurité
Validation	• Les sauvegardes doivent être protégées à l'aide de mots de passe forts. Le mot de passe est requis pour restaurer les données.

Mise à niveau, mise à jour et correctif

Pour se protéger efficacement des attaques réseau, il faut s'informer en continu sur les menaces. Au fur et à mesure que de nouveaux programmes malveillants apparaissent, les entreprises doivent acquérir la version la plus récente de leur logiciel antivirus.

La meilleure façon de limiter les risques d'attaque de ver est de télécharger les mises à jour de sécurité du fournisseur du système d'exploitation et d'appliquer des correctifs sur tous les systèmes vulnérables. L'administration d'un grand nombre de systèmes implique la création d'une image logicielle standard (système d'exploitation et applications accréditées dont l'utilisation est autorisée sur les systèmes clients) déployée sur les systèmes nouveaux ou mis à niveau. Toutefois, les exigences de sécurité évoluent et il sera peut-être nécessaire d'installer des correctifs de sécurité mis à jour sur les systèmes déjà déployés.

Une solution pour la gestion des correctifs de sécurité critiques consiste à s'assurer que tous les systèmes finaux téléchargent automatiquement les mises à jour, comme illustré pour Windows 10 dans la figure. Les correctifs de sécurité sont automatiquement téléchargés et installés sans intervention de l'utilisateur.

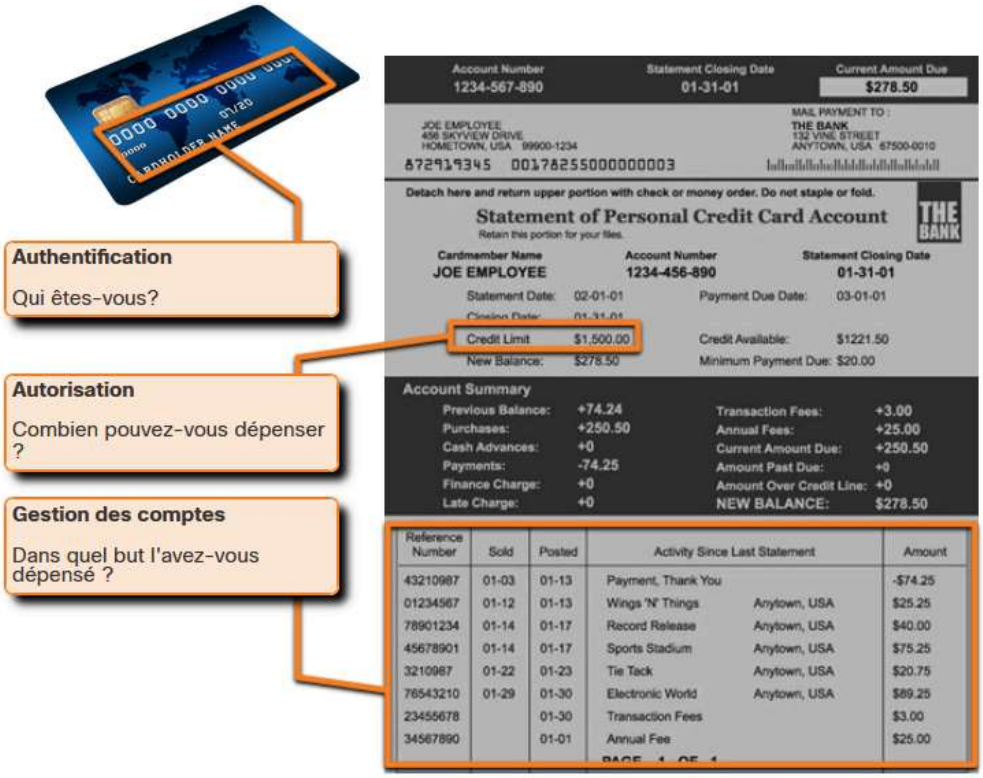


Authentification, autorisation et gestion des comptes

Tous les périphériques réseau doivent être configurés en toute sécurité de manière à ne fournir l'accès qu'aux personnes autorisées. Les services de sécurité réseau d'authentification, d'autorisation et de gestion des comptes fournissent la structure principale permettant de mettre en place un contrôle d'accès sur un périphérique réseau.

L'AAA est un moyen de contrôler qui est autorisé à accéder à un réseau (authentification), quelles sont les actions qu'il effectue lors de l'accès au réseau (autorisation), et d'enregistrer ce qui a été fait pendant son séjour (gestion des comptes).

Le concept des services d'authentification, d'autorisation et de gestion des comptes est similaire à l'utilisation d'une carte de crédit. La carte de crédit identifie qui est autorisé à l'utiliser, combien cet utilisateur peut dépenser et consigne les achats de l'utilisateur (cf. figure).



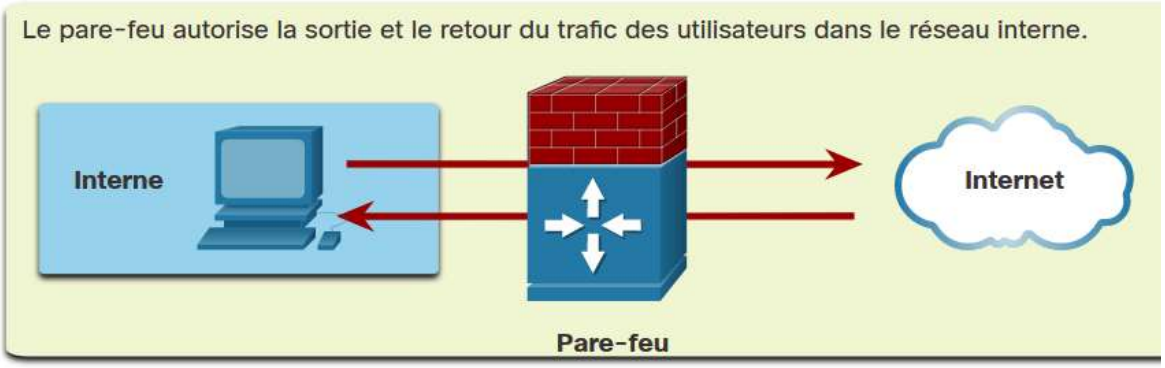
Pare-feu

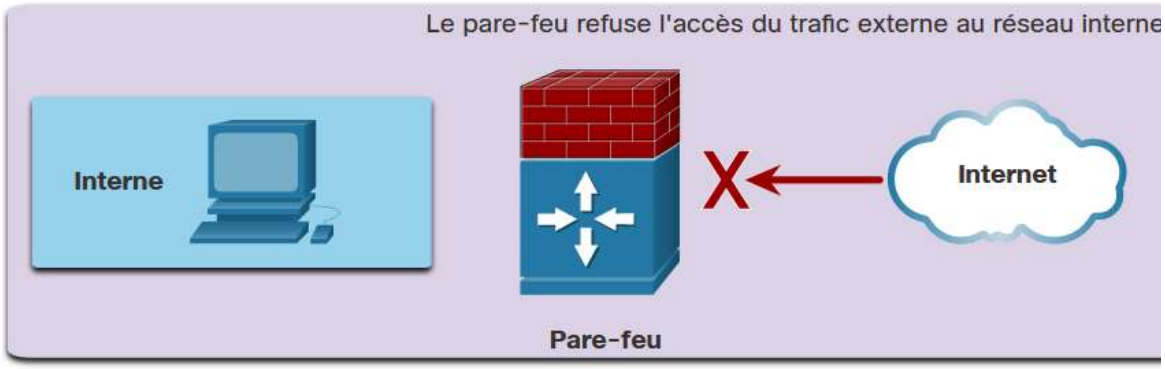
Un pare-feu est l'un des outils de sécurité disponibles les plus efficaces pour protéger les utilisateurs contre les menaces externes. Un pare-feu protège les ordinateurs et les réseaux en empêchant le trafic indésirable de pénétrer dans les réseaux internes.

Un pare-feu se trouve entre deux réseaux, ou plus, et contrôle le trafic entre eux tout en contribuant à interdire les accès non autorisés. Par exemple, la topologie supérieure de la figure montre comment le pare-feu permet au trafic provenant d'un hôte réseau interne de quitter le réseau et de revenir vers le réseau interne. La topologie inférieure montre comment le trafic initié par le réseau externe (c'est-à-dire Internet) se voit refuser l'accès au réseau interne.

La figure montre un rectangle, étiqueté Inside. À l'intérieur du rectangle, il y a un pc. À l'extérieur et à droite du rectangle, il y a un pare-feu. Au droit du pare-feu, il y a un cloud étiqueté, Internet. Il y a deux flèches, une indiquant le trafic laissant le PC passer par le pare-feu et vers le L'Internet. La deuxième flèche indique que le pare-feu autorise le trafic depuis l' internet à l'ordinateur. La figure montre un autre rectangle, étiqueté Inside. À l'intérieur du rectangle, il y a un pc. À l'extérieur et à droite du rectangle, il y a un pare-feu. Au droit du pare-feu, il y a un cloud étiqueté, Internet. Il y a une flèche pointant d'Internet vers le pare-feu avec un X indiquant que le trafic est étant refusé de l'Internet au réseau interne.

Fonctionnement du pare-feu

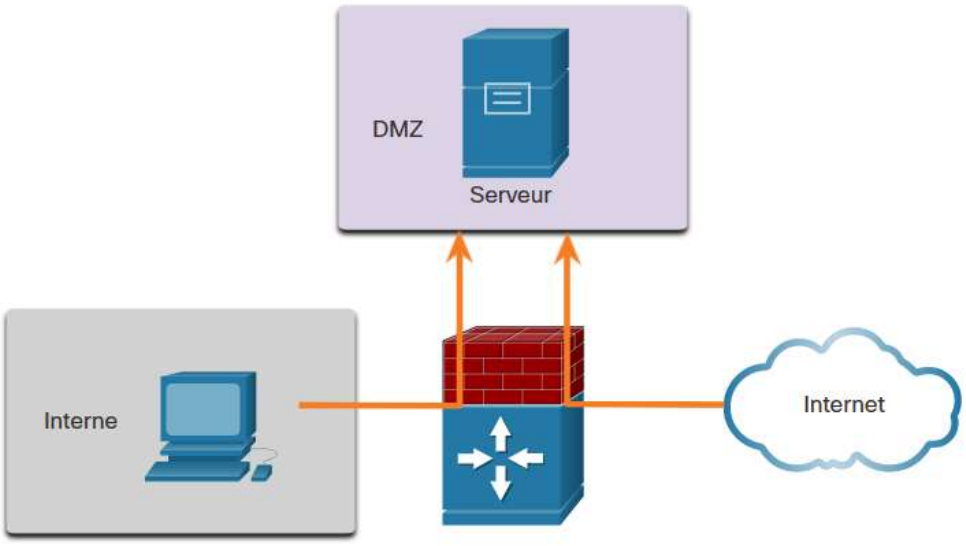




Un pare-feu permet aux utilisateurs externes de contrôler l'accès à des services spécifiques. Par exemple, les serveurs accessibles aux utilisateurs externes se trouvent généralement sur un réseau spécial appelé «zone démilitarisée» (DMZ), comme le montre la figure. La zone DMZ permet à un administrateur réseau d'appliquer des politiques spécifiques pour les hôtes connectés à ce réseau.

La figure montre un rectangle, étiqueté Inside. À l'intérieur du rectangle, il y a un pc. À l'extérieur et à droite du rectangle, il y a un pare-feu. Au droit du pare-feu, il y a un nuage étiqueté Internet. Au-dessus du pare-feu, est un serveur DMZ à l'intérieur d'un rectangle. Il y a deux flèches, l'une va depuis le PC via le pare-feu vers le serveur DMZ et un autre allant du Internet via le pare-feu vers le serveur DMZ.

Topologie de pare-feu avec DMZ



Types de pare-feu

Les pare-feu sont disponibles sous plusieurs formes, comme l'illustre la figure. Les pare-feu emploient diverses techniques pour déterminer les accès autorisés à un réseau ou les accès à interdire. On trouve notamment les produits suivants:

- **Filtrage des paquets** - Empêche ou autorise l'accès sur la base d'adresses IP ou MAC
- **Filtrage des applications** - Interdit ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de ports.
- **Filtrage des URL** - Empêche ou permet l'accès à des sites web basés sur des URL ou des mots clés spécifiques

- **Inspection minutieuse des paquets (SPI)** - Les paquets entrants doivent être des réponses légitimes aux demandes des hôtes internes. Les paquets non sollicités sont bloqués, sauf s'ils sont expressément autorisés. L'inspection SPI peut éventuellement reconnaître et filtrer des types d'attaques spécifiques telles que le déni de service (DoS).

16.3.7

Sécurité des points de terminaison

Un point de terminaison, ou hôte, est un système informatique ou un périphérique qui tient lieu de client réseau. Les terminaux les plus courants sont les ordinateurs portables, les ordinateurs de bureau, les serveurs, les smartphones et les tablettes. La sécurisation des points de terminaison est l'une des tâches les plus difficiles pour un administrateur réseau, car elle implique de prendre en compte le facteur humain. L'entreprise doit mettre en place des stratégies bien documentées et les employés doivent en être informés. Ils doivent également être formés sur l'utilisation appropriée du réseau. Les stratégies incluent souvent l'utilisation de logiciels antivirus et la prévention des intrusions sur les hôtes. Des solutions plus complètes de sécurisation des terminaux reposent sur le contrôle de l'accès au réseau.

Modifié le: mardi 5 mars 2024, 14:14

◄ 16.2.1 - Attaques de réseau

Aller à...

16.4.1 - Sécurité des périphériqu