Considérations de sécurité liées aux pare-feu

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Novembre 2023 | ITSAP.80.039

Un pare-feu est un mécanisme de sécurité permettant de surveiller et de contrôler le trafic entrant et sortant en fonction des règles établies dans les politiques de l'organisation. Les pare-feu constituent un volet essentiel du contrôle de sécurité qui permet de segmenter votre réseau pour empêcher qu'un flux non autorisé de données passe d'une zone du réseau à une autre. Le trafic qui circule par les pare-feu contient souvent les données de votre organisation. Si les pare-feu ne sont pas correctement configurés ou entretenus, ceux-ci risquent d'être exploités par des auteures et auteurs de menace, ce qui risquerait de compromettre vos données. Qu'il s'agisse d'une petite, d'une moyenne ou d'une grande organisation, la présente publication saura fournir à l'organisation des directives sur les mesures à prendre pour assurer la protection de ses pare-feu.

Quels sont les cas d'utilisation de déploiement général pour les pare-feu?

Les pare-feu peuvent être placés à différents points de votre réseau pour créer des zones de trafic en fonction de votre cas d'utilisation. La liste qui suit présente des scénarios de déploiement pour des pare-feu:

En réseau: Il s'agit de pare-feu matériels ou basés sur un logiciel qui sont en général installés entre les limites du réseau ou au périmètre de celui-ci. Leur mission est de protéger le réseau contre des menaces, par exemple, en empêchant l'accès d'un trafic Internet malveillant à votre réseau d'entreprise. Dans un environnement virtualisé, ces pare-feu peuvent aussi être utilisés pour concevoir des secteurs segmentés de zones de confiance à même le réseau. Ils sont habituellement utilisés dans des solutions de réseau à définition logicielle (SDN pour *Software Defined Networking*) et de réseau étendu (WAN pour *Wide Area Network*) pour améliorer la sécurité et la gestion des réseaux.

En mode hôte: Il s'agit de pare-feu logiciels ou en mode agent qui sont installés aux points d'extrémité ou sur des serveurs; des ordinateurs ou des dispositifs en sont des exemples. Leur rôle est de limiter le trafic réseau entrant et sortant pour protéger le dispositif sur lequel a été configuré le pare-feu. Un exemple courant est le pare-feu qui est intégré dans les principaux systèmes d'exploitation.

Sur application: Ces pare-feu sont déployés pour gérer le trafic entrant et sortant d'une application de système ou d'un service sur place ou sur le nuage. Ils sont proposés comme option matérielle ou virtuelle, et leur objectif principal est d'assurer une protection contre des attaques de couche application. Ils sont généralement déployés pour protéger les applications Web et mobiles, les interfaces de programmation d'applications (API pour *Application Programming Interface*) et les services. Les pare-feu d'applications Web (ou WAF) servent à détecter et à bloquer tout trafic malveillant de protocole de transfert hypertexte (HTTP). Des solutions par mandataire intègrent également ces capacités de sorte qu'il sera plus difficile pour les auteures et auteurs de menace de lancer une attaque par déni de service distribué (ou attaque par DDoS).

Basé sur l'infonuagique: Ces pare-feu virtuels sont principalement déployés dans un environnement infonuagique pour contrôler le flux du trafic qui entre et sort de l'architecture infonuagique (p. ex. entre des zones non fiables, comme Internet, et des zones fiables, comme les segments sur place de votre organisation). Les pare-feu basés sur l'infonuagique imposent des politiques et des autorisations pour protéger les données et les ressources sur le nuage.

Quels sont les risques associés aux pare-feu?

Lors de la mise en œuvre de pare-feu, une des plus graves erreurs consiste à conserver les configurations par défaut du fournisseur. Les pare-feu ne sont pas vendus avec des paramètres établis pouvant être utilisés dès leur sortie de l'emballage; ils doivent plutôt être configurés en fonction des utilisations prévues pour chaque réseau. Le fait de ne pas changer les configurations par défaut peut accroître la vulnérabilité de votre organisation face à des compromissions. De la même façon, des pare-feu mal configurés peuvent également rendre votre réseau vulnérable face à des auteures et auteurs de menace. Les menaces potentielles suivantes sont associées au déploiement et à la gestion des pare-feu:

- des vulnérabilités du jour zéro peuvent se trouver dans les progiciels ou logiciels des pare-feu et être exploitées par des auteures et auteurs de menace pour accéder à vos réseaux et ressources informatiques.
- des composants ou des maliciels exploitables peuvent se trouver dans les pare-feu fabriqués par des fournisseurs qui n'ont pas recours à des pratiques de sécurité adéquates et solides.
- des correctifs logiciels ou matériels désuets peuvent être présents.
- les pare-feu mal configurés peuvent entraîner des violations de données ou des pertes de données et rendre votre organisation non conforme aux normes réglementaires.

Qu'est-ce qu'un pare-feu de prochaine génération (NGFW)?

Les types traditionnels de pare-feu contrôlent le trafic sur le réseau en fonction des états, des ports et des protocoles qui sont des filtres s'appuyant sur des règles prédéfinies. Un pare-feu de prochaine génération (NGFW pour *Next-Generation Firewall*) procure toute la fonctionnalité d'un pare-feu traditionnel, mais il comporte aussi des capacités renforcées, notamment la détection de maliciels. Les NGFW peuvent non seulement inspecter l'en-tête du paquet, mais aussi son contenu et sa source. Parmi les autres fonctionnalités que peuvent offrir les NGFW, notons:

- le système de prévention d'intrusion (SPI)
- le système de détection d'intrusion (SDI)
- la protection standard basée sur des politiques
- le filtrage d'applications
- le blocage de la géolocalisation
- la protection antivirus (AV)
- le filtrage par localisateur de ressources uniforme (URL pour *Uniform Resource Locator*)
- le soutien au réseau privé virtuel (RPV)
- l'inspection du trafic à travers les protocoles SSL/TLS
- la protection par DDoS
- la prévention de la perte de données (DLP pour *Data Loss Prevention*)
- la protection de courriels

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Considérations de sécurité liées aux pare-feu

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Novembre 2023 | ITSAP.80.039

Protection de votre pare-feu

Les pare-feu à eux seuls, même s'ils sont adéquatement configurés, ne suffisent pas à protéger votre réseau contre du trafic vers des réseaux malveillants. Comme la plupart des contrôles de sécurité et conformément à une pratique exemplaire, les pare-feu devraient être utilisés dans le cadre d'une approche de défense en profondeur/défense en couches pour renforcer la résistance de votre organisation aux cyberattaques. Pour connaître d'autres mesures à mettre en œuvre pour protéger vos réseaux et dispositifs, consultez Les outils de sécurité préventive (ITSAP.00.058). Selon les besoins de votre organisation, et les biens à risque, voici quelques importantes mesures qui peuvent aider à protéger vos pare-feu:

- ☐ Acheter des produits à des fournisseurs de confiance qui font appel à des pratiques strictes de protection de la sécurité. Il est nécessaire de valider leur intégrité en effectuant une vérification de hachage pour s'assurer que les valeurs correspondent à la base de données du fournisseur.
- ☐ Actualiser les dispositifs réseau au moyen de progiciels de confiance, et ce, avant leur première utilisation. Effectuer une vérification de hachage ou de somme de contrôle pour vérifier l'intégrité du fichier de progiciel téléchargé. Ainsi, il sera possible de réduire les risques liés à la cybersécurité et à la chaîne d'approvisionnement, comme l'introduction d'un progiciel malveillant.
- ☐ Installer des mises à jour logicielles et des correctifs régulièrement et dès qu'ils sont disponibles.
- ☐ Surveiller et vérifier les journaux de vérification des pare-feu pour détecter toute activité inhabituelle ou suspecte. Passer régulièrement en revue les journaux pour identifier de potentiels incidents liés à la sécurité, comme des tentatives d'accès non autorisées ou des habitudes de trafic inhabituelles. Pour obtenir plus de renseignements, consultez Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085).
- ☐ Définir des processus des changements stricts pour assurer que tous les changements fassent l'objet d'un suivi et soient conformes aux politiques de sécurité de l'organisation.
- ☐ Établir un poste de travail administratif sécurisé pour gérer la configuration des pare-feu. Ce poste doit être isolé du réseau et ne pas autoriser l'accès à Internet. S'il existe un motif valable sur le plan professionnel pour qu'un poste de travail ait accès à Internet, il faut alors protéger ce poste en intégrant des contrôles supplémentaires comme l'authentification multifacteur (AMF) ou une liste d'IP autorisés limitant l'accès aux adresses IP de confiance. Pour obtenir plus de renseignements, consultez Les 10 mesures de sécurité des TI : N°3 Gestion et contrôle des privilèges d'administrateur (ITSM.10.094).
- ☐ Changer tous les mots de passe administratifs par défaut et limiter le nombre d'administratrices et d'administrateurs de système qui peuvent apporter des modifications aux dispositifs de coupe-feu. S'assurer que chacun possède son propre compte avec des phrases passe ou mots de passe forts et une AMF, dans la mesure du possible.
- ☐ Utiliser un antivirus et un antimaliciel (ou les activer s'ils font partie d'une fonction intégrée des pare-feu) pour protéger les systèmes contre des programmes malveillants. Pour obtenir plus de renseignements, consultez Protéger votre organisation contre les maliciels (ITSAP.00.057).
- ☐ Gérer les politiques sur les pare-feu en examinant et en mettant à jour régulièrement les règles pour s'assurer qu'elles sont dans le bon ordre et qu'elles reflètent l'architecture actuelle. Vérifier si les règles présentent des failles de sécurité (p. ex. des services, des ports ou des protocoles vulnérables). Nettoyer et supprimer les règles qui sont temporaires ou qui ne devraient plus être utilisées.
- ☐ Désactiver les ports (physiques et virtuels) et les services non utilisés sur les pare-feu. Cette mesure peut réduire le risque que des auteures et auteurs de menace se connectent au réseau s'ils arrivent à accéder physiquement à ces dispositifs.
- ☐ Retirer les pare-feu réseau qui ne sont plus pris en charge par le fournisseur. Mettre ces dispositifs à niveau ou les remplacer dès que possible.
- ☐ Utiliser plusieurs pare-feu pour segmenter et sécuriser les réseaux essentiels qui comportent des données sensibles. Isoler les réseaux essentiels d'Internet et des autres secteurs du réseau d'entreprise. Pour obtenir plus de renseignements, consultez Les 10 mesures de sécurité des TI : N° 5, Segmenter et séparer les informations (ITSM.10.092).
- ☐ Envisager de recourir à des pare-feu vendus par différents fournisseurs pour protéger les zones sensibles du réseau. Ainsi, si un fabricant signale un défaut ou une vulnérabilité de sécurité de son produit, il est possible que les produits d'un autre fabricant ne présentent pas les mêmes vulnérabilités.
- ☐ Utiliser une solution de pare-feu de système de noms de domaine (DNS) pour le filtrage du contenu afin de protéger les employées/employés qui pourraient visiter par inadvertance des domaines malveillants sur Internet. Votre organisation pourrait ainsi être protégée contre des attaques par hameçonnage, car le pare-feu de DNS bloquera l'accès au site malveillant. Pour obtenir plus de renseignements, consultez Système d'adressage par domaine de protection (ITSAP.40.019). L'Autorité canadienne pour les enregistrements Internet (ACEI) propose un DNS de protection appelé le Bouclier canadien.
- ☐ Penser à activer le mode transparent s'il est offert sur les pare-feu. Les pare-feu transparents sont associés à un épuisement des adresses IP dans le réseau, ce qui fait en sorte que les auteures et auteurs de menace ont plus de difficulté à les détecter. Ces pare-feu sont donc moins vulnérables aux cyberattaques, comme l'attaque par déni de service (DoS pour *Denial of Service*).
- ☐ Conserver des sauvegardes de pare-feu pour être en mesure de rapidement restaurer les paramètres en cas de panne ou d'incident de sécurité. Stocker en toute sécurité les sauvegardes et tester le processus de restauration régulièrement. Il faut à tout le moins faire une sauvegarde des configurations de pare-feu et, si possible, réaliser une sauvegarde physique de l'équipement avec ou sans les configurations.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada