LIVRE BLANC

Protection de votre réseau de l'intérieur

Firewall de Segmentation Interne (Internal Segmentation Firewall - ISFW)

Table des matières

Résumé

Au cours de la dernière décennie, les entreprises ont essayé de protéger leurs réseaux en élaborant des systèmes de défenses à travers les frontières de leur réseau. Cela comprend la périphérie d'Internet, le périmètre, le terminal et le datacenter (y compris le DMZ). Cette approche « du périmètre au cœur » repose sur le concept que les entreprises peuvent très bien contrôler des points d'entrée définis et sécuriser leurs précieuses ressources. La stratégie consistait à élaborer une défense périphérique aussi robuste que possible tout en considérant que rien ne pouvait franchir le Firewall.

Tandis que les entreprises se développent et adoptent les dernières technologies informatiques comme Mobility et le Cloud, les limites des réseaux traditionnels sont de plus en plus complexes à contrôler et à sécuriser. Les réseaux comprennent désormais de nombreuses failles de sécurité.

Il n'y a pas si longtemps, les fournisseurs de Firewall marquaient les ports de leurs appliances comme suit : « Externe » (non fiable) et « Interne » (fiable). Les menaces avancées exploitent cela à leur avantage car, une fois à l'intérieur, le réseau est très plat et ouvert. Le réseau interne est généralement constitué d'appareils « conscients » non sécurisés comme des switches, des routeurs et même des ponts. Par conséquent, dès que vous accédez au réseau en tant que hacker, prestataire, voire même employé malhonnête, vous disposez d'un libre accès à l'intégralité du réseau de l'entreprise, y compris à toutes les ressources précieuses.

La solution : une nouvelle catégorie de Firewall, le Firewall de Segmentation Interne (ISFW). Ce Firewall est installé en des points stratégiques du réseau interne. Il peut être installé devant des serveurs spécifiques sur lesquels sont conservés des biens intellectuels précieux ou devant un ensemble d'appareils utilisateur ou d'application Web sur le Cloud.

Principales exigences

- **PROTECTION COMPLÈTE**
  Protection de l'intérieur continue contre les menaces avancées avec une seule infrastructure de sécurité
- **AXÉE SUR LA STRATÉGIE**
  Pour mieux contrôler et segmenter les utilisateurs et limiter l'accès des vecteurs de menace aux ressources sensibles
- **DÉPLOIEMENT AISÉ**
  Un mode transparent par défaut signifie qu'il n'est pas nécessaire de redéfinir l'architecture du réseau ni de mettre en place un déploiement et une gestion centralisés
- **HAUTES PERFORMANCES**
  Les performances de plusieurs gigabits prennent en charge le débit filaire du trafic est-ouest

Une fois en place, l'ISFW doit garantir une « visibilité » instantanée de cette ressource réseau précieuse, en évitant une planification ou un déploiement du réseau s'échelonnant sur plusieurs mois.

Mais surtout, l'ISFW doit également offrir une « protection », car la détection ne constitue qu'une partie de la solution. Étudier les journaux et les alertes peut prendre des semaines ou des mois. L'ISFW doit donc assurer une segmentation proactive et une protection en temps réel s'appuyant sur les dernières mises à jour en matière de sécurité.

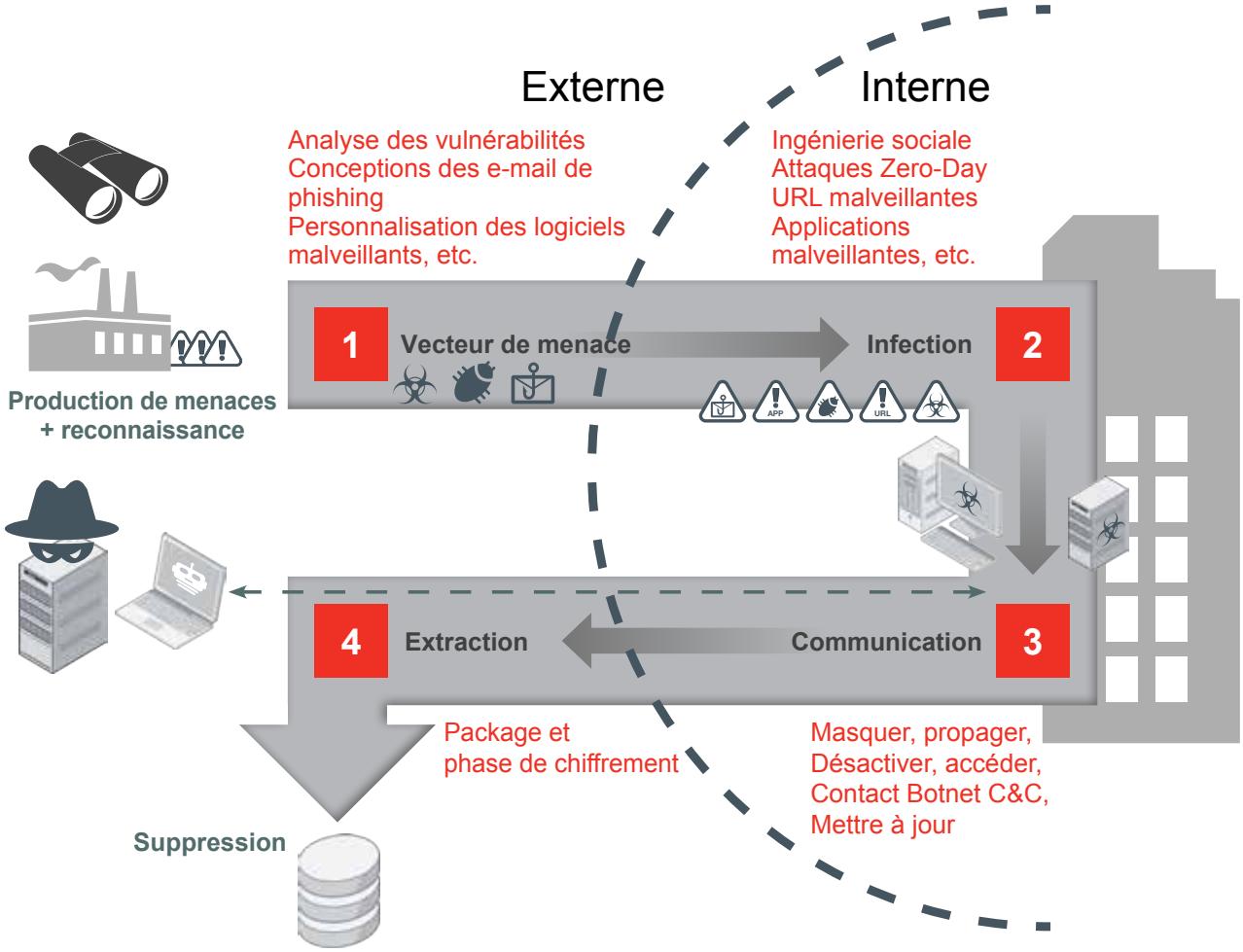
Enfin, l'ISFW doit être suffisamment flexible pour être installé n'importe où au sein du réseau interne et s'intégrer aux autres parties de la solution de sécurité de l'entreprise à partir d'un point de gestion unique. Les autres solutions de sécurité (passerelle de messagerie, passerelle Web, Firewall de périmètre, Firewalls de Cloud et terminaux) peuvent également offrir une visibilité et une protection supplémentaires. En outre, les Firewalls de Segmentation Interne doivent être dimensionnés pour supporter des débits faibles à élevés permettant le déploiement à l'échelle du réseau.

Les menaces avancées tirent profit du réseau « interne plat »

Les cybercriminels créent des attaques personnalisées pour éviter les défenses traditionnelles, puis, une fois à l'intérieur, pour ne pas se faire détecter et récupérer des données précieuses. Une fois à l'intérieur du réseau, peu de systèmes sont mis en place pour détecter ou mieux protéger le réseau contre les menaces persistantes avancées.

Le cycle de vie des menaces, illustré sur la figure 1, montre un franchissement de la limite périphérique ; la majeure partie de l'activité se produit dans le périmètre du réseau. Parmi ces activités figurent la désactivation de la sécurité reposant sur les agents, les mises à jour à partir du système de commande et de contrôle botnet, ainsi que l'infection/la récupération et l'extraction supplémentaires de ressources ciblées.

FIGURE 1 – CYCLE DE VIE DES MENACES AVANCÉES



La réponse : une nouvelle catégorie de Firewall – le Firewall de Segmentation Interne (ISFW)

Le développement de la plupart des Firewall au cours de la dernière décennie s'est concentré sur la frontière, la périphérie d'Internet, le périmètre (Firewall hôte), le terminal, le datacenter (DMZ) ou le Cloud. Tout a commencé par les Firewalls stateful avant d'évoluer vers la gestion unifiée des menaces (UTM) pour les réseaux distribués, réunissant le Firewall, la détection des intrusions et un antivirus. Est venu ensuite le Next Generation Firewall (NGFW), qui comprend la prévention contre les intrusions et le contrôle des applications au niveau de la périphérie Internet. Enfin, dernièrement, suite à la hausse considérable du débit, les Firewalls de datacenter (DCFW) sont apparus pour offrir un débit supérieur à 100 Gbps. Tous ces Firewalls se caractérisent par une approche commune : ils sont conçus pour assurer une protection par l'extérieur.

Pour un déploiement et une protection internes rapides, une nouvelle catégorie de Firewall s'impose, le Firewall de Segmentation Interne (ISFW). Le Firewall de Segmentation Interne intègre quelques caractéristiques différentes par rapport à un Firewall Border. Ces différences sont présentées sur la figure 2.

Fondement de l'ISFW

Les entreprises doivent déployer l'ISFW avec des fonctionnalités de nouvelle génération en des points stratégiques du réseau interne, afin d'apporter une couche de protection supplémentaire et fournir les avantages suivants en termes de sécurité :

- Contrôle des accès aux ressources aussi proche que possible de l'utilisateur par le biais d'une segmentation axée sur la stratégie en vigueur.
- Établissement de barrières de sécurité permettant d'interrompre et de limiter la propagation incontrôlée des menaces et de l'activité des hackers au sein du réseau interne par le biais de la mise en œuvre de mécanismes de sécurité avancés.
- Limitation des dommages potentiels inhérents aux menaces au sein du périmètre.
- Augmentation de la visibilité des menaces et amélioration de la détection et de la neutralisation des brèches.
- Renforcement de la stratégie de sécurité globale de l'entreprise.

Mode de déploiement	ISFW	NGFW	DCFW	UTM	CCFW
Objectif	Visibilité et protection pour les segments internes	Visibilité et protection contre les menaces externes et les activités Internet	Protection du réseau haute performance avec une faible latence	Visibilité et protection contre les menaces externes et les activités des utilisateurs	Sécurité du réseau pour les prestataires de services
Localisation	Couche d'accès	Passerelle Internet	Couche centrale/ passerelle CC	Passerelle Internet	Divers
Mode de fonctionnement du réseau	Mode transparent	Mode NAT/routage	Mode NAT/routage	Mode NAT/routage	Mode NAT/routage
Exigences matérielles	Densité de port supérieure pour protéger plusieurs ressources	Ports GbE et 10GbE	Haut débit (GbE/10 GbE/40 GbE/100) et densité de port élevée, accélération matérielle	Densité de port GbE élevée, connectivité sans fil intégrée et POE	Haut débit (GbE/ 10 GbE/40 GbE) et densité de port élevée, accélération matérielle
Composants de sécurité	Firewall, IPS, ATP, contrôle des applications	(Basé sur les utilisateurs) Firewall, VPN, IPS, contrôle des applications	Firewall, protection DDoS	Intégration complète et extensible des clients et des appareils	Firewall, CGN, LTE & sécurité mobile
Autres caractéristiques	Déploiement rapide – quasiment aucune configuration	Intégration à la protection contre les menaces avancées (Sandbox)	Haute disponibilité	WAN différent Options de connectivité comme 3G4G	Haute disponibilité

FIGURE 2 – DIFFÉRENCES ENTRE LES TYPES DE FIREWALL

L'ISFW doit fournir une segmentation axée sur la stratégie en vigueur

La segmentation axée sur la stratégie en vigueur offre un meilleur contrôle et segmente l'accès de l'utilisateur aux applications et aux ressources via l'association de l'identité de l'utilisateur à l'application de stratégies de sécurité spécifiques. La segmentation axée sur la stratégie en vigueur peut limiter les menaces et les vecteurs d'attaque potentiels véhiculés par l'utilisateur.

La segmentation axée sur la stratégie en vigueur peut être définie comme étant l'association automatique de l'identité de l'utilisateur à la stratégie de sécurité appliquée. L'identité de l'utilisateur peut être définie comme un ensemble d'attributs : emplacement physique, type d'appareil utilisé pour accéder au réseau, application utilisée, etc. Comme l'identité de l'utilisateur peut changer de manière dynamique, la stratégie de sécurité appliquée doit s'adapter automatiquement et de manière dynamique également.

Afin d'obtenir l'identification utilisateur requise et les paramètres globaux indispensables à la création de stratégies de sécurité granulaires, un ISFW doit pouvoir :

1. Autoriser l'identification de l'utilisateur, de l'appareil et de l'application
2. Garantir l'intégration aux solutions de services d'annuaire pour identifier l'identité de l'utilisateur
3. Mapper de manière dynamique l'identité de l'utilisateur en fonction d'une application et d'une stratégie de sécurité spécifiques

L'ISFW doit fournir une protection complète

Le premier élément de sécurité est la visibilité. La visibilité ne peut pas être meilleure que la connaissance des paquets réseau : aspect du flux de paquets pour une application précise, origine, destination, actions entreprises (téléchargement, chargement…).

Le second élément, tout aussi important, est la protection. L'application, le contenu ou les actions ont-ils un caractère malveillant ? Ce type de trafic doit-il interagir entre deux ensembles de données ? Bien que très difficile à mettre en œuvre à travers différents types d'applications et de contenu, tout cela constitue une part importante de l'ISFW. La capacité à détecter une malveillance (fichier, application ou brèche) donne à l'entreprise le temps de réagir et de contenir la menace. Tous ces éléments de protection doivent figurer sur un seul appareil pour être efficaces.

La visibilité et la protection sont particulièrement dépendantes du service de renseignement central sur les menaces de sécurité en temps réel. Vous devriez toujours vous poser la question suivante : quelles sont les performances de la visibilité et de la protection ? Sont-elles adaptées aux dernières menaces ? C'est pourquoi tous les services de sécurité doivent être évalués régulièrement par des services de test et de certification tiers.

L'ISFW doit fournir un déploiement facile

L'ISFW doit être facile à déployer et à gérer. Garantir la simplicité signifie pour le service informatique qu'il doit pouvoir exécuter le déploiement avec la configuration minimale requise sans devoir retravailler l'architecture du réseau existant.

L'ISFW doit également pouvoir protéger différents types de ressources internes situés à différents endroits du réseau comme un ensemble de serveurs contenant des informations précieuses sur le client ou un ensemble de terminaux impossible à mettre à jour avec la dernière protection de sécurité.

Enfin, l'ISFW doit pouvoir s'intégrer aux autres composants de la solution de sécurité de l'entreprise. Les autres solutions de sécurité (passerelle de messagerie, passerelle Web, Firewall de périmètre, Firewalls de Cloud et terminaux) peuvent également offrir une visibilité et une protection supplémentaires. Ici aussi une approche de gestion depuis un point unique est requise. Cela permet de préserver la cohérence des stratégies de sécurité au niveau périphérique, dans le réseau et même en dehors du réseau, sur le Cloud.

En outre, les Firewalls traditionnels sont généralement déployés dans un mode de routage. Les interfaces (ports) sont correctement définies avec des adresses IP. Des mois de planification et de déploiement sont généralement requis. Ce temps est précieux dans l'univers actuel des cyberattaques instantanées. Il est possible de déployer rapidement un ISFW sur le réseau en limitant l'interruption au minimum. La procédure doit être aussi simple que de mettre un appareil sous tension et de s'y connecter. La transparence est indispensable au niveau du réseau et de l'application.

L'ISFW doit fournir des performances de vitesse filaire

Comme les Firewalls de Segmentation Interne sont déployés en ligne pour le zonage du réseau, ils doivent être particulièrement performants pour satisfaire les exigences du trafic « est/ouest » et ne pas se transformer en goulet d'étranglement au niveau de ces points stratégiques. Contrairement aux Firewalls situés en périphérie qui gèrent l'accès au réseau étendu ou les débits d'Internet inférieures à 1 gigabit par seconde, les réseaux internes sont nettement plus rapides avec des débits de plusieurs gigabits. Par conséquent, les ISFW doivent utiliser des débits de plusieurs gigabits et pouvoir garantir une inspection approfondie des paquets/de la connexion sans ralentir le réseau.

Exigences de la technologie ISFW

Un système d'exploitation du réseau flexible

Presque tous les modes de déploiement de Firewall requièrent l'allocation d'adresses IP et la reconfiguration du réseau dans le cadre du déploiement du routage réseau. Ce dernier offre la visibilité du trafic et des fonctions de prévention contre les menaces. À l'autre extrémité du spectre figure le mode renifleur. Plus facile à configurer, il assure la visibilité sans fournir de protection.

Le mode transparent offre l'avantage du routage réseau et des modes renifleur grâce à un déploiement rapide, la visibilité et, encore plus important, la protection. Les différences sont présentées sur la figure 3.

Mode de déploiement	Complexité du déploiement	Fonctions réseau	Haute disponibilité	Visibilité sur le trafic	Protection contre les menaces
Routage réseau	Élevée	Routage L3	✓	✓	✓
Transparent	Faible	Pont L2	✓	✓	✓
Sniffer	Faible	X	X	✓	X

FIGURE 3 – DIFFÉRENCES ENTRE LES TYPES DE FIREWALL

Une architecture matérielle évolutive

Comme les réseaux internes utilisent des débits nettement plus élevés, l'ISFW doit être conçu pour supporter un débit de protection de plusieurs gigabits. Bien que les architectures reposant uniquement sur le processeur soient flexibles, elles se transforment en goulet d'étranglement lorsqu'un débit élevé est requis. L'architecture supérieure utilise encore un processeur pour la flexibilité auquel vient s'ajouter des ASIC personnalisés pour accélérer le trafic réseau et l'inspection du contenu.

Comme l'ISFW est déployé plus près des données et des appareils, il doit parfois faire face à des environnements plus hostiles. La disponibilité d'un format plus robuste est, par conséquent, une autre exigence des ISFW.

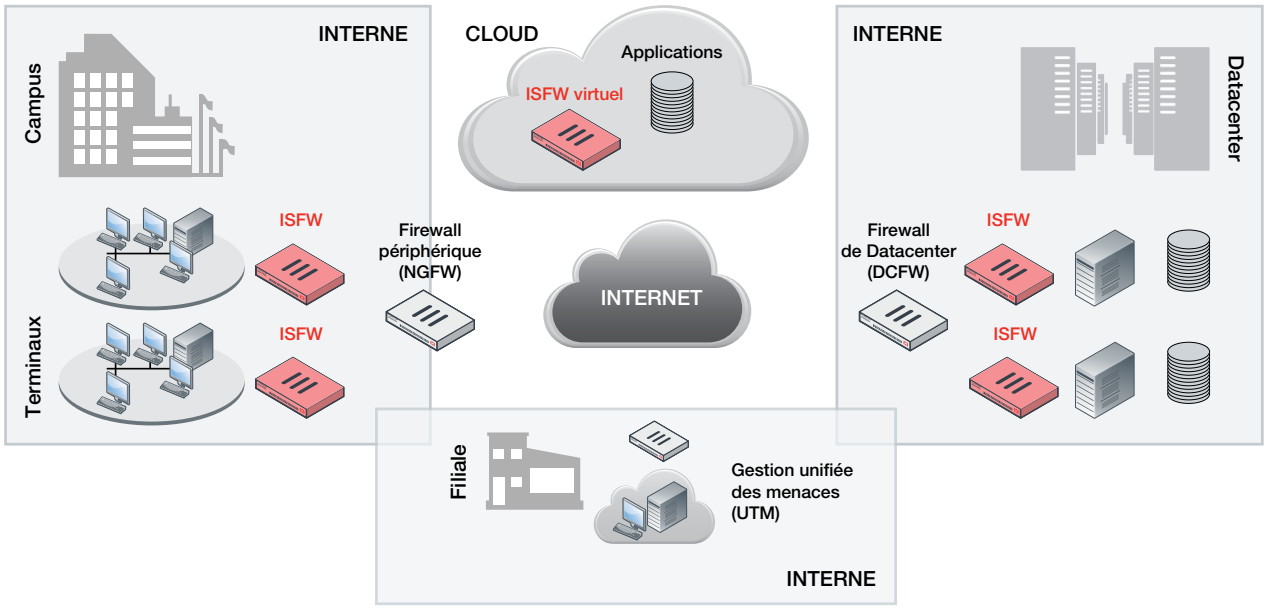


FIGURE 4 – Déploiement d'un Firewall de Segmentation Interne (ISFW)

Segmentation du réseau – Commutation haut-débit intégrée

Un aspect évolutif du mode transparent se situe dans sa capacité à séparer physiquement les sous-réseaux et les serveurs à l'aide d'un switch. Les Firewalls commencent à apparaître sur le marché sous la forme d'appliances intégrant des switches totalement fonctionnels. Ces nouveaux Firewalls, dotés de plusieurs ports 10GbE, deviennent la solution idéale pour le datacenter en permettant de sécuriser les serveurs physiquement et virtuellement. De même, des Firewalls similaires dotés de switches et de nombreuses interfaces de ports 1GbE s'imposent pour séparer les segments secondaires des réseaux locaux. Les ISFW doivent pouvoir assurer ces deux rôles, et en conséquence, intégrer idéalement des fonctionnalités de commutation totalement fonctionnelles.

Sécurité en temps réel

Les Firewalls de Segmentation Interne doivent pouvoir fournir un spectre complet de services de sécurité avancée, y compris un IPS, la visibilité sur les applications, un antivirus, un antispam et l'intégration à la technologie Sandbox basée sur le Web, afin de renforcer les stratégies qui complètent les Firewall Border standard. Cette protection et cette visibilité en temps réel sont stratégiques pour limiter la propagation des programmes malveillants au sein du réseau.

Exemple de déploiement d'un ISFW à l'échelle du réseau

La plupart des entreprises ont défini une protection périphérique avec des Firewalls, des NGFW et des UTM. Ces composants occupent toujours une place cruciale dans la protection du réseau. Cependant, afin d'améliorer la posture de sécurité, il est possible d'installer des Firewalls de Segmentation Interne à des emplacements stratégiques du réseau interne. Il peut s'agir d'un ensemble spécifique de terminaux sur lesquels mettre à jour la sécurité est compliqué ou dont les serveurs sont utilisés pour le stockage de la propriété intellectuelle.

Exemple de déploiement d'un ISFW sur un segment

L'ISFW est généralement déployé au niveau de la couche d'accès et protège un ensemble spécifique de ressources. À l'origine, le déploiement est transparent entre les switches de distribution et d'accès. À plus long terme, la commutation intégrée peut remplacer le switch d'accès et de distribution et assurer une protection physique supplémentaire.

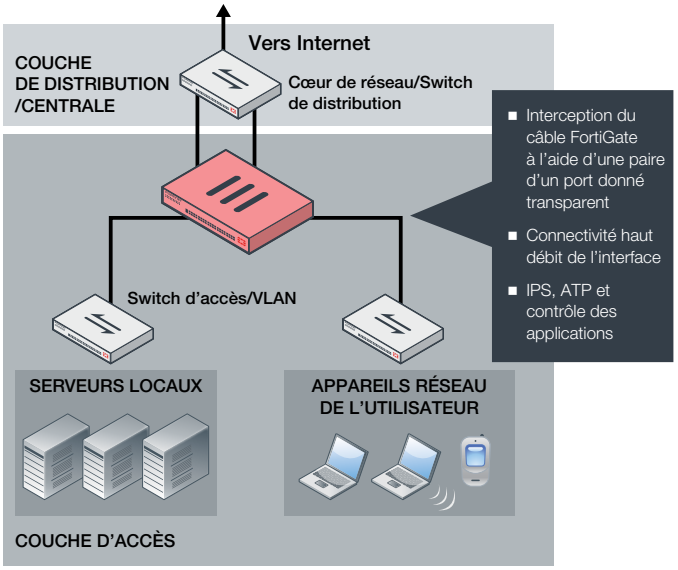


FIGURE 5 – DÉPLOIEMENT D'UN FIREWALL DE SEGMENTATION INTERNE (ISFW)

Amélioration de la protection contre les menaces avancées avec une visibilité interne

Une approche appropriée de neutralisation des menaces avancées doit intégrer un cycle continu de prévention, de détection et de neutralisation. Un Firewall de nouvelle génération sera plus précisément utilisé comme le socle principal du composant de prévention en permettant à un Firewall de niveau 2/3, un système de prévention des intrusions, le contrôle des applications et plus encore de bloquer les menaces connues tout en analysant les éléments inconnus présentant un risque élevé via la technologie Sandbox pour garantir la détection. Cependant, avec le déploiement traditionnel d'un NGFW en périphérie du réseau, vous ne profitez que d'une visibilité partielle sur le cycle de vie des attaques en observant principalement l'activité des entrées et des sorties.

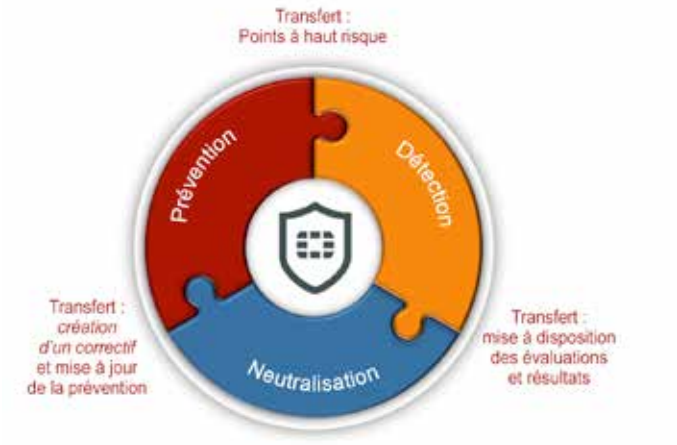


FIGURE 6 – INFRASTRUCTURE DE PROTECTION CONTRE LES MENACES AVANCÉES (ATP)

Le déploiement d'un ISFW peut offrir une visibilité complète sur l'activité interne supplémentaire des hackers une fois qu'ils ont franchi la périphérie. Les mouvements latéraux peuvent compter pour une part significative de l'activité malveillante tandis que les hackers essaient d'identifier les ressources précieuses et d'extraire les données. En outre, disposer d'une image complète de l'activité périphérique et interne améliore l'infrastructure de protection contre les menaces avancées (ATP) à tous les niveaux. Sachant que le trafic réseau interne représente souvent plusieurs fois la capacité de la bande passante du trafic périphérique, un ISFW peut offrir de nombreuses autres opportunités de limiter la propagation de la brèche à partir de techniques connues et de transmettre aisément des éléments à plus haut risque au dispositif Sandbox pour une inspection approfondie.

Conclusion

Les menaces avancées tirent profit du réseau interne plat. Dès qu'elles ont franchi les défenses périphériques, peu de choses peuvent arrêter leur propagation et l'extraction éventuelle de ressources ciblées précieuses. Comme les Firewalls traditionnels ont été conçus pour des débits plus lents en périphérie d'Internet, il est difficile de déployer ces systèmes de sécurité en interne. Enfin, le déploiement de la configuration réseau d'un Firewall (adresses IP) prend du temps.

Les Firewalls de Segmentation Interne représentent une nouvelle catégorie de Firewalls dont le déploiement est rapide et ne nécessite qu'une interruption minimale du réseau tout en conservant des débits de plusieurs gigabits au sein des réseaux internes. Il est ainsi possible de profiter d'une visibilité et d'une protection instantanée de parties spécifiques du réseau interne.

SIÈGE SOCIAL MONDIAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1 408 235 7700
www.fortinet.com/sales

SUCCURSALE EMEA
120, rue Albert Caquot
06560, Sophia Antipolis,
France
Tél. : +33 (0)4 89 87 05 10

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapour 199555
Tél. : +65 6513 3730

SUCCURSALE AMÉRIQUE LATINE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
Mexico D.F.
Tél. : 011 52 (55) 5524 8428

FRANCE
TOUR ATLANTIQUE
11ème étage, 1 place de la Pyramide
92911 Paris La Défense Cedex
France
Ventes: +33-1-8003-1655