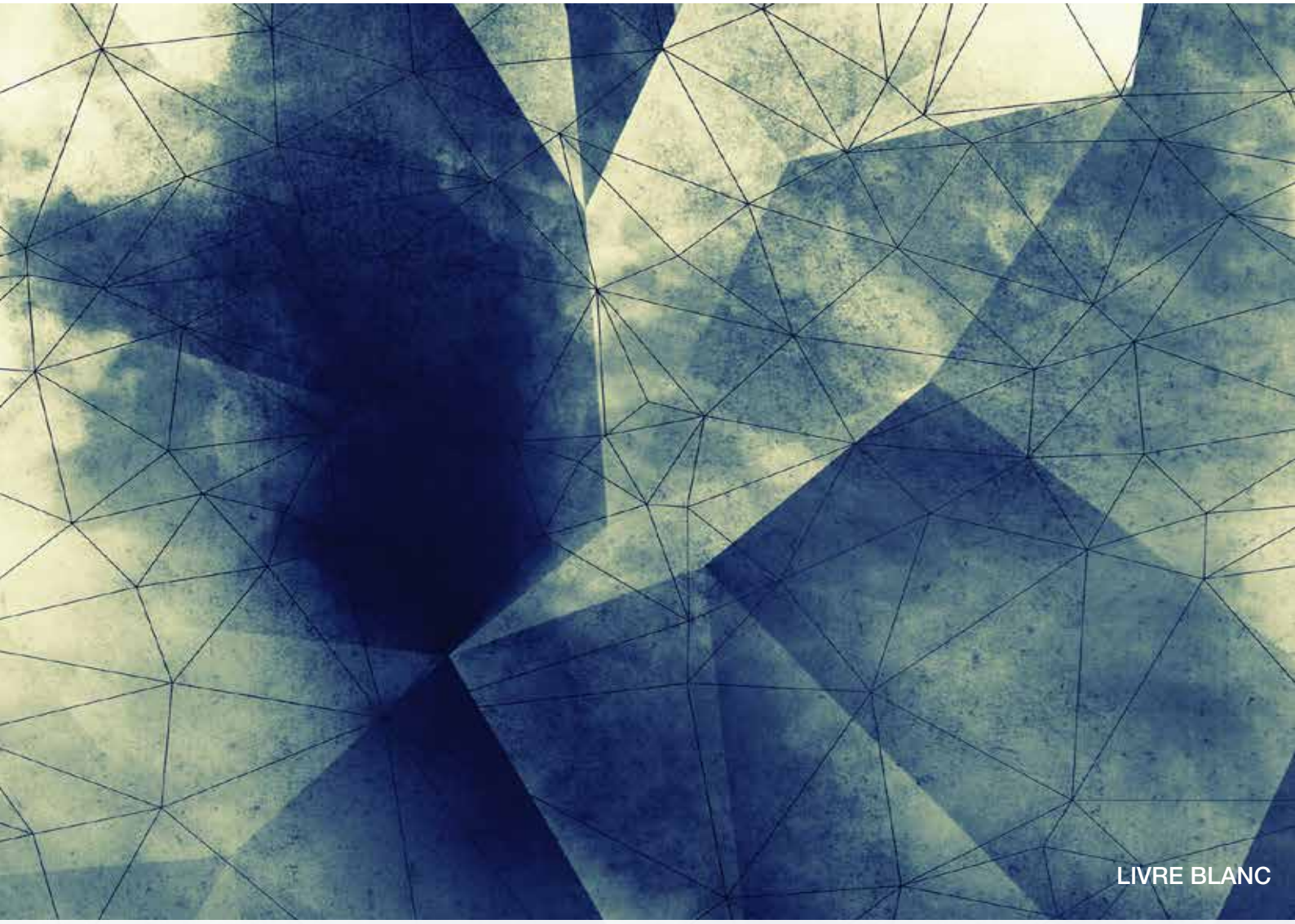


LIVRE BLANC

Une nouvelle approche de la sécurité réseau d'entreprise

FORTINET

NOXENT
Une entreprise du groupe Victrix

Table des matières

Synthèse

Beaucoup de choses ont été dites et écrites sur les défis auxquels les entreprises sont confrontées aujourd'hui en termes d'accroissement de l'activité des cybermenaces et de leur degré de sophistication. Comment une entreprise peut-elle se protéger contre ces brèches toujours plus régulières et médiatisées ? La technologie est-elle incapable de répondre à ces nouvelles menaces ?

Le problème réside peut-être davantage dans le peu d'attention prêté à la sécurité dans le cadre du déploiement des technologies informatiques que dans les technologies elles-mêmes. Si tel est le cas, il faut y voir un appel général à repenser la sécurité au sein des entreprises.

Il existe plusieurs façons de sécuriser un réseau. Les entreprises adoptent des approches diverses en fonction de leurs besoins et de leur budget. Pour les banques et le secteur de la vente au détail par exemple, le respect de réglementations telles que la norme PCI-DSS revêt un caractère essentiel. Toutefois, bien que la conformité vis-à-vis de la norme PCI-DSS soit de mise dans ces secteurs verticaux, la sécurité ne doit pas se limiter à ces exigences d'ordre général. D'autres entreprises vont plus loin en réalisant une évaluation des risques et en allouant les dépenses de sécurité en fonction des probabilités. Cette approche dépasse la simple conformité mais, étant donné la variabilité des risques de sécurité des entreprises, on peut douter de la pertinence de leur évaluation annuelle. Enfin, l'approche par produits ciblés consiste à déployer des produits clés provenant de différents fournisseurs, en partant du principe que chacun de ces produits est le meilleur de sa catégorie. Bien que cette approche ait été considérée comme la plus aboutie, la complexité et le coût qu'implique ce type de gestion ne peuvent être ignorés.

Ce document a pour but de présenter un nouveau concept de mise en œuvre de la sécurité réseau qui repose sur trois principes fondateurs :

- **GLOBALITÉ : UNE APPROCHE DE BOUT EN BOUT,** du datacenter aux terminaux et au-delà, capable de réagir aux menaces grâce à des capacités intégrées de prévention, de détection et de correction
- **COLLABORATION : LES COMPOSANTS DE LA SOLUTION TRAVAILLENT DE CONCERT,** et sont associés aux capacités du réseau à rassembler et à partager des données sur les menaces en temps réel
- **TRANSFORMATION : FAIRE ÉVOLUER** le réseau des entreprises d'un ensemble de boîtiers vers une plateforme combinant technologie et expertise humaine

L'érosion d'un périmètre du réseau clairement défini est un autre problème majeur pour les entreprises. Les modifications technologiques ainsi que la manière dont la technologie est utilisée au sein des entreprises ont créé une surface d'attaque illimitée, augmentant ainsi la probabilité d'une attaque réussie et de violations de données consécutives.

Fortinet croit qu'il est grand temps de changer les postures à l'égard de la sécurité réseau et, plus important encore, la manière dont celle-ci est mise en œuvre. À l'heure actuelle, le rôle d'un réseau au sein de la stratégie métier d'une entreprise revêt une importance plus essentielle que jamais. Dans un contexte de paysage de menaces en constante évolution, ne pas sécuriser cette ressource essentielle est un risque que la plupart des entreprises ne peuvent pas se permettre de courir.

Un besoin de changement

Pourquoi la sécurité réseau est-elle devenue si importante en si peu de temps ? Au cours des 20 dernières années, les entreprises ont réalisé d'importants changements dans leur façon de fonctionner ou créé des modèles économiques inédits, inconcevables avant l'avènement de la technologie. La technologie a révolutionné le fonctionnement des entreprises : l'information a remplacé le produit fini en tant que pièce maîtresse du puzzle, et la possibilité d'analyser ces données à volonté permet aux entreprises de développer leur activité. De simples centres de coûts, les datacenters et les sites Web sont devenus les pivots du commerce. Toutefois, pour un fonctionnement optimal, un réseau robuste et sécurisé est indispensable. Si les données client forment le sommet de la pyramide, comme illustré ci-dessous, le réseau sous-jacent sur lequel elles reposent constitue sa base (fig. 1). Et quand celle-ci présente des faiblesses, les données sont exposées à des risques.

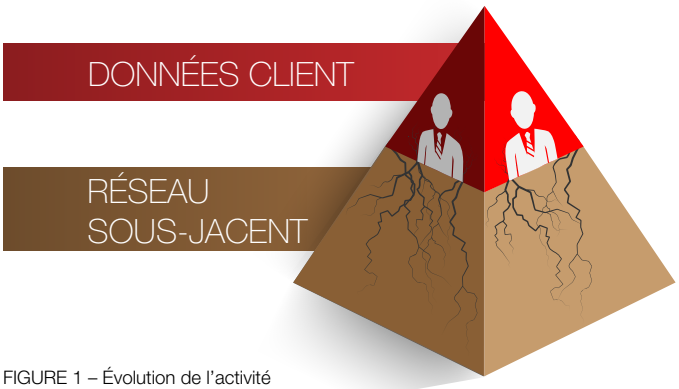


FIGURE 1 – Évolution de l'activité

L'expansion des entreprises étant la principale source d'élargissement des réseaux, il a tout d'abord fallu que le réseau soit en mesure de prendre en charge les activités. Bien que la sécurité ait toujours été plus ou moins présente, elle était souvent ajoutée après coup et constituée de quelques fonctionnalités de base greffées au réseau. Au fil du temps, ce modèle de sécurité s'est révélé inapproprié ; ensemble, les défaillances, les trop nombreuses vulnérabilités exploitables et la capacité de l'homme à créer des programmes malveillants performants ont submergé les entreprises.

Le fondement d'une approche globale et flexible de la sécurité

Aucune structure de sécurité réseau ne peut écarter tous les programmes malveillants du réseau en toutes circonstances. Les objectifs consistent donc à bloquer l'accès au réseau à autant de programmes malveillants que possible, à détecter toute intrusion au sein du réseau aussi rapidement que possible, et à garantir la protection des ressources clés en cas d'attaque. Comment y parvenir ?

Chez Fortinet, nous partons du principe que la sécurité doit être intégrée au tissu même de l'infrastructure réseau. En appliquant cette méthode, les vulnérabilités entre les deux couches sont automatiquement réduites, voire éliminées, et le créneau pour le pirate se referme peu à peu. Cependant, même étroitement intégrée à l'infrastructure réseau, l'introduction de technologies ne suffit pas à faire face au paysage de menaces d'aujourd'hui. Déployées au cœur du système, dans les succursales, sur les postes de travail, ces technologies doivent travailler de concert avec une base commune qui les rassemble en tant que solution unifiée.

Fortinet déploie les technologies adaptées aux emplacements appropriés à travers le réseau : Next Generation Firewall FortiGate, Web Application Firewall (WAF) FortiWeb, Secure Email Gateway (SEG) FortiMail, Sandbox réseau FortiSandbox et logiciel client EndPoint Protection (EPP) FortiClient (fig. 2). Toutes ces technologies s'appuient sur des données communes relatives aux menaces générées par l'équipe FortiGuard Labs de Fortinet : c'est ce qui distingue l'approche Fortinet des approches traditionnelles. Un ou plusieurs services de sécurité sont exécutés sur chacun de ces produits. Certains de ces services, comme la solution antispam dans SEG, sont essentiels au fonctionnement du produit, tandis que d'autres, comme les antivirus et les systèmes de prévention des intrusions dans FortiGate, sont conçus pour améliorer l'efficacité de la sécurité. Par rapport à une approche fragmentée traditionnelle de solution ciblée, chaque fournisseur possède ses propres données relatives aux menaces. Le problème est que l'efficacité de la sécurité de chaque produit est variable et que des vulnérabilités exploitables risquent de se développer. Puisqu'il existe plusieurs vecteurs d'attaque, les programmes malveillants susceptibles d'être bloqués par un

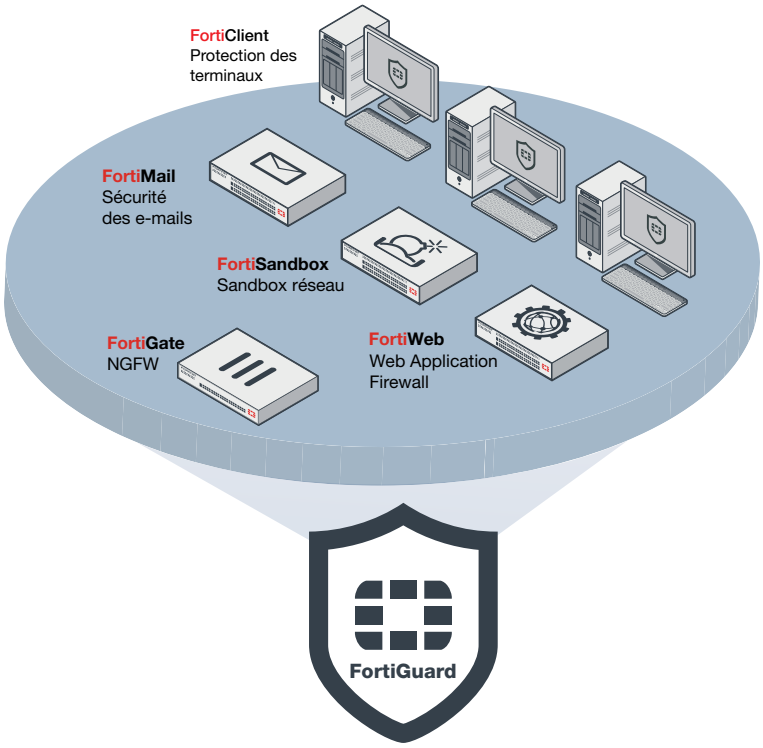


FIGURE 2 – Sécurité à travers le réseau

firewall peuvent réussir à accéder au réseau par le biais d'un site Web compromis, d'une pièce jointe, ou d'une URL dans un courriel de phishing. Les différents services de sécurité inclus dans l'approche Fortinet sont mis à jour et synchronisés par l'équipe FortiGuard Labs, qui empêche le développement de vulnérabilités entre les produits. Figure centrale de l'écosystème Fortinet, l'équipe FortiGuard Labs reçoit des données relatives aux menaces en temps réel provenant de millions de capteurs et d'autres sources à travers le monde. Ces informations sont optimisées par la recherche avancée sur les menaces et la détection de vulnérabilités zero-day, également conduites par l'équipe de cyberexperts FortiGuard Labs, qui met constamment à jour les différents services exécutés dans les appliances Fortinet. Ces mises à jour proviennent d'une seule et unique source et permettent d'éliminer les vulnérabilités entre les différentes appliances.

Afin d'éliminer toute vulnérabilité éventuelle, ces produits ont été conçus pour travailler de concert, comme une seule et même solution, permettant de prévenir ou de détecter l'intrusion de programmes malveillants dans le réseau, offrant des fonctions de neutralisation clés pour minimiser les dommages à l'issue d'une attaque et garantissant la mise à jour de la solution pour optimiser la protection lors des attaques suivantes.

Grâce à la technologie Sandbox, la sécurité offerte par Fortinet est encore plus étroitement intégrée. Ici, il faut absolument prendre en compte la façon dont le Sandbox interagit avec les autres éléments de sécurité du réseau. Son approche agressive consiste à chercher en permanence des échantillons de programmes malveillants, en intégrant tous les éléments rencontrés dans son processus. Inconvénient de cette approche : le temps. Parfois, des heures s'écoulent entre le moment de l'intrusion et le moment où le Sandbox détecte le programme malveillant, heures que le programme malveillant pourrait mettre à profit pour se répandre dans le réseau. L'approche de Fortinet consiste en une intégration étroite entre le Sandbox et les autres technologies du réseau. Les technologies qui forment la couche de prévention agissent comme un préfiltre, empêchant une grande partie des programmes malveillants de pénétrer le réseau. Les échantillons suspects sont ensuite transférés au Sandbox pour analyse. Si un échantillon se révèle malveillant, le Sandbox peut communiquer avec les autres éléments de la solution afin de prendre des mesures spécifiques et de lancer les premières étapes de la neutralisation.

Utilisant diverses technologies conçues pour travailler de façon collaborative et alimentées par des données relatives aux menaces en temps réel, la solution Fortinet permet au réseau de se défendre en profondeur contre les attaques, profondeur qu'une approche traditionnelle uniquement basée sur la prévention ne peut offrir.

FIGURE 3 – Risque croissant lié aux menaces

Opérer la sécurité réseau en profondeur

Dans l'imaginaire collectif façonné par Hollywood, les attaques réseau ont systématiquement lieu dans un datacenter rempli d'ordinateurs. En réalité, ces attaques peuvent se produire n'importe où dans le réseau. Le réseau doit être perçu comme une série de cercles concentriques ; le cœur du réseau se trouve au centre de ces cercles (fig. 3). Pour des raisons économiques, c'est généralement à cet endroit que la sécurité est focalisée. Le nombre de points d'attaques potentielles augmente de façon exponentielle avec l'expansion des cercles, du cœur vers les succursales, les postes de travail individuels et au-delà. Ainsi, plus on est éloigné du cœur du réseau, plus la probabilité d'une intrusion non détectée sur le réseau augmente.

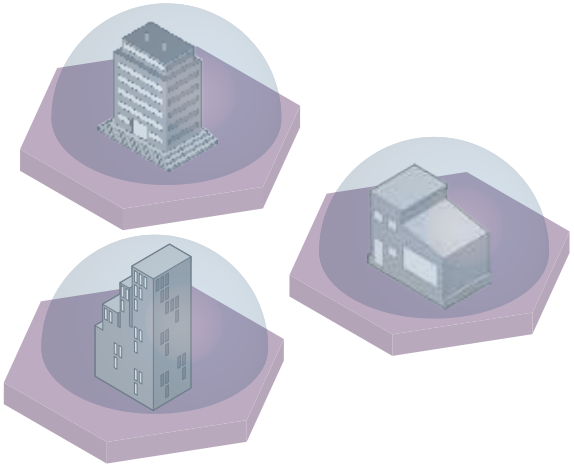


FIGURE 4 – Un réseau segmenté mais non sécurisé

Cette stratégie est réduite à néant lorsque des produits de différents fournisseurs sont mêlés les uns aux autres avec, par exemple, un fournisseur pour le datacenter, un autre pour le campus et un troisième pour les sites distants. Chaque produit individuel peut permettre d'obtenir les résultats escomptés, mais il reste isolé, ce qui complique et rallonge considérablement la gestion des stratégies de sécurité sur l'ensemble du réseau.

FortiOS, le système d'exploitation commun à chaque FortiGate, permet à Fortinet de résoudre de tels problèmes. Quel que soit l'emplacement où elle est déployée sur le réseau, la fonctionnalité commune de FortiOS distribuée à travers le réseau offre aux entreprises un environnement gagnant-gagnant : un réseau plus sécurisé grâce à la segmentation interne et des stratégies de sécurité cohérentes sur la totalité du réseau. FortiOS est également le moteur des différents services de sécurité pris en charge par FortiGate et garantit que l'ensemble du réseau est protégé équitablement (fig. 5).

Cependant, cette segmentation continue de concentrer ses efforts sur le périmètre du réseau et ne réagit pas lorsqu'un pirate parvient à pénétrer le réseau sans être détecté, particulièrement s'il a utilisé des identifiants de connexion valides mais compromis. La technologie Sandbox peut résoudre ce problème, mais il est impossible d'arrêter les mouvements d'un pirate tant que celui-ci n'a pas implanté le programme malveillant dans le réseau. Impossible ?

Fortinet pense que le temps est venu d'étendre le concept de la segmentation à l'intérieur du réseau. Les réseaux ont depuis longtemps mis en œuvre le concept de segmentation aux fins de mise en réseau et non pour empêcher les programmes malveillants ou les pirates informatiques de se déplacer librement dans le réseau. La solution Internal Segmentation Firewall (ISFW) résout ce problème.

La solution ISFW utilise un firewall d'entreprise performant déployé dans le réseau au plus près des utilisateurs et des applications, tant dans le campus d'entreprise qu'au sein du datacenter. Cette proximité optimise les possibilités de réduction des risques de déplacements latéraux. Autre facteur clé : l'adéquation entre les stratégies de sécurité pour l'identification des utilisateurs. Rattacher la stratégie de sécurité à l'identité de l'utilisateur faciliterait la création d'une stratégie bloquant aux utilisateurs l'accès aux régions du réseau dont ils

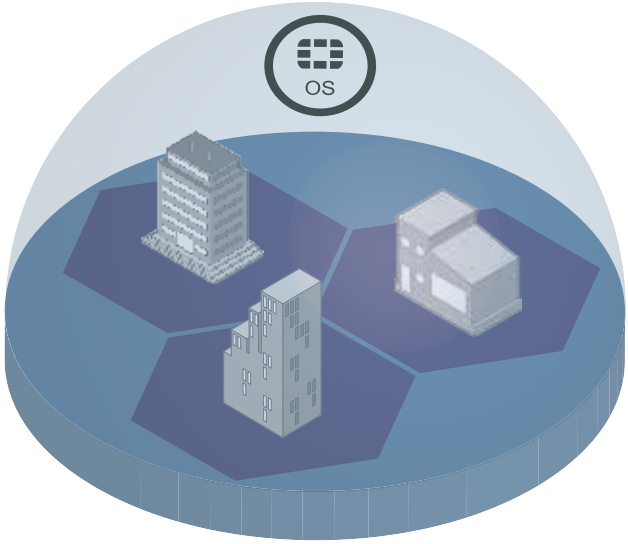


FIGURE 5 – Protection par FortiOS

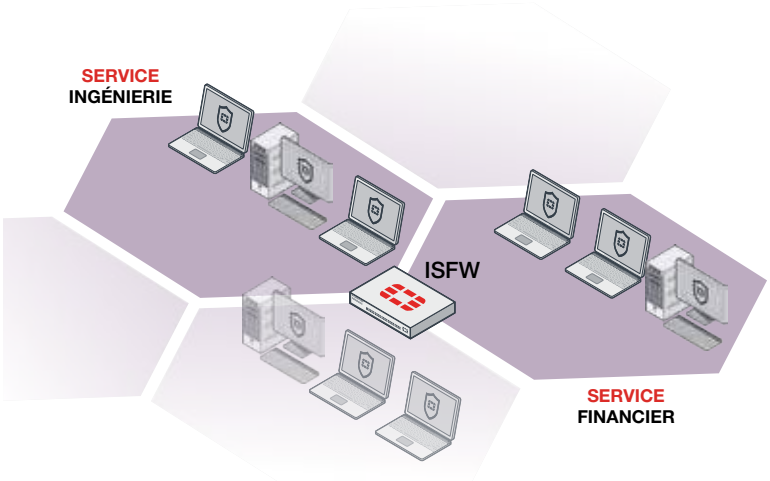


FIGURE 6 – La solution : ISFW

n'ont pas besoin pour leur travail habituel. Prenons l'exemple d'un utilisateur du VLAN Finance qui tente d'accéder au VLAN Développement d'ingénierie. Si un ISFW est en place, un pirate essayant de se déplacer depuis le point initial d'intrusion (dans ce cas précis, le service Finance) vers le VLAN Développement d'ingénierie serait bloqué par le firewall et des alarmes se déclencheraient pour indiquer ce qui s'est passé (fig. 6).

La solution ISFW a donné lieu à une évolution dépassant la sécurité multifonction : la sécurité multicouche, qui requiert des appliances de sécurité très performantes. Grâce à sa technologie FortiASIC qui assure une sécurité en profondeur pour les réseaux internes fonctionnant à des vitesses de 10, 40 et 100 gigabits, Fortinet possède un avantage considérable et différencié. L'approche ISFW de Fortinet offre une visibilité et une protection continues du réseau de l'intérieur, minimisant ainsi l'exposition aux menaces et les dommages éventuels.

La sécurité sans fil et sans filet

La technologie sans fil est passée de fonctionnalité pratique à incontournable dans les entreprises d'aujourd'hui, autant pour son utilisation interne que pour l'amélioration de l'expérience client. Elle pose toutefois le défi suivant : proposer un environnement d'accès unifié sans compromettre la sécurité. Le réseau sans fil traditionnel des succursales consiste en une superposition, c'est-à-dire que le réseau sans fil est indépendant de l'infrastructure réseau sous-jacente. Bien que le réseau sans fil propose une sécurité sous forme de contrôle d'accès, par exemple avec la méthode Wi-Fi Protected Access (WPA et WPA2), elle est différente de la sécurité réseau. Ici, une infrastructure de sécurité commune à tous les utilisateurs est requise, quelle que soit la méthode d'accès.

Dans la solution Secure Access Architecture de Fortinet, le réseau sans fil est une extension de FortiGate. Outre le contrôle d'accès et les fonctionnalités de sécurité typiques des réseaux sans fil (WPA), tous les utilisateurs du réseau sont soumis aux mêmes mesures d'authentification et stratégies. L'authentification peut être effectuée localement par FortiGate ou via des systèmes externes comme RADIUS ou Active Directory. L'authentification à 2 facteurs peut également être mise en œuvre afin de minimiser les risques liés aux identifiants de connexion valides, mais compromis. Une fois identifiés et authentifiés, les utilisateurs peuvent seulement accéder aux ressources du réseau définies dans leur stratégie. Puisque leur accès réseau s'opère depuis FortiGate, le risque d'accès de programmes malveillants est considérablement réduit.

Sécurité et contrôle de bout en bout

Parallèlement à différents éléments interdépendants de la solution mise en œuvre, un autre élément clé de l'adoption d'une approche proactive en matière de sécurité est la centralisation de la gestion et de l'analyse de la sécurité. Pour y voir clair dans cette activité débordante du réseau, des outils complets sont requis pour configurer correctement les différents éléments de la solution. Fortinet inclut FortiManager, une approche de la gestion réseau à partir d'une interface unique, afin de faciliter la configuration des produits individuels, la définition des configurations basées sur les stratégies, la gestion des mises à jour et la surveillance du réseau de bout en bout. L'interface utilisateur graphique de FortiManager est conçue de façon à ce que l'utilisateur parvienne en quelques clics au niveau de détail requis pour prendre connaissance des alarmes et autres événements qui surviennent dans le réseau. Une fois le réseau installé et configuré, l'objectif suivant est de comprendre ce qui se passe dans le réseau en transformant ces alarmes et événements en une vision claire du réseau. FortiManager s'intègre de manière transparente avec FortiAnalyzer pour détecter en profondeur, analyser, hiérarchiser et signaler les événements liés à la sécurité réseau.

Opérer la transformation de l'entreprise : le facteur humain

La mise en œuvre et le maintien de la sécurité réseau ne constituent pas une tâche ponctuelle et limitée. Les entreprises doivent constamment tester leurs solutions de sécurité et tirer parti des services professionnels mis à disposition par leurs partenaires technologiques. Les entreprises ne disposent pas toutes en interne de l'ensemble nécessaire de connaissances et de compétences sur toutes les technologies de sécurité pour garantir la bonne configuration et le bon déploiement de celles-ci. Le test et l'évaluation des vulnérabilités, la révision des configurations et la formation sont à envisager afin de garantir le bon déploiement des technologies au sein du réseau et ne constituent pas des moyens détournés d'y parvenir. L'entreprise peut également tirer profit des services de réponse aux incidents, en mettant les connaissances et compétences des fournisseurs de technologies au service de leur personnel en interne. Fortinet travaille en étroite collaboration avec ses clients afin de fournir ces services et de préparer les services de demain pour répondre à un marché en constante évolution. Fortinet propose également une offre de services d'assistance premium dans plusieurs domaines spécifiques pour améliorer la valeur reçue par les entreprises : amélioration et collaboration proactives et continues. Ces services incluent notamment le responsable technique de compte dédié, des accords de niveaux de service améliorés, et la prédéfinition des mises à niveau et des ateliers, afin que la solution Fortinet réponde aux besoins des entreprises tout au long de leur cycle de vie.

La sécurité sans compromis

Au vu des relations entre les entreprises d'aujourd'hui et les technologies qui les pilotent, il est fondamental d'accorder la priorité à la sécurité de l'infrastructure informatique. Trop d'entreprises considèrent encore la sécurité comme une dépense contestable plutôt que comme un investissement stratégique. Attendre l'apparition d'une brèche de données sans avoir évalué sa posture actuelle en matière de sécurité revient à fermer sa maison à clé une fois qu'un cambriolage y a été perpétré.

Fortinet poursuit deux objectifs clés : être à l'avant-garde du travail de changement des mentalités à l'égard de la sécurité des entreprises, et gagner la confiance de ses partenaires afin de les guider dans ces transformations.

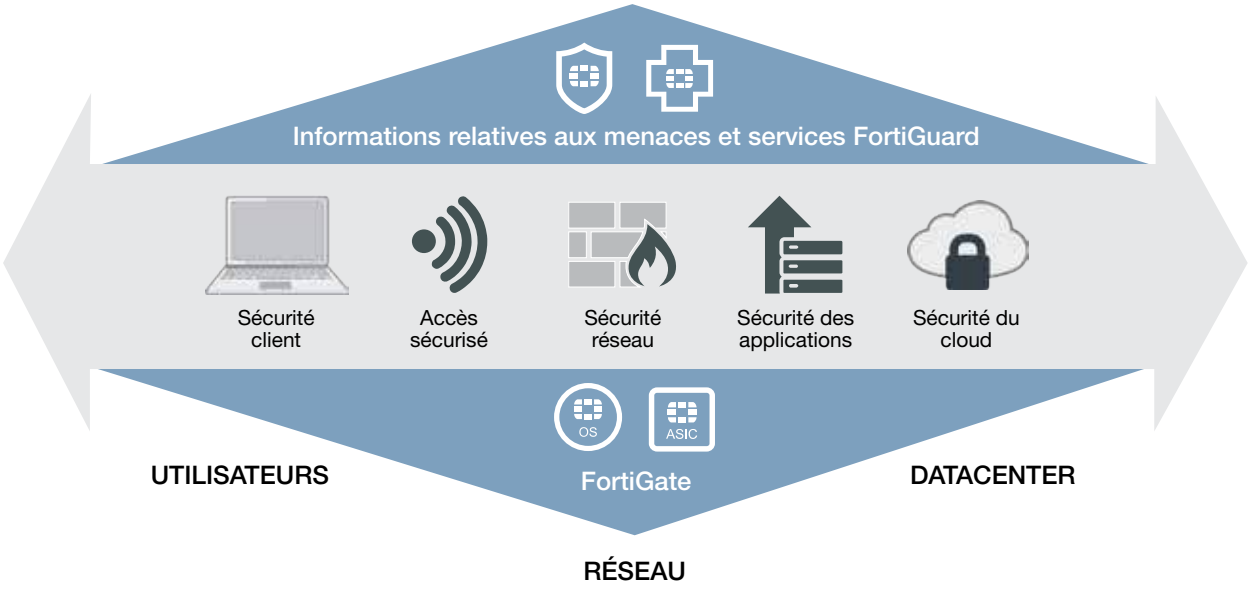
> Le réseau est une entité unique qui doit être considérée selon un point de vue global. Les technologies adaptées doivent être introduites aux emplacements appropriés pour améliorer la capacité du réseau à détecter les attaques et à se défendre tout au long du cycle de vie des menaces.

Afin d'augmenter les capacités de détection des menaces, la technologie doit être alimentée par des données continues et pertinentes sur les menaces, données qu'elle pourra exploiter pour prendre des mesures spécifiques et ainsi améliorer l'efficacité de sa sécurité.

Grâce à l'étendue et à la profondeur de sa gamme de produits – des produits adaptés à chaque région fonctionnelle du réseau et conçus pour fonctionner ensemble –, Fortinet est en mesure d'appliquer cette nouvelle conception de la sécurité réseau. La réponse ne consiste pas en une simple action locale ; la solution Fortinet est en effet conçue pour fonctionner de façon collaborative et pour prendre des mesures automatisées et performantes. Chaque mesure prise nourrit l'écosystème des données relatives aux menaces afin de renforcer la solution globale, de manière automatique et cohérente.

Enfin, l'intelligence et l'intervention humaines viennent compléter le tableau, assistant à la fois la technologie et les ressources humaines employées dans les entreprises. En fusionnant leur expertise humaine, Fortinet et les entreprises travaillent de pair pour supprimer les maillons faibles et améliorer les capacités générales de défense de ces dernières.

Les menaces auxquelles les entreprises font face gagnent chaque jour en ampleur et en complexité. Les entreprises doivent donc modifier la façon dont elles pensent la sécurité réseau. Fortinet se propose de les aider à évoluer en passant d'une approche réactive de la sécurité réseau à une approche adaptative, globale et collaborative qui rassemble le meilleur de la technologie et des capacités humaines.



TRANSPARENCE
Posture cohérente, de bout en bout et transparente vis-à-vis des menaces

INTELLIGENCE
Protection intelligente de l'intérieur, avec une visibilité totale de la surface d'attaque

PUISSANCE
Puissance et performance pour aujourd'hui et pour demain

www.noxent.com/fortinet

SIÈGE SOCIAL NOXENT
6400, boul. Taschereau, bureau 220
Brossard, Québec
J4W 3J2
Tél. : 450 926-0662

1670, rue Semple, bureau 240
Québec (Québec)
G1N 4B8
Tél. : 418 871-7022

www.fortinet.com

Fortinet Technologies (Canada) ULC.
4190, Still Creek Drive, Suite 400
Burnaby (BC)
V5C 6C6
Tél. : 604 430-1297

Canada Ottawa
1826 Robertson Road
Ottawa (ON)
K2H 5Z6

Canada Sales
1 866 868-3678
option 1, puis option 5