FICHE SOLUTION

Pare-feu de nouvelle génération FortiGate : une visibilité granulaire sur les applications, les utilisateurs et les dispositifs

Synthèse

Les pare-feu traditionnels se contentent généralement d'autoriser ou de bloquer les connexions en fonction du port et du protocole utilisé. Cependant, l'accès réseau est désormais devenu dynamique et contextuel, fonctionnant selon les principes du Zero Trust. L'entreprise moderne est devenue hybride et son périmètre couvre les data centers sur site, les clouds publics, le campus d'entreprise et les sites distants. Les équipes informatiques ont besoin d'une visibilité détaillée sur les applications, les utilisateurs et les dispositifs pour renforcer la défense des réseaux d'entreprise contre les cybermenaces sur l'ensemble de l'environnement d'entreprise. Un vrai défi !

Plus de 95 % du trafic internet est désormais chiffré.[1]

Désormais, c'est la quasi-totalité du trafic Internet qui est chiffré, ce qui accentue la problématique de visibilité. Les entreprises se retrouvent avec des segments importants de leur réseau sur lesquels ils n'ont aucune visibilité, lorsqu'elles migrent leurs architectures en étoile onéreuses vers un modèle multisite qui permet aux sites distants d'accéder directement à Internet. Les acteurs malveillants peuvent tirer parti des zones d'ombre sur le réseau pour dissimuler leurs menaces dans le trafic chiffré.

Le pare-feu de nouvelle génération (NGFW) FortiGate offre une visibilité sur le trafic chiffré, ainsi que sur l'activité des utilisateurs, des applications et des dispositifs. Il devient possible d'élaborer des politiques réseau et de sécurité contextuelles et évolutives pour sécuriser la transformation numérique des entreprises. Le NGFW FortiGate peut identifier tous les utilisateurs, applications et dispositifs sur le réseau via des techniques sophistiquées de collecte et d'analyse des données. En tant que composant clé d'une solution de type *Hybrid Mesh Firewall* (HMF), le NGFW FortiGate déploie cette visibilité et cette protection sur tous les domaines informatiques, couvrant ainsi l'ensemble de l'infrastructure réseau.

Contrôle applicatif

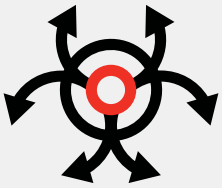
Le service de contrôle applicatif FortiGuard vient en complément des NGFW FortiGate pour identifier rapidement le trafic applicatif connu et inconnu qui transite sur le réseau. Il permet de créer facilement des politiques pour autoriser, refuser ou restreindre l'accès aux applications, à certaines fonctions de ces applications et à des catégories d'applications.

#	Risque	Application	Catégorie	Technologies	Utilisateurs	Bande passante	Session
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
4	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
5	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
6	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
7	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
8	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
9	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
10	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38

Les NGFW FortiGate peuvent identifier les applications en fonction du port et du protocole utilisés, de la signature applicative, du comportement et d'autres critères d'identification. En associant des signatures applicatives aux applications répertoriées dans la base de données des services Internet (ISDB) de FortiGuard Labs, FortiGate peut définir plus de 4 200 règles de contrôle applicatif. Vous trouverez ci-dessous des exemples montrant comment FortiGate identifie les applications au-delà des couches 3 et 4.

Signatures applicatives : une signature est attribuée au trafic réseau autorisé en fonction des caractéristiques de la transaction et du fait que le port de l'application est celui par défaut ou non. Le trafic est analysé pour détecter les menaces et assurer une inspection approfondie.

Chiffrement : si FortiGate détecte un chiffrement tel que SSL (secure sockets layer)/TLS (transport layer security), HTTPS (Hypertext Transfer Protocol Secure), ou SSH (secure shell), et qu'une règle de déchiffrement est en place, la session est déchiffrée et les signatures applicatives sont appliquées sur le flux déchiffré.



"Les entreprises qui ont inspecté le trafic entrant estiment que 70 % des logiciels malveillants ont été acheminés via un lien chiffré "[2]

Décodeurs : si le protocole applicatif est connu, il est utilisé pour appliquer des signatures contextuelles supplémentaires afin de détecter d'autres applications susceptibles d'emprunter des tunnels du protocole. Les décodeurs valident que le trafic est conforme aux spécifications du protocole. Ils assurent la translation d'adresse NAT et l'activation de fonctions pour des applications SIP ou FTP.

Analyse comportementale : ce type d'analyse réalisé par FortiGate utilise un traitement analytique des données comportementales pour déterminer l'identité d'applications inconnues, notamment les applications utilisant le port 80, le port 443 ou qui effectuent des sauts de port. Par exemple, les applications de voix sur IP (VoIP), de collaboration et de peer-to-peer (P2P) qui ne peuvent pas être identifiées par une analyse de protocole ou basée sur des signatures.

Si FortiGate n'est pas en mesure d'identifier une application compte tenu de sa signature, il s'intéressera à des caractéristiques comportementales pour catégoriser cette application inconnue dans un groupe applicatif existant, avec mise en œuvre de filtres dynamiques ou de règles de forwarding.

L'identification d'applications fournit des éléments de contexte sur le réseau. FortiGate peut révéler des informations sur les fonctions, les ports applicatifs, les protocoles, la technologie et les caractéristiques comportementales de l'application, ce qui permet aux équipes informatiques d'élaborer des politiques d'accès de confiance et fiables. Une fois que l'équipe comprend comment une application est utilisée sur le réseau, différentes politiques peuvent être définies, pour autoriser/bloquer le trafic et au-delà.

FortiGuard Application Control permet également aux entreprises de définir des politiques et des fonctions de contrôle au sein de chaque application, par exemple :

- Autoriser l'accès à Facebook mais bloquer les transferts de fichiers via Facebook Messenger
- Permettre aux utilisateurs d'accéder à Gmail mais désactiver Google Chat
- Neutraliser le téléversement de fichiers vers Dropbox, Box ou Google Drive
- Filtrer les catégories de vidéos indésirables pour éviter qu'elles ne soient visionnées sur YouTube

FortiOS, le système d'exploitation de FortiGate, offre une visibilité étendue sur l'utilisation des applications en temps réel, ainsi que sur les tendances au fil du temps, au travers de perspectives, graphiques et rapports. Le contrôle applicatif empêche les applications malveillantes, à risque et indésirables de pénétrer sur le réseau grâce à des points de contrôle situés au niveau du périmètre, dans le data center et entre les segments du réseau.

Identification des utilisateurs

L'identification des utilisateurs, au-delà des adresses IP, est une autre fonction essentielle de la sécurité d'entreprise. FortiOS peut identifier les utilisateurs à l'aide de différentes sources et méthodes : Microsoft Active Directory (AD), serveurs LDAP, syslog, mapping de ports et entêtes XFF.

L'identification des utilisateurs par FortiGate améliore la visibilité sur l'activité du réseau et la détection des comportements malveillants ou nuisibles. L'identification des utilisateurs FortiGate identifie les utilisateurs, quel que soit le système d'exploitation qu'ils utilisent ou leur localisation, offrant une meilleure visibilité de l'utilisation des applications en fonction des utilisateurs. Les équipes informatiques disposent ainsi d'une image plus pertinente de l'activité sur le réseau.

L'identification des utilisateurs est essentielle dès qu'une application inconnue est détectée sur le réseau. Que ce soit à l'aide de FortiView ou des logs de contrôle applicatif, les équipes de sécurité peuvent identifier :

- L'application
- L'utilisateur
- La consommation de bande passante et la session
- La source et la destination du trafic applicatif
- Toute menace associée

Mapping des utilisateurs

FortiGate peut créer des profils d'utilisateurs du réseau et assurer un mapping entre les noms d'utilisateurs et les adresses IP associées aux paquets reçus. Les informations sur les utilisateurs peuvent être mises en correspondance avec les politiques de sécurité pour une utilisation plus sécurisée du réseau, en restreignant l'accès aux applications uniquement à ceux qui en ont besoin. Ce mapping des utilisateurs peut activer un ensemble de règles ou de politiques pour les applications moins risquées comme SalesForce ou PowerPoint. Cependant, des politiques plus strictes peuvent être définies pour des applications sensibles comme les outils de test de pénétration ou les outils de contrôle distant d'ordinateurs.

Mapping de groupes

La définition de règles pour des groupes d'utilisateurs simplifie les tâches d'administration. En effet, les politiques et règles sont déjà en vigueur et n'ont pas besoin d'être reconfigurées lorsqu'un utilisateur est rajouté à un groupe. FortiGate peut appliquer ces règles et actualiser les groupes, en faisant appel à différents types d'annuaire : Microsoft AD, Novell eDirectory et Sun ONE Directory Server notamment. Après activation de l'identification des utilisateurs et en assurant un mapping des groupes, les politiques de sécurité peuvent être configurées pour des utilisateurs et groupes spécifiques. Ceci porte sur les catégories et les sous-catégories d'applications, les technologies sous-jacentes et les caractéristiques des applications. Les règles des politiques peuvent être définies pour activer en toute sécurité les applications, sur la base des utilisateurs et groupes d'utilisateurs, pour les flux entrants ou sortants.

Voici quelques exemples de politiques basées sur les utilisateurs ou groupes d'utilisateurs :

- Les outils tels que SSH, Telnet et FTP sur les ports standards sont réservés aux services informatiques des entreprises
- Les règles comme :
  - Permettre aux commerciaux d'accéder à SalesForce et à Microsoft 365
  - Autoriser tous les utilisateurs à consulter YouTube, mais bloquer certaines catégories de vidéos

L'identification des utilisateurs permet d'élaborer des politiques qui accompagnent et protègent les collaborateurs, les invités et utilisateurs. FortiGate peut fournir des informations approfondies sur les utilisateurs et automatiser le contrôle des politiques.

Identification des dispositifs

L'identification des utilisateurs permet de définir une politique basée sur l'utilisateur. De son côté, l'identification des applications assure une politique pour chaque application.Enfin, l'identification des dispositifs favorise des règles et une politique applicables aux dispositifs, quels que soient leur adresse IP ou leur localisation. En assurant la traçabilité des dispositifs et en associant les événements du réseau à des dispositifs spécifiques, l'identification des dispositifs fournit des éléments de contexte sur la façon dont les événements sont liés aux appareils. Les politiques sont associées aux dispositifs plutôt qu'aux utilisateurs, à leur localisation ou aux adresses IP, des attributs qui peuvent changer au fil du temps. L'identification des dispositifs est une fonction essentielle pour la sécurité, le déchiffrement, la qualité de service (QoS) et les politiques d'authentification.

Avec FortiGate, les politiques avancées et la priorisation des dispositifs peuvent être catégorisées selon les critères suivants :

- Classe, comme les dispositifs réseau sécurisés
- Dispositifs critiques, tels que les serveurs et les dispositifs médicaux
- Dispositifs d'environnement, tels que lecteurs de badges, caméras et alarmes incendie
- Les dispositifs de l'Internet des objets (IoT), comme les montres intelligentes et autres objets "intelligents" connectés

Déchiffrement SSL/TLS 1.3

Les logiciels malveillants se dissimulent régulièrement dans le trafic chiffré, et ce dernier doit donc être inspecté. Les NGFW FortiGate assurent le déchiffrement des flux SSL/TLS 1.3 sans ralentir le réseau. Ces pare-feu peuvent aussi déchiffrer des types de trafic spécifiques, avec une gestion des exceptions en fonction des sites ou des catégories. Grâce aux processeurs de sécurité propriétaires et haute performance de Fortinet, nul besoin d'arbitrer entre sécurité et performances.

Gestion centralisée et unifiée

Une administration et une gestion unifiées sont essentielles à la mise en œuvre d'un *Hybrid Mesh Firewall*. Les différents domaines, tels que les sites d'entreprise, les clouds publics et privés et les télétravailleurs à distance, doivent être protégés à partir de tableaux de bord distincts, ce qui induit davantage de complexité informatique et pèse sur la visibilité.

La gestion centralisée coordonne et unifie différents domaines de sécurité en une seule solution de sécurité IT d'entreprise, pour une protection simple, unifiée et automatisée qui s'étend des sites de l'entreprise au cloud et aux travailleurs distants. Et comme les entreprises présentent des exigences différentes en matière de gestion de leurs pare-feu réseau disséminés, la gestion centralisée doit prendre en charge tous les formats de pare-feu : appliances physiques, VM, SaaS et services de pare-feu gérés.

La gestion centralisée apporte également une valeur ajoutée considérable en réunissant les équipes des centres d'opérations réseau (NOC) et des centres d'opérations de sécurité (SOC) dans un seul et même endroit, pour ainsi gérer, surveiller et sécuriser l'ensemble de la surface d'attaque.

Services de sécurité FortiGuard optimisés par IA

Avec plus de 8 millions de capteurs déployés dans le monde entier, les NGFW FortiGate bénéficient d'une veille actualisée sur les menaces mondiales, fournie par les services de sécurité FortiGuard optimisés par IA. Avec des mises à jour de sécurité complètes et en temps réel, FortiGate protège l'ensemble du réseau à l'aide de différentes couches de sécurité : filtrage d'URL et de DNS, anti-malware, sandboxing en ligne, ainsi que fonctions IPS accélérées par matériel et capables d'assurer un virtual patching performant. Ces services de cybersécurité protègent les entreprises contre les attaques connues et inconnues. Les tests indépendants de CyberRatings.org[3] montrent que les NGFW FortiGate sont efficaces à 99,88 % contre les exploits malveillants et les tentatives de contournement.

Conclusion

L'identification des applications, des utilisateurs et des dispositifs sur le réseau est essentielle à la gestion et à la sécurisation des réseaux d'entreprise. Les NGFW FortiGate ont fait leurs preuves en matière de visibilité et de contrôle sur le trafic réseau, ainsi que de performances de premier rang. FortiGate définit et automatise des politiques qui garantissent une utilisation appropriée du réseau, déjouent les menaces et réduisent la surface d'attaque des entreprises. La gestion centralisée et unifiée porte sur différents formats de FortiGate : appliance physique, pare-feu virtuels, pare-feu cloud et Firewall-as-a-Service, pour bâtir un écosystème HMF transparent sur l'ensemble de l'environnement IT. Les nouveaux services de sécurité FortiGuard optimisés par IA garantissent une ligne de défense à jour contre les attaques les plus récentes et les plus sophistiquées.

[1] "HTTPS encryption on the web," Google Transparency Report, consulté le 15 mai 2023.

[2] Maria Korolov, "Network Encryption: A Double-edged Sword for Cybersecurity," Datacenter Knowledge, 8 mars 2023.

[3] "Fortinet FortiGate 600F,"pare-feu d'entreprise, CyberRatings.org, Q2 2023.

juin 20, 2023 1:40 PM
1711466-A-0-FR