LIVRE BLANC

Sécuriser l'écosystème IoT avec Fortinet

L'impact potentiel d'une cyberattaque réussie sur l'écosystème des objets connectés peut aboutir à la mise à l'arrêt de systèmes critiques, voire mettre en danger la vie de personnes physiques ou l'environnement. Pour les fournisseurs de solutions IoT, la sécurité devient un impératif.

Les fournisseurs de service managés (MSP), les fournisseurs de services de sécurité managés (MSSP) et les opérateurs de réseaux mobiles (MNO) doivent intégrer la sécurité dans le cadre de leurs solutions IoT pour tenir trois objectifs :

1. Sécuriser la totalité de l'écosystème IoT et assurer la continuité de service
2. Offrir des accords de niveau de services (SLA) pour l'IoT pour encourager son adoption
3. Fournir des offres commerciales de services de sécurité IoT

Solution de sécurité IoT de Fortinet

La solution de sécurité IoT de Fortinet consiste en des modules de sécurité qui, lorsque associés à de bonnes pratiques, protègent intégralement les écosystèmes IoT. Le terme d'IoT étant suffisamment large, toute solution doit bénéficier d'un panel de fonctionnalités intégrées et automatisées, capable de s'appliquer lorsque nécessaire à chaque cas d'utilisation.

Les fonctions de sécurité IoT de Fortinet sont fournies par un large panel de produits de sécurité réseau, interconnectés entre eux et intégrés à la Security Fabric de Fortinet, pour définir une plateforme puissante pour la sécurité de l'écosystème IoT.

Les fonctions de sécurité de Fortinet pour l'IoT sont proposées par le pare-feu nouvelle génération FortiGate et le pare-feu applicatif FortiWeb, des solutions proposées sous un format physique ou virtuel.

Segmentation FortiGate et pare-feu stateful

Dans de nombreux cas, le comportement du trafic d'un dispositif IoT est prévisible et un pare-feu stateful peut neutraliser tout trafic vers des destinations non-autorisées, ou émettre une alerte lorsqu'un objet connecté affiche une anomalie de comportement. Au sein d'un environnement IT classique, le trafic vers des destinations non-autorisées n'est pas rare et ces communications ne sont généralement pas acheminées. Mais dans le cas de l'IoT et des réseaux de type machine-to-machine, ces communications sont généralement le signe d'erreurs de configuration ou d'actes malveillants. Pour cette raison, des règles spécifiques doivent être paramétrées, donnant lieu à une action pertinente qui assure que toute alerte générée est prise en charge automatiquement.

Prévention d'intrusion par FortiGate

Le service de prévention d'intrusion de FortiGate est conçu pour détecter et neutraliser différents types d'attaques IoT, parmi lesquelles :

- **Les exploits :** ces attaques sur une vulnérabilité aboutissent généralement à un déni de service (DoS), en provoquant des crashs systèmes ou en alourdissant les charges de travail au sein d'un logiciel. Il peut s'agir également d'un code logiciel exécuté en local pour télécharger un exécutable malveillant.
- **Attaque par scan :** cette approche consiste à identifier des ports TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol), ainsi que des logiciels ou versions de protocole connus. De manière générale, l'objectif d'une reconnaissance est d'identifier les cibles vulnérables de valeur.
- **Attaques de fuzzing :** cette autre méthode d'identification des vulnérabilités s'effectue généralement en local, au sein d'un environnement géré. Il donne lieu à des anomalies délibérées de protocole, à l'utilisation de champs extrêmement longs ou à des données non valides ou peu usuelles. Toutes ces techniques sont conçues pour déclencher des erreurs de programmation. L'objectif est d'identifier des vulnérabilités ou de causer des perturbations.

Toutes ces attaques sont identifiées par le module IPS (intrusion prevention system) de FortiGate qui compte plus de 30 000 règles, ainsi qu'un ensemble de règles en option pour les environnements industriels. Ces règles sont mises à jour quotidiennement pour garantir une sécurité actualisée.

Fortinet IPS peut également définir des règles basées sur le débit des paquets. Nombre de dispositifs IoT présentent un débit de paquet prévisible qui peut être utilisé pour détecter toute activité peu habituelle, causée par un dysfonctionnement ou un acte malveillant potentiel, et ainsi exclure les dispositifs compromis du réseau.

Le chiffrement des données est une tendance générale qui touche également l'IoT, un domaine où les données sont de nature privée. TLS (Transport Layer Security) est souvent utilisé dans ce contexte et l'IPS peut inspecter les flux TLS et détecter les attaques perpétrées sur de tels liens sécurisés.

Contrôle applicatif et de protocole par FortiGate

La fonction de contrôle applicatif permet de surveiller ou de limiter les protocoles pouvant être utilisés par le dispositif IoT. Tout protocole non autorisé peut générer une alerte et être neutralisé si nécessaire. Les définitions des applications intègrent plus de 4 000 règles applicatives dans 24 catégories. Les protocoles IoT utilisés communément, tels que MQTT, AMQP, HTTP et CoAP sont pris en charge. Pour l'IPS, l'inspection TLS peut être utilisée avec une configuration appropriée. De nombreux protocoles industriels sont également pris en charge pour les solutions IIoT (Industrial Internet-of-Things).

Antivirus

Fortinet bénéficie d'un antivirus éprouvé qui bénéficie directement des recherches et des techniques d'intelligence artificielle des FortiGuard Labs. En association avec la prévention d'intrusion, la vaste majorité des fichiers malveillants sont neutralisés en amont de leur cible.

L'antivirus est une fonction essentielle pour les infrastructures IoT, qu'il s'agisse des plateformes ou des serveurs web. Les chercheurs anticipent néanmoins la montée en puissance, dans les années à venir, de malware qui attaqueront les dispositifs eux-mêmes, à l'instar du malware IoT Mirai.

Depuis près de 20 ans, FortiGuard Labs lutte contre les malware de tout type. Aujourd'hui, même si les malware qui s'en prennent directement aux dispositifs sont rares, des recherches sont en cours pour assurer d'une protection de tout premier rang.

Anti-botnet

Toute activité de botnet, détectée par adresse de destination, domaine ou protocole, peut générer une alerte et être neutralisée. De plus, des connexions vers d'autres destinations malveillantes et identifiées par le Service FortiGuard d'identification des indicateurs de compromission, peut générer une alerte. FortiGuard Labs dispose d'une liste à jour des paires adresse/ports de destination connue pour les botnets. Chaque session sortante est ainsi validée par rapport à cette liste. Les botnets qui utilisent des domaines qui changent continuellement de mapping d'adresse IP (domaines fast-flux) peuvent être vérifiés par rapport au domaine en lui-même, en interceptant et en vérifiant la requête DNS (Domain Name System). Au final, même si l'adresse de destination et le domaine sont inconnus, nombre de botnets peuvent être détectés grâce à leurs communications command-and-control. En utilisant ces trois méthodes en parallèle, Fortinet s'assure les meilleures chances de pouvoir détecter des dispositifs infectés par un botnet.

Protection des API avec FortiWeb

Les API sont utilisées dans de nombreux domaines des réseaux IoT. De manière générale, les interactions entre les dispositifs et les plateformes IoT se font via des API. Ceci implique généralement des protocoles comme MQTT, HTTP et CoAP, ainsi que JSON ou XML pour l'encodage des données. Un encodage binaire comme CBOR est souvent utilisé pour les environnements à forte compression et faible bande passante. Les API sont également utilisées pour les communications entre les applications et la plateforme IoT, généralement via HTTP.

Fortinet propose une protection optimale des API avec FortiWeb. Différentes contraintes peuvent être définies, de règles simples encadrant les longueurs des en-têtes et des champs, à la validation et la mise en œuvre d'un schéma focalisé sur HTTP, avec JSON ou XML.

Avec FortiWeb, les attaques génériques ou celles visant les API REST (Representational State Transfer) ou les front-ends web peuvent être maîtrisées.

Automatisation

Fortinet dispose d'un framework d'automatisation complet qui permet d'associer différents déclencheurs à des actions : alertes, suppression de dispositifs indésirables du réseau, ou appels API vers d'autres dispositifs.

Chacun des évènements ci-dessus, lorsque détectés, peut causer la mise en quarantaine d'un dispositif et neutraliser toutes ses communications, jusqu'à identification de la cause et remédiation.

La Security Fabric de Fortinet

Face à de si nombreux défis de sécurité liés à l'IoT, une disparité des produits entraîne de nouveaux défis opérationnels.

La Security Fabric a été conçue pour relever ces défis, grâce à une intégration étroite des modules de sécurité, dans l'optique d'assurer que les dispositifs fonctionnent de manière cohérente, partagent leurs informations de veille sur les menaces, permettent une visibilité et un reporting unifiés, traitent et analysent les logs de manière agrégée et permettent une gestion unifiée à partir d'une interface unique. Les solutions pour IoT de Fortinet comptent parmi les multiples fonctionnalités offertes par la Security Fabric à l'intention des entreprises, MSP, MSSP et MNO.

Intégration avec les partenaires technologiques

Aptilo et Fortinet IoT Connectivity Control Service

La Security Fabric de Fortinet tire également parti de produits tiers, référencés dans le cadre du programme Fabric-Ready. Chacun de ces produits est conçu par un partenaire dans l'optique de pouvoir s'intégrer étroitement au sein de la plateforme Security Fabric, et ainsi générer davantage de valeur pour cette plateforme dans sa globalité.

Fortinet collabore avec de multiples partenaires technologiques pour intégrer leurs solutions IoT. Ceci permet d'améliorer la capacité des fournisseurs de services de communication à offrir un large panel de services IoT innovants aux entreprises. Cet écosystème de solutions pré-intégrées offre une intégration rapide et efficace de services IoT toujours plus nombreux.

Aptilo IoT Connectivity Control Service (IoT CCS) est un exemple d'une intégration IoT réussie au sein de la Security Fabric pour créer davantage de valeur pour les MNO.

IoT CCS permet aux MNO de répondre à certaines contraintes associées aux cœurs de paquets mobiles lors de la conception de services IoT évolutifs :

- Les difficultés à offrir des identifiants du point d'accès réseau (APN) à un large panel d'entreprises
- L'incapacité à offrir des services de sécurité IoT au-delà des APN
- L'intégration automatique des nouveaux clients n'est pas possible
- Les difficultés pour les clients à gérer leurs propres règles de sécurité et de connectivité
- L'impossibilité de définir des règles uniques par client ou par dispositif
- Difficultés à définir des APN vers différentes parties prenantes, à partir d'un même dispositif
- Difficulté à instaurer une connectivité IoT globale sans roaming et avec un trafic local à base de règles

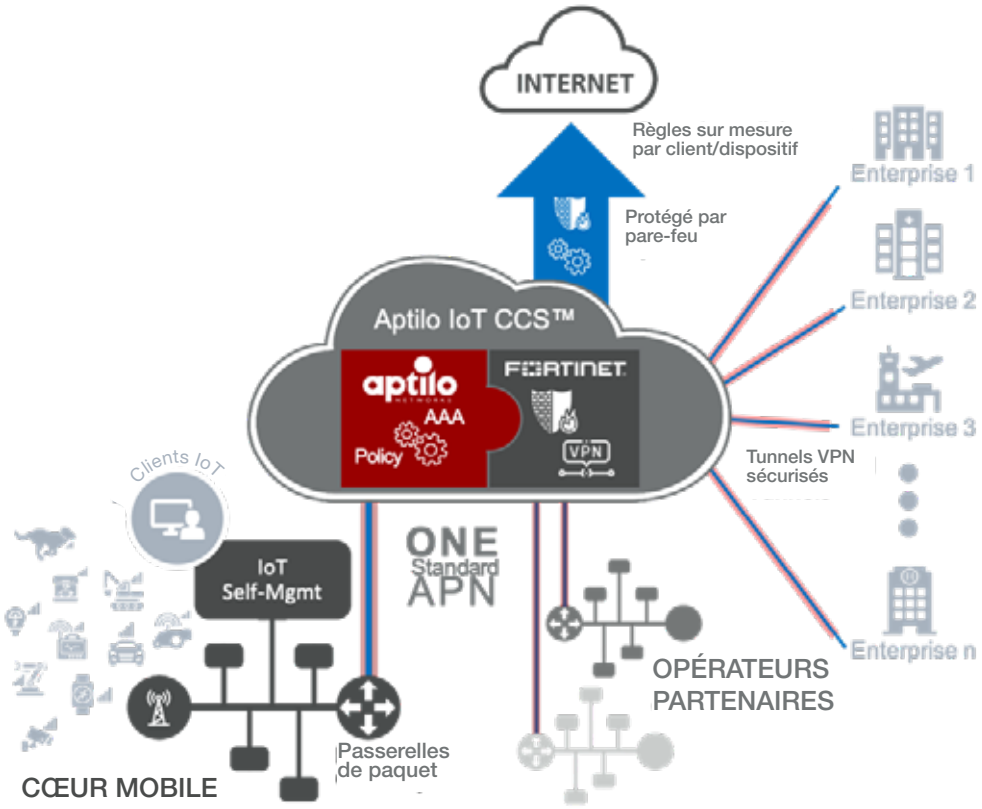
Avec la solution commune de Fortinet et Aptile, les opérateurs mobiles ne touchent pas à leur cœur mobile et définissent de nouveaux services de connectivité IoT. La fourniture d'IoT CCS sous forme de service sur Amazon AWS offre un contrôle flexible de la connectivité et une couche de sécurité dédiée aux cœurs mobiles actuels et futurs. Les opérateurs mobiles peuvent activer des services de connectivité IoT innovants en quelques jours plutôt que mois et avec des coûts maîtrisés.

Les pare-feux réseau FortiGate gèrent la sécurité, le plan de données et le trafic d'IoT CCS. Avec FortiGate, le service IoT CCS bénéficie d'une application des règles sur l'edge, des fonctions de routage, d'une gestion des VPN, d'un filtrage du trafic des dispositifs, d'une protection contre les dénis de service (DDoS), de la limitation des connexions TCP et davantage. La détection des anomalies fait également parti de la couche de sécurité de l'IoT CCS.

Les APN virtuelles et multi-tenant de IoT CCS simplifient le déploiement d'APN privés individuels pour chaque entreprise, avec seulement **un** APN standard au service de **toutes** les entreprises connectées au service. Les VPN sont activés automatiquement via une API, ce qui facilite l'intégration de nouveaux clients.

En utilisant le même nom d'APN, les opérateurs mobiles peuvent rajouter leurs partenaires opérateurs mobiles internationaux à leurs services IoT CCS. Avec leur capacité à localiser instantanément l'eSIM (eUICC) par voie aérienne, les opérateurs peuvent offrir une connectivité globale et sécurisée, sans frais de roaming.

Via l'APN virtuelle multi-tenant IoT CCS, les opérateurs peuvent offrir une connectivité internationale sécurisée, avec breakout optionnel du trafic sélectionné au niveau du point de présence AWS le plus proche, ce qui optimise les performances grâce aux capacités SD-WAN de FortiGate. C'est une fonctionnalité unique qu'il est impossible d'obtenir dans le 3GPP standard.



Synthèse

L'IoT bouleverse le monde dans lequel nous opérons : ces technologies sont des vecteurs d'opportunités majeures, mais offrent aussi de défis importants. Les CSP ont un rôle essentiel à jouer pour apporter un écosystème IoT sécurisé à leurs clients.

Fortinet est idéalement positionné pour sécuriser et répondre aux besoins des services et écosystème IoT des entreprises et des fournisseurs de services. Avec des performances optimales, la prise en charge des environnements multi-tenant et des modèles d'utilisation flexibles, Fortinet apporte aux CSP une plateforme de sécurité IoT qui protège les services IoT, favorise les opportunités commerciales autour de ces technologies et en concrétise les promesses.

785701-0-1-FR
mars 5, 2021 1:07 PM
wp-FA-securing-the-iot-ecosystem-with-fortinet-A4_FR