Livre blanc

Bypass inline : Dimensionner les outils de prévention des menaces inline afin de s'adapter aux réseaux haute vitesse

Vos outils de prévention ont-ils du mal à faire face à la vitesse croissante du réseau de votre entreprise ? Est-ce que le nombre et la diversité d'outils de sécurité dont vous pensez avoir besoin commencent à peser sur votre budget et à compliquer à l'extrême votre infrastructure de sécurité ?

Ce livre blanc présente la façon dont la fonctionnalité de bypass inline de la plateforme de sécurité GigaSECURE® facilite le déploiement des initiatives de sécurité en permettant aux outils de prévention des menaces d'évoluer et de rester en phase avec les réseaux haute vitesse. Avec la Plateforme de sécurité GigaSECURE, les entreprises peuvent améliorer à moindre coût leur posture de sécurité sans avoir à sacrifier les performances réseau.

Le casse-tête « Perturbation/Défense »

Sur les marchés actuels évoluant rapidement, les entreprises dépendent de réseaux haute vitesse afin de stimuler la collaboration, d'améliorer l'innovation et d'accroître la productivité. Malheureusement, les débits de données réseaux croissants et les mises à niveau de réseau qui en résultent ont des répercussions considérables pour les administrateurs sécurité, particulièrement ceux qui dépendent d'outils inline de prévention des menaces haut de gamme. Ces outils n'arrivent tout simplement pas à s'adapter à la vitesse croissante des réseaux. Comme le trafic est transmis plus rapidement, les outils ne disposent pas soit du temps nécessaire, soit de la capacité requise pour traiter l'ensemble du trafic. En conséquence, le risque d'attaque s'accroît, ce qui en retour peut invalider les investissements et les bénéfices des réseaux haute vitesse pour les entreprises.

Tous les trafics ne sont pas égaux ; ou du moins ils n'ont pas tous besoin d'être inspectés de la même manière

Dans de nombreux cas, les outils de sécurité inline ne sont pas en mesure de gérer des débits de trafic plus élevés lors d'une mise à niveau du réseau - par exemple, de 10 Gb à 40 Gb -, et les entreprises se voient contraintes de mettre à niveau leur infrastructure de sécurité, ce qui s'avère fastidieux, voire impossible du point de vue architecture ou irréalisable financièrement.

Une alternative à une mise à niveau complète et onéreuse est d'accroître l'efficacité des outils existants en leur transmettant uniquement des données appropriées à traiter. Il n'est pas nécessaire que tous les outils de sécurité inspectent l'ensemble du trafic. Par exemple, un pare-feu pour application Web (WAF) doit uniquement inspecter le trafic Web, il n'est pas nécessaire qu'un système de prévention d'intrusion (IPS) ait à ré-inspecter du trafic déjà inspecté dans une autre zone, et un système pour menaces avancées persistantes (ATP) n'a peut-être pas à inspecter le trafic issu d'une zone interne ou d'une catégorie de trafic spécifique raisonnablement sécurisé.

Autrement dit, différents trafics doivent être traités différemment. En bref, il s'agit in fine de transmettre le trafic approprié à l'outil adéquat au moment opportun. Si un outil de sécurité reçoit uniquement les données réseau précises devant être inspectées, plutôt que de se voir surchargé par des données non pertinentes, alors l'outil peut faire face aux volumes de données croissants et commencer à détecter et prévenir plus de menaces.

Bypass inline dans la Plateforme de sécurité GigaSECURE : Améliorer la sécurité sans compromettre la disponibilité du réseau

La Plateforme de sécurité GigaSECURE constitue un collecteur de paquets réseau de nouvelle génération, spécialement conçu aux fins de sécurité. Un élément intégral de la solution est un ensemble de fonctionnalités, appelé « bypass inline », conçu afin de maximiser l'efficacité des outils de prévention inline sans compromettre la disponibilité du réseau en permettant au personnel opérationnel de sélectionner et de distribuer le trafic spécifique d'intérêt vers différents outils de sécurité inline.

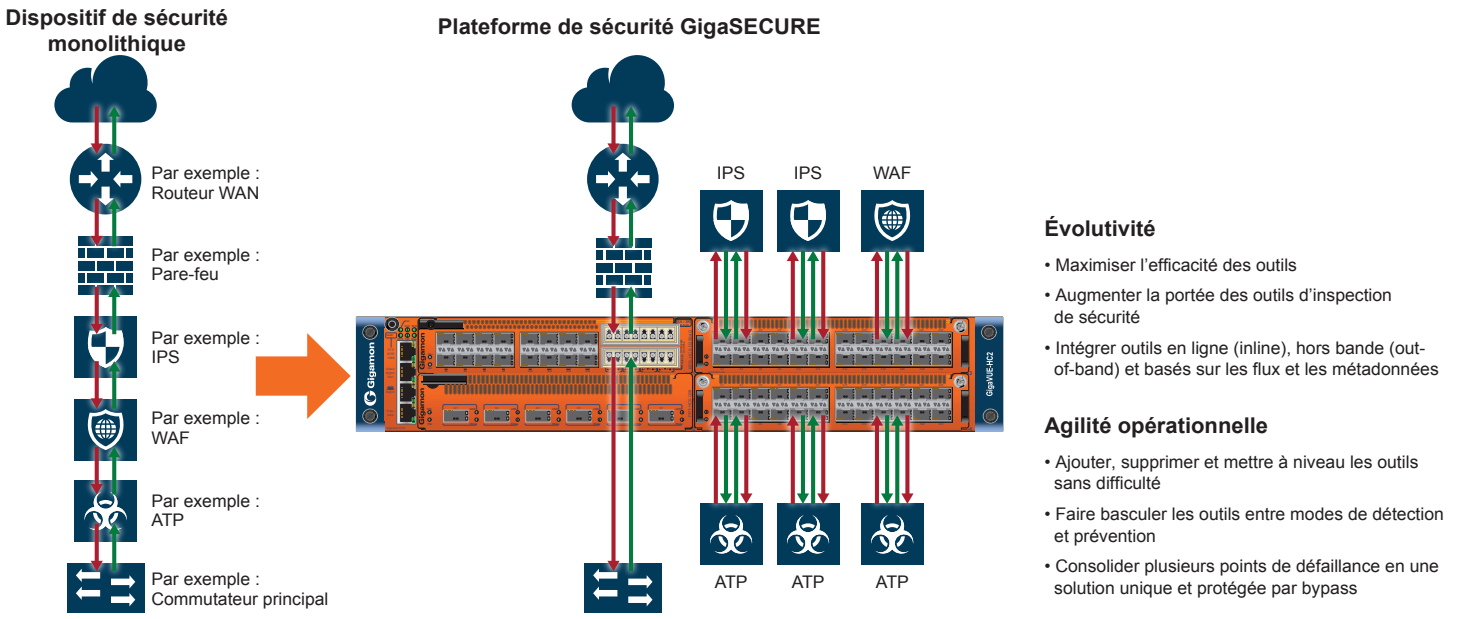

Figure 1 : Adapter les outils de prévention des menaces avec GigaSECURE®

Protection par bypass logique et physique intégrée

En offrant une protection par bypass physique intégrée, la Plateforme de sécurité GigaSECURE ne peut elle-même devenir un point unique de défaillance. Bien que redondantes, les sources d'alimentation à partage de charge rendent une telle situation peu probable, la Plateforme de sécurité GigaSECURE peut faire appel à des relais en mode « fail-to-wire » (protection bypass) afin de maintenir le réseau fonctionnel même dans l'éventualité d'une panne. De plus, les paquets et flux ne sont pas traités au niveau logiciel, et par conséquent, elle n'est pas vulnérable aux types de surcharges de traitement fréquents avec les outils de sécurité. En outre, sa capacité à prendre des décisions quant à la transmission de paquets au niveau matériel aide à garantir qu'aucun délai ne soit ajouté au trafic réseau.

De façon assez similaire à la façon dont un système de navigation GPS fournit des mises à jour de la circulation en temps réel et suggère des routes alternatives autour des zones de congestion, la protection bypass peut détecter la défaillance d'un outil actif et rediriger le trafic vers un outil de secours. La Plateforme de sécurité GigaSECURE évalue constamment l'état des outils inline par le biais de paquets « heartbeat » (battements de cœur) bidirectionnels. En cas de défaillance d'un outil de sécurité inline, les options de configuration permettent de contourner soit le lien réseau défectueux soit l'outil de sécurité défaillant afin de maximiser la disponibilité.

Contrairement à une configuration actif/secours traditionnelle, pour laquelle un outil de sécurité inline de secours demeure complètement inutilisé jusqu'à la défaillance d'un outil actif, le bypass inline offre l'option d'envoyer le trafic vers un outil de secours selon un mécanisme de protection 1+1 ou N+1. Dans ce dernier cas, le trafic peut être distribué simultanément à plusieurs outils inline : par exemple, l'ensemble des trois dispositifs ATP peuvent être utilisés dans un groupe d'outils, plutôt que de recourir à un mode de dispositif de type « 2 ATP actifs + 1 ATP de secours », pour lequel le dispositif ATP de secours reste inutilisé la plupart du temps. Un tel modèle contribue à garantir que l'ensemble des actifs du dispositif de prévention de sécurité inline sont utilisés à leur plein potentiel, et ainsi les entreprises peuvent obtenir le maximum des investissements réalisés dans les outils de sécurité existants.

Dans l'éventualité d'une défaillance d'outil de sécurité inline, la Plateforme de sécurité GigaSECURE détecte la défaillance et redistribue le trafic vers les outils fonctionnels restants du groupe d'outils concerné. Une fois l'outil défaillant de retour en ligne - ce qui est détecté en mesurant la réémergence des paquets « heartbeat » - la Plateforme de sécurité GigaSECURE peut de nouveau recommencer à transmettre le trafic vers l'outil récupéré aux fins d'inspection. Les paramètres des heartbeats (battements de cœur) peuvent être définis afin de répondre aux pannes en moins de 50 millisecondes, ou leur temporisation peut être ajustée afin de contourner tout outil surchargé ou ajoutant une latence excessive.

Contrairement au dispositif de sécurité monolithique, montré à gauche sur la figure 1, la Plateforme de sécurité GigaSECURE (à droite) offre une couche d'isolation protégeant le réseau et les outils de sécurité de tout changement survenant chez l'un ou les autres. De plus, cette approche permet aux NetOps de conserver le contrôle sur un ensemble d'éléments de l'infrastructure ; par exemple : routeur WAN, pare-feu ou commutateur principal, et les SecOps peuvent traiter séparément les mises à niveau, la maintenance, les ajouts ou suppression d'outils en ligne, par exemple : IPS, WAF, ATP, sans compromettre la disponibilité du réseau.

Maximiser l'efficacité des outils de sécurité

Parfaitement adaptée pour répondre aux disparités entre réseau, débit de données et capacité du dispositif de sécurité, la Plateforme de sécurité GigaSECURE peut distribuer la charge vers plusieurs outils de sécurité, de sorte que la sécurité réseau soit ajustée de façon linéaire conformément au nombre d'outils déployés, tout en assurant qu'un outil de sécurité donné puisse voir l'ensemble du trafic correspondant à un utilisateur et à des sessions de serveur spécifiques.

Ce type de transfert de trafic ciblé est crucial pour détecter plus rapidement les APT. Plutôt que de surveiller l'ensemble du trafic circulant à travers le réseau, la Plateforme de sécurité GigaSECURE peut recourir à la technologie Flow Mapping® afin de transmettre sélectivement des sessions spécifiques aux fins de surveillance, et contourner les autres, à l'aide de critères de filtrage basés sur le type d'application, par exemple : base de données, Web, e-mail ; port TCP/UDP ; adresse IP et MAC des serveurs et terminaux ; ou toute combinaison possible. Non seulement, il s'agit d'un compromis pratique entre performances et sécurité, mais cela élimine le besoin d'achat inutile de plus d'outils de sécurité ou d'outils à capacité plus élevée. Les entreprises peuvent appliquer dynamiquement ces configurations à l'aide des API exposées par la Plateforme de sécurité GigaSECURE, et les intégrer à un environnement de sécurité DevSecOps moderne.

Le résultat net ? Les outils de sécurité inspectent désormais le trafic le plus pertinent et accroissent la probabilité de découverte et de réponse rapide aux risques.

Consolider et optimiser la surveillance de sécurité

Bien que certaines cybermenaces sophistiquées justifient de disposer de dispositifs de sécurité sur chaque segment et à tout endroit, il est souvent extrêmement onéreux de placer des pare-feux, des anti-malwares et dispositifs d'inspection de contenu sur chaque segment du réseau ou chaque point de sortie de passerelle Internet. Il est bien plus efficace et moins coûteux d'agréger le trafic réseau depuis plusieurs segments du réseau vers la Plateforme de sécurité GigaSECURE, et d'envoyer le trafic agrégé présentant un intérêt à un outil de sécurité centralisé et à capacité plus élevée aux fins d'inspection. Les entreprises peuvent adopter une approche similaire aux bureaux distants, notamment s'ils font transiter l'ensemble du trafic depuis ces bureaux distants vers quelques points d'agrégation. Cette approche centralisée aide à s'assurer qu'elles obtiennent le maximum des investissements informatiques de sécurité à grande échelle au niveau des points d'agrégation tels que les centres de données et campus.

La Plateforme de sécurité GigaSECURE peut agréger et transmettre les flux de trafic depuis plusieurs segments du réseau, et envoyer le trafic pertinent à un outil de sécurité commun. La Plateforme de sécurité GigaSECURE marque le trafic, de sorte que le trafic aller et retour soit envoyé vers le segment approprié. Cette capacité est également utile dans les architectures réseau utilisant un routage asymétrique.

Dans les réseaux avec chemins redondants, la Plateforme de sécurité GigaSECURE peut surveiller autant les liens réseau actifs que de secours, éliminant le besoin de répliquer l'intégralité du dispositif de sécurité pour chaque lien. En maintenant l'intégrité de la session indépendamment du chemin pris, les dispositifs de sécurité reçoivent les sessions entières du trafic bidirectionnel.

Puisque la plupart des architectures de sécurité sont constituées d'ensembles multi-fournisseurs de produits spécialisés haut de gamme, leur besoin d'inspecter le même trafic peut générer des conflits et surcharger le réseau. La Plateforme de sécurité GigaSECURE répond à ce problème en agrégeant les fonctions de transfert et de distribution du trafic, et en y intégrant de l'intelligence qui non seulement résout les goulots d'étranglement associés aux paquets, mais permet également d'optimiser les outils de sécurité. Par exemple, la Plateforme de sécurité GigaSECURE enverra uniquement le trafic de messagerie à l'outil d'inspection d'e-mail, uniquement le trafic WEB à un WAF, et l'ensemble du trafic, si souhaité, à un groupe d'IPS. Une telle consolidation des politiques de distribution du trafic facilite l'adaptation du dispositif de sécurité afin de permettre l'intégration de nouvelles technologies ainsi que les mises en place de maquettes, sans interruption du réseau. De plus, tout outil supplémentaire nécessitant un accès au trafic réseau n'a qu'à simplement se connecter à la Plateforme de sécurité GigaSECURE afin d'obtenir la visibilité nécessaire.

Ajouter, supprimer et mettre à niveau sans difficulté des outils de sécurité

Avec la Plateforme de sécurité GigaSECURE, les équipes SecOps peuvent appliquer des correctifs logiciels, effectuer des mises à jour sans besoin de coordination fastidieuse des fenêtres de maintenance, sans interruption du réseau et sans sécurité amoindrie. Plutôt que d'être directement connectés en ligne, les outils de sécurité sont connectés à la Plateforme de sécurité GigaSECURE, à partir d'où ils peuvent être retirés, redémarrés ou mis à jour sans affecter le réseau. Avant la mise hors service de l'outil inline, la Plateforme de sécurité GigaSECURE peut permettre au trafic de contourner cet outil jusqu'à qu'il soit de nouveau opérationnel, prêt à inspecter à nouveau.

Lors du déploiement de plusieurs outils inline, les équipes SecOps peuvent les mettre à niveau de façon séquentielle sans avoir à disposer d'une fenêtre de maintenance, ni devoir interrompre le réseau pendant une durée prolongée, et mieux encore, elles peuvent ajouter des outils à la Plateforme de sécurité GigaSECURE sans aucun besoin de fenêtre de maintenance. Le trafic peut être dirigé vers un nouvel outil avec une commande logicielle et un impact minimal sur le réseau.

Basculement d'outils de sécurité entre modes de prévention et de détection

De nombreuses solutions de sécurité inline peuvent également opérer en mode hors bande (out-of-band). De fait, certains dispositifs disposent de « modes d'apprentissage » par le biais desquels ils passent des jours voire des semaines à surveiller passivement le réseau afin d'établir un comportement normal de base et d'identifier des anomalies ultérieurement. Lorsque hors bande, le dispositif de sécurité recevra uniquement une copie du trafic. Une fois ajusté et prêt à opérer dans une configuration inline, il peut être déplacé programmatiquement par la Plateforme de sécurité GigaSECURE sans besoin d'un quelconque recâblage.

La capacité de la Plateforme de sécurité GigaSECURE à faire basculer un outil de sécurité entre les modes de prévention et de surveillance, ou de détection, constitue une capacité puissante que les administrateurs sécurité peuvent employer de nombreuses façons. Par exemple, ils peuvent :

- Valider l'opération d'un outil de prévention en mode détection après qu'il a été mis à niveau avec un nouveau logiciel.
- Déployer des outils de prévention des menaces en mode détection des menaces dans des environnements applicatifs sensibles à la latence, ou des environnements où la disparité entre réseau, débit de données et niveau de sécurité est élevée ; par exemple, pour les fournisseurs de services, ou sur les réseaux 40 Gb / 100 Gb exécutant des outils 1 Gb / 10 Gb. Lorsqu'un outil détecte une menace, la Plateforme de sécurité GigaSECURE peut être programmée afin de faire rapidement basculer l'outil inline en mode prévention. Une telle approche garantit que la latence est réduite lorsqu'aucune menace malveillante n'est détectée, et que des latences supérieures sont uniquement observées lorsque l'outil inline bloque activement des flux malveillants.

Intégrer outils inline, hors bande, basés sur les flux et métadonnées

Afin d'accroître davantage l'efficacité du dispositif d'une entreprise, un administrateur sécurité peut mettre à profit la Plateforme de sécurité GigaSECURE afin de transmettre simultanément le trafic d'intérêt autant aux outils inline qu'aux outils hors bande (out-of-band). Elle peut également être utilisée afin de générer des données de flux - par exemple NetFlow ou IPFIX - vers les outils basés sur les flux et alimenter en métadonnées d'autres outils de sécurité hors bande, tels que gestion d'information et d'événements de sécurité (SIEM), analyse de comportement utilisateur et entité (UEBA), analyses de sécurité. En mettant à profit la Plateforme de sécurité GigaSECURE afin de puiser dans les infrastructures virtuelles et cloud, une entreprise peut considérablement étendre la portée de son dispositif de sécurité, et cela à moindre coût. De la même manière, les outils de surveillance des performances applicatives (APM) et de surveillance des performances réseau (NPM) non sécuritaires peuvent recevoir du trafic réseau depuis cette même Plateforme de sécurité GigaSECURE, permettant ainsi à plusieurs équipes au sein de l'entreprise de bénéficier de cet investissement.

De plus, la Plateforme de sécurité GigaSECURE peut également décharger depuis les outils inline le déchiffrement SSL avide en ressources ; elle déchiffre simplement le trafic une seule fois et le distribue à autant d'outils inline ou hors bande que nécessaire. Grâce à cette approche, les entreprises peuvent réaliser un ROI considérable, et obtenir des avantages significatifs en matière de performance et d'efficacité.

Récapitulatif

Avec l'accroissement constant des débits de données réseau, les architectes et administrateurs de sécurité ont besoin d'une architecture permettant à leurs dispositifs de prévention de menaces de faire face efficacement sans compromettre la résilience du réseau. La capacité de bypass inline logique et physique intégrée constitue un composant clé de la Plateforme de sécurité GigaSECURE, permettant aux administrateurs sécurité de maximiser simultanément la prévention des menaces, la résilience de la sécurité et la disponibilité du réseau. Avec cette approche, les architectes de sécurité peuvent mettre fin à la démultiplication des outils, réduire les coûts imputables aux outils et réduire significativement le temps nécessaire pour le déploiement d'initiatives de prévention des menaces au sein de leurs entreprises.

3260-01 02/18

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 États-Unis | +1 (408) 831-4000 | www.gigamon.com