Gigamon®

Aperçu de la solution

Visibilité active pour une sécurité multiniveau

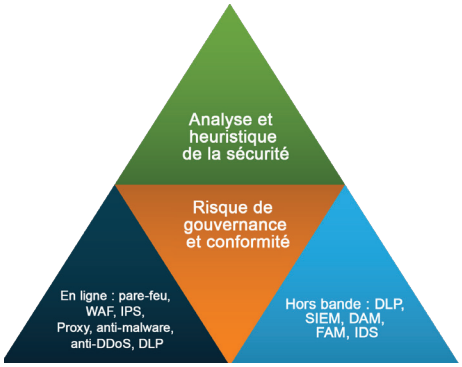
Introduction

Les cyber menaces deviennent de plus en plus complexes et répandues. Les approches traditionnelles de la sécurité comme les pare-feu et la protection antivirus ne sont pas équipées pour parer aux menaces et risques de la sécurité moderne . Heureusement, les outils de sécurité deviennent aussi plus complexes. La dernière génération de pare-feu, de systèmes de prévention et de détection des intrusions, les dispositifs de protection contre le malware, les dispositifs de prévention contre la perte de données et d'autres outils de sécurité ont augmenté pour contrer les menaces complexes et sophistiquées. Le combat que doivent livrer les agents de sécurité de l'information ne porte pas sur les outils à déployer, mais sur la manière de le faire.

Aperçu de la sécurité multiniveau

La sécurité multiniveau ne consiste pas à se fier à des remèdes miracles ni à des solutions ponctuelles. Elle suppose que des effractions seront commises, que le malware se déplacera verticalement et horizontalement à travers le réseau, et admet que protéger son entrée ne suffit pas. Ceci signifie que l'on doit adopter une attitude de zéro confiance et appliquer un suivi de la sécurité et des meilleures pratiques à travers tout le réseau et pour tout le trafic. Au sens large, les niveaux considérés sont :

- Outils hors bande – Ces outils reçoivent des paquets de ports SPAN et TAP et analysent les sessions et les charges utiles quant à la présence de menaces. Ces outils peuvent vérifier le trafic de manière très détaillée, mais n'ont qu'une vue partielle du trafic en fonction de l'endroit et de la manière dont ils sont déployés. Parmi les exemples, on citera les systèmes de détection d'intrusions, de prévention de pertes de données et de détection de malware.
- Outils en ligne – Intégrés dans le réseau de production, les outils en ligne analysent les paquets au fur et à mesure de leur passage. Ces outils peuvent bloquer immédiatement un trafic suspect étant donné qu'ils entrent en action plutôt que d'attendre une mesure administrative. De nombreux outils de ce type peuvent fonctionner soit hors bande, soit en ligne. Parmi les exemples, on citera les systèmes de protection anti-intrusion, les pare-feu pour applications Web et les outils conçus pour se défendre contre le malware ou rejeter des attaques de services.
- Analyse basée sur le débit – L'analyse et l'heuristique de la sécurité utilisent les technologies NetFlow et analogues pour dépasser l'identification de la signature, afin de découvrir de nouvelles menaces et capter des comportements suspects qui peuvent être invisibles au niveau du paquet.



- Conformité réglementaire – Les normes réglementaires rigoureuses imposées par le Conseil des normes de sécurité PCI et autres mandats gouvernementaux comme la loi HIPAA, la loi SOX et la loi GLB font qu'il est très difficile de préserver la confidentialité de l'utilisateur et de respecter la conformité. Il ne suffit pas d'être conforme : vous devez pouvoir prouver votre conformité pendant un audit.

Gigamon offre une architecture qui alimente en trafic les outils de sécurité et apporte donc la visibilité dont ils ont besoin, mais améliore également leurs résultats et leur résilience.

Défis pour la sécurité

Le déploiement d'une plateforme de sécurité multiniveau peut comprendre les défis suivants:

- Contention du port SPAN
- Le trafic chiffré ainsi que le cloud ne peut pas être inspecté
- Les outils de sécurité en ligne introduisent des risques de défaillance pour le réseau
- Les outils de sécurité peuvent ne pas être adapté aux vitesses croissantes du réseau ni au nombre d'utilisateurs et d'applications
- L'application NetFlow Generation peut ne pas être autorisée ou même disponible sur les commutateurs et les routeurs de productionNetzwerksicherheit und Anwendungsleistung können oft in Konflikt geraten

- La sécurité du réseau et les performances des applications peuvent souvent être conflictuels. Les restrictions budgétaires empêchent le déploiement des meilleures solutions de leur catégorie.

Étapes d'une visibilité active pour la sécurité multiniveau

La sécurité multiniveau à zéro confiance exige une plateforme avec la flexibilité et l'évolutivité qui permettent de l'adapter en fonction de l'évolution de l'infrastructure informatique ou des menaces. Les étapes suivantes identifient les éléments clés pour la construction de la visibilité d'un bout à l'autre qui peut contribuer à maximiser l'efficacité d'une approche à sécurité multiniveau.

Étape 1 – EXPLOITER tous les liens critiques

La sécurité commence par la visibilité et celle-ci commence par l'exploitation du réseau. En exploitant de multiples points dans les réseaux et en les dotant de ports SPAN, vous pouvez obtenir une visibilité de cent pour cent sur le trafic. Les exploitations (TAP) peuvent être déployées sur des dizaines ou des centaines de points du réseau avec une incidence zéro sur les performances du réseau ou de l'application. Les TAP optiques sont complètement passifs, n'exigent pas d'énergie ni de gestion. Même les réseaux à grande vitesse avec des liens bidirectionnels de 40 Go peuvent être exploités et suivis ; des connexions cuivre de 1 Go et 10 Go peuvent aussi être exploitées avec les dispositifs actifs gérés.

Des ports SPAN ne sont utilisés que seulement si cela est nécessaire. Les ports SPAN représentent la priorité la plus faible sur les équipements réseau et peut générer des ralentissements et des pertes de paquets. Ceci entraîne une vue imprécise sur ce qui se passe dans le réseau et ouvre la porte à la présence de menaces restées inaperçues.

Étape 2 – Connecter les liens à une Visibility Fabric

Placés entre l'infrastructure et les outils de sécurité et de suivi qui nécessitent d'accéder aux données, les nœuds de la Visibility Fabric de Gigamon offrent une plateforme extensible et élastique pour l'évolution de la technologie et du réseau. La Visibility Fabric comprend un ou plusieurs nœuds de visibilité qui reçoivent le trafic depuis des TAP et des SPAN de réseau. Une fois à l'intérieur du tissu, le trafic peut être acheminé vers tous les outils hors bande, peu importe leur connexion physique et l'endroit où cette connexion est établie. Ceci fournit une plateforme flexible sur laquelle il est possible de construire la sécurité multiniveau. Étant donné les progrès des techniques de la surveillance de sécurité et l'accélération des vitesses de réseau, de nouveaux outils peuvent être ajoutés et les outils existants peuvent être étendus en douceur sans perturber le réseau. Avec la Visibility Fabric, vous pouvez grouper, filtrer, répliquer et modifier intelligemment le trafic vers vos outils de sécurité.

Gigamon utilise sa technologie Flow Mapping® brevetée pour acheminer sélectivement le trafic vers des outils spécifiques sans éliminer le trafic que d'autres outils doivent analyser. Après l'acheminement d'un trafic spécifique à un outil, une autre règle pour la collecte de données achemine la totalité du trafic restant vers un système de suivi générique ou un dispositif de stockage , éliminant ainsi les angles morts de la sécurité.

Le Flow Mapping fonctionne aussi pour les outils en ligne, en définissant des profils de trafic spécifiques pour différents outils de manière à ce que chacun d'eux traite des paquets du type de trafic qu'il souhaite. Le trafic qui est connu comme sûr peut contourner entièrement les outils en ligne et/ou être envoyé en parallèle vers les outils hors bande, comme un IDS. Cette sensibilisation de l'application améliore non seulement l'efficacité, mais aussi la performance de l'outil de sécurité. Parmi les avantages de la Visibility Fabric, on citera :

- la visibilité instantanée et omniprésente dans le réseau, y compris les environnements physiques et virtuels
- la réduction des dépenses par la simplification des opérations et la centralisation du suivi
- l'élimination de la contention parmi les outils et les services informatiques pour l'accès aux données
- l'optimisation des performances des outils de sécurité pour une meilleure rentabilité des investissements.

Étape 3 – Connecter les outils de sécurité en ligne

Les outils en ligne, depuis les pare-feu simples jusqu'aux systèmes de pointe pour la prévention des intrusions (IPS), sont cruciaux pour toute solution de sécurité multiniveau. Il va de soi que tout déploiement en ligne dans le réseau représente un point de défaillance potentiel, mais ces risques peuvent être diminués par la technologie bypass. Une protection de bypass physique permet au trafic réseau de continuer à transiter en cas de panne de courant. La protection de bypass logique est la capacité à détecter la défaillance d'un outil de sécurité en ligne et à contourner l'outil (non inspecté) ou à amener le trafic réseau à emprunter un trajet redondant. Des paquets sont générés au travers de l'outil de sécurité pour vérifier la santé constante de l'outil. La bascule automatique est opérée si les paquets sont bloqués / ralenti ou que l'interface est perdue.

Lorsque la solution Gigamon est déployée sur des réseaux redondants, la fonctionnalité de propagation de l'état du lien garantit que l'état du lien amont ou aval de la plateforme Gigamon peut être transmise. Ainsi, le routage en place activera un chemin réseau secondaire automatiquement. Les outils de sécurité en ligne représentent aussi un goulot d'étranglement potentiel du réseau. Pour pallier à ceci Gigamon assure la répartition de charge dynamique entre plusieurs outils de sécurité. La fonctionnalité de redondance N+1 permet d'avoir un (ou plusieurs) outil de sécurité reprenant la charge de celui ou ceux qui sont défaillants.

Les différents outils en ligne peuvent recevoir grâce au filtrage différents types de trafic, ce qui permet l'optimisation de ces outils pour des applications spécifiques. Le trafic déjà sécurisé peut contourner totalement un outil en ligne, ce qui minimise la latence et améliore les performances. Les outils en ligne qui doivent inspecter le même trafic peuvent être configurés en série. Si un outil es défaillant, le trafic peut être dévié jusqu'à l'outil suivant en série. Par conséquent, de multiples points potentiel de défaillance sont consolidés et protégés, ce qui rend le réseau plus sûr et plus robuste.

Des liens réseau multiples, qu'ils fassent partie d'un agrégat ou qu'il s'agisse de segments indépendants, peuvent être regroupés et protégés par les mêmes outils, tout en maintenant l'intégrité du trajet de données Ceci optimise 'investissement réalisé pour l'acquisition de l'outil en ligne et maximise la sécurité pour des liens à vitesse inférieure.

Pour mieux réagir aux menaces détectées, de nombreux outils de sécurité hors bande qui surveillaient le trafic passivement passent aujourd'hui à des déploiements en ligne (inséré dans le réseau de production). Il est souvent utile d'installer, de configurer et d'optimiser d'abord un outil hors bande avant de l'insérer en ligne. Ceci peut être réalisé simplement avec un paramétrage logiciel au lieu d'un recâblage et d'une reconfiguration de l'infrastructure réseau de production.

Étant donné que les outils de sécurité en ligne ne sont pas connectés directement au réseau de production, des outils peuvent être ajoutés, étendus ou enlevés sans perturbation ou presque du trafic de production. Les alertes émises à partir de la Visibility Fabric lorsque le bypass physique ou logique est déclenché permet de réagir immédiatement évitant d'aggraver la situation.

Étape 4 – Connecter les outils de sécurité hors bande

S'agissant des menaces, la majorité des outils de sécurité fonctionnent hors bande, en suivant passivement le réseau et en émettant des alertes lorsqu'une mesure est nécessaire. La sécurité multiniveau exige que les outils de sécurité aient accès à la totalité du trafic par le biais de la Visibility Fabric. Les données utiles malveillantes qui passent outre les sentinelles du périmètre peuvent être détectées dans le noyau ou lors de leur déplacement vers différents hôtes de manière à dissimuler leur emplacement.

Des outils peuvent choisir sélectivement le trafic à suivre et ne pas tenir compte du reste, mais le simple fait de procéder à ce choix utilise des cycles de CPU. S'agissant de menaces, un outil de sécurité qui se spécialise dans le suivi des emails par exemple, n'a pas besoin de voir le trafic non-email. En même temps, les outils axés sur les applications Web ou le suivi de bases de données voudront voir ce trafic, mais pas les courriels.

Le Flow Mapping® achemine un trafic spécifique vers un ou plusieurs outils sur la base de règles de topographie définies par l'utilisateur. Les outils hors bande peuvent aussi compléter des outils en ligne en inspectant une copie du trafic envoyé à, ou reçu depuis, les outils en ligne. Une détection d'intrusion peut avoir lieu en parallèle avec la prévention d'intrusion. En outre, un trafic hors ligne peut être distribué sur de multiples outils hors bande de manière à partager la charge et obtenir une visibilité complète sur la sécurité.

Étape 5 – Tirer profit de la capacité de traitement du trafic GigaSMART®

La technologie GigaSMART étend les performances et la valeur de l'architecture de la Visibility Fabric de Gigamon en élargissant la visibilité, en générant des données NetFlow, en améliorant les performances de l'outil et en protégeant la vie privée tout en facilitant la conformité réglementaire. Tout le trafic vers des outils de suivi hors bande peut bénéficier de l'intelligence GigaSMART quel que soit l'endroit où il est entré dans la Visibility Fabric.

- Décryptage SSL – Le trafic crypté peut représenter une portion importante du trafic sur le réseau, mais la plupart des outils sont soit dans l'incapacité de décrypter et de suivre le trafic crypté, soit leur passage est nettement ralenti de ce fait. En outre, du malware peut se dissimuler dans des activités dans

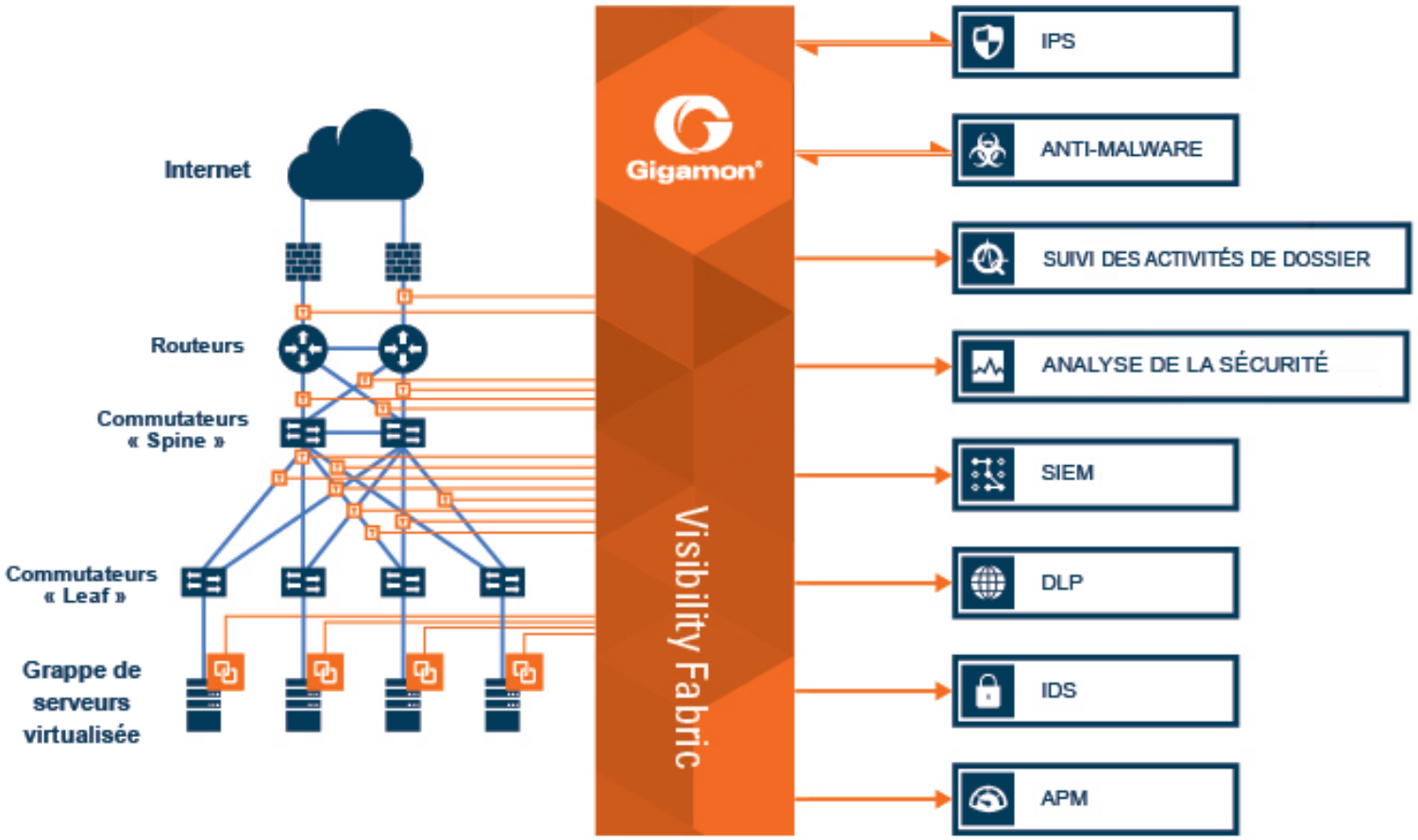


Figure 1 : Sécurité multiniveau supportée par la Visibility Fabric unifiée de Gigamon

le cadre de sessions cryptées. GigaSMART a le pouvoir de décrypter des paquets et d'envoyer un trafic clair vers les outils de suivi hors bande.

- Stripping d'en-têtes – Le trafic intégré dans des protocoles comme VXLAN ou Cisco FabricPath peut ne pas convenir à des outils de suivi ou utiliser de précieuses ressources de traitement. GigaSMART peut retirer ces en-têtes avant d'envoyer les paquets vers les outils.
- Tunneling – Les outils de sécurité sont souvent trop coûteux pour être déployés sur des sites distants, ce qui les rend vulnérables aux attaques ou à la perte de données. GigaSMART peut transmettre le trafic de sites distants vers les outils dans le centre de données principal où il peut être inspecté.
- NetFlow Generation – GigaSMART peut décharger l'application NetFlow Generation du réseau de production et envoyer les données vers des collecteurs multiples. Il le fait sans échantillonner le trafic, de sorte que les outils de sécurité basés sur le débit obtiennent l'image la plus complète et la plus claire possible.
- Déduplication – Des paquets doubles gaspillent des ressources et la puissance de traitement. En éliminant les doublons du débit de trafic avant de les envoyer aux outils, GigaSMART améliore les performances et l'extensibilité du suivi de la sécurité.
- Équilibrage de charge – Le trafic distribué vers des outils multiples sans GigaSMART maintient les sessions, mais n'entraîne pas toujours un équilibre égal du trafic entre les outils. L'équilibrage de charge GigaSMART peut tenir compte de la bande passante , du nombre de connexions et de la pondération.
- Filtrage de paquets adaptatif – GigaSMART offre un filtrage de trafic basé sur les en-têtes de paquets de même que sur la couche 7 et les données de charge (pload). Ceci permet à des outils de sécurité d'inspecter des applications spécifiques différentes même si celles-ci utilisent les mêmes adresses IP et ports TCP.
- Découpage et masquage de paquets – Les informations privées et sensibles contenues dans les paquets peuvent représenter un casse-tête réglementaire (n° de carte de crédit, n° de sécurité sociale etc…). En enlevant ou masquant ces données avant l'envoi des paquets aux outils, GigaSMART évite les préoccupations relatives au stockage des données et aux audits de conformité.

Ces applications peuvent être combinées et/ou appliquées à différents profils de trafic pour maximiser la couverture de sécurité. Par exemple, le trafic SSL peut être décrypté puis masqué pour que les données privées restent sécurisées ou

bien NetFlow peut être généré à partir du trafic avant ou après l'enlèvement des en-têtes d'encapsulation.

Étape 6 - Ajouter les outils autres que les outils de sécurité pour maximiser le rendement de l'investissement

Une fois en place, la Visibility Fabric peut aussi offrir le trafic aux outils de non-sécurité, y compris la mesure de la performance applicative l'expérience de l'utilisateur et le suivi de services commerciaux. Étant donné que le trafic peut être répliqué vers des outils multiples, la sécurité et le monitoring autre que la sécurité peuvent inspecter les mêmes paquets sans devoir lutter pour accéder aux mêmes ports SPAN que dans un déploiement traditionnel. D'autres outils peuvent alors être ajoutés, enlevés et étendus sans incidence sur les outils sécurité et sans que le réseau soit rendu vulnérable. Ces outils bénéficient également d'une visibilité étendue sur l'ensemble du réseau, dans le cloud et dans des sessions chiffrées et des paquets encapsulés. Le fait d'offrir la visibilité sur de multiples outils représente une rentabilisation immédiate de l'investissement.

Résumé

Le paysage changeant des menaces et l'infrastructure des réseaux en évolution obligent les organisations à repenser fondamentalement leur approche de la sécurité de manière à tenir à distance les menaces modernes. Les équipes de sécurité se tournent vers des déploiements multiniveau, en tirant profit des tout derniers outils d'information sur les menaces de manière à protéger leur réseau. Toutefois, ces outils ne sont efficaces que dans la mesure où ils voient les informations. La capacité à faire la part des choses dans l'abondance de Big Data depuis le réseau en temps réel est vitale pour identifier et atténuer les menaces actuelles et futures.

La Visibility Fabric de Gigamon offre une plateforme de services de sécurité totale et complexe. Il offre l'extensibilité tout en améliorant la résilience, en simplifiant la gestion et en permettant le déploiement des solutions les meilleures dans leur genre. Gigamon travaille avec des outils de sécurité pour augmenter leur champ de vision, améliorer leurs performances, soutenir la résilience, diminuer les temps de dépannage et accélérer la rentabilité des investissements. La Visibility Fabric de Gigamon offre la plateforme pour une visibilité de bout en bout associée à des renseignements sur le trafic qui sont nécessaires pour gérer efficacement les risques et faire face aux menaces dans cet environnement de menaces et de réseau en évolution constante.

À propos de Gigamon

Gigamon offre une Unified Visibility Fabric™ intelligent pour permettre la gestion de réseaux de plus en plus complexes. La technologie Gigamon donne aux architectes, responsables et opérateurs d'infrastructures une visibilité et un contrôle omniprésents du trafic dans des environnements à la fois physiques et virtuels sans incidence négative sur les performances ou la stabilité du réseau de production. Par le biais de technologies brevetées, d'une gestion centralisée et d'un portefeuille de nœuds de tissus à haute disponibilité et à haute densité, le trafic de réseau est délivré de manière intelligente aux systèmes de gestion, de suivi et de sécurité. Les solutions Gigamon sont déployées mondialement dans les entreprises, les centres de données et auprès des prestataires de services, ceci comprenant plus de la moitié des entreprises figurant sur la liste Fortune 100 et de nombreuses agences gouvernementales et fédérales.

Pour plus de détails sur la Visibility Fabric unifiée de Gigamon, merci de consulter le site : **www.gigamon.com**

FR - 3127 04/15

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