Solution de sécurité du data center - La gestion des menaces avec l'IPS NextGen Guide de conception—Dernière mise à jour : 24 avril , 2015

Nous créons des architectures à la mesure de vos challenges

À propos des auteurs

Tom Hogue

Tom Hogue, Responsable des solutions de sécurité, Security Business Group, Cisco

Tom Hogue est responsable des solutions de sécurité du data center chez Cisco. Il travaille depuis plus de 20 ans dans le domaine du développement de solutions intégrées chez Cisco après avoir occupé d'autres postes dans le secteur IT. Il a dirigé le développement de solutions de data center renommées telles que Flexpod, Vblock et Secure Multi-Tenancy, et pilote actuellement le développement du portefeuille de solutions de sécurité du data center. Il a également coécrit le guide de conception validée Cisco (CVD) de la solution de mise en cluster sur un seul site avec TrustSec.

Mike Storm

Mike Storm, Directeur de l'ingénierie technique, Security Business Group, Cisco Certification CCIE Security n° 13847

Expert de la sécurité globale chez Cisco Systems, Mike Storm est spécialisé dans la stratégie et les architectures concurrentielles. L'un de ses domaines de prédilection est la sécurité dans le data center. Il développe également des architectures axées sur une intégration étroite entre les services de sécurité nouvelle génération et les technologies de data center et de virtualisation. Mike a plus de 20 ans d'expérience dans les domaines des réseaux et de la cybersécurité. Il a notamment occupé des postes de consultant, de rédacteur technique et de conférencier dans ces domaines. Mike est l'auteur de plusieurs publications, dont le guide pratique de conception de solutions de sécurité du data center, et est le coauteur du guide de conception validée Cisco (CVD) sur la mise en cluster sur un seul site avec TrustSec.

Bart McGlothin

Bart McGlothin, Architecte de systèmes de sécurité, Security Business Group, Cisco

Bart McGlothin est architecte de solutions de sécurité chez Cisco et a plus de 15 ans d'expérience dans le domaine. Il représente également Cisco auprès du comité de standardisation des technologies pour le commerce de l'association américaine des commerçants, la NRF. Avant d'intégrer Cisco, Bart McGlothin était architecte réseau chez Safeway.

Matt Kaneko

Matt Kaneko, Architecte de systèmes de sécurité, Security Business Group, Cisco

Matt Kaneko est le responsable technique de l'équipe chargée des solutions de sécurité du data center. Pour créer des architectures, Matt et son équipe travaillent en étroite collaboration avec les équipes de marketing produits des diverses entités commerciales de l'entreprise et tiennent également compte des commentaires des clients. Auparavant, Matt a travaillé en tant que responsable marketing technique pour diverses gammes de produits de sécurité Cisco, notamment le pare-feu nouvelle génération Cisco ASA, le système de protection contre les intrusions (IPS) Cisco, Cisco AnyConnect et la gamme de produits de gestion associée.

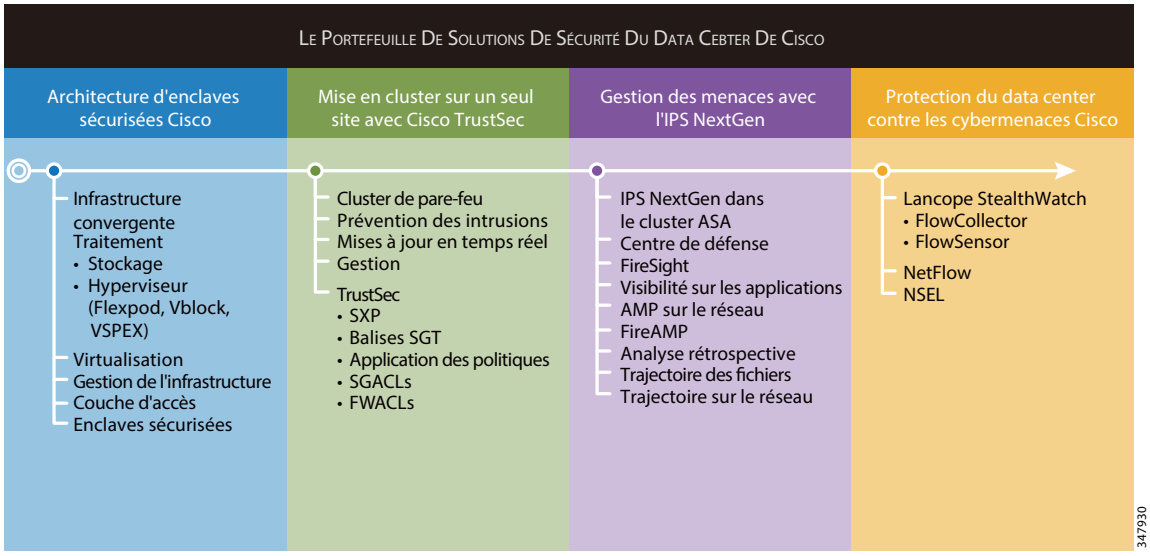
SOMMAIRE

Introduction

Objectif de ce document

Notre portefeuille de solutions de sécurité du data center comprend des services de conseils de conception et de mise en œuvre destinés aux entreprises qui souhaitent déployer des charges de travail physiques et virtualisées dans leur data center tout en garantissant la meilleure protection possible contre les risques pesant sur la sécurité des données. Vous trouverez dans ce document des conseils de conception en vue d'intégrer la solution de gestion des menaces avec le système de prévention des intrusions de nouvelle génération (IPS NextGen) dans une architecture de data center. Ce document complète les conseils de conception et de déploiement fournis pour les solutions associées, comme illustré dans la grille des solutions (voir la Figure 1 ci-dessous).

Figure 1 Le portefeuille de solutions de sécurité du data center de Cisco



Pour consulter des documents traitant de sujets non abordés dans ce document, rendez-vous sur le portail des solutions de sécurité du data center :
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-secure-data-center-portfolio/index.html

Siège social :
Cisco Systems., 170 West Tasman Drive, San Jose, CA 95134-1706 États-Unis

Public visé

Ce guide de conception s'adresse principalement aux architectes d'infrastructure de sécurité, aux concepteurs de systèmes, aux ingénieurs concepteurs de réseaux, aux ingénieurs système, aux consultants et aux spécialistes des services avancés. Il s'adresse également aux clients qui souhaitent comprendre comment déployer une architecture de sécurité robuste dans un data center capable de répondre aux menaces avancées, tout en conservant la flexibilité d'utiliser des charges de travail virtualisées et physiques, et d'exploiter des infrastructures classiques ou de migrer vers des modèles d'exploitation cloud. Il fait également référence à d'autres solutions complémentaires qui sont documentées dans des guides de conception et de déploiement distincts. La lecture de ce guide implique une maîtrise des concepts de base des protocoles IP, de qualité de service (QoS), de haute disponibilité et des technologies de sécurité. Elle implique également de posséder une bonne connaissance des exigences générales des systèmes et des architectures de réseau et de data center d'entreprise.

Présentation des solutions de sécurité du data center

Synthèse

Le portefeuille de solutions de sécurité du data center ne se composait au départ que d'une solution documentée dans un guide de conception visant à expliquer comment mettre en œuvre des pare-feu Cisco ASA dans le fabric du data center. En novembre 2013, le portefeuille s'est enrichi d'un ensemble complet de solutions documentées dans des guides de conception pour permettre l'adoption d'une approche modulaire de la sécurité. La solution de mise en cluster sur un seul site avec TrustSec a permis de regrouper des appliances ASA 5585-X pour favoriser l'évolutivité, et d'intrégrer TrustSec pour l'agrégation des politiques ainsi que des systèmes de prévention des intrusions pour la protection. Lorsque cette solution est combinée avec l'architecture de référence dite d'enclaves sécurisées et avec la solution de sécurité du data center contre les cyberattaques, l'ensemble forme un portefeuille de solutions de sécurité très puissantes que nous appelons « Portefeuille de solutions de sécurité du data center pour l'entreprise » et qui sera étoffé au fil du temps.

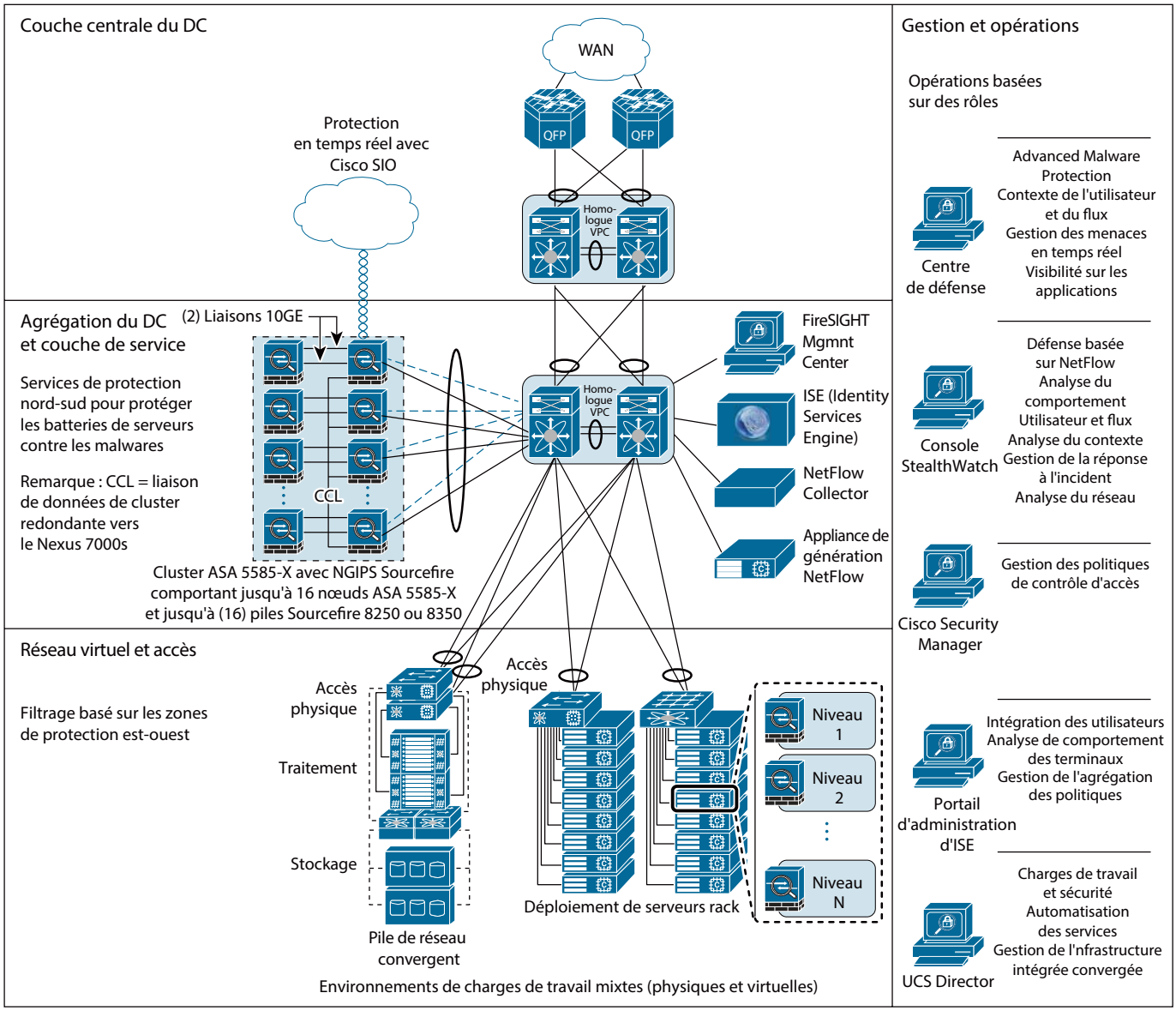
La prochaine solution à intégrer ce portefeuille est documentée dans la CVD intitulée « Gestion des menaces avec l'IPS NextGen ». Cette nouvelle CVD repose sur la solution de mise en cluster sur un seul site avec TrustSec. Elle explique comment intégrer le système de prévention des intrusions nouvelle génération FirePOWER, l'IPS NextGen, dans l'architecture et présente la gamme étendue de fonctionnalités de la solution. Dans le guide de conception, la sécurité n'est pas abordée du point de vue de l'entreprise, mais des cybercriminels. Nous allons examiner leur mode opératoire, que nous appelons « chaîne d'attaque ». En nous plaçant de l'autre côté de la barrière, il devient évident que les « acteurs de la cyberprotection » doivent développer de nouvelles fonctionnalités, puis les mettre en œuvre pour créer un système de gestion des menaces. Dans cette CVD, nous n'allons pas détailler les mesures de sécurité « fondamentales », par exemple s'assurer que les mots de passe par défaut ne sont pas utilisés. Nous vous invitons donc vivement à prendre des mesures de sécurité conformes à votre secteur d'activité et à les appliquer comme il convient. Cette CVD vise à vous présenter un nouvel ensemble de fonctionnalités et à vous expliquer comment intégrer la nouvelle plate-forme de prévention des intrusions nouvelle génération, l'IPS NextGen FirePOWER, dans le fabric.

Vue d'ensemble de la conception de la solution

La gestion des menaces avec l'IPS NextGen

La figure 2 présente le cadre architectural de la solution. Pour rappel, cette solution repose sur la solution de mise en cluster sur un seul site avec TrustSec pour la protection du data center. Elle doit donc être considérée comme un prérequis pour cette conception.

Figure 2 La gestion des menaces avec l'IPS NextGen



La solution de gestion des menaces avec l'IPS NextGen repose sur la solution de mise en cluster sur un seul site avec TrustSec qui tire parti de technologies de renforcement de la sécurité dans tout le data center. Dans la CVD associée, nous vous avions fourni les conseils de conception suivants :

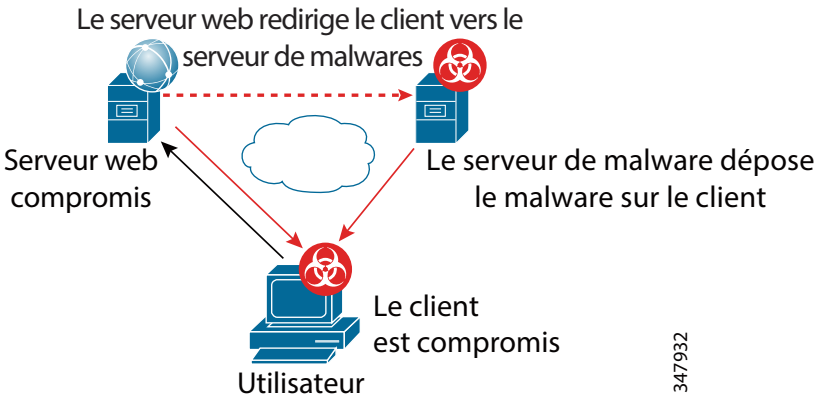
- Mettre en cluster les pare-feu ASA pour l'évolutivité
- Intégrer le fabric avec les canaux de port virtuel (vPC)
- Agréger des liaisons pour simplifier les opérations
- Mettre en œuvre des mécanismes de protection contre les intrusions et de visibilité sur les applications
- Permettre la mise à jour en temps réel des signatures
- Utiliser les balises SGT pour l'agrégation des politiques

Dans ce guide de conception, nous vous donnons des conseils pour étendre la solution de mise en cluster sur un seul site avec TrustSec via l'intégration de la plate-forme IPS NextGen FirePOWER dans l'architecture tant d'un point de vue physique que virtuel. L'appliance FirePOWER offre des fonctionnalités de protection qui vont bien au-delà de celles d'un système IPS classique Lorsque ces fonctionnalités sont associées à celles qui étaient incluses dans le portefeuille de solutions de sécurité du data center pour l'entreprise, il en résulte une solution globale de protection extrêmement efficace capable de faire face aux cyberattaques actuelles grâce à des workflows de gestion des menaces ultrapuissants.

Quelles cybermenaces pèsent sur le data center ?

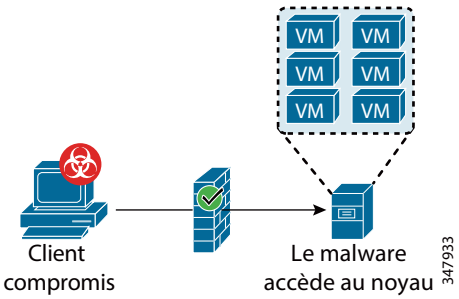
Un data center classique est l'endroit où les données les plus essentielles et les plus précieuses à l'entreprise résident. Il peut s'agir de la propriété intellectuelle, des coordonnées et des numéros de carte bancaire des clients, des informations financières et des comptes bancaires de l'entreprise, des informations sur les collaborateurs, etc. Si ces données sont précieuses pour l'entreprise, elles le sont également pour les cybercriminels quelles que soient leurs motivations : intérêt financier, espionnage ou autres. Il fait peu de doute que les data centers constituent une ressource essentielle à protéger. La plupart des entreprises segmentent plus ou moins leur réseau et appliquent des politiques de contrôle d'accès visant à n'autoriser l'accès au data center qu'aux utilisateurs qui en ont besoin. Malheureusement, cette approche repose sur certaines hypothèses obsolètes, ce qui nécessite de repenser la façon dont les data centers sont protégés. Nombre d'entreprises ont exclusivement recours à l'application de listes de contrôle d'accès. L'une des principales hypothèses est que l'utilisateur « autorisé » est vraiment celui qu'il dit être ou que l'utilisateur autorisé maîtrise l'appareil avec lequel il accède au data center. Pour un cybercriminel, l'un des moyens les plus simples de mettre un pied dans le réseau d'une entreprise consiste à installer un rootkit sur le terminal d'un utilisateur. Cette opération peut être facilement effectuée lorsqu'un utilisateur peu méfiant surfe sur un site web malveillant alors qu'il est chez lui et qu'il n'est pas connecté au réseau d'entreprise. (Voir la Figure 3.)

Figure 3 Les kits d'exploits



Une fois que l'utilisateur retourne au travail avec son appareil infecté, le malware peut usurper l'identité de l'utilisateur et accéder à l'ensemble des ressources du data center auxquelles il est autorisé à accéder. À ce stade, les listes de contrôle d'accès permettent au malware de traverser le réseau et de pénétrer dans le data center (voir Figure 4). Cette approche ne tient pas encore compte des vols d'informations d'identification et de la possibilité pour les cybercriminels d'accéder aux ressources des data centers avec une simple autorisation.

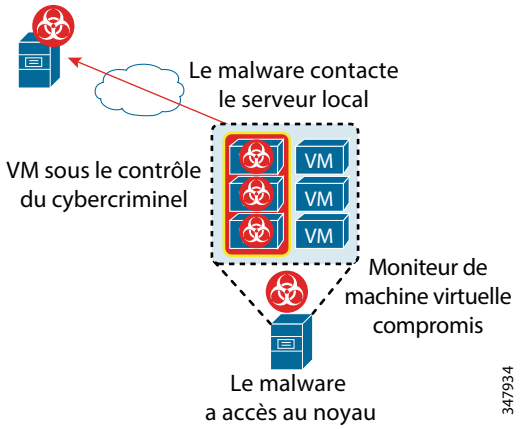
Figure 4 Un serveur compromis



Les rootkits basés sur une machine virtuelle

Lorsque le cybercriminel dispose d'un accès direct au data center, il essaie alors de compromettre les serveurs et les applications qu'ils hébergent. Des exploits relativement récents ciblent directement les data centers. Il s'agit de rootkits basés sur une machine virtuelle (VMBR), comme illustré à la Figure 5. Des chercheurs ont démontré la capacité de nuisance d'exploits VMBR tels que Blue Pill, Vitriol et SubVirt lors de conférences Black Hat. Que ces exploits soient utilisés ou non par les cybercriminels, la menace est réelle.

Figure 5 Un rootkit VMBR



La première question à se poser est : « Le contrôle d'accès est-il suffisamment robuste pour protéger les ressources du data center ? ». S'il ne fait aucun doute que les cyberattaques ciblent le data center, c'est la combinaison des modèles de sécurité existants et des nouvelles cyberattaques qui représente un nouveau risque réel pour les data centers.

Si les exemples présentés ci-dessus sont plutôt simplistes, les menaces qui pèsent sur le data center sont très complexes. La section suivante présente la chaîne d'attaque et un nouveau modèle de sécurité, et les sections qui suivent indiquent comment transposer ce nouveau modèle dans les sous-fonctions.

La chaîne d'attaque

Dans la section précédente, nous avons présenté de façon succincte le fonctionnement d'un rootkit, mais pour continuer à remettre en question les hypothèses que nous venons d'évoquer, il convient d'étudier plus attentivement les défis à relever. Il est primordial de savoir que les cyberattaques les plus fructueuses sont extrêmement ciblées. Les plus sophistiquées sont réalisées en plusieurs phases et obéissent à un mode opératoire précis. La Figure 6 présente la chaîne d'attaque du point de vue d'un cybercriminel.

Figure 6 La chaîne d'attaque

Dans un article. intitulé « Find, Track, Target, Engage, Assess », publié en juillet 2000 dans Air Force Magazine, John A. Tirpak avance l'hypothèse que le concept de *kill chain*, ou chaîne de frappe, a été mentionné pour la première fois par le général Ronald R. Fogleman, Chef d'état-major des forces aériennes américaines lors d'un discours prononcé en octobre 1996. Le général a en effet affirmé qu'« il sera possible de trouver, de corriger ou de suivre tout ce qui se déplace sur la surface de la terre ». De ces concepts est née la chaîne de frappe « Trouver, corriger, cibler, impliquer, évaluer ». Au fil du temps, plusieurs branches de l'armée ont modifié ce concept pour l'adapter à leur contexte. Ce document propose encore une autre version de la chaîne de frappe qui est plus adaptée à l'état d'esprit d'un développeur de logiciels (ou d'un cyberpirate). Notez que la chaîne d'attaque n'est pas liée à un calendrier, car certains cybercriminels peuvent travailler leurs cibles pendant plus d'un an pour éviter toute détection, alors que d'autres peuvent lancer une attaque en seulement quelques minutes. Nombre d'entreprises ont basé leurs mécanismes de défense sur la chaîne de frappe.

Repérer

Pour préparer une attaque, il est important de bien cerner l'environnement :

- Quels sont les ports ouverts ? Le rootkit devra-t-il fonctionner sur plusieurs ports ?
- Quels sont les systèmes d'exploitation identifiables ?
- Quel type de parade et de technique d'évasion le cybercriminel devra-t-il déployer ?
- Quelles sont les principaux mécanismes de défense mis en œuvre par l'entreprise ciblée ?
- Jusqu'où l'utilisation des mots de passe par défaut peut-elle mener le cybercriminel ?
- Est-il possible d'identifier un ensemble d'adresses e-mail d'utilisateurs auquel envoyer des messages d'hameçonnage ?

Malheureusement, les campagnes d'hameçonnage sont toujours très performantes, comme l'indique *le rapport sur les compromissions de données publié par Verizon en 2014.* Leur taux de réussite serait de 90 % pour seulement 10 e-mails envoyés à des utilisateurs.

Développer

Au terme de la phase de repérage, le cybercriminel commence à développer les fonctionnalités qui lui permettront de mener à bien son attaque. Il est important de noter que le mot *développer* ne signifie pas nécessairement écrire un tout nouveau malware. Un cybercriminel a à sa disposition un large éventail de malwares « prêts à l'emploi » parmi lesquels choisir ceux qui ne nécessitent aucune écriture de code. Même si cela est bien connu, il est à peine croyable que l'on puisse vendre un malware sous licence et le contrat d'assistance qui va avec. Si le cybercriminel souhaite créer un programme malveillant personnalisé en fonction de sa cible, il existe une grande quantité de code open source qu'il pourra modifier. Cela crée un processus incroyablement efficace pour la communauté des cybercriminels.

Tester

Doté des outils appropriés, le cybercriminel passe à l'étape de test et de validation. Il est très important qu'il puisse accéder aux ressources cibles sans être détecté. S'il est détecté trop tôt, il doit tout recommencer, car la cible déploiera une nouvelle parade. Le cybercriminel doit vérifier l'efficacité de ses techniques d'esquive. Son objectif est d'accéder au réseau, de rester non détecté et de prendre son temps pour atteindre son objectif.

Exécuter

Une fois la validation terminée, il est alors prêt à infiltrer les ressources de la cible. Il peut déposer un programme malveillant sur l'appareil d'un utilisateur ou accéder aux serveurs d'applications web, aux serveurs de messagerie et à tout autre appareil lui permettant de traverser le réseau. Une fois qu'il est infiltré, le cyberpirate cherche alors à établir une méthode d'accès secondaire au cas où sa cible principale aurait déployé une parade. Il s'agit d'une étape importante à retenir. Nous y reviendrons plus loin dans ce document.

Frapper

Maintenant que le cybercriminel a réussi à accéder au réseau cible, il est temps pour lui de mener à bien sa mission : extraire des données critiques, détruire des données, fabriquer des preuves, ou effectuer toute autre action qui va lui permettre d'atteindre son objectif. Le cybercriminel recherche également des emplacements pour y cacher son malware en vue de mener d'autres cyberattaques.

Les indicateurs de compromission

Dans de nombreux cas, il peut s'écouler plus d'un an entre les phases d'exécution et de frappe. Beaucoup de cybercriminels utilisent une technique d'affût pour rentabiliser leur attaque au maximum. Ces techniques d'affût génèrent très peu d'*indicateurs de compromission*, si tant est qu'il y en ait. Comme cette approche produit bien peu d'indications de compromission comparé aux milliers d'alertes générées par les systèmes d'attaque existants, il n'est pas étonnant que ces types d'attaque soient extrêmement difficiles à détecter. Avant que les indicateurs de compromission ne soient identifiés, les entreprises se fiaient aux indicateurs d'une attaque. Les systèmes classiques de prévention des intrusions signalaient une attaque en déclenchant des alertes lorsqu'une correspondance avec une signature à un point dans le temps donné était établie. Malheureusement, les systèmes IPS généraient un grand nombre de faux positifs. Les flux de trafic correspondant aux signatures étaient en fait inoffensifs. Les opérateurs ont ensuite identifié des signatures qui correspondaient au trafic inoffensif d'hôtes particuliers afin que ces flux de trafic ne génèrent pas d'alertes. Les alertes restantes étaient traitées comme des indicateurs d'attaques tels qu'ils étaient identifiés par le système IPS. Malheureusement, ces fausses alertes étaient si nombreuses que les véritables alertes étaient souvent noyées dans la masse et qu'elles passaient facilement inaperçues. Lorsque l'entreprise avait identifié une indication crédible de compromission, elle devait alors effectuer une analyse fastidieuse et extrêmement difficile pour tenter de savoir :

- Quelle méthode a été utilisée et quel était le point d'entrée ?
- Quels systèmes ont été touchés ?
- Quels ont été les effets de l'attaque ?
- Comment peut-on stopper l'attaque et en identifier les causes premières ?
- Comment procéder à une récupération ?
- Comment empêcher que cela se reproduise ?

Les équipes chargées de la cybersécurité avaient besoin d'une nouvelle approche basée sur un ensemble plus large de données précises afin de produire des indicateurs de compromission fiables. Pour analyser précisément ce qui s'était passé, elles avaient notamment besoin d'apporter des réponses à des questions telles que les suivantes :

- Quelle est la nature de l'attaque ? Par exemple, était-elle d'un type ou d'une catégorie connus ?
- Quelles sont ses caractéristiques ? Par exemple, comment est-elle/a-t-elle été exécutée ? Qu'est-ce qui a pu changer sur le terminal cible, etc. ?

- D'où provenait l'attaque ?
- Comment a-t-elle été déterminée ?
- Quel est le terminal cible ? Son système d'exploitation ?
- La cible est-elle vulnérable à cette attaque ?
- Ce terminal a-t-il été compromis par cette attaque ou par d'autres attaques, maintenant ou dans le passé ?
- Quelles autres machines ce terminal a-t-il contactées ?
- Quelle est l'application ciblée (par exemple, cliente ou web) ?
- La cible est-elle susceptible d'être impactée par cet incident ?
- S'agit-il d'un nouveau type d'incident ou a-t-il été introduit via une source externe, par exemple un appareil connecté dans le cadre du BYOD ?
- L'hôte attaquant réside-t-il actuellement sur le réseau ou hors de celui-ci ?
- Quelle est/était la principale cause ?
- Le système peut-il identifier immédiatement le nombre d'hôtes ou d'appareils connectés au réseau susceptibles d'être vulnérables à cette attaque ?
- Si cette attaque est bloquée, comment le système peut-il déterminer s'il s'agit d'un faux positif ou d'un vrai positif ?

Un exemple d'indicateur de compromission fort serait une application Java commençant à installer et à exécuter des applications, ce qui ne doit jamais se produire. Malheureusement, Java est un vecteur d'attaque courant qui reste prisé par bon nombre de cybercriminels. Ce type d'attaque peut facilement être conforme à des listes de contrôle d'accès. Sa détection peut également facilement échapper à un système IPS classique, car la signature des fichiers ne déclenche pas d'alerte. Pour que les indicateurs de compromission soient efficaces, les incidents doivent être mis en corrélation avec :

- L'activité des malwares
- La détection des intrusions
- Les connexions réseau
- La trajectoire des fichiers sur le réseau
- La trajectoire des appareils
- Le flux des appareils sur le réseau, notamment, les déplacements latéraux, les relations parent-enfant ou le contexte

L'objectif est de mettre en corrélation tous les éléments ci-dessus avec le contexte (réseau, terminaux, applications et utilisateurs). Les données obtenues offrent la capacité unique de fournir des indications de compromission à l'échelle du réseau qui sont suffisamment précises pour être fiables et immédiatement exploitables.

L'évolution et le développement des menaces

Les réseaux étendus modernes et leurs composants évoluent constamment. De nouveaux vecteurs d'attaque émergent : terminaux mobiles, applications web et mobiles, hyperviseurs, réseaux sociaux, navigateurs web et ordinateurs embarqués, sans parler de la multiplication du nombre d'appareils connectés liés à l'Internet of Everything dont nous ne mesurons pas encore la portée.

Les utilisateurs accèdent à n'importe quelle application sur n'importe quel appareil, sur le réseau ou en dehors, et sur plusieurs clouds. C'est le challenge que pose cette *interconnectivité généralisée*. Et si ces évolutions favorisent de meilleures communications, elles ont également augmenté les points d'entrée et les méthodes utilisés par les hackers. Malheureusement, la plupart des entreprises n'ont pas modifié leur approche de la sécurité en conséquence. La majorité d'entre elles sécurisent leurs réseaux étendus avec des technologies disparates incapables de fonctionner ensemble. Et certaines comptent également trop sur leurs fournisseurs cloud et leurs hébergeurs pour protéger l'infrastructure Internet. Dans ce nouveau paysage, les administrateurs de la sécurité ne disposent généralement pas d'une visibilité ou d'un contrôle suffisants sur les appareils et les applications accédant au réseau de l'entreprise, et n'ont pas les moyens de s'adapter rapidement aux nouvelles menaces.

Confrontés à la fois aux attaques avancées et à un accès généralisé à l'infrastructure, les professionnels de la sécurité sont confrontés à trois défis majeurs :

1. Comment assurer la sécurité et la conformité de notre infrastructure face aux nouveaux modèles commerciaux et aux vecteurs d'attaque alors que notre infrastructure IT continue d'évoluer ?

   Les entreprises s'ouvrant au cloud, à la virtualisation ou à la mobilité en raison des bénéfices que ces technologies représentent en matière de productivité, d'agilité et d'efficacité doivent adapter leur infrastructure de sécurité en conséquence.

2. Comment renforcer la continuité de notre protection contre les nouveaux vecteurs d'attaque et les menaces toujours plus sophistiquées ?

   Les cyberpirates ne font pas de distinction ; ils s'attaquent à tous les maillons faibles de la chaîne. Ils mènent leurs attaques sans relâche en utilisant souvent des outils développés spécialement pour contourner l'infrastructure de sécurité de leur cible. Ils déploient d'importants efforts pour ne pas être détectés grâce à des technologies et à des méthodes qui ne laissent quasiment aucune trace de compromission.

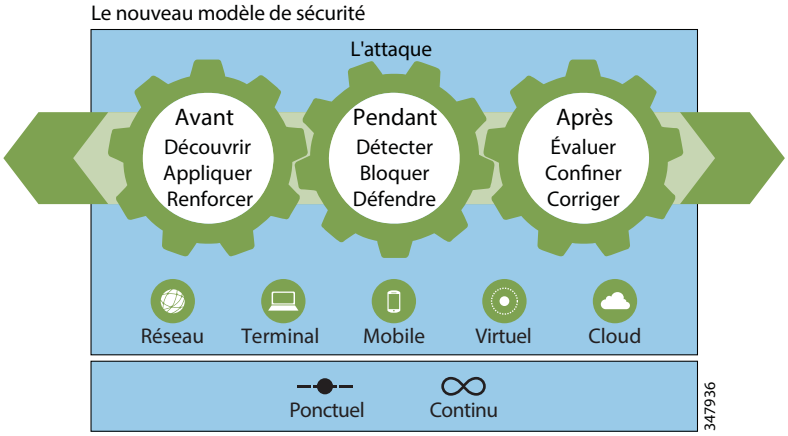
3. Comment répondre aux deux premières questions, tout en réduisant la complexité et la fragmentation des solutions de sécurité ?

   Les entreprises ne peuvent pas se permettre de laisser des failles qui sont actuellement exploitées par des hackers dont les techniques sont perfectionnées. Par ailleurs, ce n'est pas en compliquant encore la situation avec des solutions de sécurité disparates non intégrées qu'elles obtiendront le niveau de protection nécessaire.

Un modèle de sécurité qui tire parti des mécanismes de défense intégrés

Comme nous l'avons évoqué, de nouveaux outils et technologies sont nécessaires pour faire face aux attaques qui affectent non seulement le data center, mais aussi l'entreprise dans son ensemble. Il faut pour cela utiliser un modèle qui réduit la complexité et qui protège les ressources de l'entreprise en permanence, tout en tenant compte des changements dans l'entreprise, la généralisation de l'interconnectivité notamment. Le système de sécurité doit être intégré directement dans le fabric de réseau pour optimiser son efficacité et ses fonctionnalités, tout en minimisant les risques normalement associés à l'ajout de contrôles de sécurité disparates et insensibles au réseau. Pour concevoir un tel système, un nouveau modèle est nécessaire afin de garantir une intégration correcte, en particulier dans le data center où la marge d'erreur est vraiment faible. Ce nouveau modèle constitue une référence utile lors du développement d'une solution de sécurité complète pour tout type de réseau. Le nouveau modèle tient compte d'un élément clé, à savoir le *déroulement de l'attaque* qui permet d'identifier chacun des mécanismes et des processus nécessaires pour assurer une protection complète. (Voir la Figure 7.)

Figure 7 Intégrer les mécanismes de défense en fonction du déroulement de l'attaque



Ce modèle permet de faire face aux menaces en tenant compte des mesures à prendre avant, pendant et après une attaque, ainsi que du large éventail de vecteurs d'attaque tels que les terminaux, les appareils mobiles, les ressources du data center, les machines virtuelles et même ceux circulant dans le cloud. En matière de protection, la plupart des solutions ont tendance à apporter une réponse ponctuelle, alors qu'il est important de la considérer comme un cycle continu.

Avant l'attaque

Parce que les cybercriminels ont une approche contextuelle, la sécurité doit être contextuelle. Les entreprises doivent désormais lutter contre des agresseurs qui possèdent plus d'informations sur l'infrastructure que les acteurs de la protection eux-mêmes. Pour se protéger avant qu'une attaque ne se produise, les entreprises doivent avoir une visibilité totale sur leur environnement, notamment sur les hôtes physiques et virtuels, les systèmes d'exploitation, les applications, les services, les protocoles, les utilisateurs, le contenu et le comportement du réseau, de manière à disposer d'un plus grand nombre d'informations que les cybercriminels. Les équipes chargées de la sécurité doivent comprendre les risques auxquels leur infrastructure est exposée en fonction de sa valeur en tant que cible, de ce qui pourrait légitimer une attaque et de l'historique. Si elles ne savent pas ce qu'elles doivent protéger, elles ne seront pas en mesure de mettre en œuvre les technologies de sécurité adaptées. La visibilité doit couvrir l'ensemble du réseau, c'est-à-dire les terminaux, les passerelles web et de messagerie, les environnements virtuels et les terminaux mobiles ainsi que le data center. Un système d'alertes doit par ailleurs permettre aux équipes chargées de la protection de prendre les bonnes décisions.

Pendant l'attaque

Certaines attaques continues et certaines menaces combinées ne sont pas ponctuelles. Elles sont en permanence actives et exigent des mesures de sécurité permanentes. Les technologies de sécurité classiques sont capables d'évaluer une attaque à un moment précis seulement, sur la base d'un seul point de donnée de l'attaque. Cette approche n'est pas à la hauteur des attaques avancées.

L'infrastructure de sécurité doit pouvoir prendre en compte le contexte et être capable de regrouper et de mettre en corrélation des données sur l'ensemble du réseau étendu, ainsi que d'exploiter l'historique des attaques et les informations de veille globales sur les menaces. Elle sera ainsi en mesure de fournir du contexte et de distinguer les menaces actives, l'exfiltration de données et les opérations de reconnaissance des simples activités d'arrière-plan. Ainsi, la sécurité n'intervient plus ponctuellement, mais consiste à analyser des données et à prendre des décisions en permanence. Si un fichier passe entre les mailles du filet et s'avère malveillant par la suite, les entreprises ont les moyens d'agir. Grâce à ces informations en temps réel, les professionnels de la sécurité peuvent automatiser intelligemment l'application de politiques de sécurité.

Après l'attaque

Pour couvrir tous les stades de l'attaque, les entreprises ont besoin de mesures de sécurité rétroactives. Leur mise en place est un challenge impliquant le Big Data et peu d'acteurs de la sécurité sont à la hauteur. Une infrastructure collectant et analysant continuellement les données à des fins de sécurité adaptative permet aux équipes chargées de la protection d'identifier les indicateurs de compromission, de détecter les programmes malveillants capables de changer de comportement pour éviter la détection, puis de remédier au problème, le tout grâce à des processus automatisés.

Des attaques auparavant indétectables pendant des semaines voire des mois peuvent ainsi être rapidement identifiées, délimitées, endiguées et éliminées. Ce modèle de sécurité axé sur les attaques assure aux entreprises une protection permanente et en temps réel à tous les stades de l'attaque, contre tous les vecteurs d'attaque.

Les fonctionnalités que doit proposer un système de gestion des menaces

Le modèle basé sur le déroulement de l'attaque que nous venons d'évoquer nous permet de savoir comment faire face aux menaces et de créer un cadre de fonctionnalités grâce auquel vous pourrez démarrer la mise en œuvre des contrôles de sécurité. Par exemple, dans la publication 800-53 intitulée « *Security and Privacy Controls for Federal Information Systems and Organizations* », le NIST indique que « les entreprises peuvent envisager de définir un ensemble de fonctionnalités de sécurité en amont du processus de sélection des contrôles de sécurité ».

Il y définit également le concept de *fonctionnalité de sécurité* comme un « élément qui considère que la protection des informations traitées, stockées ou transmises par des systèmes d'information découle rarement d'une seule mesure de sécurité ou contre-mesure (c.-à-d. d'un contrôle de sécurité) ». Chaque entreprise doit s'efforcer d'être en conformité avec les standards en vigueur dans son secteur d'activité. Bien que la conformité à proprement parler ne soit pas abordée dans ce document, le concept de *fonctionnalités* est au cœur de tout système de gestion des menaces et de ce document. Dans le Tableau 1, les fonctionnalités d'un système de gestion des menaces et leur description sont mises en lien avec les différents stades de l'attaque et avec les produits associés. Certains produits couvrant plusieurs fonctionnalités, il n'y a donc pas toujours de correspondance parfaite.

Tableau 1 Les fonctionnalités que doit proposer un système de gestion des menaces

Fonctionnalités	Description	Avant	Pendant	Après	Produits
Confinement et élimination des menaces	Inspection et analyse des menaces sur la base des fichiers, paquets et flux	Agents de protection des terminaux, protection de flux sur le réseau	Analyse des terminaux dans le cloud, analyse des fichiers sur le réseau, analyse des flux sur le réseau, analyse basée sur les signatures, analyse en sandbox	Analyse des connexions et des flux, et élimination	Sourcefire FireSIGHT, protection contre les intrusions, AMP (Advanced Malware Protection) sur le réseau, AMP pour la messagerie, AMP CWS, FireAMP pour utilisateur et mobile
Contrôle d'accès et segmentation	Politiques de contrôle d'accès, segmentation, séparation sécurisée	Affectations de terminaux à des groupes, zones de sécurité, accès des utilisateurs aux ressources régi par des politiques	Application au niveau du fabric, application de politiques relatives aux pare-feu, standardisation du trafic et conformité au protocole	Application des politiques et consignation	ASA 5585-X, SGT, SGACL, SXP, et fabric de commutation compatible TrustSec ou fabric ACI avec ASAv
Gestion des identités	Identité des utilisateurs et comportement d'accès, contexte utilisateur basé sur le réseau	Association des utilisateurs avec des groupes, des ressources et des emplacements d'accès acceptables	Analyse contextuelle des utilisateurs	Analyse de l'accès utilisateur et de l'origine des menaces, et élimination	Active Directory, Cisco ISE (Identity Services Engine), Sourcefire FireSIGHT

Tableau 1 Les fonctionnalités que doit proposer un système de gestion des menaces (suite)

Fonctionnalités	Description	Avant	Pendant	Après	Produits
Contrôle et visibilité sur les applications	Contrôle et analyse de la trajectoire, analyse de la trajectoire des fichiers circulant sur le réseau, mise en quarantaine d'applications, prévention des pertes de données	Politiques de limitation et de contrôle des accès aux applications internes et externes	Application des politiques de contrôle des applications, inspection des données sensibles	Visibilité sur toutes les applications utilisées et exécutées sur le réseau	Contrôle d'accès Sourcefire, NGFW Sourcefire
Gestion des journaux et de la traçabilité	Analyse des menaces et conformité	Configuration correcte des rapports du système de gestion des menaces	Consignation hors bande active	Accès immédiat via la plate-forme de gestion des menaces Consolidation des journaux dans le référentiel central pour analyse et mise en conformité ultérieures	FireSIGHT Management Center pour les journaux à court terme, Lancope StealthWatch pour les journaux d'analyse NetFlow à plus long terme, SIEM pour la mise en conformité de la gestion des incidents (SIEM non couvert dans ce projet)

Le confinement et l'élimination des menaces

Il est nécessaire de pouvoir identifier les cybermenaces et de les éliminer aussi rapidement que possible. Il ne s'agit pas d'une fonction ponctuelle, mais d'une fonction continue qui utilise l'analyse rétrospective. Ainsi, si un malware n'est pas initialement identifié, le système peut toujours le localiser plus tard et l'éliminer.

Le contrôle d'accès et la segmentation

Les politiques de contrôle d'accès et leur mise en application ont été le socle de la protection du réseau et vont continuer à en être un élément fondamental. La segmentation a également été un élément essentiel pour séparer le trafic, mais les entreprises n'ont pas su tirer pleinement parti du potentiel de cette technique. Ces deux fonctionnalités étant généralement considérées comme distinctes, elles sont associées à des contrôles séparés dans la plupart voire dans tous les standards de conformité. Elles sont combinées ici en raison de leur interconnexion lors de la conception et du déploiement du réseau. Dans chaque réseau où une stratégie de segmentation appropriée est déployée, des politiques de contrôle d'accès doivent également être déployées pour définir leur domaine de sécurité. Les domaines de sécurité de grande envergure ont tendance à exposer les entreprises à des risques significatifs en cas d'atteinte à l'intégrité des données. Les nouvelles techniques de segmentation disponibles permettent de réduire la taille de ces domaines de sécurité et de faciliter leur gestion.

La gestion de l'identité

Toutes les entreprises utilisent un mécanisme ou un autre de gestion des identifications et des autorisations, comme Active Directory pour l'authentification des utilisateurs. Malheureusement, certaines n'ont pas déployé de fonctionnalité leur permettant d'évaluer le niveau de sécurité de l'utilisateur lors de l'authentification, et d'affecter ce dernier à la politique de sécurité appropriée en fonction de son terminal, de son emplacement ou d'autres critères importants. Il est également essentiel de pouvoir associer le contexte de l'utilisateur aux flux de trafic, à l'analyse de fichiers, aux connexions au réseau et à toute autre activité se produisant sur le réseau de manière à bénéficier d'une fonctionnalité robuste de gestion des menaces.

La visibilité sur les applications

La visibilité sur les applications hébergées sur l'ensemble du réseau est une fonctionnalité essentielle dont chaque entreprise devrait disposer dans son arsenal de lutte contre les cyberattaques. Les applications restent un vecteur d'attaque principal. Il est donc important de pouvoir analyser leurs comportements anormaux quand elles accèdent aux ressources de data center et à leurs flux de communication.

La gestion des journaux et de la traçabilité

La possibilité de générer des journaux détaillés sur tous les aspects de l'activité du réseau et des terminaux reste essentielle. La traçabilité va bien au-delà du simple horodatage des alertes. Il s'agit également de déterminer la trajectoire d'un fichier lorsque le malware transite par le réseau. L'entreprise doit être en mesure de réaliser une enquête approfondie en cas de découverte d'une menace.

Mise en correspondance des fonctionnalités avec les contrôles du NIST

Bien que la mise en correspondance des contrôles de conformité ne soit pas abordée dans ce document, une brève discussion s'impose par souci d'exhaustivité. Un examen rapide de l'article SP 800-53 du NIST et de la liste des 20 contrôles de sécurité essentiels dressée par le SANS Institute permet d'établir une correspondance entre les fonctionnalités que nous venons d'évoquer et les contrôles présentés dans ces deux documents. Comme l'indique le Tableau 2, les contrôles ne correspondent pas tous, mais la plupart de ceux ayant trait à la cybersécurité sont couverts.

Tableau 2 Mise en correspondance des fonctionnalités de gestion des menaces avec les contrôles

	Confinement des attaques	Contrôle d'accès et segmentation	Gestion de l'identité	Gestion d'applications	Journaux et traçabilité
Fonctionnalité	Inspection et analyse des menaces sur la base des fichiers, paquets et flux	Contrôle d'accès et segmentation	Identité des utilisateurs et comportement d'accès, contexte utilisateur basé sur le réseau	Contrôle et visibilité sur les applications	Analyse des menaces et conformité
Contrôles appropriés selon l'institut NIST	Réponse aux incidents, maintenance, protection des données, évaluation des risques, intégrité des systèmes et des informations	Contrôle d'accès, protection des systèmes et des communications	Contrôle d'accès	Intégrité des systèmes et des informations, contrôle d'accès	Audit et responsabilité
Les 20 contrôles de sécurité essentiels selon le SANS Institute	Évaluation et élimination continues des vulnérabilités, protection contre les programmes malveillants, protection des données	Inventaire des appareils autorisés et non autorisés, protection des frontières, accès limité aux données dont les utilisateurs ont besoin, ingénierie réseau sécurisée	Accès limité aux données dont les utilisateurs ont besoin, ingénierie réseau sécurisée	Inventaire des logiciels autorisés et non autorisés, ingénierie réseau sécurisée	Maintenance, surveillance et analyse des journaux d'audit

Les impératifs de la stratégie de mise en œuvre des mécanismes de protection intégrés

Pour que la stratégie de protection « avant, pendant et après une attaque » fonctionne sur tous les vecteurs d'attaque et pour assurer une riposte précise, continue et en temps réel, certains impératifs doivent être respectés. La stratégie doit être :

Orientée sur la visibilité

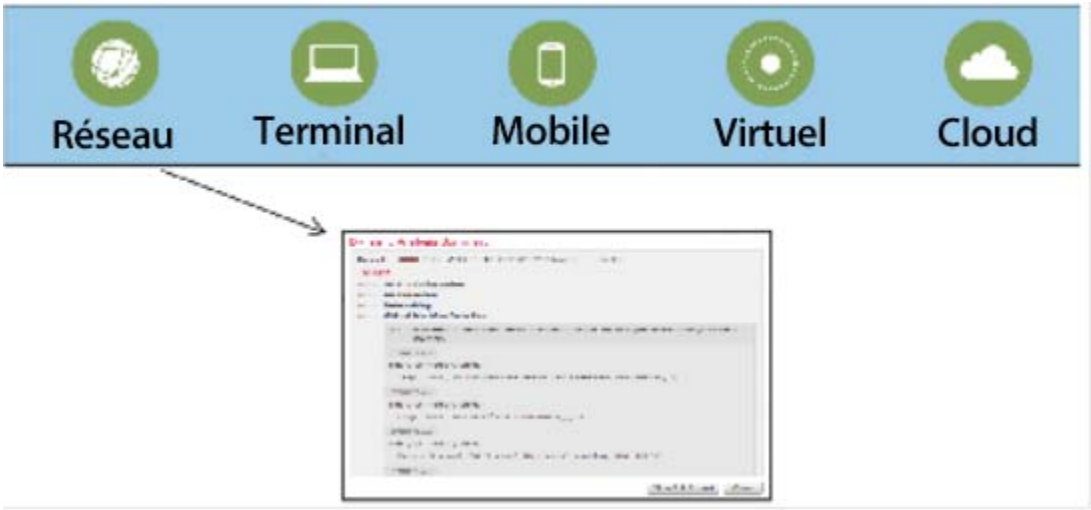
Afin d'être efficaces, les équipes chargées de la sécurité doivent être en mesure d'identifier avec précision les incidents qui se sont déjà produits et ceux en train de se produire. Cela nécessite de connaître l'ampleur des vecteurs d'attaque ainsi que l'étendue de chaque vecteur. Cela consiste à avoir accès aux données de tous les vecteurs d'attaque potentiels sur l'ensemble du fabric de réseau, des terminaux, des passerelles web et de messagerie, des terminaux mobiles, des environnements virtuels et du cloud pour connaître les environnements et les menaces.

Capable de mesurer l'étendue

L'objectif est de mettre ces informations en corrélation, d'utiliser les données de veille, de mieux comprendre le contexte, de prendre des décisions plus éclairées et de mettre en place des mesures de manière manuelle ou automatique. FireSIGHT est la technologie à la base de cette surveillance contextuelle complète. Elle constitue le socle technologique de FireSIGHT Management Center.

La Figure 8 montre l'ampleur requise de la solution ainsi qu'un exemple de « résumé d'analyse » qui explore en profondeur « tout ce qui s'est passé » sur chaque vecteur suite à un ou plusieurs incidents dans l'ampleur des vecteurs d'attaque. Ce résumé d'analyse permet à l'équipe chargée de la sécurité d'avoir une vue en profondeur de la situation et d'atténuer l'impact de certains éléments du processus d'attaque.

Figure 8 Exemple d'ampleur et d'étendue de tout ce qui s'est passé



Axée sur les menaces

Les réseaux étendus actuels offrent aux employés un accès où qu'ils soient, où que se trouvent les données et leur point d'accès. En dépit des efforts mis en œuvre, il est extrêmement difficile pour les personnes impliquées de suivre en permanence l'évolution des vecteurs d'attaque, ce qui représente une opportunité pour les cybercriminels. Ces derniers gagnent leur vie en exploitant les failles dans le système. Les politiques et les contrôles sont nécessaires pour réduire la surface exposée aux attaques, mais ils ne sont pas suffisants. Par conséquent, les technologies doivent également être spécialisées dans la détection, la compréhension et le blocage des attaques. Une approche axée sur la menace doit se placer du point de vue de l'attaquant, se servir de la visibilité et du contexte pour comprendre les événements et s'adapter aux changements de l'environnement, puis faire évoluer les protections pour prendre des mesures et stopper les attaques. Pour plus d'efficacité contre les programmes malveillants et les attaques de type « zero-day » avancés, ce processus continu doit bénéficier d'analyses permanentes et d'informations de sécurité adaptative en temps réel issues du réseau local et du cloud, et partagées avec tous les produits.

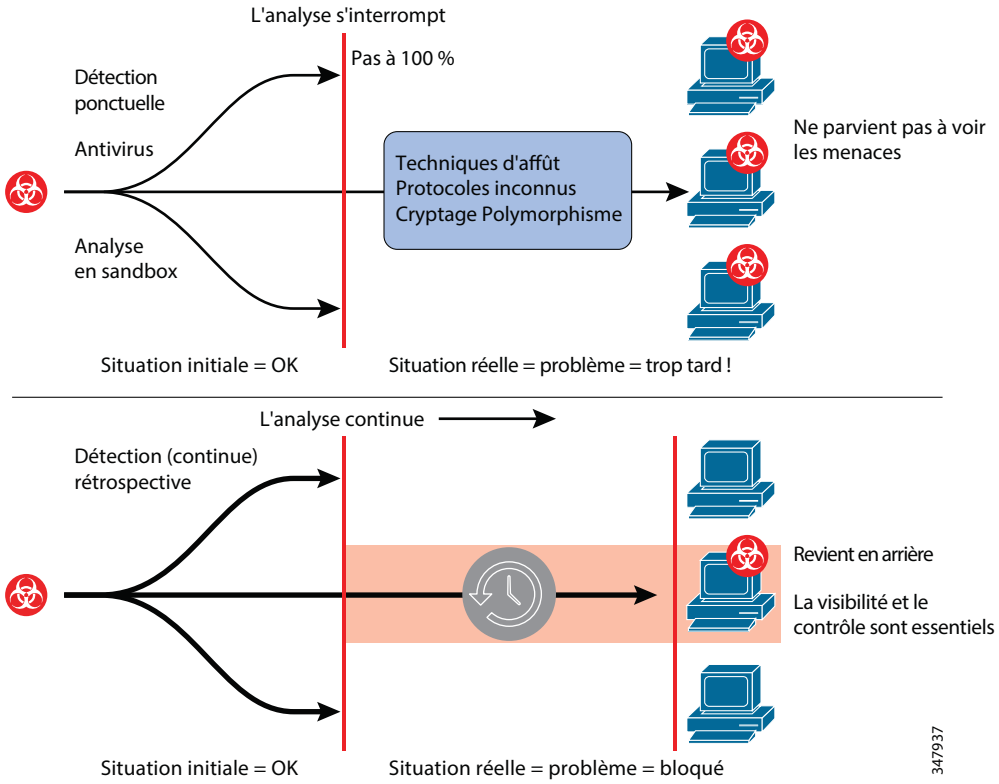
Les technologies de gestion des menaces

La sécurité rétrospective - Voir au-delà de l'horizon de l'événement

La sécurité rétrospective est une fonction exclusive de la solution de sécurité Cisco, fondamentale pour combattre les attaques avancées et les malwares modernes. Elle repose sur une fonctionnalité active en permanence qui fait appel au traitement analytique du Big Data pour collecter les données et les informations relatives aux événements survenus sur le réseau étendu en vue d'un suivi et d'une analyse en continu, pour envoyer des alertes et éliminer les éléments tels que les fichiers malveillants considérés au départ comme sûrs. Si un fichier passe au travers des systèmes de détection et est considéré comme inoffensif ou inconnu, mais est ultérieurement identifié comme malveillant, il peut faire l'objet d'une identification rétrospective qui permet de connaître l'envergure de l'attaque et de la confiner. Il est ainsi possible de revenir en arrière pour éliminer automatiquement les programmes malveillants. Avant cette fonctionnalité, il n'y avait aucun moyen de suivre une attaque au-delà de l'horizon de l'événement (par exemple, le « point de non-retour » pour le suivi des fichiers), c'est-à-dire le moment où le fichier arrive sur le réseau avec une « bonne » réputation, puis se dissimule et s'ancre immédiatement dans le réseau en vue d'agir plus tard.

La Figure 9 montre un exemple d'analyse rétrospective au-delà de l'horizon de l'événement. Elle compare également la détection ponctuelle à l'analyse continue rétrospective au moyen de quelques solutions ou techniques courantes de protection contre les programmes malveillants, telles qu'un antivirus, un système de prévention des intrusions et le sandboxing, qui sont considérées comme les éléments clés d'un système de gestion des menaces. Cette fonctionnalité revêt encore plus d'importance face aux attaques modernes susceptibles d'être « sensibles au sandbox ». La partie supérieure de la Figure 9 illustre les manquements des mécanismes de détection ponctuelle standard sans analyse rétrospective. La partie inférieure ajoute une analyse permanente à la « situation initiale » ponctuelle, de manière à montrer pourquoi l'analyse rétrospective est requise pour intercepter les programmes malveillants modernes et se protéger contre les attaques avancées. La partie inférieure montre également pourquoi la visibilité sur la cible est primordiale pour comprendre la façon dont le système de gestion des attaques peut révéler l'« envergure » exacte de la menace, au-delà de l'horizon de l'événement, et appliquer avec précision des mesures de prévention dynamique des attaques ultérieures.

Figure 9 Horizon de l'événement - Comparaison entre détection ponctuelle et analyse continue



L'analyse de la trajectoire : la technologie au cœur de l'analyse rétrospective

L'analyse de la trajectoire est une technologie exclusive de Cisco qui empêche à la solution de sécurité de perdre de vue les programmes malveillants au-delà de l'horizon de l'événement. Elle représente une composante essentielle du modèle de sécurité axé sur les événements ou sur les menaces, qui devrait avoir sa place dans tout data center moderne. En plus de la visibilité renforcée qu'elle procure, l'analyse de la trajectoire permet également à l'équipe chargée de la sécurité de déterminer l'envergure d'une attaque lorsqu'elle se produit, et de suivre les fichiers malveillants ou suspects sur l'ensemble du réseau et au niveau du système ou des terminaux. La fonctionnalité d'analyse de la trajectoire est étendue à l'ensemble de la gamme de solutions AMP (Advanced Malware Protection).

L'analyse de la trajectoire revient à disposer d'un enregistreur de vol réseau pour les programmes malveillants, consignant toutes leurs activités et leurs déplacements. Les malwares actuels sont dynamiques et peuvent donc s'introduire sur un réseau ou un terminal par le biais de différents vecteurs. Une fois exécutés sur la cible prévue, ils lancent généralement un certain nombre d'activités malveillantes et/ou apparemment anodines, y compris le téléchargement de programmes malveillants supplémentaires. En tirant parti de la puissance du traitement analytique du Big Data, la solution capture et crée une carte visuelle de ces activités de fichiers, offrant ainsi une visibilité sur l'ensemble de l'activité au niveau du réseau, des terminaux et du système. Les équipes chargées de la sécurité peuvent alors localiser rapidement le point d'entrée des programmes malveillants ainsi que suivre leur propagation et leur comportement. Cela procure une visibilité inédite sur l'activité des attaques de programmes malveillants et permet ainsi d'établir le lien entre la détection, l'élimination et le contrôle d'un programme malveillant. C'est un facteur clé de la sécurité rétrospective que seul Cisco est à même de proposer.

L'analyse de la trajectoire des fichiers et des équipements connectés au réseau

Les équipes chargées de la sécurité ont du mal à appréhender l'impact, le contexte et le mode de propagation des programmes malveillants sur le réseau et les terminaux. Il est vraiment essentiel de savoir si le programme malveillant détecté est un élément isolé ou si plusieurs systèmes sont touchés. L'analyse de la trajectoire des fichiers offre la possibilité de suivre les programmes malveillants sur le réseau à l'aide des appliances FirePOWER ou des connecteurs FireAMP existants. Elle permet ainsi de disposer d'informations détaillées sur le point d'entrée, la propagation, les protocoles utilisés ainsi que sur les utilisateurs ou terminaux impliqués (voir la Figure 10 et la Figure 11).

La fonctionnalité d'analyse de la trajectoire des fichiers réseau examine l'ensemble de l'environnement de l'entreprise et apporte des réponses aux questions suivantes :

- Quels systèmes ont été infectés ?
- Qui a été infecté en premier (« patient 0 ») et à quel moment ?
- Quel était le point d'entrée ?
- Quand cela s'est-il produit ?
- Quels ont été les autres éléments introduits ?

Figure 10 Analyse de la trajectoire d'un fichier sur le réseau

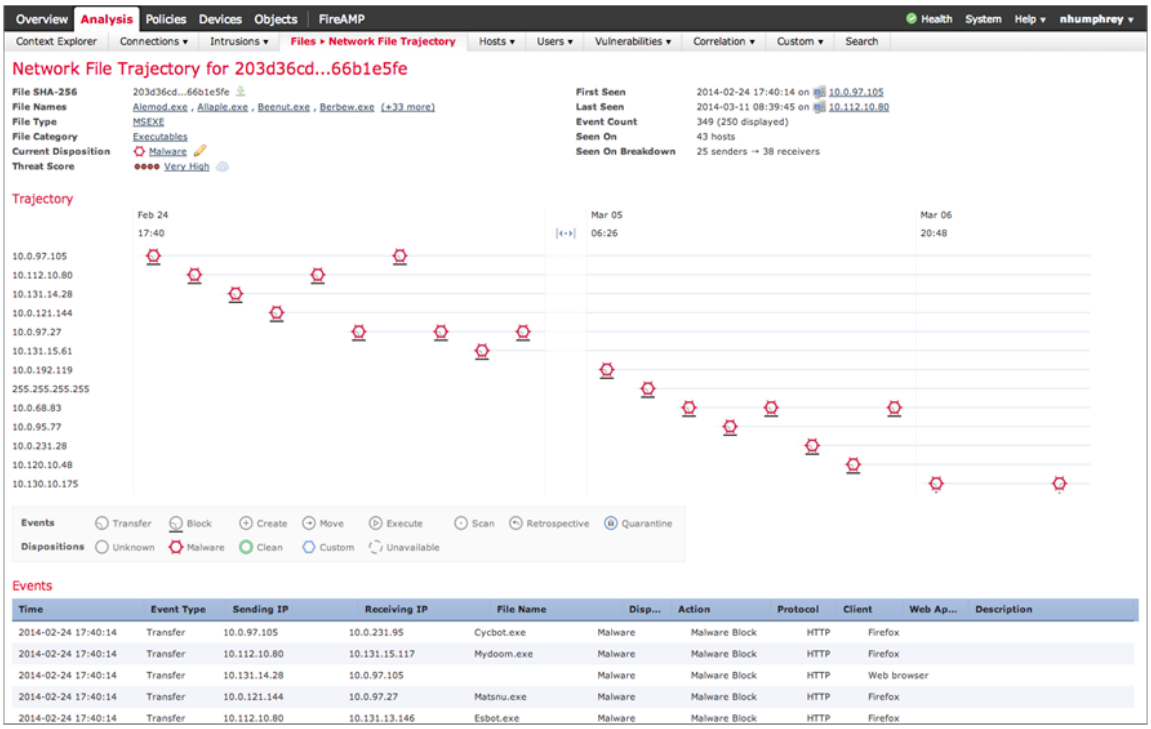
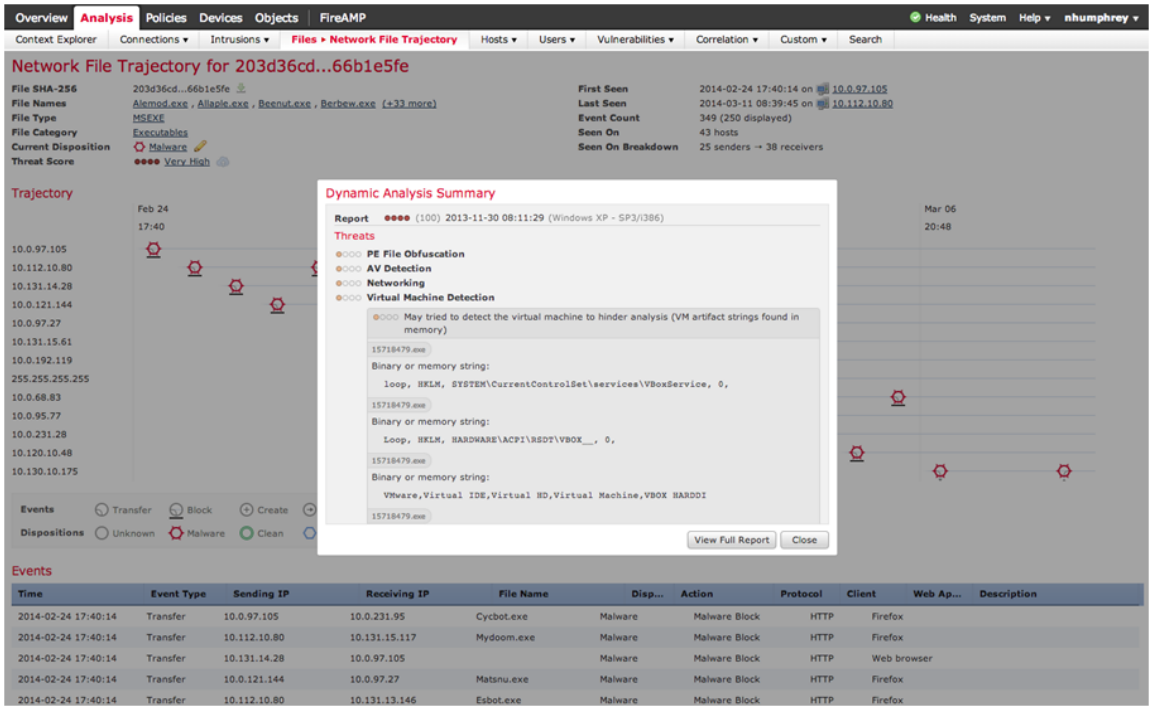


Figure 11 Résumé dynamique d'analyse du fichier



La fonctionnalité basée sur les fichiers fournie par l'analyse de la trajectoire des fichiers et des équipements améliore encore la capacité de Cisco à fournir un niveau plus avancé de collecte des données et de visualisation de l'activité des programmes malveillants et des fichiers au niveau du système. Les équipes chargées de la sécurité et de la réponse aux incidents bénéficient ainsi de fonctionnalités d'analyse essentielles pour isoler la cause première des problèmes et retracer la relation exacte entre les programmes malveillants sur les systèmes compromis et les éventuelles infections de plus grande ampleur. L'analyse de la trajectoire des équipements permet au système de rompre le cycle de vie de réinfection grâce à une analyse rapide de la cause première.

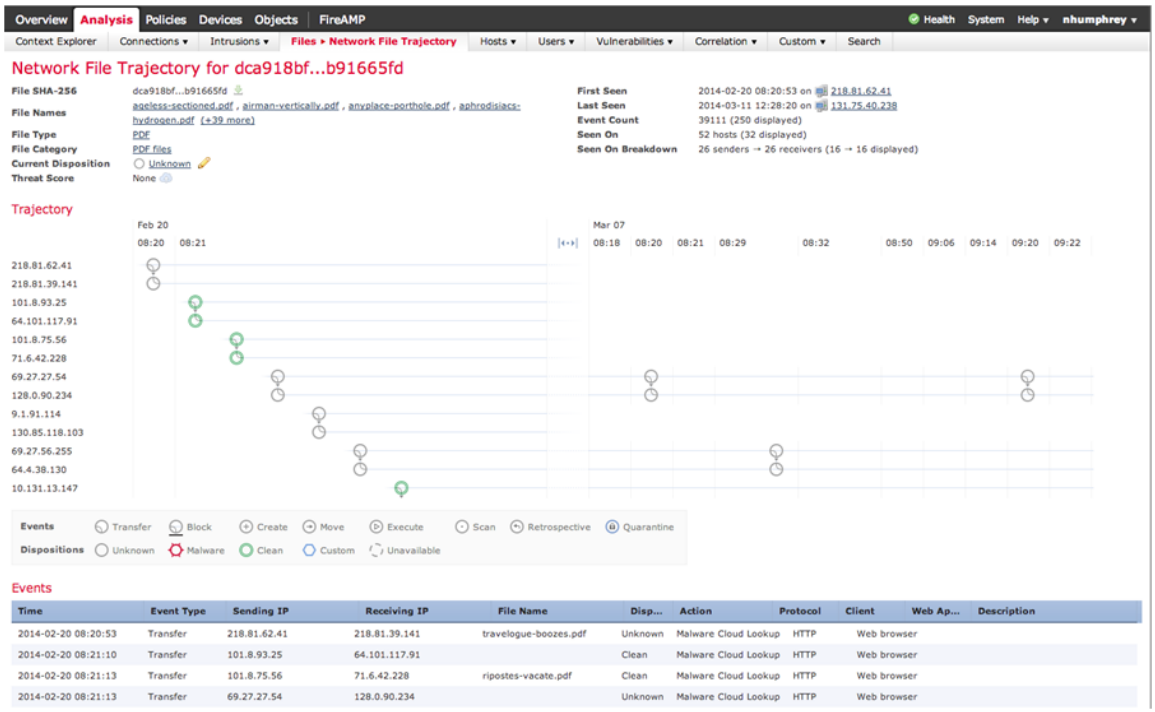
Elle retrace la relation exacte entre les programmes malveillants sur les systèmes compromis et les infections plus larges au moyen de puissantes fonctions de recherche et de filtrage. Ces dernières recherchent toute activité suspecte sur l'ensemble des systèmes, avec une analyse encore plus approfondie sur les systèmes dotés de FireAMP. La fonctionnalité permet de détecter rapidement les activités suspectes et malveillantes sur un système, puis de faire une recherche très rapide sur tous les systèmes pour détecter des indicateurs similaires. Elle suit l'activité et les données telles que l'origine et la relation parent-enfant : quels fichiers ou applications ont été créés par quels fichiers, et quels fichiers ont téléchargé d'autres fichiers, ou inversement. La fonctionnalité s'intéresse également aux processus initiaux, par exemple au processus qui a engendré ou exécuté un autre processus. Elle trace par ailleurs les communications, y compris les adresses IP, les ports, les protocoles et les URL. (Voir la Figure 12.)

En outre, les informations dynamiques de trajectoire permettent d'identifier rapidement les indicateurs de compromission, tels que des changements et d'autres comportements indiquant l'existence d'une compromission et d'une attaque probable. L'analyse de la trajectoire des équipements explore en profondeur chaque appareil et apporte des réponses aux questions suivantes :

- Comment l'attaque s'est-elle introduite dans le système ?
- Quel est le degré de gravité de l'infection sur un équipement donné ?
- Quelles ont été les communications effectuées ?

- Qu'est-ce que je ne sais pas ?
- Quelle est la séquence des événements ?

Figure 12 Analyse de la trajectoire des fichiers et des équipements



À l'instar de la chaîne d'attaque précédemment décrite, FireSIGHT Management Center permet de naviguer naturellement entre les écrans pour faire face à une intrusion ou traiter un indicateur de compromission. Le diagramme de la Figure 13 présente un exemple de flux qu'un technicien suit pour analyser des menaces potentielles. La section suivante présente des exemples de captures d'écran à chaque étape du processus d'analyse de la cause première.

Remarque Ceci n'est qu'un exemple de workflow. Il ne permet pas de démontrer toute la puissance et toutes les capacités du système de gestion FirePOWER.

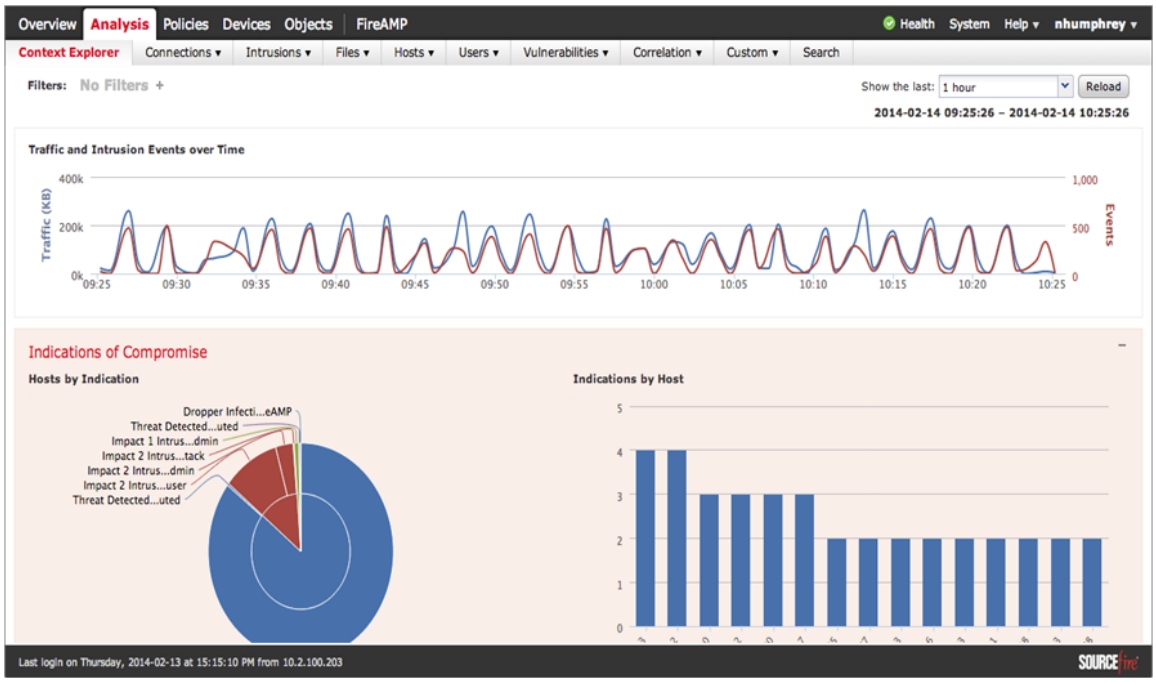
Figure 13 Exemple de workflow d'analyse de cyberdéfense

À partir de l'explorateur de contexte, les opérateurs peuvent effectuer une analyse plus approfondie. (Voir la Figure 14.)

Figure 14 Écran principal de l'explorateur de contexte

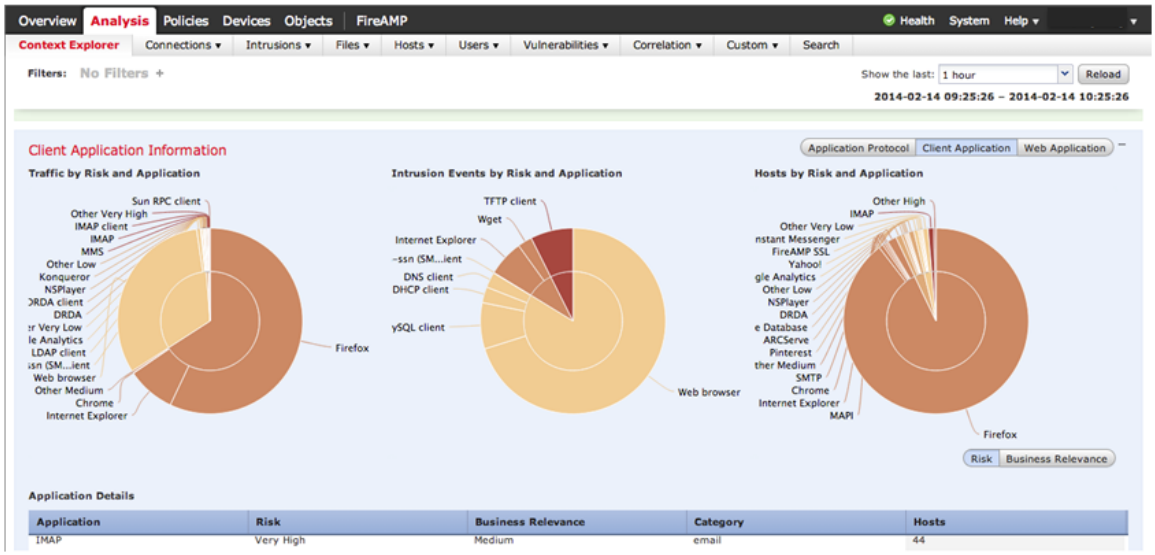
Il est possible d'approfondir l'analyse et de visualiser les indicateurs de compromission par hôte et les hôtes par indicateur (voir la Figure 15). À partir de l'écran des indicateurs de compromission, l'opérateur peut accéder rapidement à un hôte ayant été identifié comme infecté, puis effectuer une analyse plus approfondie à partir de l'écran du profil de l'hôte qui donne plus de contexte.

Figure 15 Indications de compromission de l'hôte



Comme l'illustre la Figure 16, il est possible d'effectuer une analyse approfondie grâce aux indications de compromission présentées : trafic par risque et par application, intrusions par risque et par application, et hôtes par risque et par application.

Figure 16 Indications de compromission par application cliente

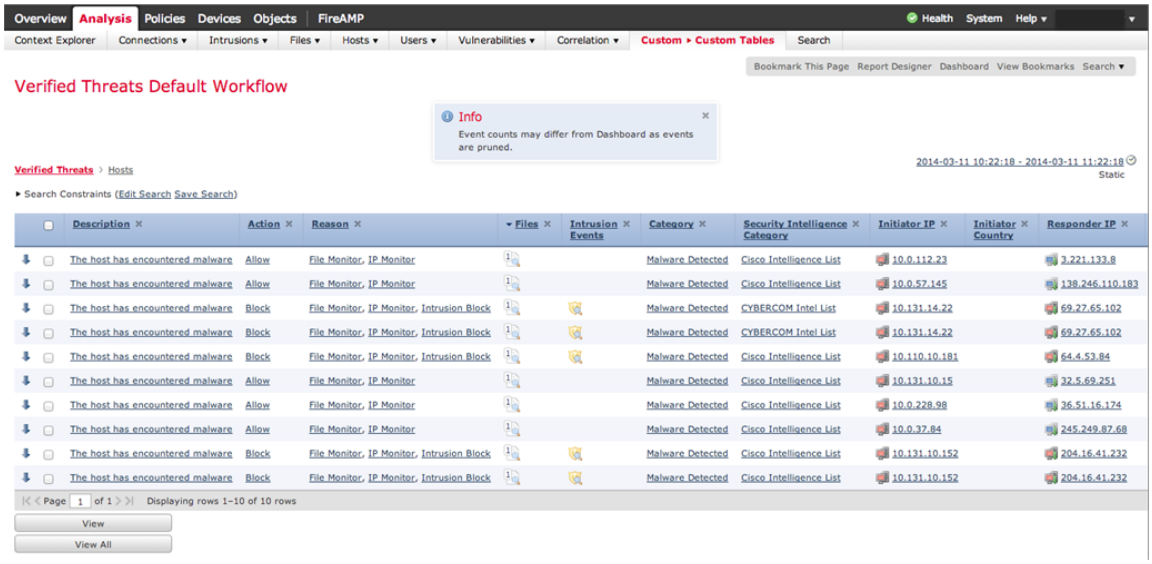


L'écran présenté dans la Figure 17 donne des informations détaillées sur l'intrusion par impact et par priorité. L'opérateur peut ainsi se concentrer sur les problèmes les plus critiques en premier. Notez qu'il est possible d'obtenir une vue détaillée pour chaque programme malveillant identifié.

Figure 17 Informations détaillées sur l'intrusion

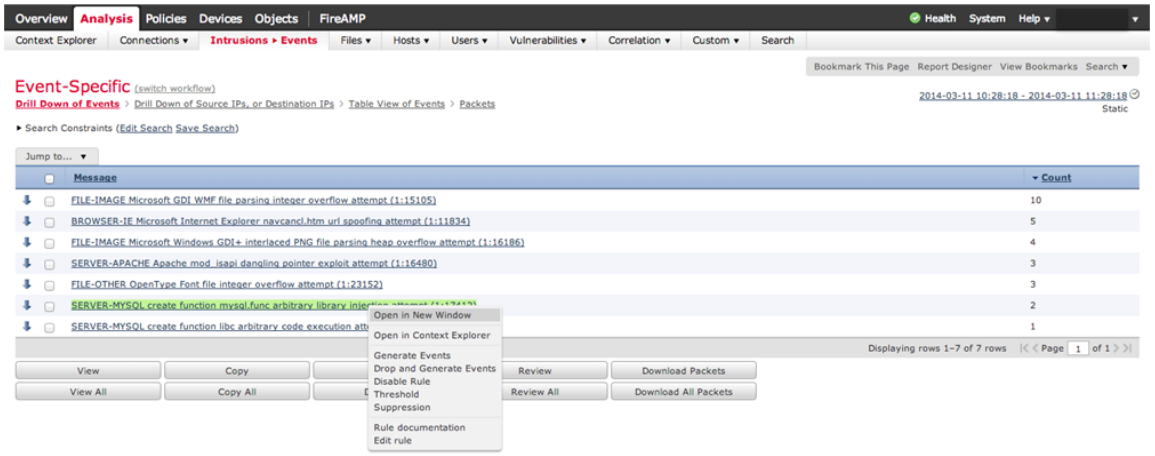
L'opérateur peut encore approfondir l'analyse et accéder aux écrans de workflow par défaut des attaques vérifiées (voir la Figure 18) et des détails de l'intrusion (voir la Figure 19).

Figure 18 Attaques vérifiées



Il peut ensuite voir les attributs de l'incident dans l'écran des détails de l'incident, présenté dans la Figure 19.

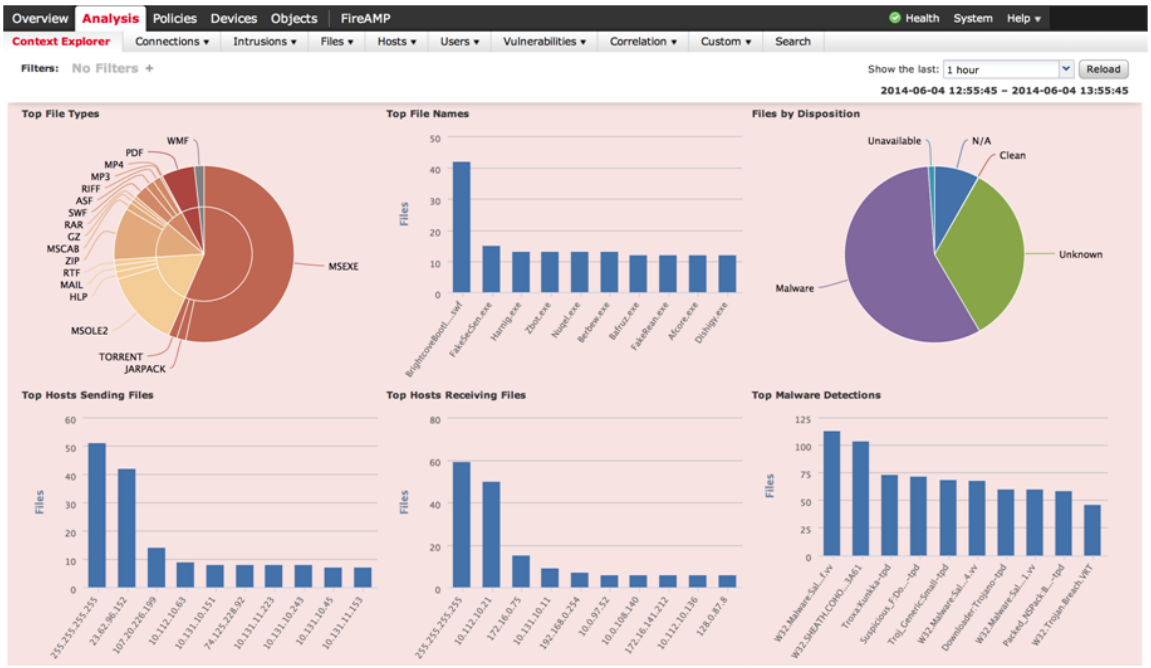
Figure 19 Détails de l'incident



Après cette plongée dans les détails de l'intrusion, la prochaine étape du workflow consiste à mieux comprendre les fichiers ciblés.

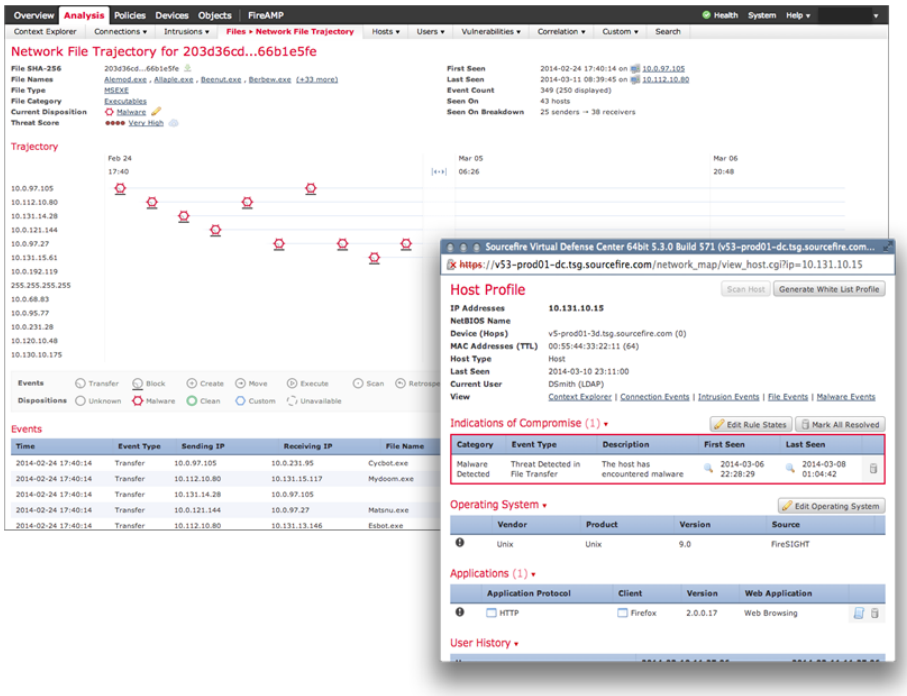
Dans l'écran d'informations sur les fichiers (voir la Figure 20), une correspondance commence à être établie entre les programmes malveillants et les fichiers corrompus détectés par la fonctionnalité AMP installée sur le réseau ou par les clients FireAMP. L'opérateur peut désormais visualiser les noms de fichier, les hôtes ainsi que les associations de programmes malveillants. Il est important de noter que cette vue se place du point de vue du réseau, car il est probable que plusieurs hôtes soient impliqués dans la détection des malwares.

Figure 20 Détails sur les programmes malveillants et les fichiers



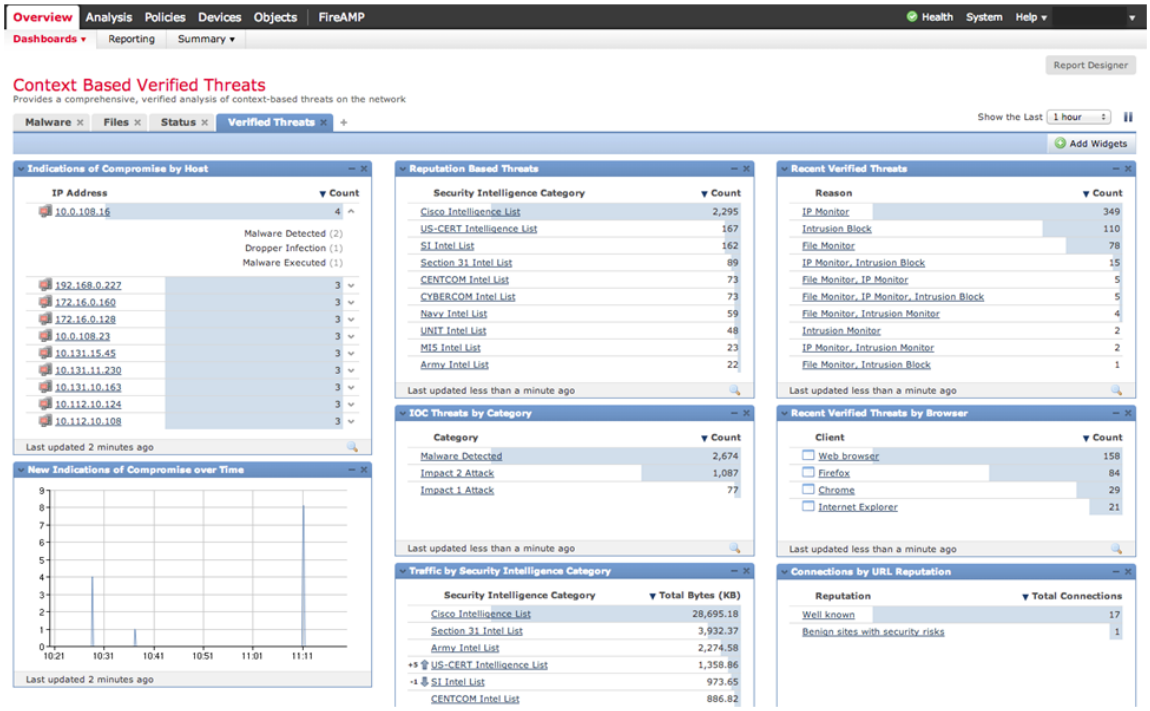
Comme nous l'avons vu dans les sections ci-dessus, la fonctionnalité d'analyse de la trajectoire des fichiers réseau génère une vue des équipements et des fichiers qui ont été compromis, et ce, à l'échelle du réseau. La Figure 21 montre l'écran de la trajectoire des fichiers réseau ainsi que des informations plus détaillées dans l'écran du profil d'hôte où une correspondance est établie entre l'indicateur de compromission et l'hôte.

Figure 21 Trajectoire sur le réseau et profil d'hôte



S'il sélectionne l'indicateur de compromission (IoC) des malwares détectés, l'opérateur peut voir les attributs détaillés des malwares pour cet hôte afin de pouvoir y remédier, comme le montre la Figure 22. Dans cet écran, des informations contextuelles sur un événement lié à un programme malveillant sont présentées. L'opérateur peut ainsi évaluer le risque que le ou les fichiers suspects présentent pour l'entreprise, avant même de décider d'envoyer les fichiers dans le cloud Cisco-Sourcefire en vue d'une analyse en sandbox. Les flux de données de sécurité adaptative qui sont issus du cloud Cisco-Sourcefire, de VRT et d'autres sources Big Data facilitent la configuration des politiques en fonction de la source et de la destination du trafic. Dans cet écran, la réputation des URL telle que fournie par le cloud Cisco-Sourcefire est également indiquée. Grâce aux sources multiples d'informations sur les incidents, l'opérateur dispose du contexte complet des menaces.

Figure 22 Attaques vérifiées en fonction du contexte



La Figure 23 présente les détails d'une analyse finale donnant lieu à une série de classifications/notations des fichiers suspects. À ce stade du workflow, l'opérateur peut choisir d'intervenir.

Figure 23 Détails de l'analyse des menaces

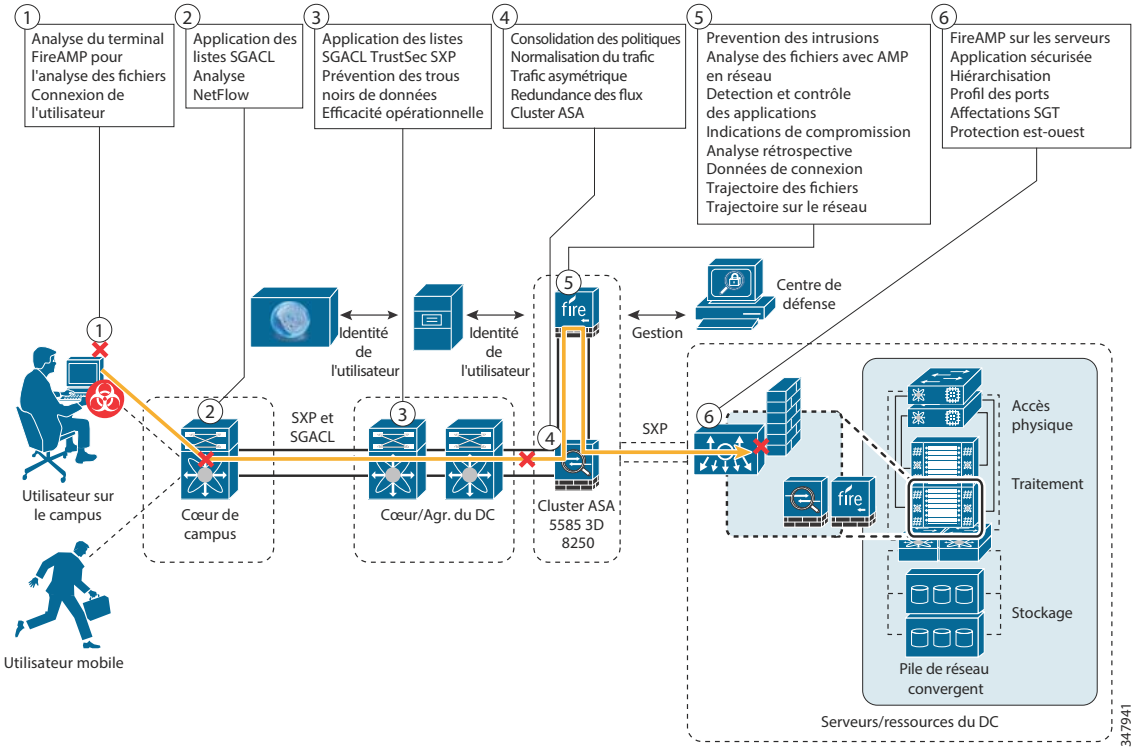
Là encore, le workflow présenté ci-dessus est un bref aperçu de la façon dont l'opérateur peut naviguer dans le processus d'analyse à l'aide de FireSIGHT Management Center afin de déterminer les prochaines étapes de la résolution.

La gestion des menaces tout au long du parcours

Le système FirePOWER procure un ensemble important de technologies à l'origine d'un large éventail de fonctionnalités de gestion des menaces. Toutefois, lors de la conception de l'architecture de sécurité selon les principes clés « avant, pendant et après une attaque », il apparaît clairement que ces fonctionnalités sont nécessaires dans l'ensemble du data center. La solution doit être bien plus qu'une solution ponctuelle qui ne traite qu'un seul vecteur d'attaque.

La figure Figure 24 montre un exemple de malware qui tente d'accéder à un serveur de data center à partir du terminal compromis d'un utilisateur.

Figure 24 Le modèle « avant, pendant, après » en action



1. Lo logiciel FireAMP installé sur le client effectue une analyse de fichiers sur le client afin d'identifier et de supprimer les malwares. ISE (Identity Services Engine) évalue le comportement de l'utilisateur et du terminal en fonction d'une liste blanche d'applications. Les informations sur l'activité de l'utilisateur sont envoyées à FireSIGHT Management Center. FireAMP communique ses résultats à FireSIGHT Management Center.
2. Le fabric de commutation Cisco applique les listes de contrôle d'accès des groupes de sécurité (SGACL) et envoie les enregistrements NetFlow à FireSIGHT Management Center et à Lancope StealthWatch en vue de l'analyse du trafic.
3. La connectivité entre le Nexus 7000 et l'appliance ASA/FirePOWER dans le fabric de cluster empêche la présence d'un « trou noir » de données et d'échapper à l'inspection.
4. Les paquets de malwares entrent dans le cluster ASA où la liste de contrôle d'accès est appliquée, et où la normalisation du trafic et l'inspection de protocole ont lieu.
5. Les paquets de malware pénètrent dans l'appliance FirePOWER qui assure la prévention des intrusions, l'analyse AMP des fichiers circulant sur le réseau, la détection et le contrôle des applications, l'analyse de la trajectoire sur le réseau ainsi que la prévention des pertes de données sensibles.
6. L'architecture d'enclaves sécurisées permet de mettre en œuvre la hiérarchisation sécurisée des applications, la sécurité est/ouest au niveau de l'hyperviseur, la sécurité d'enclave est/ouest, le provisionnement automatisé et sécurisé des charges de travail ainsi que le chaînage des services. En outre, l'appliance virtuel de sécurité adaptatif (ASAv) et l'appliance FirePOWER virtuel exécutés dans l'architecture d'enclaves sécurisées renforcent la protection.

Les composants validés

La validation repose sur la solution de mise en cluster sur un seul site avec TrustSec. Les autres composants validés de cette solution sont répertoriés dans le Tableau 3.

Tableau 3 Les composants validés

Composant	Fonction	Matériel	Version
Cisco ASA (Adaptive Security Appliance)	Cluster de pare-feu du data center	Cisco ASA 5585-SSP60	Logiciel Cisco ASA version 9.2
Appliance FirePOWER	Plate-forme IPS NextGen	3D8250	5.3
Appliance Cisco FireSIGHT Management Center	Gestion de la plate-forme IPS NextGen	DC3500	5.3
FireAMP	Protection des terminaux contre les malwares	S/O	Version XX
Cisco Nexus 7000	Agrégation et commutateur d'accès FlexPod	Cisco 7004	NX-OS version 6.1(2)

Remarque Cisco FireSIGHT Management Center incluait la licence pour FireSIGHT, la protection contre les programmes malveillants, ainsi que le contrôle des applications et des URL. Ces fonctions sont donc activées sur l'appliance FirePOWER.

La gestion des menaces avec l'IPS NextGen - Recommandations de conception

Comme nous l'avons vu, il est essentiel de ne pas négliger les fonctions de protection dans la conception d'un système capable de protéger efficacement le data center. Dans la section suivante, nous vous expliquerons comment intégrer l'appliance IPS NextGen FirePOWER dans le fabric. Puis, nous vous présenterons les technologies et les capacités avancées de l'appliance FirePOWER et d'AMP (Advanced Malware Protection) pour les terminaux. Notre objectif est de montrer comment déployer la totalité des fonctionnalités du système de gestion des menaces pour sécuriser efficacement le data center.

L'intégration de l'appliance FirePOWER et de la plate-forme de gestion

La gestion de la plate-forme avec FireSIGHT Management Center

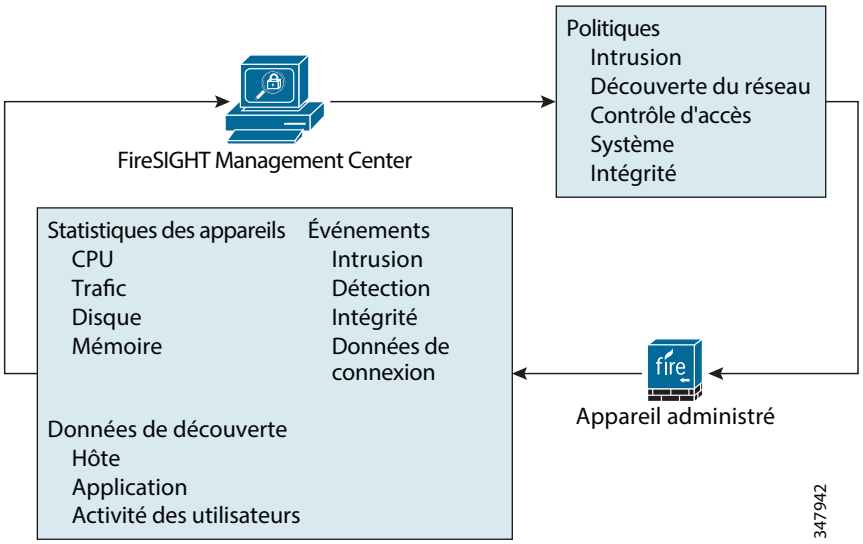
FireSIGHT Management Center est un appliance de gestion centralisée et une base de données sur les incidents destinés à une utilisation avec les appliances FirePOWER. FireSIGHT Management Center regroupe et met en corrélation les données relatives aux intrusions, aux fichiers, aux programmes malveillants, aux détections, aux connexions et aux performances. Il est ainsi possible de surveiller les informations fournies par chaque appliance FirePOWER, ainsi que d'évaluer et de contrôler l'activité globale sur le réseau.

FireSIGHT Management Center permet notamment de :

- Gérer les appareils, les licences et les politiques
- Afficher les événements et les informations contextuelles à partir de tableaux, de graphiques et de diagrammes
- Surveiller l'intégrité et les performances
- Envoyer des notifications et des alertes externes
- Consulter les données corrélées et les indicateurs de compromission pour riposter en temps réel
- Générer des rapports
- Assurer la continuité des opérations grâce à la haute disponibilité (redondance)

La gestion avec FireSIGHT Management Center des appliances physiques et virtuels FirePOWER nécessite une connectivité réseau pour assurer la circulation des informations. La Figure 25 montre comment les informations qui circulent entre les appliances physiques et virtuels FirePOWER et FireSIGHT Management Center.

Figure 25 Circulation des informations entre FireSIGHT Management Center et les appliances FirePOWER



Utiliser des appliances FireSIGHT Management Center redondants

Deux appliances FireSIGHT Management Center peuvent fonctionner en tant que paire redondante pour garantir la disponibilité en cas de panne de l'un des deux. Les deux appliances FireSIGHT Management Center partagent les politiques, les comptes d'utilisateur et d'autres informations. Les événements sont automatiquement envoyés aux deux appliances FireSIGHT Management Center.

Les deux appliances FireSIGHT Management Center mettent mutuellement à jour leur configuration à partir des modifications effectuées. Toute modification apportée à l'un des appliances FireSIGHT Management Center est répercutée à l'autre en 10 minutes. Chaque FireSIGHT Management Center a un cycle de synchronisation de 5 minutes, mais étant donné que les cycles peuvent être désynchronisés de 5 minutes, deux cycles de 5 minutes sont nécessaires pour appliquer les modifications. Dans cette fenêtre de 10 minutes, les configurations des appliances FireSIGHT Management Center peuvent être différentes.

Deux appliances FireSIGHT Management Center associés dans une paire hautement disponible partagent les informations suivantes :

- Les attributs des comptes d'utilisateur
- Les configurations d'authentification
- Les rôles d'utilisateur personnalisés
- Les objets d'authentification des comptes d'utilisateur et de reconnaissance des utilisateurs ainsi que les informations sur les utilisateurs et les groupes qui figurent dans les conditions relatives aux utilisateurs dans les règles de contrôle d'accès
- Les tableaux de bord personnalisés
- Les tables et les workflows personnalisés
- Les attributs des appareils, notamment leur nom d'hôte, l'emplacement de stockage des événements qu'ils génèrent ainsi que le groupe dans lequel ils résident
- Les politiques d'intrusion et l'état des règles qui leur sont associées
- Les politiques de fichier
- Les politiques de contrôle d'accès et les règles qui leur sont associées
- Les règles locales
- Les classifications de règles d'intrusion personnalisées
- Les valeurs des variables et les variables définies par l'utilisateur
- Les politiques de découverte des activités du réseau
- Les détecteurs de protocoles d'application définis par l'utilisateur et les applications qu'ils détectent
- Les empreintes personnalisées activées
- Les attributs des hôtes
- Les commentaires des utilisateurs sur la découverte des activités du réseau, notamment des remarques et des commentaires portant sur la criticité des hôtes, la suppression des hôtes, des applications et des réseaux de la carte réseau ainsi que sur la désactivation ou la modification des vulnérabilités
- Les politiques et les règles de corrélation, les listes blanches de conformité et les profils de trafic
- Les instantanés de réconciliation des modifications et les paramètres de rapport
- Les mises à jour des règles d'intrusion, des bases de données de géolocalisation et des bases de données de vulnérabilités

L'appliance FireSIGHT Management Center se décline en trois modèles dont les performances sont présentées dans le Tableau 4.

Tableau 4 Performances des FireSIGHT Management Centers

	DC750	DC1500	DC3500
Nombre maximal d'appareils administrés	10	35	150
Nombre maximal d'événements IPS	20 M	30 M	150 M
Stockage d'événements	100 Go	125 Go	400 Go

Tableau 4 Performances des FireSIGHT Management Centers (suite)

	DC750	DC1500	DC3500
Nombre maximal de mappages réseau (hôtes/utilisateurs)	2 000/2 000	50 000/50 000	300 000/300 000
Débit maximal	2 000 images/s	6 000 images/s	10 000 images/s
Fonctionnalités haute disponibilité	Gestion LOM (Lights-out Management)	RAID 1, LOM, couplage haute disponibilité (HA)	RAID 5, LOM, haute disponibilité, alimentation CA redondante

Remarque Une version virtuelle de l'appliance FireSIGHT Management Center existe. Il est capable de gérer jusqu'à 25 appliances physiques et/ou virtuels. Il est compatible avec VMware ESX 4.5/5.x ou version supérieure et nécessite au moins 4 cœurs de processeur et 4 Go de mémoire.

Les licences

La question des licences des produits et des applications n'est en général pas traitée dans nos conceptions validées, mais étant donné que les appliances FirePOWER prennent en charge un ensemble complet de technologies et de fonctionnalités, il convient de présenter les licences dans ce document.

FireSIGHT

Une licence FireSIGHT est fournie avec FireSIGHT Management Center et est requise pour la découverte des hôtes, des applications et des utilisateurs. La licence FireSIGHT sur FireSIGHT Management Center détermine le nombre d'hôtes et d'utilisateurs individuels pouvant être surveillés par FireSIGHT Management Center et le nombre d'appareils qu'il administre ainsi que le nombre d'utilisateurs pour le contrôle d'accès des utilisateurs. (Voir le Tableau 5.) Cisco recommande que les licences soient ajoutées lors de la configuration initiale de FireSIGHT Management Center. Sinon, tous les appareils enregistrés lors de la configuration initiale sont ajoutés à FireSIGHT Management Center sans licence. Après la configuration initiale, les licences doivent être activées individuellement sur chaque appareil.

Tableau 5 Limites de FireSIGHT selon le modèle de FireSIGHT Management Center

Modèle de FireSIGHT Management Center	FireSIGHT - Limite du nombre d'hôtes et d'utilisateurs
Appliance FireSIGHT Management Center virtuel	50 000
DC500	1 000 (aucun contrôle d'utilisateurs)
DC750	2 000
DC1000	20 000
DC1500	50 000
DC3000	100 000
DC3500	300 000

La protection

Avec une licence de protection, les appareils administrés peuvent détecter et empêcher les intrusions, contrôler les fichiers et filtrer les données de sécurité adaptative.

Le contrôle

Avec une licence de contrôle, les appareils administrés peuvent effectuer le contrôle des utilisateurs et des applications. Ils peuvent également effectuer la commutation et le routage (notamment le relais DHCP), la traduction d'adresses réseau (NAT) et la mise en cluster des appareils et des piles. Une licence de contrôle nécessite une licence de protection.

Le filtrage des URL

Avec une licence de filtrage des URL, les appareils administrés peuvent utiliser les informations cloud de catégorie et de réputation régulièrement mises à jour pour déterminer quel trafic est autorisé à traverser le réseau, en fonction des URL demandées par les hôtes surveillés. Une licence de filtrage des URL nécessite une licence de protection.

La protection contre les programmes malveillants

Avec une licence AMP (Advanced Malware Protection), les appareils administrés peuvent contrer les programmes malveillants circulant sur le réseau. La plate-forme peut ainsi détecter, capturer et bloquer les fichiers de programmes malveillants transmis sur le réseau et les soumettre à une analyse dynamique. L'opérateur peut alors analyser la trajectoire des fichiers transmis sur le réseau. Une licence AMP nécessite une licence de protection.

L'intégration de l'IPS NextGen dans le fabric

Lorsque les appliances FirePOWER sont déployés en ligne, ils peuvent agir sur le flux du trafic en fonction de différents critères. Les appliances FirePOWER comportent des fonctionnalités de gestion des menaces bien supérieures à celles des IPS classiques. Ces fonctionnalités sont décrites plus en détail dans les sections suivantes.

L'intégration d'un cluster ASA

La CVD de la solution de mise en cluster sur un seul site avec TrustSec comprend des informations détaillées concernant la conception et le déploiement de l'appliance ASA 5585-X en mode cluster. Depuis la publication de cette CVD, la version 9.2 du système d'exploitation ASA est sortie. Cette version offre une meilleure évolutivité, car jusqu'à 16 liaisons actives sont désormais prises en charge avec EtherChannel. Un cluster peut donc comporter jusqu'à 16 appliances ASA 5585-X pour une bande passante pouvant atteindre 640 Gbit/s.

Tous les appliances ASA du cluster doivent avoir exactement la même configuration pour que le système ASA fonctionne correctement. En outre, ils doivent être déployés de manière homogène. Le même type de ports doit être utilisé sur toutes les unités pour assurer la connexion au fabric. Utilisez les mêmes ports pour la liaison de contrôle du cluster au fabric de commutation et les liaisons des données. Lorsque le cluster ASA est correctement déployé, l'unité principale du cluster réplique sa configuration sur les autres unités du cluster pour qu'elles aient la même configuration.

Les performances du cluster ASA

L'ajout d'un appliance ASA 5585-X dans le cluster entraîne une augmentation du débit global du système d'environ 70 % de la capacité de traitement totale de cette unité. Le débit d'un appliance ASA 5585-X-SSP60 atteint 40 Gbit/s de trafic optimal (trames géantes ou paquets UDP) et environ 20 Gbit/s de trafic IMIX/EMIX. Les connexions et les connexions par seconde maximales peuvent évoluer de 60 % et de 50 % respectivement. (Voir le Tableau 6.)

Tableau 6 Les performances du cluster ASA

Fonction	Performances
Débit du pare-feu ASA 5585-X - Multiprotocole	20 Gbit/s
Cluster de 16 nœuds ASA 5585-X (IMIX/EMIX)	224 Gbit/s
Nombre de connexions TCP par seconde (1 châssis)	350 K cps
Nombre de connexions TCP par seconde du cluster de 16 nœuds ASA 5585-X	2,8 M cps
Nombre (maximal) de connexions TCP simultanées (1 châssis)	10 M (max.)
Nombre maximal de connexions dans le cluster de 16 nœuds ASA 5585-X	96 M (max.)

L'état de l'intégrité du cluster ASA

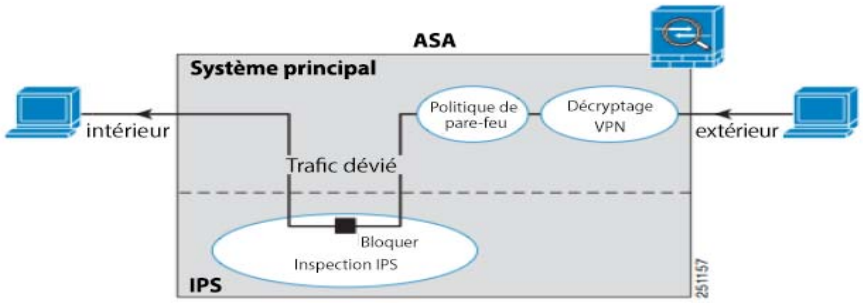
L'unité principale surveille toutes les unités du cluster en envoyant des messages keepalive via la liaison de contrôle du cluster. Lorsque les interfaces ASA fonctionnent en mode EtherChannel fractionné, chaque unité surveille les messages cLACP et envoie un état de liaison à l'unité principale. Lorsque la surveillance de l'intégrité est activée, les unités en panne sont supprimées automatiquement du cluster. Si l'unité principale tombe en panne, l'unité du cluster avec la priorité la plus élevée la remplace.

Le flux du trafic entre le système ASA et l'IPS Cisco classique

Comme nous l'indiquons tout au long de ce document, cette solution repose sur l'architecture de mise en cluster sur un seul site avec TrustSec. Par conséquent, il est essentiel que l'intégration des appliances FirePOWER dans le cluster de 16 nœuds ASA5585-X soit cohérente du point de vue de l'architecture. Un bref rappel de la façon dont le trafic du module IPS transite dans l'appliance ASA 5585-X s'impose afin d'expliquer la logique sur laquelle repose l'architecture présentée dans ce guide de conception.

L'appliance ASA 5585-X est un châssis à deux logements dans lequel le module ASA 5585-X-SSP60 occupe le premier logement. Le guide de conception de l'architecture de la solution de mise en cluster sur un seul site avec TrustSec indiquait comment intégrer le module IPS (5585-SSP-IPS60) dans le second logement. Lorsque le module IPS est installé dans le second logement, le trafic circule de façon très similaire à l'approche « IPS on a stick ». Avec cette approche, les politiques de trafic configurées sur l'appliance ASA identifient le trafic qui doit transiter par le module IPS pour une inspection approfondie des paquets, comme illustré à la Figure 26. Bien que le trafic reste dans le châssis ASA, il quitte le module ASA et traverse le module IPS 5585-SSP-IPS60, puis le retraverse dans l'autre sens. Dans la section suivante, nous allons voir comment ce modèle fondamental a été modifié pour permettre l'intégration de l'appliance FirePOWER dans le fabric du data center.

Figure 26 Flux entre le module ASA et le module IPS 5585-SSP-IPS60



La gestion des menaces avec l'IPS NextGen

Dans cette section, nous proposons plusieurs conceptions afin de permettre aux détenteurs de data centers Nexus et ASA de tirer parti de la fonctionnalité avancée de gestion des menaces du système Cisco FirePOWER. L'objectif de chaque conception vise à assurer une intégration irréprochable du système de sécurité en termes d'impact sur le réseau, à réduire les risques, les pertes de paquets et les périodes d'indisponibilité, et à optimiser l'évolutivité et la performance du data center hautement disponible déjà en place. Pour vous aider à pérenniser votre investissement lorsque vous actualisez votre architecture avec des produits du portefeuille de solutions de sécurité du data center, nous vous proposons des conseils de conception spécifiques pour trois options initiales de conception. Les options varient en fonction du type de déploiement, notamment en ligne ou passif, physique ou virtuel, de l'évolutivité et de la gestion du trafic, ainsi que de l'évolutivité de la solution de sécurité elle-même oujdes fonctionnalités prises en charge. Toutes les options respectent scrupuleusement les attentes de nos clients en matière de fonctionnalités qu'un réseau de data center doit impérativement proposer, à savoir :

- La haute disponibilité
- Aucune interruption
- La pérennité des flux
- La redondance du matériel et des liaisons
- La diversité des liaisons et le traitement déterministe des flux
- Le traitement correct des flux de paquets asymétriques prévus
- La détection des anomalies ou des trous noirs de trafic inacceptables
- L'évolutivité élastique
- Une latence faible
- Aucune pénalité de perte de paquets par défaut pour les services
- La facilité de gestion, la visibilité, l'orchestration
- La conformité aux normes de sécurité et à la réglementation

Les options de gestion des menaces avec l'IPS NextGen que nous allons aborder sont les suivantes :

- Option 1 : FirePOWER dans une conception en ligne (couplage de contextes de cluster ASA)
- Option 2 : FirePOWER dans une conception passive
- Option 3 : conception appliance FirePOWER virtuel et appliance ASA virtuel

Chaque option est décrite plus en détail dans les pages suivantes. Une série de diagrammes illustrant la circulation des menaces montre comment l'approche centrée sur les menaces fonctionne avant, pendant et après une attaque.

Option 1 : FirePOWER dans une conception en ligne avec un cluster ASA

L'utilisation de la technique de couplage de contextes de cluster ASA offre une évolutivité optimale pour le déploiement d'un IPS NextGen FirePOWER en ligne utilisant l'appliance ASA lorsque le déploiement doit tenir compte de l'encombrement physique en raison de la taille. Les déploiements en ligne présentent l'avantage de pouvoir rejeter le trafic nuisible avant qu'il atteigne la cible désignée, et cela à l'emplacement optimal dans le fabric de réseau, c'est-à-dire à la source. Le couplage de contextes de cluster ASA permet à la solution de sécurité du data center d'exploiter l'ensemble des fonctionnalités de sécurité dans l'ensemble du cluster ASA.

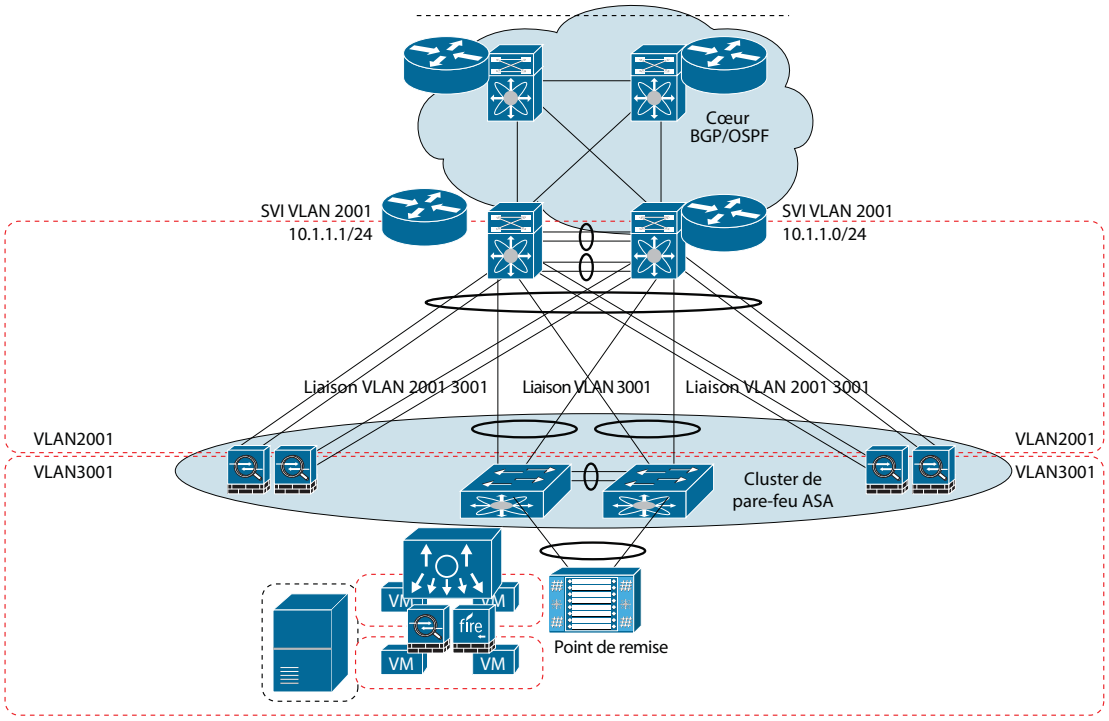
- La visibilité et le contrôle sur les applications avec OpenAppID™
- La catégorisation des URL et les indicateurs de compromission associés
- Les fonctionnalités de visibilité sur les terminaux et de contexte ainsi que les indicateurs de compromission associés de FireSIGHT™
- Un IPS NextGen avec les fonctionnalités de gestion avancée des menaces de FirePOWER™
- Advanced Malware Protection (AMP)
- Des options de gestion de l'identité des utilisateurs
- Le traitement analytique du Big Data dans le cloud et l'utilisation du service de gestion du système de protection Cisco
- L'analyse de la trajectoire des fichiers et sur le réseau
- L'analyse ponctuelle et rétrospective (continue)
- La gestion des vulnérabilités
- La gestion des correctifs
- Des analyses
- Une fonctionnalité d'échec à l'ouverture ou à la fermeture pour le système IPS NextGen
- L'ensemble complet de fonctionnalités réseau avancées standard sur les ASA (reprise après sinistre et continuité de l'activité, notamment)
- L'intégration directe avec le composant virtuel d'architecture d'enclaves sécurisées (voir l'option 3 : gestion virtuelle des attaques dans l'enclave sécurisée plus loin dans ce document)

L'option de conception Couplage de contextes de cluster ASA induit des modifications minimes au déploiement réseau du data center physique pour un système en ligne. Elle permet d'effectuer le déploiement sans interruption du data center et elle exploite la fonctionnalité inhérente de gestion des flux de trafic asymétriques du cluster ASA pour éviter toute perte de paquets lorsqu'une unité ASA ou un appliance FirePOWER tombe en panne.

La conception requiert l'interconnexion de l'appliance FirePOWER à l'appliance ASA 5585-X via les deux interfaces 10GE sur chaque châssis et la réécriture des balises VLAN. Le flux entre les appareils est similaire aux flux type lorsque l'IPS est intégré à l'appliance ASA 5585-X en tant que module, à ceci près que le flux dispose d'un contexte supplémentaire. Le second contexte ASA, soit le contexte descendant, ou Sud, est nécessaire pour assurer la prise en charge continue des flux de trafic asymétriques dans le data center. Il s'intègre également dans l'architecture d'enclaves sécurisées pour garantir une virtualisation multilocataire sécurisée. Étant donné que l'appliance ASA comporte deux contextes pour chaque châssis ASA, il n'est pas nécessaire d'acheter des licences supplémentaires pour ce déploiement, surtout si aucun déploiement multicontexte n'a été effectué précédemment et si des licences de contexte ont déjà été achetées.

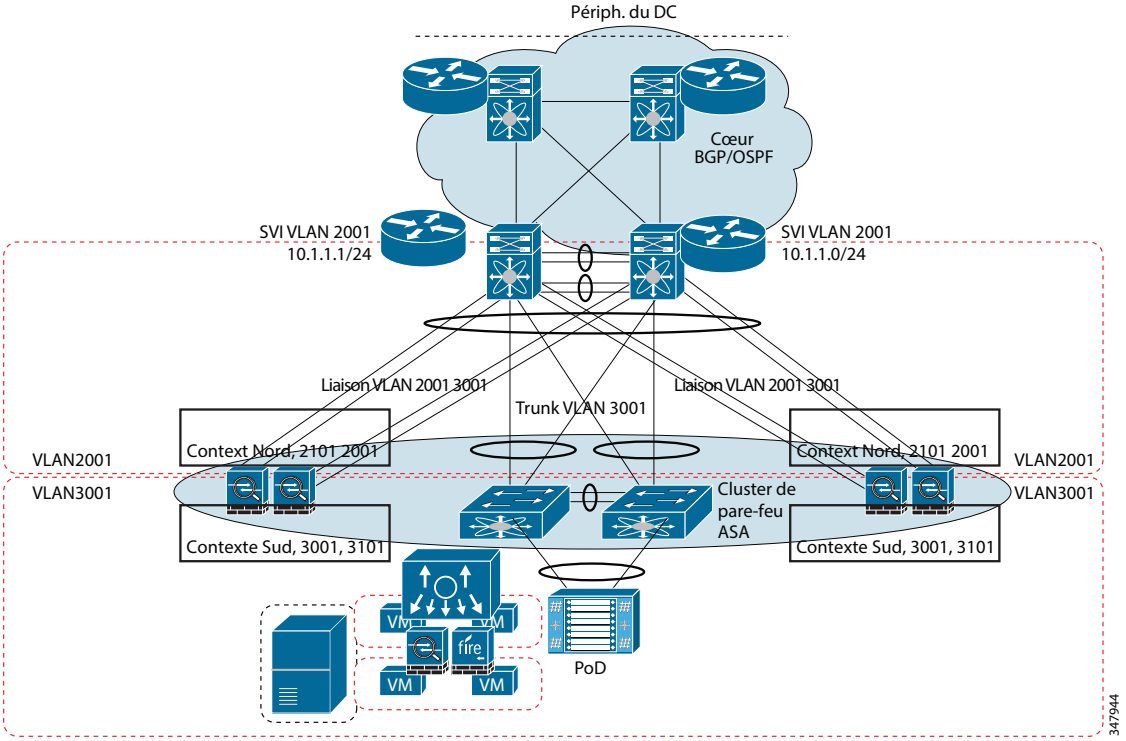
La Figure 27 et la Figure 28 illustrent les modifications minimes à apporter à l'infrastructure de réseau du data center pour l'option de couplage de contextes de cluster ASA.

Figure 27 Diagramme du réseau avant la mise en œuvre de FirePOWER



Dans cet exemple, le cluster ASA est mis en œuvre en mode transparent en utilisant le protocole cLACP entre les VLAN 2001 et 3001. Notez les masques de flux de VLAN sur les liaisons entre le cluster ASA et les commutateurs Nexus 7K vers les VLAN 2001 et 3001 et comparez-les à ceux figurant dans le diagramme « après » de la Figure 28.

Figure 28 Conception réseau « après » la mise en œuvre de FirePOWER



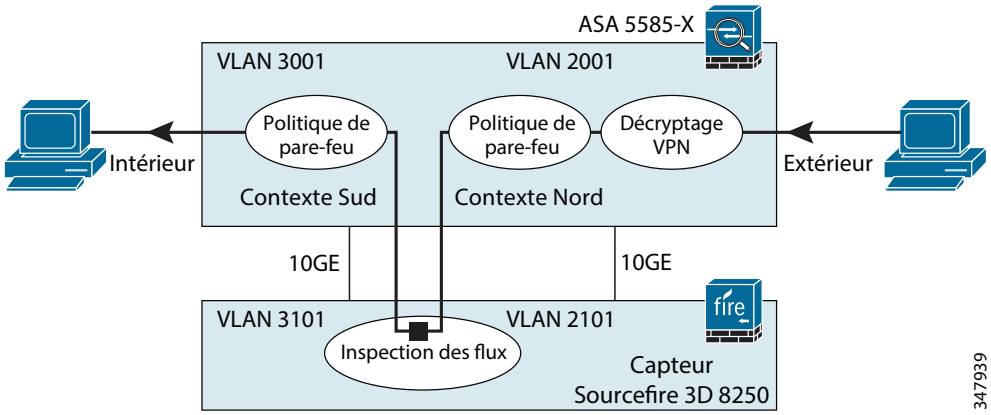
Le diagramme « après » présenté à la Figure 28 montre les modifications mineures appliquées à l'unité principale du cluster ASA. Les appliances ASA utiliseront un second contexte descendant, appelé Sud, pour traiter le trafic asymétrique circulant vers et depuis les appliances FirePOWER. Le VLAN 2001 reste dans le contexte d'origine (sauf si plusieurs contextes sont déjà utilisé) ; dans ce cas, il devient un membre du contexte Nord ou ascendant (Nord est un nom arbitraire). Le VLAN 3001 devient un membre du nouveau contexte Sud ou descendant (Sud est également un nom arbitraire). Un nouveau VLAN est ajouté à chacun de ces contextes, 2101 vers le Nord et 3101 vers le Sud. Vous constaterez qu'il n'y a aucune passerelle ni aucun changement de VLAN sur les hôtes, et aucun changement de masque de flux de liaison (élagage). La solution utilise les liaisons déjà en place dans le cluster ASA pour se connecter aux commutateurs Nexus 7K sans qu'aucune modification ne soit nécessaire.

Les deux nouveaux VLAN sont utilisés pour incorporer l'appliance FirePOWER dans le flux, c'est-à-dire entre les contextes ASA Nord et Sud. Ceci afin que la gestion du flux de trafic asymétrique soit possible des deux côtés des appliances FirePOWER en exploitant les fonctionnalités inhérentes du réassemblage asymétrique CCL du cluster ASA. L'appliance FirePOWER est ajouté à un nouveau port 10G physique sur chaque appliance ASA et affecté à chaque contexte ASA, afin de fournir un flux réseau de type fond de panier qui exploite la sémantique de flux hautement optimisée du cluster ASA.

La commutation des balises VLAN avec l'appliance FirePOWER

Les appliances FirePOWER peuvent être configurés pour un déploiement de couche 2 pour assurer la commutation des paquets entre au moins deux segments du réseau. Dans le déploiement de type couplage de contextes de cluster ASA, vous devez configurer les interfaces commutées et les commutateurs virtuels sur les appareils administrés pour qu'ils fonctionnent en tant que domaines de diffusion autonomes. Un commutateur virtuel utilise l'adresse MAC d'un hôte pour déterminer où envoyer les paquets. Dans ce cas, l'appliance ASA est l'hôte référencé. Ce déploiement de couche 2 de l'appliance FirePOWER est utilisé pour effectuer la commutation des balises VLAN entre les deux interfaces 10G Ethernet sur l'appliance FirePOWER vers les interfaces 10G dédiées sur l'appliance ASA local. (Voir la Figure 29.)

Figure 29 Flux entre le cluster ASA 5585-X et l'IPS 3D8250

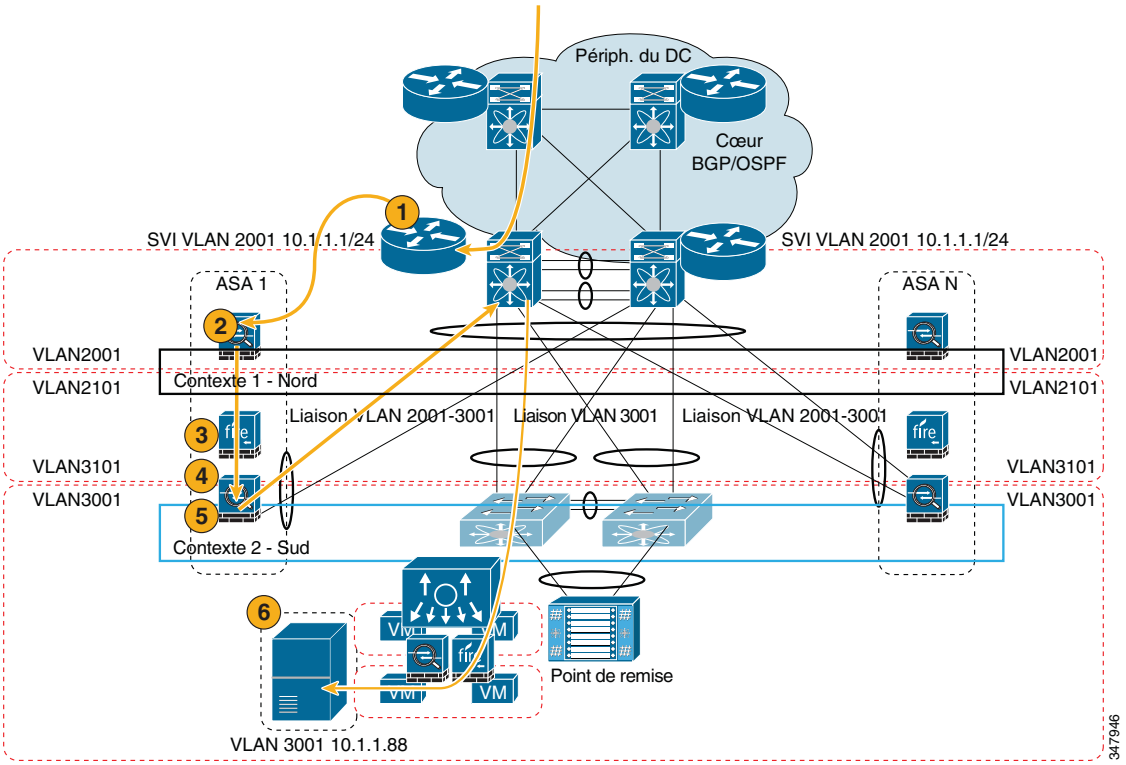


La Figure 30 illustre la transmission via le cluster ASA 5585-X avec l'appliance FirePOWER intégré comme suit.

Le flux de paquets

1. Le paquet arrive sur SVI VLAN 2001-Requête ARP au serveur 10.11.1.88. L'appliance ASA répond avec l'adresse MAC de l'interface externe.
2. Le paquet passe par le contexte ASA 1 Nord pour aboutir au VLAN 2101 FirePOWER en utilisant l'interface physique destinée au contexte ASA 2 Sud. Les politiques des paquets qui arrivent sur le VLAN 2001 sur l'appliance ASA sont traitées sur celui-ci (propriétaire/directeur de mise en cluster) et ainsi de suite. Le flux symétrique est assuré pour cette session.
3. Le paquet inspecté par l'appliance FirePOWER est transféré à l'interface (externe/interne) du contexte ASA 2. La balise VLAN est transmise au VLAN 3101.
4. Le contexte ASA 2 traite la politique, réécrit la balise du paquet sur la liaison vers le VLAN 3001. Le paquet est renvoyé au commutateur Nexus 7K avec le VLAN 3001.
5. Le commutateur Nexus 7K transfère le paquet au serveur via le VLAN 3001.
6. Le paquet atteint le serveur 10.11.1.88.

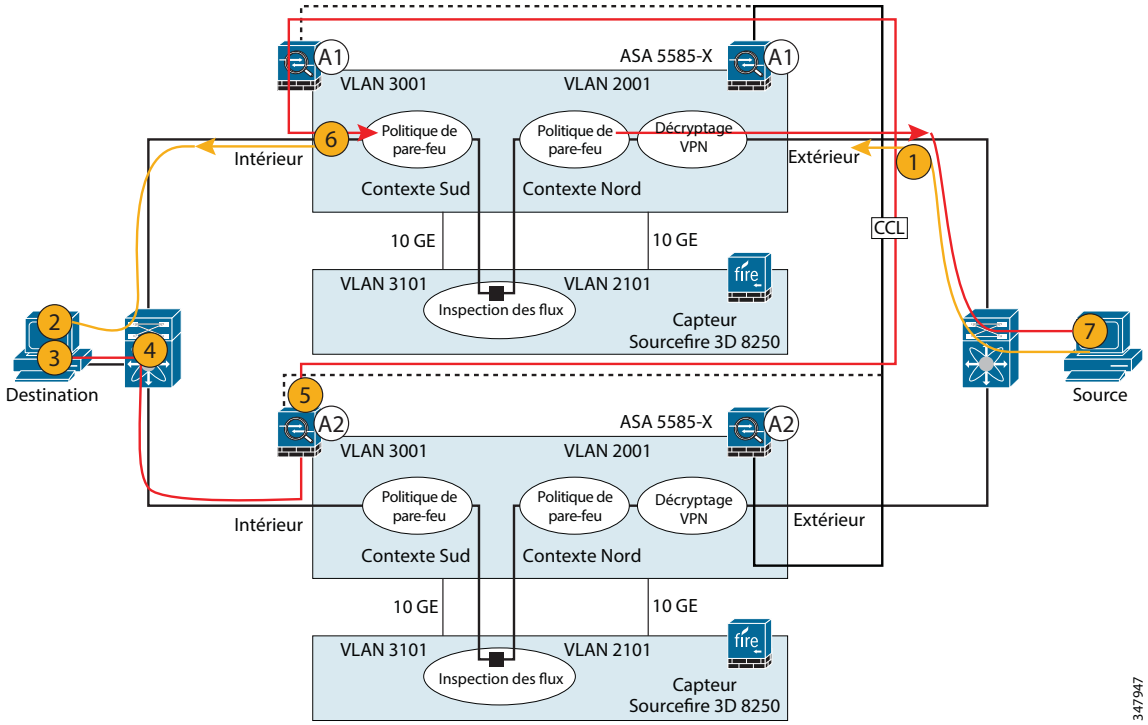
Figure 30 Le flux de paquets



Le traitement des flux de trafic asymétrique pour sécuriser les flux

Dans un data center ultra disponible correctement conçu, les flux de trafic asymétrique sont non seulement attendus, mais dans de nombreux cas, voulus, pour tirer pleinement parti des composants de commutation réseau pour le data center, qui représentent souvent un investissement important, et pour utiliser de façon optimale les liaisons (ascendantes) évolutives. Étant donné que les sessions sont toujours bidirectionnelles, il est toujours possible que du trafic provenant de la même source et ayant la même destination selon les hachages LACP symétriques, prenne un chemin physique de retour différent. Du point de vue de la sécurité, la précision prime toujours, mais un système tel qu'un système IPS NextGen ne peut pas vous offrir une visibilité totale et il ne peut agir de façon adéquate sur les paquets qu'il ne voit pas. Ce type de précision n'a pas une tolérance très élevée pour les paquets manquants qui prennent un autre chemin. Le couplage de contextes de cluster ASA place l'appliance FirePOWER entre deux clusters ASA logiques. Ainsi, le traitement inhérent du flux de trafic asymétrique par le cluster garantit que chaque paquet dans une session soit visible par l'appliance FirePOWER correct. Et cela, quelle que soit la direction du trajet entre la source et la destination pour une session d'application donnée. Lorsque l'appliance FirePOWER voit chaque paquet dans une session sans exception, la précision requise pour assurer une sécurité complète est garantie. La Figure 31 illustre un exemple de flux de trafic asymétrique entre la source et la destination et montre comment la paire de contextes de cluster ASA garantit la constance de chaque session à l'aide du CCL ASA.

Figure 31 Traitement du flux asymétrique dans la paire de contextes de cluster ASA



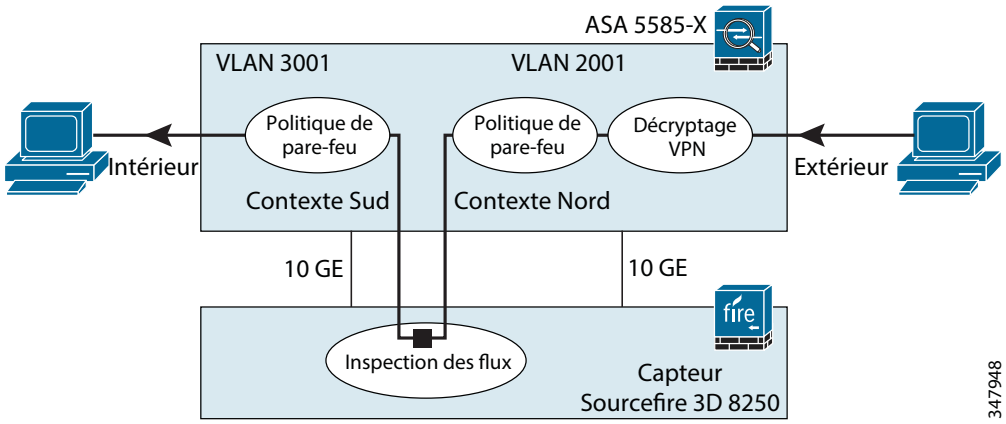
Le flux de paquets

1. Le paquet provenant de l'hôte source est envoyé par le commutateur local sur un chemin à ASA A1 pour le traitement de la politique et, en supposant que la politique est autorisée et que la situation initiale est présumée propre par l'appliance FirePOWER, le paquet est transféré.
2. Le paquet propre arrive sur l'hôte de destination en suivant le chemin prévu.
3. L'hôte de destination renvoie le paquet.
4. Le commutateur local sélectionne le chemin qui permet au paquet d'arriver au ASA A2.
5. ASA A2, utilisant la sémantique CCL pour le réassemblage asymétrique, transmet le paquet sur le CCL, et le paquet arrive au ASA A1 pour être traité.
6. Le paquet est envoyé via la paire de contextes à l'aide du chemin correct pour que l'appliance FirePOWER puisse visualiser tous les paquets dans la session et vérifier avec précision si le flux est sécurisé.
7. Le paquet propre arrive sur la source comme prévu.

L'option de conception : paire de clusters ASA sans VLAN supplémentaires

Si l'architecture d'enclaves sécurisées pour la virtualisation multilocataire n'est pas utilisée ni envisagée, il est possible de déployer la paire de clusters ASA en utilisant simplement les deux VLAN précédents, dans ce cas 2001 et 3001. Dans cette option de conception, comme le montre la Figure 32, les interfaces qui se connectent à l'appliance FirePOWER depuis l'appliance ASA sont les interfaces physiques dédiées qui sont affectées aux contextes Nord et Sud sans qu'aucune balise VLAN soit attribuée. Avec cette option de conception il n'est pas nécessaire que l'appliance FirePOWER procède à la commutation des balises VLAN. La configuration du gestionnaire d'événements intégré (EEM) s'applique cependant à cette option de conception.

Figure 32 Paire de contextes de cluster ASA sans VLAN supplémentaires



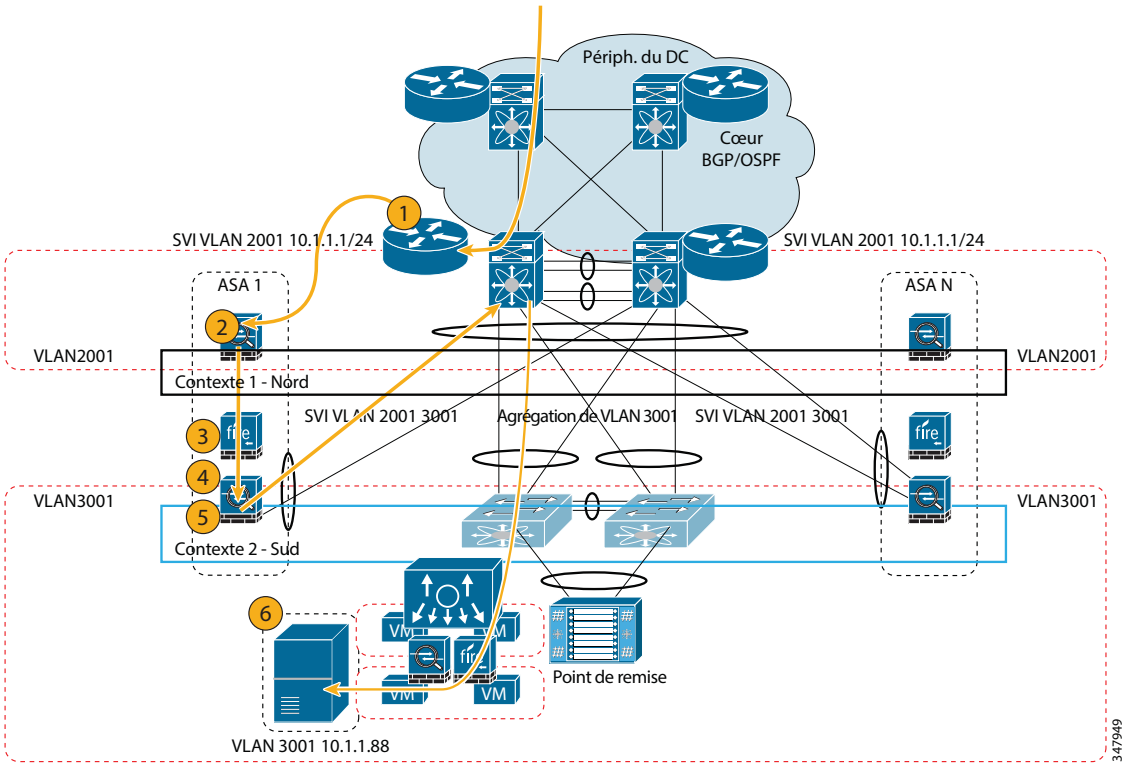
La Figure 33 illustre le flux de communication via le cluster ASA 5585-X avec l'appliance FirePOWER déployé sans balises supplémentaires de VLAN attribuées.

Remarque Cette option n'est pas validée dans les guides de déploiement.

Le flux de paquets

1. Le paquet arrive sur SVI VLAN 2001-Requête ARP au serveur 10.1.1.88. L'appliance ASA répond avec l'adresse MAC de l'interface externe.
2. Le paquet passe par le contexte ASA 1 Nord pour aboutir à SF en utilisant l'interface physique destinée au contexte ASA 2 Sud. Les politiques des paquets qui arrivent sur le VLAN 2001 sur l'appliance ASA sont traitées sur celui-ci (propriétaire/directeur de mise en cluster) et ainsi de suite. Le flux symétrique est assuré pour cette session.
3. Le paquet est inspecté par l'appliance FirePOWER et est transféré à l'interface (externe/interne) du contexte ASA 2.
4. Le contexte ASA 2 traite la politique, réécrit la balise du paquet sur la liaison vers le VLAN 3001. Le paquet est renvoyé au commutateur Nexus 7K avec le VLAN 3001.
5. Le commutateur Nexus 7K transfère le paquet au serveur via le VLAN 3001.
6. Le paquet atteint le serveur 10.1.1.88.

Figure 33 Flux de paquets pour la paire de contextes de cluster ASA sans VLAN supplémentaires



L'échec à l'ouverture de l'IPS

Il est très important d'éviter le blocage du trafic en cas de panne d'un appareil. Le type de module suivant a été sélectionné en raison de la capacité du module d'interface à échouer « en ouverture » pour que le trafic ne soit pas bloqué. La bande passante de l'interface a été sélectionnée en raison de la configuration des ports de l'appliance ASA 5585-X et du commutateur Nexus 7000 associé :

- Interfaces à fibre optique double port 10GBASE MM avec fonctionnalité de contournement configurable

D'autres interfaces avec une fonctionnalité de contournement sont disponibles, mais elles peuvent ne pas être compatibles avec le débit de cette conception. Il s'agit des interfaces suivantes :

- Interface en cuivre quadruple port 1000BASE-T avec fonctionnalité de contournement configurable
- Interface à fibre optique quadruple port 1000BASE-SX avec fonctionnalité de contournement configurable
- Interface à fibre optique double port 40GBASE-SR4 avec fonctionnalité de contournement configurable (appareils 2U uniquement)

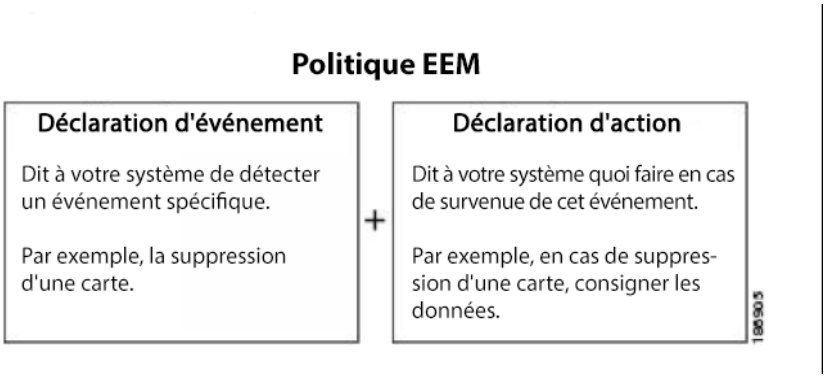
Notez que les plates-formes de la série 8200 proposent des modules Quadruple port 10G mais elles *ne prennent pas en charge* la fonctionnalité de contournement.

Le déploiement en option du gestionnaire d'événements intégré (EEM)

En cas de panne d'un appliance FirePOWER ou d'une liaison entre l'appliance ASA et l'appliance FirePOWER, il peut y avoir un délai de 9 secondes dans la vérification de l'état d'intégrité du cluster ASA avant que l'appliance ASA soit supprimé, ainsi que l'appliance FirePOWER, du cluster. Ce délai est dû à un mécanisme de récupération EtherChannel qui existe sur l'appliance ASA. Même si les interfaces connectant le VLAN 2101 ASA (Nord) et le VLAN 3101 ASA (Sud) à l'appliance FirePOWER sont des interfaces dédiées uniques, les interfaces de plan de données du cluster ASA doivent être placées dans un EtherChannel. Dans le cas présent, il s'agit d'un Ethernet à une seule liaison. Étant donné que les mécanismes de récupération EtherChannel sur l'appliance ASA utilisent des minuteurs pour permettre la récupération d'une liaison interrompue et la réintégrer au bundle de liaisons, ces minuteurs sont nécessaires. La valeur de temps par défaut (et minimale) des minuteurs est actuellement de 9 secondes pour la récupération de liaisons sur l'appliance ASA. Bien que ce minutage soit en cours de modification pour les versions futures du code ASA, il est possible d'éliminer facilement ce délai en utilisant le gestionnaire d'événements intégré (EEM) pour surveiller l'interface. Il est recommandé d'établir des liaisons secondaires, de tout débit, sur l'appliance ASA et l'appliance FirePOWER dans le commutateur Nexus 7000 en utilisant un VLAN isolé pour qu'un script EEM puisse détecter les pannes et procéder à la récupération immédiate de la liaison unique de cet EtherChannel.

EEM permet de surveiller les événements et d'adopter des mesures informelles ou correctives lorsque les événements surveillés se produisent ou lorsqu'un seuil est atteint. Une politique EEM est une entité qui définit un événement et les actions à entreprendre lorsque cet événement se produit (voir la Figure 34). Il existe deux types de politique EEM : un applet et un script. Un applet est une forme simple de politique qui est définie dans la configuration de l'interface de ligne de commande. Un script est une forme de politique qui est écrite en langage TCL (Tool Command Language).

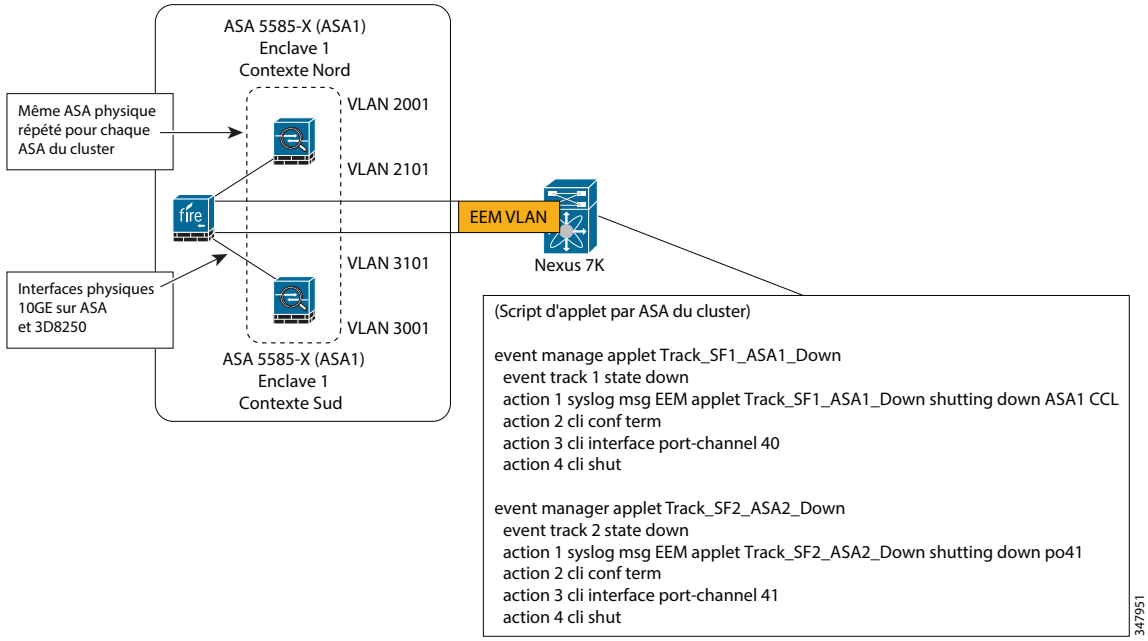
Figure 34 Politique EEM



Remarque Bien que l'appliance ASA mette en œuvre une version légère d'EEM, cette solution utilise l'EEM sur le commutateur Nexus 7000 qui met en œuvre une version intégrale d'EEM.

La Figure 35 montre l'appliance FirePOWER entre les contextes Nord et Sud pour l'enclave 1 avec une connexion supplémentaire au commutateur Nexus 7000 dans un VLAN EEM dédié. Une fois la connexion établie, il suffit de configurer le commutateur Nexus 7000 avec un script EEM, tel que celui montré dans le diagramme, pour supprimer le délai de 9 secondes en cas de panne de l'appliance FirePOWER.

Figure 35 Déploiement EEM



Le flux associé aux défenses intégrées - Avant, pendant, après une attaque

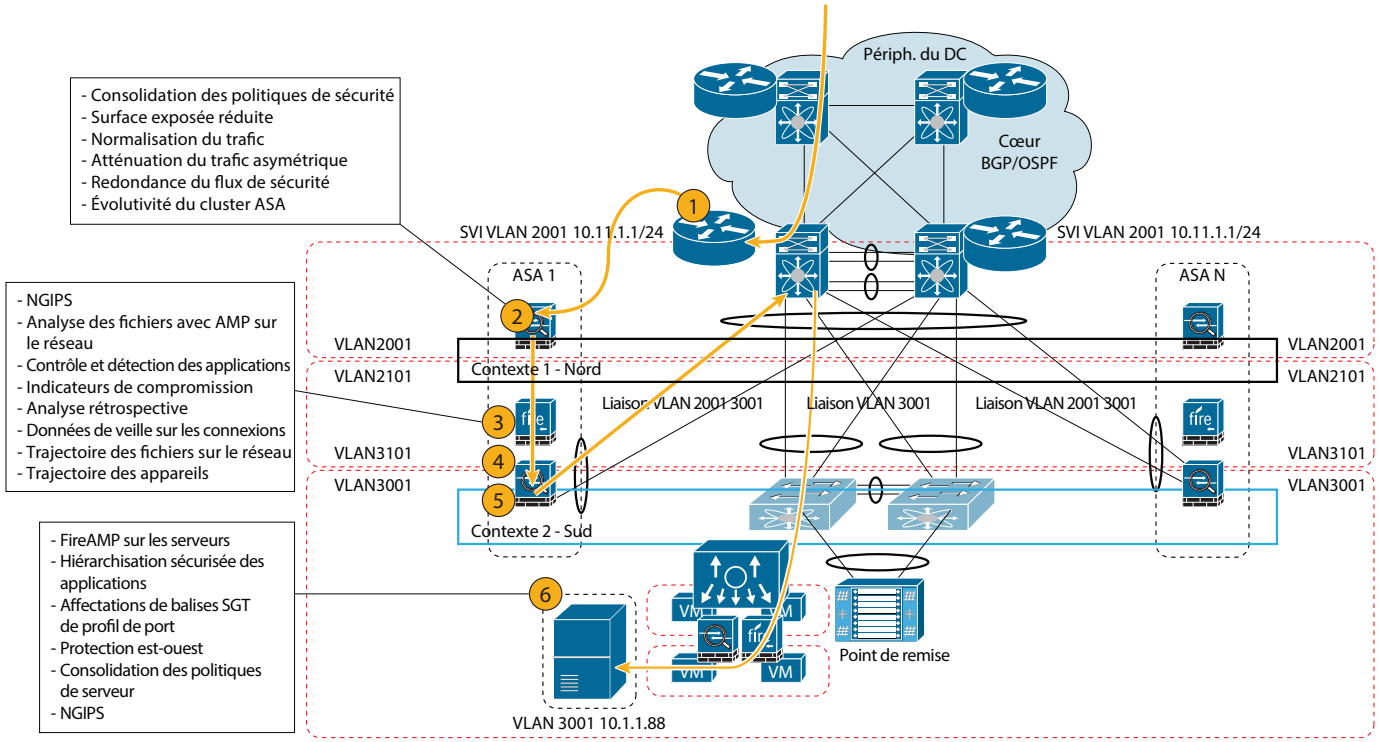
La Figure 36 montre un exemple de malware qui tente d'accéder à un serveur du data center à partir d'un terminal compromis en tirant profit du couplage de contextes de cluster ASA. Sur la figure, vous pouvez voir les éléments avant, pendant et après une attaque, à mesure qu'ils s'appliquent à l'option de déploiement « couplage de contextes de cluster ASA ». Le processus suppose qu'une connexion du Nord de la périphérie du data center tente d'accéder à un fichier ou une application sur un serveur cible dans la couche d'accès du data center.

Le flux de paquets

1. La requête au serveur 10.1.1.88 arrive sur le commutateur Nexus 7000. Les processus normaux de couche 3 et de couche 2 s'ensuivent et la requête est transmise au contexte ASA Nord pour traiter la politique sur le VLAN 2001.
2. L'appliance ASA applique la politique et vérifie que la source, la destination, les ports, les informations de balises SGT, etc., sont autorisés, ce qui réduit la surface d'exposition aux attaques. Une fois que la requête est confirmée comme étant autorisée, les balises des paquets sont réécrites sur la liaison vers le VLAN 2101 et les paquets sont transmis à la paire de clusters Sud en utilisant l'adresse MAC de l'IPS NextGen.
3. Les paquets de la requête sont traités par l'IPS NextGen, qui effectue la totalité des vérifications de sécurité en ligne, l'analyse et la gestion. Cette étape implique la mise à profit de tous les éléments et fonctionnalités du système de gestion des attaques, notamment la visibilité des applications, l'analyse des politiques de géolocalisation, la protection avancée contre les programmes malveillants (AMP), les indicateurs de compromission, le contexte des appareils, l'analyse de la trajectoire, etc. Si la situation initiale est correcte, les balises des paquets sont réécrites pour le VLAN 3101 et les paquets sont transmis à l'adresse MAC du contexte ASA Sud.
4. Les paquets arrivent sur le contexte ASA Sud et les politiques peuvent être revérifiées.

5. Une fois que les politiques sont confirmées, le contexte ASA Sud réécrit les balises des paquets pour le VLAN 3001 et transfère les paquets au commutateur Nexus 7000 pour les remettre au serveur de destination 10.1.1.88.
6. Une fois que les paquets arrivent dans la couche d'accès, l'architecture d'enclaves sécurisées assure la hiérarchisation sécurisée des applications, la sécurité est/ouest au niveau de l'hyperviseur, la sécurité d'enclave est/ouest via l'ASAv et l'appliance FirePOWER virtuel, le provisionnement automatisé et sécurisé des charges de travail, ainsi que le chaînage des services. L'AMP sur les terminaux peut également intervenir ici. Il est également possible de recourir aux affectations de balises SGT de profil de port si le commutateur Nexus 1000v est utilisé. Pour plus d'informations sur cette étape, consultez le guide de conception de l'architecture d'enclaves sécurisées.

Figure 36 Flux des attaques dans le couplage de contextes de cluster ASA – Avant, pendant et après une attaque



Avant
Politiques de contrôle d'incendie
Profils d'hôte
Listes blanches
Évaluation du niveau de sécurité des terminaux
Contrôles de conformité des terminaux
Contrôle des applications

Pendant
Détection des applicationsDétection SSL
Détection SSL
Détection et contrôle des données sensibles
Trajectoire des fichiers sur le réseau

Après
Trajectoire des fichiers sur le réseau
Détection SSL
Détection et contrôle des données sensibles
Trajectoire des fichiers clients
Application de notifications utilisateur

Pour plus d'informations sur chacun des composants, avant, pendant et après une attaque, reportez-vous à la section consacrée aux fonctionnalités du système de gestion des attaques plus loin dans ce document.

L'option 2 : appliances FirePOWER avec une conception passive

L'option 2, dans laquelle le système FirePOWER est utilisé avec un modèle de conception passive, offre une évolutivité optimale avec un impact de latence minime lorsque le déploiement doit tenir compte de l'encombrement physique en raison de la taille. En outre, cette option prévoit la surveillance des flux de trafic au niveau de la couche de virtualisation, ce qui est parfois recommandé.

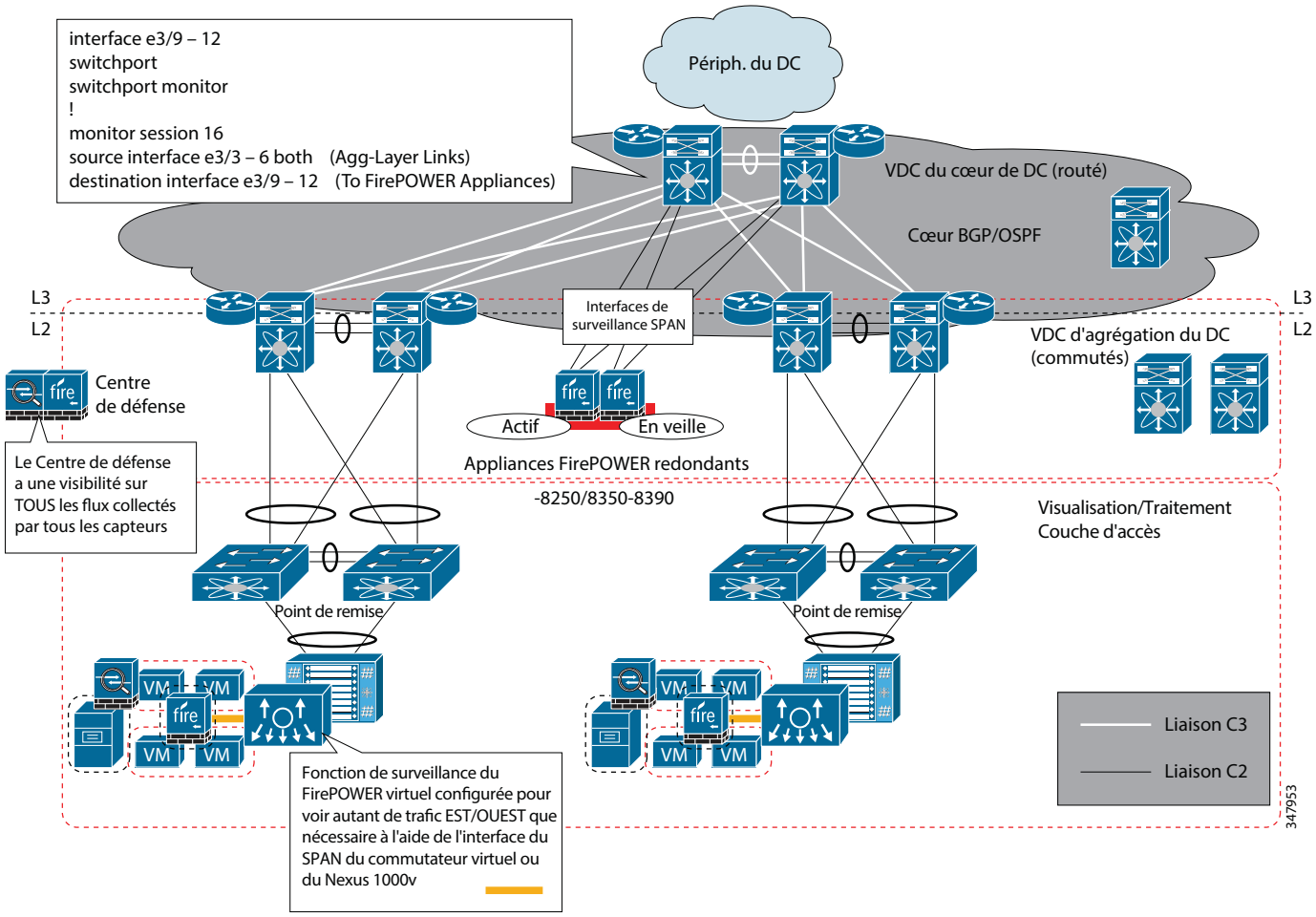
Les déploiements passifs n'ont pas la capacité de rejeter le trafic nuisible avant qu'il atteigne la cible désignée, mais lorsque la visibilité des attaques est primordiale, ils permettent de les contrer très efficacement, même manuellement. La conception passive offre cependant à la solution de sécurité du data center des fonctionnalités de sécurité incomparables à l'échelle du cluster ASA :

- La visibilité et le contrôle sur les applications avec OpenAppID™
- La catégorisation des URL et les indicateurs de compromission associés
- Les fonctionnalités de visibilité sur les terminaux et de contexte ainsi que les indicateurs de compromission associés de FireSIGHT™
- Un antivirus et une protection contre les programmes malveillants
- Un IPS NextGen avec les fonctionnalités de gestion avancée des menaces de FirePOWER™
- Advanced Malware Protection (AMP)
- Des options de gestion de l'identité des utilisateurs
- Le traitement analytique du Big Data dans le cloud et l'utilisation du service administré de protection contre les attaques de Cisco
- L'analyse de la trajectoire des fichiers et sur le réseau
- L'analyse ponctuelle et rétrospective (continue)
- La gestion des vulnérabilités
- La gestion des correctifs
- Des analyses

Dans la Figure 37, une paire redondante d'appliances FirePOWER est mise en œuvre dans une configuration active/de veille. Une session de surveillance SPAN est créée pour chacun des principaux commutateurs Nexus 7000. Nexus 7000 prend en charge jusqu'à 48 sessions de surveillance, et comme la plupart des autres commutateurs, il prend en charge plusieurs VLAN/interfaces source et de destination. En outre, il permet de surveiller les flux de trafic TX, RX, c'est-à-dire le trafic dans les deux sens. L'option, telle que présentée à la Figure 37, permet une visibilité sur l'ensemble du trafic qui passe par le cœur depuis ou vers toute couche d'agrégation ou la périphérie. En outre, il est possible de configurer les appliances FirePOWER en mode surveillance pour permettre la visibilité sur le trafic est/ouest depuis la couche d'accès. FireSIGHT Management Center surveille tous ces systèmes et constitue une source fiable et unique pour toutes les données collectées. L'exemple suivant prend en compte plusieurs types de panne : panne du châssis Nexus 7000, panne d'une liaison ascendante entre le cœur et la couche d'agrégation, panne de l'appliance FirePOWER ou panne d'une interface dans l'équation. Une configuration de base est présentée à la Figure 37. Pour plus d'informations sur la configuration SPAN sur le commutateur Nexus 7000, rendez-vous sur www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/113038-span-nexus-config.html.

La Figure 37 montre les flux nord-sud physiques et les flux est-ouest de la couche de virtualisation surveillés.

Figure 37 Solution passive IPS NextGen globale



Comme pour tous les déploiements IPS passifs, l'un des principaux points à prendre en compte est l'échelle. Si les liaisons sont fortement chargées, vous ne verrez vraisemblablement pas tout le trafic sur une liaison 10G entre le commutateur Nexus 7000 et les appliances FirePOWER. Il existe plusieurs possibilités pour garantir une visibilité complète, notamment ajouter des liaisons aux appliances FirePOWER, ajuster l'échelle si le déploiement est petit et facile à gérer ou encore utiliser des interfaces 40G sur les appliances FirePOWER. La Figure 37 montre qu'il existe un potentiel pour 80G de trafic total si toutes les liaisons principales sont des liaisons 10G. Ajustez la solution de surveillance en conséquence.

L'appliance FirePOWER haute disponibilité utilisé dans cet exemple est un système de base actif/en veille. Les deux appliances FirePOWER reçoivent une copie du trafic dans cette conception, mais seul le système actif crée des enregistrements d'événements dans FireSIGHT Management Center.

Option 3 : conception appliance FirePOWER virtuel et appliance ASA virtuel

L'option 1, dans laquelle le couplage de contextes de cluster ASA est utilisé, concernait un déploiement d'IPS NextGen utilisant un cluster ASA, étant donné que le déploiement a été effectué en tenant compte de l'encombrement physique en raison de l'échelle. L'option 3, gestion des attaques dans l'architecture d'enclaves sécurisées, continue à s'appuyer sur l'option de couplage de contextes de cluster ASA, le déploiement EEM, etc. ; mais en outre, cette conception utilise désormais les formats virtuels d'ASAv et de l'appliance FirePOWER virtuel dans les enclaves.

Remarque Pour des informations complètes sur l'architecture d'enclaves sécurisées, consultez la CVD qui lui est consacrée.

Cette section présente un résumé de l'option, car elle exploite le couplage de contextes de cluster ASA et les appliances ASAv, et les appliances ASAv offrent exactement la même protection intégrée. De plus, dans le cas de l'appliance FirePOWER virtuel, tous les workflows de gestion des menaces sont gérés par une plate-forme centralisée FireSIGHT Management Center. Comme l'option de couplage de contextes de cluster ASA, l'option de conception reposant sur les appliances ASA virtuel et FirePOWER virtuel tire parti d'un ensemble de fonctions de protection intégrées :

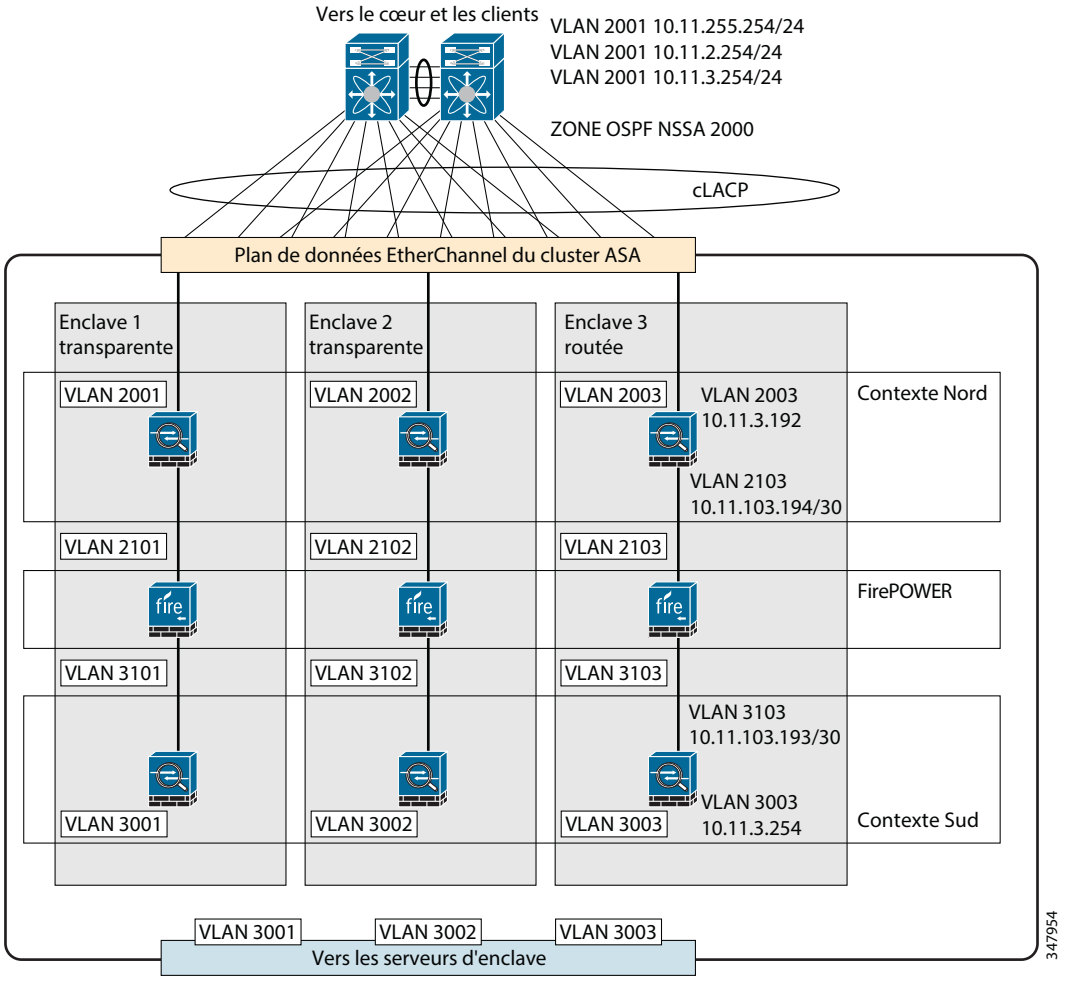
- La visibilité et le contrôle sur les applications avec OpenAppID™
- La catégorisation des URL et les indicateurs de compromission associés
- Les fonctionnalités de visibilité sur les terminaux et de contexte ainsi que les indicateurs de compromission associés de FireSIGHT™
- Un antivirus et une protection contre les programmes malveillants
- Un IPS NextGen avec les fonctionnalités de gestion avancée des menaces de FirePOWER™
- Advanced Malware Protection (AMP)
- Des options de gestion de l'identité des utilisateurs
- Le traitement analytique du Big Data dans le cloud et l'utilisation du service administré de protection contre les attaques de Cisco
- L'analyse de la trajectoire des fichiers et sur le réseau
- L'analyse ponctuelle et rétrospective (continue)
- La gestion des vulnérabilités
- La gestion des correctifs
- Des analyses
- Une fonctionnalité d'échec à l'ouverture ou à la fermeture pour le système IPS NextGen
- L'ensemble complet de fonctionnalités réseau avancées standard sur les ASA (reprise après sinistre et continuité de l'activité, notamment)
- L'intégration directe avec le composant virtuel d'architecture d'enclaves sécurisées

En outre, cette option de conception permet l'intégration avec les plates-formes de virtualisation :

- VXLAN
- Chaînage des services
- vMotion
- Mappage de balises SGT dans les profils de port

La Figure 38 montre un exemple de la gestion des menaces virtuelles dans l'architecture d'enclaves sécurisées. Vous pouvez remarquer qu'il existe des paires de VLAN pour chaque enclave, certaines enclaves sont routées et certaines sont transparentes. Notez également l'importance du composant de virtualisation.

Figure 38 Couplage de contextes de cluster ASA lié à l'architecture d'enclaves sécurisées



Les points à prendre en compte concernant les performances de l'appliance FirePOWER

Le Tableau 7 indique les performances de base de l'appliance FirePOWER. Bien que le tableau indique un débit de 10 Gbit/s pour un IPS 3D8250, en intégrant celui-ci dans le cluster ASA, le débit maximal passe à 160 Gbit/s, ce qui permet d'adapter le système en fonction de l'activité.

Tableau 7 Performances de l'appliance FirePOWER

Fonction	Performances
Débit IPS	10 Gbit/s
Débit IPS dans un cluster ASA 5585-X de 16 nœuds	160 Gbit/s
Pare-feu uniquement (pas d'IPS)	20 Gbit/s
Nombre de connexions TCP par seconde.	180 000
Nombre de connexions TCP par seconde dans un cluster ASA 5585-X de 16 nœuds	2 800 000

Tableau 7 Performances de l'appliance FirePOWER (suite)

Nombre de connexions TCP simultanées	12 000 000
Nombre de connexions TCP simultanées dans un cluster ASA 5585-X de 16 nœuds	96 000 000

Une faible latence

Bien que le déploiement avec la latence la plus basse soit un déploiement passif comme nous l'avons vu plus haut, les appliances FirePOWER peuvent être configurés pour une latence encore plus basse. Il est possible de parvenir à un équilibre entre la sécurité et un niveau de latence acceptable en établissant un seuil de latence des règles. Le seuil de latence des règles mesure le temps qu'il faut à chaque règle pour traiter un paquet, il suspend une règle et le groupe de règles associées pour une durée spécifiée si cette règle dépasse le seuil de latence un certain nombre de fois consécutives (ce nombre est configurable) et il restaure la règle au terme de la période de suspension.

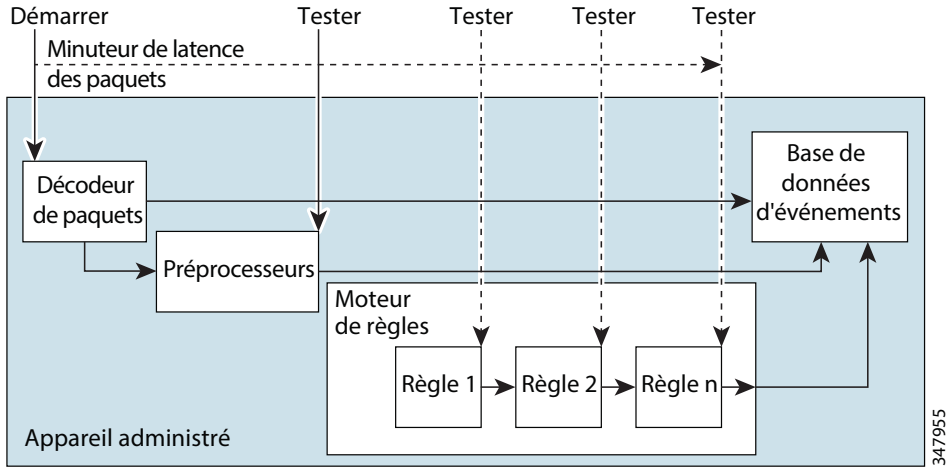
Le seuil de latence des règles mesure le temps écoulé, et pas seulement le temps de traitement, pour déterminer plus précisément le temps réel nécessaire à la règle pour traiter un paquet. Toutefois, le seuil de latence, qui est exécuté par un logiciel, n'implique pas un minutage strict.

Lorsque vous activez le seuil de latence de traitement des paquets, un minuteur se déclenche pour chaque paquet lorsque le processus de décodage commence. Le minutage continue jusqu'à la fin du traitement du paquet ou jusqu'à ce que le temps de traitement dépasse le seuil à un point de test.

Comme le montre la Figure 39, le minutage de la latence de traitement des paquets est testé aux points suivants :

- À l'issue du processus de décodage et de prétraitement et avant que la règle commence à traiter un paquet.
- Après le traitement effectué par chaque règle. Si le temps de traitement dépasse le seuil à un point donné, l'inspection du paquet cesse.

Figure 39 La latence des paquets



La détermination des seuils de latence des paquets permet d'améliorer les performances système dans les déploiements passifs et en ligne, et de réduire la latence dans les déploiements en ligne en supprimant l'activité chronophage d'inspection des paquets. Cas dans lesquels les performances peuvent être optimisées :

- Pour les déploiements passifs et en ligne, lorsque l'inspection séquentielle d'un paquet par de nombreuses règles prend énormément de temps ;
- Pour les déploiements en ligne, lorsqu'une baisse de performance du réseau, par exemple lorsque quelqu'un télécharge un fichier très volumineux, ralentit le traitement des paquets.

Les ports de communication

Certaines fonctionnalités des appliances FirePOWER nécessitent une connexion Internet et sont configurées par défaut pour se connecter directement à Internet.

En outre, certains ports doivent rester ouverts pour permettre une communication bidirectionnelle entre les appliances FirePOWER. Cette communication bidirectionnelle repose sur un canal de communication avec cryptage SSL et utilise le port 8305/TCP. Généralement, les ports associés à une fonctionnalité restent fermés jusqu'à ce qu'ils soient activés ou que la fonctionnalité associée soit configurée.

Les appliances FirePOWER autorisent les modifications des ports de communication, mais celles-ci doivent être effectuées avec précaution afin d'éviter toute incidence négative sur le déploiement. Par exemple, si vous bloquez le trafic sortant du port 25/TCP (SMTP) sur un équipement administré, ce dernier ne pourra pas envoyer d'e-mail de notification en cas d'intrusion.

Autre exemple, l'accès à l'interface web d'un équipement physique administré peut être désactivé en fermant le port 443/TCP (HTTPS), mais cela empêche également l'équipement d'envoyer les fichiers suspectés de contenir un programme malveillant dans le cloud en vue de leur analyse dynamique.

Les ports personnalisés peuvent être configurés pour une authentification LDAP et RADIUS lorsqu'une connexion est configurée entre le système et le serveur d'authentification. Le port de gestion (8305/TCP) peut être modifié, mais Cisco recommande vivement de conserver le paramètre par défaut. Si le port de gestion est modifié, il doit l'être pour tous les appliances FirePOWER du réseau qui doivent communiquer entre eux. Le port 32137/TCP peut être utilisé pour permettre aux appliances FireSIGHT Management Center de communiquer avec le cloud Sourcefire. Toutefois, Cisco recommande que le port de communication soit remplacé par le port 443.

Pour plus d'informations, consultez le tableau des ports de communication par défaut pour les opérations et les fonctionnalités du système 3D Sourcefire dans le *Guide d'utilisation du système 3D Sourcefire*.

Le réseau de gestion

Pour protéger FireSIGHT Management Center, l'appliance doit être installé sur un réseau de gestion protégé. Bien que FireSIGHT Management Center soit configuré pour disposer uniquement des services et des ports nécessaires, des mesures doivent être prises pour s'assurer qu'aucune menace extérieure au pare-feu ne puisse atteindre ni FireSIGHT Management Center, ni un autre équipement administré. Si FireSIGHT Management Center et ses équipements administrés résident sur le même réseau, les interfaces de gestion des équipements peuvent être connectées au même réseau de gestion protégé que FireSIGHT Management Center. Des mesures doivent être prises pour s'assurer que la communication entre les appliances FirePOWER ne puisse pas être interrompue, bloquée ou perturbée, par exemple via une attaque DDoS ou de l'homme du milieu.

SNMP

Il est possible d'interroger un appliance via SNMP (Simple Network Management Protocol) à l'aide de la politique système. La fonctionnalité SNMP prend en charge les versions 1, 2 et 3 du protocole SNMP. L'appliance n'enverra pas de traps SNMP en cas d'activation de la fonctionnalité SNMP de la politique système. Cela permettra uniquement au système de gestion du réseau d'interroger les informations contenues dans les MIB. L'accès SNMP doit être activé pour tous les ordinateurs qui interrogeront l'appliance. La MIB SNMP contient des informations qui pourraient être utilisées pour attaquer les appliances FirePOWER. Cisco recommande de limiter l'accès SNMP aux hôtes spécifiques qui seront utilisés pour interroger les données de la MIB. Sourcefire recommande également d'utiliser le protocole SNMPv3, ainsi que des mots de passe forts pour l'accès aux fonctionnalités de gestion du réseau.

La communication avec le cloud Cisco Sourcefire

L'appliance FirePOWER communique avec le cloud Cisco Sourcefire pour obtenir divers types d'informations :

- Si l'entreprise a souscrit un abonnement à FireAMP, le système peut recevoir des événements de programme malveillant au niveau des terminaux.
- L'association de politiques de fichiers et de règles de contrôle d'accès permet aux équipements administrés de détecter les fichiers transitant sur le réseau.
- FireSIGHT Management Center utilise les données du cloud Cisco Sourcefire pour savoir si les fichiers sont des programmes malveillants.
- Lorsque le filtrage des URL est activé, FireSIGHT Management Center peut récupérer les données de catégorie et de réputation de nombreuses URL courantes et effectuer des recherches sur les URL non classifiées.

Les mises à jour automatiques

Les mises à jour automatiques permettent au système de communiquer régulièrement avec le cloud Cisco Sourcefire pour mettre à jour les données des URL dans les jeux de données locaux des appliances FirePOWER. Même si le cloud met généralement ses données à jour une fois par jour, l'activation des mises à jour automatiques oblige FireSIGHT Management Center à vérifier toutes les 30 minutes qu'il dispose bien des dernières données disponibles. Les mises à jour quotidiennes sont souvent petites, mais si vous effectuez une mise à jour au bout de 5 jours, le téléchargement des nouvelles données de filtrage des URL peut prendre jusqu'à 20 minutes en fonction de la bande passante. Ensuite, la mise à jour en elle-même peut prendre jusqu'à 30 minutes.

Remarque Nous recommandons d'activer les mises à jour automatiques ou d'utiliser le planificateur pour planifier les mises à jour à intervalles réguliers afin d'avoir accès aux données d'URL les plus récentes et les plus pertinentes.

Le partage de données URI

FireSIGHT Management Center peut envoyer des informations sur les fichiers détectés sur le trafic réseau au cloud Cisco Sourcefire. Ces informations incluent des données URI relatives aux fichiers détectés et à leurs valeurs de hachage SHA-256. Même si le partage de ces informations n'est pas obligatoire, communiquer ces informations à Cisco facilitera l'identification et le suivi des programmes malveillants.

L'accès à Internet et la haute disponibilité

Le système utilise les ports 80/HTTP et 443/HTTPS pour communiquer avec le cloud Cisco Sourcefire et prend également en charge l'utilisation d'un proxy. Bien que toutes les configurations et informations de filtrage des URL soient synchronisées entre les différents appliances FireSIGHT Management Center dans un déploiement à haute disponibilité, seul l'appliance FireSIGHT Management Center principal télécharge les données de filtrage des URL. Si l'appliance FireSIGHT Management Center principal rencontre un problème, assurez-vous que l'appliance FireSIGHT Management Center secondaire a un accès direct à Internet et activez l'appliance FireSIGHT Management Center secondaire à partir de son interface web.

Deux appliances FireSIGHT Management Center administrés dans une paire haute disponibilité ne partagent ni les connexions cloud, ni les structures de programme malveillant. Pour assurer la continuité des opérations et la cohérence des structures de fichiers de programme malveillant détectés dans les deux appliances FireSIGHT Management Center (principal et secondaire), ces derniers doivent avoir accès au cloud.

Les fonctionnalités du système de gestion des menaces - Recommandations de conception

Une fois l'appliance FirePOWER correctement intégré au fabric, l'objectif est maintenant d'activer ses fonctionnalités et d'observer comment elles répondent aux menaces, aux différents stades des attaques. Vous trouverez dans les sections suivantes des conseils pour la conception des fonctionnalités. Une description du rôle de chaque fonctionnalité est donnée en fonction du stade de l'attaque. Certaines fonctionnalités s'appliquent à plusieurs stades, comme indiqué ci-après.

Le confinement et l'élimination des menaces

Les listes et les flux de sécurité adaptative - Stades de l'attaque : avant, pendant

Dans le cadre d'une politique de contrôle d'accès, la fonctionnalité de sécurité adaptative limite le trafic sur le réseau en fonction de l'adresse IP source ou de destination. Cela permet notamment de bloquer certaines adresses IP avant que le trafic ne soit analysé par les règles de contrôle d'accès. De même, certaines adresses IP peuvent être autorisées pour obliger le système à gérer leurs connexions via le contrôle d'accès.

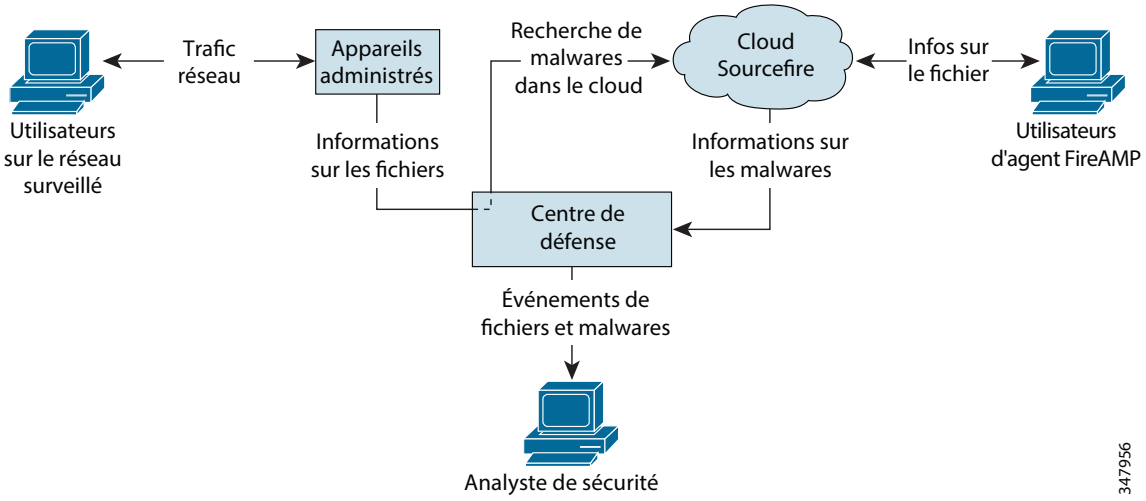
Une liste blanche et une liste noire globales sont incluses par défaut dans chaque politique de contrôle d'accès et s'appliquent à toutes les zones. En outre, dans chaque politique de contrôle d'accès, une liste blanche et une liste noire distinctes peuvent être créées à partir d'une combinaison de groupes et d'objets réseau ainsi que de listes et de flux de données de sécurité adaptative, et qui peuvent être limitées à une zone de sécurité spécifique.

Un flux de données de sécurité adaptative est un ensemble dynamique d'adresses IP que FireSIGHT Management Center télécharge depuis un serveur HTTP ou HTTPS selon un calendrier établi. Comme les flux sont régulièrement mis à jour, le système FirePOWER peut filtrer le trafic réseau à l'aide des dernières données disponibles. Pour faciliter la création de listes noires, Cisco propose une fonctionnalité de collecte de données de sécurité adaptative qui répertorie les adresses IP jugées peu fiables par l'équipe de recherche sur les vulnérabilités (VRT) de Sourcefire.

Fonctionnalité AMP installée sur le réseau - Stades de l'attaque : avant, pendant

La fonctionnalité AMP de protection avancée contre les programmes malveillants installée sur le réseau permet au système d'inspecter le trafic réseau pour détecter des programmes malveillants dans plusieurs types de fichier. Les appliances peuvent stocker les fichiers détectés sur leur disque dur ou dans un pack de stockage de programmes malveillants en vue d'une analyse approfondie. Que le fichier détecté ait été stocké ou non, il peut être envoyé au cloud Cisco Sourcefire pour vérifier si sa structure est connue à partir d'une recherche sur sa valeur de hachage SHA-256. Les fichiers peuvent également être soumis à une analyse dynamique qui génère un score de menace, comme expliqué ci-après. Ces informations contextuelles permettent de configurer le système de manière à ce qu'il bloque ou autorise certains fichiers. La configuration de la protection contre les malwares intervient dans le cadre de la configuration globale de contrôle d'accès. Les politiques de fichiers associées aux règles de contrôle d'accès analysent le trafic réseau en fonction des règles définies. La Figure 40 décrit les flux de communication entre le cloud Cisco Sourcefire, FireSIGHT Management Center, la fonctionnalité AMP installée sur le réseau et les terminaux.

Figure 40 Flux d'informations relatives aux programmes malveillants



FireAMP - Stades de l'attaque : avant, pendant

Bien que la protection des terminaux n'entre pas dans la conception de l'architecture de data center, le sujet est tout de même traité dans ce document, car les terminaux accèdent aux ressources du data center.

La solution professionnelle d'analyse et de protection avancées contre les programmes malveillants Cisco FireAMP détecte, analyse et bloque les programmes malveillants et les menaces persistantes avancés, ainsi que les attaques ciblées. Si l'entreprise a souscrit un abonnement à FireAMP, les utilisateurs doivent installer des connecteurs FireAMP sur leurs ordinateurs et terminaux mobiles. Ces agents légers communiquent avec le cloud Cisco Sourcefire, qui communique à son tour avec FireSIGHT Management Center. Une fois que FireSIGHT Management Center est configuré pour se connecter au cloud, son interface web est utilisée pour afficher les programmes malveillants détectés sur les terminaux suite à l'analyse et à la mise en quarantaine des terminaux. FireSIGHT Management Center utilise également les données FireAMP pour générer et suivre les indicateurs de compromission des hôtes, et afficher les trajectoires des fichiers sur le réseau.

Rendez-vous sur le portail FireAMP (http://amp.sourcefire.com/) pour configurer un déploiement FireAMP. Ce portail permet d'identifier rapidement les programmes malveillants et de les mettre en quarantaine. La solution FireAMP identifie les menaces au moment où elles surviennent, surveille leur trajectoire, analyse leurs effets et trouve une mesure corrective adaptée. Elle offre également la possibilité de créer des règles de protection personnalisées, de bloquer l'exécution de certaines applications en fonction de la politique de groupe et de créer des listes blanches personnalisées.

Les différences entre la solution AMP installée sur le réseau et les clients FireAMP installés sur les terminaux

Comme FireAMP procède à la détection des programmes malveillants au moment du téléchargement ou de l'exécution sur les terminaux alors que les équipements administrés détectent les programmes malveillants sur le réseau, les informations relevées sont différentes. Par exemple, les informations relatives aux malwares détectés sur les terminaux indiquent notamment le chemin du fichier invoquant l'application cliente, tandis que les informations détectées sur le réseau indiquent notamment le port, le protocole d'application et l'adresse IP d'origine de la connexion utilisée pour transmettre le fichier.

Autre exemple : pour les malwares détectés sur le réseau, les données concernant l'utilisateur sont celles de l'utilisateur qui s'est connecté en dernier à l'hôte destinataire du malware, tel qu'identifié au moment de l'analyse du réseau. De l'autre côté, les données concernant l'utilisateur recueillies par FireAMP sont celles de l'utilisateur actuellement connecté au terminal sur lequel a été détecté le malware, tel qu'identifié par le connecteur local.

Remarque Il est possible que les adresses IP des terminaux sur lesquels les malwares sont détectés ne figurent pas sur la carte du réseau et ne soient même pas surveillées sur le réseau, en fonction du déploiement, de l'architecture du réseau et du niveau de conformité, entre autres. En outre, il se peut que les terminaux sur lesquels sont installés les connecteurs ne figurent pas parmi les hôtes surveillés par les équipements administrés.

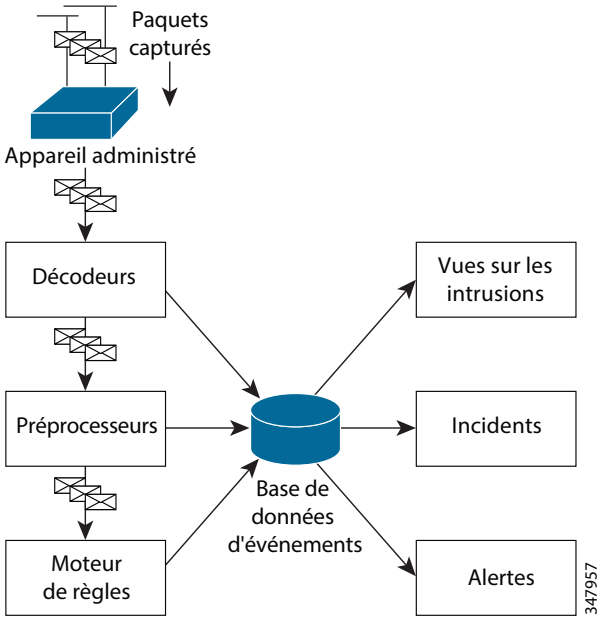
La détection et la prévention des intrusions - Stade de l'attaque : pendant

La fonctionnalité de détection et de prévention des intrusions est basée sur des politiques et intégrée aux règles de contrôle d'accès. Lorsqu'elle est déployée en ligne, elle analyse le trafic réseau à la recherche de brèches et bloque ou de modifie le trafic malveillant. Une politique de détection des intrusions comprend de nombreux éléments, notamment :

- Des règles qui analysent les valeurs d'en-tête des protocoles, le contenu des charges utiles et certaines caractéristiques relatives à la taille des paquets
- La configuration de l'état des règles en fonction des recommandations de FireSIGHT
- Des paramètres avancés, tels que des préprocesseurs et d'autres fonctionnalités de détection et de performance
- Des règles de préprocesseur qui peuvent générer des événements pour les préprocesseurs associés et les options de préprocesseur

Le système utilise la technologie Snort® primée pour analyser le trafic réseau et générer des événements d'intrusion qui signalent tout trafic non conforme à la politique de détection des intrusions en vigueur sur l'équipement qui surveille un segment de réseau spécifique. La Figure 41 décrit un flux d'inspection de base.

Figure 41 Flux d'inspection de base



Les opérateurs peuvent afficher les événements pour évaluer leur niveau d'importance par rapport au réseau. Éléments pouvant déclencher des événements d'intrusion :

- Un décodeur de couche de liaison, tel que le décodeur Ethernet II
- Un décodeur de couche réseau, tel que le décodeur IP
- Un décodeur de couche de transport, tel que le décodeur TCP
- Un préprocesseur ou un décodeur de couche d'applications, tel que le préprocesseur d'inspection HTTP
- Un moteur de règles

Les événements incluent diverses informations, notamment :

- La date et l'heure auxquelles l'événement a été généré
- Le niveau de priorité de l'événement
- Lorsque l'option de découverte du réseau est activée, l'indicateur d'impact associé à l'événement
- Si le paquet ayant déclenché l'événement a été ignoré ou aurait été ignoré dans un contexte de déploiement en ligne, commuté, ou routé
- Le nom de l'équipement qui a déclenché l'événement
- Le protocole du paquet qui a déclenché l'événement
- Le port et l'adresse IP source de l'événement d'intrusion
- Le port et l'adresse IP de destination de l'événement d'intrusion
- Le nom de l'utilisateur connecté à l'hôte source
- Le code et le type de protocole ICMP (pour le trafic ICMP)
- Le composant du système Cisco FirePOWER qui est à l'origine de l'événement (par exemple, le moteur de règles, le décodeur ou le préprocesseur)
- Une brève description de l'événement

- La catégorie de la règle à l'origine de l'événement
- Le VLAN auquel l'hôte appartient

FireSIGHT - Stades de l'attaque : pendant, après

La technologie de détection et de reconnaissance Cisco FireSIGHT collecte des informations sur les hôtes, les systèmes d'exploitation, les applications, les utilisateurs, les fichiers, les réseaux, les vulnérabilités et des données de géolocalisation. Cet ensemble complet de données offre une vue complète du réseau et permet un signalement fiable des indicateurs de compromission. FireSIGHT Management Center permet d'afficher et d'analyser les données collectées par FireSIGHT. Ces données peuvent également être utilisées pour appliquer le contrôle d'accès et modifier l'état des règles d'intrusion. En outre, les indicateurs de compromission des hôtes peuvent être suivis sur l'ensemble du réseau en fonction des données d'événement corrélées pour les hôtes. Le Tableau 8 répertorie tous les éléments sur lesquels FireSIGHT offre une visibilité.

Tableau 8 Visibilité offerte par FireSIGHT

Catégories	Échantillons	Cisco NGIPS et NGFW	IPS standard	NGFW standard
Menaces	Attaques, anomalies	Oui	Oui	Oui
Utilisateurs	AD, LDAP, POP3	Oui	Non	Oui
Applications web	Chat Facebook, Ebay	Oui	Non	Oui
Protocoles d'application	HTTP, SMTP, SSH	Oui	Non	Oui
Applications clientes	Firefox, IE6, BitTorrent	Oui	Non	Non
Serveurs réseau	Apache 2.3.1, IIS4	Oui	Non	Non
Systèmes d'exploitation	Windows, Linux	Oui	Non	Non
Routeurs et commutateurs	Cisco, Nortel, sans fil	Oui	Non	Non
Points d'accès sans fil	Linksys, Netgear	Oui	Non	Non
Terminaux mobiles	iPhone, Android	Oui	Non	Non
Imprimantes	HP, Xerox, Canon	Oui	Non	Non
Téléphones VoIP	Avaya, Polycom	Oui	Non	Non
Machines virtuelles	VMware, Xen	Oui	Non	Non

Les indicateurs de compromission - Stades de l'attaque : pendant, après

Le système peut établir une corrélation entre certains types d'intrusion, de programmes malveillants, ainsi que d'autres événements se produisant sur les hôtes du réseau pour identifier les hôtes potentiellement compromis et les marquer d'un indicateur de compromission (IoC). Les données IoC donnent une image claire et précise des menaces qui pèsent sur les hôtes du réseau surveillé.

Le système utilise toutes ces informations à des fins d'analyse, de profilage comportemental, de contrôle d'accès, mais aussi pour limiter et gérer les vulnérabilités et les attaques auxquelles doit faire face l'entreprise.

L'analyse dynamique des fichiers (sandboxing) - Stades de l'attaque : pendant, après

Pour optimiser l'analyse des programmes malveillants et l'identification des menaces sur les fichiers, des fichiers éligibles peuvent être envoyés au cloud Sourcefire en vue de leur analyse dynamique. Le cloud Cisco Sourcefire exécute le fichier dans un environnement test, et selon les résultats, renvoie un score de menace et un rapport récapitulatif de l'analyse dynamique à FireSIGHT Management Center. Les fichiers éligibles peuvent également être envoyés au cloud Cisco Sourcefire pour y subir une analyse Spero qui examine la structure des fichiers afin d'optimiser l'identification des programmes malveillants. L'envoi d'un fichier dans le cloud pour une analyse dynamique dépend du type de fichier, mais aussi de la taille minimale et maximale de fichiers autorisée dans la configuration de la politique de contrôle d'accès. Les fichiers peuvent être envoyés comme suit :

- Automatiquement en vue d'une analyse dynamique si une règle de fichier effectue une recherche de programme malveillant dans le cloud sur le fichier exécutable et si la structure du fichier n'est pas connue
- Manuellement jusqu'à 25 fichiers en même temps en vue d'une analyse dynamique si les fichiers sont enregistrés et si leur format est pris en charge (par exemple : documents PDF, Microsoft Office, etc.)

Une fois envoyés, les fichiers sont placés dans la file d'attente d'analyse dans le cloud. La liste des fichiers enregistrés et la trajectoire d'un fichier permettent de déterminer si un fichier a été envoyé en vue d'une analyse dynamique. Chaque fois qu'un fichier est envoyé en vue d'une analyse dynamique, le cloud analyse le fichier, même si la première analyse a généré des résultats. Le cloud effectue l'analyse dynamique en exécutant le fichier dans un environnement en sandbox. L'analyse cloud renvoie les éléments suivants :

- Le score de menace, qui représente le degré de probabilité qu'un fichier contienne un programme malveillant
- Un rapport récapitulatif de l'analyse dynamique, qui explique pourquoi le cloud a attribué ce score de menace

En fonction de la configuration de la politique de fichier, les fichiers dont le score de menace se situe au-dessus d'un seuil défini peuvent automatiquement être bloqués. Un examen plus approfondi du rapport récapitulatif de l'analyse dynamique permet de mieux identifier les programmes malveillants et d'ajuster les fonctionnalités de détection.

Les données de connexion - Stades de l'attaque : pendant, après

Les appliances FirePOWER surveillent en permanence le trafic généré par les hôtes sur le réseau. La fonctionnalité de contrôle d'accès peut être utilisée pour générer des événements de connexion lorsque le trafic réseau répond à certaines conditions. Les événements de connexion contiennent des données sur les sessions détectées, y compris les indicateurs horaires, les adresses IP, les données de géolocalisation, les applications, etc. Cas dans lesquels les politiques de contrôle d'accès consignent les événements de connexion :

- Le trafic réseau est sur liste noire ou surveillé par la fonctionnalité de données de sécurité adaptative, ce qui génère également des événements de sécurité adaptative
- Le trafic réseau répond aux conditions d'une règle de contrôle d'accès sans surveillance
- Le trafic réseau est géré par l'action par défaut d'une politique de contrôle d'accès
- Le trafic réseau répond aux conditions d'au moins une règle de surveillance (option activée automatiquement)
- Une politique de détection des intrusions associée à une règle de contrôle d'accès génère un événement (option activée automatiquement)

- Une politique de fichier associée à une règle de contrôle d'accès détecte ou bloque un fichier ou un programme malveillant (option activée automatiquement)

En associant la consignation des connexions à différentes configurations, politiques et règles de contrôle d'accès, vous bénéficiez d'un contrôle précis sur les connexions à consigner.

Les résumés de connexion - Stades de l'attaque : après

Cisco FirePOWER agrège les données de connexion collectées par tranches de 5 minutes en résumés de connexion que le système utilise pour générer des graphiques de connexion et des profils de trafic. Il est possible de créer des workflows personnalisés basés sur les données de résumé de connexion qui seront utilisés de la même manière que les workflows basés sur des événements de connexion spécifiques. Il n'existe pas de résumé de connexion spécifique aux événements de sécurité adaptative, même si des événements de fin de connexion associés peuvent être agrégés dans les données de résumé de connexion. Pour pouvoir être agrégées, les connexions doivent :

- Représenter les événements de fin de connexion
- Avoir les mêmes adresses IP source et de destination et utiliser le même port sur l'hôte de destination
- Utiliser le même protocole (TCP ou UDP)
- Utiliser le même protocole d'application
- Être détectées par le même appareil FireSIGHT administré ou exportées par le même appareil NetFlow. Chaque résumé de connexion inclut les statistiques du trafic global, ainsi que le nombre de connexions prises en compte dans le résumé.

Remarque : les résumés de connexion ne contiennent pas toutes les informations associées aux connexions agrégées. Par exemple, comme les données clientes ne sont pas utilisées pour agréger les connexions dans les résumés de connexion, elles ne sont pas incluses dans les résumés.

Le contrôle d'accès et la segmentation

L'association de la mise en cluster sur un seuil site avec TrustSec et de l'architecture d'enclaves sécurisées offre un ensemble complet de fonctionnalités de contrôle d'accès et de segmentation.

Le contrôle d'accès - Stades de l'attaque : avant, pendant

Une politique de contrôle d'accès détermine la manière dont le système gère le trafic sur le réseau. Plusieurs politiques de contrôle d'accès peuvent être configurées, puis appliquées à un ou plusieurs appliances FirePOWER. Une seule politique peut être appliquée par appareil.

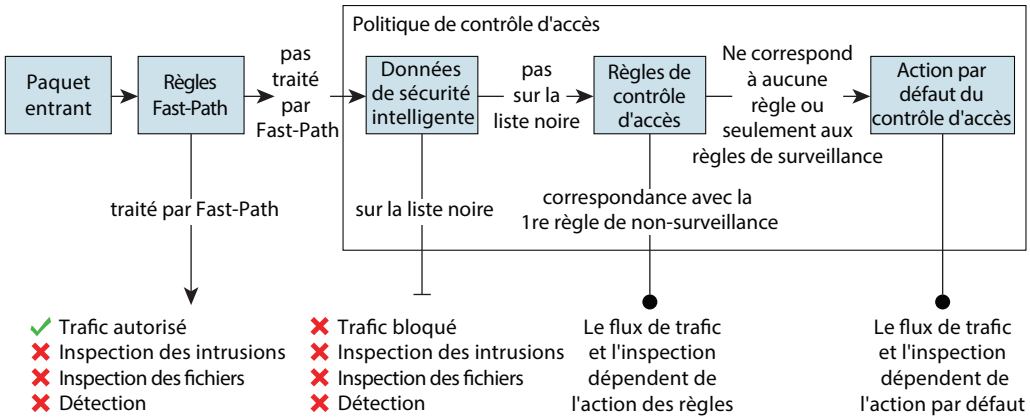
Une politique de contrôle d'accès standard filtre le trafic en fonction des données de sécurité adaptative, puis gère le trafic ne figurant pas sur la liste noire selon l'action par défaut sélectionnée :

- Bloquer l'ensemble du trafic à l'entrée du réseau
- Autoriser l'ensemble du trafic à accéder au réseau sans analyse approfondie
- Autoriser l'ensemble du trafic à accéder au réseau, puis analyser le trafic à l'aide d'une politique de découverte du réseau
- Autoriser l'ensemble du trafic à accéder au réseau, puis analyser le trafic à l'aide d'une politique de découverte du réseau et d'une politique de détection des intrusions

Des règles de contrôle d'accès peuvent être ajoutées à une politique pour offrir un contrôle précis de la gestion et de la consignation du trafic réseau. Chaque règle est associée à une action qui consiste à autoriser, surveiller, bloquer ou analyser le trafic correspondant à l'aide d'une politique de détection des intrusions ou de fichier. Chaque règle inclut un ensemble de conditions qui identifient la partie du trafic à surveiller. Les règles peuvent être simples ou complexes et associées à une partie du trafic combinant divers éléments (zones de sécurité, réseaux, VLAN, continent ou pays source ou de destination, utilisateurs ou groupes LDAP Active Directory, applications, ports de protocole de transport ou URL).

La Figure 42 décrit le flux de trafic transitant par l'appliance FirePOWER et les différentes inspections réalisées sur ce trafic. Notez que le système n'inspecte pas le trafic Fast-path ni le trafic sur liste noire. Pour le trafic traité par une action par défaut ou une règle de contrôle d'accès, le flux et le type d'inspection dépendent de l'action de la règle. Pour simplifier le schéma, nous n'y avons pas fait figurer les actions de règle. Cependant, il convient de préciser que le système n'exécute aucune inspection sur le trafic autorisé ou bloqué. De plus, l'inspection de fichier n'est pas prise en charge par l'action par défaut.

Figure 42 Schéma du flux de la politique de contrôle d'accès



La page de réponse HTTP - Stade de l'attaque : après

Lorsqu'une règle de contrôle d'accès bloque la requête HTTP d'un utilisateur, ce qui s'affiche dans le navigateur web de l'utilisateur dépend de la façon dont le système a été configuré pour bloquer la session. Lorsque vous choisissez une action de règle, sélectionnez :

- Blocage ou Blocage avec réinitialisation pour refuser la connexion. Lorsque la session bloquée expire, le système réinitialise les connexions « Blocage avec réinitialisation ». Pour les deux actions de blocage, la page du serveur ou du navigateur par défaut peut être remplacée par une page personnalisée expliquant que la connexion a été refusée.
- Blocage interactif ou Blocage interactif avec réinitialisation pour afficher une page de réponse HTTP qui avertit les utilisateurs et leur permet de cliquer sur un bouton pour continuer ou actualiser la page et accéder au site initialement demandé.

Les utilisateurs et administrateurs seront plus compréhensifs s'ils savent que le blocage du trafic intervient dans le cadre d'une politique de contrôle d'accès.

Les pages de réponse HTTP ne s'affichent pas pour tout trafic bloqué en raison de sa présence sur une liste noire de sécurité adaptative ou pour une application détectée à partir d'un certificat SSL.

La gestion de l'identité

Lorsqu'un appliance FirePOWER détecte une connexion, il transmet les informations suivantes à FireSIGHT Management Center qui les consigne en tant qu'activité utilisateur :

- Le nom d'utilisateur identifié au moment de la connexion
- L'heure de connexion
- L'adresse IP associée à la connexion
- L'adresse e-mail de l'utilisateur (pour les connexions POP3, IMAP et SMTP)
- Le nom de l'appareil qui a détecté la connexion. Si l'utilisateur a déjà été identifié auparavant, FireSIGHT Management Center met à jour l'historique de connexion de cet utilisateur.

FireSIGHT Management Center peut utiliser les adresses e-mail associées aux connexions POP3 et IMAP pour identifier les utilisateurs LDAP. Par exemple, si FireSIGHT Management Center détecte une nouvelle connexion IMAP et que l'adresse e-mail associée à cette connexion correspond à celle d'un utilisateur LDAP existant, le système ne crée pas de nouvel utilisateur, mais se contente de mettre à jour l'historique de cet utilisateur LDAP. Si l'utilisateur n'a jamais été identifié auparavant, FireSIGHT Management Center l'ajoute dans la base de données utilisateur. Les connexions uniques AIM, SIP et Oracle créent systématiquement de nouvelles entrées utilisateur, car elles ne contiennent aucune donnée que FireSIGHT Management Center puisse mettre en corrélation avec d'autres types de connexion.

Cas dans lesquels FireSIGHT Management Center n'enregistre pas l'activité ou l'identité de l'utilisateur :

- La politique de découverte du réseau est configurée pour ignorer ce type de connexion
- Un appareil administré détecte une connexion SMTP, mais la base de données utilisateur ne contient aucun utilisateur LDAP, POP3 ou IMAP associé à cette adresse e-mail

Cisco recommande l'installation des agents utilisateur Sourcefire sur tous les serveurs LDAP Microsoft Active Directory afin de pouvoir surveiller l'activité des utilisateurs via les serveurs Active Directory. Pour activer la fonctionnalité de contrôle des utilisateurs, les agents utilisateur Sourcefire doivent être installés afin que les utilisateurs puissent être associés aux adresses IP. Cela permet également le déclenchement des règles de contrôle d'accès basées sur les données utilisateur.

Un agent utilisateur Sourcefire peut surveiller l'activité des utilisateurs sur 5 serveurs Active Directory. Pour utiliser un agent, configurez une connexion entre chaque appliance FireSIGHT Management Center connecté à l'agent et les serveurs LDAP surveillés. Cette connexion permet non seulement de collecter les métadonnées des utilisateurs dont les connexions et les déconnexions ont été détectées par les agents utilisateur, mais aussi d'identifier les utilisateurs et les groupes à prendre en compte dans les règles de contrôle d'accès.

Le serveur LDAP fournit à FireSIGHT Management Center les informations et métadonnées suivantes pour chaque utilisateur :

- Nom d'utilisateur LDAP
- Nom et prénom
- Adresse e-mail
- Département
- Numéro de téléphone

La base de données des activités utilisateur contient des données relatives à l'activité des utilisateurs sur le réseau obtenues lors d'une connexion à un serveur LDAP Active Directory qui est également surveillé par un agent utilisateur Sourcefire, ou via la fonctionnalité de découverte du réseau.

Le système enregistre un événement :

- Lorsqu'il détecte une connexion ou une déconnexion
- Lorsqu'il détecte un nouvel utilisateur
- Lorsqu'un utilisateur est supprimé manuellement
- Lorsqu'il ne peut pas ajouter un nouvel utilisateur dans la base de données, car la limite autorisée par la licence FireSIGHT a été atteinte

La visibilité et le contrôle sur les applications

Les profils d'hôte - Stades de l'attaque : avant, pendant

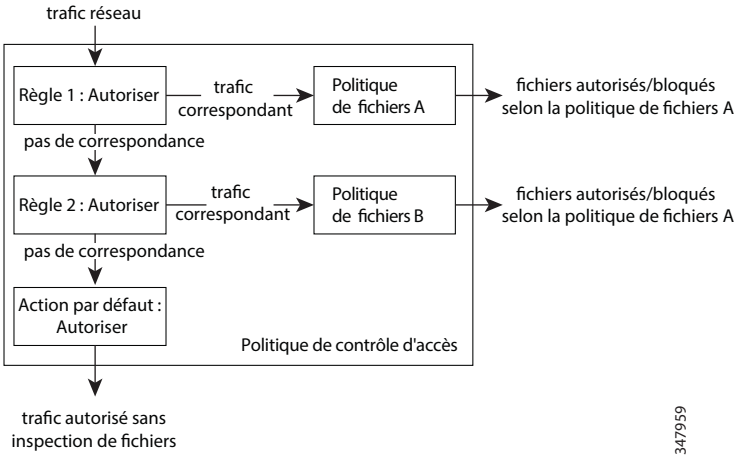
Un profil d'hôte offre une vue d'ensemble de toutes les informations collectées par le système de gestion FireSIGHT pour un hôte spécifique, notamment son adresse MAC, son nom d'hôte et son système d'exploitation. Il inclut également des attributs d'hôte qui représentent des données utilisateur associées à un hôte. Un attribut d'hôte peut par exemple indiquer dans quel bâtiment se trouve l'hôte. Le profil d'hôte vous permet d'afficher les attributs d'hôte associés à l'hôte et d'en modifier les valeurs. Les profils d'hôte contiennent également des informations relatives aux protocoles serveur, client et hôte exécutés pour un hôte donné, notamment s'ils figurent sur la liste blanche de conformité. Vous pouvez supprimer certains serveurs de la liste blanche et continuer à afficher les données associées.

D'autres informations sont disponibles, telles que les événements de connexion des serveurs, les données consignées pour la session au cours de laquelle le trafic serveur a été détecté, mais aussi les événements de connexion des clients, et les protocoles serveur, client et hôte supprimés à partir du profil d'hôte. Vous pouvez afficher l'historique d'un hôte si le système a été configuré pour consigner de telles données. Le profil d'hôte inclut une liste de vulnérabilités modifiable qui répertorie les vulnérabilités qui ont été corrigées pour l'hôte.

Le contrôle de fichier - Stades de l'attaque : avant, pendant

Le contrôle de fichier permet aux appareils administrés d'identifier et d'empêcher les utilisateurs de charger (envoyer) ou de télécharger (recevoir) certains types de fichier via certains protocoles d'application. Le contrôle de fichier peut être configuré dans le cadre de la configuration globale du contrôle d'accès en spécifiant des politiques de fichier à associer aux règles de contrôle d'accès. Une politique de fichier est un ensemble de configurations que le système utilise pour offrir une protection contre les programmes malveillants et un contrôle de fichier avancés dans le cadre de la configuration globale du contrôle d'accès. La Figure 43 décrit une politique de contrôle d'accès standard dans un déploiement en ligne.

Figure 43 Politique de contrôle d'accès standard



À l'instar de la politique de contrôle d'accès parente, une politique de fichier contient des règles qui déterminent comment le système traite les fichiers qui répondent aux conditions de chaque règle. Des règles de fichier spécifiques peuvent être configurées pour mettre en place différentes actions en fonction des types de fichier, des protocoles d'application ou des itinéraires de transfert. Lorsqu'un fichier répond aux conditions d'une règle, la règle peut :

- Autoriser ou bloquer le fichier en fonction de son type
- Bloquer le fichier en fonction de la structure du fichier de programme malveillant
- Stocker le fichier enregistré sur l'appareil
- Envoyer le fichier enregistré pour analyse dynamique

En outre, la politique de fichier peut :

- Traiter automatiquement un fichier en tant que fichier sain ou programme malveillant selon qu'il figure sur la liste de fichiers sains ou sur la liste de détection personnalisée
- Traiter un fichier en tant que programme malveillant si son score de menace dépasse le seuil configuré

Le Tableau 9 répertorie les composants d'une règle de fichier.

Tableau 9 Les composants d'une règle de fichier

Composant de la règle de fichier	Description
Protocole d'application	Le système peut détecter et analyser les fichiers transmis via FTP, HTTP, SMTP, IMAP, POP3 et NetBIOS-ssn (SMB).
Itinéraire de transfert	Le système peut inspecter le trafic entrant FTP, HTTP, IMAP, POP3 et NetBIOS-ssn (SMB) à la recherche de fichiers téléchargés (reçus). De même, il peut inspecter le trafic sortant FTP, HTTP, SMTP et NetBIOS-ssn (SMB) à la recherche de fichiers chargés (envoyés).

Tableau 9 Les composants d'une règle de fichier (suite)

Catégories et types de fichier	Le système peut détecter divers types de fichier appartenant à des catégories de base comme les fichiers multimédias (swf, mp3), les fichiers exécutables (exe, torrent) et les fichiers PDF.
Action de règle de fichier	L'action d'une règle de fichier détermine comment le système gère le trafic répondant aux conditions de la règle. Les règles de fichier s'exécutent par action de règle et non par ordre chronologique.

La détection des applications SSL - Stade de l'attaque : pendant

Le système FirePOWER intègre des détecteurs qui peuvent utiliser les informations d'une session SSL pour identifier le protocole d'application, l'application cliente ou l'application web de la session.

Lorsque le système détecte une connexion cryptée, il définit cette connexion comme une connexion HTTPS générique ou un protocole sécurisé plus spécifique tel que SMTPS. Lorsque le système détecte une session SSL, il ajoute le **client SSL** dans le champ Client des événements de connexion pour cette session. S'il identifie une application web pour la session, le système génère des événements de découverte pour le trafic.

Pour le trafic d'applications SSL, les appareils administrés exécutant la version 5.2 ou une version ultérieure peuvent également détecter le nom commun du certificat du serveur et trouver l'application cliente ou web correspondante à partir d'un modèle d'hôte SSL. Lorsque le système identifie un client spécifique, il remplace le **client SSL** par le nom du client identifié. Comme le trafic d'applications SSL est crypté, le système peut uniquement utiliser les informations du certificat à des fins d'identification et non les données applicatives dans le flux crypté. Cela explique pourquoi les modèles d'hôte SSL peuvent parfois uniquement identifier l'entreprise à l'origine de l'application et que les applications SSL produites par la même entreprise peuvent avoir le même identifiant.

La trajectoire de fichier sur le réseau - Stades de l'attaque : pendant, après

La fonctionnalité de trajectoire de fichier sur le réseau utilise les valeurs de hachage SHA-256 pour suivre le chemin de transfert d'un fichier sur le réseau.

Pour suivre la trajectoire d'un fichier sur le réseau, le système doit, au choix :

- Calculer la valeur de hachage SHA-256 du fichier et effectuer une recherche de programmes malveillants dans le cloud en utilisant cette valeur
- Collecter des données relatives à la mise en quarantaine du fichier et à la menace qu'il représente au niveau des terminaux via l'intégration de FireSIGHT Management Center à l'abonnement FireAMP de l'entreprise

Chaque fichier est associé à une carte des trajectoires qui présente visuellement les transferts d'un fichier au fil du temps, ainsi que des informations complémentaires sur le fichier.

La détection des applications - Stades de l'attaque : pendant, après

Lorsque FireSIGHT Management System analyse le trafic IP, il tente d'identifier les applications courantes utilisées sur le réseau. L'identification des applications est essentielle pour mettre en place un contrôle d'accès basé sur les applications. Le système détecte trois types d'application :

- Les protocoles d'application tels que HTTP et SSH
- Les applications clientes telles que les navigateurs web et les clients de messagerie
- Les applications web telles que les vidéos MPEG et Facebook

Pour identifier les applications dans le flux de trafic réseau, le système utilise soit les modèles ASCII ou hexadécimaux des en-têtes de paquet, soit le port utilisé par le trafic. Certains détecteurs d'applications utilisent à la fois le port et la détection par modèle pour augmenter les chances d'identifier correctement une application spécifique dans le trafic réseau.

Le système FireSIGHT comprend deux types de détecteur d'applications :

- Les détecteurs Sourcefire qui détectent les applications web, les applications clientes et les protocoles d'application
- Les détecteurs de protocole d'application basés sur l'utilisateur qui peuvent être créés pour optimiser les fonctionnalités de détection des protocoles d'application du système

Les protocoles d'application peuvent également être détectés via la détection implicite de protocole d'application qui implique l'existence d'un protocole d'application basé sur la détection d'un client. Le système de gestion FireSIGHT utilise un ensemble de caractéristiques pour créer des filtres d'applications qui peuvent être utilisés dans le cadre du contrôle d'accès, ainsi que pour filtrer les recherches, les rapports et les widgets du tableau de bord.

La détection des données sensibles - Stades de l'attaque : pendant, après

Les données sensibles telles que les numéros de sécurité sociale, les numéros de carte de crédit ou les numéros de permis de conduire peuvent circuler sur Internet avec ou sans l'accord de leur détenteur. Le système intègre un préprocesseur de données sensibles qui détecte et génère des événements pour les données sensibles en code ASCII qui s'avèrent particulièrement utiles pour détecter les fuites accidentelles de données.

Le système ne détecte pas les données sensibles cryptées, non visibles, ou dans un format compressé ou codé tel qu'une pièce jointe d'e-mail avec un codage Base64. Le système détecte les données sensibles par session TCP en identifiant les différents types de données du trafic. Les paramètres par défaut peuvent être modifiés pour chaque type de données et pour les options générales qui s'appliquent à tous les types de données dans la politique de détection des intrusions. Le système de gestion FireSIGHT intègre des types de données courantes prédéfinis et permet également de créer des types de données personnalisés. Une règle de préprocesseur de données sensibles est associée à chaque type de données. La détection des données sensibles et la génération d'événements peuvent être activées pour chaque type de données au moyen de la règle correspondante du préprocesseur. Le système utilise le prétraitement du flux TCP pour établir des sessions surveillées. Ainsi, le prétraitement du flux TCP doit être activé pour intégrer la détection des données sensibles à la politique de détection des intrusions.

Remarque La détection des données sensibles peut avoir un impact important sur les performances. Vous trouverez de plus amples informations sur le déploiement de cette fonctionnalité dans le *Guide d'utilisation du système Sourcefire FirePOWER*.

La gestion des journaux et de la traçabilité

L'accès à la base de données

FireSIGHT Management Center peut être configuré pour offrir un accès en lecture seule à la base de données à une application ou un client tiers. Notez que lorsqu'un client externe souhaite se connecter à la base de données, celui-ci doit utiliser le nom d'utilisateur et le mot de passe d'un administrateur ou d'un utilisateur externe de la base de données enregistré dans FireSIGHT Management Center.

Les limites d'événements de base de données

Pour optimiser les performances, configurez le nombre maximal d'événements de chaque type pouvant être stockés. Accédez à la page de la base de données et spécifiez le nombre maximal de chaque type d'événement que peut stocker FireSIGHT Management Center. Si le nombre d'événements dans la base d'enregistrement des événements d'intrusion dépasse la limite autorisée, les événements et les paquets les plus anciens sont supprimés jusqu'à ce que la limite soit à nouveau respectée. Les bases de données utilisateur et de découverte peuvent également être nettoyées manuellement. De plus, vous pouvez configurer une adresse e-mail pour recevoir une notification à chaque fois que des événements d'intrusion et des données d'audit sont supprimés de la base de données. Le Tableau 10 indique les nombres d'enregistrements minimaux et maximaux qui peuvent être stockés pour chaque type d'événement.

Tableau 10 Limites d'événements de base de données

Type d'événement	Nombre maximal d'événements	Nombre minimal d'événements
Événements d'intrusion	2,5 millions (DC500) 10 millions (DC1000, FireSIGHT Management Center virtuel) 20 millions (DC750) 30 millions (DC1500) 100 millions (DC3000) 150 millions (DC3500)	10 000
Événements de découverte	10 millions	zéro (stockage désactivé)
Événements de connexion / événements de sécurité adaptative	10 millions (DC500, DC1000, FireSIGHT Management Center virtuel) 50 millions (DC750) 100 millions (DC1500, DC3000) 500 millions (DC3500) Le nombre maximal d'événements inclut à la fois les événements de connexion et les événements de sécurité adaptative. La somme des limites maximales autorisées pour les deux types d'événement ne peut dépasser le nombre maximal d'événements.	zéro (stockage désactivé)
Résumés de connexion / (événements de connexion agrégés)	10 millions (DC500, DC1000, FireSIGHT Management Center virtuel) 50 millions (DC750) 100 millions (DC1500, DC3000) 500 millions (DC3500)	zéro (stockage désactivé)
Événements de la liste blanche de conformité et de corrélation	1 million	1
Événements de programme malveillant	10 millions	10 000
Événements de fichier	10 millions	zéro (stockage désactivé)
Événements d'état	1 million	zéro (stockage désactivé)

Tableau 10 Limites d'événements de base de données (suite)

Type d'événement	Nombre maximal d'événements	Nombre minimal d'événements
Données d'audit	100 000	1
Événements d'état de résolution	10 millions	1
Historique de violation de la liste blanche des hôtes sur votre réseau	30 jours d'historique	1 jour d'historique
Activités utilisateur (événements utilisateur)	10 millions	1
Connexions utilisateur (historique utilisateur)	10 millions	1
Entrées du journal d'importation de mise à jour des règles	1 million	1

Les journaux d'audit système

Les appliances du système FirePOWER créent une entrée dans le journal d'audit à chaque fois qu'un utilisateur communique avec l'interface web et enregistrent les messages d'état du système dans le journal système.

Les appliances de gestion FireSIGHT et les appliances FirePOWER administrés offrent également des fonctionnalités de reporting complètes qui permettent de générer des rapports pour la plupart des types de données accessibles pour un événement, notamment les données d'audit. Le journal d'audit peut stocker jusqu'à 100 000 entrées. Lorsque le nombre d'entrées du journal d'audit est supérieur à 100 000, l'appliance supprime les enregistrements les plus anciens de la base de données pour réduire le nombre d'entrées à 100 000.

L'envoi du journal d'audit

Vous pouvez configurer une politique système pour que l'appliance envoie un journal d'audit à un hôte externe. L'hôte externe doit être en état de fonctionnement et accessible par l'appliance qui transmet le journal d'audit. Si l'ordinateur censé recevoir le journal d'audit n'est pas configuré pour accepter les messages distants, l'hôte n'acceptera pas le journal d'audit.

Le journal système

La page du journal système (syslog) contient les informations du journal système de l'appliance. Le journal système répertorie toutes les informations relatives aux messages générés par le système dans l'ordre suivant :

- La date à laquelle le message a été généré
- L'heure à laquelle le message a été généré
- L'hôte qui a généré le message
- Le contenu du message

Remarque Les informations du journal système sont stockées localement. Par exemple, vous ne pouvez pas afficher les messages d'état du journal système d'un appliance FirePOWER à partir de FireSIGHT Management Center. Un filtre permet d'afficher uniquement les messages du journal système relatifs à certains composants.

NetFlow

Pour certains réseaux, les appliances FirePOWER détectent les enregistrements exportés par les appareils NetFlow, génèrent des événements de connexion à partir des données de ces enregistrements et envoient ces événements à FireSIGHT Management Center qui les consigne dans la base de données.

La solution de sécurité du data center inclut la CVD Protection du data center contre les cybermenaces, une solution basée sur le système Stealthwatch de Lancope et optimisée pour l'analyse des menaces sur les appareils NetFlow. Ce guide de conception n'a pas vocation à fournir des recommandations d'utilisation de NetFlow avec les appliances de gestion FireSIGHT et FirePOWER.

Résultats de la validation

Cette solution a été validée pour chacun des déploiements décrits dans ce document. Les détails de chaque déploiement et les données de validation associées figureront dans les guides de mise en œuvre.

Synthèse

Les équipes chargées des opérations du data center font face à un défi sans précédent en matière de cybersécurité. Depuis de nombreuses années, les cybercriminels ne cessent de développer de nouveaux stratagèmes qui leur permettent d'accéder, à tout moment, à tous les réseaux et à tous les équipements. La solution de sécurité du data center avec la technologie IPS NextGen de gestion des menaces fait partie d'un portefeuille de solutions plus vaste qui offre aux acteurs de la protection une gamme complète de fonctionnalités pour protéger leurs data centers tout en préservant l'efficacité et l'évolutivité des opérations.

Références

- Secure Data Center for the Enterprise : Single Site Clustering with TrustSec - www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/sdc-dg.pdf
- Secure Data Center for the Enterprise: Secure Enclaves Architecture
- Secure Data Center for the Enterprise : Cyber Threat Defense for the Data Center - www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-secure-data-center-portfolio/sea_ctd.pdf
- Guide d'utilisation du système 3D Sourcefire 60
- Guide d'installation du système 3D Sourcefire
- Guide de configuration du système de gestion Cisco Nexus 7000 Series NX-OS - www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg.pdf

- Rapport spécial NIST 800-53 révision 4, « Security and Privacy Controls for Federal Information Systems and Organizations » - www.nist.gov/manuscript-publication-search.cfm?pub_id=915447
- Présentation « Subvirt : Implementing Malware with Virtual Machines », Samuel T. King, Peter M. Chen, Université du Michigan - www.cse.psu.edu/~mcdaniel/cse544/slides/cse544-subvirt-sawani.pdf
- « Top 20 Critical Security Controls - Version 5 », SANS Institute - www.sans.org/critical-security-controls/
- « Find, Fix, Track, Target, Engage, Assess », John A. Tirpak - www.airforcemag.com/magazinearchive/pages/2000/july%202000/0700find.aspx