

Systèmes de prévention des intrusions TippingPoint

FICHE TECHNIQUE



Performance équivalente à celle d'un commutateur

- Filtrage des attaques à plusieurs Gigabit par seconde
 - TippingPoint 50 (50 Mbps)
 - TippingPoint 100E (100 Mbps)
 - TippingPoint 200 (200 Mbps)
 - TippingPoint 400 (400 Mbps)
 - TippingPoint 1200 (1,2 Gbps)
 - TippingPoint 2400 (2,0 Gbps)
 - TippingPoint 5000E (5,0 Gbps)
- Latence inférieure à 215 µs
- Sur un mix réaliste de transferts TCP/UDP
- Plus de deux millions de sessions simultanées
 - TCP/UDP/ICMP
- Plus de 750 000 connexions par seconde

Protection des clients et des serveurs

- Prévention des attaques contre les applications et systèmes d'exploitation vulnérables
- Evite les corrections de programmes coûteuses au coup par coup
- Blocage multi-mode des attaques

Protection de l'infrastructure du réseau

- Protection des infrastructures, IOS Cisco, serveurs DNS et autres
- Protection contre les anomalies de trafic, dénis de service, SYN Floods, Process Table Floods
- Listes de contrôle d'accès

Normalisation du trafic

- Extension de la bande passante et amélioration des performances des routeurs
- Normalisation des trafics invalides
- Optimisation des performances du réseau

Protection des performances des applications

- Extension de la bande passante et de la capacité des serveurs
- Limitation ou blocage des trafics indésirables
 - P2P / messagerie instantanée
- Bande passante garantie pour les applications critiques

Inoculation en temps réel par Digital Vaccine™

- Protection contre les attaques de type ZDE
- Distribution automatique des nouveaux filtres

Système d'administration de la sécurité

- Administration de plusieurs systèmes TippingPoint
- Tableau de bord instantané
- Reporting automatique
- Configuration et surveillance des équipements
- Définition de règles avancées et analyse a posteriori

Haute disponibilité et redondance dynamique

- Double alimentation
- Relocalisation au niveau 2
- Redondance dynamique active-active ou active-passive
- Haute disponibilité en tension nulle

Un niveau inégalé de sécurité et de performance

Jamais encore la sécurité n'avait été aussi puissante. Le système de prévention des intrusions (IPS) TippingPoint, leader du marché, n'a pas son pareil en termes de sécurité, de performance, de disponibilité et de simplicité d'emploi. Seul système de prévention des intrusions à avoir reçu le NSS Gold Award et la certification Common Criteria, entre autres récompenses, le système TippingPoint est LA référence en matière de prévention des intrusions sur le réseau.

Une sécurisation proactive

Comme leur nom l'indique, les systèmes de détection des intrusions se contentent de détecter les trafics indésirables, sans les bloquer. L'IPS TippingPoint, en ligne sur le réseau, bloque les trafics nuisibles et intempestifs, tout en laissant passer sans gêne le trafic sain. En fait, le système TippingPoint optimise les performances du trafic sain en nettoyant le réseau en permanence et en priorisant les applications critiques. Les performances des systèmes TippingPoint et leur extraordinaire précision dans la prévention des intrusions redéfinissent les normes de la sécurité des réseaux et modifient fondamentalement la manière dont les acteurs de l'entreprise protègent leur réseau.

Ainsi, il est désormais inutile de faire le ménage lorsqu'une cyber-attaque contamine vos serveurs et vos stations de travail. Finis les patches appliqués en urgence ou au coup par coup. Oubliées les applications dévoyées incontrôlables, comme le P2P et la messagerie instantanée, endémiques sur le réseau. Reléguées aux oubliettes de l'histoire les dénis de service qui asphyxient vos connexions Internet et bloquent vos applications critiques.

Les solutions TippingPoint réduisent continûment le coût de la sécurisation de vos réseaux informatiques en vous évitant les patches et en réagissant aux alertes à votre place. Elles améliorent inlassablement la productivité et la rentabilité de vos systèmes informatiques en préservant la bande passante et en protégeant les applications critiques.

« TippingPoint a une vision exceptionnelle de la prévention des intrusions. »

Eric Ogren, Yankee Group

Des performances hors pair

Les produits TippingPoint sont les plus performants du marché. Pour bloquer les cyber-attaques à des vitesses de plusieurs gigabits, vous avez besoin d'un matériel dédié, et seul TippingPoint s'est engagé dans le développement de l'architecture révolutionnaire nécessaire à une véritable prévention des intrusions.

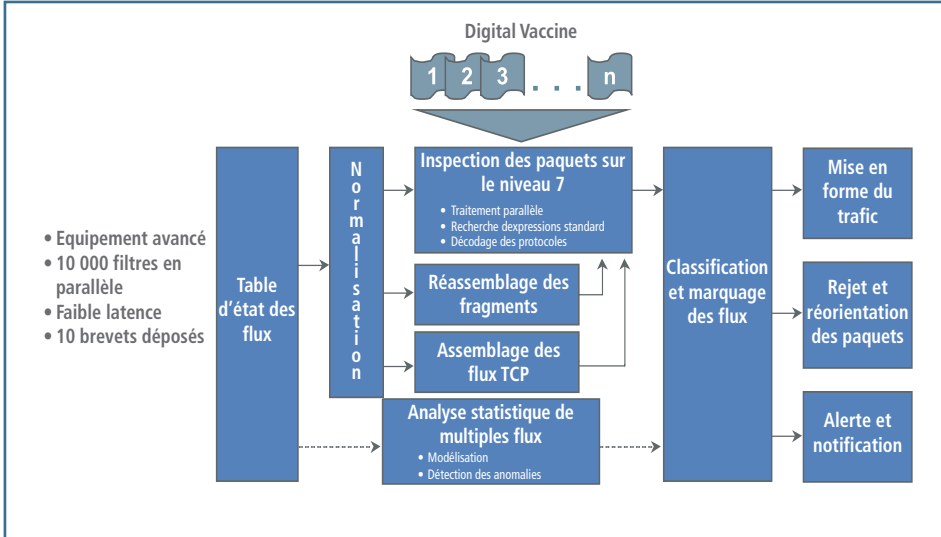
Les solutions classiques, tant logicielles que matérielles, fonctionnent à partir d'équipements et de processeurs généralistes : elles sont tout bonnement incapables de fonctionner sans nuire aux performances du réseau. Par des tests rigoureux, réalisés par des cabinets indépendants, les systèmes TippingPoint ont prouvé leur capacité à prévenir les intrusions à une vitesse de plusieurs gigabits et avec une précision hors du commun. La plate-forme TippingPoint a largement démontré qu'elle est la plus performante et la plus sûre du marché pour la prévention des intrusions.

« Dès que nous avons installé le système TippingPoint sur notre réseau, et presque sans configuration, les attaques dont nos accès par modem câble étaient la cible ont cessé. Je n'avais jamais imaginé pouvoir fournir un tel niveau de protection à nos abonnés haut débit. »

André Foster, vice-président, IT Cable Bahamas

Le moteur de suppression des risques
 Le moteur de suppression des risques (baptisé TSE), un ASIC TippingPoint, a révolutionné la sécurisation des réseaux. Grâce à des processeurs pipelinés et

Une sécurité totale
 De par leurs performances exceptionnelles, les systèmes TippingPoint assurent une sécurisation sans compromis. Ils réalisent une inspection exhaustive des flux de paquets, jusqu'au niveau 7, pour épurer en permanence les trafics Internet et intranet et éradiquer avec la plus grande précision les attaques (vers, virus, chevaux de Troie, menaces mixtes, dénis de service, saturations, portes dérobées, « Walk-in Worms »*, captages de bande passante) avant qu'elles en provoquent des dommages. TippingPoint protège l'infrastructure du réseau en bloquant les attaques contre les routeurs, les commutateurs, les serveurs de DNS et autres équipements d'infrastructure.



*Walk-in Worm : ver qui se répand de l'intérieur du réseau à partir d'un ordinateur portable infecté.

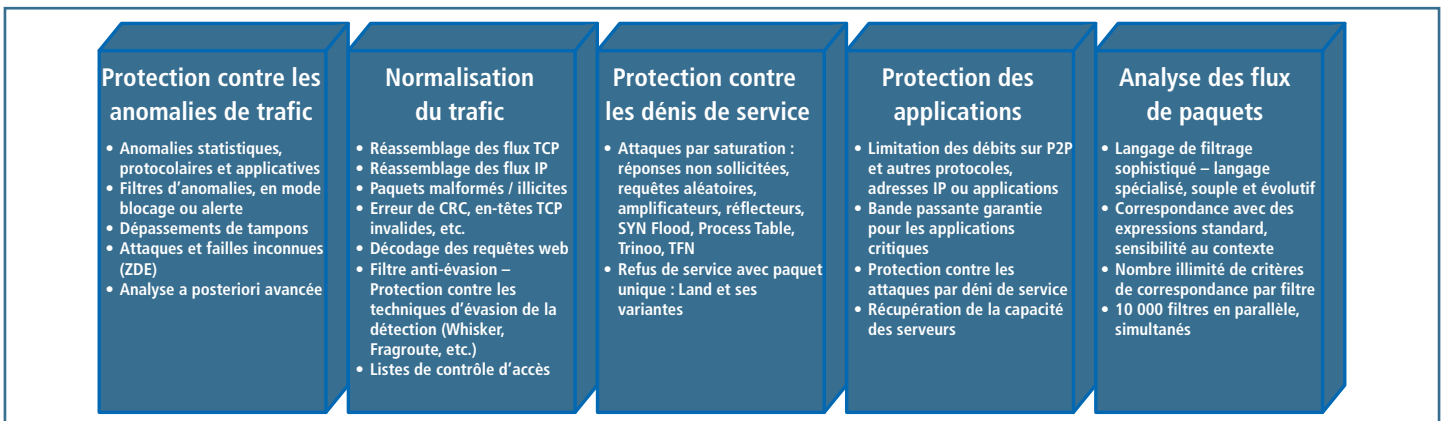
« TippingPoint a si bien bloqué le virus Sobig, (alors que nous étions encore en phase d'évaluation du produit) que nous avons immédiatement acheté plusieurs systèmes afin de protéger l'ensemble de notre réseau. »

John Oberlin, vice-président, IT University, Caroline du Nord

massivement parallèles, le TSE effectue simultanément des milliers de contrôles sur chaque flux de paquets. L'architecture du TSE utilise des ASIC dédiés, un fond de panier tournant à 20 Gbps et des processeurs réseaux hautes performances pour réaliser une inspection complète des paquets sur les niveaux 2 à 7. Les traitements parallèles assurent la progression des flux de paquets dans l'IPS, ne provoquant qu'une latence inférieure à 215 microsecondes, quel que soit le nombre de filtres appliqués.

Cette architecture permet également la classification du trafic et la mise en forme des débits. Des algorithmes sophistiqués modélisent le trafic « normal », permettant de définir des seuils et des régulateurs automatiques qui assureront le traitement prioritaire des applications critiques sur le réseau.

Par le traitement des anomalies statistiques, protocolaires et applicatives, les systèmes TippingPoint protègent le réseau des pointes de trafic et des dépassements de tampons, mais aussi des attaques et des failles inconnues. Ils assurent la normalisation du trafic et éliminent les paquets malformés ou illicites, réassemblent les paquets TCP et défragmentent les paquets IP, élargissant ainsi la bande passante du réseau qu'ils défendent contre les techniques d'évasion. Les systèmes TippingPoint peuvent également se comporter comme un firewall et remplacer les listes de contrôle d'accès des routeurs et des commutateurs, particulièrement gourmandes en traitements. De plus, en limitant la bande passante utilisée par les trafics indésirables, voire en les bloquant totalement, les systèmes TippingPoint préservent la bande passante et la capacité des serveurs et assurent aux applications une protection complète. Ils offrent :

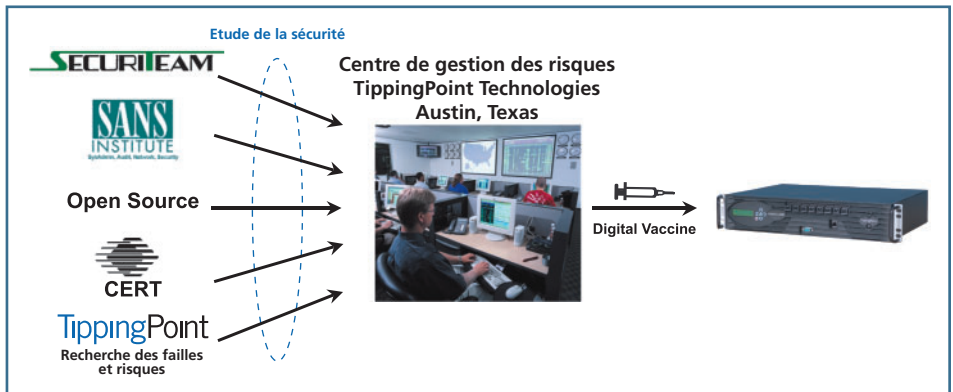


Une évaluation des vulnérabilités de classe internationale
 L'équipe Sécurité de TippingPoint propose la meilleure analyse des vulnérabilités du marché. TippingPoint est le principal contributeur au bulletin électronique @RISK coordonné par le SANS Institute et qui regroupe les dernières informations sur les failles de sécurité des réseaux. Diffusé tous les jeudis auprès de quelques 300 000 abonnés dans le monde, pour la plupart spécialistes de la sécurité des réseaux, @RISK décrit les dernières failles découvertes, explique leur impact et les actions qu'ont initié les grandes entreprises pour protéger leurs utilisateurs. @RISK peut être obtenu gratuitement sur <http://www.sans.org/newsletters/risk/>.

Une inoculation en temps réel avec Digital Vaccine
 Pour une sécurité totale, TippingPoint propose une prévention continue contre les nouvelles failles. En plus de fournir son analyse des vulnérabilités chaque semaine au SANS Institute, l'équipe Sécurité de TippingPoint développe de nouveaux filtres contre les risques découverts et les incorpore à ses mises à jour Digital Vaccine. Ces filtres sont conçus pour combattre à la fois des risques spécifiques et leurs permutations potentielles, protégeant ainsi leurs utilisateurs des attaques de type ZDE. Digital Vaccine est envoyé à nos clients chaque semaine, ou dès l'apparition d'une faille critique, et peut être déployé automatiquement, sans intervention de l'utilisateur.

Ce service unique en son genre redonne de l'efficacité aux correctifs de sécurité. Inutile en effet d'installer ces correctifs en urgence ou au coup par coup : le personnel informatique peut ne les appliquer que lorsque c'est nécessaire et à des moments prévus et prévisibles.

L'administration à l'échelle de l'entreprise
 Les solutions TippingPoint incluent une administration de pointe, avec des fonctions aussi puissantes que conviviales. Le système d'administration de la sécurité (SMS) de TippingPoint est une appliance renforcée permettant la visualisation et le contrôle de multiples systèmes TippingPoint. Il couvre l'identification, la surveillance, la configuration, le diagnostic et le reporting pour un millier de systèmes TippingPoint. Equipement rackable, le SMS TippingPoint comprend une interface client Java sécurisée et ultramoderne permettant d'effectuer une analyse globale des statistiques de trafic, des attaques filtrées, des hôtes et des services du réseau, de l'inventaire et de l'état des IPS,



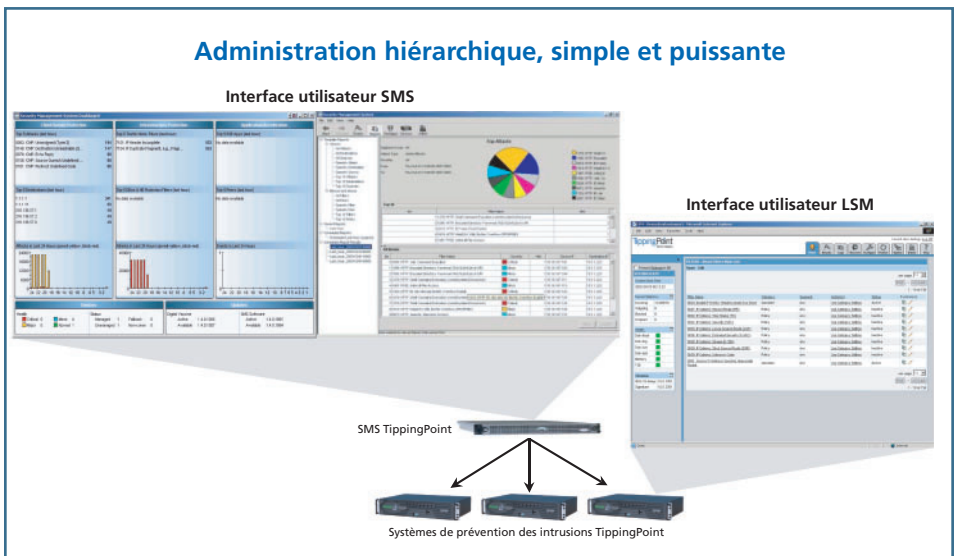
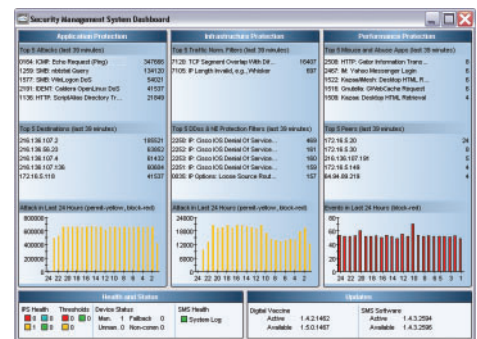
avec rapports de tendances, corrélation et graphiques en temps réel.

En proposant un modèle opérationnel évolutif basé sur des règles, le SMS TippingPoint permet d'administrer en direct les déploiements d'IPS les plus vastes. Un déploiement TippingPoint sur le réseau regroupera en général plusieurs clients SMS (Java sécurisé), un SMS (Security Management System) central et de multiples systèmes TippingPoint.

Elément majeur du SMS TippingPoint, le tableau de bord SMS inclut des fonctions de surveillance visuelle et permet le lancement d'applications d'administration externes. Ce tableau de bord affiche en temps réel une vue d'ensemble des performances de l'ensemble des systèmes TippingPoint du réseau, notifications de mises à jour et des problèmes réclamant attention comprises.

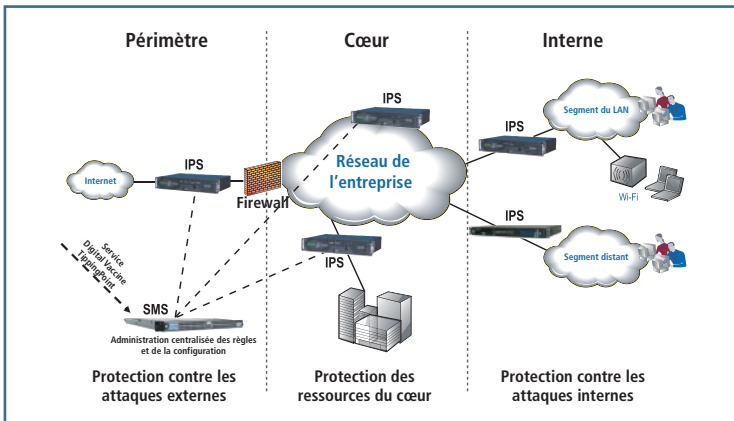
De plus, chaque IPS est fourni avec une interface LSM (Local Security Manager) embarquée et une interface par ligne de commande (CLI). LSM est une application graphique pour l'administration, la configuration et le reporting, présentée sous la forme d'une interface web simple d'emploi et sécurisée.

« Puissant et souple, le système d'administration est aussi simple d'emploi et intuitif. L'éditeur de profils est le meilleur que nous avons rencontré sur des équipements d'IPS/IDS. »
 Bob Walder, président, NSS Group



Un déploiement simplifié
De par sa conception, l'IPS TippingPoint est transparent vis-à-vis du réseau :

- L'IPS TippingPoint se déploie en toute transparence sur le réseau, sans adresse IP ou MAC, et commence immédiatement à filtrer les trafics nuisibles et indésirables.



- La rapidité et la faible latence de l'IPS permettent son installation à la périphérie comme au cœur du réseau, qu'il protège contre les menaces externes.

Deuxièmement, des horloges de surveillance contrôlent en permanence les moteurs de sécurisation et d'administration. En cas d'erreur interne, le système TippingPoint peut revenir automatiquement ou manuellement à l'état de simple équipement de niveau 2, configurable par segment. De plus, pour les câblages cuivre, TippingPoint propose une option haute disponibilité en tension nulle (ZPHA). En cas de coupure totale du courant sur le centre de données, les interfaces peuvent s'appuyer sur le relais externe ZPHA pour transmettre l'ensemble du trafic.

Redondance dynamique du réseau
La haute disponibilité peut être obtenue par l'association transparente de deux IPS TippingPoint. L'IPS, simple « accroissement du câble », n'a pas d'adresse IP et ne prend pas part aux protocoles de routage, aussi les systèmes TippingPoint peuvent-ils être déployés par paire, dans des configurations haute disponibilité, sans modification de la configuration du réseau. Les protocoles de routage haute disponibilité tels que VRRP (Virtual Router Redundancy Protocol), OSPF (Open Shortest Path First) et le HSRP (Hot Standby Router Protocol) de Cisco, sont transférés en toute transparence par l'IPS et fonctionnent aussi bien avec ou sans IPS en

« Un véritable baptême du feu. En des temps de catastrophe météorologique, le trafic sur le site peut augmenter brutalement, et nous voulons être certains que tous les équipements, réseau ou infrastructure, que nous installons sont capables de gérer la surcharge. »

Dan Agronow, vice-président, Technologies, Weather.com

des infrastructures critiques, isole les attaques et détecte les équipements vulnérables du réseau.

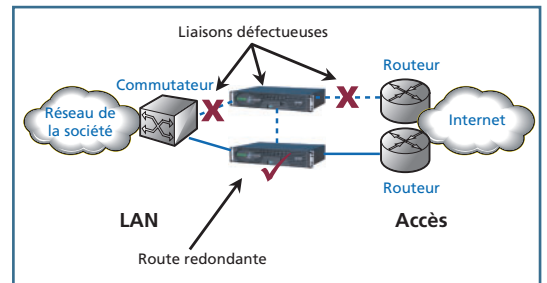
- Les paramètres « recommandés », soigneusement étudiés, permettent un déploiement instantané, dès le déballage de l'appareil, sans intervention manuelle.

La haute disponibilité

En terme de haute disponibilité, les systèmes de prévention des intrusions TippingPoint n'ont pas leur pareil. Les IPS TippingPoint sont conçus pour garantir que le trafic s'écoule à vitesse filaire en permanence, même en cas d'erreur du réseau ou d'un

équipement interne, voire de coupure totale de l'alimentation électrique. Deux modes de fonctionnement en haute disponibilité supplémentaires, baptisés Haute disponibilité intrinsèque et Redondance dynamique du réseau, assurent une disponibilité maximum.

Diverses fonctions intégrées assurent la haute disponibilité intrinsèque. En premier lieu, tous les systèmes TippingPoint sont équipés de deux alimentations échangeables à chaud.



ligne. La paire de systèmes TippingPoint peut être configurée en mode Actif-Actif ou Actif-Passif, de manière à partager comme il se doit les informations d'état afin que la protection reste totalement opérationnelle pendant et après une panne de réseau.

Une haute disponibilité intrinsèque

