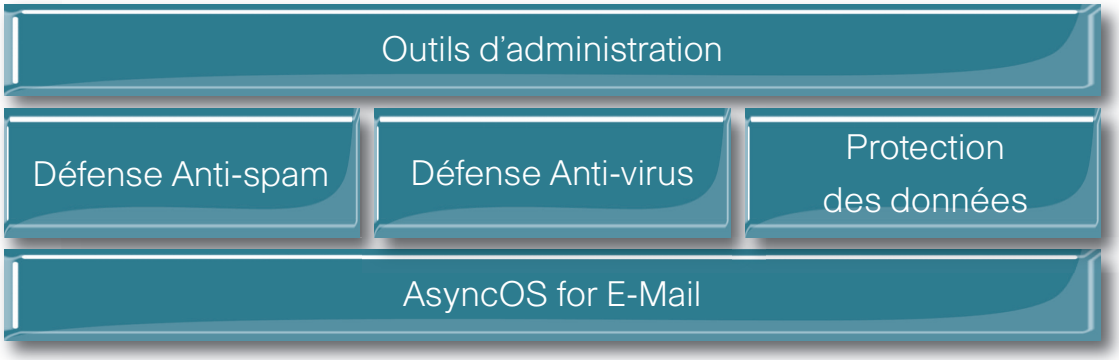
Cisco IronPort C Series

Spam, malware, phishing... les menaces véhiculées par le courrier électronique ne cessent de proliférer. Cette tendance se traduit par des attaques non seulement en nombre croissant, mais aussi de plus en plus complexes et professionnelles. C'est ainsi que 180 milliards de messages de spam sont envoyés par jour en moyenne. De nombreuses entreprises rapportent que d'ores et déjà plus de 90% des messages qu'elles reçoivent sont indésirables. Alors que les spams renfermaient traditionnellement des codes malveillants dans des pièces jointes, par exemple au format PDF, Excel ou MP3, la plupart d'entre eux comportent aujourd'hui une simple lien vers un site Internet infecté. Les e-mails entrants ne constituent toutefois qu'un aspect du problème, car des données sensibles d'une entreprise peuvent également parvenir via la messagerie à des tiers non autorisés. L'appliance de sécurité e-mail Cisco IronPort et les services associés vous permettent de garder le contrôle du trafic de messages entrants et sortants sur le réseau de l'entreprise.

Maîtrise de la messagerie avec l'appliance de sécurité e-mail Cisco IronPort C Series

L'appliance de sécurité e-mail Cisco IronPort C Series s'adresse aux entreprises de toutes tailles. Ce système de défense à plusieurs niveaux se caractérise en particulier par la combinaison de filtres e-mail de premier ordre, à base de réputation, avec des outils d'analyse anti-spam et anti-virus. La conjugaison de mécanismes de protection préventive et réactive, épaulés par le puissant système d'exploitation AsyncOS, garantit un niveau maximal de performance et de fiabilité. C'est ainsi que, grâce aux filtres IronPort, les messages indésirables sont bloqués en majorité au niveau même de la passerelle, du fait de la mauvaise réputation de leurs expéditeurs. Les technologies qui ont permis à IronPort de se hisser au rang de leader mondial sur le marché des appliances de sécurité sont également disponibles sous forme de services managés, hébergés ou hybrides. Grâce à ce choix de modèles, les clients sont libres de décider du mode de protection de leur trafic e-mail (sécurisation sur site, externalisée ou en mode cloud, voire une combinaison des trois).



L'appliance Cisco IronPort C Series repose sur un système de protection à plusieurs niveaux et garantit ainsi une sécurisation complète du trafic e-mail entrant et sortant.

Une puissante plate-forme de sécurité

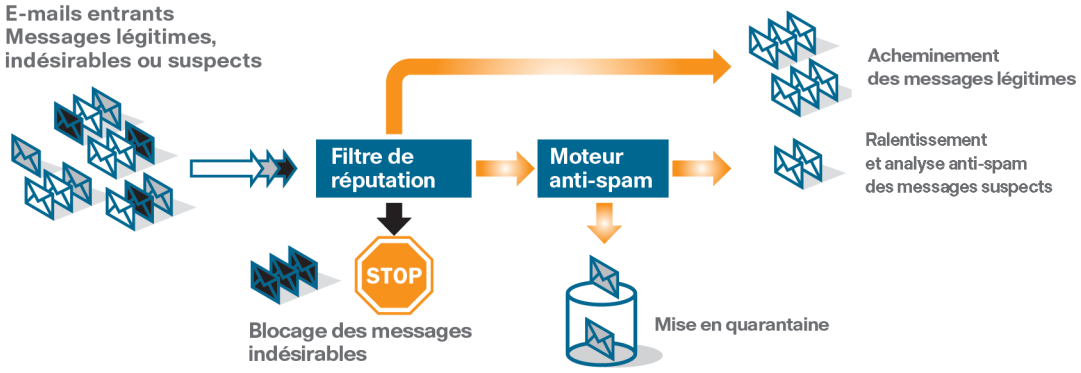
Les appliances de sécurité e-mail Cisco IronPort s'appuient pour cela sur le système d'exploitation propriétaire **AsyncOS**, développé depuis 2001. Outre 10 000 connexions actives simultanément, AsyncOS offre des fonctions avancées, telles que la gestion dynamique des files d'attente par domaine et des redirections de faux messages d'erreur. De plus, il permet de freiner la réception des messages suspects. Vous avez ainsi l'assurance que votre infrastructure de messagerie ne sera à aucun moment submergée par des attaques massives de virus ou de spam.

Défense Anti-spam

Les filtres **Cisco IronPort Reputation Filters** agissent comme un premier rempart de défense pour bloquer les messages indésirables avant même leur réception. Ils exploitent à cette fin les informations en temps réel de SensorBase, la plus vaste base mondiale de données de réputation sur Internet. Depuis sa création en 2002, SensorBase ne cesse de se développer et analyse, dans le cadre du réseau Cisco Security Intelligence Operations, plus de 30% des communications planétaires. A partir de ces informations, les filtres de réputation emploient plus de 200 paramètres pondérés afin de calculer des notes de réputation spécifiques (s'échelonnant de -10 à +10). Il est alors possible d'accepter, de bloquer, ou de soumettre le message à une analyse complémentaire en fonction de sa note. 90% du trafic indésirable est en moyenne éliminé dès la passerelle.

Cisco IronPort Anti-Spam collabore en toute transparence avec les filtres de réputation. Il analyse en détail la provenance du message, son contenu, sa structure, ainsi que les URL éventuelles qu'il renferme. Il en résulte un filtrage extrêmement précis avec un taux de capture leader sur le marché, pour un taux de faux positifs d'à peine 1 message sur 1 million.

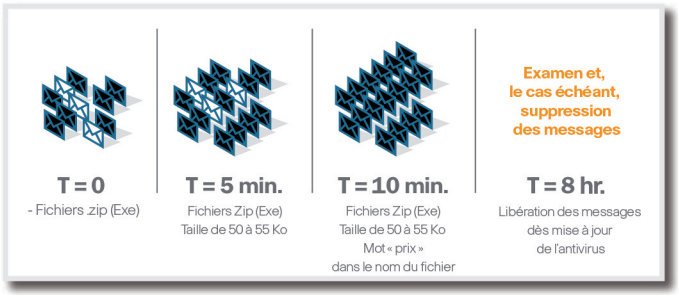
Les filtres Cisco IronPort Reputation Filters bloquent plus de 90% du spam entrant au niveau de la connexion, ce qui se traduit par un gain d'efficacité considérable.



Défense Anti-virus

Les filtres **Cisco IronPort Virus Outbreak Filters** assurent une protection préventive contre des virus jusque-là inconnus. Les nouvelles attaques virales sont détectées par SensorBase au travers des anomalies dans les échanges mondiaux de données. Les messages suspects font alors l'objet d'une mise en quarantaine dynamique.

Les **filtres Anti-Virus Cisco IronPort** font appel aux technologies éprouvées de McAfee et Sophos dans ce domaine. L'intégration de ces filtres à base de signatures au niveau de la passerelle garantit, en combinaison avec IronPort Virus Outbreak Filters, une protection extrêmement efficace, y compris contre les attaques auparavant inconnues.



La mise en quarantaine dynamique permet de franchir le laps de temps critique entre l'attaque virale et la publication de la signature correspondante par les éditeurs de logiciels anti-virus.

Protection des données

Afin d'éviter la fuite de données confidentielles lors de l'envoi de messages, les filtres **Cisco IronPort Content Filters** contrôlent le contenu de toutes les informations sortantes, y compris les en-têtes et fichiers joints, à la recherche de critères spécifiques ou d'expressions prédéfinies. Suivant les règles en vigueur, les données sensibles sont mises en quarantaine, corrigées, archivées ou bien directement chiffrées, le tout sans intervention nécessaire (ou possible) de l'expéditeur. En outre, les directives de conformité de l'entreprise sont appliquées au moyen de dictionnaires prédéfinis (HIPAA, PCI ou SOX, par exemple). Les filtres de contenu sont complétés par d'autres fonctions de protection fournies par RSA, qui peuvent être ajoutées via une licence logicielle totalement intégrée.

La technologie de **chiffrement Cisco IronPort PXE** est une méthode exclusive de chiffrement des messages. Elle ne nécessite ni installation de logiciel ni connaissance particulière de la part de l'utilisateur final et opère indépendamment de S/MIME ou d'Open-PGP. Les messages sont déchiffrés directement sur le poste du destinataire, dans son navigateur Web, sans logiciel supplémentaire. L'expéditeur peut affecter un délai de validité aux informations envoyées, rappeler sans difficulté les messages non lus ou encore contrôler l'envoi de fichiers volumineux. Il a également la possibilité de demander un accusé de réception et de lecture, mais aussi de permettre au destinataire de lui répondre en chiffrant son e-mail.

Outils d'administration

L'administration centralisée assure une gestion extrêmement simple, sécurisée et fiable des installations combinant plusieurs appliances. Elle permet également des adaptations locales dans le cadre des règles globales définies. Sur autorisation de l'administrateur, ces paramétrages peuvent s'appliquer à des individus et groupes d'utilisateurs spécifiques dans l'entreprise, à différents équipements, mais aussi à l'ensemble des appliances de sécurité e-mail installées. La configuration s'effectue, au choix, via une interface graphique intuitive ou en ligne de commande.

Des **fonctions de reporting et de suivi** sont intégrées à toutes les appliances de sécurité e-mail Cisco IronPort. Elles permettent par exemple, d'un simple clic, de suivre instantanément différents messages selon des critères tels que l'expéditeur, le destinataire, le nom de domaine, l'adresse IP ou certains mots-clés. De plus, toutes les informations concernant les appliances installées sont disponibles en permanence grâce à des rapports fournis en temps réel. Il est également possible de programmer l'envoi automatique de rapports par e-mail à des destinataires prédéfinis.

Cisco IronPort C-Series

CARACTÉRISTIQUES TECHNIQUES	C160	C360	C360D	C660	X1060
Boîtier/Unité centrale					
Dimensions	1 U (5,5 x 44,5 x 54,6 cm)	2 U (8,9 x 44,5 x 74,9 cm)	2 U (8,9 x 44,5 x 74,9 cm)	2 U (8,9 x 44,5 x 74,9 cm)	2 U (8,9 x 44,5 x 74,9 cm)
Poids	9,5 kg	23,5 kg	23,5 kg	23,5 kg	25,4 kg
Alimentation	750 W, 100/240 V	750 W, 100/240 V	750 W, 100/240 V	750 W, 100/240 V	750 W, 100/240 V
Dégagement thermique	546 – 853 BTU	820 – 1228 BTU	820 – 1228 BTU	891 – 1330 BTU	990 – 1478 BTU
Processeur	1 Intel	1 Intel multicœur	1 Intel multicœur	2 Intel multicœur	2 Intel multicœur
Espace de stockage	2 x 80 Go 7200 tr/min SATA	2 x 146 Go 10 000 tr/min U320 SCSI	2 x 146 Go 10 000 tr/min U320 SCSI	4 x 146 Go 10 000 tr/min U320 SCSI	4 x 146 Go 10 000 tr/min U320 SCSI
RAID	RAID 1	RAID 1	RAID 1	RAID 10	RAID 10
Réseau	2 ports Ethernet 10/100/1000 BaseT	3 ports Ethernet 10/100/1000 BaseT	3 ports Ethernet 10/100/1000 BaseT	3 ports Ethernet 10/100/1000 BaseT	3 ports Ethernet 10/100/1000 BaseT
Capacité	10 Go (file d'attente)	35 Go (file d'attente)	35 Go (file d'attente)	70 GB (file d'attente)	70 Go (file d'attente)

Standard	
Protocoles e-mail	SMTP, ESMTP, Secure SMTP via TLS
DNS	Résolution/cache interne ; possibilité de résolution via serveur DNS local ou root Internet
LDAP	Intégration notamment avec Active Directory, Notes, Domino et OpenLDAP
Interfaces/configuration	
Interface Web	Accessible via HTTP ou HTTPS
Ligne de commande	Accessible via SSH ou port série DB-9, assistant de configuration et saisie de commandes
Transfert de fichiers	SCP ou FTP
Supervision	XML via HTTPS, SNMP
Fichiers de configuration	XMLe

GAMME DE PRODUITS

C160	Solution conviviale complète pour les petites et moyennes entreprises
C360	Pour les moyennes à grandes entreprises
C360D	Pour toutes les entreprises ayant des besoins spécifiques d'émissions d'e-mails
C660	Pour les grandes entreprises et les fournisseurs d'accès Internet
X1060	Spécialement conçu pour protéger les réseaux les plus exigeants
Services hébergés	Protection via une Infrastructure e-mail dédiée, exploitée dans un réseau de centres de données Cisco
Services hybrides	Combinaison de boîtiers sur site et de l'infrastructure hébergée Cisco.
Services managés	Externalisation de la gestion et de la surveillance des boîtiers de sécurité e-mail auprès des experts sécurité de Cisco

Bénéficiez de notre offre d'évaluation gratuite pendant 30 jours afin de tester, sans engagement, l'appliance de sécurité e-mail Cisco IronPort. Commandez dès à présent votre modèle d'évaluation sur le site www.ironport.com/try ou en nous contactant par courriel à l'adresse cisco-security-fr@cisco.com

Cisco Systems
11 rue Camille Desmoulins - Imm. L'Atlantis
92782 Issy-Les-Moulineaux cedex - France
TEL : +33 1 58 04 60 00 FAX : +33 1 58 04 61 00
EMAIL : **cisco-security-fr@cisco.com** WEB : **www.ironport.com**

Cisco a plus de 200 bureaux ou filiales dans le monde. Les adresses, numéros de téléphone et numéros de fax sont listés sur le site web Cisco à l'adresse www.cisco.com/go/offices.