LOGICIEL PARE-FEU CISCO PIX VERSION 7.0

RESUME DES FONCTIONNALITES DE CETTE VERSION

SERVICES EVOLUES POUR L'ENTREPRISE

- Services d'inspection détaillée des paquets sur les protocoles HTTP, FTP, ESMTP et bien d'autres
- Blocage des applications de messagerie instantanée, peer-to-peer et de tunnellisation
- Cisco Modular Policy Framework avec politiques de sécurité sur les flux
- Services de pare-feu virtuel
- Pare-feu de niveau 2 transparent
- Services de sécurité sans fil mobile de troisième génération

SERVICES IPSEC ROBUSTES POUR VPN

- Contrôle de l'état de la sécurité sur les clients VPN
- Mise à jour automatique du logiciel client VPN
- Routage OSPF dynamique sur les tunnels VPN

SERVICES DE HAUTE DISPONIBILITE

- Basculement actif/actif avec support de routage asymétrique
- Basculement à inspection d'état des VPN à accès distant et de site à site
- Mises à jour logicielles sans interruption de service

SERVICES DE RÉSEAU INTELLIGENT

- Routage multicast PIM
- Qualité de service (QoS)
- Réseau compatible IPv6

SOLUTIONS DE GESTION SOUPLES

- SSHv2 et SNMPv2c
- Reprise de configuration
- Plus grande simplicité d'utilisation

Leader de son marché, Cisco fournit à travers la gamme PIX, des solutions économiques et faciles à déployer qui assurent la mise en œuvre de politiques de sécurité robustes et fiables pour les entreprises de toute tailles. Des solutions qui permettent aujourd'hui une sécurisation par utilisateur ou par application et luttent contre les attaques multi-vecteurs.

Ces équipements spécialement conçus pour la sécurité mettent à votre disposition une large gamme de services intégrés de sécurité et de réseau, notamment :

- des services évolués de pare-feu sensibles aux applications (pare-feu applicatif)
- l'une des meilleures sécurités VoIP (Voix sur IP) et multimédia du marché,
- une connectivité VPN IPSec robuste pour les accès distants de postes nomades ou interconnexions site à site,
- une tolérance de panne reconnue parmi les meilleures de l'industrie,
- des services de réseau intelligent,
- Une administration embarquée intuitive et efficace

La gamme de pare-feu Cisco PIX s'étend des boîtiers spécialisés et compacts de type « plug-and-play » pour petits bureaux et bureaux à domicile jusqu'aux systèmes Gigabits modulaires. Chaque produit apporte aux environnements de réseau, quelle que soit leur taille, une protection robuste, de hautes performances et une grande fiabilité.

DES SERVICES DE PARE-FEU EVOLUES POUR UNE PROTECTION ET UN CONTROLE RENFORCÉ DES APPLICATIONS CRITIQUES DE L'ENTREPRISE

Inspection d'état et inspection applicative

Les pare-feu Cisco PIX protègent l'entreprise contre les agressions qui ciblent leurs activités Internet et leurs infrasctructures réseau. Pierre angulaire de toute sécurité, les pare-feu Cisco PIX offrent des services de de blocage de ports et d'autorisation de trafic avec inspection d'état. Reposant sur des services évolués d'inspection applicative, les pare-feu Cisco PIX garantissent de plus, un niveau de sécurité qui agit au niveau de la couche applicative. Ceci grâce à des moteurs d'inspection intelligents qui examinent dans leurs détails les flux de réseau au niveau des couches 4 à 7 et qui sont capables de détecter toute déviation par rapport aux spécifications.
Pour défendre les réseaux contre les attaques sur la couche applicative et donner à l'entreprise un meilleur contrôle sur les applications et les protocoles de son environnement, ces moteurs d'inspection intègrent une connaissance exhaustive des applications et des protocoles. Ils utilisent également des technologies d'application de la sécurité comprenant la détection des anomalies de protocoles, le suivi d'état des applications et des protocoles, les services de traduction d'adresses de réseau (NAT) ainsi que des techniques de détection et de limitation des attaques comme le filtrage des commandes d'applications et de protocoles, la vérification des contenus et le démasquage des URL. Ces moteurs d'inspection fournissent également à l'entreprise un contrôle sur la messagerie instantanée, sur le partage des fichiers en « peer-to-peer » et sur les applications de tunnellisation pour lui permettre de mettre en œuvre des politiques d'utilisation et de conserver la bande passante du réseau pour ses seules applications métiers seules application légitimes sur l'infrastructure.

Protection contre les attaques multivecteurs

Les pare-feu Cisco PIX intègrent des services de protection multi-niveau qui renforcent les défenses de l'entreprise contre de nombreuses formes courantes d'attaques (attaques par saturation, masquage par fragmentation, par réémission ou par paquets mal formés). Grâce à leur vaste éventail de fonctions de protection, comme le réassemblage de flux TCP, la normalisation du trafic, DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify et les interceptions TCP, les pare-feu Cisco PIX identifient et bloquent les attaques les plus variées et peuvent alerter les administrateurs en temps réel.

Contrôle d'accès souple et puissance des politiques à base de flux

Les technologies souples de contrôle d'accès des pare-feu Cisco PIX (groupes d'objets réseau et d'objets services, politiques par utilisateur ou par groupe, et plus de 100 applications et protocoles prédéfinis) permettent en outre à l'administrateur de créer aisément ses propres politiques de sécurité. La puissance de Modular Policy Framework, une première du logiciel Cisco PIX version 7.0, donne à l'administrateur la possibilité de définir des politiques granulaires par flux et par classe et offre à chaque élément un ensemble de services de sécurité comme les politiques par moteur d'inspection, les politiques de qualité de service (QoS), les temporisateurs de connexion et plus encore. En associant les différents éléments de sécurité offerts par les pare-feu Cisco PIX (contrôle d'accès souple, services de sécurité par flux ou par classe, pare-feu à inspection d'état, inspection applicative, protection contre les attaques multivecteurs) l'entreprise se donne les moyens d'appliquer des politiques de sécurité complètes qui la protégeront contre les attaques de nouvelles générations

DES SERVICES DE SECURITE VoIP PARMI LES MEILLEURS DU MARCHE POUR LA PROTECTION DES RESEAUX CONVERGENTS DE PROCHAINE GENERATION

Les pare-feu Cisco PIX assurent une des meilleures protections du marché pour la Voix sur IP (VoIP) et les autres applications multimédias, afin de permettre à l'entreprise de profiter, en toute sécurité, de tous les avantages des réseaux convergents voix, vidéo et données en termes de productivité, de frais d'exploitation et de compétitivité. En associant les VPN et la Qualité de Service (QoS) aux services d'inspection évoluée des protocoles fournis par les pare-feu Cisco PIX pour les réseaux convergents, l'entreprise peut tirer ainsi le maximum des bénéfices des services voix et multimédias pour les bureaux distants ou à domicile et les utilisateurs mobiles grâce à un niveau de sécurité inégalé.

Les pare-feu Cisco PIX supportent les normes VoIP et multimédias comme H.323 Version 4, SIP (Session Initiation Protocol), SCCP (Cisco Skinny Client Control Protocol), RTSP (Real-Time Streaming Protocol) ou MGCP (Media Gateway Control Protocol), pour permettre à l'entreprise de déployer en toute sécurité une large gamme d'applications VoIP et multimédias de dernière et de prochaine générations. Les pare-feu Cisco PIX fournissent également des services de sécurité pour les applications TAPI (Telephony Application Programming Interface) et JTAPI (Java TAPI) lorsque, comme Cisco IP SoftPhone et Cisco CRS (Customer Response Solution), celles-ci utilisent le mécanismes de transport réseau CTIQBE (Computer Telephony Interface Quick Buffer Encoding).

DES SERVICES VPN IPSEC ROBUSTES POUR CONNECTER LES RESEAUX ET LES UTILISATEURS MOBILES DE MANIERE ECONOMIQUE

Grâce à de nouvelles fonctionnalités VPN des pare-feu Cisco PIX, l'entreprise peut connecter par Internet, de façon économique et en toute sécurité, ses réseaux et ses utilisateurs mobiles depuis le monde entier. Les solutions supportées vont des VPN de site à site utilisant les normes VPN IKE (Internet Key Exchange) et IPSec (IP Security) jusqu'aux fonctionnalités innovantes d'accès à distance de Cisco. Par exemple, les fonctionalités Easy VPN sont maintenant présentes sur les pare-feu Cisco PIX, comme pour les routeurs Cisco IOS® et la gamme des concentrateurs Cisco VPN 3000. Cisco Easy VPN, contrairement aux solution VPN traditionnelles, permet de bâtir une architecture de VPN à accès distant dont l'évolutivité, la rentabilité et la simplicité d'utilisation sans équivalent éliminent les frais d'exploitation liés à la gestion des configurations des équipements distants. Cisco Easy VPN apporte d'autres services comme le contrôle de l'état de la sécurité sur les clients VPN et les mises à jour logicielles automatiques des clients VPN Cisco, afin de fournir un accès à distance sécurisé et facile à gérer vers les réseaux d'entreprise. Les pare-feu Cisco PIX cryptent les données à l'aide des normes DES (Data Encryption Standard) à 56 bits, 3DES (Triple DES) à 168 bits ou AES (Advanced Encryption Standard) jusqu'à 256 bits.

Certains modèles Cisco PIX disposent de l'accélération matérielle intégrée des VPN pour des services hautes performances et particulièrement évolutifs.

UNE ARCHITECTURE ROBUSTE ET RECONNUE POUR ASSURER UNE DISPONIBILITE DE SERVICE MAXIMUM

Les modèles de pare-feu Cisco PIX fournissent des services de redondance avec maintient de sessions reconnus parmi les meilleurs de l'industrie. Les pare-feu Cisco PIX peuvent être déployés dans une architecture à haute disponibilité de service de type actif/veille ou, de manière plus évoluée, de type actif/actif qui supporte les environnements de réseau complexes exigeant un support de routage asymétrique. Les pare-feu mis en redondance l'un de l'autre synchronisent de façon permanente l'état des connexions actives qui les traversent ainsi que le paramétrage des boîtiers ce qui fournit une solution à haute disponibilité très facile à gérer. La synchronisation peut s'effectuer sur une connexion de type Ethernet, ce qui assure à l'entreprise un niveau supplémentaire de protection en lui permettant de séparer géographiquement les pare-feu. Dans le cas d'une défaillance du système primaire ou du réseau, les sessions actives sont automatiquement basculées d'un pare-feu à l'autre, en toute transparence pour l'utilisateur.

DES SERVICES DE RESEAU INTELLIGENTS POUR UN DEPLOIEMENT PLUS SIMPLE ET UNE INTEGRATION DE RESEAU TRANSPARENTE

Les pare-feu dédiés Cisco PIX capatilisent sur plus de vingt années d'expertise et d'innovation dans le domaine des technologies Internet fournissant ainsi un vaste éventail de services intelligents qui s'intègrent de manière transparente aux nombreux types d'environnements réseaux actuels. Grâce au support natif de la norme 802.1q pour VLAN, l'administrateur peut intégrer facilement les pare-feu Cisco PIX dans les environnements de réseau commutés. Le déploiement de téléphone IP Cisco profite des services de provisionnement de ressources automatiques fournis par les pare-feu Cisco PIX qui, sans intervention de l'utilisateur, permettent aux téléphones de s'enregistrer auprès du serveur de téléphonie centralisé Cisco CallManager dont ils dépendent et de télécharger les informations de configuration et les images logicielles supplémentaires dont ils ont besoin. De plus, l'entreprise accroît la robustesse de l'ensemble de son réseau en tirant profit des services de routage dynamique OSPF (Open Shortest Path First) supportés nativement par les pare-feu Cisco PIX qui, en quelques secondes, détectent les pannes de réseau et participent de façon active au recalcul des routes réseau. Le support intégral du multicast PIM-Sparse Mode v2 et du routage bidirectionnel PIM (Protocol Independent Multicast) permet la télédistribution en temps réel et de façon sécurisée des applications métiers de l'entreprise, des applications de calcul collaborative et la diffusion multimédia. L'entreprise peut envisager le déploiement des réseaux IPv6 de prochaine génération grâce aux services de sécurité étendues IPv6 des pare-feu Cisco PIX. Et ceci tout en assurant simultanément la protection des environnements IPv4 existants pendant la transition vers la nouvelle infrastructure.

DES SOLUTIONS DE GESTION INTUITIVES POUR REDUIRE LES FRAIS D'EXPLOITATION

Les pare-feu Cisco PIX offrent une grande diversité d'options de configuration, de surveillance et de dépannage pour offrir à l'entreprise toute la souplesse du choix des méthodes qui conviennent le mieux à ses besoins. Les solutions d'administration vont des outils de gestion centralisés à base de politiques jusqu'à la gestion intégrée par le Web pour prendre en charge des protocoles de surveillance à distance comme SNMP (Simple Network Management Protocol) et syslog. Les pare-feu Cisco PIX acceptent jusqu'à 16 niveaux de rôles administratifs personnalisables qui permettent à l'entreprise d'accorder à l'administrateur comme au personnel opérationnel les niveaux d'accès appropriés à chaque serveur dédié (accès en surveillance seule, accès à la configuration en lecture seule, configuration de réseau seule ou configuration du pare-feu seule, par exemple). Les pare-feu Cisco PIX disposent également de robuste fonctionnalités de mise à niveau automatiques (Auto Update). C'est un ensemble de services sécurisés de gestion à distance qui assure la mise à jour automatique de la configuration des pare-feu et des images logicielles.

Des solutions de gestion centralisées de prochaine génération

Les pare-feu dédiés Cisco PIX qui exécutent le logiciel Cisco PIX Version 7.0 peuvent être gérés de manière centralisée grâce à la version 2.3 de CiscoWorks VMS (VPN/Security Management Solution) qui sortira prochainement. Cette solution de gestion à trois niveaux hautement évolutive de prochaine génération assure :

- la gestion complète des configurations et des images logicielles,
- la hiérarchisation des unités par héritage de configuration à base de « règles intelligentes »,
- l'attribution personnalisable de rôles administratifs et de privilèges d'accès,
- la gestion et l'audit complets des modifications administratives à l'échelle de l'entreprise,
- la découverte et l'optimisation intelligentes des politiques de sécurité et des groupes objets,
- la gestion automatisée des images logicielles pour les pare-feu dédiés Cisco PIX distants,
- le support des pare-feu à adressage dynamique.

Solutions de limitation des risques d'attaques et surveillance des événements

La gamme de produits Cisco CS-MARS (Security Monitoring, Analysis, and Response System) permet d'identifier, de confiner et d'éliminer avec grande simplicité et précision les attaques circulant sur un réseau. Les équipements d'alertes CS-MARS analysent et collectent les événements de sécurité ainsi que les données syslog et NetFlow provenant d'un grand nombre de solutions de sécurité du marché Cisco ou non Cisco, que l'on trouver sur les ordinateurs de bureau, les serveurs et l'infrastructure. Ils identifient le parcours réseau empreinté par les attaques et proposent des contre mesure, simplifiant la gestion des incidents de sécurité dans les environnements qui ne disposent éventuellement pas de leur propre analyste de sécurité.

Cisco propose également la solution SIMS (CiscoWorks Security Information Management Solution) bien adaptée aux grandes entreprises et aux fournisseurs de services de sécurité administré disposant de leurs propres analystes de sécurité qui ont besoin d'une solution de collecte approfondie de données, d'analyse judiciaire, d'audit, de mise en conformité et de reporting pour des réseaux multiconstructeurs complexes.

Une administration intuitive et simplifiée

Le gestionnaire Cisco ASDM (Adaptive Security Device Manager) est une interface de gestion Web de qui simplifie considérablement le déploiement, la configuration au jour le jour et la surveillance d'un pare-feu Cisco PIX sans qu'il soit nécessaire d'installer d'autres logiciels qu'un navigateur Web standard et une extension Java sur l'ordinateur de l'administrateur. Des assistants intelligents de configuration et de gestion des VPN garantissent une intégration facile dans tous les environnements de réseau, tandis que les fonctions de surveillance (notamment un tableau de bord et une visionneuse syslog en temps réel) fournissent, d'un seul coup d'œil, des informations vitales sur la santé des unités et du réseau comme sur les événements.

A défaut, l'administrateur peut, à distance, configurer, surveiller et dépanner ses pare-feu Cisco PIX par l'intermédiaire de l'interface de commande en ligne (CLI). L'accès sécurisé à la CLI s'effectue de plusieurs manières, notamment par le protocole SSH (Secure Shell) v2 et Telnet sur IPSec ou, hors bande, par un port console.

LES NOUVELLES FONCTIONNALITES DU LOGICIEL SERVEUR DE SECURITE DEDIE CISCO PIX VERSION 7.0

Le logiciel serveur de sécurité Cisco PIX Version 7.0 offre un vaste ensemble de nouvelles fonctionnalités dont plusieurs sont décrites dans le Tableau 1. Pour voir la liste complète de ces fonctionnalités, consultez les instructions d'utilisation du logiciel serveur de sécurité Cisco PIX Version 7.0.

Tableau 1. Les nouvelles fonctions et leurs avantages

Caractéristiques	Avantages
Services évolués de pare-feu	
Cisco Modular Policy Framework	• Ce cadre particulièrement puissant et souple pour la définition des politiques par flux ou par classe permet aux administrateurs d'identifier un flux ou une classe de réseau en fonction de diverses conditions, avant d'appliquer un ensemble de services personnalisables à chacun. • Améliore le contrôle des applications en permettant pour la première fois de disposer de politiques de pare-feu/d'inspection par flux ou par classe, de politiques QoS, de limites et de temporisateurs de connexion, et plus encore.
Advanced Web Security Services	• Ces nouveaux services d'inspection en profondeur du trafic Web offrent un contrôle granulaire sur les sessions HTTP et garantissent ainsi une protection renforcée contre une grande variété d'attaques Internet. • Offre à l'entreprise un contrôle précis sur les méthodes et les commandes HTTP qui peuvent être utilisées en fonction du flux (les politiques sont différentes selon que le trafic provient d'Internet ou d'un serveur Web intermédiaire vers un serveur Web de production, par exemple) et protège ainsi l'entreprise contre une grande variété d'attaques Web, notamment la suppression ou la modification non autorisée de contenus Web. • Fournit un vaste éventail de puissants services de sécurité HTTP supplémentaires, notamment l'application de la conformité RFC, la détection des anomalies de protocole, le suivi d'état des protocoles, la validation de réponse, la validation et le contrôle des contenus de type MIME , l'application des règles de longueur URI (Uniform Resource Identifier), et bien plus encore.
Contrôle des applications de tunnellisation	• Introduit de nouveaux services d'inspection pour détecter et éventuellement bloquer les applications de messagerie instantanée, de partage « peer-to-peer » des fichiers, etc., qui réalisent une tunnellisation par les ports d'application Web. • Bloque les applications de messagerie instantanée comme AOL Instant Messenger, Microsoft Messenger et Yahoo Messenger. • Bloque les applications de partage « peer-to- peer » de partage de fichiers comme KaZaA et Gnutella. • Stoppe les applications de tunnellisation comme GoToMyPC.
Sécurité contextuelle	• Permet la création, sur un même serveur dédié Cisco PIX, de multiples contextes de sécurité (pare-feu virtuels) disposant chacun de son propre ensemble de politiques de sécurité, de ses interfaces logiques et de ses domaines administratifs. • Supporte, selon la licence, jusqu'à cinq niveaux de contextes de sécurité : 5, 10, 20, 50 et 100 (le nombre maximal de contextes supportés dépend du modèle de serveur Cisco PIX).

Caractéristiques	Avantages
	• Apporte à l'entreprise un moyen pratique de consolider de multiples pare-feu dans un équipement unique ou une paire d'équipements redondants, tout en conservant la possibilité de gérer individuellement les différentes instances de pare-feu virtuels. • Permet aux fournisseurs de services de proposer de robustes services de pare-feu à plusieurs clients en même temps sur une paire de pare-feu redondants.
Pare-feu transparent au niveau 2	• Supporte le déploiement d'un pare-feu Cisco PIX en mode de pont de niveau 2 sécurisé, offrant ainsi de nombreux services de sécurité de pare-feu des niveaux pour le réseau à protéger, tout en demeurant « invisible » aux systèmes d'extrémité situés en amont et en aval. • Simplifie le déploiement des pare-feu Cisco PIX dans les environnements de réseau existants en permettant à l'entreprise d'éviter la redifinition du plan d'adressage IP. • Supporte la création d'une sécurité périmétrique de niveau 2 par application de politiques de contrôle d'accès basée sur le champ Ethertype de la trame Ethernet
Filtrage des commandes de session FTP	• Développe les services d'inspection FTP existants fournis par les pare-feu Cisco PIX, notamment la détection des anomalies de protocoles, le suivi d'état des protocoles, le support de traduction d'adresses de réseau et de ports NAT/PAT, et l'ouverture et la fermeture dynamiques des ports, afin de donner à l'administrateur un meilleur contrôle de l'utilisation des nombreuses commandes FTP en précisant ce que les utilisateurs et les groupes opérationnels peuvent effectuer au cours d'une session FTP (comme les commandes FTP get et put). • Offre de nouvelles techniques de masquage des serveurs ainsi que des signatures d'attaques complémentaires qui permettent de renforcer la protection des serveurs FTP contre les attaques. Services ESMTP (Extended Simple Mail Transport Protocol) pour l'inspection du courrier électronique
Services ESMTP (Extended Simple Mail Transport Protocol) pour l'inspection du courrier électronique	• Etend les fonctionnalités ESMTP au moteur d'inspection SMTP, offrant ainsi des services de sécurité comprenant la détection des anomalies de protocole, le suivi d'état des protocoles et le support des nouvelles commandes du protocole ESTMP : AUTH, DATA, EHLO, ETRN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML et VRFY. • Protège l'entreprise contre les commandes SMTP et ESTMP malveillantes grâce au filtrage automatique des commandes.
Services de sécurité pour la téléphonie mobile de troisième génération	• Assure une grande diversité de services de sécurité pour les environnements mobiles sans fil de troisième génération qui fournissent des services de données par commutation de paquets par l'intermédiaire de la norme GTP (GPRS [General Packet Radio Service] Tunneling Protocol) • Assure des services évolués d'inspection GTP qui permettent aux fournisseurs de services mobiles sans fil de disposer d'interactions sécurisées avec des partenaires itinérants grâce aux robustes fonctionnalités de filtrage reposant sur des paramètres GTP spécifiques comme les préfixes IMSI (International Mobile Subscriber Identity), les valeurs APN (Access Point Name) et bien plus encore. **Note :** Cette fonction fait l'objet d'une licence particulière.

Caractéristiques	Avantages
Services d'inspection Sun RPC/NIS+	• Améliore le support des applications UNIX à saut de ports par l'intermédiaire de nouveaux services à inspection d'état et de traductions d'adresses de réseau NAT pour Sun RPC les transactions de session NIS+ qui utilisent Portmapper v2 ou RPCBind v3/v4.
Services d'inspection ICMP (Internet Control Message Protocol)	• Garantit l'utilisation sécurisée d'ICMP pour le dépannage et l'amélioration des performances du réseau en assurant des services de suivi d'état des connexions ICMP et fournit des contrôles supplémentaires pour les messages d'erreur ICMP.
Moteur de sécurité TCP amélioré	• Introduit plusieurs nouvelles fonctionnalités fondamentales qui facilitent la détection des attaques sur les protocoles et sur la couche applicative. • Fournit des services de réassemblage et d'analyse des flux TCP qui facilitent la détection des attaques distribuées sur un groupe de paquets. • Offre des services de normalisation du trafic TCP avec des techniques supplémentaires de détection des attaques comme le contrôle évolué des marques et des options, la vérification des sommes de contrôle (checksum) sur les paquets TCP, la détection des données altérées dans les paquets retransmis, et plus encore.
Listes de contrôle d'accès sortant	• Améliore la souplesse de la définition des politiques de contrôle d'accès par l'ajout du support des listes de contrôle d'accès sortant (en plus des listes existantes de contrôle d'accès entrant), en permettant l'application du contrôle d'accès sur le trafic de réseau entrant ou sortant d'une interface.
Listes de contrôle d'accès à gestion temporelle	• Donne à l'administrateur un meilleur contrôle de l'utilisation des ressources en définissant à quel moment certaines listes de contrôle d'accès sont actives, avec des intervalles de temps personnalisables en fonction des différentes listes.
Activation et désactivation des entrées individuelles des listes de contrôle d'accès	• Un outil de dépannage particulièrement utile qui permet à l'administrateur de tester et d'ajuster au mieux les listes de contrôle d'accès sans avoir besoin de supprimer ou de remplacer les entrées de ces listes.
Performances de filtrage URL Websense améliorées	• Améliore considérablement l'évolutivité des recherches de filtrage URL simultanées grâce aux solutions EIM (Enterprise Employee Internet Management) de Websense.
Services de sécurité VoIP et multimédias	
T.38 Fax Over IP (FoIP)	• Renforce les services d'inspection H.323 en leur apportant le support du protocole T.38, norme ITU qui définit la transmission en temps réel du protocole FoIP.
Signalisation GKRCS (Gatekeeper Routed Control Signaling)	• Renforce les services d'inspection H.323 par la signalisation GKRCS en plus de la méthode DCS (Direct Call Signaling) actuellement supportée. • Permet aux pare-feu dédiés Cisco PIX de supporter les messages de signalisation d'appels échangés directement entre les contrôleurs d'accès H.323.
Inspection fragmentée et segmentée des flux multimédias	• Introduit l'inspection des flux voix et multimédias H.323, SIP, et SCCP fragmentés ou segmentés.
Services de traduction d'adresses MGCP	• Exploite les services de sécurité MGCP aux multiples fonctionnalités fournis par les pare-feu dédiés Cisco PIX en leur ajoutant les services de traduction d'adresse NAT et PAT pour les connexions MGCP entre les passerelles multimédias et les agents d'appels ou les contrôleurs de passerelles multimédias.
Services de traduction d'adresses RTSP	• Fournit des services de traduction d'adresses NAT pour les flux multimédias RTSP afin d'en améliorer le support dans une grande variété d'environnements de réseau.

Caractéristiques	Avantages
Services IPSec robustes pour VPN	
Contrôle de l'état de la sécurité sur les clients VPN	• Introduit la possibilité de vérifier l'état de la sécurité des clients VPN lors de la réception d'une tentative de connexion VPN, notamment en exigeant l'utilisation de produits de sécurité hôte autorisés (comme Cisco Security Agent) et en vérifiant le numéro de version ainsi que leur état avant de permettre à des utilisateurs distants d'accéder au réseau d'entreprise.
Blocage des clients VPN en fonction de leur système d'exploitation et de leur type	• Donne la possibilité de limiter l'accès au réseau des différents types de clients VPN (client logiciel, routeur, VPN 3002 ou Cisco PIX, par exemple) en fonction de leur type, du système d'exploitation installé et de leur version du logiciel client VPN. • Permet de limiter ou d'interdire l'accès aux clients VPN non conformes.
Mises à jour automatiques du logiciel client VPN	• Introduit le support des mises à jour logicielles automatiques des clients Cisco VPN et des clients matériels Cisco VPN 3002, avec la possibilité de déclencher les mises à jour une fois les connexions VPN établies, ou à la demande pour les clients VPN déjà connectés.
Support amélioré pour les environnements VPN à accès distant sans partage de tunnellisation	• Permet de faire aboutir les connexions VPN d'accès à distance sur l'interface externe d'un serveur de sécurité dédié Cisco PIX, afin de d'autoriser le trafic vers Internet provenant des tunnels VPN des utilisateurs distants à sortir par la même interface que celle d'arrivée (après application des éventuelles règles de pare-feu, des politiques de filtrage des URL et des autres contrôles de sécurité).
Transparence améliorée des traductions NAT pour les VPN	• Elargit encore le support des VPN IPSec de site à site et à accès distant vers les environnements de réseau qui utilisent la traduction d'adresse NAT ou PAT, comme les aéroports, les hôtels, les hot spots sans fil et les environnements haut débit. • Complète le support actuel des mécanismes d'encapsulation IETF UDP par le support des méthodes de traversée Cisco TCP et NAT UDP (User Datagram Protocol) pour renforcer la protection des traversées de limites NAT et PAT.
Intégration native avec les services d'authentification utilisateur les plus utilisés	• Offre une méthode pratique pour l'authentification des utilisateurs VPN grâce à l'intégration native avec les services d'authentification les plus courants comme Microsoft Active Directory, Microsoft Windows Domains, Kerberos, Lightweight Directory Access Protocol (LDAP) et RSA SecurID, sans qu'il soit nécessaire d'installer un serveur RADIUS/TACACS+ intermédiaire.
Routage OSPF dynamique sur les tunnels VPN	• Etend les services complets de routage dynamique OSPF pour le support des voisins sur les tunnels VPN IPSec, ce qui garantit une plus grande fiabilité pour les réseaux connectés à des VPN. • Supporte l'injection inversé de route OSPF qui améliore la souplesse et les performances du routage réseau.
Support des VPN « de périphérique à périphérique »	• Améliore le support des communications VPN « de périphérique à périphérique » lorsqu'un serveur de sécurité dédié Cisco PIX est utilisé comme concentrateur, en permettant au trafic VPN d'entrer et de sortir par la même interface.
Support renforcé des certificats X.509	• Introduit la possibilité de s'inscrire manuellement auprès d'autorités de certification X.509 grâce au support des requêtes de certificats au format PKCS (Public Key Cryptography Standard) #10. • Supporte l'importation manuelle des certificats sous PKCS #7, ainsi que l'importation de certificats avec clé privée sous PKCS #12

Caractéristiques	Avantages
	• Permet le déploiement dans des environnements disposant d'une hiérarchie d'autorités de certification à plusieurs niveaux grâce au support du chaînage multipartite des certificats. • Elargit le support des clés RSA jusqu'à 4096 bits • Ajoute le support des certificats X.509 DSA (Digital Signature Algorithm) avec des clés pouvant aller jusqu'à 1024 bits.
Support de l'autorité de certification de la plate-forme logicielle Cisco IOS	• Introduit le support de l'inscription en ligne auprès de la nouvelle autorité de certification de la plate-forme logicielle Cisco IOS : une autorité de certification X.509 légère qui simplifie le déploiement des VPN de site à site avec infrastructure de gestion des clés publiques.
Services haute disponibilité	
Redondance active/active avec maintient de session	• Réalise une solution qui complète le système primé de basculement actif/actif des pare-feu Cisco PIX dans lequel les deux systèmes actif/actif qui sont en redondance l'un de l'autre transmettent simultanément du trafic réseau : ceci permet de doubler le débit de l'ensemble pour répondre aux pointes soudaines du trafic de réseau. • Supporte le partage d'état bidirectionnel pare-feu actif/actif afin de supporter les environnements de réseau évolués avec des topologies de routage asymétrique : les flux qui entrent par l'un des pare-feu Cisco PIX et peuvent, si nécessaire, ressortir par l'autre. **Note** : Cette fonction n'est disponible que sur les modèles Unrestricted et Failover-Active/Active ; la mise à niveau des modèles Failover en modèles Failover-Active/Active implique l'acquisition d'une licence de mise à niveau.
Redondance avec maintient de session pour les connexions VPN	• Maximise le temps de fonctionnement des connexions VPN grâce à la nouvelle fonctionnalité de basculement avec maintient de session pour les connexions VPN y compris en mode de redondance active / active. • Synchronise toutes les informations d'état d'association de sécurité et les éléments de clés de session entre les pare-feu redondants pour garantir une soluion VPN particulièrement robuste.
Amélioration des délais de transition en cas de basculement	• Garantit un délai de basculement inférieur à la seconde sur câble série et de trois secondes sur réseau LAN grâce au contrôle encore plus granulaire des intervalles qui séparent les signaux de présence et de l'échange des informations d'état entre les membres des paires de serveurs de basculement.
Mises à jour logicielles sans interruption de service	• Permet à l'entreprise de réaliser des mises à niveau de maintenance logicielle sur les paires de serveurs de basculement Cisco PIX sans affecter les temps de fonctionnement ni les connexions du réseau grâce au partage des informations d'état entre les différentes versions du logiciel serveur Cisco PIX (version 7.0(1) ou ultérieures).
Services de réseau intelligent	
Routage multicast PIM	• Simplifie l'acheminement du trafic multimédia dans les applications de vidéoconférence, de calcul collaboratif et autres applications en temps réel vitales pour l'entreprise. Ceci grâce au support complet du routage PIM-Sparse Mode v2 et PIM bidirectionnel (reposant sur la technologie multicast Cisco IOS).

Caractéristiques	Avantages
Services QoS.	• Fournit des services QoS par flux et à base de politiques avec support de LLQ (Low-Latency Queuing) et du contrôle du trafic afin de donner la priorité au trafic réseau sensible à la latence et de limiter l'utilisation de la bande passante par les applications que désigne l'administrateur. • Permet à l'entreprise de disposer de politiques QoS de bout-en-bout pour son réseau élargi.
Réseau compatible IPv6	• Fournit des services de contrôle d'accès et d'inspection en profondeur par le pare-feu pour les environnements de réseau IPv6 natifs et les environnements mixtes IPv4/IPv6 grâce au support d'une double pile. • Fournit des services d'inspection compatibles IPv6 pour les applications qui utilisent les protocoles HTTP, FTP, SMTP, ICMP, TCP et UDP. • Supporte la gestion SSHv2, Telnet, HTTP/Secure HTTP (HTTPS) et ICMP sur IPv6.
Niveau de sécurité commun pour des interfaces multiples	• Elargit le concept de niveau de sécurité des interfaces des pare-feu Cisco PIX pour permettre à plusieurs interfaces de partager un niveau de sécurité commun. • Simplifie le déploiement des pare-feu Cisco PIX dans les environnements intranet en permettant à l'administrateur de définir des politiques de sécurité personnalisées pour le trafic circulant entre des interfaces qui partagent le même niveau de sécurité, sans permettre intrinsèquement le passage d'un trafic automatique quel qu'il soit.
Amélioration du support des VLAN.	• Augmente le nombre d'interfaces VLAN 802.1q supportées par les pare-feu dédiés Cisco PIX pour accroître la densité de ports sur chaque plate-forme. • Permet à l'entreprise de segmenter davantage son réseau en zones de sécurité distinctes, ce qui constitue une protection supplémentaire. • Supporte jusqu'à 25 VLAN sur les pare-feu Cisco PIX 515 et 515E, jusqu'à 100 VLAN sur les pare-feu Cisco PIX 525 et jusqu'à 200 VLAN sur les pare-feu Cisco PIX 535.
Services de translation d'adresses en option	• Simplifient le déploiement des pare-feu Cisco PIX en éliminant la nécessité de définir des politiques de translation d'adresses avant de permettre le passage du trafic réseau, comme c'était le cas auparavant ; désormais seuls les hôtes et les réseaux qui nécessitent une translation d'adresses devront disposer de politiques correspondantes configurées.
Solutions de gestion souples	
Surveillance SNMP améliorée	• Introduit le support de SNMPv2c qui offre une visibilité accrue de l'état des pare-feu Cisco PIX. • Fournit de nouveaux services comme les compteurs 64 bits (pour une meilleure surveillance des interfaces Ethernet Gigabit) et le support des transferts MIB de données en vrac. • Ajoute le support de nombreuses MIB SNMP supplémentaires, notamment la MIB SNMPv2 (RFC 1907), la MIB Interfaces Group (RFC 1573 et 2233), la MIB IP (RFC 2011) et la MIB Entity (RFC 2737). • Assure une visibilité complète des connexions VPN avec des statistiques détaillées par tunnel, notamment la durée d'établissement du tunnel, le nombre d'octets et de paquets transférés et plus encore, grâce au support de la MIB Cisco IPSec Flow Monitoring.

Caractéristiques	Avantages
SSHv2 et protocole SCP (Secure Copy Protocol).	• Permet l'utilisation de SSHv2 pour gérer à distance les pare-feu dédiés Cisco PIX en offrant une compatibilité améliorée avec les outils SSH d'autres constructeurs. • Introduit le support SCP en tant que méthode sécurisée supplémentaire de transfert de fichiers, comme les images de configuration et les images logicielles, en direction et en provenance des pare-feu Cisco PIX.
Stockage de configurations multiples en mémoire Flash	• Permet à l'administrateur de réaliser des reprises de configuration grâce à l'introduction d'un nouveau système de fichiers Flash et de la possibilité de stocker et d'utiliser de nombreuses configurations dans la mémoire Flash.
Récupération sécurisée des actifs	• Empêche l'accès non autorisé aux données sensibles de configuration, aux certificats et aux documents clés stockés sur les pare-feu Cisco PIX en effaçant automatiquement les contenus Flash dans le cas d'une procédure de réinitialisation de mot de passe ou de récupération d'actif, lorsque cette fonctionnalité a été préalablement configurée.
Rechargements systèmes programmés	• Permet à l'administrateur de programmer le rechargement sur un serveur de sécurité Cisco PIX soit à une heure donnée soit à l'expiration d'un délai, ce qui simplifie la planification des périodes d'arrêt du réseau et la notification des utilisateurs de VPN à distance d'une réinitialisation imminente.
Interface dédiée de gestion hors bande	• Permet aux entreprises de mettre en œuvre des pratiques optimales pour l'utilisation des fonctions de gestion hors bande sur les pare-feu Cisco PIX telles que ces pratiques sont décrites dans le schéma directeur Cisco SAFE, grâce à la possibilité nouvelle de désigner une interface spécifique qui jouera seule le rôle d'interface de gestion hors bande.
Services de ping ICMP évolués	• Offre des méthodes nouvelles et utiles de dépannage grâce au nouveau support des adresses IPv6 et des options ICMP élargies, notamment les modèles de données, df-bit, le compteur de répétition, la taille des datagrammes, le délai avant interruption, la sortie prolixe et l'intervalle de balayage des tailles.
Amélioration de la convivialité de l'interface de commande en ligne	• Améliore la convivialité de l'interface de commande en ligne des pare-feu Cisco PIX en intégrant de nombreux services de commande en ligne pratiques de la plate-forme logicielle Cisco IOS comme la saisie partielle des commandes avec complétion, l'aide contextuelle et les alias.
Alertes SMTP par courrier électronique	• Offre une méthode pratique pour alerter l'administrateur en cas d'événement critique, en envoyant par courrier électronique un message électronique aux adresses définies par l'administrateur.
Gestion administrative par TACACS+	• Introduit la possibilité de générer des enregistrements d'authentification, d'autorisation et d'administration (AAA) TACACS+ pour le suivi des accès administratifs aux pare-feu dédiés Cisco PIX, ainsi que le suivi de toutes les modifications de configuration réalisées au cours d'une session administrative, ce qui complète le support syslog existant pour les sessions administratives déjà supportées par les serveurs Cisco PIX.
Administration RADIUS vers de multiples serveurs	• Ajoute la possibilité d'envoyer simultanément des informations d'administration vers de multiples serveurs RADIUS.

Caractéristiques techniques

Les Tableaux 2, 3 et 4 présentent des informations sur la compatibilité entre les pare-feu dédiés Cisco PIX et les clients VPN, les produits VPN et certaines normes cryptographiques.

Compatibilité avec les clients VPN Cisco

Les pare-feu dédiés Cisco PIX supportent de nombreux clients VPN Cisco logiciels et matériels, et notamment ceux du Tableau 2.

Tableau 2. Compatibilité entre les pare-feu dédiés Cisco PIX et les clients VPN

Client VPN Cisco	Versions logicielles supportées
Clients VPN IPSec logiciels	• Client VPN Cisco pour Windows, versions 3.6 et ultérieures • Client VPN Cisco pour Linux, versions 3.6 et ultérieures • Client VPN Cisco pour Solaris, versions 3.6 et ultérieures • Client VPN Cisco pour Mac OS X, versions 3.6 et ultérieures
Clients VPN IPSec matériels (Cisco Easy VPN Remote)	• Client matériel VPN Cisco 3002, versions 3.0 et ultérieures • Plate-forme logicielle Cisco IOS Easy VPN Remote, version 12.2(8)YJ • Logiciel serveur de sécurité dédié Cisco PIX, versions 6.2 et 6.3

Compatibilité avec les VPN Cisco de site à site

En plus d'assurer l'interopérabilité avec un grand nombre de produits VPN d'autres constructeurs, les pare-feu Cisco PIX sont compatibles avec les produits VPN Cisco suivants pour la connectivité de site à site :

Tableau 3. Compatibilité VPN de site à site entre les pare-feu dédiés Cisco PIX et les produits VPN

Produit VPN Cisco	Versions logicielles supportées
Routeurs Cisco IOS	Plate-forme logicielle Cisco IOS versions 12.1(6)T et ultérieures
Serveur de sécurité dédié Cisco PIX	Logiciel serveur de sécurité dédié Cisco PIX, versions 6.0 (1) et ultérieures
Concentrateurs VPN Cisco 3000	Logiciel concentrateur VPN Cisco 3000, versions 3.0 et ultérieures

Normes cryptographiques supportées

Les pare-feu dédiés Cisco PIX supportent de nombreuses norme cryptographiques et produits et services associés fournis par d'autres constructeurs, notamment :

Tableau 4. Normes et produits cryptographiques supportés par les pare-feu dédiés Cisco PIX

Normes et produits cryptographiques	Description
Algorithmes de cryptage asymétrique (à clé publique)	• Paires de clés RSA publiques et privées, de 512 à 4096 bits • Paires de clés RSA publiques et privées, de 512 à 4096 bits
Algorithmes de cryptage symétrique	• AES : 128, 192 et 256 bits • DES : 56 bits • 3DES : 168 bits • RC4 : 40, 56, 64 et 128 bits
Perfect Forward Secrecy (négociation de clés Diffie-Hellman)	• Groupe 1 : 768 bits • Groupe 2 : 1024 bits • Groupe 5 : 1536 bits • Groupe 7 : 163 bits (courbe elliptique de Diffie-Hellman)

Algorithmes de hachage	• MD5 : 128 bits • SHA-1 : 160 bits
Autorités de certification X.509	• Baltimore UniCERT • Plate-forme logicielle Cisco IOS • Entrust Authority • iPlanet/Netscape CM • Microsoft Certificate Services • RSA KEON • VeriSign OnSite
Méthodes d'inscription pour les certificats X.509	• Simple Certificate Enrollment Protocol (SCEP) • Manuelle (PKCS #7 et #10)

Configuration système nécessaire

Le Tableau 5 décrit la configuration système nécessaire pour les pare-feu dédiés Cisco PIX qui exécutent le logiciel serveur Cisco PIX Version 7.0.

Tableau 5. Configuration système nécessaire

Configuration système nécessaire	Description
Plates-formes supportée	• Serveur de sécurité dédié Cisco PIX 515 • Serveur de sécurité dédié Cisco PIX 515E • Serveur de sécurité dédié Cisco PIX 525 • Serveur de sécurité dédié Cisco PIX 535
Mémoire RAM minimale	**Pare-feu dédiés Cisco PIX 515 et 515E** • 64 Mo sur les modèles Restricted • 128 Mo sur les modèles Unrestricted, Failover et Failover-Active/Active. **Note :** Cette version du logiciel exige davantage de mémoire pour les pare-feu dédiés Cisco PIX 515 et 515E que les précédentes, une mise à niveau de la mémoire sera peut-être nécessaire. **Serveur de sécurité dédié Cisco PIX 525** • 128 Mo sur les modèles Restricted • 256 Mo sur les modèles Unrestricted, Failover et Failover-Active/Active. **Serveur de sécurité dédié Cisco PIX 535** • 512 Mo sur les modèles Restricted • 1024 Mo sur les modèles Unrestricted, Failover et Failover-Active/Active.
Mémoire Flash minimale	• 16 Mo Cartes d'extension supportées • Carte un port Fast Ethernet 10/100 • Carte quatre ports Fast Ethernet 10/100 • Carte (SX) SC un port Ethernet Gigabit multimode • Carte VAC (VPN Accelerator Card) • Carte VAC+ (VPN Accelerator Card+)

Commande produit

Le Tableau 6 présente les informations de commande pour le logiciel serveur de sécurité Cisco PIX.

Tableau 6. Commande de matériel

Référence	Description
PIX-SW-UPGRADE=	Mise à niveau unique du logiciel serveur de sécurité dédié Cisco PIX pour les clients ne disposant pas d'un contrat Cisco SMARTnet® valide.

Services d'assistance

Les services d'assistance sont disponibles auprès de Cisco et de ses partenaires. Le service Cisco SMARTnet augmente les possibilités d'assistance de nos clients en offrant à tout moment et en tous lieux un accès aux ressources techniques en ligne comme par téléphone, la capacité de télécharger le logiciel système mis à jour et le remplacement préventif du matériel.

Pour toute information supplémentaire

Pour tout renseignement complémentaire, visitez les liens suivants :

Gamme de pare-feu dédiés Cisco PIX : http://www.cisco.com/go/pix

Cisco Adaptive Security Device Manager : http://www.cisco.com/go/asdm

Cisco Secure ACS : http://www.cisco.com/go/acs

CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software et Security Monitor : http://www.cisco.com/go/vms

Schéma directeur Cisco SAFE : http://www.cisco.com/go/safe

Pour télécharger la dernière version du logiciel serveur de sécurité Cisco PIX et Cisco Adaptive Security Device Manager (nécessite un identifiant de connexion Cisco.com valide), visitez :

http://www.cisco.com/cgi-bin/tablebuild.pl/pix

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camilles Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :
www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France • Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas Pérou • Philippines •Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine Russie • Singapour • Slovaquie •Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe

XXXXXXXXX