Fiche Technique

Packages routeurs **Sécurité** et VPN pour les gammes Cisco 1700, 2600, 3600 et 3700

Les packages routeurs sécurité et VPN Cisco sont développés autour des plates-formes de routage modulaires multiservices Cisco 1700, 2600XM, 2691, 3600 et 3700. Ces packages pour réseau privé virtuel (VPN) permettent à nos clients d'utiliser un unique numéro de référence pour commander un routeur Cisco disposant de toutes les composantes VPN et de sécurité nécessaires, et pour un prix inférieur à la somme de chacun des éléments qui les composent. Pour mieux répondre aux besoins de nos clients, chaque package VPN peut être renforcé par des modules supplémentaires. Tous les packages se composent de la plate-forme de routage choisie, d'une carte d'encryption hardware IPSec VPN, de modules mémoires supplémentaires, du logiciel Cisco IOS® qui exécute le cryptage IPSec (IP Security) 3DES (Triple Digital Encryption Standard) ainsi que d'un firewall Cisco IOS équipé d'un système de détection des intrusions (IDS).

Ces packages donnent à nos clients la possibilité de déployer des fonctionnalités de sécurité éprouvées comme les VPN sécurisés, les systèmes de détection d' intrusions et les firewalls, sur des accès Internet haut-débit et la capacité de créer des extranets ou des zones démilitarisées (DMZ). Ces packages VPN peuvent également prendre en charge le déploiement d'intranets, d'extranets et de VPN à accès distant.

Pour les accès distants, le package VPN comprend le Client VPN Cisco 3.0. Les packages routeurs sécurité et VPN Cisco sont par ailleurs idéalement adaptés aux VPN de site à site. Ils réunissent des fonctionnalités avancées et intégrées de routage, de firewall, d'accès commuté et de passerelle voix ainsi que des fonctions VPN pour les applications VPN multiservices. Les gammes Cisco 1700, 2600, 3600 et 3700 équipées du module VPN constituent la parfaite solution VPN IPSec pour connecter des bureaux de toutes tailles à d'autres sites distants, au siège social, à l'intranet du site central ou aux extranets des partenaires.

Les VPN aident l'entreprise à tirer pleinement profit de toute une série d'avantages – réduction considérable du coût des réseaux étendus (WAN), amélioration de la connectivité globale ou plus grande fiabilité – tout en mettant à leur service des fonctionnalités comme les communications extranets sécurisées. Qu'il s'agisse d'accès commuté à distance, Internet, intranet ou extranet, toutes ces connexions peuvent être réunies sur une unique liaison WAN vers Internet. Le Tableau 2 donne la liste complète des références de ces packages.

Fonctionnalités et avantages des packages sécurité et VPN

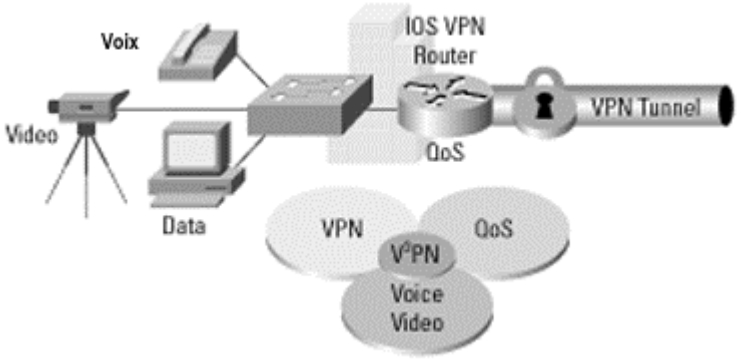
VPN IPSec compatible voix et vidéo

Les packages routeurs sécurité et VPN Cisco sont tous compatibles voix et vidéo IPSec. Cisco fournit une infrastructure VPN capable d'acheminer le trafic convergent voix, vidéo et données sur un réseau sécurisé IPSec. A la différence de nombreux équipements VPN sur le marché, les plates-formes VPN Cisco s'adaptent aux différentes topologies de réseau et aux caractéristiques des trafics des VPN IPSec multiservices, et garantissent que l'infrastructure VPN ne perturbe pas les applications multiservices déployées, que ce soit maintenant ou à l'avenir.

Avec ses packages routeurs sécurité et VPN, Cisco fournit des produits adaptés à toutes les caractéristiques des VPN multiservices.

L'architecture de réseau de la solution Cisco V³PN (Voice and Video-Enabled IPSec VPN : VPN IPSec compatible voix et vidéo) s'appuie sur les routeurs VPN Cisco équipés de la plate-forme logicielle Cisco IOS, les Cisco CallManager et les téléphones IP. De plus, Cisco propose un modèle global de déploiement de ses produits avec l'architecture Cisco AVVID (Architecture for Voice, Video and Integrated Data) pour la création de réseaux convergents, et le schéma directeur SAFE de sécurité des réseaux VPN. Ces modèles de déploiement garantissent une solution de réseau sécurisée, interopérable et fiable avec un support produit de bout en bout (voir Figure 1).

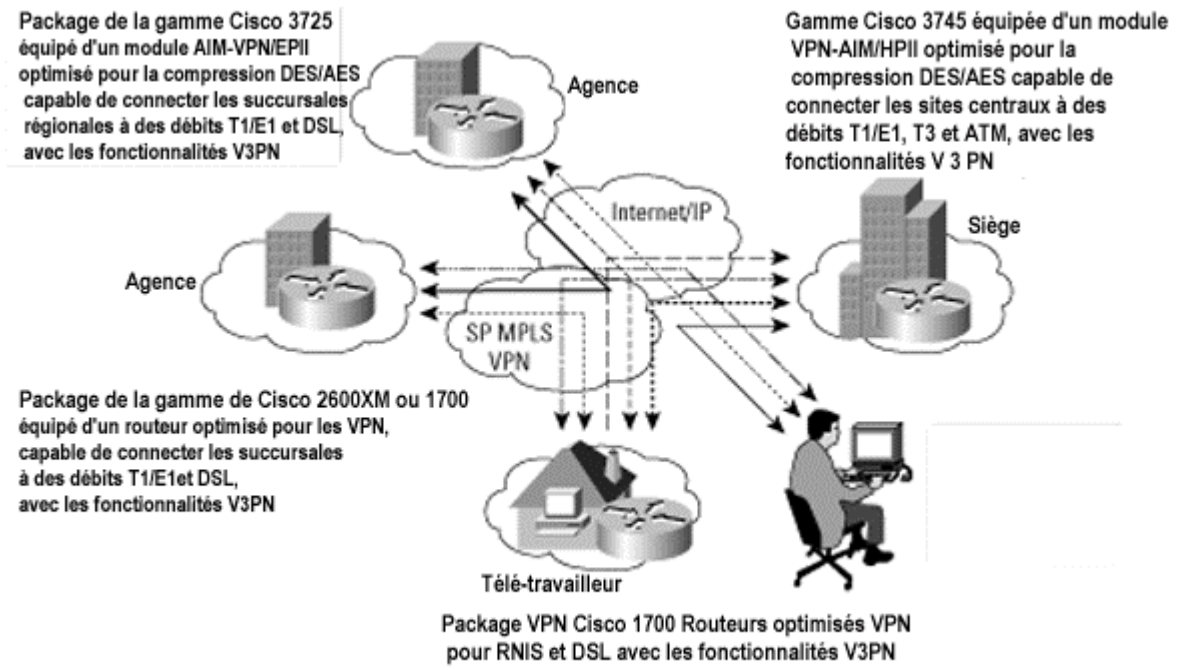
Figure 1 VPN IPSec compatible voix et vidéo Cisco



Multipoint dynamique pour IPSec

Avec la plate-forme logicielle Cisco IOS Version 12.2(13)T, Cisco introduit le multipoint dynamique (Dynamic Multipoint) pour IPSec. Actuellement, dans un réseau maillé, *tous* les tunnels IPSec point à point (ou les tunnels IPSec + GRE [Generic Routing Encapsulation]) doivent être configurés sur *tous* les équipements, même si certains, voire la plupart, de ces tunnels ne fonctionnent pas ou restent le plus souvent inutilisés. Avec la fonction Dynamic Multipoint VPN pour les routeurs Cisco, un routeur est désigné comme « concentrateur » et tous les autres routeurs « périphériques » sont configurés avec des tunnels en direction du concentrateur. Les tunnels concentrateurs – périphériques sont actifs en permanence. Toutefois, les routeurs « périphériques » ne disposent pas – et n'ont pas besoin non plus – de configuration pour des tunnels qui les relieraient entre eux. En revanche, lorsqu'un routeur « périphérique » veut transmettre un paquet à un autre périphérique – ou plutôt vers le sous-réseau qui se trouve derrière ce routeur périphérique – il utilise le protocole NHRP (Next Hop Resolution Protocol) pour déterminer de manière dynamique l'adresse de destination du routeur cible. Le routeur concentrateur joue le rôle de serveur NHRP et gère la requête pour le compte du routeur périphérique source. Les deux routeurs périphériques établissent alors – de manière dynamique – un tunnel IPSec entre eux (par l'intermédiaire de l'interface mGRE unique) pour permettre la transmission directe de données. Une fonction de temporisation désactive automatiquement le tunnel après une période d'inactivité prédéfinie (voir Figure 2).

Figure 2 VPN multipoint dynamique



Cisco Easy VPN

Cisco Easy VPN est une extension logicielle pour les routeurs et les dispositifs de sécurité Cisco qui simplifie considérablement le déploiement des VPN pour les bureaux distants et les télétravailleurs. Cisco Easy VPN s'articule autour de Cisco Unified Client Framework. Il centralise toute la gestion des clés et des politiques, et réduit la complexité du déploiement des VPN.

Les deux composants de Cisco Easy VPN sont Cisco Easy VPN Remote et Cisco Easy VPN Server Cisco Easy VPN Remote permet aux routeurs et aux dispositifs de sécurité Cisco d'établir et de gérer automatiquement un tunnel VPN vers un équipement sous Cisco Easy VPN Server en faisant l'économie des complications d'une configuration à distance. Cisco Easy VPN Server accepte les appels entrants des équipements sous Cisco Easy VPN Remote ou des clients logiciels VPN et garantit la mise à jour de leurs politiques de sécurité avant l' établissement de ces connextions.

Cisco Easy VPN fournit une méthode de gestion cohérente des politiques et des clés des connexions et offre un multiple choix d'équipements VPN distants – routeurs, clients hardware ou clients logiciels – lors d'un même déploiement vers n'importe quelle plateforme sous Cisco Easy VPN Server.

Norme de cryptage évoluée

Cisco supporte DES, 3DES et AES (Advanced Encryption Standard) sur la plate-forme logicielle Cisco IOS Version 12.2(13)T munie de la fonctionnalité IPSec. Cette fonction ajoute la prise en charge de la nouvelle norme de cryptage AES, en mode CBC (Cipher Block Chaining).

AES permet l'utilisation de clés de longueur variable – l'algorithme peut travailler sur des clés de 128 bits (par défaut), de 192 bits ou de 256 bits. Tous les packages VPN Cisco prennent en charge AES en mode logiciel et les routeurs 2691, 3725 et 3745 disposent d'une accélération AES matérielle.

AES a été développé par l'organisme de normalisation NIST (National Institute of Standards and Technology) en tant que nouvelle publication du FIPS (Federal Information Processing Standard). Pour des détails supplémentaires sur AES, visitez le site Web NIST : http://csrc.nist.gov/encryption/aes/.

Cisco VPN Client (supporte Easy VPN Remote)

Facile à déployer et à exploiter, Cisco VPN Client permet aux utilisateurs d'établir des tunnels sécurisés et cryptés de bout en bout vers n'importe quel serveur Cisco VPN. Le design détaillé de l'implémentation IPSec est disponible sur Cisco.com et un CD-ROM est livré avec chaque package routeur VPN. Le client peut être préconfiguré pour des déploiements multiples et les ouvertures de sessions initiales exigent très peu d'intervention de la part de l'utilisateur. Les configurations et les politiques d'accès VPN sont téléchargées à partir de la passerelle centrale et poussées vers le client au moment où la connexion est établie, ce qui offre une plus grande simplicité de déploiement et d'administration ainsi qu'une forte capacité d'extension. Cisco VPN Client assure le support de Windows 95 (OSR2+), 98, ME, NT 4.0, 2000, et XP, ainsi que de Linux (Intel), de Solaris (UltraSPARC – 32 et 64 bits) et de MacOS X 10.1 et 10.2 (Jaguar) (voir Figure 3).

Figure 3 Cisco VPN Client

Modules VPN pour les routeurs des gammes Cisco 1700, 2600XM, 3600 et 3700.

Les modules VPN inclus dans les packages routeurs VPN Cisco cryptent les données à l'aide des algorithmes DES et 3DES à des vitesses compatibles avec des connexions séries T1/E1 en mode full-duplex. Les modules de cryptage VPN gèrent un grand nombre de tâches IPSec, dont le cryptage, le hachage, l'échange de clés et le stockage des associations de sécurité – le processeur principal et la mémoire sont ainsi libres d'exécuter d'autres fonctions de routage, de transmission de la voix ou de firewall.

Les packages VPN Cisco 2691, 3725 et 3745 sont dotés de modules VPN qui offrent désormais le cryptage AES et la compression matérielle en plus des fonctionnalités DES et 3DES.

Firewall Cisco IOS avec détection des intrusions

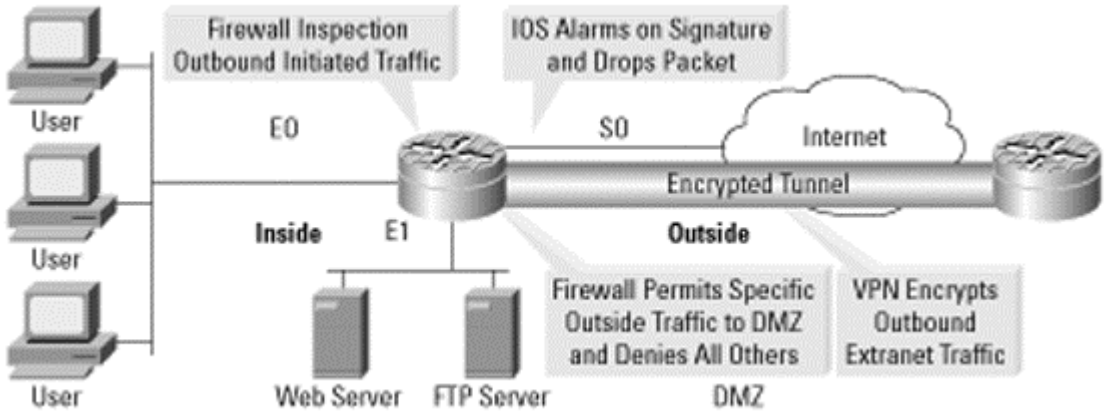
Le firewall Cisco IOS (avec détection des intrusions IDS intégrée au package) protège le réseau local des attaques de réseau (voir Figure 4).

Le contrôle d'accès contextuel CBAC (Context-Based Access Control) réalise un filtrage dynamique ou à inspection d'état application par application, ce qui permet au trafic autorisé de n'entrer sur le réseau local que si une session est active. Cette fonctionnalité CBAC est souvent considérée comme indispensable à l'efficacité d'un firewall. Le firewall Cisco IOS prend également en charge d'autres fonctions clés comme le blocage Java, la détection et la prévention des attaques par saturation, les pistes de vérification et les alertes en temps réel.

Les fonctions d'authentification, d'autorisation et d'accounting (AAA) du firewall Cisco IOS assurent l'authentification des utilisateurs distants, autorisent l'accès à certaines ressources spécifiques du réseau et rendent compte de cette activité. Le firewall Cisco IOS à détection d'intrusion (IDS) identifie 59 des attaques les plus courantes en utilisant des signatures pour déceler des trafics anormaux sur le réseau.

Les signatures de détection d'intrusion intégrées à la nouvelle version du firewall Cisco IOS ont été choisies dans un large échantillon représentatif de signatures de ce type. Ces signatures permettent de repérer les violations graves de la sécurité ainsi que les attaques réseau et les tentatives de récupération d'informations les plus courantes.

Figure 4 Firewall Cisco IOS avec détection des intrusions



Tunnellisation et cryptage

IPSec offre les services de sécurité de réseau suivants :

• Confidentialité – IPSec peut crypter les paquets avant de les transmettre sur un réseau.

• Intégrité – IPSec authentifie les paquets au niveau du destinataire pour s'assurer que les données n'ont pas été altérées au cours de la transmission.

• Authentification – les extrémités des tunnels IPSec authentifient la source de tous les paquets protégés par IPSec.

• Protection anti-réémission – IPSec empêche la capture et la réémission des paquets et contribue ainsi à déjouer les attaques par saturation.

• Tunnels cryptés – IPSec protège les données contre leur interception et leur consultation par des entités non-autorisées et réalise également l'encapsulation multiprotocole.

Le package logiciel IPSec de l'IOS prend en charge le cryptage DES (56 bits) et 3DES (168 bits). Avec la plate-forme logicielle Cisco IOS Version 12.2(13)T, le package logiciel IPSec de l'IOS prendra également en charge le cryptage AES. L'algorithme AES peut travailler sur des clés de 128 bits (par défaut), de 192 bits ou de 256 bits. Tous les packages VPN Cisco prennent en charge AES en mode logiciel et les routeurs 2691, 3725 et 3745 disposent d'une accélération AES matérielle.

L'encapsulation GRE avec IPSec est une solution originale développée par Cisco qui permet la transmission d'updates de routage sur le VPN et garantit ainsi une plus grande disponibilité du réseau que les solutions IPSec seules. En plus d'offrir un mécanisme de correction automatique en cas de panne, les tunnels GRE permettent de crypter les paquets multicast et broadcast ainsi que les protocoles non IP. Ainsi, grâce à l'association de GRE et d'IPSec, Cisco peut prendre en charge AppleTalk et Novell Internetwork Packet Exchange (IPX) sur sa solution VPN de site à site.

La fonction Cisco Tunnel Endpoint Discovery de la plate-forme logicielle Cisco IOS, améliore le déploiement à grande échelle des tunnels dans les environnements de réseau VPN maillé de site à site – en permettant aux connexions tunnellisées de s'auto-configurer de manière dynamique en fonction de la politique de sécurité du réseau et réduit ainsi la nécessité de configurer manuellement chaque tunnel point à point du VPN.

Dynamic Multipoint for IPSec, une fonction de la plate-forme logicielle Cisco IOS qui simplifie l'établissement de connexions entre site VPN distant dans une architecture « hub&spoke », permet à chaque routeur d'établir une connexion dynamique avec n'importe quel autre routeur en utilisant NHRP.

Certifications

Cisco s'est engagé à gérer un programme actif de certification et d'évaluation de ses produits pour ses clients du monde entier. Cisco, qui reconnaît toute l'importance de ces démarches pour ses clients, demeure l'un des premiers constructeurs du marché à commercialiser des produits certifiés et évalués. Cisco poursuit sa collaboration avec les organismes internationaux de normalisation en matière de sécurité afin de contribuer à modeler l'avenir des produits certifiés et évalués et continuera à œuvrer pour l'accélération des processus de certification et d'évaluation. Cet impératif est pris en compte dès les premières phases du cycle de développement d'un produit, et Cisco maintiendra sa politique de positionnement des produits de sécurité pour garantir à ses clients la plus grande diversité de produits certifiés et évalués capables de répondre à leurs besoins.

FIPS

Les routeurs Cisco des séries 1700, 2600, 3600 et 3700 ainsi que les modules VPN Cisco ont été conçus pour répondre aux normes de sécurité FIPS 140-1 niveau 2. Actuellement, seuls les routeurs Cisco 2611, 2651, 3640 et 3660 possèdent la certification FIPS 140-1 niveau 2. Le NIST a fait évoluer la norme FIPS 140-1 à FIPS 140-2. Cisco soumettra de nombreux routeurs à l'agrément FIPS 140-2 niveau 2. Pour connaître l'état actuel de la certification FIPS des produits Cisco, visitez :

http://www.cisco.com/warp/public/779/largeent/issues/security/secvpncert.html

ainsi que :

http://csrc.nist.gov/cryptval/.

IPSec ICSA

L'ICSA (International Computer Security Association) est un organisme commercial de certification de sécurité qui propose les certifications IPSec ICSA et Firewall ICSA pour différents types de produits de sécurité. Cisco participe au programme IPSec de l'ICSA ainsi qu'à son programme de firewall. Pour connaître l'état actuel de la certification ICSA des produits Cisco, visitez :

http://www.cisco.com/warp/public/779/largeent/issues/security/secvpncert.html

Common Criteria

Common Criteria est une norme internationale d'évaluation de la sécurité informatique. Développée par un consortium de pays afin de remplacer les nombreux processus d'évaluation de la sécurité propres à chaque nation, elle a pour vocation d'établir une norme unique à usage international. Actuellement, 14 pays reconnaissent officiellement la norme Common Criteria. Plusieurs versions de la plate-forme logicielle Cisco IOS IPSec et des routeurs Cisco ont été évalués dans le cadre du programme AISEP (Australasian Information Security Evaluation Program) pour vérifier leur conformité à l'ITSEC ou à Common Criteria. Pour connaître l'état actuel de la certification Common Criteria des produits Cisco, visitez :

http://www.cisco.com/warp/public/779/largeent/issues/security/secvpncert.html

ainsi que :

http://www.dsd.gov.au/infosec/aisep/EPL/ns.html

Utilitaires d'administration pour les réseaux VPN d'entreprise

CiscoWorks VPN/Security Management Solution

CiscoWorks VPN/Security Management Solution (VMS), qui fait partie intégrante du schéma directeur SAFE pour la sécurité des réseaux, réunit des utilitaires Web pour la configuration, la surveillance et le dépannage des VPN d'entreprise, des firewalls ainsi que des systèmes de détection des intrusions (IDS) réseaux et host-IDS. CiscoWorks VMS (voir Figure 5) offre la première base du secteur et le premier ensemble de fonctions à la fois robustes et évolutives capables de répondre aux besoins de déploiement de VPN de petite et de grande taille.
CiscoWorks VMS 2.1 se compose de centres d'administration pour les routeurs VPN Cisco, les firewalls Cisco PIX®, les sondes IDS et d'un centre de surveillance de la sécurité.

Caractéristiques

• Centres d'administration pour le routage VPN et centre de surveillance de la sécurité

• Nouvelle interface utilisateur, définition de rôle d'administrateur et de validation des processus

• SRH (Smart Rules Hierarchy) et groupements souples pour la duplication rapide des politiques de sécurité

• Contrôle exhaustif des modifications et fonctions d'audit

• Prise en charge centralisée du contrôle d'accès par rôle d'administrateur (RBAC)

Le centre d'administration des routeurs CiscoWorks Router Management Center, composant de CiscoWorks VMS, permet l'administration évolutive de la sécurité pour la configuration et le déploiement de connexions VPN. Le Router Management Center est un moyen puissant, adaptable et intuitif de configurer et de déployer des connexions VPN à grande échelle et de site à site. Il fournit un contrôle individuel des utilisateurs qui assurent les tâches de déploiement après approbation pour permettre aux grandes entreprises de définir de nombreux rôles administratifs et opérationnels. De

plus, le Router Management Center est doté d'une interface graphique utilisateur (GUI) pour simplifier la définition des politiques, un modèle de filiation hiérarchique, des options de déploiement souples et des capacités de reporting évoluées.

CiscoWorks VPN Monitor

CiscoWorks VPN Monitor est un utilitaire d'administration par le Web qui permet aux administrateurs de réseau de collecter, de stocker et de visualiser des informations sur les connexions VPN IPSec accès distant ou de site à site. Un tableau de bord facile à utiliser et configurable à partir d'un navigateur Web permet de visualiser de nombreux équipements (voir Figure 6). CiscoWorks VPN Monitor utilise la MIB (Management Information Base) IPSec prise en charge par tous les modules VPN des routeurs Cisco.

Chaque fois qu'un VPN est déployé, l'administrateur réseau doit être en mesure de surveiller l'état des tunnels et des équipements VPN pour garantir les meilleurs services VPN possibles. Il doit pour cela disposer des informations suivantes :

• nombre de tunnels opérationnels

• débit de chaque tunnel

• état des négociations de sécurité et des sessions

• état des performances des équipements VPN

• violations des seuils de performances.

CiscoWorks VMS fournit une solution unique d'administration intégrée pour configurer, surveiller et dépanner les firewalls, les VPNs et les équipements IDS du réseau et des hôtes. CiscoWorks VMS est seul à proposer des fonctions comme Auto Update et Smart Rules Hierarchy, qui permettent aux clients de déployer des infrastructures de sécurité à grande échelle.

Figure 6 CiscoWorks VPN Monitor

Cisco VPN Solution Center 2.2 (en option)

Grâce à Cisco VPN Solution Center (VPNSC) version 2.2, le même utilitaire offre désormais au fournisseur de services la possibilité de gérer à la fois les VPN IPSec et les VPN IP sur MPLS (Multiprotocol Label Switching). De plus, VPNSC met à sa disposition une suite de solutions d'administration de services qui lui permet de planifier, de dimensionner, d'exploiter et de facturer les services VPN.

Les fournisseurs de services réalisent maintenant des VPN qui intègrent des commutateurs WAN, des routeurs, des firewalls, des concentrateurs VPN. Ils doivent administrer tous ces équipements sur l'ensemble de leur infrastructure réseau et proposer à leur clients des contrats de niveau de service. Ils ont également besoin de permettre à leurs clients de personnaliser leur accès aux services et aux applications du réseau. VPNSC leur apporte dès à présent la première solution d'administration de services VPN économique de qualité opérateur télécoms qui leur permet de déployer rapidement les services VPN externalisés que de nombreuses entreprises réclament aujourd'hui. Le portefeuille se compose de services VPN IPSec avec toutes les autres fonctions de Cisco IOS sur des plates-formes adaptées à chaque site, du petit bureau jusqu'au siège social d'entreprise. Cisco VPNSC offre :

• la possibilité de dimensionner les VPN IP IPSec en configurant un tunnel IKE et IPSec entre les équipements Cisco – tous les équipements Cisco IOS

• des vues topologiques complètes et détaillées du concentrateur et des périphériques, avec maillage VPN complet , partiel ou de type Hub&spoke.

• la possibilité de constituer les topologies VPN de leur choix en ajoutant de multiples sites au VPN, y compris des VPN extranet et intranet

• le dimensionnement et l'audit des fonctions IPSec de site à site

• la surveillance des contrats de niveau de service pour IPSec et MPLS

• un gestionaire de tâches .

• des collecteurs d'événements API, y compris le bus d'événements TIBCO et le collecteur d'événements API CORBA (Common Object Request Broker Architecture)

• une interface XML (Extensible Markup Language) pour faciliter l'importation et l'exportation de données vers le Cisco VPN Solution Center

Cisco VPNSC 2.2 supporte les routeurs des gammes Cisco 1700 et 2600 en tant qu'équipements clients MPLS et qu'équipements IPSec pour permettre au fournisseur de services de gérer des VPN IPSec et MPLS. Le routeur Cisco 2691, qui subit actuellement des tests de fonctionnalité PE sur une version IOS en cours de dévelopement, n'est pas encore supporté.

Cisco VPNSC 2.2 supporte également les routeurs des gammes Cisco 3600 et 3700 en tant qu'équipements client MPLS et équipements IPSec. De plus, les routeurs Cisco 3640, 3660 et 3700 peuvent être supportés en tant qu'équipements PE grâce à Cisco VPNSC 2.2.

Caractéristiques techniques et performances

Le test de performances a été réalisé en mode Fast Ethernet full-duplex et Ethernet vers un SmartBits SMB2000 de Spirent Communications qui opère en tant que générateur et compteur de trafic full-duplex. Des paquets ICMP (Internet Control Message Protocol) ont été générés par SmartBits via Ethernet en direction d'un équipement testé. L'utilitaire de test SmartBits supporte par défaut une définition de paquets mixtes appelée IMIX. Le trafic IMIX est défini par les flux suivants dans l'application Smart Windows :

• sept flux de données en paquets de 64 octets

• quatre flux de données en paquets de 570 octets

• un flux de données en paquets de 1518 octets

Le Tableau 1 détaille les caractéristiques des châssis, le Tableau 2 présente les informations relatives à la commande des matériels et le Tableau 3 résume les différentes données.

Table 1 Packages VPN Cisco

Package	Fire wall avec IDS	GRE et IPSec	*Compression IPPCP (IP Payload Compression Protocol)	**Haute disponi-bilité ou reprise	***VPN MPLS	QoS VPN	AES matériel	Tunnels max.	Paquets 3DES IMIX	3DES Mbps Packet 1400
Packages Cisco 1700	Oui	Oui	Logicielle	Oui	CPE	Oui	Non	100	3.5	8
Packages Cisco 2600XM	Oui	Oui	Logicielle	Oui	CPE	Oui	Non	800	4	14
VPN Cisco 2691	Oui	Oui	Matérielle	Oui	CPE	Oui	Oui	800	25	80
VPN Cisco 3640A	Oui	Oui	Logicielle	Oui	PE	Oui	Non	1000	5	18
VPN Cisco 3662	Oui	Oui	Logicielle	Oui	PE	Oui	Oui	1800	9	40
VPN Cisco 3725	Oui	Oui	Matérielle	Oui	PE	Oui	Non	2000	47	150
VPN Cisco 3745	Oui	Oui	Matérielle	Oui	PE	Oui	Oui	2000	75	180.

Remarque : les débits 3DES en Mbits/s sont déterminés à partir de tests sur des routeurs Fast Ethernet dos à dos ; les débits constatés peuvent varier en fonction du débit WAN, de la capacité mémoire et des autres applications exécutées par la plate-forme logicielle Cisco IOS.
* La compression IPPCP logicielle de couche 3 est désormais compatible avec les modules VPN actuels. Ceci permet au protocole IPPCP de s'exécuter sur le processeur du routeur (exige Cisco IOS version 12.2(13) T ou ultérieure).
**Haute disponibilité ou reprise : prise en charge par Cisco IOS des protocoles RRI (Reverse Route Injection) et HSRP (Hot Standby Router Protocol) avec IPSec.
*** MPLS : tous les packages routeurs sécurité et VPN prennent en charge les extensions MPLS pour les routeurs d'extrémité client. L'extrémité client VRF (multi-VPN routing and forwarding) élargit la fonctionnalité limitée de PE au routeur d'extrémité client dans un modèle VPN MPLS. Les routeurs d'extrémité client ont désormais la capacité de gérer des tables VRF distinctes.

Le Tableau 2 présente les informations de commande de matériel des packages routeurs VPN Cisco.

Tableau 2 Commande des packages routeurs VPN

Référence Cisco	Description	Cartes WIC disponibles en option	Modules de réseau disponibles en option	Secours RNIS ou analogique en option
CISCO1721-VPN/K9	Package VPN Cisco 1721 avec module VPN, 64 Mo DRAM, IP Plus/FW/3DES	Oui	Non	Oui
CISCO1721-VPN/K9-A	Package VPN Cisco 1721 avec WIC ADSL, module VPN, 64 Mo DRAM, IP Plus/FW/3DES	Oui	Non	Oui
CISCO1751-VPN/K9	Package VPN Cisco 1751 avec module VPN, 64 Mo DRAM, IP Plus/FW/3DES	Oui	Non	Oui

Référence Cisco	Description	Cartes WIC disponibles en option	Modules de réseau disponibles en option	Secours RNIS ou analogique en option
CISCO1751-VPN/K9-A	Package VPN Cisco 1751 avec WIC ADSL, module VPN, 64 Mo DRAM, IP Plus/FW/3DES	Oui	Non	Oui
CISCO1760-VPN/K9	Package VPN Cisco 1760 avec module VPN, 64 Mo DRAM, IP Plus/FW/3DES	Oui	Non	Oui
CISCO1760-VPN/K9-A	Package VPN Cisco 1760 avec WIC ADSL, module VPN, 64 Mo DRAM, IP Plus/FW/3DES	Oui	Non	Oui
CISCO1760-V3PN/K9	Package VPN Cisco 1760 V^{3}PN avec WIC ADSL, module VPN, 32 Mo Flash, 96 Mo DRAM, unité de traitement numérique du signal (DSP) 4 voies, IP Plus/ADSL/VOX/FW/IDS/3DES	Oui	Non	Oui
C2611XM-2FE/VPN/K9	Package VPN Cisco 2611XM, AIM-VPN/EP/2FE/IOS FW/ IPSec 3DES, 96 Mo DRAM	Oui	Oui	Oui
C2621XM-2FE/VPN/K9	Package VPN Cisco 2621XM, AIM-VPN/EP/2FE/IOS FW/ IPSec 3DES, 96 Mo DRAM	Oui	Oui	Oui
C2651XM-2FE/VPN/K9	Package VPN Cisco 2651XM, AIM-VPN/EP/2FE/IOS FW/ IPSec 3DES, 96 Mo DRAM	Oui	Oui	Oui
C2691-VPN/K9	Package VPN Cisco 2691, AIM-VPN/EPII, Plus FW/ IPSec 3DES, 128 Mo DRAM	Oui	Oui	Oui
C3640A-2FE/VPN/K9	Package VPN Cisco 3640, NM-VPN/MP, 2 ports FE, Cisco IOS FW/IPSec 3DES, 2 WAN, 64 Mo DRAM	Oui	Oui	Oui

Tableau 2 Commande des packages de routeurs VPN

Référence Cisco	Description	Cartes WIC disponibles en option	Modules de réseau disponibles en option	Secours RNIS ou analogique en option
C3662-2FE/VPN/K9	Package VPN Cisco 3662, AIM-VPN/HP, 2×FE, Cisco IOS FW/IPSec 3DES, 96 Mo DRAM	Oui	Oui	Oui
C3725-VPN/K9	Package VPN Cisco 3725, AIM-VPN/EPII, Plus Cisco IOS FW/IPSec 3DES, 128 Mo DRAM	Oui	Oui	Oui
C3745-VPN/K9	Package VPN Cisco 3745, AIM-VPN/HPII, Plus Cisco IOS FW/IPSec 3DES, 128 Mo DRAM	Oui	Oui	Oui

Remarque : dans tous les cas, les packages sont livrés avec l'image logicielle Cisco IOS IPSec la plus récente disponible pour la plate-forme.

En résumé

Bâtis autour de la plate-forme logicielle Cisco IOS, les routeurs VPN Cisco tirent parti des meilleurs services réseaux du marché pour établir un standart des solutions VPN de site à site.

• *Support de divers environnements de mise en réseau* – IPSec est un protocole unicast IP seulement. Les routeurs VPN Cisco, qui exploitent les fonctions de la plate-forme logicielle Cisco IOS, autorisent le trafic multicast et multiprotocole ainsi que le routage sur les VPN et offrent ainsi des solutions adaptables pour les environnements VPN les plus variés.

• *Acheminement rapide et fiable du trafic sensible aux délais* – les fonctionnalités de gestion de la bande passante des routeurs VPN Cisco permettent de classer le trafic jusqu'à la couche application et autorisent ainsi la mise en place de politiques différenciées de qualité de service (QoS) par véritable type d'application, et pas seulement en fonction des numéros de port TCP.

• *V³PN* – V³PN offre une infrastructure VPN capable de transporter le trafic convergent voix, vidéo et données sur un réseau sécurisé IPSec.

• *Capacité d'extension des VPN spécifique aux sites* – Cisco fournit la plus large gamme d'équipements VPN complets qui s'étend des routeurs VPN de tête de réseau dédiés jusqu'aux solutions de routeurs VPN à boîtier unique pour les bureaux distants, comprenant les interfaces WAN et un firewall à inspection d'état.

Les packages sécurité et VPN des gammes Cisco 1700, 2600, 3600 et 3700 permettent aux entreprises comme aux fournisseurs de services de déployer facilement des routeurs Cisco en tant que VPN pour bénéficier de services nouveaux et puissants. Ces packages complètent de manière idéale les packages VPN Cisco 7100 et 7200 également disponibles auprès de Cisco et permettent à nos clients de bénéficier d'une large gamme de produits VPN en terme de fonctionnalités et de coûts.

Table 3 Résumé des caractéristiques des châssis

Package routeur VPN	Ports Fast-Ethernet	Emplace-ment combiné pour carte WIC ou VWIC	Emplacement combiné pour carte VIC (Voice Interface Card) ou emplacements pour cartes WIC ou VWIC	Empla-cement s pour cartes VIC seuls	Empla-cements pour modules de réseau	Plate-forme logicielle IOS Cisco	Mémoire Flash (Mo)*	Mémoi-re DRAM (Mo)*	Carte VPN	Autres modules
c1721-VPN/K9	1	2	–	–	–	IP Plus/FW/ IDS/3DES	16	64	MOD1700-VPN	En option
c1721-VPN/K9-A	1	2	–	–	–	IP Plus/FW/ IDS/3DES	16	64	MOD1700-VPN	Carte WIC à 1 port ADSL intégrée
c1751-VPN/K9	1	–	2	1	–	IP Plus/FW/ IDS/3DES	16	64	MOD1700-VPN	En option
c1751-VPN/K9-A	1	–	2	1	–	IP Plus/FW/ IDS/3DES	16	64	MOD1700-VPN	Carte WIC à 1 port ADSL intégrée
c1760-VPN/K9	1	–	2	2	–	IP Plus/FW/ IDS/3DES	16	64	MOD1700-VPN	En option
c1760-VPN/K9-A	1	–	2	2	–	IP Plus/FW/ IDS/3DES	16	64	MOD1700-VPN	Carte WIC à 1 port ADSL intégrée
c1760-V3PN/K9	1	–	2	2	–	IP Plus/ ADSL/VOX/ FW/IDS/ 3DES	32	96	MOD1700-VPN	DSP à 4 voies intégré
c2611XM-VPN/K9 **c2621XM-VPN/K9**										
c2651XM-VPN/K9	2	2	–	–	1	IP Plus/FW/ IDS/3DES	32	96	AIM-VPN/EP	En option
c2691-VPN/K9	2	3	–	–	1	IP Plus/FW/ IDS/3DES	32	128	AIM-VPN/EPII **	En option
3640A-VPN/K9	2	2	–	–	4	IP Plus/FW/ IDS/3DES	16	64	AIM-VPN/MP	En option
3662-VPN/K9	2	2	–	–	6	IP Plus/FW/ IDS/3DES	32	96	AIM-VPN/HP	En option
3725-VPN/K9	2	3	–	–	2	IP Plus/FW/ IDS/3DES	32	128	AIM-VPN/EPII **	En option
3745-VPN/K9	2	3	–	–	4	IP Plus/FW/ IDS/3DES	32	128	AIM-VPN/HPII**	En option

* Tous les packages Cisco 1700, 2600 et 3600 sont équipés de mémoire Flash et DRAM supplémentaire.
** Les modules VPN Cisco 2691, 3725 et 3745 prennent en charge DES, 3DES, AES et la compression.

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 européen

Cisco Systems Europe

11 rue Camilles Desmoulins

92782 Issy Les moulineaux Cédex 9

France

www-europe.cisco.com

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 fax sur le site Web de Cisco 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

(0208R)

LW3851 11/02