FONCTIONS DE SÉCURITÉ DES ROUTEURS À SERVICES INTÉGRÉS CISCO 1800, 2800 ET 3800

Cette fiche technique décrit les fonctions de sécurité des routeurs à services intégrés Cisco® 1800, 2800 et 3800

DESCRIPTION DU PRODUIT

Cisco Systems révolutionne le routage avec une nouvelle gamme de routeurs à services intégrés spécifiquement conçus pour délivrer à la vitesse du câble des services convergents vidéo, voix, données. Fruit de vingt années d'innovation et d'expertise dans le domaine des technologies Internet, la gamme de routeurs à services intégrés Cisco® 1800, 2800 et 3800 intègre au sein d'un même système de routage, des services de téléphonie d'entreprise, des services de routage multi protocole et des services de sécurité d'entreprise. Ces plateformes apportent une solution complètement intégrée qui est parfaitement adaptée aux besoins des entreprises en termes de services, de performances et de sécurité. La gamme Cisco® 3800 est conçue autour d'une nouvelle architecture interne qui se caractérise, en plus de plus de puissance, par une très haute densité d'interface et une très haute fiabilité. Cette nouvelle architecture s'articule autour d'ASIC spécialisés et intègre de façon native dans son hardware la sécurité, la téléphonie d'entreprise et le traitement des flux multimédia.

Composante clé de la stratégie «les réseaux qui se défendent tout seuls» (Cisco Self-Defending Network), les routeurs à services intégrés Cisco ISR permettent la conception d'infrastructures de routage robustes dotées de fonctions de sécurité adaptées aux évolutions de la physionomie du risque. Avec de puissantes fonctionnalités comme les réseaux VPN, l'accélération matérielle de l'encryption, un pare-feu à inspection d'état, un système de prévention des intrusions (IPS), des modules réseau de diffusion de contenus (gammes Cisco 2800 et 3800), Cisco fournit la solution de sécurité la plus robuste et la plus adaptable du marché pour les sites distants d'entreprise.

En associant les fonctionnalités éprouvées de la plate-forme logicielle Cisco IOS, une connectivité de réseau LAN et WAN parmi les plus riches de l'industrie, des fonctions de sécurité conformes aux critères communs de qualité, les solutions de sécurité intégrées permettent à nos clients de bénéficier des avantages suivants :

- «Exploitez ce que vous avez» – vous tirez le meilleur parti de votre infrastructure de réseau existante tandis que la plate-forme logicielle Cisco IOS active de nouvelles fonctions de sécurité sur le routeur sans qu'il soit nécessaire d'acquérir des serveurs supplémentaires ;
- «Déployez la sécurité aux endroits stratégiques» – vous disposez d'une souplesse totale qui vous permet de mettre en œuvre les fonctionnalités de sécurité comme les pare-feu, les systèmes de prévention des intrusions (IPS) et les VPN aux points névralgiques de votre réseau pour en maximiser la protection ;
- «Protégez vos passerelles» – vous déployez les meilleures fonctionnalités de sécurité du marché à tous les points d'entrée de votre réseau ;
- «Gagnez du temps et de l'argent» – vous réduisez le nombre d'unités dont vous avez besoin et donc les coûts de formation et de gestion associés ;
- «Protégez votre infrastructure» – vous protégez votre routeur et vous vous défendez ainsi contre les menaces qui visent directement l'infrastructure réseau comme les attaques par saturation et dépassement de capacité.

CISCO LE RÉSEAU QUI SE DÉFEND TOUT SEUL

Les routeurs Cisco 1800, 2800 et 3800 supportent un vaste éventail de fonctions de sécurité qui agissent dans le cadre de la stratégie des réseaux qui se défendent tout seuls, une solution qui permet aux organisations de toutes natures d'identifier et de prévenir les menaces de sécurité et d'y réagir efficacement. Le réseau à autodéfense Cisco (Cisco Self-Defending Network) dispose de quatre catégories de protection qui s'appliquent au niveau du routeur :

- Connectivité sécurisée – vous bénéficiez d'une connectivité de réseau sécurisée et évolutive qui reconnaît de nombreux types de trafics simples mais aussi complexes tels que les trafics voix et vidéo. La conception d'architectures VPN de grande tailles fait partie des services disponibles en standards dans cette nouvelle gamme de routeurs. Ces services VPN sont renforcés en terme de robustesse et simplifiés en terme de configuration grâce aux fonctions DMVPN (Dynamic Multipoint VPN), Multi-VRF, MPLS Secure Contexts, et V3PN (Voice and Video Enabled VPN),

- la défense contre les menaces Internet – elle consiste à faire en sorte que le réseau sache détecter et maîtriser dynamiquement les attaques circulant à travers lui grâce à des services de blocage ou de confinement des attaques comme le système Cisco IPS (Intrusion Prevention System) et le pare-feu à inspection d'état Cisco IOS ;
- la sécurisation et l'identification – le réseau protège de manière intelligente les points d'extrémité grâce à des technologies de contrôle renforcé à l'accès comme le service NAC (Network Admission Control) et les services d'identification AAA (Autorisation, Authentification, Administration)
- la protection de l'infrastructure de réseau – l'infrastructure de votre réseau est protégée des attaques dont elle serait elle-même la cible, et ce grâce à des fonctions comme la protection du plan de contrôle (protection des fonctions systèmes du routeur) la reconnaissance des applications complexes NBAR (Network-Based Application Recognition) et AutoSecure (durcissement du routeur)

FONCTIONNALITÉ DES ROUTEURS À SERVICES INTÉGRÉS

Les fonctions de sécurité des routeurs des gammes Cisco 1800, 2800 et 3800 sont distribuées dans les ensembles de fonctionnalités des packages logiciels Cisco IOS suivants :

- Advanced Enterprise Services
- Advanced Enterprise Services
- Advanced Security

Pour savoir comment choisir les fonctionnalités, visitez :
http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/prod_bulletin09186a00801af451.html

CONNECTIVITÉ SÉCURISÉE : TUNNELLISATION ET CRYPTAGE VPN, DMVPN, EASY VPN, V3PN ET CONTEXTES MULTI-VRF

Tunnellisation et cryptage des VPN

Les VPN sont le mode de connectivité de réseau qui a connu la plus forte croissance et Cisco renforce sa valeur ajoutée dans ce domaine en intégrant les fonctions correspondantes au niveau matériel dans la gamme routeurs à services intégrés. Les routeurs Cisco 1800, 2800 et 3800 sont équipés d'une accélération matérielle intégrée des fonctions de cryptage qui décharge le processeur des tâches de cryptage IPSec (AES, 3DES et DES) et des processus VPN pour augmenter le débit des réseaux privé virtuels. Si l'utilisateur souhaite accroître encore le débit des VPN ou leur évolutivité, les modules AIM (Advanced Integration Module) plus puissants sont disponibles en option pour le cryptage matériel haute performance. Résultat : des VPN aux performances améliorées – jusqu'à quatre fois plus rapides qu'avec les modèles précédents – et la réduction de l'utilisation globale du processeur. Le module AIM en option offre des performances de cryptage jusqu'à dix fois supérieures à celles des modèles précédents tout en permettant l'évolutivité de la tunnellisation. Parmi les principales fonctions des accélérateurs VPN intégrés et sur module AIM, signalons :

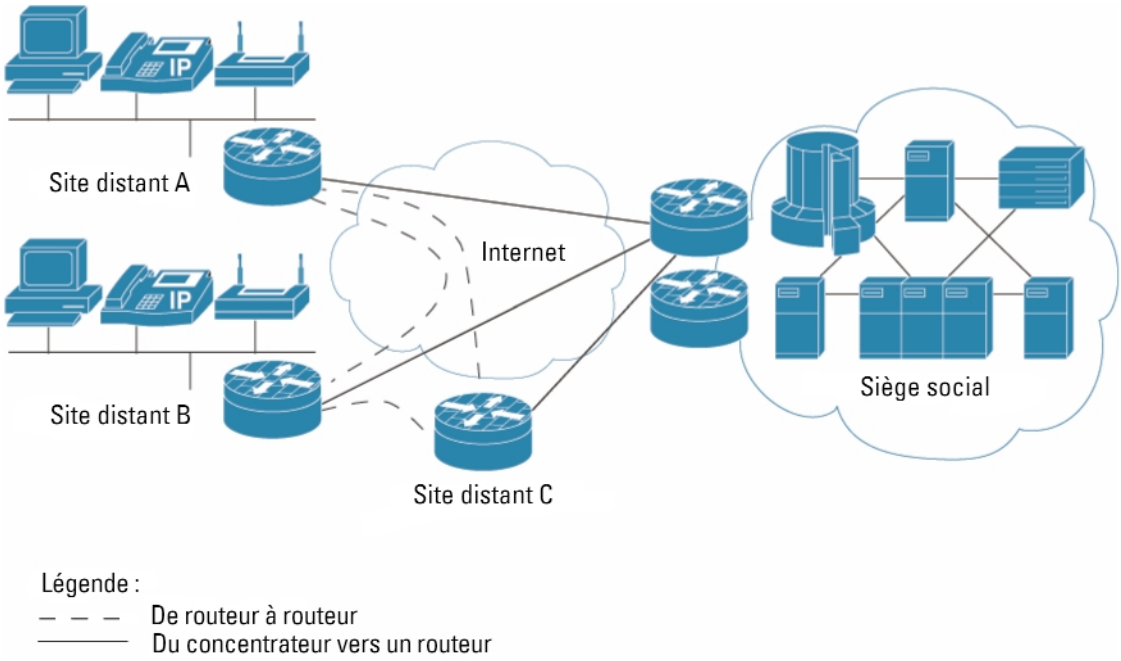
- l'accélération du cryptage IPSec à des vitesses compatibles avec des débits T3/E3 full-duplex multiples,
- l'accélération matérielle des algorithmes de cryptage DES, 3DES et AES (128, 192 et 256) sur tous les modules (intégré et AIM),
- le support des signatures de l'algorithme RSA (Rivest, Shamir, Aldeman) et Diffie-Hellman pour l'authentification,
- l'utilisation des algorithmes de hachage SHA-1 (Secure Hash Algorithm 1) ou MD5 (Message Digest Algorithm 5) qui garantissent l'intégrité des données,
- le support de la compression de couche 3 (IPPCP) au niveau matériel avec l'ajout du module de cryptage des VPN.

En plus des services génériques IPSec, les routeurs à services intégrés peuvent également utiliser une technique de tunnellisation particulière qui associe les protocoles IPSec et GRE (Generic Routing Encapsulation). L'encapsulation GRE avec IPSec est une solution originale développée par Cisco qui permet la transmission de protocoles de routage dynamiques sur le VPN et garantit ainsi une plus grande robustesse de 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 autres que IP. Avec la tunnellisation GRE – IPSec, les routeurs à services intégré Cisco peuvent supporter des protocoles comme AppleTalk et IPX (Internetwork Packet Exchange) de Novell ainsi que des applications multicast et broadcast comme la vidéo.

Dynamic Multipoint VPN (DMVPN)

Avec les premiers routeurs à offrir la fonctionnalité DMVPN, Cisco se place résolument en tête de l'industrie. Cisco DMVPN permet d'établir à la demande des tunnels VPN sites distants vers sites distants. Ceci permet la reproduction d'un maillage complet du réseaux VPN qui permet de réduire les risques de latence lorsque le trafic remonte vers un site de concentration, économise la bande passante et simplifient considérablement le déploiement des architectures VPN (voir la Figure 1). Le service DMVPN s'appuie sur le savoir-faire de Cisco en matière de routage et de protocole IPSec en permettant la configuration dynamique des tunnels GRE, du cryptage IPSec et des protocoles NHRP (Next Hop Resolution Protocol), OSPF et EIGRP. Cette configuration dynamique des tunnels VPN associée à des technologies comme la qualité de service (QoS) et le multicast, optimise le déploiement des applications sensibles aux temps de latence comme la voix et la vidéo. DMVPN réduit également les tâches administratives en éliminant la nécessité de reconfigurer un concentrateur VPN central pour ajouter de nouveaux routeurs périphériques ou pour établir des connexions entre deux de ces routeurs périphériques.

Figure 1. Exemple de solution DMVPN



Easy VPN

Easy VPN est une solution IPSec conçue pour supporter aisément et de manière très évolutive les topologies VPN à concentrateur et routeurs périphériques. Easy VPN simplifie le dimensionnement et la gestion des solutions VPN entre des pare-feu PIX, des VPN 3000 et des routeurs de toutes tailles. Easy VPN, qui a fait ses preuves au travers de plusieurs milliers d'installations clients, utilise une technologie de téléchargement des politiques («policy push») pour simplifier la configuration tout en garantissant une grande diversité de fonctionnalités et le contrôle des politiques.

Easy VPN présente les avantages suivants :

- Easy VPN supporte aussi bien les clients VPN matériels (routeurs d'accès, pare-feu PIX) que les clients VPN logiciels distants à partir d'un même routeur installé sur le site central. Le client logiciel Cisco VPN Software Client peut être installé sur des PC, des Mac et des systèmes UNIX pour fournir, sans supplément de coût, une connectivité d'accès à distance aux VPN du routeur. La même technologie (Easy VPN) sert à la fois aux clients VPN matériels et aux clients VPN logiciels, ce qui se traduit par une réduction du coût total d'acquisition grâce à la simplification et à l'unification des services de dimensionnement, de surveillance et AAA (Authentification, Autorisation, Administration).
- Easy VPN offre des options d'authentification locale sur le routeur ou centralisée de type RADIUS et AAA portant aussi bien sur les équipements de routage clients que sur les utilisateurs individuels. L'authentification 802.1x permet également d'authentifier les hôtes sur chaque site d'équipement client.

- Easy VPN supporte l'utilisation des certificats digitaux, ce qui améliore la sécurité par rapport aux échanges préalables de clés.
- L'équilibrage de charge sur de multiples concentrateurs Easy VPN au site central permet une répartition automatique de la charge sur de nombreux serveurs Easy VPN. Le téléchargement de politique vers les équipements clients à partir des informations sauvegardées sur le concentrateur permet de faire évoluer la solution sans avoir à reconfigurer ces équipements.
- Le serveur Easy VPN virtualisé donne aux fournisseurs de services la possibilité d'offrir des services VPN à un grand nombre de clients à partir d'une plate-forme unique.
- Easy VPN offre une intégration de l'ensemble des fonctionnalités, notamment l'affectation dynamique de politiques de qualité de service (QoS), le pare-feu et le système IPS de prévention des intrusions, la tunnellisation partagée ainsi que SAA (Service Assurance Agent) et NetFlow pour la surveillance des performances.
- Cisco SDM (Security Device Manager) permet un déploiement rapide et assisté de Easy VPN avec AAA et pare-feu, ainsi qu'une surveillance graphique en temps réel des clients Easy VPN distants, tandis que Easy VPN Server Administrator donne la possibilité de fermer les sessions des clients distants.
- Easy VPN est supporté sur toutes les gammes de produits de services Cisco VPN : la plate-forme logicielle Cisco IOS, les pare-feu Cisco PIX® et la gamme de concentrateurs Cisco VPN 3000

V3PN : VPN IPSec compatible voix et vidéo

Les routeurs des gammes Cisco 1800, 2800 et 3800 supportent le service V3PN. V3PN correspond à la capacité pour l'infrastructure de réaliser une architecture VPN qui permet la convergence des données, de la voix et de la vidéo sur un réseau IPSec sécurisé avec qualité de service (QoS). Sur un transport IP, les utilisateurs obtiennent ainsi – de manière sécurisée et économique – les mêmes performances pour leurs applications voix et vidéo que sur une liaison de réseau WAN. Contrairement à la plupart des unités VPN du marché, les routeurs à services intégrés Cisco se plient aux nombreuses exigences de trafic et de topologie de réseau qui autorisent les VPN IPSec multiservice. L'architecture de réseau de bout en bout V3PN exploite les routeurs sécurisés Cisco et la plate-forme logicielle Cisco IOS pour protéger le trafic voix.

L'établissement de VPN IPSec voix et données de haute qualité exige beaucoup plus que la simple capacité à crypter le trafic – il faut pouvoir disposer d'un ensemble harmonisé de technologies multiservices et VPN IPSec évoluées. Les principales technologies de la plate-forme logicielle Cisco IOS qui permettent la mise en œuvre des V3PN Cisco sont les suivantes : qualité de service (QoS) centrée sur le multiservice, support des différents types de trafic et des topologies de réseau multiservice et fonctionnalités améliorées de reprise réseau.

Contextes sécurisés Multi-VRF et MPLS pour les fournisseurs de services

Multi-VRF, également appelé VRF-Lite, permet de configurer et de gérer plusieurs instances d'une table de routage et de transfert sur le même routeur physique. En association avec les technologies VLAN Ethernet VLAN et VPN WAN comme Frame Relay, Multi-VRF permet de fournir plusieurs services logiques sur un même réseau physique, apportant ainsi la confidentialité et la sécurité jusqu'au réseau local d'un site distant.

Un même routeur Cisco avec Multi-VRF peut supporter plusieurs organisations avec des plans adressages IP superposées tout en garantissant le cloisonnement des données, du routage et des interfaces physiques. Pour plus d'informations sur Multi-VRF, consultez le Product Bulletin.

DÉFENSE CONTRE LES MENACES LIÉES AU «CYBER RISQUE» : PARE-FEU CISCO IOS, PARE-FEU TRANSPARENT, PRÉVENTION DES INTRUSIONS, FILTRAGE DES URL ET SÉCURITÉ DES CONTENUS

Pare-feu Cisco IOS

Le pare-feu Cisco IOS est un service de pare-feu à inspection d'état parmi les meilleures du intégré aux routeurs Cisco. Développé à partir des technologies de pare-feu PIX –marché – le pare-feu Cisco IOS est supporté par tous les routeurs à services intégrés exécutant au minimum l'ensemble de fonctionnalités Advanced Sécurité de la plate-forme logicielle Cisco IOS. Solution de sécurité et de routage tout en un, le pare-feu Cisco IOS est idéal pour protéger le point d'entrée WAN de votre réseau. Bien que le concentrateur soit généralement le lieu d'installation d'un pare-feu et d'inspection du trafic malveillant, ce n'est pas le seul emplacement à envisager pour le déploiement d'une solution de sécurité efficace. Les sites distants sont également des points vulnérables de votre réseau où le trafic doit être filtré et inspecté.

Les principales fonctionnalités du pare-feu Cisco IOS comprennent :

- le pare-feu à inspection d'état avec protection contre les attaques par débordement de capacité,
- la sensibilité améliorée aux applications, au trafic et aux utilisateurs pour l'identification, l'inspection et le contrôle des applications,
- l'inspection évoluée des protocoles pour la voix, la vidéo et les autres applications complexes,
- les politiques de sécurité par utilisateur, par interface ou par sous-interface,
- les services d'identification fortement intégrés fournissant l'authentification et l'autorisation par utilisateur,
- la simplicité de gestion grâce à des fonctions comme l'accès par rôle et les vues de l'interface de commande en ligne qui réalisent une séparation logique et sécurisée du routeur entre les administrateurs sécurité et les administrateurs infrastructure.

Le pare-feu Cisco IOS ne se contente pas de réaliser un point de protection unique sur le périmètre du réseau : il contribue également à garantir que l'application de la politique de sécurité demeure une composante inhérente du réseau lui-même. Par leur souplesse et les économies réalisées, les deux modes d'application des politiques – dédié et intégré – simplifient les solutions de sécurité sur les périmètres extranet et intranet ainsi que sur la connectivité Internet des bureaux ou des sites distants. Intégré au réseau grâce à la plate-forme logicielle Cisco IOS, le pare-feu Cisco IOS donne également aux utilisateurs la possibilité d'exploiter les fonctionnalités évoluées de qualité de service (QoS) sur le même routeur.

Cisco IOS supporte le pare-feu IPv6 qui autorise un déploiement dans des environnements mixtes IPv4 et IPv6. Le pare-feu Cisco IOS IPv6 permet l'inspection d'état des protocoles (détection des anomalies) des paquets IPv6 ainsi que la prévention IPv6 des attaques par saturation.

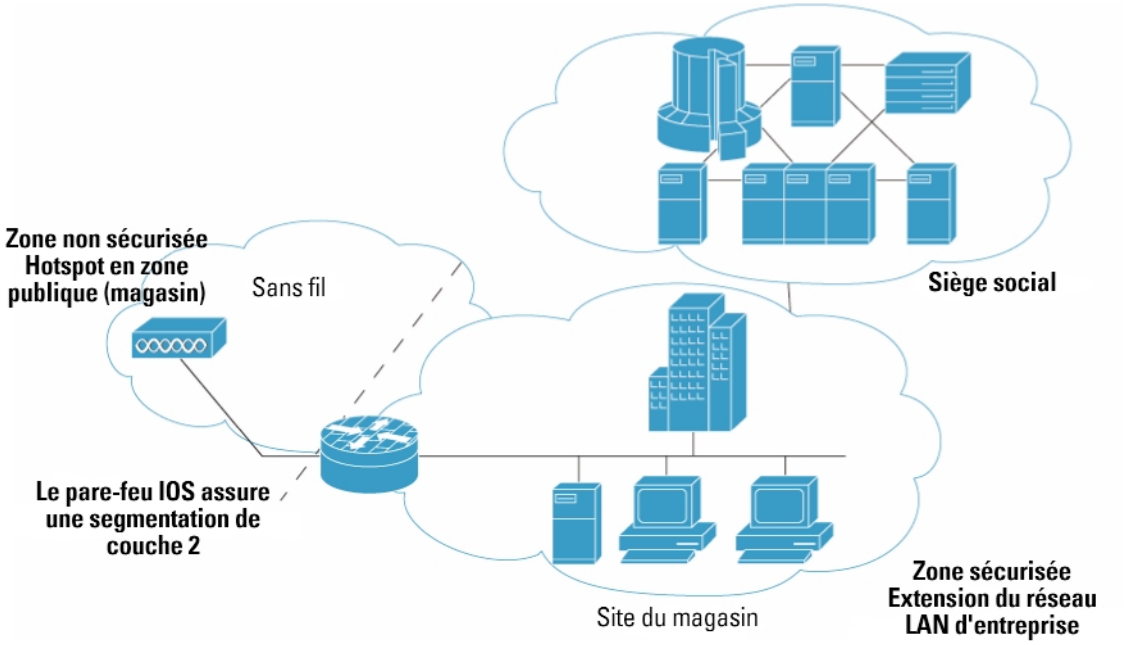
Pare-feu transparent

En plus du pare-feu à inspection d'état de couche 3, les routeurs des gammes Cisco 1800, 2800 et 3800 supportent le pare-feu transparent, autrement dit la possibilité d'appliquer des fonctionnalités de pare-feu de couche 3 à une connectivité de couche 2. Les avantages d'un pare-feu transparent sont, notamment :

- la possibilité d'ajouter facilement un pare-feu sur des réseaux existants sans avoir à modifier le plan d'adressage IP
- le support des interfaces VLAN ;
- le support du protocole Spanning Tree – pour gérer correctement les paquets BPDU (Bridge Protocol Data Unit) conformément à la norme 802.1d, et ne pas se contenter de les laisser passer ou de les rejeter ;
- le support d'une solution mixte de pare-feu de couches 2 et 3 sur un même routeur ;
- les interfaces qui n'ont pas besoin d'adresse IP ;
- le support de tous les outils de gestion standard ;
- le support du transit DHCP (Dynamic Host Configuration Protocol) qui permet d'affecter des adresses DHCP sur des interfaces opposées (trafic bidirectionnel).

La Figure 2 présente une application du pare-feu transparent.

Figure 2. Segmentation des déploiements de réseau existants en zones sécurisées sans changements d'adresses. Le pare-feu Cisco IOS autorise la segmentation transparente de la couche 2



Système de prévention d'intrusions (IPS)

Avec les premiers routeurs à offrir la fonctionnalité IPS, Cisco se place résolument en tête de l'industrie. Cisco IOS IPS est une solution en ligne d'inspection en profondeur des trafics applicatifs qui permet à la plate-forme logicielle Cisco IOS de limiter de manière efficace la circulation d'attaques virales à travers le réseau. Utilisé pour la prévention des intrusions et la notification des événements, le système Cisco IOS IPS exploite au maximum la technologie des familles de sondes Cisco IDS, notamment les serveurs dédiés Cisco IDS 4200, le module de services Catalyst 6500 IDS et les serveurs matériels dédiés IDS en module réseau. Cisco IOS IPS est un logiciel en ligne : il peut ainsi rejeter le trafic, envoyer une alarme ou réinitialiser la connexion, ce qui permet au routeur de répondre immédiatement aux menaces de sécurité et de protéger le réseau.

Bien que le concentrateur VPN soit généralement le lieu d'installation d'un pare-feu et d'inspection du trafic malveillant, ce n'est pas le seul emplacement à envisager pour le déploiement d'une solution de sécurité efficace – les attaques pouvant également provenir des sites distants. Grâce à sa collaboration avec les VPN IPSec, GRE et le pare-feu Cisco IOS, Cisco IOS IPS permet le décryptage, le raccordement des tunnels, la protection par pare-feu et l'inspection du trafic au premier point d'entrée du réseau, au niveau du site distant ou du concentrateur – une première dans l'industrie. Cisco IOS IPS arrête le trafic malveillant aussi près que possible de sa source.

Avec la commercialisation des routeurs Cisco 1800, 2800 et 3800, plusieurs nouvelles fonctionnalités sont désormais disponibles :

- la possibilité de charger et d'activer les signatures IDS sélectionnées de la même manière que les sondes de détection d'intrusion spécialisées Cisco IDS Sensor ;
- l'augmentation du nombre de signatures supportées (plus de 700 signatures supportées par les plates-formes Cisco IDS Sensor) ;
- la capacité pour l'utilisateur de modifier une signature existante ou de créer une nouvelle signature pour répondre aux menaces nouvellement découvertes (chaque signature peut être paramétrée pour l'envoi d'une alarme, le rejet du paquet ou la réinitialisation de la connexion) ;

Une autre fonctionnalité permet à l'utilisateur qui souhaite une protection maximale contre les intrusions de sélectionner un fichier de signatures facile à utiliser et contenant les signatures des vers et des attaques «les plus probables». Le trafic correspondant à ces signatures est alors systématiquement rejeté. Cisco SDM réalise une interface utilisateur intuitive pour la fourniture de ces signatures, notamment grâce à sa capacité à télécharger, sans qu'il soit nécessaire de modifier l'image logicielle, de nouvelles signatures à partir de Cisco.com et de configurer le routeur en conséquence.

Filtrage des URL (off-box/on-box en option)

Cisco fournit un filtrage des URL qui supporte le pare-feu Cisco IOS. Ceci permet à un utilisateur d'exploiter les produits de filtrage des URL Websense ou N2H2 avec les routeurs de sécurité Cisco. La fonction Websense de filtrage des URL permet au pare-feu Cisco IOS d'interagir avec les logiciels Websense ou N2H2, et donc d'empêcher les utilisateurs d'accéder à certains sites Web désignés en fonction de la politique de sécurité. Le pare-feu Cisco IOS travaille avec le serveur Websense et N2H2 pour déterminer si une URL donnée doit être autorisée ou interdite (bloquée). Sur les routeurs Cisco 2800, le module réseau de diffusion de contenu dispose également de fonctionnalités de filtrage des URL pour un filtrage complet on-box des URL et la protection des contenus.

Modules réseau de sécurité évoluée (en option sur Cisco 2800 et 3800)

Pour les utilisateurs qui recherchent une solution matérielle dédiée pour la détection des intrusions et la protection des contenus, deux modules réseaux sont disponibles pour les routeurs 2800 et 3800.

Module réseau de détection des intrusions

Lorsque le module réseau de détection des intrusions Cisco (référence NM-CIDS) est installé sur les routeurs Cisco 2800 ou 3800, il fournit un système de détection des intrusions complet qui appartient à la famille des sondes Cisco IDS Sensor. Ces sondes IDS travaillent de concert avec les autres composants IDS, notamment Cisco IDS Management Console, CiscoWorks VMS (VPN/Security Management Solution) et Cisco IDS Device Manager, afin d'assurer une protection efficace de vos données et de votre infrastructure d'informations. Le module réseau Cisco IDS possède son propre processeur dédié pour la détection des intrusions ainsi qu'un disque dur de 20 Go pour la journalisation, et supporte plus de 1000 signatures IPS. Grâce à sa collaboration avec les trafics VPN IPSec, GRE et le pare-feu Cisco IOS, ce module permet le décryptage, le raccordement des tunnels, la protection par pare-feu et l'inspection du trafic au premier point d'entrée du réseau – une première dans cette industrie. L'utilisateur peut ainsi faire l'économie des unités supplémentaires qui, avec d'autres solutions, sont généralement indispensables au système, ce qui réduit les frais d'exploitation et d'investissements tout en améliorant la sécurité.

Module réseau de protection des contenus

Le module réseau Cisco Content Engine (référence NM-CE) installé sur les routeurs Cisco 2800 et 3800 réalise un système de diffusion de contenus à routage intégré avec des fonctionnalités de protection des contenus. En plus de la mise en mémoire cache intelligente et du routage des contenus, le module Cisco Content Engine permet également le filtrage des URL. Chaque module réseau de diffusion de contenus est livré avec une copie du logiciel de filtrage des URL SecureComputing.

PROTECTION ET CONTRÔLE DES POINTS D'EXTRÉMITÉ : CONTRÔLE NAC, AUTHENTIFICATION, AUTORISATION ET ADMINISTRATION (AAA,) 802.1X ET AUTHENTIFIANTS RÉVOCABLES

Contrôle NAC (Network Admissions Control)

Le contrôle NAC (Network Admission Control) est le fruit d'une collaboration menée par Cisco Systems avec l'ensemble de l'industrie pour garantir que chaque point d'extrémité respecte les politiques de sécurité avant de pouvoir obtenir un accès au réseau, et de réduire ainsi les dégâts que peuvent occasionner les virus et les vers. NAC contrôle l'accès au réseau en interrogeant les postes de travail au moment de leur connexion au réseau pour vérifier qu'ils sont en conformité avec la politique de sécurité de l'entreprise.

NAC permet aux réseaux de repérer les systèmes vulnérables et d'appliquer des contrôles efficaces d'admission au réseau en ne permettant qu'aux unités d'extrémité sécurisées – celles qui disposent des mises à jour antivirus et des correctifs de système d'exploitation les plus récents prévus dans la politique de sécurité – d'accéder au réseau. Les hôtes vulnérables ou non conformes sont isolés et ne disposent que d'un accès restreint jusqu'à ce qu'ils exécutent le bon correctif ou qu'ils soient correctement protégés : le contrôle NAC évite ainsi qu'ils deviennent la cible ou la source d'infections par virus ou par vers.

Le contrôle NAC peut être activé sur les routeurs des gammes Cisco 1800, 2800 et 3800 disposant des packages logiciels IOS Advanced Security, Advanced IP Services ou Advanced Enterprise Services.

Le contrôle NAC présente les avantages suivants :

- grand nombre de contrôles – les méthodes d'accès les plus courantes utilisées par les hôtes pour se connecter au réseau sont reconnues : liaisons de réseau WAN par routeur, accès IPSec à distance et accès commuté ;
- solution multi-constructeurs – NAC est le fruit d'une collaboration pilotée par Cisco avec les plus grands fournisseurs de logiciels antivirus, notamment : Network Associates, Symantec et Trend Micro ;

- extension des technologies et des normes existantes – NAC élargit l'utilisation des protocoles de communication existants et des technologies de sécurité actuelles comme EAP (Extensible Authentication Protocol), 802.1x et les services RADIUS ;
- extension des investissements consentis dans les réseaux et la protection antivirus – NAC associe les investissements consentis dans l'infrastructure de réseau et dans la technologie antivirus pour fournir des solutions de contrôle des admissions.

Authentification, autorisation et administration (AAA)

Les services de sécurité de réseau AAA (Authentification, Autorisation, Administration) de la plate-forme logicielle Cisco IOS constituent le cadre principal de la définition du contrôle d'accès sur un routeur ou un serveur d'accès. AAA est conçu pour permettre aux administrateurs de configurer de manière dynamique le type d'authentification et d'autorisation qu'ils souhaitent en fonction de la ligne (par utilisateur) ou du service – IP, IPX ou VPDN – à l'aide de listes de méthodes applicables à des services ou des interfaces spécifiques.

802.1x

Les applications 802.1x rendent plus difficile l'accès non autorisé aux ressources d'information protégées en exigeant des authentifiants d'accès valides. En déployant des applications 802.1x, l'administrateur réseau peut également éliminer efficacement la capacité des utilisateurs à déployer des points d'accès sans fil non sécurisés – l'un des problèmes majeurs posés par la simplicité de déploiement des équipements de réseau WLAN.

Port USB / authentifiants révocables

Tous les routeurs des gammes Cisco 1800, 2800 et 3800 disposent de ports USB 1.1 intégrés. Ces ports seront bientôt configurables pour permettre de travailler avec un jeton USB qui permettra la diffusion sécurisée des configurations et le stockage hors plate-forme des authentifiants VPN. En utilisant le jeton USB pour les authentifiants de sécurité, l'administrateur réseau peut renforcer la protection de sa gestion en expédiant séparément le routeur et le jeton.

PROTECTION DES UNITÉS RÉSEAU (PLATE-FORME LOGICIELLE CISCO IOS, VERSIONS IP BASE ET SUPÉRIEURES) : SECURISATION DU PLAN DE CONTRÔLE, AUTOSECURE, NBAR, DÉFINITION DE SEUILS PROCESSEUR ET MÉMOIRE, SSHV2, SNMP ET ACCES PAR RÔLE À L'INTERFACE DE COMMANDE EN LIGNE

Securisation du plan de contrôle

Même la mise en œuvre logicielle et l'architecture matérielle les plus solides demeurent potentiellement vulnérables aux attaques par dépassement de capacité – actions malveillantes qui cherchent à paralyser l'infrastructure de réseau en l'inondant de trafic sans intérêt et maquillé en paquets de commande d'un type précis destiné au processeur du plan de contrôle des routeurs, autrement dit, du trafic de service destiné aux fonctions systèmes des routeurs. Pour bloquer ces menaces, et d'autres attaques analogues, qui visent directement le cœur du réseau, la plate-forme logicielle Cisco IOS intègre des fonctionnalités de définition de politiques programmables sur les routeurs qui limitent les débits – on pourrait parler de «police du trafic» – destinés au plan de contrôle. Cette fonctionnalité, appelée Control Plane Policing, peut être configurée afin d'identifier et de réduire certains types de trafic de services destinés aux routeurs soit totalement soit lorsqu'ils atteignent un seuil défini à l'avance.

AutoSecure

AutoSecure est une fonction de la plate-forme logicielle Cisco IOS qui simplifie la configuration de sécurité du routeur et réduit les risques d'erreurs de configuration. Le mode interactif, à l'usage des utilisateurs expérimentés, permet de personnaliser les paramètres de sécurité et les routeurs de services, offrant ainsi un meilleur contrôle sur les fonctions de sécurité du routeur. Pour les utilisateurs moins spécialisés qui ont besoin de sécuriser rapidement un routeur sans trop d'intervention humaine, AutoSecure dispose d'un mode non-interactif qui active automatiquement les fonctions de sécurité du routeur avec les paramètres par défaut définis par Cisco Systems. Une commande unique permet de configurer instantanément les paramètres de sécurité des routeurs et de désactiver les processus et les services non indispensables du système, éliminant par là même les menaces potentielles sur la sécurité du réseau.

NBAR

NBAR est un moteur de classification de la plate-forme logicielle Cisco IOS : il réalise une inspection d'état en profondeur des trafics qui lui permet de reconnaître un vaste éventail d'applications complexes, notamment les protocoles Web et d'autres protocoles difficiles à classer, qui utilisent les affectations dynamiques des ports TCP/UDP. Utilisé dans un contexte de sécurité, NBAR peut détecter les vers en fonction de leur signature. Lorsqu'une application est reconnue et catégorisée par NBAR, le réseau peut invoquer

des services spécifiques à cette application. NBAR permet également de garantir l'utilisation efficace de la bande passante du réseau en travaillant avec les fonctionnalités de qualité de service (QoS) pour fournir une bande passante garantie, la limitation de la bande passante, le formatage du trafic et la coloration des paquets. SDM 2.0 (voir Security Device Manager, ci-dessous) possède un assistant convivial qui permet l'activation de NBAR et fournit une vue graphique du trafic d'application.

Définition de seuils d'utilisation pour le processeur et la mémoire

La plate-forme logicielle Cisco IOS permet de définir des seuils globaux d'utilisation de la mémoire du routeur et de générer des notifications lorsque ce seuil est atteint. En préservant les ressources processeur et mémoire, cette fonction permet au routeur de rester opérationnel même lorsque la charge est importante – ce qui correspond parfois à une attaque.

Secure Shell Version 2

Secure Shell version 2 (SSHv2) offre de nouvelles et puissantes fonctionnalités d'authentification et de cryptage pour les accès en administrateurs dans les routeurs. De nouvelles options sont désormais disponibles et permettent la tunnellisation de types de trafic supplémentaires sur des connexions cryptées, notamment la copie de fichiers et les protocoles de courrier électronique. Avec ses fonctionnalités élargies d'authentification – notamment les certificats digitaux et des options d'authentification à plus de deux facteurs – SSHv2 renforce la sécurité de réseau.

Le protocole SNMPv3 (Simple Network Management Protocol version 3)

SNMPv3 (Simple Network Management Protocol Version 3) est un protocole normalisé et interopérable de gestion de réseau. SNMPv3 fournit un accès réseau sécurisé aux unités en associant des paquets d'authentification et de cryptage. Les fonctionnalités de sécurité de SNMPv3 sont, notamment :

• l'intégrité des messages – elle permet de s'assurer qu'un paquet n'a pas été altéré au cours de son transit ;

• l'authentification – elle vérifie que le message provient d'une source autorisée ;

• le cryptage – il brouille le contenu d'un paquet pour qu'il ne puisse pas être lu par un utilisateur non autorisé.

SNMPv3 fournit aussi bien des modèles de sécurité que des niveaux de sécurité. Un modèle de sécurité est une stratégie d'authentification définie pour un utilisateur et pour le groupe auquel il appartient. Un niveau de sécurité est un niveau d'autorisation attribué au sein d'un modèle de sécurité. L'association d'un modèle et d'un niveau de sécurité détermine le mécanisme de sécurité employé pour gérer un paquet SNMP. Les modèles de sécurité sont de trois types : SNMPv1, SNMPv2c et SNMPv3

Accès par rôle à l'interface de commande en ligne (CLI)

La fonction d'accès par rôle à l'interface de commande en ligne (Role-Based CLI Access) permet à l'administrateur réseau de définir des «vues», ensembles de commandes opérationnelles et de possibilités de configuration qui fournissent un accès sélectif ou partiel à la plate-forme logicielle Cisco IOS. Les vues limitent l'accès de l'utilisateur à l'interface de commande en ligne et aux informations de configuration de Cisco IOS ; elles peuvent définir les commandes acceptées et les informations de configuration visibles. Parmi ses nombreuses applications, Role-Based CLI Access donne à l'administrateur réseau la possibilité d'accorder au personnel chargé de la sécurité un accès à des fonctions particulières. De plus, un fournisseur de service peut, grâce à cette fonction, donner un accès limité à ses clients finaux afin de faciliter la résolution des problèmes du réseau. Cisco SDM est livré avec les vues par défaut Administrators, Read-Only (pour les utilisateurs finaux), Firewall Policy (politique de pare-feu) et EzVPN Remote. Les utilisateurs qui ouvrent une session sur Cisco SDM dans ce mode ne peuvent consulter que les écrans de l'interface graphique qui correspondent au rôle qui leur a été attribué.

GESTION DE SERVICES INTÉGRÉS : CISCO ROUTER AND SECURITY DEVICE MANAGER (SDM).

Cisco Router and Security Device Manager (SDM).

Cisco Router and Security Device Manager (SDM) est installé sur tous les routeurs des gammes Cisco 1800, 2800 et 3800. Cisco SDM est un gestionnaire d'unité intuitif à interface graphique qui permet le déploiement et la gestion des routeurs Cisco (voir la Figure 1). Cisco SDM facilite la configuration et la surveillance des routeurs grâce à son assistant de démarrage qui accélère le déploiement et l'installation initiale des routeurs, ses assistants intelligents qui facilitent l'activation des fonctions de sécurité et de routage, ses configurations routeurs validées par le Centre d'assistance technique Cisco TAC et des contenus d'aides contextuels.

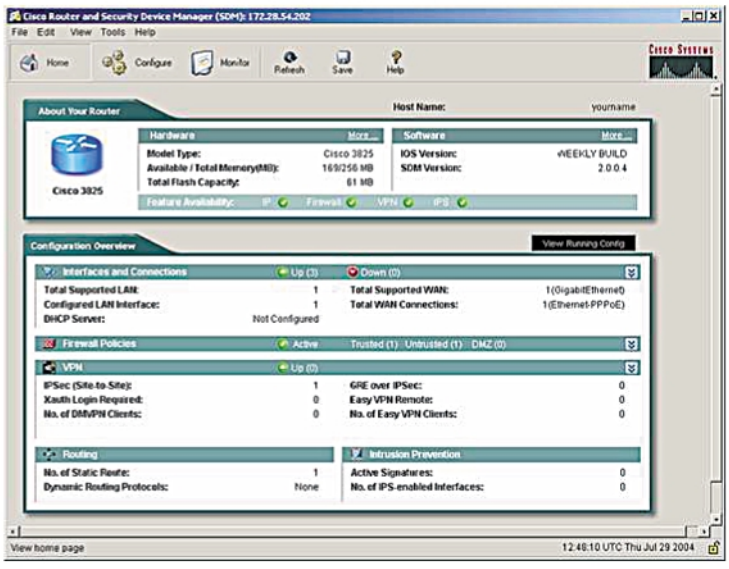
Avec ses assistants intelligents et ses fonctionnalités de dépannage en profondeur qui permettent la gestion en toute simplicité du routage et des services de sécurité, Cisco SDM 2.0 est un outil qui vous permet de profiter de tous les avantages de l'intégration de services sur le routeur. L'utilisateur peut désormais synchroniser les politiques de routage et de sécurité sur l'ensemble du réseau, disposer d'une vision plus complète de l'état des services du routeur services et réduire ses frais d'exploitation.

Parmi ses nouvelles fonctionnalités, Cisco SDM 2.0 supporte :

- le système IPS en ligne avec possibilité de mise à jour des signatures, personnalisation des mises à jour Dynamic Signature et personnalisation des signatures (voir IPS) ;
- l'accès par rôle au routeur ;
- le serveur Easy VPN et AAA ;
- les certificats digitaux pour les VPN IPSec ;
- le dépannage des connexions VPN et WAN ;
- la configuration des politiques de qualité de service (QoS) et la surveillance NBAR du trafic d'applications.

Pour en savoir plus sur Cisco SDM, visitez : http://www.cisco.com/go/sdm.

Figure 3. Cisco Security Device Manager



CiscoWorks VMS (VPN/Security Management Solution) est un ensemble logiciel pour la gestion des fonctionnalités de pare-feu et des VPN. Pour en savoir plus sur CiscoWorks VMS, visitez : http://www.cisco.com/go/vms

Le Tableau 1 énumère les principales fonctionnalités des gammes Cisco 1800, 2800 et 3800.

Tableau 1. Caractéristiques matérielles des routeurs des gammes Cisco 1800, 2800 et 3800

Caractéristiques	Cisco 3800	Cisco 2800	Cisco 1800
Accélération matérielle intégrée du cryptage VPN (IPSec DES, 3DES et AES 128, 192 et 256)	De série sur tous les modèles Son activation exige au minimum l'ensemble de fonctionnalités Advanced Sécurité de Cisco IOS	De série sur tous les modèles Son activation exige au minimum l'ensemble de fonctionnalités Advanced Sécurité de Cisco IOS	De série sur tous les modèles Son activation exige au minimum l'ensemble de fonctionnalités Advanced Sécurité de Cisco IOS
Accélération matérielle du cryptage VPN Compression matérielle avec IPPCP	Fonctionnalité en option qui améliore les performances et l'évolutivité des tunnels Référence : Cisco 3825 : AIM-VPN/EPII-PLUS Cisco 3845 : AIM-VPN/HPII-PLUS	Fonctionnalité en option qui améliore les performances et l'évolutivité des tunnels (Référence : AIM-VPN/EPII-PLUS)	Fonctionnalité en option qui améliore les performances et l'évolutivité des tunnels (Référence : AIM-VPN/BPII-PLUS)
Module réseau IDS*	Fonctionnalité en option (Référence : NM-CIDS)	Fonctionnalité en option (Référence : NM-CIDS*)	N/D
Module réseau Content Engine pour la sécurité des contenus*	Fonctionnalité en option grâce au module réseau Cisco Content Engine (Référence : CE-NM)	Fonctionnalité en option grâce au module réseau Cisco Content Engine (Référence : CE-NM*)	N/D

*Option non disponible sur le routeur Cisco 2801.

Le Tableau 2 présente les caractéristiques et les avantages des gammes Cisco 1800, Cisco 2800 et Cisco 3800.

Tableau 2. Principales caractéristiques et avantages des gammes Cisco 1800, 2800 et 3800.

Caractéristiques	Avantages
Connectivité sécurisée	
Accélération intégrée du cryptage des VPN sur tous les routeurs services intégrés	Cette fonctionnalité supporte les modes de cryptage IPSec DES, 3DES et AES 128, 192 et 256 sans occuper un emplacement de module AIM.
Accélération de sécurité sur module AIM	Grâce au support d'un module AIM de sécurité dédié en option, les routeurs peuvent offrir des performances et une évolutivité supplémentaires ainsi que la compression IPPCP de couche 3.
Support des VPN à commutation MPLS (Multiprotocol Label Switching)	Fonctionnalité de périphérie de réseau client optimisée pour les sites distants et renforcée par un mécanisme qui élargit les réseaux VPN MPLS au-delà de la périphérie client avec un pare-feu sensible Multi-VRF et la sécurité IPSec
Contextes sécurisés Multi-VRF et MPLS	Supporte de nombreux contextes indépendants (adressage, routage et interfaces) sur le site distant afin de permettre la séparation entre les services, les filiales ou les clients. Tous les contextes peuvent partager une connexion montante unique vers le cœur du réseau (par exemple, des VPN IPSec ou Frame Relay sur ATM), tout en restant isolés les uns des autres pour plus de sécurité.
Support de Cisco Easy VPN Remote et Server	Cette fonction facilite l'administration et la gestion des VPN de point à point en poussant activement à partir d'une unique tête de réseau de nouvelles politiques de sécurité vers les sites distants.
V3PN	Pour la fourniture sur VPN de services intégrés voix, vidéo et données vers n'importe quel site.
DMVPN	Un moyen souple et évolutif d'établir des tunnels IPSec virtuels à maillage global de site à site. L'ajout de nouveaux routeurs de périphérie ne nécessite aucune configuration au niveau du concentrateur.

Caractéristiques	Avantages
Défense contre les menaces	
Pare-feu Cisco IOS	Solution de sécurité et de routage tout en un : idéal pour protéger le point d'entrée WAN de votre réseau. Supporte désormais IPv6.
Pare-feu transparent	Segmente les déploiements de réseau existants en zones sécurisées sans qu'il soit nécessaire de modifier les plans d'adressages IP ! Supporte les VLAN. Supporte simultanément le pare-feu transparent et le pare-feu de couche 3 !
Prévention des intrusions	Solution en ligne pour l'inspection en profondeur des trafics qui travaille avec la plate-forme logicielle Cisco IOS pour limiter efficacement la circulation des attaques virales au sein du réseau. IPS peut rejeter le trafic, envoyer une alarme ou réinitialiser la connexion, ce qui permet au routeur de répondre immédiatement aux menaces de sécurité et de protéger le réseau.
Filtrage des URL (off box)	Permet au pare-feu Cisco IOS d'interagir avec les logiciels Websense ou N2H2, et donc d'empêcher les utilisateurs d'accéder à certains sites Web désignés en fonction de la politique de sécurité.
Protection et contrôle des points d'extrémité	
Contrôle NAC (Network Admissions Control)	Limite la diffusion des virus et des vers sur le réseau en limitant l'accès aux seuls postes de travail sécurisés et en conformité avec les politiques d'accès et de sécurité définies.
AAA	Permet aux administrateurs de configurer de manière dynamique le type d'authentification et d'autorisation qu'ils souhaitent en fonction de la ligne (par utilisateur) ou du service – IP, IPX ou VPDN.
Support standard 802.1x sur la commutation intégrée	Les applications compatibles 802.1x exigent des authentifiants valides ce qui rend plus difficile l'accès non autorisé aux ressources d'informations protégées et le déploiement de points d'accès sans fil non sécurisés.
Authentifiants révocables	Les authentifiants VPN révocables (clés VPN) permettent d'obtenir à l'avance des certificats VPN et des configurations de routeur.
Ports USB 1.1 sur carte	Ces ports seront bientôt configurables pour permettre de travailler avec un jeton USB qui permettra la diffusion sécurisée des configurations et le stockage hors plate-forme des authentifiants VPN.
Protection des unités réseau	
Définition de politiques pour le plan de commandes	Réduit l'incidence des attaques par saturation en régulant le débit du trafic entrant sur le plan de commandes : elle permet de maintenir la disponibilité du réseau même en cas d'attaque.
AutoSecure	Simplifie la configuration de sécurité du routeur et réduit le risque des erreurs de configuration.
NBAR	Ce moteur de classification de la plate-forme logicielle Cisco IOS reconnaît un vaste éventail d'applications. Lorsqu'une application est reconnue, le réseau peut invoquer des services spécifiques pour cette application, lui apportant ainsi le niveau de contrôle dont elle a besoin.
Définition de seuils pour le processeur et la mémoire	En préservant les ressources processeur et mémoire, cette fonction permet au routeur de rester opérationnel même lorsque la charge est importante – ce qui correspond parfois à une attaque.
Accès par rôle à l'interface de commande en ligne (CLI)	Fournit un accès par vue aux commandes de la CLI pour permettre une séparation logique et sécurisée du routeur entre les responsables de l'infrastructure et, les responsables de la sécurité.
Gestion	
Gestion sécurisée avec Cisco Router and Security Device Manager (SDM).	Intuitif et facile à utiliser, cet outil de gestion d'équipements par le Web intégré à la plate-forme logicielle Cisco IOS permet d'accéder à distance aux routeurs d'accès à l'aide des protocoles HTTPS et SSH (Secure Shell)

Caractéristiques	Avantages
Gestion de sécurité pour l'entreprise	Deux outils permettent les déploiements sécurisés en entreprise : - CiscoWorks VMS est un outil de gestion complet pour les déploiements de VPN de grande taille ou de taille moyenne ; il permet de configurer aussi bien les tunnels IPSec que les règles de pare-feu. - Cisco IP Solution Center (ISC) 3.0 est un outil de gestion IPSec MPLS pour fournisseurs de services.

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 IOS VPN a obtenu les homologations FIPS 140-2, ICSA et Common Criteria EAL4+ tandis que la certification du pare-feu Cisco IOS est en cours. Cisco reconnaît que ces homologations sont des composantes critiques de sa stratégie de sécurité intégrée et s'engage à poursuivre sa politique d'obtention des certifications FIPS, ICSA et Common Criteria.

FIPS

Les gammes Cisco 1800, 2800 et 3800 ont été reconnues conformes au niveau 2 de sécurité de l'agrément FIPS 140-1. Le NIST a fait évoluer la norme FIPS 140-1 à FIPS 140-2. Cisco s'apprête à soumettre un grand nombre de ses routeurs à l'agrément FIPS 140-2 niveau 2.

ICSA

ICSA (International Computer Security Association) est un organisme commercial de certification de sécurité qui propose la certification 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 pare-feu.

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.

COMMANDE DE MATÉRIEL

Pour passer commande, visitez Cisco Ordering Home Page. Le Tableau 3 présente les informations de commande pour les routeurs des gammes Cisco 1800, Cisco 2800 et Cisco 3800.

Tableau 3. Informations de commande pour les routeurs des gammes Cisco 1800, Cisco 2800 et Cisco 3800.

Nom du produit	Référence
Package de sécurité Cisco 1841 avec Cisco IOS Advanced Security	CISCO1841-SEC/K9
Package de sécurité Cisco 2801 avec Cisco IOS Advanced Security	CISCO2801-SEC/K9
Package de sécurité Cisco 2811 avec Cisco IOS Advanced Security	CISCO2811-SEC/K9
Package de sécurité Cisco 2821 avec Cisco IOS Advanced Security	CISCO2821-SEC/K9
Package de sécurité Cisco 2851 avec Cisco IOS Advanced Security	CISCO2851-SEC/K9
Package de sécurité Cisco 3825 avec Cisco IOS Advanced Security	CISCO3825-SEC/K9
Package de sécurité Cisco 3845 avec Cisco IOS Advanced Security	CISCO3845-SEC/K9
Package de sécurité renforcée Cisco 1841 avec module AIM-VPN BPII-PLUS et Cisco IOS Advanced IP	CISCO1841-HSEC/K9
Package de sécurité renforcée Cisco 2801 avec module AIM-VPN EPII-PLUS et Cisco IOS Advanced IP	CISCO2801-HSEC/K9
Package de sécurité renforcée Cisco 2811 avec module AIM-VPN EPII-PLUS et Cisco IOS Advanced IP	CISCO2811-HSEC/K9

Nom du produit	Référence
Package de sécurité renforcée Cisco 2821 avec module AIM-VPN EPII-PLUS et Cisco IOS Advanced IP	CISCO2821-HSEC/K9
Package de sécurité renforcée Cisco 2851 avec module AIM-VPN EPII-PLUS et Cisco IOS Advanced IP	CISCO2851-HSEC/K9
Package de sécurité renforcée Cisco 3825 avec module AIM-VPN EPII-PLUS et Cisco IOS Advanced IP	CISCO3825-HSEC/K9
Package de sécurité renforcée Cisco 3845 avec module AIM-VPN HPII-PLUS et Cisco IOS Advanced IP	CISCO3845-HSEC/K9
Package de sécurité renforcée Cisco 2801 V3PN avec module AIM-VPN EPII-PLUS, PVDM2-8, Cisco IOS Advanced IP, 64 Mo de mémoire Flash, 256 Mo de mémoire DRAM	CISCO2801-V3PN/K9
Package de sécurité renforcée Cisco 2811 V3PN avec module AIM-VPN EPII-PLUS, PVDM2-16, Cisco IOS Advanced IP, FL-SRST-36, 64 Mo de mémoire Flash, 256 Mo de mémoire DRAM	CISCO2811-V3PN/K9
Package de sécurité renforcée Cisco 2821 V3PN avec module AIM-VPN EPII-PLUS, PVDM2-32, Cisco IOS Advanced IP, FL-SRST-48, 64 Mo de mémoire Flash, 256 Mo de mémoire DRAM	CISCO2821-V3PN/K9
Package de sécurité renforcée Cisco 2851 V3PN avec module AIM-VPN EPII-PLUS, PVDM2-48, Cisco IOS Advanced IP, FL-SRST-72, 64 Mo de mémoire Flash, 256 Mo de mémoire DRAM	CISCO2851-V3PN/K9
Package de sécurité renforcée Cisco 3825 V3PN avec module AIM-VPN HPII-PLUS, PVDM2-64, Cisco IOS Advanced IP, FL-SRST-168, 64 Mo de mémoire Flash, 256 Mo de mémoire DRAM	CISCO3825-V3PN/K9
Package de sécurité renforcée Cisco 3845 V3PN avec module AIM-VPN HPII-PLUS, PVDM2-64, Cisco IOS Advanced IP, FL-SRST-240, 64 Mo de mémoire Flash, 256 Mo de mémoire DRAM	CISCO3845-V3PN/K9
Module AIM de compression et de cryptage VPN DES, 3DES et AES à performances renforcées pour Cisco 1800	AIM-VPN/BPII-PLUS
Module AIM de compression et de cryptage VPN DES, 3DES et AES à performances renforcées pour Cisco 2800	AIM-VPN/EPII-PLUS
Module AIM de compression et de cryptage VPN DES, 3DES et AES à performances renforcées pour Cisco 3800	AIM-VPN/HPII-PLUS
Cisco 1841 avec Cisco IOS Advanced Security	c184x-advsecurityk9
Cisco 2801 avec Cisco IOS Advanced Security	S28AESK9
Cisco 2800 avec Cisco IOS Advanced Security	S28NAESK9
Cisco 3825 avec Cisco IOS Advanced Security	S382AESK9
Cisco 3845 avec Cisco IOS Advanced Security	S384AESK9
Module réseau IDS (Intrusion Detection System)	NM-CIDS-K9
Module réseau Content Engine 20 Go	NM-CE-BP-20G-K9
Module réseau Content Engine 40 Go	NM-CE-BP-40G-K9
Module réseau Content Engine 80 Go	NM-CE-BP-80G-K9

MAINTENANCE ET ASSISTANCE

Cisco propose à ses client une large gamme de programmes de services. Le succès de ces programmes de services innovants est offert grâce à une combinaison unique de spécialistes, de processus, d'outils et de partenaires qui maximisent la satisfaction de nos clients. Cisco Services vous aide à protéger votre investissement dans les réseaux, à optimiser leur exploitation et à le préparer aux nouvelles applications afin d'en étendre l'intelligence business de l'entreprise et d'accroître le succès de votre activité. Pour plus d'informations sur Cisco Services, consultez Cisco Technical Support Services ou Cisco Advanced Services.

POUR PLUS D'INFORMATIONS

Pour de plus amples informations sur les gammes Cisco 1800, 2800 et 3800, visitez le site http://www.cisco.com/go/routing ou contactez votre responsable de compte Cisco.

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

204064_ETMG_EC_08.04