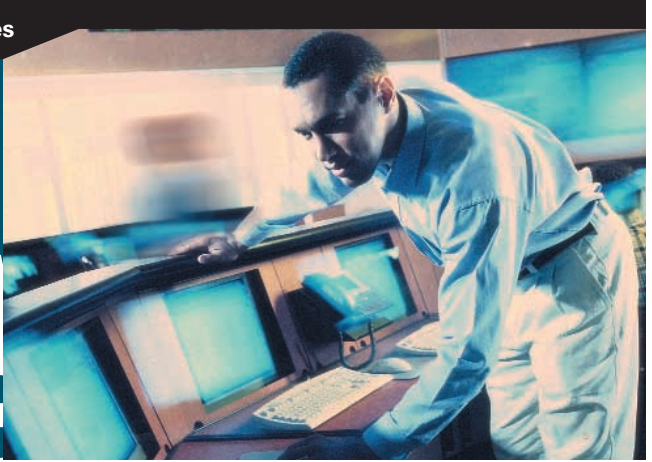




CONSTRUISONS LA GÉNÉRATION INTERNET™

Sécurisation des entreprises



# Guide des solutions **sécurité** et **VPN** CISCO SYSTEMS



# Sommaire

---

<b>Pourquoi Cisco ?</b> .....	1
<b>Section 1 - VPN</b>	
Réseaux privés virtuels (VPN) .....	.5
VPN site-à-site .....	.5
VPN Cisco à accès distant .....	.10
<b>Section 2 - FIREWALLS</b>	
Firewalls .....	.17
Cisco PIX Firewall .....	.17
Cisco IOS Firewall .....	.20
<b>Section 3 - DETECTION D'INTRUSION</b>	
Détection d'intrusion .....	.25
Système de détection d'intrusion sécurisé Cisco .....	.26
<b>Section 4 - RECHERCHE ACTIVE/PASSIVE DE VULNERABILITES</b>	
Recherche active/passive de vulnérabilité .....	.33
Cisco Secure Scanner .....	.33
<b>Section 5 - CONTROLE D'ACCES</b>	
Contrôle d'accès .....	.39
Serveur de contrôle d'accès Cisco Secure ACS .....	.39
<b>Section 6 - GESTION DE LA POLITIQUE DE SECURITE</b>	
Gestion de la politique de Sécurité .....	.45
Cisco Secure Policy Manager .....	.45
<b>Section 7 - PROGRAMME SECURITY ASSOCIATES</b>	
Produits complémentaires Cisco Security Associates .....	.51
<b>Section 8 - REPRESENTATION GRAPHIQUE DES SOLUTIONS</b>	
Solutions pour les grandes entreprises .....	.58
Solutions pour les entreprises de taille moyenne .....	.59
Solutions pour les petites entreprises .....	.60
Solutions pour les entreprises de la nouvelle économie .....	.61
Solutions pour les fournisseurs de services .....	.62
<b>Section 9 - GLOSSAIRE</b>	
Terminologie VPN et sécurité .....	.65



### Pourquoi faire appel à Cisco en matière de sécurité et de réseaux privés virtuels ?

Depuis son origine, Cisco Systems a pour objectif de permettre à ses clients de développer leur activité en s'appuyant sur des réseaux performants. Or un réseau non sécurisé n'offre pas toutes les garanties nécessaires à une entreprise pour le développement de son activité, pire il peut mettre en péril l'intégralité de l'entreprise. Assurer la sécurité des réseaux des entreprises, quelle que soit leur taille, est donc devenu un des objectifs majeurs de Cisco. Et qui mieux que le leader du marché des solutions réseaux peut garantir la sécurité, l'interopérabilité et la cohérence des réseaux ?

Fort de son expertise réseau, Cisco Systems a ainsi développé la gamme de solutions de sécurité et de réseaux privés virtuels (VPN) la plus complète du marché.

Reconnu comme le leader du marché de la sécurité, Cisco Systems propose aujourd'hui à ses clients et partenaires de bénéficier des avantages suivants :

- *Gamme de solutions* : Cisco propose un large éventail de produits VPN et de sécurité pour répondre à la diversité des problématiques clients : firewalls, systèmes de détection d'intrusion, concentrateurs VPN et routeurs et ce, quelle que soit leur taille et leur configuration.
- *Leadership et expertise du secteur* : selon le groupe d'experts IDC, les firewalls dédiés de la gamme Cisco PIX, occupent aujourd'hui la première place du marché mondial et, selon le cabinet Frost & Sullivan, il en est de même pour le système sécurisé de détection d'intrusion Cisco (IDS). De plus, les listes de contrôle d'accès Cisco (ACL) sont la technologie de sécurité la plus largement utilisée dans le monde, et le magazine Network Computing a élu le concentrateur Cisco VPN 3060 "Produit matériel de l'année".
- *Assistance technique 7 j/7 et 24 h/24* : les produits de sécurité et VPN Cisco bénéficient du même service d'assistance technique performant que les autres équipements Cisco, comprenant un support 24 h/24. Les services d'assistance et de maintenance Cisco incluent également les outils, l'expertise et les ressources nécessaires à l'installation, la maintenance et l'optimisation rapides des produits de sécurité et VPN Cisco de façon à protéger efficacement le réseau d'entreprise.

## Pourquoi Cisco ?

---

- *Interopérabilité garantie* : Cisco vous garantit la compatibilité de tous ses produits VPN et de sécurité. De plus, la compatibilité des produits tiers avec les produits Cisco est désormais garantie par le test officiel et indépendant du programme Security Associates, et ne repose pas sur des slogans publicitaires ambigus.
- *Formation et certification* : au-delà de son expertise technologique, Cisco Systems a développé un programme complet de certification permettant à ses partenaires de bénéficier de son expérience et de devenir de véritables spécialistes de la sécurité des réseaux
- *Sensibilisation des Entreprises* : La sécurité des réseaux informatiques est un domaine qui touche l'ensemble de l'entreprise, dirigeants comme employés. Qu'il s'agisse de sensibiliser les directeurs informatiques sur la nécessité de déployer une véritable politique de sécurité, ou les employés sur l'importance de protéger leurs outils de travail, Cisco Systems a développé une gamme d'outils de communication et de guides pour les informer sur l'ensemble des solutions à mettre en œuvre.



# Section 1

## VPN



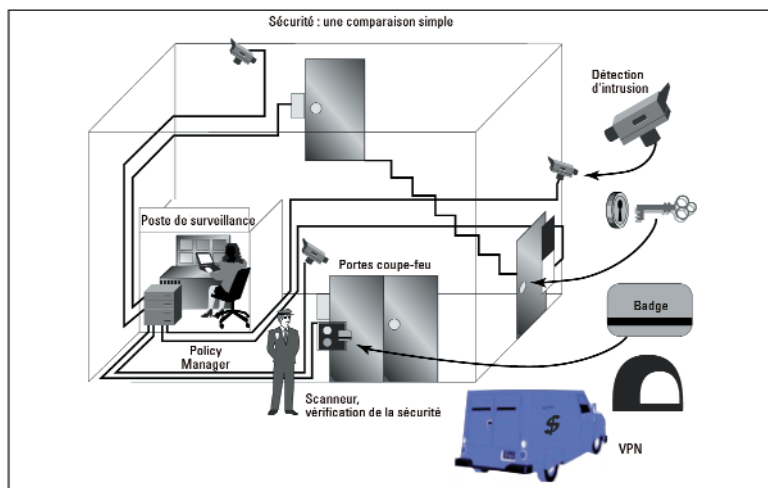
# Section 1

## **VPN**



## Réseaux privés virtuels (VPN)

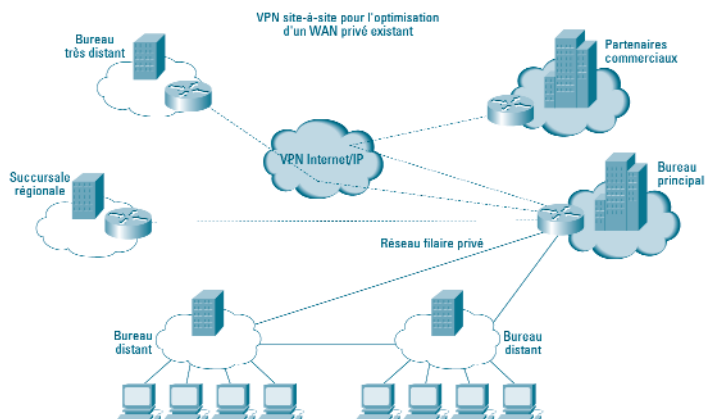
Afin d'assurer la sécurité des connexions entre sites distants tout en utilisant le réseau public pour limiter les coûts de communications, de plus en plus d'entreprises déploient des réseaux privés virtuels. Les VPN ont deux applications principales : la connectivité site-à-site et la connectivité accès distant. Dans le schéma ci-dessous illustrant un système de sécurité physique, les VPN sont comparés à des fourgons blindés, assurant la confidentialité et la sécurité du transfert entre deux ou plusieurs entités d'un réseau public.



## VPN site-à-site

Les VPN site-à-site sont un autre type d'infrastructure WAN (réseau étendu). Ils remplacent et améliorent les réseaux privés existants utilisant les lignes louées, les protocoles de relais de trame ou le mode ATM (mode de transfert asynchrone) pour connecter les sites distants et les succursales à la ou aux maisons mères. Les VPN site-à-site ne modifient pas en profondeur les exigences des réseaux étendus privés, telles que la prise en charge des divers protocoles, une grande fiabilité ou une évolutivité optimale. Au contraire, ils répondent à ces exigences tout en diminuant les coûts inhérents à ces infrastructures et en offrant une flexibilité accrue. Les VPN site-à-site peuvent utiliser les technologies de transport les plus répandues aujourd'hui, telles que le réseau public Internet ou les réseaux des fournisseurs d'accès, via la tunnellation et le cryptage afin d'assurer la confidentialité des données et la qualité de service (QoS) pour la fiabilité du transport.

## VPN site-à-site Cisco



### Produits

Les VPN site-à-site sont plus performants s'ils utilisent les routeurs optimisés VPN Cisco. Ces derniers garantissent l'évolutivité du système face aux progrès continus du cryptage matériel. De plus, les routeurs VPN de Cisco intègrent les fonctions de routage, de sécurité et de qualité de service inhérentes au logiciel IOS Cisco garantissant un déploiement VPN site-à-site sécurisé, évolutif et fiable. Cisco a créé une large gamme de routeurs VPN pour permettre de répondre aux différents besoins des configurations d'entreprises, qu'elles souhaitent connecter des sites de 10 personnes ou de plus de 200 personnes et ce, quelle que soit la technologie utilisée (ADSL...).

### Principaux avantages et fonctionnalités des solutions VPN Cisco

- Prise en charge de la tunnellation et du cryptage en utilisant les protocoles standard du marché, tels que IPsec (Internet Protocol Security) et 3DES (Digital Encryption Standard 3).
- Périmètre de sécurité absolue du réseau privé virtuel, avec fonction de filtrage de session et détection d'intrusion assurée par le logiciel Cisco IOS.
- Qualité de service sensible à l'application et gestion de la bande passante garantissant la fiabilité du transfert VPN.



Segment	Vitesse Mode d'accès VPN	Produit
Micro-entreprise	Jusqu'à 144 Kbits/sec RNIS, DSL	Cisco série 800
PME	Jusqu'au câble T1	Cisco série uBR900
	DSL avec interfaces Ethernet DSL avec modem intégré	Cisco série 1710 Cisco 806 Cisco 827 Cisco 1700- ADSL
Succursale	Jusqu'à T1/E	Cisco série 1700
	Jusqu'à T1/E1 double	Cisco série 2600
Filiale	n x T1/E1	Cisco série 3600 Cisco 7120
Maison mère	Jusqu'à OC-3	Cisco série 7100
		Cisco série 7200

- Routage intégral jusqu'à la couche 3, y compris les protocoles de routage externes, tels que BGP (Border Gateway Protocol) pour l'accès à Internet ou au réseau privé virtuel.
- Différents interfaçages avec le réseau local (LAN) ou étendu (WAN) pour l'accès à Internet ou au réseau privé virtuel et la connectivité du réseau local.

### La solution VPN de Cisco offre les avantages suivants :

- *Solution VPN globale avec intégration des périphériques* : les solutions VPN site-à-site de Cisco regroupent dans un équipement unique toutes les fonctions essentielles aux déploiements VPN sécurisés, évolutifs et fiables. Ainsi, les architectures de réseaux sont simplifiées et l'investissement total limité. La plupart des offres concurrentes disponibles sur le marché sont d'autant plus complexes qu'elles nécessitent l'utilisation de plusieurs équipements pour mettre en œuvre une solution VPN site-à-site globale.
- *Evolutivité des performances* : grâce à une gamme étendue de routeurs optimisés VPN, Cisco répond à tous les cas de figures en matière de déploiement VPN, quelle qu'en soit la taille, avec une ligne RNIS ou OC-3.

## VPN site-à-site Cisco

---

- *Compatibilité des fonctions* : les routeurs VPN de Cisco offrent une solution VPN site-à-site globale dans un équipement unique, et assurent une meilleure interopérabilité des fonctions VPN, telles que le firewall, la qualité de service, la tunnellation et le cryptage.
- *Auto-rétablissement du réseau* : les routeurs VPN de Cisco utilisent les capacités de résilience du réseau inhérentes au système d'exploitation inter-réseau (IOS) Cisco, telles que l'indication du maintien du tunnel, le TED (Tunnel Endpoint Discovery) et la découverte dynamique du routage via les tunnels GRE (encapsulation générique du protocole de routage), pour assurer une redondance du VPN et une récupération dynamique inégalées.
- *Optimisation de l'investissement matériel* : les solutions VPN site-à-site de Cisco offrent une interface LAN/WAN et une grande souplesse d'adaptation aux évolutions matérielles, ainsi que de nombreuses options d'entrée-sortie (E/S). Cette modularité vous aide à optimiser votre investissement matériel en vous permettant d'adapter les routeurs VPN de Cisco aux nouvelles technologies de réseaux.

### Questions-réponses

Q. Quelle est la différence entre les routeurs optimisés VPN et les autres routeurs Cisco ?

R. Les routeurs VPN optimisés de Cisco proposent une accélération matérielle du cryptage en option et sont compatibles IPsec, offrant ainsi l'évolutivité nécessaire aux applications VPN site-à-site.

Q. Les routeurs optimisés VPN de Cisco peuvent-ils être utilisés dans des VPN à accès distant ?

R. Oui, les routeurs optimisés VPN de Cisco peuvent assurer la connectivité des VPN à accès distant telle qu'elle est déclarée dans les environnements VPN hybrides accès distant/site-à-site. Toutefois, le concentrateur Cisco VPN série 3000 est spécialement conçu pour les VPN à accès distant ; il est donc parfaitement adapté aux environnements dont l'application principale repose sur la connectivité du VPN à accès distant (reportez-vous au chapitre "VPN Cisco à accès distant" ci-après).

Q. Les routeurs optimisés VPN de Cisco peuvent-ils être utilisés si un firewall est déjà installé sur le réseau ?

R. Oui, les routeurs optimisés VPN de Cisco peuvent être installés en amont, en aval ou au même niveau que le firewall existant.

Q. Quels sont les avantages des routeurs optimisés VPN de Cisco par rapport aux solutions VPN avec firewall ?

R. Certains firewalls peuvent assurer la tunnellation et le cryptage ; toutefois, ils ne sont pas équipés des fonctions indispensables au déploiement VPN site-à-site, telles que la prise en charge multi-protocoles, la qualité de service ou les fonctions de routage.



## Pourquoi mettre en œuvre ce produit ?

- Les VPN site-à-site permettent de mettre à niveau, à moindre coût, les architectures multi-points utilisant le réseau commuté limité en bande passante et généralement obsolètes, employées par la plupart des chaînes de magasins, les établissements financiers et les réseaux d'agences. La mise à niveau vers un VPN vous permet de distribuer un accès à Internet et des applications Web depuis leurs emplacements. Les VPN site-à-site étendent le WAN à moindre coût et en toute sécurité vers des entités non desservies, telles que des filiales internationales, des succursales et des partenaires commerciaux (extranet).
- Les solutions VPN site-à-site de Cisco, totalement intégrées et composées d'un équipement unique, peuvent être déployées et configurées en toute simplicité.

## Types de réseaux

Tous les types. La gamme étendue des routeurs optimisés VPN de Cisco permet de répondre à tous les types de déploiement, quel que soit le mode d'accès au réseau.

## Mise en œuvre

Ces routeurs peuvent être installés à la limite physique du réseau étendu (WAN) ou en aval, généralement au niveau de la couche d'accès à Internet.

## Équipements associés/nécessaires à la mise en œuvre

Pour suivre l'évolution de la technologie du cryptage, certains routeurs Cisco (Cisco séries 1700, 2600, 3600, 7100 et 7200) sont équipés de cartes supplémentaires d'accélération du cryptage. Chacune de ces plate-formes offre des interfaces LAN et WAN modulaires adaptables aux exigences de chaque site. Aucun équipement supplémentaire n'est nécessaire pour faire fonctionner le routeur. Dans le cas d'une gestion de plusieurs entités, il est conseillé d'utiliser Cisco Secure Policy Manager (CSPM).

Pour de plus amples informations sur les solutions VPN site-à-site de Cisco :

[www.cisco.com/go/evpn](http://www.cisco.com/go/evpn)

## VPN Cisco à accès distant

---

### VPN Cisco à accès distant

Aujourd'hui, les VPN sont la solution incontournable pour assurer les connexions accès distant à moindre coût. En effet, en permettant aux entreprises d'utiliser Internet via des fournisseurs d'accès pour favoriser l'échange d'informations entre des PC distants et le siège de l'entreprise par exemple, le déploiement d'une solution VPN évite des connexions téléphoniques point à point coûteuses. C'est la solution idéale pour offrir aux personnes en déplacement, aux travailleurs distants ou effectuant des heures supplémentaires de bénéficier d'une connectivité sécurisée et haut débit via le câble et les lignes DSL.

#### Concentrateur VPN Cisco série 3000

Le concentrateur Cisco VPN série 3000, solution VPN pour accès distant, intègre des fonctions avancées à haute disponibilité dans une architecture dédiée unique. Il permet ainsi aux entreprises d'implémenter des infrastructures VPN performantes, évolutives et fiables pour gérer leurs applications critiques depuis un accès distant.

Le concentrateur Cisco VPN série 3000 comprend un client VPN simple d'utilisation et conforme aux normes, ainsi que des plate-formes de terminaisons de tunnel évolutive et un système de gestion facilitant l'installation, la configuration et la surveillance de vos VPN à accès distant. Inédit sur le marché, ce concentrateur est la seule plate-forme évolutive offrant des composants extractibles et pouvant facilement être mis à niveau. Afin de prendre en charge tout type d'architecture, le concentrateur Cisco VPN série 3000 est décliné dans différentes versions, dont le Cisco VPN série 3060, élu "Produit matériel de l'année" par le magazine *Network Computing*.





## Principaux avantages et fonctionnalités

- *Déploiement et utilisation simplifiés* : le concentrateur Cisco VPN série 3000 est conçu de manière à s'intégrer à l'infrastructure du réseau sans qu'aucune modification ne soit nécessaire. Il s'adapte également au protocole RADIUS (Remote Access Dial-In User Service) existant, aux serveurs de domaine NT et 2000 ou aux serveurs Security Dynamics ACE. Cette grande souplesse d'authentification propose une interface d'identification visuelle semblable à celle dont vous disposez en utilisant directement le réseau commuté. En outre, il n'est plus nécessaire de créer une seconde base de données d'authentification. Si l'architecture n'en prévoit pas, le concentrateur Cisco VPN série 3000 dispose d'un serveur d'authentification intégré, permettant d'identifier les utilisateurs. Le concentrateur Cisco VPN série 3000 est compatible avec Cisco VPN 3000 Client, Microsoft Windows 2000 L2TP/IPsec Client ou PPTP (protocole de tunnellation point-à-point), vous garantissant ainsi une flexibilité optimale.
- *Performances et évolutivité* : le concentrateur Cisco VPN série 3000 fournit le niveau de performances le plus élevé du marché. La plate-forme prend actuellement en charge un débit des données cryptées 3DES maximal de 100 Mbts/sec, et jusqu'à 10 000 tunnels simultanés. Pour augmenter le débit des données cryptées, vous pouvez ajouter au concentrateur Cisco VPN série 3000 des modules SEP (à traitement évolutif du cryptage) basés sur un ASIC dédié.
- *Sécurité* : le concentrateur Cisco VPN série 3000 prend totalement en charge un certain nombre de systèmes d'authentification, tels que RADIUS, l'identification de domaine Microsoft NT/2000, RSA SecurID et les certificats numériques. De plus, le concentrateur Cisco VPN série 3000 peut être géré en toute sécurité à l'aide de SSL (Secure Sockets Layer) ou via telnet sécurisé.
- *Haute disponibilité* : le concentrateur Cisco VPN série 3000 est une plate-forme stable avec un temps moyen entre les pannes (MTBF) supérieur à 200 000 heures (soit plus de 22 ans). L'équipement est muni de sous-systèmes redondants (ventilateurs, alimentations, modules SEP) et de fonctionnalités d'équilibrage de charges et VRRP (Virtual Router Redundancy Protocol) assurant un temps de fonctionnement optimal. Grâce aux fonctions de surveillance étendues du concentrateur Cisco VPN série 3000, les administrateurs réseau connaissent l'état du système en temps réel et reçoivent des avertissements sans délai.

## VPN Cisco à accès distant

- *Gestion sécurisée* : la gestion du concentrateur Cisco VPN série 3000 peut être assurée via un navigateur Web standard (Hypertext Transfer Protocol [HTTP] ou Secure HTTP [HTTPS]), via telnet, telnet sécurisé ou un port de console. La mise en place et la maintenance des politiques de sécurité sont simplifiées grâce à une configuration des niveaux d'accès par utilisateur et par groupe.

### VPN Cisco Client série 3000 (hardware ou software)

Le VPN Cisco Client série 3000 est simple à déployer et à mettre en œuvre. Il est utilisé pour garantir la sécurité au niveau des tunnels cryptés de bout-en-bout du concentrateur Cisco VPN série 3000. Le concentrateur Cisco VPN série 3000, idéalement conçu et offrant une implémentation compatible IPsec, est livré avec une licence pour un nombre illimité d'utilisateurs. Le client peut être préconfiguré pour les déploiements de masse et les premières ouvertures de sessions se font en toute simplicité. Les politiques d'accès au VPN sont élaborées, centralisées et appliquées au niveau du client lorsque la connexion est établie.

### Questions-réponses

Q. Quelles différences existe-t-il entre les cinq modèles du concentrateur Cisco VPN série 3000 disponibles ?

Concentrateur	Cisco 3005	Cisco 3015	Cisco 3030	Cisco 3060	Cisco 3080
Nb d'utilisateurs	100	100	1 500	5 000	10 000
Type de cryptage	Logiciel	Logiciel	Matériel	Matériel	Matériel
SEP pris en ch.	0	0	1	2	4
Débit crypté maximum	4 Mbits/sec	4 Mbits/sec	50 Mbits/sec	100 Mbits/sec	100 Mbits/sec
Mémoire (Mo)	32	64	128	256	256
Alimentation redondante	Non	En option	En option	En option	Standard



**Q. Comment les concentrateurs Cisco VPN série 3000 intègrent-ils le cryptage ? Les ressources du système sont-elles affectées ? Est-ce évolutif ?**

R. Les concentrateurs Cisco des séries 3005 et 3015 procèdent au cryptage au niveau logiciel. Les concentrateurs Cisco milieu et haut de gamme des séries 3030, 3060 et 3080 utilisent les modules SEP pour exploiter leurs fonctions de cryptage. L'utilisation d'un équipement dédié, de type SEP, les séries 3030, 3060 et 3080 peuvent prendre en charge un grand nombre de tunnels cryptés et s'adapter sans que les performances globales du système n'en soient affectées.

**Q. Quelles sont les caractéristiques de haute disponibilité ou de tolérance aux pannes des concentrateurs VPN Cisco ?**

R. Les concentrateurs Cisco VPN série 3000 prennent en charge les modules SEP, les alimentations et les ventilateurs redondants. De plus, ils intègrent le protocole VRRP pour assurer la redondance et le basculement multi-châssis, ainsi qu'un mécanisme d'équilibrage de charge entre concentrateurs.

**Q. Qu'est-ce que la tunnellation fractionnée ? Est-elle prise en charge par les concentrateurs VPN Cisco ?**

R. La tunnellation fractionnée garantit un accès sécurisé aux données de l'entreprise tout en offrant un accès direct à Internet via les ressources du FAI (allégeant ainsi l'accès à Internet du réseau interne à l'entreprise). L'administrateur active et contrôle la prise en charge de la tunnellation fractionnée via le concentrateur.

**Q. Le VPN Cisco Client série 3000 fonctionne-t-il lorsque des dispositifs équipés de NAT/PAT (Network/Port Address Translation) sont installés ?**

R. Oui. Une intervention de l'utilisateur est nécessaire pour faire fonctionner le NAT/PAT de manière transparente avec le concentrateur VPN Cisco série 3000. Un administrateur peut centraliser le contrôle lorsqu'un utilisateur doit employer IPsec ou NAT/PAT Transparent IPsec. Si le NAT/PAT Transparent IPsec est activé pour un utilisateur spécifique, une négociation est automatiquement enclenchée et la transmission des données via le NAT/PAT peut aboutir.

## **Pourquoi mettre en œuvre ce produit ?**

Grâce aux connexions Internet à accès distant de qualité professionnelle via le concentrateur VPN Cisco série 3000, vous réalisez des économies sans précédent, bénéficiez d'une flexibilité et d'une fiabilité inégalées pour un excellent niveau de performances. La mise en œuvre du concentrateur VPN Cisco série 3000 est une alternative rentable aux serveurs distants à numérotation directe. Il permet aux entreprises de réduire le nombre d'appels longue distance et d'oublier les problèmes liés à leur modem. Les personnes en déplacement, travaillant à distance ou effectuant des heures supplémentaires remplacent les appels longue distance par des appels locaux via des modems câble ou ADSL pour accéder à leur FAI.

## VPN Cisco à accès distant

---

### Types de réseaux

Tous les types. La gamme des concentrateurs VPN Cisco série 3000 prend en charge toutes les tailles d'entreprises et de réseaux.

### Mise en œuvre

Le concentrateur VPN Cisco série 3000 et le firewall sont généralement placés derrière le routeur d'accès à Internet. Le concentrateur peut être placé parallèlement, en amont ou en aval du firewall. L'option la plus simple dans un réseau existant est de brancher le concentrateur en parallèle du firewall ; aucune modification de configuration du firewall n'est alors requise et le concentrateur accède directement aux services internes du réseau (Dynamic Host Configuration Protocol [DHCP] ou RADIUS, par exemple). Vous pouvez renforcer la sécurité en verrouillant toutes les interfaces des périphériques réseau déclarés dans le chemin du VPN. Lorsque le concentrateur est installé en amont du firewall, ce dernier filtre le trafic entrant, mais l'accès aux services du réseau est plus compliqué. Si le concentrateur est protégé (derrière) le firewall, il convient d'installer un conduit à travers le firewall pour permettre au concentrateur d'accéder au trafic du VPN. Il est possible d'implémenter des variantes avec les interfaces DMZ placées en aval du firewall, mais les configurations décrites ci-dessus sont les plus répandues.

### Equipements associés/nécessaires à la mise en œuvre

Le concentrateur VPN Cisco série 3000 est un périphérique Ethernet-à-Ethernet pouvant être branché derrière tout routeur Internet. Toutefois, il n'est pas nécessaire d'installer une interface Ethernet d'authentification client sur le routeur. L'authentification client peut être gérée par des bases de données d'authentification utilisateur externes compatibles ou par une base de données interne (100 utilisateurs maximum).

Pour de plus amples informations sur les concentrateurs VPN et Client Cisco :

[www.cisco.com/go/evpn](http://www.cisco.com/go/evpn)

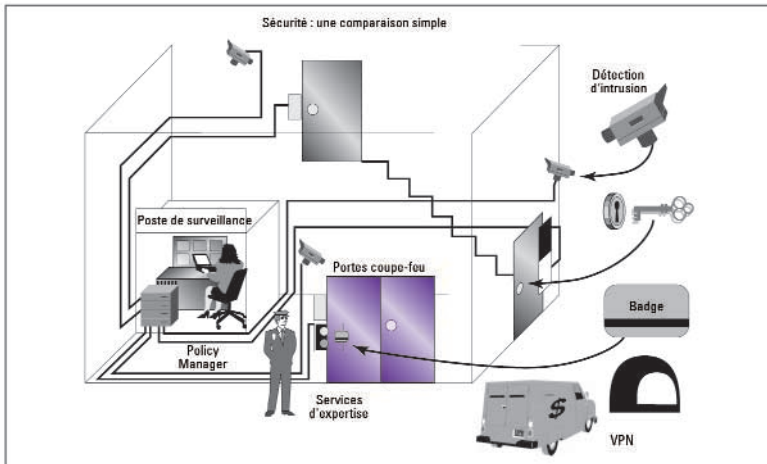
## Section 2 **FIREWALLS**



## Section 2 **FIREWALLS**

## Firewalls

Un firewall est une solution mise en place dans une architecture réseau afin de renforcer la politique de sécurité de l'entreprise et de restreindre l'accès aux ressources du réseau. Le schéma ci-dessous illustrant un système de sécurité physique compare le firewall à un verrou bloquant l'accès à un périmètre ou l'entrée d'un bâtiment. Seuls certains utilisateurs (détenant une clé ou un badge) sont autorisés à entrer.



## Cisco PIX Firewall

Cisco PIX Firewall, considéré comme le produit le plus performant, occupe la première place du marché. A ce titre, il est le produit phare de Cisco en matière de sécurité depuis 1996. Installé sur un réseau, le PIX détermine si le trafic est autorisé, dans un sens ou dans l'autre. Le cas échéant, il active la connexion ; celle-ci aura un impact quasiment nul sur les performances du réseau. Les données d'un trafic non autorisé sont détruites.



# Cisco PIX Firewall

## Produits de la gamme Cisco PIX Firewall

Modèle	Pix 501	Pix 506	Pix 515-UR	Pix 525-UR	Pix 535-UR
Marché	SOHO	PME	PME	Entreprise	Entreprise
Nb utilisateurs par license	10 ou 50	Illimité	Illimité	Illimité	Illimité
Nb max de tunnelsVPN	5	25	2000*	2000*	2000*
Taille (RU)	< 1	1	1	3	3
Processeur	133	200	200	600	1 GHz
RAM (MB)	16	32	64	256	1 GB
Max. Interfaces	1 10BaseT + switch 4 ports 10/100	2 10BaseT	6	8	10
Redondance	Non	Non	Oui	Oui	Oui
3DES (Mbps)	3	10	11	70*	95*

\*Utilisant une carte accélératrice VPN

## Principaux avantages et fonctionnalités

- **Sécurité** : Cisco PIX Firewall utilise un système d'exploitation sécurisé dédié à la protection du routeur et des réseaux. La plupart des autres firewalls non Cisco reposant sur de gros systèmes d'exploitation généralistes destinés à diverses fonctions, sont, par conséquent, plus vulnérables aux menaces provenant d'Internet.
- **Performances** : le PIX prend en charge plusieurs fois la capacité des routeurs concurrents et assure un niveau de sécurité sans égal, avec un impact minimum sur les performances du réseau.
- **Stabilité** : le PIX étant dédié à un objectif unique, la sécurité, il est particulièrement stable. La stabilité est un point essentiel pour un dispositif d'une telle importance dans l'architecture du réseau. Le temps moyen entre les défaillances d'un PIX est supérieur à six ans.
- **Évolutivité** : les plate-formes PIX sont disponibles dans de nombreux formats afin de s'adapter parfaitement aux divers contextes possibles, de la PME ou succursale au siège social. Toutes les plate-formes PIX sont équipées du même logiciel et utilisent les mêmes solutions de gestion, disposant ainsi d'une évolutivité et d'une intégration optimales.
- **Installation et maintenance simplifiées** : Cisco a créé Pix Device Manager, un utilitaire web intégré et sécurisé pour configurer simplement et graphiquement votre firewall.
- **VPN conforme aux normes** : la fonctionnalité VPN selon les normes IPsec compte parmi les fonctions de sécurité du PIX Firewall. Outre ses performances hors de commun, le PIX est doté des fonctions VPN site-à-site et à accès distant.



## Questions-réponses

**Q. Quel est l'impact du Cisco PIX Firewall sur les performances du réseau ?**

R. Aucun réseau n'étant identique à un autre, il est difficile de quantifier l'impact du firewall d'une manière globale et précise. Toutefois, les performances du réseau sont peu voire pas affectées. Le PIX ne ralentit pas le trafic et traite les paquets de données le plus rapidement possible. En conclusion, il affecte moins les performances du réseau que les autres dispositifs de firewall.

**Q. Le PIX est-il un serveur filtrant ou un serveur proxy ?**

R. Le PIX utilise une technologie de filtrage de session, ainsi que l'interaction avec les applications en cours, et offre les avantages des deux approches. En revanche, les utilisateurs du PIX ne subissent aucun des inconvénients des serveurs proxy, tels que des performances limitées et une configuration complexe. Cisco PIX Firewall est réputé pour assurer une sécurité inviolable et une fiabilité sans faille pour une base client conséquente.

## Pourquoi mettre en œuvre ce produit ?

- Les firewalls sont des dispositifs de sécurité classiques installés sur les réseaux. Si le réseau de l'entreprise se connecte à un réseau public comme Internet, celle-ci doit être équipée de firewalls.

Les performances du réseau étant cruciales pour le bon fonctionnement de l'entreprise, Cisco PIX Firewall saura parfaitement assurer la sécurité des données sans ralentir pour autant leur transfert grâce à son système de fonctionnement dédié et de codage sécurisé garantissant une sécurité et une disponibilité absolues.

## Types de réseaux

La gamme PIX étant disponible dans de nombreux formats, ce produit peut s'adapter à tous les types de réseaux.

## Mise en œuvre

Le PIX est mis en place au niveau des passerelles du réseau. Il est généralement installé sur le périmètre du réseau, entre le réseau et l'intranet d'une autre entreprise ou le réseau public Internet.

## Équipements associés/nécessaires à la mise en œuvre

Aucun équipement supplémentaire n'est nécessaire au bon fonctionnement de ce produit. Pour la gestion de plusieurs unités, reportez-vous à la section "Gestion de la sécurité".

Pour de plus amples informations sur Cisco PIX Firewall :

[www.cisco.com/go/pix](http://www.cisco.com/go/pix)

### Cisco IOS Firewall

Cisco IOS Firewall offre des fonctionnalités avancées de firewall et intègre diverses techniques de sécurité, telles que le cryptage IPsec DES pour VPN, la détection de l'intrusion et l'authentification. Ce module est un ajout au logiciel Cisco IOS. Il est disponible pour la plupart des routeurs et commutateurs Cisco. Il permet d'améliorer les fonctions de sécurité existantes du logiciel Cisco IOS en y intégrant des fonctions plus avancées et élabore un système de sécurité dynamique à partir de l'infrastructure Cisco de l'entreprise.

#### Principaux avantages et fonctionnalités

- *Sécurité intégrée au réseau* : en intégrant cette technologie au système d'exploitation du réseau, Cisco renforce la sécurité à la base du réseau. De ce fait, Cisco IOS Firewall innove sur le marché de la sécurité réseau et propose une intégration sans précédent.
- *Flexibilité* : Cisco IOS Firewall peut être déployé sur divers types de routeurs et commutateurs Cisco, ses fonctions de sécurité avancées pouvant être placées en différents points du réseau.
- *Utilisation de l'infrastructure existante* : Cisco IOS Firewall est conçu pour les équipements de mise en réseau Cisco et vous permet de convertir la plupart des routeurs ou commutateurs Cisco en une plate-forme de sécurité.
- *IDS intégré* : les solutions Cisco IOS et PIX Firewall comprennent un système de détection d'intrusion (IDS) garantissant une sécurité renforcée de l'infrastructure du réseau.

**Cisco IOS<sup>®</sup>**  
**TECHNOLOGIES**





### Questions-réponses

**Q. Quel est l'impact de Cisco IOS Firewall sur les performances du réseau ?**

R. Dans la plupart des cas, Cisco IOS Firewall a un faible impact sur le routeur. Pour minimiser encore cet impact, il est conseillé d'ajouter un processeur ou des modules de mémoire au routeur.

**Q. Cisco IOS Firewall propose-t-il autant de fonctions de sécurité que les versions matérielles dédiées ?**

R. Les dispositifs dédiés proposent sans doute des fonctions de sécurité plus complètes dans leur domaine d'application spécifique ; par contre, les solutions intégrées, telles que Cisco IOS Firewall, ont davantage de fonctions réseau. Un réseau équipé d'une passerelle VPN dédiée, d'un firewall dédié et d'un système IDS dédié, couplé à un routeur, offrent plus de fonctions et de meilleures performances à un prix bien supérieur à celui d'un routeur équipé de Cisco IOS Firewall.

Cisco IOS Firewall est une solution intégrée dotée de toutes les fonctionnalités d'un routeur Cisco, ainsi qu'une fonction supplémentaire de sécurité dans plusieurs domaines (cryptage, application d'un firewall et système IDS).

### Pourquoi mettre en œuvre ce produit ?

- Les firewalls sont des dispositifs de sécurité classiques installés sur les réseaux. Si la stabilité et la sécurité sont des critères essentiels au bon fonctionnement du réseau de l'entreprise, installez autant de firewalls que nécessaire.
- Cisco IOS Firewall étend la sécurité au-delà d'un périmètre physique autour du réseau et la garantit à moindre coût. Des points de contrôle de sécurité installés sur le réseau assurent une sécurité globale et optimale du réseau.
- Qu'il s'agisse de diriger le trafic via une petite, une moyenne ou une grande passerelle, un PIX allié à IOS Firewall vous fournissent les solutions firewalls idéales. PIX est un firewall dédié, extrêmement rapide et particulièrement fiable. IOS Firewall fonctionne avec le routeur en tout point du réseau, garantissant ainsi une solution flexible et peu onéreuse.
- Pour la plupart des réseaux, l'installation de systèmes de firewalls dédiés et intégrés en différents points du réseau permet d'assurer une sécurité optimale.

### Types de réseaux

Ce produit convient à tous les types de réseaux car il est proposé sur une gamme étendue de routeurs, des plate-formes Cisco série 800 aux Cisco série 7500, ainsi que sur certains commutateurs.

## Cisco IOS Firewall

---

### Mise en œuvre

Cisco IOS Firewall s'adapte sur quasiment tout routeur ou commutateur Cisco. Il est principalement utilisé dans les succursales des entreprises, les passerelles des PME, les réseaux internes, lors des déploiements des services et dans les architectures extranet pour lesquels prix et performances sont une priorité mais pour lesquels la globalité des fonctions n'est pas une nécessité.

### Equipements associés/nécessaires à la mise en œuvre

Les routeurs et commutateurs Cisco, qu'ils soient bas de gamme ou haut de gamme, prennent en charge cette solution. Pour obtenir des informations sur la gestion de plusieurs Cisco IOS Firewall, reportez-vous à la section "Gestion de la sécurité".

Pour de plus amples informations sur Cisco IOS Firewall :

[www.cisco.com/go/csis](http://www.cisco.com/go/csis)



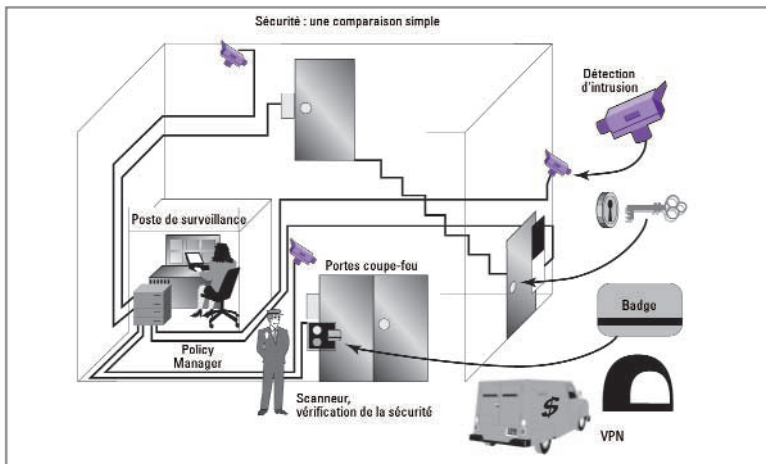
Section 3  
**DETECTION  
D'INTRUSION**



Section 3  
**DETECTION  
D'INTRUSION**

## Détection d'intrusion

La plupart des entreprises continue à mettre en place des firewalls comme moyen de protection principal afin d'empêcher les utilisateurs non autorisés d'accéder à leurs réseaux. Toutefois, la sécurité réseau s'apparente beaucoup à la sécurité "physique", dans la mesure où une seule technologie ne peut répondre à tous les besoins, mais qu'une défense à plusieurs niveaux donne les meilleurs résultats. Les entreprises se tournent de plus en plus vers des technologies de sécurité supplémentaires, pour se protéger des risques et vulnérabilités auxquels les firewalls ne peuvent faire face. Les solutions IDS (Intrusion Detection System) pour réseaux garantissent une surveillance du réseau permanente. Ces systèmes analysent le flux de paquets de données du réseau, à la recherche de toute activité non autorisée, telle que les attaques menées par les pirates informatiques (hackers), permettant de ce fait d'y remédier rapidement. Lorsqu'une activité non autorisée est détectée, un système IDS peut envoyer à une console de gestion des alertes accompagnées d'informations détaillées concernant l'activité suspecte. Un IDS peut également ordonner à d'autres équipements, tels que des routeurs, d'arrêter les sessions non autorisées. Dans l'exemple de sécurité physique illustré ci-dessous, les solutions IDS sont l'équivalent des caméras vidéo et des détecteurs de mouvement. Ces systèmes détectent les activités non autorisées ou suspectes et sont associés à des systèmes de réponse automatique, tels que les sentinelles, pour mettre un terme à l'activité incriminée.



### Système de détection d'intrusion sécurisé Cisco

Cisco Systems propose deux systèmes de détection d'intrusion complémentaires :

- les HIDS (Host Intrusion Detection Systems). Ces sondes host-based (powered by Entcept™) s'insèrent entre les applications et le cœur du système d'exploitation pour protéger des applications ou des serveurs critiques. Le host sensor Cisco permet de détecter des attaques connues (en utilisant une base de signatures), mais également protège d'attaques non encore connues en empêchant un appel malicieux (non autorisé) au système d'exploitation, offrant ainsi une prévention contre les attaques futures.
- les NIDS (Network Intrusion Detection Systems), nommées auparavant Cisco NetRanger®. Ces sondes réseau en temps réel peuvent être déployées dans de nombreux environnements réseau sensibles, des institutions financières majeures aux environnements militaires secret défense. La gamme Cisco Secure IDS est composée de sondes et d'une console de gestion centrale. Les sondes totalement indétectables de l'intérieur comme de l'extérieur de par la technologie -furtive-utilisée, détectent toute activité non autorisée sur le réseau, répondent à ces événements en mettant un terme à la session incriminée et envoient une alerte à la console de gestion centrale. La console de gestion IDS (Director) offre une présentation visuelle des alarmes et comprend un utilitaire de configuration distante du système ainsi qu'une fonctionnalité unique offerte aux réseaux équipés de routeurs d'accès Cisco : le "shunning" autrement appelé reconfiguration dynamique des listes de contrôle d'accès (ACL) des routeurs, directement par la sonde de détection d'intrusion lors d'événements nécessitant une telle action"

Cisco est le fabricant d'IDS leader du marché selon le cabinet d'analystes Frost & Sullivan.

#### Le kit sonde Cisco Secure IDS comprend les éléments suivants :

- Carte de détection d'intrusion pour Catalyst® 6000 IDS.
- Equipements réseau.
- Fonctionnalité IDS intégrée au firewall Cisco IOS et PIX Firewall.

#### Le kit de gestion Cisco Secure IDS comprend les éléments suivants :

- Cisco Secure Policy Manager.
- Director UNIX basé sur HP OpenView.
- Partenaires écosystème IDS.



### Principaux avantages et fonctionnalités

- *Gamme de sondes* : Cisco offre la plus vaste gamme de sondes du marché. Des applications réseau dédiées aux cartes de lignes IDS pour commutateurs Catalyst en passant par les fonctionnalités IDS intégrées au logiciel IOS de Cisco, l'ensemble de ces produits permet de répondre aux besoins de chaque entreprise.
- *Technologie intégrée* : Cisco est idéalement placé pour intégrer sa technologie IDS, leader du marché, aux équipements réseaux, tels que les routeurs et les commutateurs.
- *Technologie avancée* : en associant son savoir-faire reconnu en matière de réseau et de sondes, Cisco développe rapidement des produits à la pointe de la technologie en matière de détection d'intrusion.
- *Evolutivité importante* : Cisco Secure IDS est conçu pour pouvoir être déployé dans des environnements très différents, des PME aux grandes entreprises.
- *Visibilité réseau* : la technologie Cisco offre une très grande "visibilité" permettant d'observer le flux de données du réseau en temps réel et de détecter toute activité non autorisée.



## Système de détection d'intrusion sécurisé Cisco

---

### Questions-réponses

#### Q. A quoi sert IDS ?

R. IDS vient compléter d'autres équipements de sécurité, tels que les firewalls, en détectant et en empêchant toute activité non autorisée sur le réseau. Contrairement aux firewalls permettant d'autoriser ou de refuser le trafic de données en fonction des politiques définies, IDS inspecte le contenu du trafic "autorisé". Ceci permet d'identifier toute activité malveillante non détectée par le firewall, dont les débordements de pile (buffer overflow), les interruptions de service et d'autres types d'attaques similaires. Les solutions IDS permettent également à l'entreprise de faire face aux menaces internes pouvant compromettre la sécurité du réseau.

#### Q. Quelle est l'orientation principale de la technologie IDS ?

R. La majorité des produits de détection sont des dispositifs ou des logiciels fonctionnant sur des équipements réseau dédiés. Cisco a intégré cette technologie aux équipements fonctionnant sous Cisco IOS via le firewall Cisco IOS et le PIX et dans le matériel directement intégré aux commutateurs (carte de détection d'intrusion pour Catalyst 6000 IDS). Cette intégration permet à la technologie IDS d'être placée quasiment n'importe où sur le réseau, offrant une sécurité et une granularité accrues.

#### Q. Quelle différence existe-t-il entre la sonde Cisco Secure IDS et le composant IDS du firewall Cisco IOS/PIX ?

R. Les sondes Cisco Secure IDS sont plus performantes et peuvent traiter environ quatre fois plus de signatures que l'IDS des firewalls Cisco IOS ou PIX. Actuellement intégré aux routeurs, le firewall Cisco IOS dispose de fonctionnalités de traitement et d'une mémoire limitées. Pour cette raison, son action se concentre sur les signatures les plus courantes, dans un souci d'optimisation des performances. Les équipements Cisco Secure IDS combinés aux firewalls Cisco IOS / PIX et à la carte de détection d'intrusion pour Catalyst 6000 IDS permettent de couvrir une vaste gamme d'attaques. Les entreprises peuvent par exemple placer un équipement au niveau de leurs passerelles et liens hauts débits principaux et utiliser un firewall Cisco PIX ou IOS dans les bureaux et services internes distants. Les alarmes émises par n'importe quelle solution IDS Cisco peuvent être envoyées au même Director.



**Q. A quelle fréquence les signatures d'attaques doivent-elles être mises à jour ?**

R. Les signatures des sondes et des cartes de lignes Catalyst 6000 IDS sont mises à jour tous les deux mois environ, ou dans un délai plus court si des événements relatifs à la sécurité l'exigent.

**Q. Comment utiliser IDS dans un environnement commuté ?**

R. La carte de détection d'intrusion pour Catalyst 6000 IDS est dotée d'une sonde matérielle s'insérant facilement dans le châssis du Catalyst 6000/6500. La carte de détection d'intrusion pour IDS traite le trafic directement à partir du fond de panier du commutateur. Pour les autres modèles de commutateurs, les sondes peuvent être connectées à un analyseur de ports commutés (SPAN) ou à un port miroir.

**Q. Où les sondes doivent-elles être installées ?**

R. Les sondes sont généralement installées au niveau des connexions Internet, extranet, serveur d'accès distant et dans les centres vitaux de traitement de l'information des entreprises. Il est conseillé d'installer les sondes au niveau de tous les équipements réseau nécessitant une protection.

**Q. Les sondes affectent-elles les performances du réseau ?**

R. Les sondes Cisco Secure IDS et la carte de détection d'intrusion pour Catalyst 6000 IDS n'affectent pas du tout les performances du réseau. Elles fonctionnent de manière passive et traitent des copies de paquets, à la manière des "sniffeurs" réseau. Le firewall Cisco IOS affecte les performances du routeur car il utilise le processeur principal et la mémoire de celui-ci.

**Pourquoi mettre en œuvre ce produit ?**

- Ce produit permet d'observer le flux de paquets de données sur le réseau et de déterminer les menaces pouvant affecter le réseau.
- Il complète d'autres dispositifs de sécurité (les firewalls et les VPN par exemple) afin de garantir une architecture réseau sécurisée. Les firewalls travaillent principalement sur la couche réseau et transport de la pile OSI (Open System Interconnection). L'acceptation ou le rejet du trafic se base sur les informations relatives à l'adresse ou au port (application) utilisé par le trafic concerné. La charge utile est rarement inspectée par les firewalls, tandis que le Cisco Secure IDS inspecte le contenu du trafic à la recherche de signatures de débordements de pile (buffer overflow), d'interruptions de service et d'autres types d'attaques. Le Cisco Secure IDS combiné à des firewalls représente une solution solide, complémentaire et intégrée.

## Système de détection d'intrusion sécurisé Cisco

---

### Types de réseau

Les systèmes de détection d'intrusion représentent des composants de sécurité indispensables pour tous les environnements réseau sur lesquels transitent des informations sensibles ou vitales. Pour les entreprises, il est conseillé d'installer le Cisco Secure IDS pour la protection des équipements et des données informatiques. Ce produit est également approprié pour les fournisseurs d'accès proposant des services à valeur ajoutée de gestion de la sécurité. L'IDS intégré aux firewalls Cisco IOS et PIX est adapté aux petites entreprises ou aux succursales utilisant un équipement non rentable ou comme logiciel de test pour déterminer les zones du réseau où l'activité est importante, et où l'installation d'un équipement est justifiée.

### Mise en œuvre

- Sur les passerelles réseau se trouvant devant le firewall afin d'effectuer une analyse des attaques menées contre le réseau.
- Derrière le firewall pour examiner le trafic accepté par le firewall et le trafic sortant du réseau de l'entreprise.
- Sur les intersections réseau internes vitales, permettant ainsi aux sondes d'analyser une grande quantité de trafic réseau interne.
- Sur les connexions WAN/extranet pour examiner les activités de/vers les connexions des partenaires commerciaux.
- En amont des systèmes sensibles et vitaux, tels que les serveurs contenant des données financières ou de recherche/développement (le risque que ces systèmes soient hackés est réduit si des dispositifs de sécurité sont situés à proximité).

### Équipements associés/nécessaires à la mise en œuvre


Les sondes sont livrées prêtes à être installées. La carte de détection d'intrusion pour Catalyst 6000 est un module matériel autonome occupant un seul connecteur dans le châssis du commutateur. Le firewall Cisco IOS est une image logicielle d'IOS que vous pouvez commander pour de nombreux routeurs Cisco.

La console de gestion (Director) est une application logicielle disponible pour les environnements UNIX ou Microsoft Windows. Sous Windows NT ou 2000, le produit Cisco Secure Policy Manager permet la prise en charge de la gestion IDS. Le Director UNIX requiert le logiciel OpenView Network Node Manager de Hewlett Packard pour les stations de travail sous HP-UX ou Sun Solaris.

**Pour de plus amples informations sur le système de détection d'intrusion sécurisé Cisco :**

[www.cisco.com/go/ids](http://www.cisco.com/go/ids)

Section 4  
**RECHERCHE  
ACTIVE/PASSIVE  
DE VULNERABILITES**

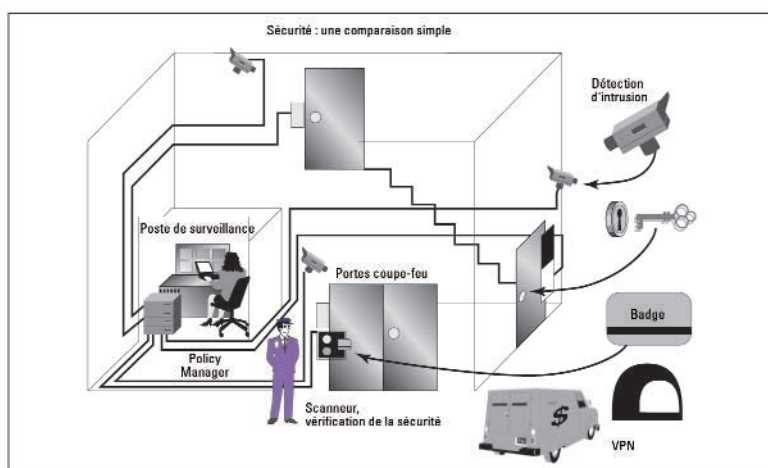


Section 4  
**RECHERCHE  
ACTIVE/PASSIVE  
DE VULNERABILITES**



### Recherche active/passive de vulnérabilités

Les scanners effectuent une analyse détaillée des systèmes mis en réseau, procèdent à un inventaire électronique des évaluations et détectent les faiblesses pouvant résulter d'une compromission de la politique de sécurité. Cette technique "proactive" consiste en une inspection préventive de l'état de la sécurité et vous permet de remédier aux éventuelles failles avant que des intrus ne s'y engouffrent. L'exploration se déroule comme une ronde périodique pour s'assurer que portes et fenêtres sont bien fermées. Cela vous permet d'évaluer les risques. Le schéma ci-dessous compare le scanning (ou exploration) à un vigile effectuant une vérification physique d'une installation.



### Cisco Secure Scanner

Cisco Secure Scanner, logiciel également connu sous le nom de Cisco NetSonar™, explore le réseau et compile les listes de tous les systèmes mis en réseau et compris dans une plage d'adresses spécifique, leurs systèmes d'exploitation et les services activés. Il compare ensuite ces informations à celles, nombreuses, d'une base de données répertoriant les faiblesses du réseau et détermine les systèmes dont la sécurité est défectueuse. Après avoir confirmé l'existence de ces faiblesses de manière opportune, Cisco Secure Scanner représente ces informations dans divers formats (tableaux, diagrammes et rapports au format texte ou recommandations détaillées) en vue d'une action corrective. La recherche active/passive de vulnérabilité permet aux utilisateurs de mesurer la sécurité, de gérer les risques et de remédier aux éventuelles faiblesses en matière de sécurité sur leurs réseaux.



### Principaux avantages et fonctionnalités

- *Simplicité d'utilisation* : Cisco Secure Scanner utilisant un format simple de type Windows et disposant d'une base de données étendue des règles et instructions en vue de mener une action corrective pour chaque défaillance détectée, il n'est pas nécessaire d'être un expert en sécurité pour obtenir des résultats optimum.
- *Reporting fiable* : Cisco Secure Scanner dispose de capacités de reporting approfondies et communique, dans divers formats, l'état de faiblesse du réseau et de chaque système spécifique.
- *Prix et licence* : pour un prix défiant toute concurrence, Cisco Secure Scanner effectue un audit minutieux du réseau sans qu'il soit nécessaire de mettre à jour la licence en cas d'extension ou de modification du réseau, ni de payer une licence pour une plage d'adresses IP spécifique.
- *Mises à jour régulières de la base de données répertorient les faiblesses* : grâce à un langage unique fondé sur des règles, la qualité de la recherche ne dépend pas de la mise à jour de la base de données répertorient les faiblesses, ni des notes de version. Les utilisateurs peuvent donc télécharger facilement et régulièrement les nouvelles règles et notes d'information à partir du site Web de Cisco.



## Recherche active/passive de vulnérabilités

### Questions-réponses

**Q. Il existe de nombreux modèles de scanners sur le marché. Quel est la supériorité de Cisco Secure Scanner ?**

R. Cisco Secure Scanner est proposé à un prix très attractif et accessible, quelle que soit la taille de l'entreprise. De plus, il propose une assistance technique en continu 7j/7 et 24h/24, des mises à jour fréquentes des signatures et un système de licence d'une grande souplesse. Ces caractéristiques s'ajoutent aux fonctions de reporting innovantes et aux fonctionnalités globales de découverte du réseau et d'exploration du niveau de sécurité. Cisco Secure Scanner est un produit sans équivalent sur le marché.

**Q. Comment le Cisco Secure Scanner s'intègre-t-il aux autres produits de sécurité Cisco ?**

R. Cisco présente ce scanner comme un soutien technologique. Il aide à mesurer l'enjeu de sécurité du réseau et recommande des actions correctives vous permettant d'améliorer constamment le réseau et de vous fier aux procédures d'anticipation que vous avez élaborées.

**Q. Quelle est la fréquence de mise à jour des signatures ?**

R. Les signatures sont mises à jour deux fois par mois. Toutes les mises à jour peuvent être téléchargées à partir du site Web de Cisco et installées très rapidement. De plus, elles ne nécessitent pas une réinstallation complète du produit, contrairement à d'autres scanners.

### Pourquoi mettre en œuvre ce produit ?

Peu d'entreprises ont une vision précise de leur niveau de sécurité ou disposent d'inventaires précis des systèmes qu'ils détiennent et maintiennent. Le scanner donne cet aperçu, vous offrant une vision globale de votre réseau et vous permettant d'identifier les faiblesses de sécurité pouvant aboutir à une compromission du réseau. En outre, il offre la possibilité de définir et de renforcer les politiques de sécurité en identifiant les systèmes mis en réseau et en validant la mise en œuvre de ces politiques.

### Types de réseaux

Tous les types de réseau peuvent intégrer le Cisco Secure Scanner. Le prix très attractif de ce produit (bien inférieur à celui des produits concurrents) a été défini de manière à permettre à tous les types d'entreprises d'acquérir le Cisco Secure Scanner. Ce module d'ajout s'adapte à la plupart des équipements de mise en réseau disponibles sur le marché. Ce produit est particulièrement adapté aux besoins des consultants car il n'est pas nécessaire d'étendre la licence pour explorer une plage d'adresses différente pour un nouveau client. Pour ce faire, une copie sous licence du scanner est suffisante.

## Cisco Secure Scanner

---

### Mise en œuvre

La mise en place de Cisco Secure Scanner en un point central du réseau interne garantit au système la visibilité maximale des systèmes mis en réseau, quel qu'en soit le nombre. De plus, le système doit être utilisé à partir d'un emplacement extérieur pour explorer le périmètre du réseau. S'il est installé sur un ordinateur portable occupant un emplacement interne ou externe du réseau, une seule licence Cisco Secure Scanner est nécessaire.

### Equipements associés/nécessaires à la mise en œuvre

Cisco Secure Scanner fonctionne avec les systèmes d'exploitation Microsoft Windows NT, 2000 et Sun Solaris.

Pour de plus amples informations sur Cisco Secure Scanner :

[www.cisco.com/go/scanner](http://www.cisco.com/go/scanner)



## Section 5

# **CONTROLE D'ACCES**

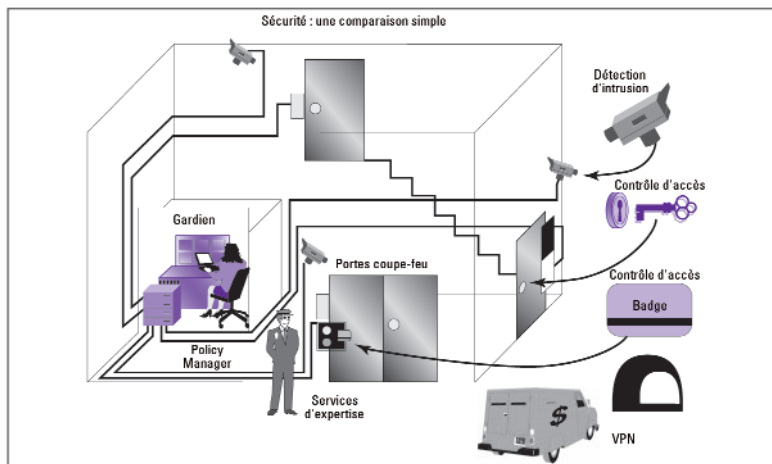


Section 5  
**CONTROLE D'ACCES**



### Contrôle d'accès

Les serveurs de contrôle d'accès déterminent les personnes autorisées à accéder à un réseau et les services qu'elles peuvent utiliser. Ils ont en mémoire un profil comprenant les informations d'authentification et d'autorisation relatives à chaque utilisateur. Les informations d'authentification valident l'identité des utilisateurs et les informations d'autorisation déterminent les éléments accessibles. Par analogie à un système de sécurité physique, les serveurs de contrôle d'accès sont équivalents aux badges d'accès, aux clés et aux gardiens responsables de la sécurité.



### Serveur de contrôle d'accès Cisco Secure ACS

Le serveur de contrôle d'accès Cisco Secure ACS (Access Control Server) pour Windows NT et 2000 est l'une des nombreuses solutions logicielles de sécurité proposées dans la suite Cisco. Il permet l'authentification, l'autorisation et la gestion du trafic et des utilisateurs ; ce service est aussi appelé AAA : (authentication, authorization, and accounting). Cisco Secure ACS pour Windows NT et 2000 facilite l'application de services AAA à tous les environnements d'accès, petits et grands. Ce service parfaitement intégré à Windows NT et 2000 facilite le déploiement et la mise en œuvre de différents services, tels que l'accès à distance des réseaux privés virtuels (VPN), le contrôle de l'accès selon l'heure et divers degrés possibles de communications sécurisées. Cisco Secure ACS convient à la mise en place initiale d'un système de sécurité et peut ultérieurement être mis à jour pour prendre en compte des environnements plus complexes et l'évolution des politiques de sécurité.

## Serveur de contrôle d'accès Cisco Secure ACS

---

Cisco Secure ACS s'appuie sur une architecture évolutive, ce qui lui permet de répondre aux besoins des environnements distribués tout en prenant en charge des milliers de ports utilisant simultanément les protocoles TACACS+ et RADIUS. La centralisation des services AAA complète le développement de n'importe quelle infrastructure d'accès.

### Principaux avantages et fonctionnalités

- *Facilité d'utilisation* : l'interface utilisateur HTML, de part son omniprésence, simplifie et répartit la configuration des profils d'utilisateurs, de groupes et la configuration ACS.
- *Intégration* : l'association avec le logiciel Cisco IOS facilite l'utilisation de fonctionnalités telles que le protocole MMP (Multichassis Multilink Point-to-Point) et l'utilisation des commandes de Cisco IOS.
- *Evolutivité* : Cisco Secure ACS est conçu de manière à prendre en charge de très grands réseaux intégrant des serveurs redondants et la sauvegarde des bases de données utilisateurs.
- *Gestion* : la prise en charge des bases de données Windows NT et 2000 utilise et consolide la gestion des noms utilisateurs et mots de passe de Windows NT/2000 et la prise en charge de l'application Performance Monitor de Windows NT/2000 afin de disposer de statistiques en temps réel.
- *Administration* : différents niveaux d'accès possibles selon l'administrateur Cisco Secure ACS et la possibilité de rassembler des entités de réseau facilitent la gestion de ces entités.
- *Flexibilité du produit* : le logiciel Cisco IOS prenant en charge des services AAA, Cisco Secure ACS peut être utilisé sur quasiment tous les serveurs d'accès réseau NAS (Network Access Server) vendus par Cisco (la version IOS doit prendre en charge le protocole RADIUS ou TACACS+).
- *Flexibilité des protocoles* : Cisco Secure ACS est compatible avec les deux protocoles TACACS+ et RADIUS, garantissant ainsi une flexibilité optimale. Un VPN d'accès à distance peut être pris en charge en amont et en aval des tunnels IPsec et PPTP.
- *Authentification* : Cisco Secure ACS peut être intégré à la plupart des systèmes d'authentification connus, tels que les solutions à mot de passe unique de RSA Security SecurID et CRYPTOCARD.



### Questions-réponses

#### Q. Pourquoi aurais-je besoin d'un Cisco Secure ACS ?

R. Cisco Secure ACS offre une structure de gestion des services AAA commune à l'utilisateur et aux entités chargées de protéger et de surveiller les accès utilisateurs et entités sur le réseau.

#### Q. Et qu'en est-il de Cisco Secure ACS pour UNIX ?

R. Cisco vend séparément un produit pour Cisco Secure ACS sous UNIX, élaboré à partir d'un code différent (présentant d'autres fonctionnalités, telles que les bases de données utilisateurs, une interface utilisateur graphique [GUI], etc.). Nous conseillons aux utilisateurs destinant Cisco Secure ACS à un environnement UNIX de considérer la solution Cisco Access Registrar. Ce produit offre une solution AAA hautes performances dotée d'une grande capacité d'extension et adaptée aux environnements UNIX.

### Pourquoi mettre en œuvre ce produit ?

- Pour les sociétés désireuses de maîtriser l'authentification et l'autorisation des utilisateurs et des entités, Cisco Secure ACS constitue un élément clé pouvant être utilisé simultanément avec des serveurs d'accès commuté, des routeurs et des firewalls.
- Grâce à la compatibilité du logiciel Cisco IOS avec les protocoles RADIUS et TACACS+, toutes les entités d'un réseau peuvent être paramétrées pour communiquer avec un ACS. Une société ou un fournisseur de services peut alors centraliser le contrôle des accès commutés.

### Types de réseaux

- Principalement aux réseaux d'entreprise ayant besoin de contrôler les accès utilisateurs et de vérifier les utilisateurs et les administrateurs du réseau.
- Cisco Secure ACS prend en charge différentes infrastructures Cisco (Cisco 1700, 2600, 3600, 7200 et 7500 par exemple), ainsi que PIX Firewall. Cisco Secure ACS permet d'authentifier les utilisateurs en vérifiant s'ils figurent sur les bases de données utilisateurs de Windows NT/2000, de Cisco Secure ACS, d'ODBC (Open Database Connectivity), de NDS (Novell Domain Server) ou sur une base de données de serveur de carte à jeton.

## Serveur de contrôle d'accès Cisco Secure ACS

---

### Mise en œuvre

- Aux points d'accès au réseau destinés aux utilisateurs distants ou en accès interne commuté.
- Sur les connexions WAN/extranet pour surveiller les activités sur le réseau et contrôler l'authentification et l'autorisation des connexions des partenaires commerciaux.
- En amont des systèmes sensibles et vitaux dont la configuration nécessite les contrôles d'autorisation TACACS+ (le protocole TACACS+ permet de contrôler, au niveau des commandes, l'autorisation d'apporter des modifications à la configuration des routeurs et de PIX Firewall).

### Equipements associés/nécessaires à la mise en œuvre

Votre serveur Windows NT doit présenter la configuration matérielle minimale suivante :

- Processeur Pentium, 350 MHz ou supérieur.
- Serveur Windows NT 4.0 ou windows 2000 Serveur, version US
- 128 Mo de mémoire RAM.
- 150 Mo d'espace disque disponible au minimum, et davantage si votre base de données est sur la même machine.
- Résolution minimale de 256 couleurs à 800 x 600 lignes.

Configuration logicielle minimale requise

Votre serveur Windows NT doit présenter la configuration logicielle minimale suivante :


- Le serveur NAS doit utiliser Cisco IOS version 11.2 ou supérieure, ou une application d'un constructeur tiers pouvant être configurée pour TACACS+ ou RADIUS.

Pour de plus amples informations sur le serveur de contrôle d'accès Cisco Secure ACS :

[www.cisco.com/go/acs](http://www.cisco.com/go/acs)



Section 6  
**GESTION DE  
LA POLITIQUE  
DE SECURITE**

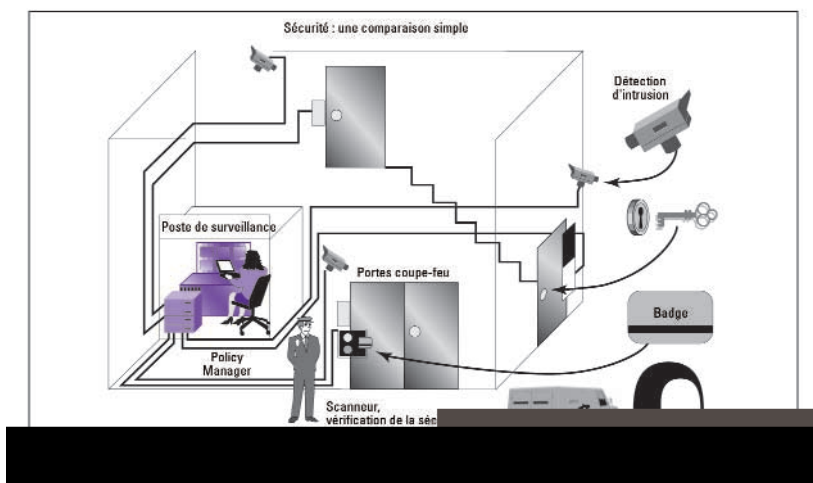


Section 6  
**GESTION DE  
LA POLITIQUE  
DE SECURITE**



### Gestion de la politique de sécurité

Un système de gestion de la sécurité permet de déployer simplement et uniformément sur un réseau une politique de sécurité ou des règles isolées. Ces politiques peuvent prendre en charge divers services de réseau, tels que la sécurité, la qualité de service et la voix. Les services de sécurité, plus particulièrement, peuvent inclure divers produits et technologies : les firewalls, les passerelles VPN, des sondes de détection d'intrusion, par exemple, ainsi que des dispositifs d'authentification et de cryptage. Le dispositif de sécurité d'un réseau est comparable à un système de sécurité physique, où le gestionnaire de la sécurité s'apparente à un poste centralisé de contrôle de la sécurité depuis laquelle le personnel qualifié peut activer et surveiller les alarmes et les ouvertures du bâtiment ou du campus.



### Cisco Secure Policy Manager

Le système Cisco Secure Policy Manager (CSPM) centralise la gestion des politiques de sécurité régissant la configuration des produits de sécurité Cisco, tels que Cisco Secure PIX Firewall et les routeurs Cisco utilisant Cisco IOS Firewall. Grâce au Policy Manager, le personnel de sécurité du réseau définit les politiques appropriées au réseau. Le CSPM peut alors convertir automatiquement ces politiques en fichiers de configuration pour les entités de sécurité concernées du réseau et distribuer sans danger ces configurations aux-dites entités.

## Cisco Secure Policy Manager

---

Les utilisateurs de CSPM n'ont pas besoin d'avoir une connaissance poussée des dispositifs et des lignes de commande utilisés par tous les dispositifs gérés. En conséquence, ce processus global de gestion de la sécurité épargne aux utilisateurs temps et efforts lors du déploiement sur leur réseau de firewalls et de services IPsec VPN.

### Principaux avantages et fonctionnalité

- *Gestion du firewall Cisco* : le CSPM permet de définir facilement des politiques de sécurité applicables au périmètre contrôlé pour les firewalls Cisco Secure PIX et les routeurs Cisco utilisant Cisco IOS Firewall.
- *Gestion de la passerelle VPN Cisco* : le CSPM permet de configurer facilement des réseaux VPN IPsec intranet/extranet pour les firewalls Cisco Secure PIX et les routeurs Cisco utilisant un système de cryptage.
- *Gestion de l'IDS Cisco* : le CSPM définit les règles de détection des entités d'IDS afin que toute activité non autorisée sur le réseau soit détectée et évitée. Ce logiciel joue également le rôle d'une console centrale avec l'affichage des alarmes générées par toutes les entités d'IDS Cisco.
- *Gestion des politiques de sécurité* : le CSPM utilise des politiques définies pour le réseau afin de gérer plusieurs centaines d'unités de sécurité Cisco sans nécessiter une connaissance approfondie de l'interface CLI (command-line interface) et sans en dépendre.
- *Gestion intelligente du réseau* : le CSPM convertit les politiques définies en commandes pour les unités concernées puis distribue en toute sécurité ces configurations sur l'ensemble du réseau, réduisant ainsi le besoin d'une gestion individuelle des unités.
- *Système de notification et de rapport* : le CSPM fournit les outils de vérification de base des unités de sécurité Cisco et des politiques définies, permettant des opérations de surveillance, d'alarme et de création de rapport et grâce auxquels l'administrateur est informé en permanence des événements survenant sur le réseau.
- *Facilité d'utilisation* : le CSPM s'intègre à l'environnement Windows NT et 2000 et utilise les règles de navigation intuitives bien connues de ce système d'exploitation, facilitant ainsi son utilisation et éliminant toute nécessité de formation préalable.



## Gestion de la politique de sécurité

### Questions-réponses

**Q. Qu'est-ce qu'une politique de sécurité, et de quelle manière le CSPM prend-il en charge cette fonctionnalité ?**

R. Une politique de sécurité est un ensemble de directives d'activité de haut niveau qui contrôle le déploiement de services sur un réseau. Généralement, les politiques de sécurité appliquées au réseau d'une entreprise sont définies à partir de pratiques établies au sein de cette entreprise. Ces politiques concernent le contrôle de différents services tels que la disponibilité, la performance et la sécurité du réseau. La création, la maintenance et la vérification de ces politiques sont essentielles à la bonne marche de l'entreprise et de son réseau.

**Q. De quelles unités le CSPM peut-il assurer la gestion au sein d'un réseau ?**

R. Le CSPM assure une gestion de la politique de sécurité pour les firewalls Cisco Secure PIX, ainsi que les routeurs Cisco utilisant le firewall Cisco IOS ou le logiciel Cisco Secure Integrated VPN. Le produit prend en charge tous les firewalls Cisco Secure PIX en version V4.2.x, 4.4.x, 5x, et 6.x ainsi que le logiciel Cisco IOS (versions 12.0.5T). En outre, le CSPM V2.3i prend en charge les sondes de détection d'intrusion Cisco, la carte de détection d'intrusion pour Catalyst 6000.

**Q. Combien d'unités de sécurité le Cisco Secure Policy Manager peut-il gérer ?**

R. Cisco Secure Policy Manager peut gérer efficacement plusieurs centaines d'unités de sécurité Cisco. Si le produit en lui-même n'est pas limité, des limites pratiques s'imposent, définies par la combinaison des éléments suivants :

- Nombre d'unités et topologie.
- Nombre d'interfaces par unité.
- Nombre et complexité des politiques appliquées au réseau.
- Puissance et résolution graphique du PC Windows NT/2000 hôte.

**Q. Le système Cisco Secure Policy Manager est-il un outil de gestion de réseau appliquant le protocole SNMP (Simple Network Management Protocol) comme HP OpenView ?**

R. Non. Cisco Secure Policy Manager n'assure pas la configuration et la surveillance des unités de réseau de la même manière que les plates-formes bien connues sur le marché qui gèrent les réseaux à l'aide du protocole SNMP. Le CSPM configure des services de sécurité du réseau tels que les firewalls, le NAT et les tunnels IPsec. Ce produit permet, en une seule fois, de définir et de mettre en place des politiques de sécurité sur l'ensemble du réseau plutôt que de répéter l'opération pour chaque unité. Bien qu'au final le produit convertisse ces politiques en configuration d'unité, l'objectif du produit est de gérer des services à l'échelle du réseau, et non de gérer individuellement des détails au niveau de chaque unité du réseau.

# Cisco Secure Policy Manager

---

## Pourquoi mettre en œuvre ce produit ?

Gérer de nombreuses unités de réseau différentes est susceptible de générer un conflit de configurations, entraînant un effet négatif sur l'intégrité du réseau et sur les opérations s'y déroulant. En outre, les configurations de masse nécessitent généralement un temps précieux et le résultat peut s'avérer décevant, tout particulièrement lorsque plusieurs types d'unités et diverses technologies entrent en jeu. Le CSPM centralise la configuration des services de sécurité d'un réseau en appliquant des règles définies. Cette technique épargne du temps en éliminant le besoin de gérer individuellement chaque unité. Elle nécessite moins d'efforts et de connaissances car sa méthode cohérente et uniforme de configuration de plusieurs types d'unités ne nécessite aucune compétence particulière en termes de ligne de commande.

## Types de réseau

L'utilisation de Cisco Secure Policy Manager peut s'avérer un atout précieux pour les entreprises, petites, moyennes ou grandes, qui déploient les produits de sécurité réseau Cisco, de même que pour les utilisateurs de firewalls Cisco Secure PIX, de sondes Cisco Secure IDS ou de routeurs utilisant le firewall Cisco IOS.

## Mise en œuvre

Le CSPM doit être placé à un point stratégique du réseau interne disposant d'un accès vers toutes les unités de sécurité devant être supervisées. Ce produit doit disposer d'une connexion IP avec toutes les unités supervisées.

## Equipements associés/nécessaire à la mise en œuvre

- PC avec serveur Windows NT 4.0 ou station de travail équipée du Service Pack 5 et Internet Explorer 5.
- Si le produit est installé en configuration distribuée, un PC Windows 95/98 ou Windows NT peut servir d'interface GUI.
- Unités de sécurité Cisco associées au logiciel approprié.

Pour de plus amples informations sur Cisco Secure Policy Manager :

[www.cisco.com/go/policymanager](http://www.cisco.com/go/policymanager)

Section 7  
**PROGRAMME  
SECURITY ASSOCIATES**



Section 7  
**PROGRAMME**  
**SECURITY ASSOCIATES**



### Produits complémentaires Cisco Security Associates

Nous avons développé le programme de marketing Security Associates dans le but d'assurer à nos clients le plein potentiel de sécurité des réseaux Cisco.

Cisco associe ses produits de sécurité de grande qualité aux solutions logicielles proposées par les grands noms du marché. Ces produits associés ont fait l'objet de tests par Cisco et ont été reconnus non seulement compatibles avec les produits Cisco Secure, mais également aptes à produire une valeur ajoutée spécifique aux réseaux Cisco. La combinaison des produits Cisco Secure et des produits de Security Associates vous permet de mettre en œuvre les stratégies de sécurité de défense en profondeur les plus complètes possibles, grâce auxquelles vous assurez à votre activité et à vos informations une protection optimale.

Explorons la manière dont les solutions de sécurité globale proposées par Cisco et les produits Security Associates vous permettent de sécuriser entièrement et efficacement un réseau professionnel.

Les catégories de solutions Cisco Security Associates traitent des principales préoccupations actuelles des entreprises utilisant un réseau :

- Authentification.
- Filtre sur le contenu/Recherche de virus.
- Outils de gestion/de rapport.
- Infrastructure de clé publique.
- Gestion à distance.
- Solutions VPN.

#### Authentification

Le système **CRYPTOCard CRYPTOAdmin** complète l'ACS CiscoSecure pour assurer des **services d'identification évolués** intégrant, par exemple, des mots de passe à usage unique afin d'améliorer la sécurité au niveau de l'authentification.

Les systèmes **RSA Security ACE/Server** et **RSA Security ACE/SecurID** sécurisent l'accès aux produits Cisco en relation avec l'ACS CiscoSecure, assurant ainsi des services centralisés **d'authentification à deux clés**.

**Secure Computing SafeWord** est associé avec l'ACS CiscoSecure pour sécuriser les transactions d'e-business à l'aide de services **d'authentification, d'autorisation et de vérification**.

## Programme Cisco Security Associates

---

### Filtre sur le contenu / recherche de virus

Les technologies de contenu MIMESweeper complètent les firewalls Cisco Secure par une fonction de **filtrage de contenu** des transmissions sur le réseau Internet et par un protocole SMTP (Simple Mail Transfer Protocol) afin de mieux protéger l'intégrité du réseau.

Le logiciel Finjan SurfinGate complète les firewalls Cisco Secure en assurant un **filtrage de code mobile** poussé prenant en charge Java, ActiveX, JScript, VBScript, les plug-ins et les cookies.

SurfCONTROL SuperScout complète les firewalls Cisco Secure à l'aide de **filtrage d'URL** extrêmement précis pour le trafic Internet afin de garantir une meilleure visibilité lors de l'utilisation du réseau.

Trend Micro InterScan VirusWall assure une **protection anti-virus** pour le trafic SMTP, HTTP et FTP (File Transfer Protocol) sur les réseaux protégés par les firewalls Cisco Secure.

Websense pour firewalls Cisco Secure PIX associé aux firewalls PIX permet un **filtrage d'URL** intégré et hautes performances du trafic **Internet des employés**.

ZoneAlarm Pro étend la sécurité du VPN jusqu'aux PC destinataires assurant ainsi la sécurité totale de l'accès distant. **ZoneAlarm Pro** propose des **firewalls, des solutions de protection d'intrusion et de gestion de la politique de sécurité** ainsi que des capacités d'exécution à tous les PC terminaux de l'entreprise étendue.

### Outils de gestion / de rapport

Intrusion.com CMDS Enterprise vous permet de recueillir, rassembler et gérer les données relatives aux événements de sécurité générées par les routeurs Cisco.

NetCom Systems netForensics est associé au système IDS Cisco Secure pour assurer une **analyse évoluée du journal et des alarmes**, améliorant ainsi la visibilité des attaques du réseau.

OpenSystems.com Private I est associé aux firewalls Cisco Secure pour garantir un **contrôle et une gestion** de qualité de l'activité au niveau des utilisateurs et du respect des règles de sécurité.



## Programme Security Associates

---

Le logiciel **Telemate.Net** est associé aux firewalls et à l'IDS Cisco Secure pour améliorer la création de **journaux et de rapports** concernant le respect des règles de sécurité et l'activité au niveau des utilisateurs.

**WebTrends pour firewalls et VPN** associés aux firewalls Cisco Secure améliorent la création de **journaux et de rapports** pour augmenter le niveau de sécurité et optimiser les ressources de réseau.

### Infrastructure de clé publique

**Baltimore Technologies UniCERT** est associé aux firewalls Cisco Secure et aux VPN clients pour fournir une **solution PKI** (Public Key Infrastructure, Infrastructure de clé publique) aux clients déployant des réseaux VPN Cisco.

**Entrust Technologies Entrust/PKI** sont associés aux firewalls Cisco Secure et aux VPN clients pour permettre le contrôle et la gestion de certificats numériques capables d'**authentifier les utilisateurs et les unités**.

**Microsoft Security Resource Kit pour Windows 2000** utilise le protocole SCEP (Simple Certificate Enrollment Protocol) pour **obtenir des certificats** et des informations de révocation sur les certificats de Microsoft Certificate Services pour toutes les solutions VPN Cisco.

**VeriSign OnSite** est associé aux firewalls Cisco Secure et aux VPN clients pour **authentifier les identités** en cas d'accès à distance, interne et externe sélectif.

### Gestion à distance

**F-Secure SSH** est associé aux routeurs Cisco pour sécuriser la **gestion du routeur à distance**, permettant ainsi aux administrateurs de se connecter en toute sécurité aux systèmes UNIX et aux routeurs Cisco sans crainte de compromettre le trafic du terminal par des écoutes électroniques.

### Solutions VPN

**F-Secure VPN+** et les routeurs Cisco peuvent être utilisés ensemble pour fournir un **accès à distance sécurisé** aux réseaux d'entreprise et des **extranets sécurisés** via Internet.

**MovianVPN v1.1** a été conçu pour répondre aux exigences de sécurité des **accès wireless et mobile** aux VPN. Le **client Certicom** fonctionne avec une large gamme de gateways VPN, permettant ainsi aux entreprises d'intégrer facilement et de manière sécurisée, des solutions wireless et mobile aux intranets.

## Programme Cisco Security Associates


---

Pour de plus amples informations sur les produits Cisco Security Associates :  
[www.cisco.com/go/securityassociate](http://www.cisco.com/go/securityassociate)

*Remarque : consultez le site Internet Security Associates pour connaître les versions certifiées par le programme Security Associates.*



Section 8  
**REPRESENTATION  
GRAPHIQUE DES  
SOLUTIONS**



Section 8  
**REPRESENTATION  
GRAPHIQUE DES  
SOLUTIONS**



## Représentation graphique des solutions

---

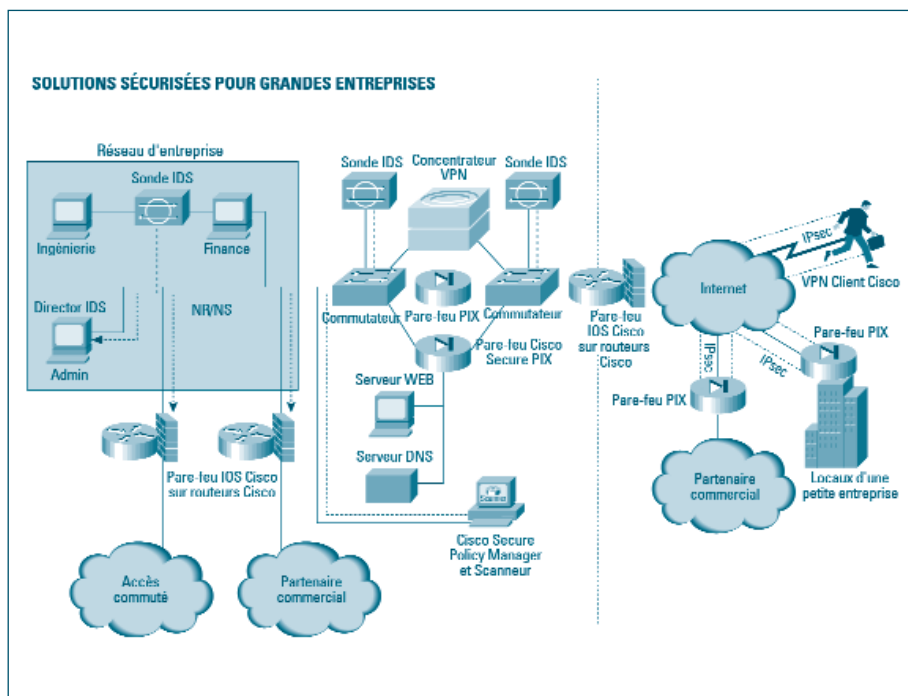
Les représentations graphiques des solutions Cisco exposées dans cette section vous donnent les bases permettant de développer les produits et technologies Cisco en fonction du type d'entreprise. Ces produits et technologies vous permettent de réaliser des transactions d'e-business en toute sécurité, grâce à une stratégie de défense en profondeur.

**Cette section présente des exemples schématisés de solutions de sécurité de réseau pour les types d'entreprises suivants :**

- Grandes entreprises,
- Entreprises de taille moyenne,
- Petites entreprises,
- Entreprises de la nouvelle économie,
- Fournisseurs de services.

## Solutions pour les grandes entreprises

Le point d'entrée de notre exemple utilise les sondes IDS de Cisco pour visualiser le flux de données et les routeurs VPN pour permettre la communication avec les bureaux des différents services et avec les partenaires commerciaux via Internet et IPsec. Les points de terminaison VPN et IPsec ne remettent pas en cause le respect des règles d'activité car le firewall PIX est évolutif et doté de la fonction de basculement. Grâce à la combinaison du firewall Cisco IOS et des technologies IDS, les bureaux des différents services bénéficient d'une protection de défense en profondeur. L'IDS est également positionné autour des dispositifs firewall pour renforcer et tester les règles de sécurité de l'entreprise. Les concentrateurs VPN 3000 de Cisco sont utilisés pour accéder à distance aux services VPN.

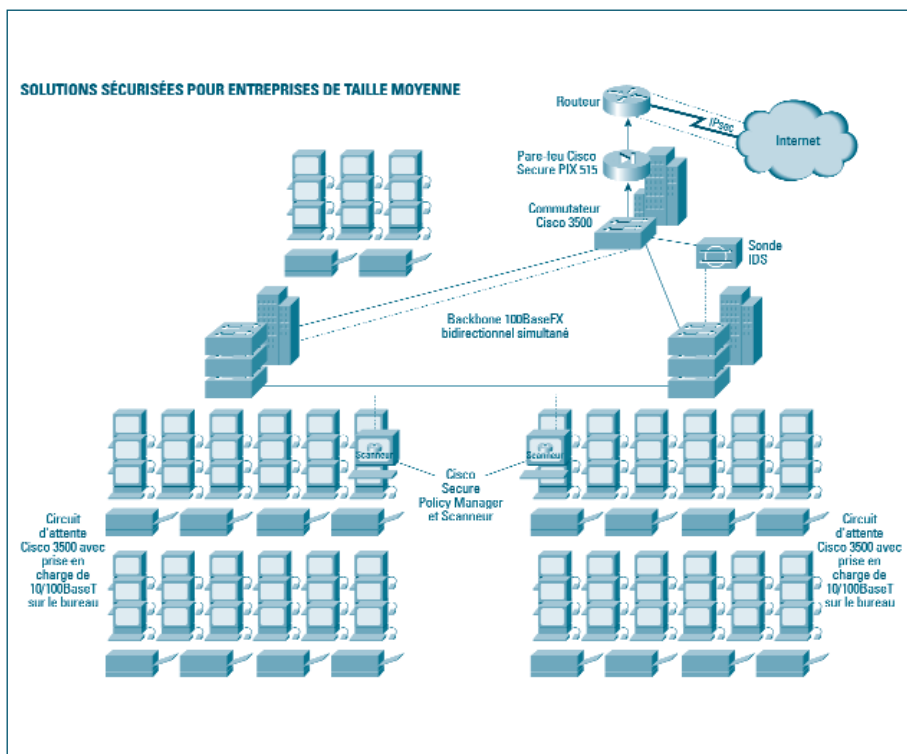




## Représentation graphique des solutions

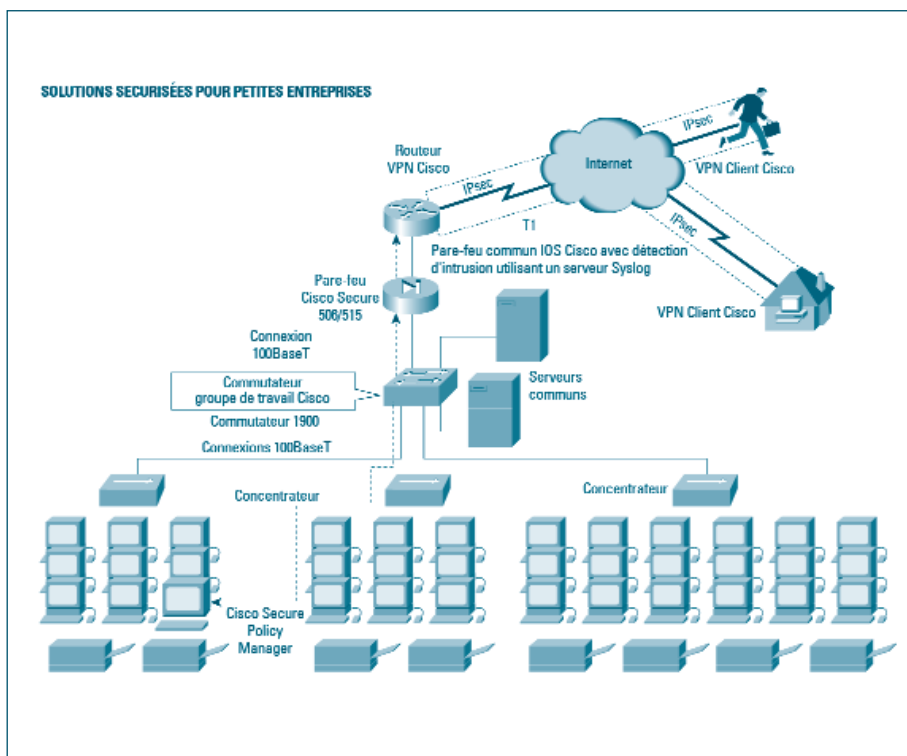
### Solutions pour les entreprises de taille moyenne

La plupart des intervenants sur site de nos clients accèdent au réseau via des routeurs VPN, ce qui leur confère un accès intégral aux réseaux internes. Ceux-ci peuvent être gérés par le CSPM. Une solution de firewall milieu de gamme (le firewall PIX 515 par exemple) assure une sécurité de périmètre à une entreprise de taille moyenne.



## Solutions pour les petites entreprises

Les routeurs VPN Cisco 1700, solutions idéales pour les PME, prennent en charge la voix et IPsec, entre autres technologies de sécurité. Le firewall PIX 506 ou 515 assure une puissance de traitement amplement suffisante aux petites entreprises. Grâce à l'intégration d'un IDS à la sortie, la visibilité du flux de données indique aux responsables du réseau les éventuelles violations du système de sécurité. L'analyse de la vulnérabilité permet d'évaluer la sécurité du réseau de manière proactive et continue à l'aide du scanneur Cisco Secure.

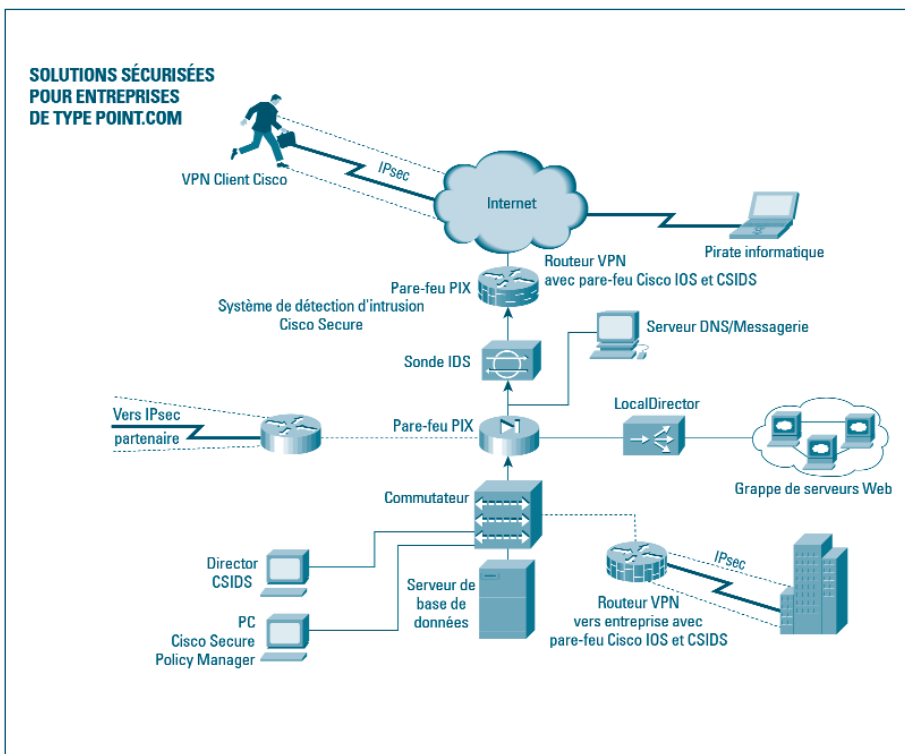




## Représentation graphique des solutions

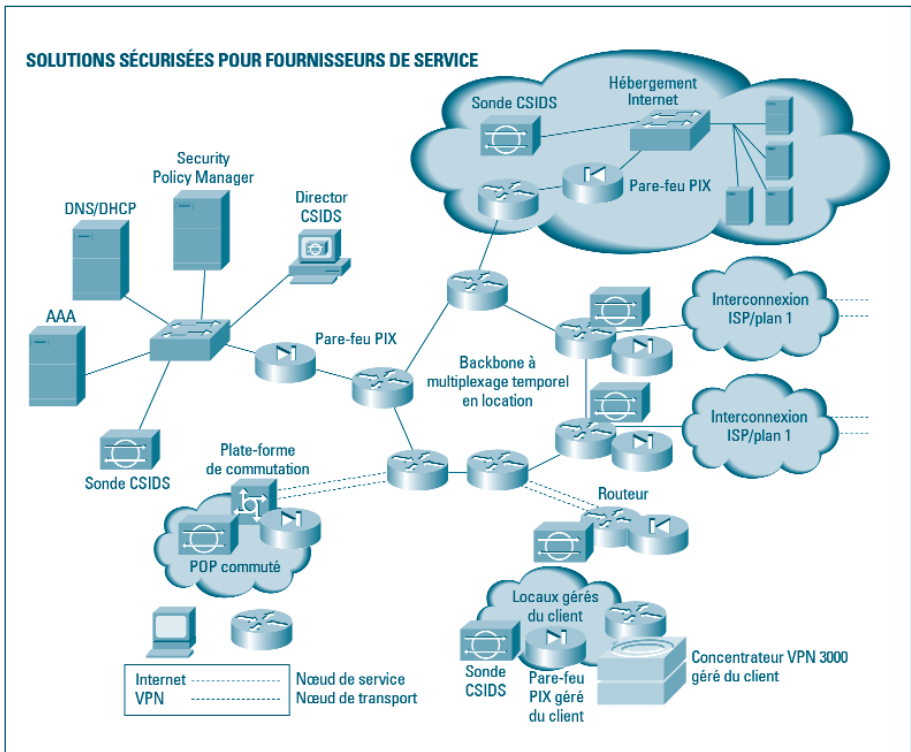
### Solutions pour les entreprises de la nouvelle économie

Les start up sont une cible privilégiée des pirates informatiques et, de plus, leur activité repose entièrement sur la disponibilité des réseaux. Elles doivent, en l'occurrence, élaborer une structure de défense en profondeur. C'est pourquoi nous leur proposons de protéger leurs transactions à l'aide d'un firewall double associé à un système d'IDS. Les réseaux utilisés par les start-up internet étant un élément crucial de leur activité, les solutions de firewall PIX et d'IDS Cisco Secure représentent des éléments de sécurité fondamentaux. Les intervenants sur site peuvent utiliser un VPN client pour accéder aux réseaux des entreprises, des clients et se connecter à un partenaire commercial.



## Solutions pour les fournisseurs de services

Le fait de développer Cisco IOS et de connecter des routeurs VPN à partir de leurs POP permet aux hôtes de transporter des données sur d'autres réseaux et de proposer à leurs clients des firewalls et des systèmes de détection d'intrusion pour protéger les services offerts à leurs clients.



Section 9  
**GLOSSAIRE**



Section 9  
**GLOSSAIRE**



### Terminologie VPN et sécurité

#### A

##### *AAA (Authentication, authorization, and accounting) :*

Éléments de sécurité généralement utilisés pour offrir un accès sécurisé aux ressources :

- Authentication (Authentification) : validation de l'identité d'un utilisateur ou d'un système (hôte, serveur, commutateur ou routeur).
- Authorization (Autorisation) : moyen permettant d'accorder l'accès à un réseau à un utilisateur, un groupe d'utilisateurs, un système ou un programme.
- Accounting (Gestion) : processus permettant d'identifier l'auteur ou la cause d'une action spécifique, tel que le pistage des connexions d'un utilisateur et la journalisation des utilisateurs du système.

##### *Analyse de risque :*

Processus comprenant l'identification des risques en matière de sécurité, leur impact et l'identification des zones nécessitant une protection.

##### *Attaque par interruption de service (DoS) :*

Action malveillante visant à empêcher le fonctionnement normal de tout ou partie d'un réseau ou d'un système hôte. Cette attaque peut être comparée à une personne qui composerait sans arrêt le même numéro de téléphone pour saturer cette ligne.

##### *Attaque SMURF (camouflage) :*

Attaque malveillante consistant à envoyer un grand nombre de paquets ping "spoofés" vers des adresses broadcast, afin d'amplifier le nombre de paquets par la réponse vers les adresses "spoofées". Cette technique offre des possibilités de saturation exponentielles, selon le nombre d'hôtes répondant à la requête.

##### *Autorité de certification (CA) :*

Entité de confiance chargée de signer les certificats numériques et d'attester de l'identité d'autres utilisateurs autorisés.

## Terminologie VPN et sécurité

---

### C

#### *CBAC (Context-Based Access Control) :*

Fonction intégrée au logiciel IOS de Cisco offrant le filtrage avancé de session de paquets pour tout le trafic routable. En configurant des ACL, il est possible d'autoriser ou de refuser le traitement ou le transfert du trafic.

#### *CERT (Computer Emergency Response Team) :*

Organisation officielle d'administrateurs système s'occupant essentiellement de problèmes liés à la sécurité des systèmes et des réseaux informatiques.

#### *Certificat :*

Message signé numériquement au moyen d'une clé privée d'une tierce partie de confiance (voir autorité de certification) et indiquant qu'une clé publique spécifique appartient à une personne ou à un système possédant un nom et un ensemble d'attributs précis.

#### *CHAP (Challenge Handshake Authentication Protocol) :*

Protocole d'authentification permettant d'empêcher les accès non autorisés. Le protocole CHAP authentifie et identifie l'entité distante. Le routeur ou le serveur d'accès détermine ensuite si l'utilisateur peut être autorisé à accéder au réseau.

#### *Clé cryptographique :*

Code numérique servant au cryptage, au décryptage et à la signature d'informations.

#### *Clé privée :*

Code numérique utilisé pour décrypter les données et vérifier les signatures numériques. Cette clé doit demeurer secrète et ne doit être connue que de son propriétaire.

#### *Clé publique :*

Code numérique utilisé pour décrypter les données et vérifier les signatures numériques. Cette clé peut être diffusée librement.

#### *Compromission :*

Dans le domaine de la sécurité informatique, ce terme signifie l'attaque d'un réseau par la violation de la politique de sécurité.

#### *Concentrateur VPN :*

Plate-forme matérielle permettant la mise en place de connexions réseaux privées bout-en-bout via une infrastructure réseau publique et offrant un accès distant ou une connectivité site à site.



### *Concentrateur VPN :*

Plate-forme matérielle permettant la mise en place de connexions réseaux privées bout-en-bout via une infrastructure réseau publique et offrant un accès distant ou une connectivité site à site.

### *Confidentialité des données :*

Moyen permettant de garantir que seules les entités autorisées peuvent voir les paquets de données dans un format intelligible.

Processus de protection des données d'un réseau contre l'espionnage ou l'altération.

Dans certains cas, la séparation des données à l'aide de technologies de tunnellation, telles que GRE (generic routing encapsulation) ou le L2TP (Layer 2 Tunneling Protocol), offre une confidentialité des données efficace. Toutefois, il est parfois nécessaire d'augmenter la confidentialité à l'aide de technologies de cryptage numérique et de protocoles tels que Ipsec, en particulier lors de la mise en œuvre de VPN.

### *Contrôle d'accès :*

Limitation du flux de données des ressources d'un système uniquement vers les personnes, programmes, processus autorisés ou vers d'autres systèmes du réseau. Les ensembles de règles de contrôle d'accès des routeurs Cisco sont appelées listes de contrôle d'accès ou ACL.

### *Contrôle de la sécurité :*

Procédure de sécurisation du réseau au moyen de tests réguliers et de SPA (Security Posture Assessments).

### *Cryptage :*

Codage des données empêchant leur lecture par une autre personne que le destinataire prévu. De plus, les données sont uniquement lisibles après avoir été correctement décryptées.

### *Cryptographie :*

Science de l'écriture et de la lecture de messages codés.

## Terminologie VPN et sécurité

---

### D

#### *DES (Data Encryption Standard) :*

Système de cryptage à clé secrète normalisé par le National Institute of Standards and Technology (voir NIST et Triple DES).

#### *Diffie Hellman :*

Système à clé publique permettant à deux utilisateurs ou équipements réseau d'échanger des clés publiques via un support non sécurisé.

#### *DSS (Digital Signature Standard) :*

Algorithme de signature numérique développé par la National Security Agency (voir NSA).

### E-H

#### *En-tête d'authentification :*

En-tête IPsec permettant de vérifier que le contenu d'un paquet n'a pas été modifié pendant le transport.

#### *Filtrage :*

Recherche dans le trafic réseau de certaines caractéristiques, telles que l'adresse source, l'adresse de destination ou le protocole, afin de déterminer, selon les critères définis, si le trafic de données concerné est accepté ou bloqué.

#### *Filtrage de paquets :*

Mécanisme de contrôle paquet par paquet du trafic routable.

#### *GRE (Generic Routing Encapsulation) :*

Protocole de tunnellation développé par Cisco permettant d'encapsuler des paquets utilisant de nombreux protocoles différents dans des tunnels IP, afin de créer un lien point à point virtuel entre des points distants et des routeurs Cisco via un réseau IP.

#### *Hack :*

Méthode utilisée pour obtenir l'accès illégal et non autorisé à un réseau, en vue de dérober des documents ou des données confidentielles ou par simple démonstration technique.

#### *HSRP (Hot Standby Router Protocol) :*

Permet aux stations de travail utilisant IP de communiquer sur l'interréseau même si leurs routeurs par défaut sont indisponibles. Ce protocole garantit une disponibilité élevée du réseau et un changement de topologie réseau totalement transparent.



### **Identité :**

Identification précise des utilisateurs, hôtes, applications, services et ressources du réseau. Les nouvelles technologies, telles que les certificats numériques, les cartes à puces, les services répertoire jouent un rôle de plus en plus important dans les solutions d'identification.

### **IDS (*Intrusion Detection System*) :**

Sentinelle de sécurité en temps réel (semblable à un détecteur de mouvement) protégeant le périmètre du réseau, les extranets et les réseaux internes de plus en plus vulnérables. Les systèmes IDS analysent le flux de données du réseau à la recherche de signatures d'attaques ou d'activités considérées comme non autorisées, déclenchent l'alarme et lancent les actions nécessaires face à cette activité.

### **IETF (*Internet Engineering Task Force*) :**

Organisme de normalisation responsable de la conception de protocoles pour Internet. Les publications émises par l'IETF s'intitulent des RFC (Request for Comments).

### **Intégrité :**

Moyen permettant de garantir que les données n'ont pas été modifiées, si ce n'est par les personnes explicitement autorisées à le faire. Le terme "intégrité du réseau" signifie qu'aucun service ou aucune activité contraire à la politique de sécurité n'est permise.

### **Intégrité des données :**

Processus permettant de garantir que les données n'ont pas été modifiées ou détruites lors du transport via le réseau.

### **IP (*Internet Protocol*) :**

Protocole basé sur l'utilisation de paquets permettant l'échange de données via des réseaux informatiques.

### **IPsec :**

Ensemble de normes de sécurité offrant des services de confidentialité et de d'authentification au niveau de la couche IP (Internet Protocol).

### **ISAKMP (*Internet Security Association and Key Management Protocol*) :**

Protocole de gestion de clés pour IPsec. Ce protocole, nécessaire à la mise en œuvre complète de IPsec, est également appelé IKE (Internet Key Management).

## Terminologie VPN et sécurité

---

### K–N

#### *Kerberos :*

Protocole d'authentification réseau à clé secrète développé par le MIT (Massachusetts Institute of Technology), basé sur l'utilisation de l'algorithme de cryptage DES pour le cryptage et une base de données de clés centralisée pour l'authentification.

#### *L2F (Layer 2 Forwarding Protocol) :*

Protocole gérant la mise en place de réseaux virtuels privés commutés via Internet.

#### *L2TP (Layer 2 Tunneling Protocol) :*

Norme IETF combinant les caractéristiques du protocole L2F de Cisco (Layer 2 Forwarding Protocol) et le protocole PPTP de Microsoft (Point-to-Point Tunneling Protocol) pour la mise en œuvre des VPN.

#### *L2TP/IPsec (Layer 2 Tunneling Protocol over IPsec) :*

Protocole VPN de Windows 2000 combinant accès distant (L2TP) et sécurité (IPsec).

#### *MD5 (Message Digest 5) :*

Algorithme de hachage utilisé pour l'authentification de données et la vérification de l'intégrité des communications.

#### *NAT (Network Address Translation) :*

Mécanisme consistant à convertir une adresse IP en une autre. Le NAT est essentiellement utilisé pour connecter un espace d'adressage interne utilisant un protocole différent d'un autre réseau, tel qu'Internet.

#### *NDS (Novell Directory Services) :*

Système de nommage général pour les environnements Novell contenant des informations relatives à un réseau, en particulier les objets de ce réseau.

#### *NIST (National Institute of Standards and Technology) :*

Agence gouvernementale américaine établissant des normes techniques à l'échelle nationale.

#### *Non-répudiation :*

Caractéristique d'un système cryptographique permettant d'empêcher qu'un expéditeur puisse nier ultérieurement avoir envoyé un message ou effectué une action spécifique.



**NSA (National Security Agency) :**

Agence gouvernementale américaine chargée de contrôler et de décoder toutes les communications émanant de pays étrangers et susceptibles de concerner la sécurité des Etats-Unis.

## P

**PAP (Password Authentication Protocol) :**

Protocole d'authentification permettant à des postes PPP de s'authentifier les uns auprès des autres. Le routeur distant qui effectue une tentative de connexion sur le routeur local doit envoyer une requête d'authentification. Contrairement à CHAP, PAP ne crypte pas le mot de passe et le nom d'hôte ou d'utilisateur. PAP détermine si un mot de passe est valide ou non.

**Firewall :**

Système matériel ou logiciel utilisé pour contrôler le trafic de données entre deux réseaux.

**Périmètre de sécurité :**

Périmètre dans lequel des contrôles de sécurité sont effectués afin de protéger les équipements réseau.

**Ping :**

Commande permettant de déterminer la présence et l'état de fonctionnement d'un autre système.

**Ping of Death (Ping de la mort) :**

Attaque par interruption de service (DoS) consistant en l'envoi d'un paquet ping de taille surdimensionnée, dans le but d'entraîner le blocage de la machine réceptrice lors de la tentative de réassemblage du paquet de données surdimensionné.

**PKI (Public Key Infrastructure) :**

Infrastructure de gestion de clés offrant un environnement sûr et fiable.

**Politique de sécurité :**

Ensemble de directives de haut niveau permettant de contrôler le déploiement des services réseau. La maintenance et l'audit du réseau font également partie de la politique de sécurité.

## Terminologie VPN et sécurité

---

### *PPP (Point-to-Point Protocol) :*

Protocole normalisé d'encapsulation de paquets IP via des liens point à point.

### *PPTP (Point-to-Point Tunneling Protocol) :*

Norme IETF soutenue par Microsoft pour la mise en œuvre des VPN à partir du système d'exploitation Windows 95/98 vers une passerelle VPN.

### *Proxy :*

Équipement (mandataire) effectuant une tâche à la place d'un autre équipement. Dans le domaine des firewalls, le proxy est un processus effectuant un certain nombre de contrôles sur le trafic entrant. Ce mécanisme peut nuire aux performances du firewall.

## R

### *RADIUS (Remote Access Dial-In User Service) :*

Protocole développé par Livingston Enterprises Inc., utilisé comme protocole d'authentification et de gestion de serveur d'accès.

### *Réinitialisation TCP :*

Réponse possible à une attaque de hacker d'une sonde Cisco Secure IDS ou d'un routeur Cisco IOS Firewall. Une commande est émise par ces équipements afin d'arrêter la connexion par laquelle l'attaque est effectuée, obligeant ainsi l'attaquant à établir une nouvelle connexion.

### *Routeur VPN :*

Routeur destiné à être installé dans les locaux du client. Ce type de routeur prend en charge la fonctionnalité VPN et offre des performances VPN optimales sur différents types de supports physiques et densités de ports.

### *RSA (Rivest, Shamir, Adelman) :*

Algorithme de cryptage à clé publique permettant de crypter ou de décrypter des données et d'appliquer ou de vérifier une signature numérique.

## S

### *Scanneur :*

Application professionnelle permettant à l'utilisateur d'identifier et de corriger les failles dans la sécurité du réseau avant qu'un hacker ne le découvre.

### *SHA (Secure Hash Algorithm) :*

Algorithme de hachage utilisé pour l'authentification et la vérification de l'intégrité des communications.



### *Shunning :*

Reconfiguration dynamique par un routeur Cisco de ses ACL afin de stopper toute attaque détectée et de bloquer toute nouvelle transmission de données de/vers l'adresse IP "attaquante", pour un laps de temps donné.

### *Signature d'attaque :*

Système d'identification d'activité malveillante sur le réseau. Les paquets de données entrants sont examinés en détail à la recherche de modèles logarithmiques identiques.

### *Signature numérique :*

Chaîne de bits ajoutée à un message électronique (hachage crypté) permettant l'authentification et l'intégrité des données.

### *Spoofing (usurpation) :*

Tentative d'accès à un système réseau par usurpation (utilisateur, système ou programme autorisés).

## T-V

### *TACACS+ (Terminal Access Controller Access Control System Plus) :*

Protocole AAA principalement utilisé pour la gestion des connexions commutées.

### *Triple DES :*

Algorithme DES combiné à une, deux ou trois clés pour le cryptage/décryptage de paquets de données.

### *Tunnel :*

Connexion sécurisée et cryptée entre deux points passant par un réseau public ou tiers.

### *VPN (Réseau privé virtuel) :*

Réseau garantissant un trafic IP sécurisé via un réseau TCP/IP public grâce au cryptage des données entre les deux réseaux concernés. Le VPN utilise la tunnellation pour crypter les informations au niveau IP.

### *VRRP (Virtual Router Redundancy Protocol) :*

Gère le basculement automatique d'une plate-forme à une autre au sein d'une installation redondante.

## Terminologie VPN et sécurité

---

### *Vulnérabilité :*

Faille au niveau des procédures de sécurité, de la conception ou la mise en œuvre du réseau, pouvant être exploitée pour contourner la politique de sécurité d'une entreprise.

### *WINS (Windows Internet Naming Service) :*

Permet à des clients de sous-réseaux IP différents de s'enregistrer dynamiquement et de naviguer sur le réseau sans recourir au broadcast.

### **Pour de plus amples informations :**

Sécurité : [www.cisco.com/go/security](http://www.cisco.com/go/security)

VPN pour l'entreprise : [www.cisco.com/go/evpn](http://www.cisco.com/go/evpn)

## **Cisco Systems Europe**

11, rue Camille Desmoulins  
92782 Issy les Moulineaux Cedex 9 - France  
Tél. : +33 (0)1 58 04 60 00  
Fax : +33 (0)1 58 04 61 00  
[www.cisco.fr](http://www.cisco.fr)



Copyright © 2000 Cisco Systems, Inc. Tous droits réservés. NetSonar et PIX sont des marques, et Catalyst, IOS, NetRanger, Cisco, Cisco IOS, Cisco Systems, ainsi que le logo Cisco Systems sont des marques commerciales de Cisco Systems, Inc. ou de ses représentants aux Etats-Unis et dans d'autres pays. Toutes les autres marques commerciales mentionnées dans le présent document sont la propriété de leur propriétaire respectif. L'utilisation du terme "partenaire" ne fait pas référence à un partenariat commercial entre Cisco et toute autre entreprise.  
(0005R)

N° doc. : 954913 ETMG-LW 08/00