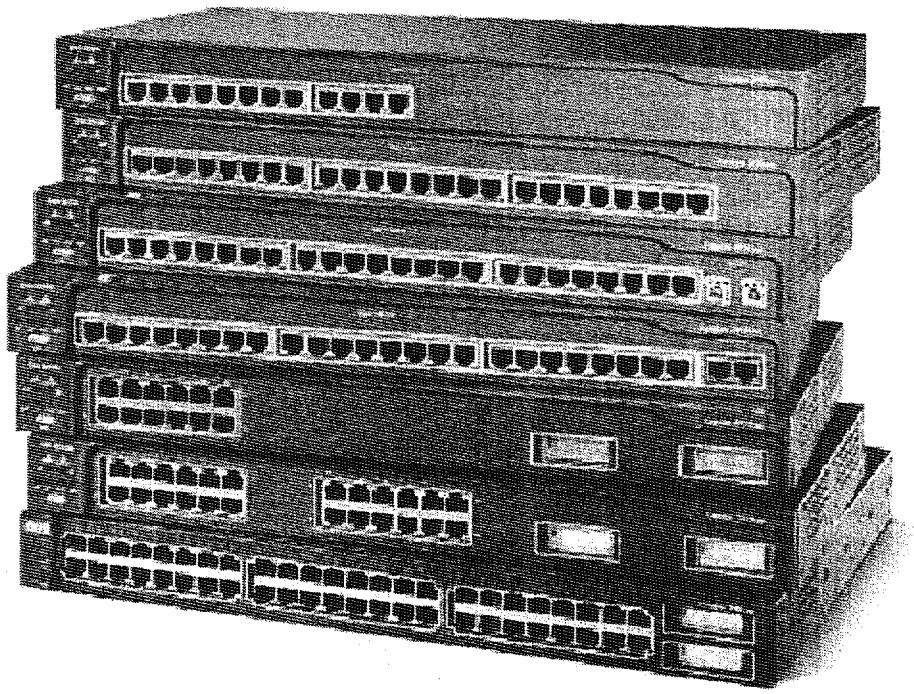
Cisco Catalyst 6500 Series 24-Port 10 FL Ethernet Module MT-RJ	WS-6024-10FL-MT
Cisco Catalyst 6500 Series 24-Port 100 BASE-FX (MMF) FE Module	WS-X6324-100FX-MM
Cisco Catalyst 6500 Series 24-Port 100 BASE-FX (SFM) FE Module	WS-X6324-100FX-SM
Cisco Catalyst 6500 Series 48-port 10/100 Fast Ethernet Module (RJ21V)	WS-X6148-RJ21V
Cisco Catalyst 6500 Series 48-port 10/100 Fast Ethernet Module (RJ45V)	WS-X6148-RJ45V
Cisco Catalyst 6500 Series 48-Port 10/100 Fast Ethernet RJ-21 Module	WS-X6148-RJ21
Cisco Catalyst 6500 Series 48-Port 10/100 Fast Ethernet RJ-45 Module	WS-X6148-RJ45
Cisco Catalyst 6500 Series 48-Port 10/100 Inline Power RJ-21 Line Card	WS-X6348-RJ21V
Cisco Catalyst 6500 Series 48-Port 10/100 Inline Power RJ-45 Line Card	WS-X6348-RJ45V
Cisco Catalyst 6500 Series Fabric-enabled 10/100 FE RJ-21 Module	WS-X6548-RJ21
Cisco Catalyst 6500 Series 10/100 Fast Ethernet RJ-45 Module	WS-X6548-RJ45
Cisco Catalyst 6500 Series 100 FX (MMF) Fast Ethernet Module	WS-X6324-100FX-MM
Advanced Integrated Services Modules	
Cisco Catalyst 6500 Series Wireless LAN Services Module	WS-SVC-WLAN-1-K9
Cisco Catalyst 6500 8 port Voice T1/E1 and Services Module	WS-X6608-T1, WS-X6608-E1
Cisco Catalyst 6500 IPSec VPN Services Module	WS-SVC-IPSEC-1
Cisco Catalyst 6500 Network Analysis Module (NAM 1/NAM 2)	WS-SVC-NAM-1, WS-SVC-NAM-2
Cisco Catalyst 6500 Series Communication Media Module	WS-SVC-CMM
Cisco Coarse Wave Division Multiplexing (CWDM) GigaBit Interface Converters (GBICs)	
1000BASE-CWDM 1470 nm GBIC (single mode only)	CWDM-GBIC-1470=
1000BASE-CWDM 1490 nm GBIC (single mode only)	CWDM-GBIC-1490=
1000BASE-CWDM 1510 nm GBIC (single mode only)	CWDM-GBIC-1510=
1000BASE-CWDM 1530 nm GBIC (single mode only)	CWDM-GBIC-1530=
1000BASE-CWDM 1550 nm GBIC (single mode only)	CWDM-GBIC-1550=
1000BASE-CWDM 1570 nm GBIC (single mode only)	CWDM-GBIC-1570=
1000BASE-CWDM 1590 nm GBIC (single mode only)	CWDM-GBIC-1590=

Gamme Cisco Catalyst 2950. Commutateurs d'étage Catalyst 10/100/1000

La gamme Catalyst® 2950 de Cisco est destinée à la commutation d'étage dédiée Ethernet 10/100/1000 Mbits/s fixe, offrant des performances, une souplesse et une facilité d'administration exceptionnelles, combinées à une protection de l'investissement inégalée. Cette gamme de commutateurs 10/100/1000 à détection automatique offre de nombreuses fonctionnalités avancées de qualité de service (QoS) et de traitement des flux multicast, il fonctionne sur le principe de commutation « store and forward ». L'interface de gestion Web fournit des fonctions d'administration faciles à utiliser via la suite CMS (Cisco Cluster Management Suite) et le logiciel Cisco IOS intégré. Le Catalyst 2950T-24 Gigabit sur cuivre, avec deux liaisons ascendantes à haut débit 10/100/1000, offre pour les petites et moyennes entreprises une solution idéale pour migrer de Fast Ethernet vers le Gigabit Ethernet tout en utilisant le câblage cuivre catégorie 5 existant.

La gamme de commutateur Catalyst 2950 est composée de 9 modèles différents permettant de combiner tous les besoins en nombre de ports 10/100 de 12 à 48 ports, et les besoins en ports 100FX, Gigabit cuivre, et Gigabit fibre.



Dénomination du commutateur	Nombre de ports 10/100TX	Nb de ports Giga	Type des ports Giga	Nb de ports 100FX[A]	Perf. en Gb/s	10⁶ de pps	Logiciel IOS utilisable
2950-12	12	0	-	0	2,4	1,8	SI
2950-24	24	0	-	0	4,4	3,6	SI
2950SX-24	24	2	SX MT-RJ	0	8,8	6,6	SI
2950C-24	24	0	-	2	5,2	3,9	EI
2950T-24	24	2	10/100/1000	0	8,8	6,6	EI
2950G-12-EI	12	2	GBIC Cisco	0	6,4	4,8	EI
2950G-24-EI	24	2	GBIC Cisco	0	8,8	6,6	EI
2950G-24-EI-DC	24	2	GBIC Cisco	0	8,8	6,6	EI
2950G-48-EI	24	2	GBIC Cisco	0	13,6	10,1	EI

[A] Connecteurs MT-RJ pour les ports 100 Base FX.

Routeurs Cisco 1700 Cisco 1721 et Cisco 1720

Les routeurs Cisco 1721 et 1720 ouvrent les portes de l'e-business en garantissant un accès sécurisé Internet, intranet et extranet grâce aux réseaux privés virtuels (VPN) et à la technologie des pare-feu. Les routeurs Cisco 1721 et 1720 offrent les avantages suivants :

- un large choix d'options d'accès WAN comprenant une connexion ADSL haut débit de qualité professionnelle
- le routage hautes performances avec gestion de la bande passante
- le routage inter VLAN (Cisco 1721 seulement)
- l'accès VPN avec option pare-feu

Le Tableau 1 ci-dessous compare les deux produits.

Caractéristiques	Cisco 1721	Cisco 1720
Performances de routage (par paquets de 64 octets)	12 000 paquets par seconde	8 400 paquets par seconde
DRAM (par défaut / maximum)	32 Mo / 96 Mo	32 Mo / 48 Mo
Flash (par défaut / maximum)	16 Mo /16 Mo (non extensible)	8 Mo / 16 Mo
Routage VLAN IEEE 802.1Q	Oui	Non
Témoin LED du module de cryptage	Oui	Non

Prise en charge complète du réseau WAN

Les routeurs Cisco 1721 et 1720 supportent jusqu'à deux des cartes WIC présentées dans le Tableau 3. Ces cartes d'interface prennent en charge un grand nombre de technologies de réseau WAN : Réseau Numérique à Intégration de Services (RNIS), liaisons séries asynchrones et synchrones comme les lignes louées, Frame Relay, ADSL, G.shdsl, Switched 56, X.25 et SMDS (Switched Multimegabit Data Service) ainsi qu'Ethernet mono port.

Tableau 2 support de réseau WAN pour les routeurs Cisco 1721 et 1720

Carte WIC	Description
WIC-1T	Un port série, asynchrone et synchrone (T1/E1)
WIC-2T	Deux ports séries, asynchrones et synchrones (T1/E1)
WIC-2A/S	Deux ports séries bas débit (jusqu'à 128 kbits/s), asynchrones et synchrones
WIC-1B-S/T	Un port RNIS BRI (Basic Rate Interface) S/T
WIC-1B-U	Interface à un port RNIS BRI U avec NT1 intégré
WIC-1DSU-56K4	Un port 56/64 kbits/s intégré, unité DSU/CSU quatre fils.
WIC-1DSU-T1	Un port T1/T1 fractionnée intégré avec unité DSU/CSU
WIC-1ADSL	Interface ADSL à un port
WIC-1ENET	Interface à un port Ethernet 10BASE-T
WIC-1SHDSL	Interface à un port G.shdsl
VWIC-1MFT-T1*	Carte VWIC à un port RJ-48 multiflex – T1
VWIC-2MFT-T1*	Carte VWIC à deux ports RJ-48 multiflex – T1
VWIC-2MFT-T1-DI*	Carte VWIC 2 ports RJ-48 multiflex – T1 avec canaux d'extraction "drop" et d'insertion "insert"
VWIC-1MFT-E1*	Carte VWIC à un port RJ-48 multiflex – E1
VWIC-2MFT-E1*	Carte VWIC à deux ports RJ-48 multiflex – E1
VWIC-2MFT-E1-DI*	Carte VWIC 2 ports RJ-48 multiflex – E1 avec canaux d'extraction "drop" et d'insertion "insert"
VWIC-1MFT-G703*	Carte VWIC à un port RJ-48 multiflex – E1 G.703
VWIC-2MFT-G703*	Carte VWIC à deux ports RJ-48 multiflex – E1 G.703

Interfaces et ports matériels

• Un port Fast Ethernet 10/100BASE-TX (RJ-45)
– Détection automatique du débit
– Négociation automatique du mode duplex
– Routage VLAN IEEE 802.1Q (Cisco 1721 seulement)

• Deux emplacements pour cartes d'interface WAN
– Supporte toute combinaison de deux cartes d'interface WAN comme le montre le Tableau 3

• Un port auxiliaire (AUX)
– Prise RJ-45 avec interface EIA/TIA-232

• Un port console
– Prise RJ-45 avec interface EIA/TIA-232

• Un emplacement d'extension interne pour la prise en charge des services à accélération matérielle comme le cryptage VPN (jusqu'à T1/E1).

Caractéristiques des cartes WIC (en option)

• Interfaces séries synchrones sur les cartes WIC
– Débit de l'interface : jusqu'à 2,0 Mbits/s (T1/E1)
- Protocoles série synchrones : Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC),
- Interfaces séries synchrones supportées sur les cartes WIC-1T, WIC-2T et WIC-2A/S : V.35, EIA/TIA-232, EIA/TIA-449, X.21, EIA- 530

• Carte WIC ADSL
– Supporte les services et les applications de la couche d'adaptation ATM AAL 5;
– Compatible avec le multiplexeur d'accès DSL (DSLAM) Alcatel avec chipset Alcatel et le DSLAM Cisco 6130/6260 avec le chipset Globespan
– Conforme avec ANSI T1.413 version 2 et ITU 992.1 (G.DMT)

• Des cartes d'interface WAN
– Accès commuté RNIS et IDSL à 64 et 128 kbits/s.
– Encapsulation sur IDSL, Frame Relay et PPP

Tableau 3 Package Routeur VPN

Package routeur VPN	Ports Fast-Ethernet	Emplacement combiné pour carte WIC ou VWIC	Emplacement combiné pour carte VIC (Voice interface Card) ou emplacements pour cartes WIC ou VWIC	Emplacements pour cartes VIC seuls	Emplacements pour modules de réseau	Plate-forme logicielle IOS Cisco	Mémoire Flash (Mo)*	Mémoire DRAM (Mo)*	Carte VPN	Autres modules
c1721-VPN/K9	1	2	–	–	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	En option
c1721-VPN/K9-A	1	2	–	–	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	Carte WIC à 1 port ADSL intégrée
c1751-VPN/K9	1	–	2	1	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	En option
c1751-VPN/K9-A	1	–	2	1	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	Carte WIC à 1 port ADSL intégrée
c1760-VPN/K9	1	–	2	2	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	En option
c1760-VPN/K9-A	1	–	2	2	–	IP Plus/FW/IDS/3DES	16	64	MOD1700-VPN	Carte WIC à 1 port ADSL intégrée
c1760-V3PN/K9	1	–	2	2	–	IP Plus/ ADSL/VO	32	96	MOD1700-VPN	DSP à 4 voies intégré

Introduction

Pour sécuriser les échanges ayant lieu sur un réseau TCP/IP, il existe plusieurs approches :

- niveau applicatif (PGP)
- niveau transport (protocoles TLS/SSL, SSH)
- niveau physique (boîtiers chiffrant).

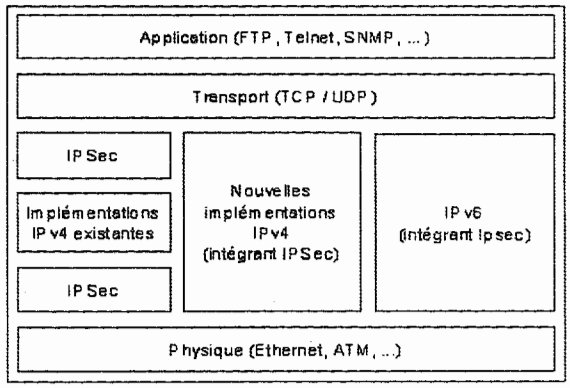
Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6.

Ces mécanismes sont couramment désignés par le terme

IPsec pour IP Security Protocols.

IPsec fournit donc :
- confidentialité et protection contre l'analyse du trafic,
- authentification des données (et de leur origine),
- intégrité des données (en mode non connecté),
- protection contre le rejeu,
- contrôle d'accès.
- authentification des données (et de leur origine),
- intégrité des données (en mode non connecté),
- protection contre le rejeu,
- contrôle d'accès.

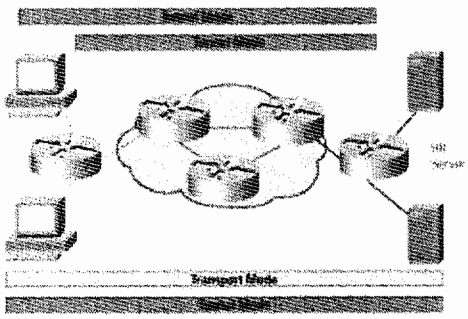
Positionnement du protocole IPSec dans la pile IP

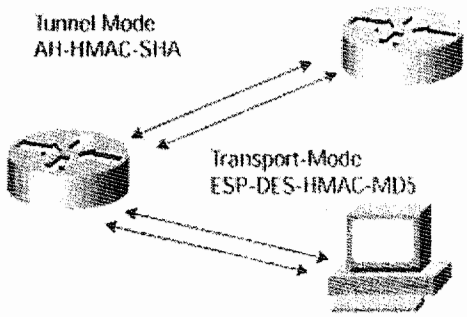


IPsec est une extension de sécurité pour le protocole Internet IP. Il peut être mis en œuvre sur tous les équipements du réseau et de nombreux fournisseurs l'intègrent désormais dans leurs produits. Exemple d'utilisation : Les réseaux privés virtuels ou VPN ou bien la sécurisation des accès distants à un intranet.

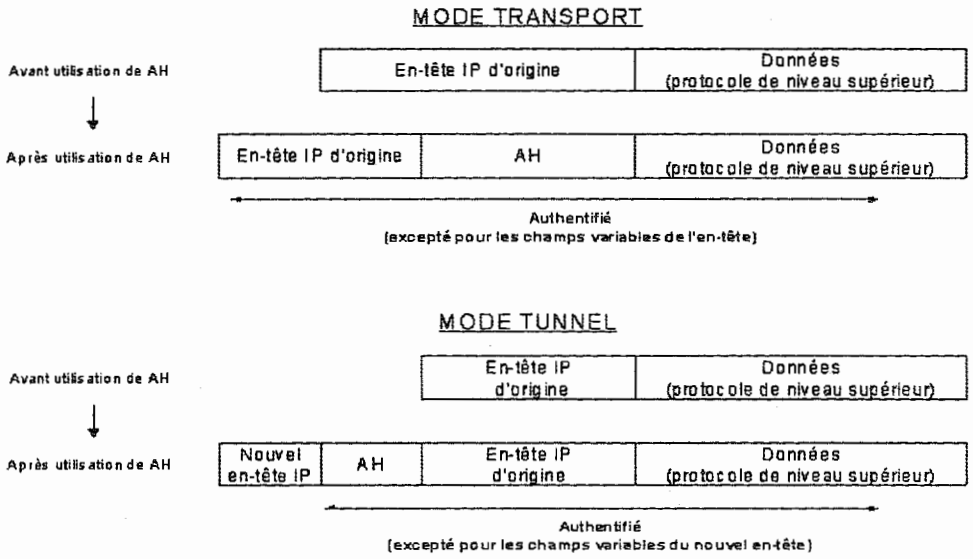
Mode transport et mode tunnel

Le mode transport prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans ce mode, l'insertion de la couche IPsec est transparente entre TCP et IP. TCP envoie ses données vers IPsec comme il les enverrait vers IPv4. L'inconvénient de ce mode réside dans le fait que l'en-tête extérieur est produit par la couche IP c'est-à-dire sans masquage d'adresse. De plus, le fait de terminer les traitements par la couche IP ne permet pas de garantir la non-utilisation des options IP potentiellement dangereuses. L'intérêt de ce mode réside dans une relative facilité de mise en œuvre.
Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche IP incluse, puis sont envoyées vers le module IPsec. L'encapsulation IPsec en mode tunnel permet le masquage d'adresses.





Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.



Protocole AH (Authentication Header)

AH est conçu pour assurer l'intégrité en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données (pas de confidentialité). L'absence de confidentialité permet de s'assurer que ce standard pourra être largement répandu sur Internet, y compris dans les endroits où l'exportation, l'importation ou l'utilisation du chiffrement dans des buts de confidentialité est restreint par la loi.

Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé "valeur de vérification d'intégrité" (Intégrity Check Value, ICV). La protection contre le rejeu se fait grâce à un numéro de séquence.

En-tête suivant	Longueur	Réservé
Index des paramètres de sécurité (SPI)		
Numéro de séquence		
Données d'authentification (longueur variable)		

Conclusions

Forces et faiblesses du cadre protocolaire IPsec
Avantages :
- Modèle de sécurité flexible et non exhaustif basé sur une boîte à outils modulaire
- Possibilité d'instaurer plusieurs crans de sécurité : chiffrement faible ou fort et/ou authentification
- Services de sécurité totalement transparent pour les applications

Inconvénients :
- Mécanismes de sécurité trop nombreux, engendrant un système complexe
- IPsec interdit la translation d'adresses (Network address translation, NAT)
- L'interaction du protocole IKE avec les infrastructures à clé publique (PKI) est possible mais il reste à normaliser
- Les outils d'administration centralisée des règles de sécurité (Security Policies) font défaut
- Entorses propriétaires nuisibles à l'interopérabilité
- IPsec est limité à l'instauration de VPN entre réseaux (passerelles-serveurs).