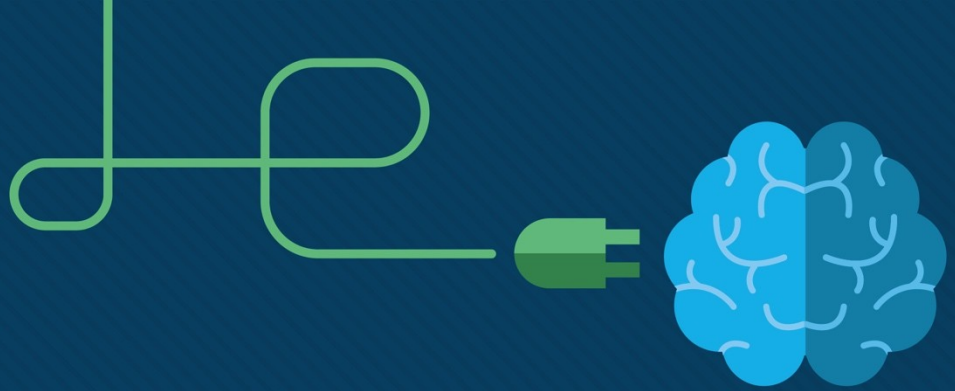


Module: Conceptions de VPN et IPsec

Réseau, Sécurité et Automatisation D'entreprise v7.0 (ENSA)

Objectifs de ce module

Module: Conceptions de VPN et IPsec

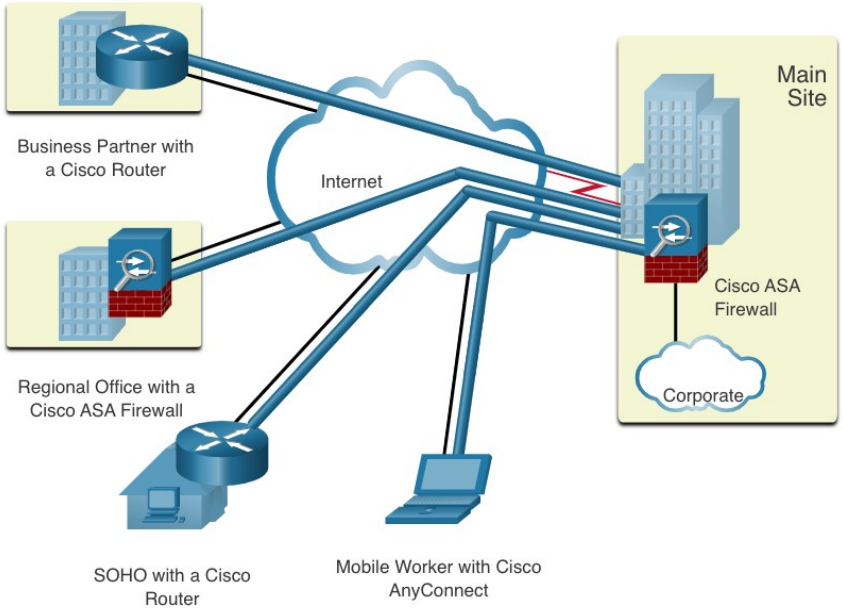
L'objectif du Module:Expliquer comment les VPN et IPsec sont utilisés pour sécuriser la connectivité de site à site et d'accès distant.

Titre du Rubrique	Objectif du Rubrique
Technologie VPN	Décrire les avantages de la technologie VPN.
Types de VPN	Décrire les différents types de VPN.
IPsec	Expliquez comment le cadre IPsec est utilisé pour sécuriser le trafic réseau.

1 Technologie VPN

Réseau privé virtuel

- Réseaux privés virtuels (VPN) pour créer des connexions de réseau privé de bout en bout.
- Un VPN est virtuel en ce sens qu'il transporte des informations au sein d'un réseau privé, mais que ces informations sont effectivement transférées via un réseau public.
- Un VPN est privé, dans le sens où le trafic est chiffré pour assurer la confidentialité des données pendant qu'il est transporté à travers le réseau public.



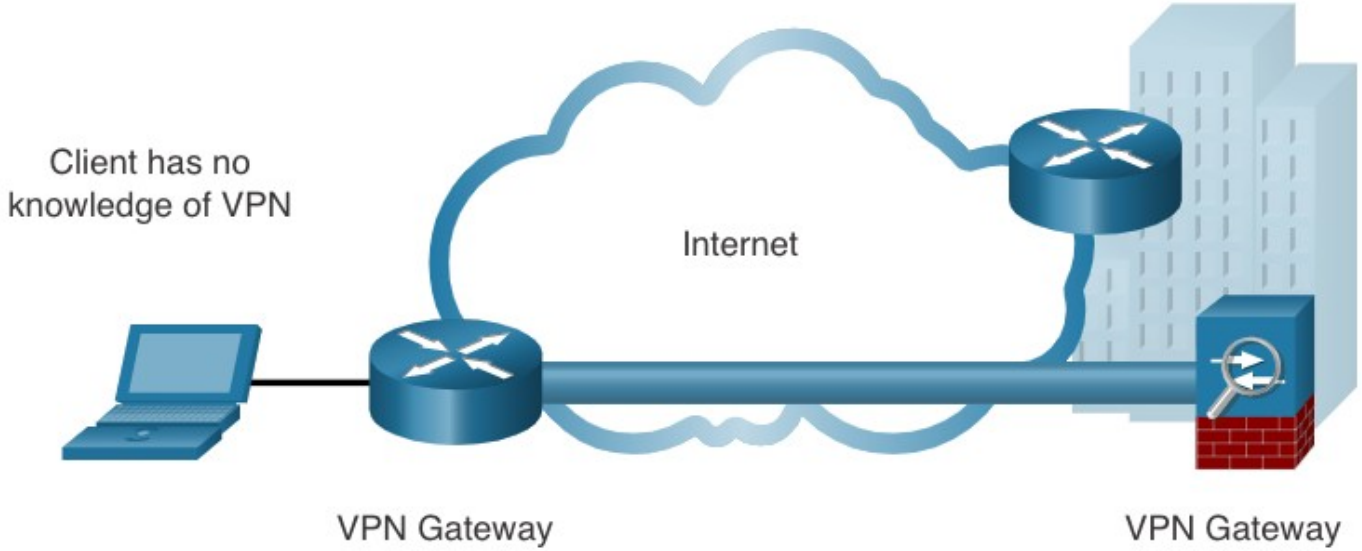
Les Bénéfices de VPN

- Les VPN modernes prennent en charge les fonctionnalités de chiffrement, telles que les protocoles IPsec (Internet Protocol Security) et SSL (Secure Sockets Layer) pour sécuriser le trafic réseau entre sites.
- Les principaux avantages des VPN sont présentés dans le tableau:

Bénéfice	Description
Réductions des coûts	Les organisations peuvent utiliser des VPN pour réduire leurs coûts de connectivité tout en augmentant simultanément la bande passante de connexion à distance.
Sécurité	Les protocoles de chiffrement et d'authentification protègent les données contre les accès non autorisé.
Extensibilité	Les VPN permettent aux organisations d'utiliser Internet, ce qui facilite l'ajout de nouveaux utilisateurs sans ajouter d'infrastructure importante.
Compatibilité	Les VPN peuvent être mis en œuvre sur une grande variété d'options de liaison WAN, y compris les technologies à large bande. Les travailleurs distants peuvent utiliser ces connexions à haut débit pour accéder en toute sécurité aux réseaux d'entreprise.

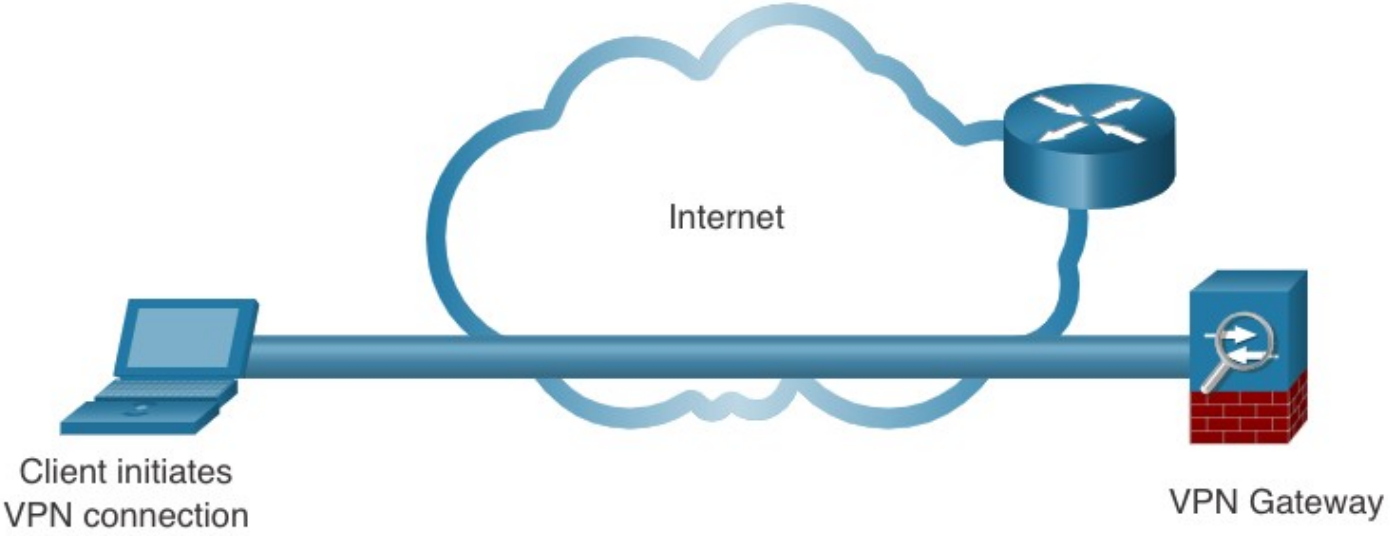
VPN de site à site et d'accès distant

Un VPN de site à site se termine sur les passerelles VPN. Le trafic VPN n'est crypté qu'entre les passerelles. Les hôtes internes ne savent pas qu'un VPN est utilisé.



VPN de site à site et d'accès distant (suite)

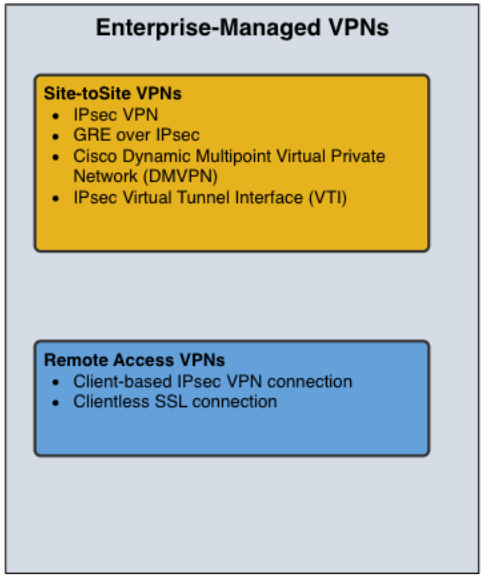
VPN d'accès à distance est créé dynamiquement lorsque cela est nécessaire pour établir une connexion sécurisée entre un client et un périphérique de terminaison VPN.

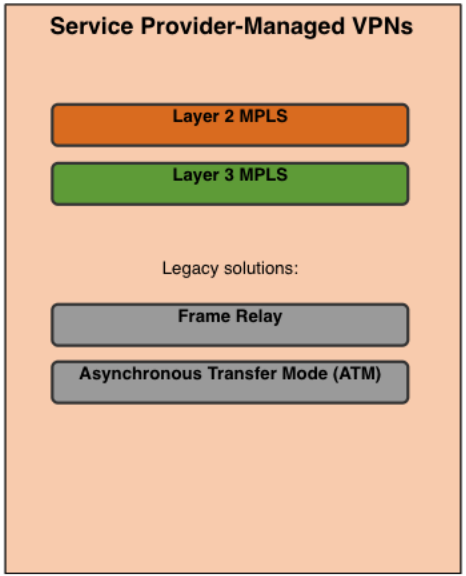


VPN d'entreprise et de prestataire de service

Les VPN peuvent être gérés et déployés comme:

- **VPN d'entreprise** - des solutions similaires pour sécuriser le trafic d'entreprise sur l'internet. Les VPN de site à site et d'accès distant sont créés et gérés par l'entreprise à l'aide de VPN IPsec et SSL.
- **VPN des prestataires de services** – sont créés et gérés sur le réseau du fournisseur. Le fournisseur utilise la commutation d'étiquette multiprotocole (MPLS) au niveau de la couche 2 ou de la couche 3 pour créer des canaux sécurisés entre les sites d'une entreprise, séparant efficacement le trafic des autres clients.

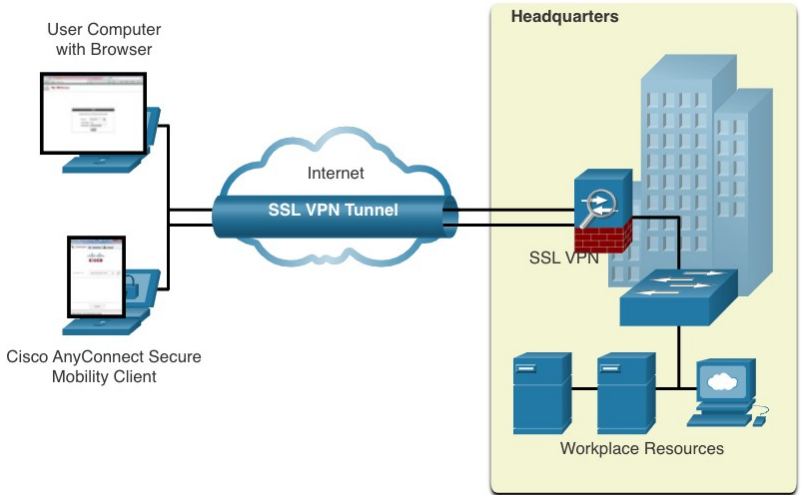




2 – Types de VPN

VPN d'accès à distance

- Les VPN d'accès à distance permettent aux utilisateurs distants et mobiles de se connecter en toute sécurité à l'entreprise.
- Les VPN d'accès à distance sont généralement activés dynamiquement par l'utilisateur lorsque cela est nécessaire et peuvent être créés à l'aide d'IPsec ou de SSL.
  - **La Connexion VPN sans client** - La connexion est sécurisée à l'aide d'une connexion SSL par navigateur Web.
  - **La Connexion VPN basée sur le client** - Le logiciel client VPN tel que Cisco AnyConnect Secure Mobility Client doit être installé sur le terminal de l'utilisateur distant.



Types de VPN

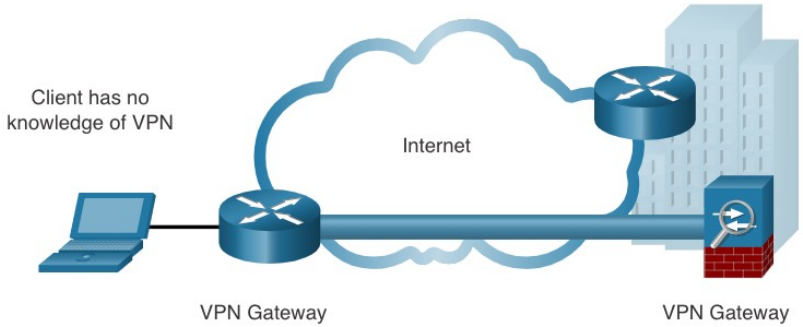
SSL VPNs

SSL utilise l'infrastructure du clé publique et les certificats numériques pour authentifier les pairs. Le type de méthode VPN mis en œuvre est basé sur les exigences d'accès des utilisateurs et les processus informatiques de l'organisation. Le tableau compare les déploiements d'accès à distance IPsec et SSL.

Fonctionnalité	IPsec	SSL
Application prise en charge	**Vaste** – Toutes les applications basées sur IP	**Limité** – Uniquement les applications Web et le partage de fichiers
Force d'authentification	**Fort** – Authentification bidirectionnelle avec clés partagées ou certificats numériques	**Modéré** - authentification unidirectionnelle ou bidirectionnelle
Force de chiffrement	**Fort** – Longueurs de clé 56-256 bits	**Modéré à fort** - Longueur des clés 40 - 256 bits
Complexité de la connexion	**Moyen** – Nécessite un client VPN installé sur un hôte	**Faible** – Nécessite un navigateur Web sur un hôte
Option de connexion	**Limité** – Seuls les appareils spécifiques avec des configurations spécifiques peuvent se connecter	**Vaste** – Tout appareil peut se connecter avec un navigateur Web

VPN IPSec site à site

- Les VPN de site à site connectent des réseaux sur un réseau non fiable tel qu'Internet.
- Les hôtes finaux envoient et reçoivent du trafic TCP / IP non chiffré normal via une passerelle VPN.
- La passerelle VPN encapsule et crypte le trafic sortant d'un site et envoie le trafic via le tunnel VPN à la passerelle VPN sur le site cible. La réception de la passerelle VPN élimine les en-têtes, déchiffre le contenu et relaie le paquet vers l'hôte cible au sein de son réseau privé.



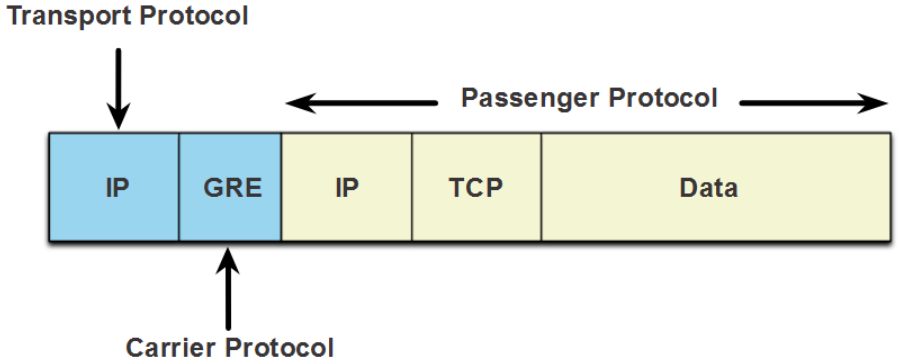
GRE sur IPsec

- Le protocole GRE (Generic Routing Encapsulation) est un protocole de tunneling VPN de site à site non sécurisé.
- Un tunnel GRE peut encapsuler divers protocoles de couche réseau ainsi que le trafic de multidiffusion et de diffusion.
- GRE ne prend pas en charge le cryptage par défaut; et par conséquent, il ne fournit pas de tunnel VPN sécurisé.
- Un paquet GRE peut être encapsulé dans un paquet IPsec pour le transmettre en toute sécurité à la passerelle VPN de destination.
  - Les VPN IPsec standard (non GRE) ne peuvent créer que des tunnels sécurisés pour le trafic unicast.
  - L'encapsulation de GRE dans IPsec permet de sécuriser les mises à jour du protocole de routage de multidiffusion via un VPN.

GRE sur IPsec (suite)

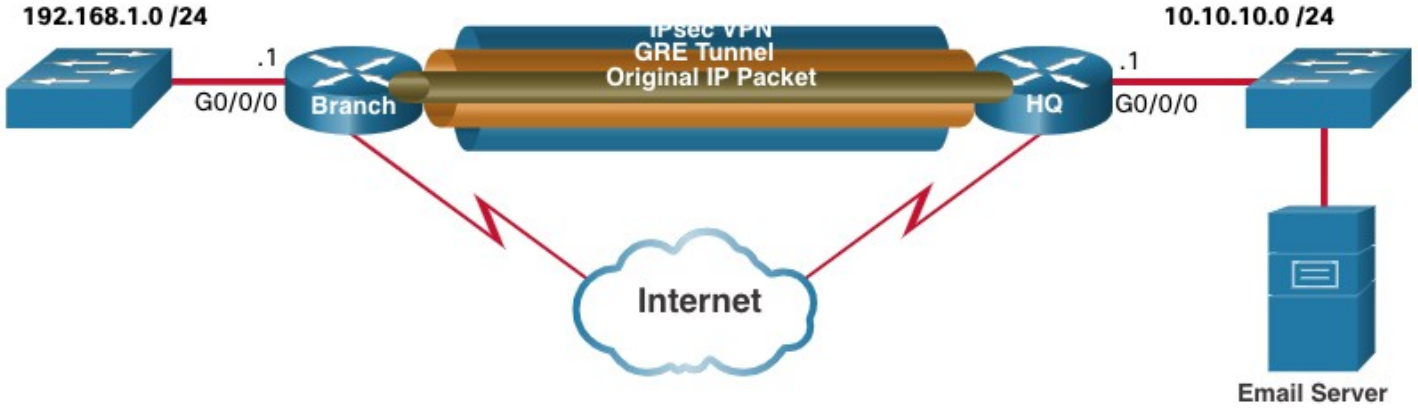
Les termes utilisés pour décrire l'encapsulation du tunnel GRE sur IPsec sont protocole de passager, protocole de transporteur et protocole de transport.

- **Protocole passager** - Il est un paquet d'origine qui doit être encapsulé par GRE. Il peut être un paquet IPv4 ou IPv6, d'une mise à jour de routage, etc.
- **Protocole de transporteur** - GRE est le protocole de transporteur qui encapsule le paquet passager d'origine.
- **Protocole de transport** - Il est un protocole qui sera réellement utilisé pour transmettre le paquet. Cela peut être IPv4 ou IPv6.



GRE sur IPsec (suite)

Par exemple, la filiale et le HQ doivent échanger des informations de routage OSPF sur un VPN IPsec. GRE sur IPsec est utilisé pour prendre en charge le trafic du protocole de routage sur le VPN IPsec. Plus précisément, les paquets OSPF (c'est-à-dire le protocole passager) seraient encapsulés par GRE (c'est-à-dire le protocole de transporteur) et ensuite encapsulés dans un tunnel VPN IPsec.



VPN multipoints dynamiques

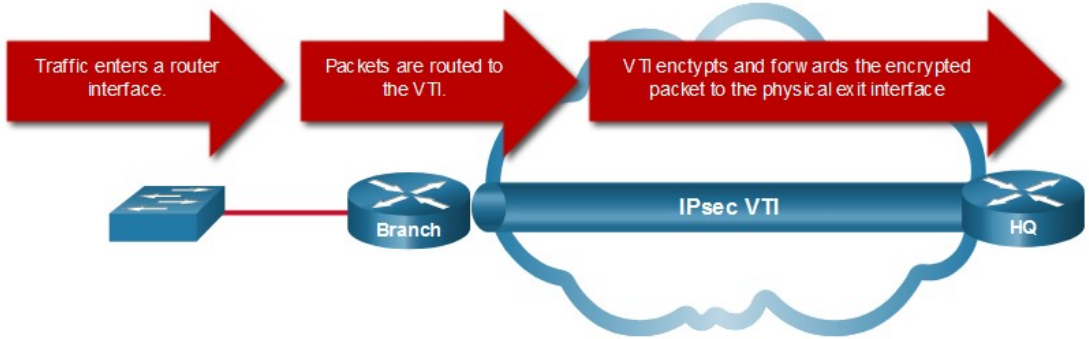
Les VPN IPsec de site à site et GRE sur IPsec ne sont pas suffisants lorsque l'entreprise ajoute de nombreux autres sites. DMVPN (Dynamic Multipoint VPN) est une solution logicielle de Cisco qui permet de créer plusieurs VPN de façon simple, dynamique et évolutive.

- DMVPN simplifie la configuration du tunnel VPN et fournit une option flexible pour connecter un site central avec les sites distant.
- Il utilise une configuration concentrateur et rayon pour établir une topologie maillée complète.
- Les sites à rayons établissent des tunnels VPN sécurisés avec le site concentrateur.
- Chaque site est configuré en utilisant Encapsulation de routage générique multipoints (mGRE). L'interface de tunnel GRE permet à une interface GRE unique de prendre en charge dynamiquement plusieurs tunnels IPsec.
- Les sites à rayons peuvent aussi obtenir des informations les uns sur les autres et construire des tunnels directs entre eux (tunnels à rayons).

L'interface de tunnel virtuel IPsec

L'interface de tunnel virtuel IPsec (VTI) simplifie le processus de configuration requis pour prendre en charge plusieurs sites et l'accès à distance.

- Les configurations IPsec VTI sont appliquées à une interface virtuelle au lieu du mappage statique des sessions IPsec à une interface physique.
- IPsec VTI est capable d'envoyer et de recevoir le trafic crypté IP unicast et multicast. Par conséquent, les protocoles de routage sont automatiquement pris en charge sans ayant configurer de tunnels GRE.
- IPsec VTI peut être configuré entre les sites ou dans une topologie en étoile (hub-to-spoke).



VPN MPLS prestataires de service

Aujourd'hui, les prestataires de services utilisent MPLS dans leur réseau principal. Le trafic est transmis via le réseau principal MPLS à l'aide d'étiquettes. Le trafic est sécurisé car les clients des fournisseurs de services ne peuvent pas voir le trafic de l'autre.

- MPLS peut fournir aux clients des solutions VPN gérées; par conséquent, la sécurisation du trafic entre les sites clients est la responsabilité du prestataire de services.
- Il existe deux types de solutions VPN MPLS prises en charge par les prestataires de services :
  - **VPN MPLS de couche 3** - Le prestataire de services participe au routage client en établissant trunking entre les routeurs du client et les routeurs du prestataire.
  - **VPN MPLS de couche 2**- Le prestataire de services n'est pas impliqué dans le routage du client. Au lieu de cela, le prestataire déploie un service LAN privé virtuel (VPLS) pour émuler un segment LAN multi-accès Ethernet sur le réseau MPLS. Aucun routage n'est impliqué. Les routeurs du client appartiennent effectivement au même réseau à accès multiple.

Mise en œuvre de GRE

- La configuration d'un tunnel GRE s'effectue en cinq étapes :
  - **Étape 1.** Créez une interface de tunnel à l'aide de la commande **interface tunnel number**.
  - **Étape 2.** Configurez une adresse IP pour l'interface du tunnel. Il s'agit normalement d'une adresse IP privée.
  - **Étape 3.** Spécifiez l'adresse IP source du tunnel.
  - **Étape 4.** Spécifiez l'adresse IP de destination du tunnel.
  - **Étape 5.** (Facultatif) Spécifiez le mode de tunnel GRE en tant que mode d'interface de tunnel.

Commande	Description
`tunnel mode gre ip`	Spécifie que le mode de l'interface du tunnel est GRE sur IP.
`tunnel source` *ip_address*	Spécifie l'adresse source du tunnel.
`tunnel destination` *ip address*	Spécifie l'adresse de destination du tunnel.
`ip address` *ip_address mask*	Spécifie l'adresse IP de l'interface du tunnel.

3 IPsec

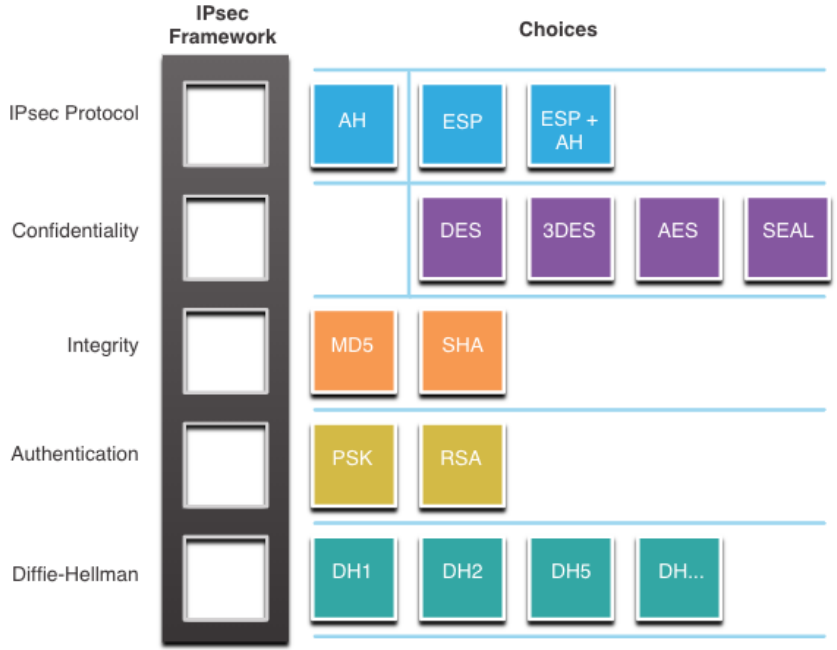
Les Technologies IPSec

IPsec est un standard IETF qui définit comment un VPN peut être sécurisé sur des réseaux IP. IPsec protège et authentifie les paquets IP entre la source et la destination et fournir les fonctions de sécurité essentiels :

- **Confidentialité** - Utilise des algorithmes de chiffrement pour empêcher les cybercriminels de lire le contenu des paquets.
- **Intégrité** - Utilise des algorithmes de hachage pour garantir que les paquets n'ont pas été modifiés entre la source et la destination.
- **Authentification d'origine** - Utilise le protocole IKE (Internet Key Exchange) pour authentifier la source et la destination.
- **Diffie-Hellman** - Utilisé pour sécuriser l'échange de clés.

Les Technologies IPSec (suite)

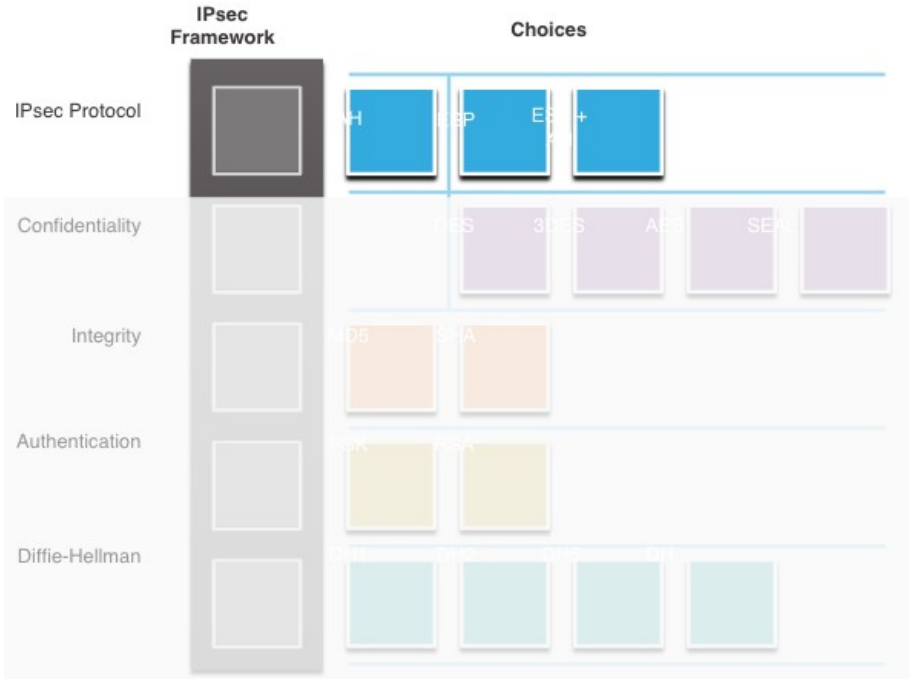
- IPsec n'est lié à aucune règle spécifique pour des communications sécurisées.
- IPsec permet d'intégrer facilement les nouvelles technologies de sécurité sans mettre à jour les standards IPsec existantes.
- Les emplacements ouverts dans la structure IPsec illustrés dans la figure peuvent être remplis avec n'importe quel choix disponibles pour cette fonction IPsec pour créer une association de sécurité (SA) unique.



Encapsulation du protocole IPsec

Le choix de l'encapsulation du protocole IPsec est le premier élément principale du structure.

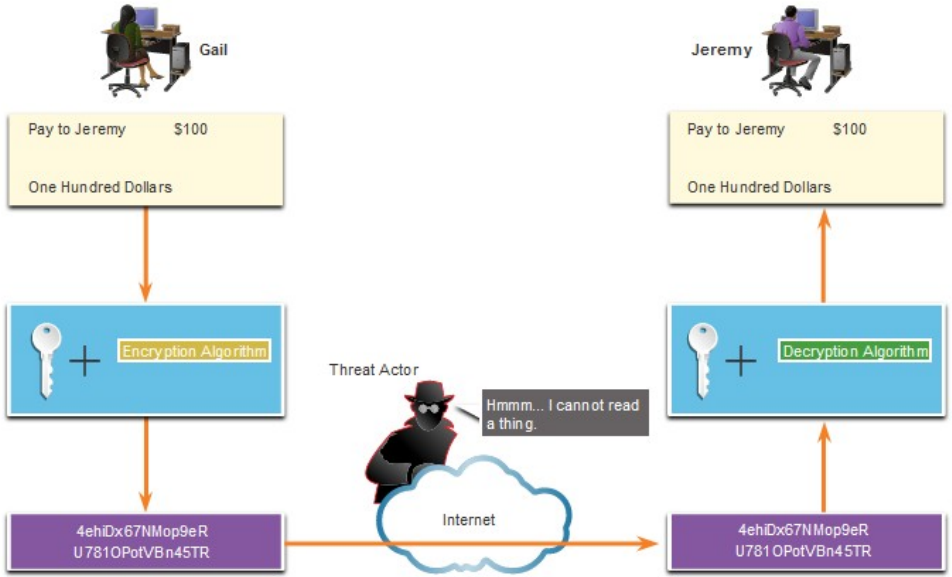
- IPsec encapsule les paquets à l'aide de l'en-tête d'authentification (AH) ou du protocole de sécurité d'encapsulation (ESP).
- Le choix de AH ou ESP détermine quels autres blocs de construction sont disponibles.
  - AH n'est approprié que lorsque la confidentialité n'est pas requise ou autorisée.
  - ESP fournit la confidentialité et l'authentification.



Confidentialité IPSec

Le degré de confidentialité dépend de l'algorithme de cryptage et de la longueur de la clé utilisée dans l'algorithme de cryptage.

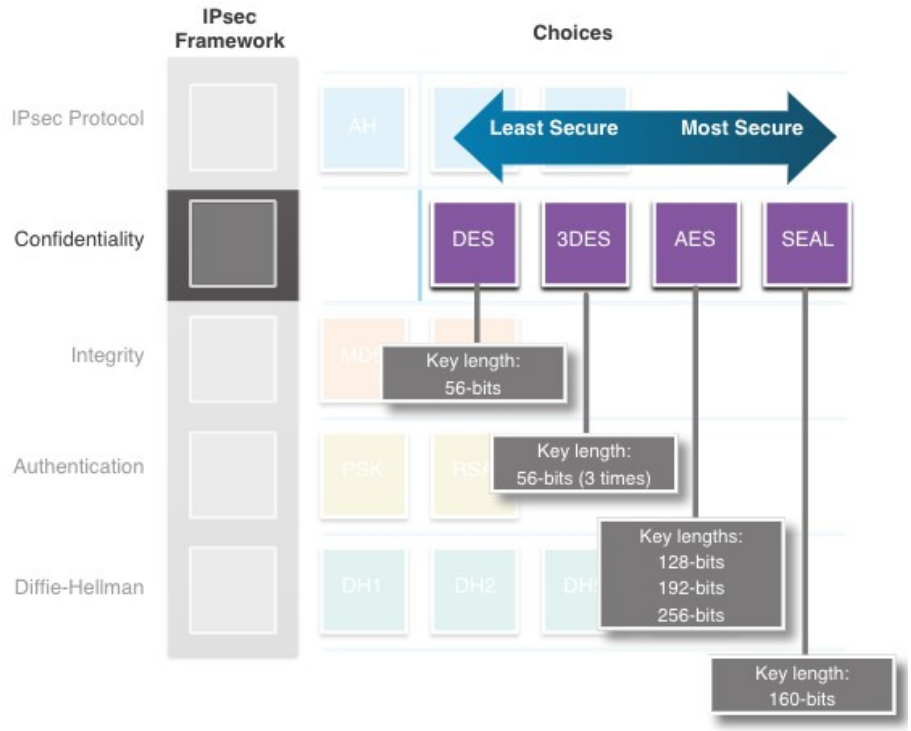
Le nombre de possibilités d'essayer de pirater la clé est fonction de la longueur de la clé - plus la clé est courte, plus il est facile de la casser.



Confidentialité IPSec (suite)

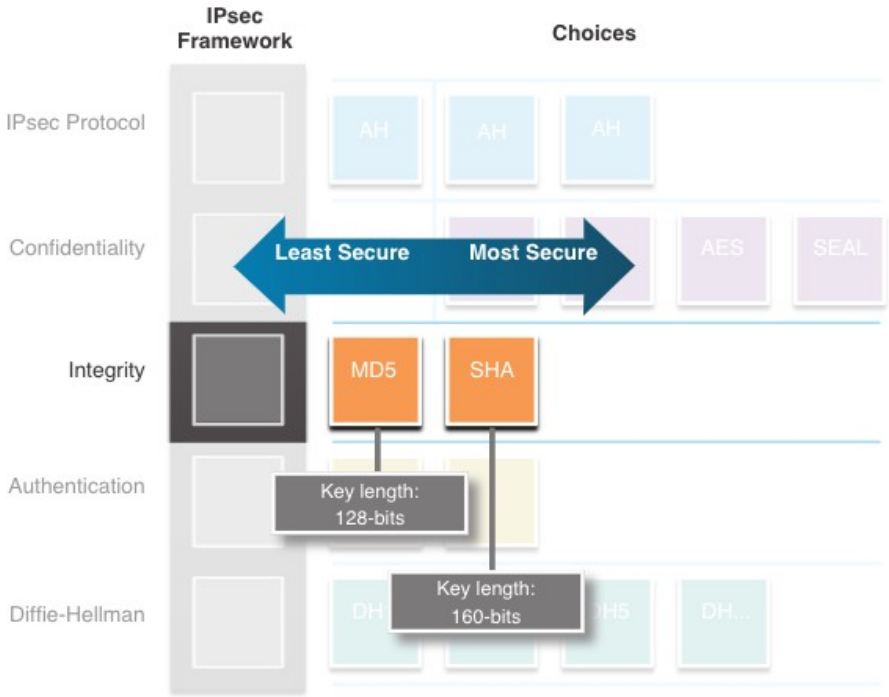
Les algorithmes de cryptage mis en évidence dans la figure sont tous des cryptosystèmes à clé symétrique:

- DES utilise une clé de 56 bits.
- 3DES utilise trois clés de chiffrement 56 bits indépendantes par bloc 64 bits.
- AES propose trois longueurs de clé différentes: 128 bits, 192 bits et 256 bits.
- SEAL est un chiffrement de flux, ce qui signifie qu'il crypte les données en continuant plutôt que de crypter des blocs de données. SEAL utilise une clé de 160 bits.



Intégrité IPSec

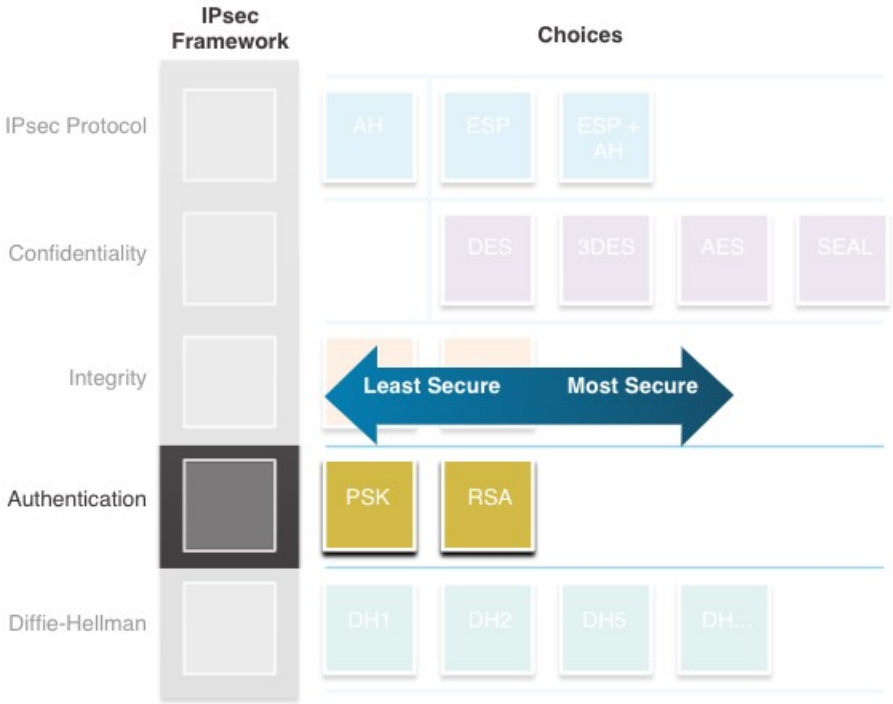
- L'intégrité des données signifie que les données n'ont pas été modifiées en transit.
- Une méthode pour prouver l'intégrité des données est requise.
- Le code d'authentification de message haché (HMAC) est un algorithme d'intégrité des données qui garantit l'intégrité du message à l'aide d'une valeur de hachage.
  - Message-Digest 5 (MD5) utilise une clé secrète partagée de 128 bits.
  - L'algorithme de hachage sécurisé (SHA) utilise une clé secrète de 160 bits.



Authentification IPsec

Il existe deux méthodes d'authentification homologue IPsec:

1. **Clé pré-partagée (PSK)** - La valeur (PSK) est entrée manuellement dans chaque homologue.
   - Facile à configurer manuellement
   - Ne s'étend pas bien
   - Doit être configuré sur chaque homologue
2. **Rivest, Shamir et Adleman (RSA)** - l'authentification utilise des certificats numériques pour authentifier les homologues.
   - Chaque homologue doit authentifier son homologue opposé avant que le tunnel soit considéré comme sécurisé.



Échange de clé sécurisé avec Diffie - Hellman

DH permet à deux pairs IPsec d'établir une clé secrète partagée sur un canal non sécurisé.

Les variations de l'échange de clés DH sont spécifiées en tant que groupes DH:

- Les groupes DH 1, 2 et 5 ne doivent plus être utilisés.
- Les groupes DH 14, 15 et 16 utilisent des tailles de clé plus grandes avec respectivement 2048 bits, 3072 bits et 4096 bits
- Les groupes DH 19, 20, 21 et 24 avec des tailles de clé respectives de 256 bits, 384 bits, 521 bits et 2048 bits prennent en charge la cryptographie à courbe elliptique (ECC), ce qui réduit le temps nécessaire pour générer des clés.


CISCO