



Présentation des technologies VPN

Licence Pro SEICOM – Module 37





SOMMAIRE

- La cryptographie
 - Terminologie
 - Algorithme de chiffrement...
 - Fonctions de hachage, signature, scellement
 - Authentification mutuelle et échange de clefs de session
 - Certificat
- La base des VPNs
- Les topologies de VPNs IPsec
- Exemples et exercices



CRYPTOGRAPHIE



Terminologie

- Définition : méthodes permettant de transmettre des données de manière confidentielle. On applique aux données une transformation qui les rend incompréhensibles :
 - Etape 1 : chiffrement qui donne un texte chiffré ou cryptogramme
 - Etape 2 : déchiffrement

Les transformations : des fonctions mathématiques appelés algorithmes cryptographiques dépendant d'un paramètre appelé clef.



Terminologie

- But :
 - Confidentialité
 - Intégrité
 - Authentification de l'origine des données ou d'un tiers
 - Non-répudiation
 - ...
- Moyens
 - Chiffrement
 - Scellement et signature
 - Protocoles d'authentification mutuelle avec échange de clefs
 - ...



Algorithme de chiffrement

- On utilise 2 types algorithmes cryptographiques.
L'algorithme est en général public, et le secret du chiffre dépend d'un paramètre appelé clé.
 - Algorithmes symétriques ou à clé privé
 - Algorithmes asymétriques ou à clef publique
 - Echange de clefs publiques
 - Signature



Algorithme de chiffrement symétrique ou à clé privée

- Clef de chiffrement = clé de déchiffrement, elle doit rester secrète.

Texte
en clair

Texte
chiffré

Texte
en clair

Bertrand

Clé secrète

Matthieu



Algorithme de chiffrement asymétrique ou à clef publique

- Clefs de chiffrement et de déchiffrement distinctes
 - Connaître la clé publique ne permet pas de retrouver la clé privée correspondante
 - Algorithmes lents pour une utilisation intensive (chiffrements des données), souvent utilisés pour l'échange de clef, la signature.



Algorithme de chiffrement asymétrique ou à clef publique

● Chiffrement

- Clé publique utilisée pour le chiffrement, seul le détenteur de la clé privée peut déchiffrer.

Bertrand

Texte
en clair

Texte
chiffré

Texte
en clair

Clé publique
Matthieu

Clé privée
Matthieu

Matthieu

● Signature

- Clé privée utilisée pour le chiffrement, seul le son détenteur peut chiffrer, mais tout le monde peut déchiffrer (et donc vérifier la signature).

Bertrand

Texte
en clair

Texte
chiffré

Texte
en clair

Clé privée
Bertrand

Clé publique
Bertrand

Matthieu



Fonctions de hachage, signature, scellement

- Hachage, Signature, Scellement : mécanisme fournissant les services d'intégrité, d'authentification de l'origine des données et la non-répudiation de la source.
 - Hachage : fonction qui permet de convertir une donnée quelconque en une chaîne de taille inférieure et fixe = empreinte numérique d'un fichier (SHA ou MD5).



Fonctions de hachage, signature, scellement

- Signature Message

Bertrand

Clé privée
Bertrand

Message

- Vérification

Identiques ?

Matthieu

Clé publique
Bertrand



Fonctions de hachage, signature, scellement

- Scellement

(le sceau confirme la véracité
de la signature)

Message

Bertrand

Clé secrète

Message Clé secrète

- Vérification

Identiques ?

Matthieu



Authentification mutuelle et échange de clefs de session

- L'échange de clefs doit être authentifié pour éviter les attaques.
- Une clef de session permet d'étendre l'authentification à l'ensemble de la communication
- Protocole d'authentification mutuelle avec échange de clefs
 - Fournit authentification mutuelle et un échange de clefs authentifié tout-en-un
- Types d'échange de clefs
 - Transport (ex : RSA)
 - Génération (ex : Diffie Hellman)



Authentification mutuelle et échange de clefs de session

Transport
de clef

Matthieu

Choisit la def de session

La chiffre avec la def
publique de Bertrand

Transmission de la
def chiffrée à
Bertrand

Cleé privée de
Bertrand

Bertrand récupère la def
de session grâce à sa def
privée

Bertrand



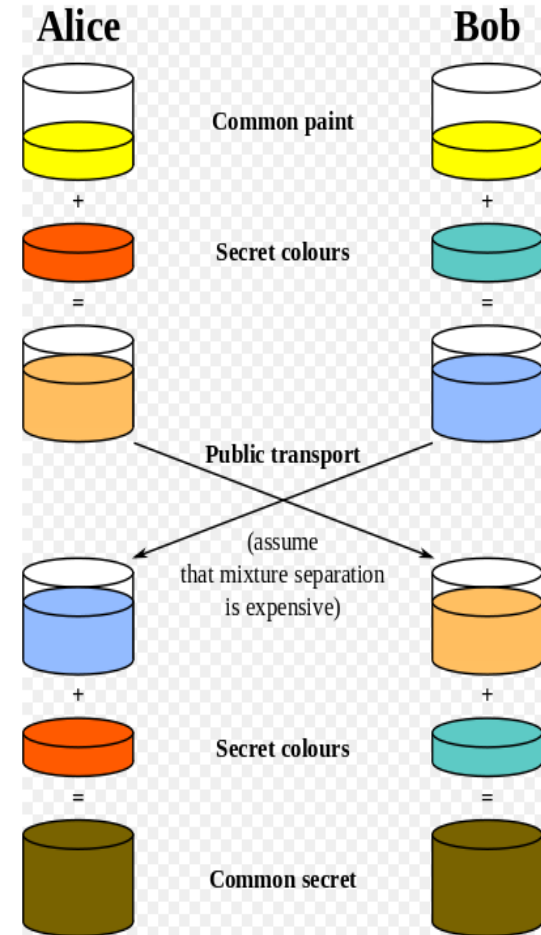
Authentification mutuelle et échange de clefs de session

- Génération de clef
 - DH permet à deux tiers de générer un secret partagé sans informations préalables l'un sur l'autre
 - 1. Matthieu génère une valeur publique à partir d'une valeur privée.
 - 2. Bertrand fait de même.
 - 3. Ils s'échangent leurs valeurs publiques mutuellement.
 - 4. Un secret partagé est généré à partir de ces échanges
 - Un espion ne peut reconstituer le secret partagé à partir des valeurs publiques

Authentification mutuelle et échange de clefs de session

Exemple :

- Alice et Bob choisissent un nombre premier p et une base g . Dans notre exemple, $p=23$ et $g=3$
- Alice choisit un nombre secret $a=6$
- Elle envoie à Bob la valeur $A = g^a \pmod{p} = 3^6 \pmod{23} = 16$
- Bob choisit à son tour un nombre secret $b=15$
- Bob envoie à Alice la valeur $B = g^b \pmod{p} = 3^{15} \pmod{23} = 12$
- Comme $(A)^b \pmod{p} = (B)^a \pmod{p}$, Alice peut maintenant calculer la clé secrète : $(B)^a \pmod{p} = 12^6 \pmod{23} = 9$
- Bob fait de même et obtient la même clé qu'Alice : $(A)^b \pmod{p} = 16^{15} \pmod{23} = 9$



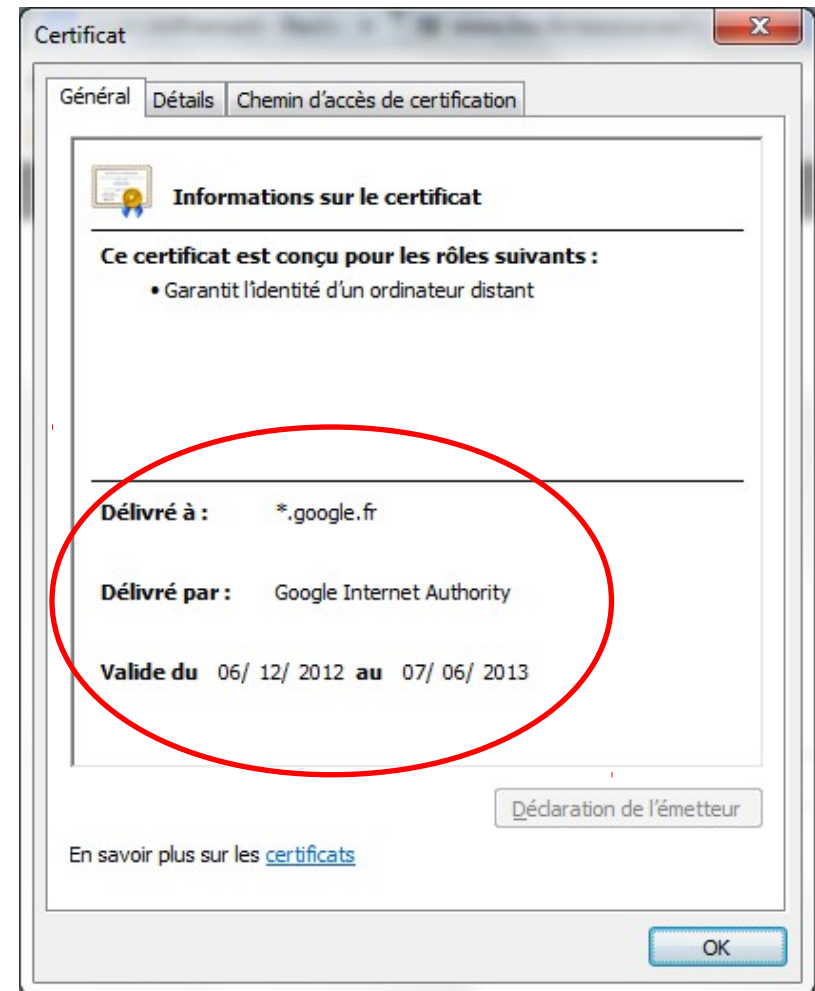


Certificats

- Certificat = structure de données
 - Permet de lier une clef publique à différents éléments au moyen de la signature d'une autorité de confiance :
 - Propriétaire
 - Date de validité
 - Type d'utilisation
 - Emis par une autorité de certification (CA)
 - Garantit l'exactitude des données
 - Listes de révocation (CRL) permettant de révoquer un certificat avec l'expiration.

Certificats

- Exemples d'utilisation :
 - Sites internet (SSL/TLS)
 - Messagerie
 - VPN Ipsec
 - Documents électroniques
 - Etc.





LA BASE DES VPNS



La problématique

- Réseaux ont été créés pour partager librement des informations
- Nativement les réseaux permettent de transférer tout type de données rapidement mais de façon non sécurisée
- Les réseaux ATM, ISDN, MPLS offrent des solutions fiables et sécurisés mais coûteuses et dépendantes de fournisseurs de services qui ne garantissent pas la sécurité des données.
- Les liaisons Point-To-Point peuvent être interceptées. Par exemple, les lignes téléphoniques sont raccordés au commutateur d'un opérateur dont les locaux ne sont pas toujours sécurisés.



Définition

- VPN (Virtual Private Network) : canal virtuel et privé (RPV) de communication entre réseaux ou équipements à travers un réseau tiers ou publique tel qu'Internet
- Les réseaux privés virtuels ou VPN se définissent comme des réseaux physiquement ou logiquement séparés que l'on interconnecte par des liens de communication virtuels. Le terme virtuel est employé car le lien n'existe pas en tant que tel (physique).
- Réseau le plus souvent utilisé : Internet => Faible coût
- Le chiffrement de l'information offre une totale sécurité des communications.
- Objectif de communication et ouverture du Système d'Information



Définition

- Utilisation d'un protocole de tunneling : circulation des informations de façon cryptée d'un bout à l'autre du tunnel.
 - Exemple : encapsuler un flux P2P dans une connexion TCP/IP (https)
- Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.
- Un tunnel IP s'effectue entre 2 machines, qui jouent le rôle de passerelles pour les autres machines de leur réseau respectif.
- Le tunneling peut rendre des services de différents ordres :
 - chiffrement et déchiffrement des données transmises.
 - compression et décompression des données envoyées dans le tunnel.
 - offrir l'impression à l'utilisateur de travailler en réseau local
 - la protection face
 - Aux pertes, destructions et expositions de données (confidentielles ou non)
 - Aux attaques, à l'espionnage

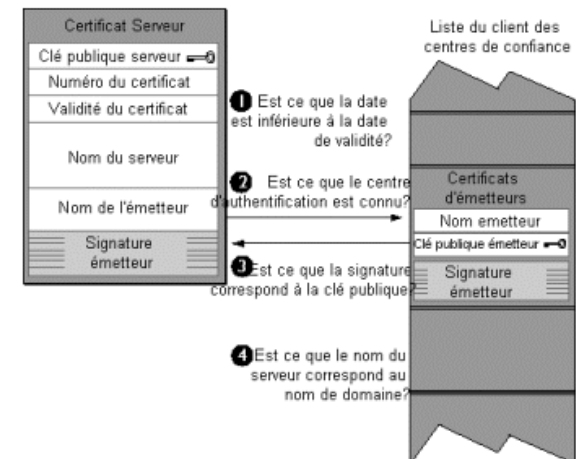


Définition

- Un serveur VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :
 - Authentification d'utilisateur
 - Gestion d'adresses privées
 - Cryptage des données
 - Gestion de clés de chiffrement
 - Confidentialité de l'information

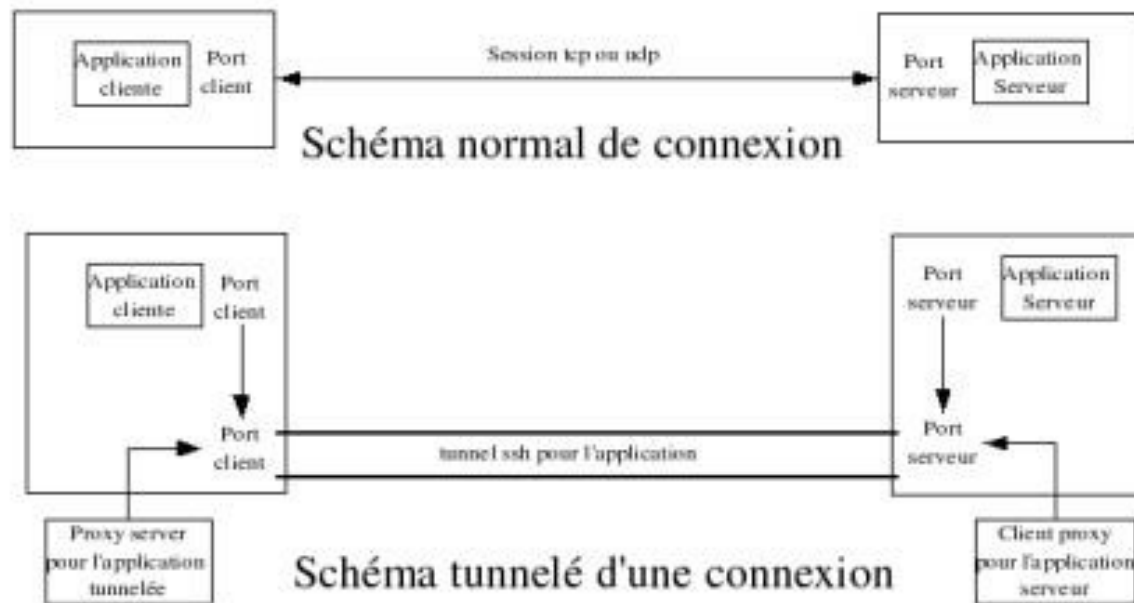
Protocoles de tunnelisation couramment utilisés

- Secure Sockets Layer / Transport Layer Security (SSL/TLS) : permet de sécuriser des connexions via un certificat.
 - Se situe entre la couche application et transport
 - Garantie l'authentification, l'intégrité et la confidentialité
 - Largement utilisé pour la sécurisation des sites www (https)
 - Mais également pour du chiffrement :
 - des processus d'authentification (LDAPs)
 - des courriels (SMTPs)
 - du transfert de données (sFTP)



Protocoles de tunnelisation couramment utilisés

- Secure Shell (SSH) est une application utilisée pour se connecter à un équipement au travers d'un réseau et d'y exécuter des commandes. Elle assure une authentification forte et sécurise les communications.





Protocoles de tunnelisation couramment utilisés

- Internet Protocol SECurity (IPSec) intègre des protocoles de cryptage, d'authentification et de gestion des clés. Développés par l'IETF (Internet Engineering Task Force).
 - Spécifications
 - Authentification, confidentialité et intégrité (protection contre l'usurpation d'IP ou de session tcp)
 - Confidentialité (session chiffrée pour se protéger du sniffing)
 - Sécurisation au niveau de la couche transport (protection L3)
 - Algorithmes utilisés
 - Authentification par signature DSA ou RSA
 - Intégrité par fonction de condensation (HMAC-MD5 ou HMAC-SHA1)
 - Confidentialité par chiffrement DES, AES, etc/
 - Ipsec utilise 2 protocoles pour implémenter la sécurité sur un réseau IP :
 - Entête d'authentification (AH) permet d'assurer l'authentification des messages
 - Protocole de sécurité encapsulant (ESP) permettant d'authentifier et de crypter les messages



Protocoles de tunnelisation couramment utilisés

- Ipsec (suite)
 - Les VPN Ipsec peuvent être utilisés pour différents types d'accès :
 - Personnel nomade (télétravailleurs, nomades, expatriés)
 - Des sites distants
 - Des partenaires (fournisseurs, clients, prestataires)
 - Afin d'établir un tunnel, les 2 équipements doivent s'accorder sur les algorithmes et les protocoles.
 - Utilisation d'une SA (Security Association)
 - Une SA comprend :
 - Un algorithme de chiffrement (DES, 3DES, AES-256)
 - Une clé de session via IKE
 - Un algorithme d'authentification (SHA1-MD5)



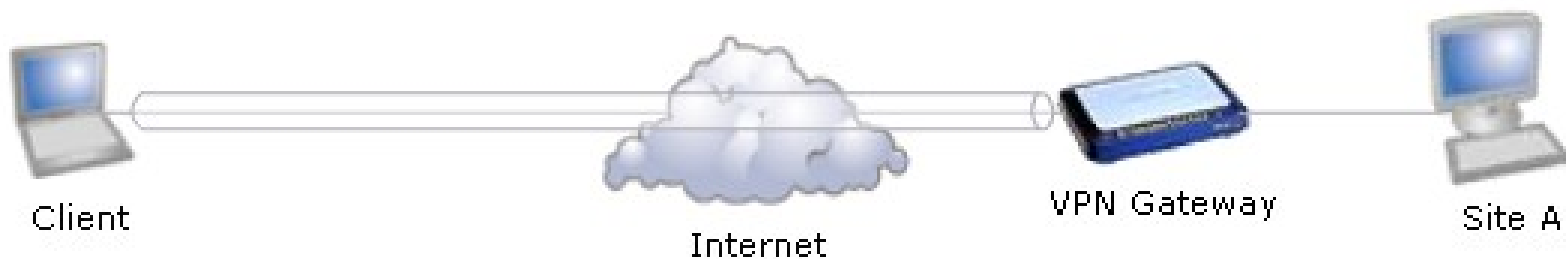
TOPOLOGIE DES VPNS IPSEC

Topologie des VPNs IPsec

- Site-To-Site

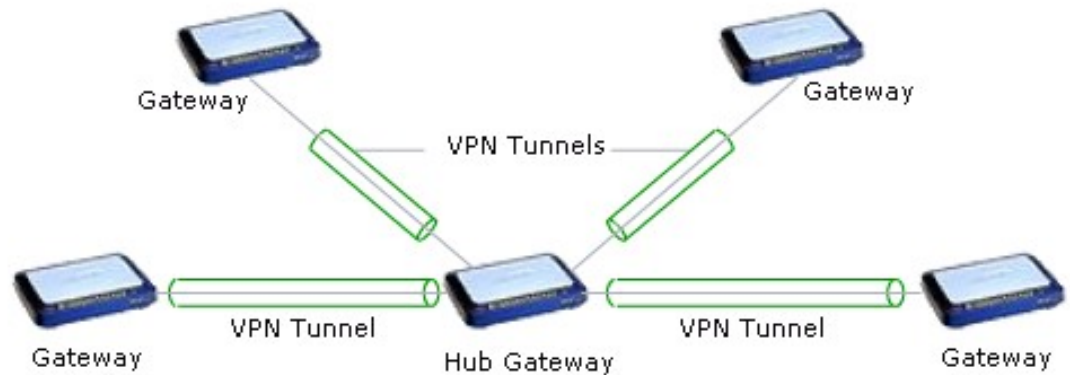


- Client-To-Site

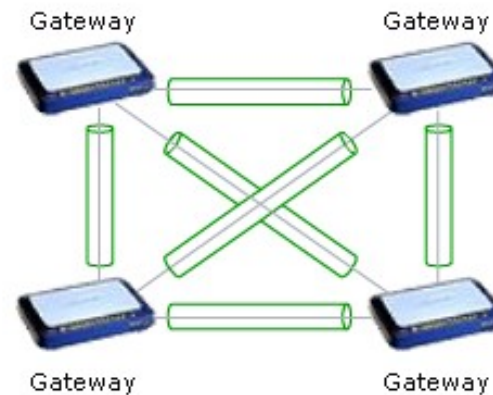


Topologie des VPNs IPsec

- Hub and Spoke (Transport / Expédition)



- Mesh (Maillé)



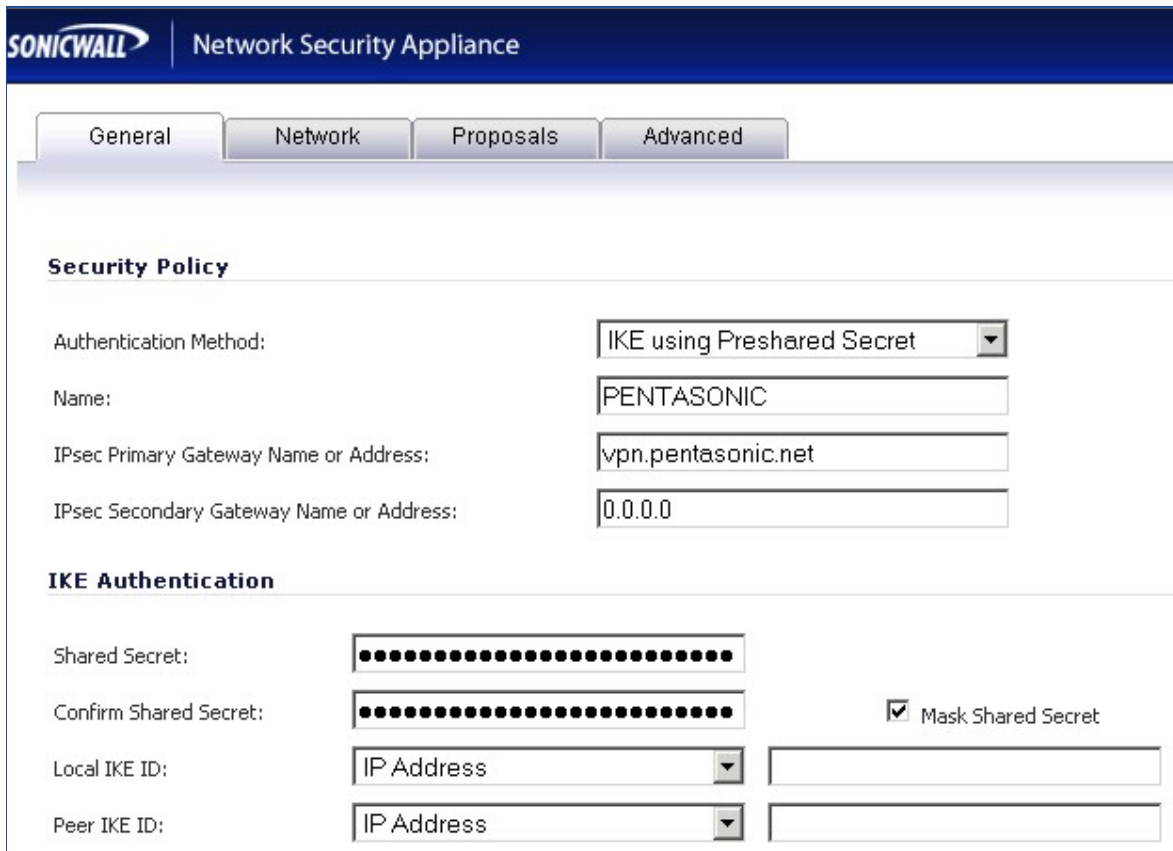


Exemples et exercices



VPN Site-To-Site

- Exemple de mise en œuvre (Dell Sonicwall)



SONICWALL | Network Security Appliance

General | Network | Proposals | Advanced

Security Policy

Authentication Method: IKE using Preshared Secret

Name: PENTASONIC

IPsec Primary Gateway Name or Address: vpn.pentasonic.net

IPsec Secondary Gateway Name or Address: 0.0.0.0

IKE Authentication

Shared Secret: [Masked]

Confirm Shared Secret: [Masked] ☒ Mask Shared Secret

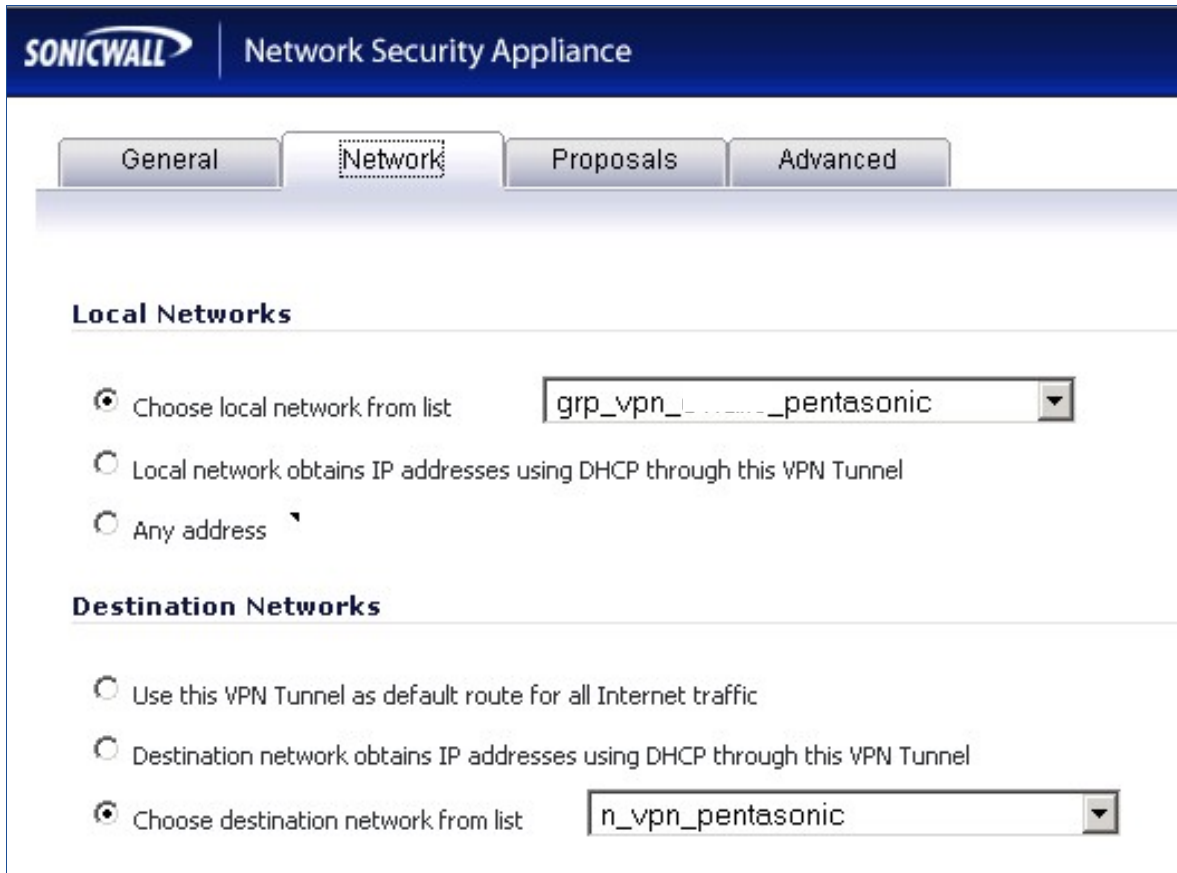
Local IKE ID: IP Address []

Peer IKE ID: IP Address []



VPN Site-To-Site

- Exemple de mise en œuvre (Dell Sonicwall)



SONICWALL | Network Security Appliance

General **Network** Proposals Advanced

Local Networks

☒ Choose local network from list grp_vpn_.....pentasonic

☐ Local network obtains IP addresses using DHCP through this VPN Tunnel

☐ Any address

Destination Networks

☐ Use this VPN Tunnel as default route for all Internet traffic

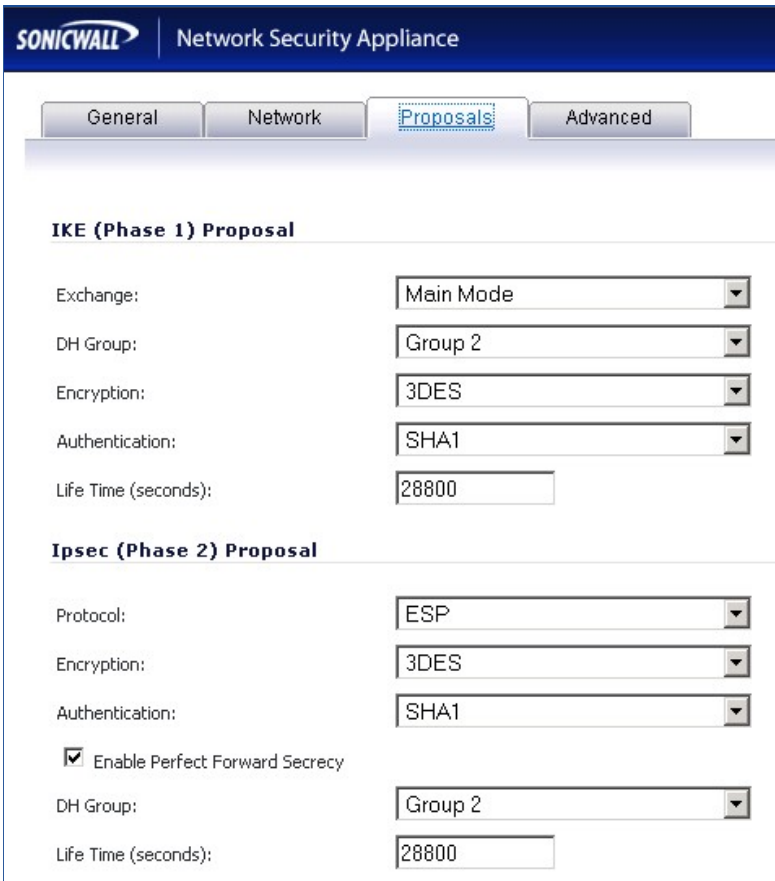
☐ Destination network obtains IP addresses using DHCP through this VPN Tunnel

☒ Choose destination network from list n_vpn_pentasonic



VPN Site-To-Site

- Exemple de mise en œuvre (Dell Sonicwall)



SONICWALL | Network Security Appliance

General | Network | **Proposals** | Advanced

IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☒ Enable Perfect Forward Secrecy

DH Group: Group 2

Life Time (seconds): 28800



VPN Site-To-Site

- Exemple de mise en œuvre (Dell Sonicwall)

<input type="checkbox"/>	#	Priority ▼	Source	Destination	Service	Action
<input type="checkbox"/>	1	1 ↑↓	Any	All XO Management IP	SSH Management	Allow
<input type="checkbox"/>	2	2 ↑↓	Any	All XO Management IP	HTTPS Management	Allow
<input type="checkbox"/>	3	3 ↑↓	Any	All XO Management IP	HTTP Management	Allow
<input type="checkbox"/>	4	4 ↑↓	Any	All XO Management IP	SNMP	Allow
<input type="checkbox"/>	5	5 ↑↓	Any	All XO Management IP	Ping	Allow
<input type="checkbox"/>	7	7	n_vpn_pentasonic	grp_vpn_ _pentasonic	Any	Allow



VPN Client-To-Site (Exemple Dell Sonicwall)

General Proposals Advanced Client

Security Policy

Authentication Method:

Name:

Shared Secret:

General Proposals Advanced Client

IKE (Phase 1) Proposal

DH Group:

Encryption:

Authentication:

Life Time (seconds):

Ipssec (Phase 2) Proposal

Protocol:

Encryption:

Authentication:

☐ Enable Perfect Forward Secrecy

DH Group:

Life Time (seconds):

General Proposals Advanced Client

Advanced Settings

☒ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

Management via this SA: ☐ HTTP ☐ HTTPS ☐ SSH

Default Gateway:

Client Authentication

☒ Require Authentication of VPN Clients via XAUTH

User Group for XAUTH users:

Allow Unauthenticated VPN Client Access:

General Proposals Advanced Client

User Name and Password Caching

Cache XAUTH User Name and Password on Client:

Client Connections

Virtual Adapter settings:

Allow Connections to:

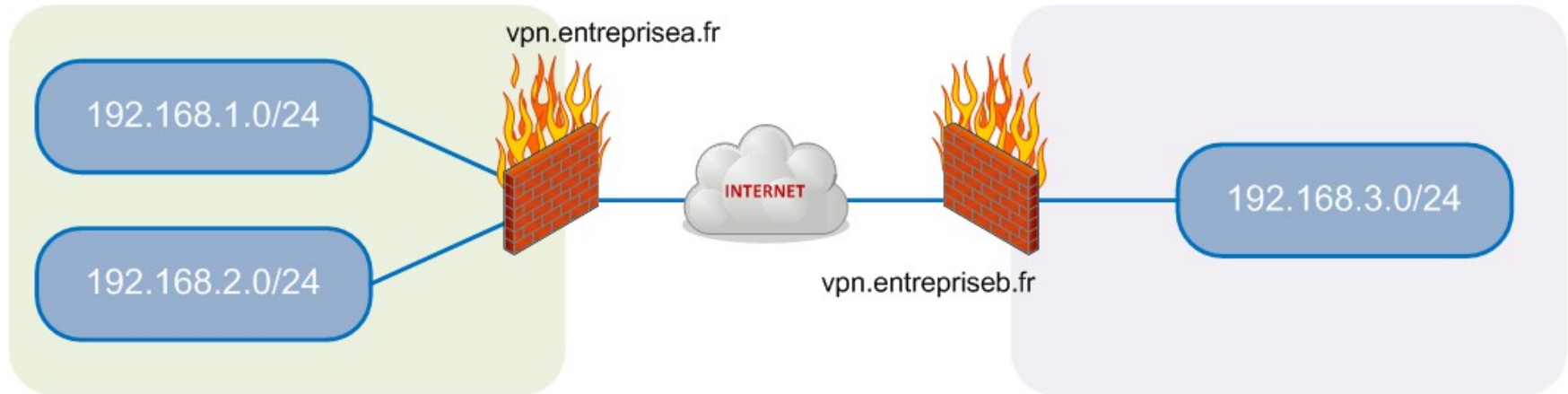
☒ Set Default Route as this Gateway

☐ Apply VPN Access Control List

Client Initial Provisioning

☐ Use Default Key for Simple Client Provisioning

Exercice



- Entreprise A :
 - Passerelle d'extrémité du tunnel VPN :
 - Domaine d'encryption distant :
- Entreprise B :
 - Passerelle d'extrémité du tunnel VPN :
 - Domaine d'encryption distant :



Exercice

- Règles de filtrage

- Entreprise A :

Source	Destination	Port source	Port destination	Action	Commentaire
*	*	*	*	DENY	Bloque tout

Source	Destination	Port source	Port destination	Action	Commentaire
*	*	*	*	DENY	Bloque tout