

## Lab8 – VPN IPsec (Site à site)

- Je copie la politique de filtrage/NAT (7) Lab\_7 vers la politique numéro 8. Je renomme la politique numéro 8 « Lab\_8 », puis j'active cette politique :

### ✚ POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(8) Lab\_8 | Editer | Exporter | i

FILTRAGE NAT

Rechercher... | + Nouvelle règle | X Supprimer | ↑ ↓ ↶ ↷ | Couper | Copier | Coller | ☰

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Comment...
FW Administration from Admin PC (contient 1 règles, de 1 à 1)								
1	on	passer	pc_adm	Firewall.	https		IPS	Créée le 2...
Internal traffic IN to DMZ (contient 6 règles, de 2 à 7)								
2	on	passer	Network	srv_dns.	dns		IPS	Créée le 2...
3	on	passer	Network	srv_web	http		IPS	Créée le 2...
4	on	passer	Network	srv_web	webmail		IPS	Créée le 2...
5	on	bloquer	pc_200	Any	ftp		IPS	Créée le 2...
6	on	passer	Network	srv_ftp_	ftp		IPS	Créée le 2...
7	on	passer	Network	srv_mail	smtp		IPS	Créée le 2...
Outgoing traffic (contient 12 règles, de 8 à 19)								
8	on	bloquer	Network	Internet geo Cor	http https		IPS	Créée le 2...
9	on	bloquer	Network	www.cni	http https		IPS	Créée le 2...
10	on	passer	jsmith @	Any	Any	icmp (requête Ech	IPS	Créée le 2...

Portail d'auth... ●? unknown

Page 1 sur 1 | Page courante 1 - 29 sur 29

### VALIDATEUR DE CONFIGURATION (1 i)

[Règle 1] Cette règle peut être couverte par une règle implicite et n'être jamais appliquée.

- J'ajoute une règle de filtrage Pass any any any en tête de cette politique :

### ✚ POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(8) Lab\_8 | Editer | Exporter | i

FILTRAGE NAT

Rechercher... | + Nouvelle règle | X Supprimer | ↑ ↓ ↶ ↷ | Couper | Copier | Coller | ☰

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Comment...
1	on	passer	Any	Any	Any		IPS	Créée le 2...
FW Administration from Admin PC (contient 1 règles, de 2 à 2)								
2	on	passer	pc_adm	Firewall.	https		IPS	Créée le 2...
Internal traffic IN to DMZ (contient 6 règles, de 3 à 8)								

- Je configure un tunnel IPsec avec une authentification par PSK pour relier mon réseau interne « 192.168.x.0/24 » à celui de l'autre entreprise en utilisant les profils de chiffrement par défaut (StrongEncryption) :

## CRÉER UNE PASSERELLE DISTANTE

### SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT



Passerelle distante:

Fw\_A

Nom:

Site\_Fw\_A

Version IKE:

IKEv2

✘ ANNULER

◀ PRÉCÉDENT

▶ SUIVANT

## CRÉER UNE PASSERELLE DISTANTE

### SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT



Passerelle distante:

Fw\_B

Nom:

Site\_Fw\_B

Version IKE:

IKEv2

✘ ANNULER

◀ PRÉCÉDENT

▶ SUIVANT

## CRÉER UNE PASSERELLE DISTANTE

### IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT

Type d'authentification:  Certificat  
 Clé pré-partagée (PSK)

Certificat:

Autorité de confiance:

Clé pré-partagée (PSK):

Confirmer:

Saisir la clé en caractères ASCII:

## CRÉER UNE PASSERELLE DISTANTE

### IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT

Type d'authentification:  Certificat  
 Clé pré-partagée (PSK)

Certificat:

Autorité de confiance:

Clé pré-partagée (PSK):

Confirmer:

Saisir la clé en caractères ASCII:



Ressources locales:

Network\_in

Choix du correspondant:

Site\_Fw\_B

Réseaux distants:

Lan\_in\_B

✗ ANNULER

✓ TERMINER



Ressources locales:

Network\_in

Choix du correspondant:

Site\_Fw\_A

Réseaux distants:

Lan\_in\_A

✗ ANNULER

✓ TERMINER

POLITIQUE DE CHIFFREMENT - TUNNELS    CORRESPONDANTS    IDENTIFICATION    PROFILS DE CHIFFREMENT

IPsec 01 (01)    Actions    Deactivate policy

SITE À SITE (GATEWAY-GATEWAY)    MOBILE - UTILISATEURS NOMADES

Entrer un filtre...    Ajouter    Supprimer    Monter    Descendre    Couper    Copier    Coller    Afficher les

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	Network_in	Site_Fw_B	Lan_in_B	StrongEncryption		Originally created...

POLITIQUE DE CHIFFREMENT - TUNNELS    CORRESPONDANTS    IDENTIFICATION    PROFILS DE CHIFFREMENT

IPsec 01 (01)    Actions    Deactivate policy

SITE À SITE (GATEWAY-GATEWAY)    MOBILE - UTILISATEURS NOMADES

Entrer un filtre...    Ajouter    Supprimer    Monter    Descendre    Couper    Copier    Coller    Afficher les

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	off	Network_in	Site_Fw_A	Lan_in_A	StrongEncryption		Originally created...

- Je génère du trafic correspondant aux extrémités de trafic et je suis les étapes de négociation des tunnels et l'activité dans les tunnels depuis les journaux et le menu de supervision correspondants :

MONITORING    CONFIGURATION    EVA1    VMSNSX09K0639A9

LOG / VPN

Dernière heure    Actualiser    Rechercher...    Recherche avancée

RECHERCHE DU - 02/10/2025 12:51:56 - AU - 02/10/2025 13:51:56

Enregistré à	Message	Utilisateur	Nom de la source	Réseau local	Nom de destination	Réseau distant
02/10/2025 13:50:05	IPSEC SA established		Firewall_out	192.168.1.0/24	Fw_B	192.168.2.0/24
02/10/2025 13:50:05	IKE SA established		Firewall_out		Fw_B	

```

02/10/2025 13:39:58 Charon daemon started
02/10/2025 13:39:58 Charon configuration reloaded
02/10/2025 13:39:58 Reloading charon configuration

```

```

user@client-training: ~
user@client-training: ~ 80x24
user@client-training:~$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=4.22 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=3.18 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=64 time=2.67 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=64 time=3.29 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=64 time=3.18 ms
64 bytes from 192.168.2.2: icmp_seq=6 ttl=64 time=2.12 ms
64 bytes from 192.168.2.2: icmp_seq=7 ttl=64 time=2.66 ms
64 bytes from 192.168.2.2: icmp_seq=8 ttl=64 time=3.70 ms
64 bytes from 192.168.2.2: icmp_seq=9 ttl=64 time=3.68 ms
64 bytes from 192.168.2.2: icmp_seq=10 ttl=64 time=2.67 ms
64 bytes from 192.168.2.2: icmp_seq=11 ttl=64 time=3.17 ms
64 bytes from 192.168.2.2: icmp_seq=12 ttl=64 time=2.68 ms
64 bytes from 192.168.2.2: icmp_seq=13 ttl=64 time=3.44 ms
64 bytes from 192.168.2.2: icmp_seq=14 ttl=64 time=3.68 ms

```

- Je modifie mes politiques IPsec pour relier cette fois mes deux réseaux Internes (IN + DM)) aux réseaux internes N + DM)) de l'autre entreprise. J'active la fonction keep-alive sur mon tunnel. Et je regarde le nombre de tunnels négociés dans la supervision :

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau**
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP
- Port
- Groupe de ports

Nom de l'objet:

Adresses IPv4

Adresse IP de réseau:

*Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0*

Commentaire:

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau**
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP
- Port

Nom de l'objet:

Adresses IPv4

Adresse IP de réseau:

*Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0*

Commentaire:

VPN / VPN IPSEC

- POLITIQUE DE CHIFFREMENT - TUNNELS**
- CORRESPONDANTS
- IDENTIFICATION
- PROFILS DE CHIFFREMENT

IPsec 01 (01) Deactivate policy

- SITE À SITE (GATEWAY-GATEWAY)**
- MOBILE - UTILISATEURS NOMADES

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	Network_in	Site_Fw_B	Lan_in_B	StrongEncryption		Originally created...
2	on	Network_in	Site_Fw_B	DMZ_In_B	StrongEncryption		Originally created...
3	on	Network_dmz1	Site_Fw_B	Lan_in_B	StrongEncryption		Originally created...
4	on	Network_dmz1	Site_Fw_B	DMZ_In_B	StrongEncryption		Originally created...

IPsec 01 (01) Actions Deactivate policy

SITE À SITE (GATEWAY-GATEWAY) MOBILE - UTILISATEURS NOMADES

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	Network_in	Site_Fw_A	Lan_in_A	StrongEncryption		Originally created...
2	on	Network_in	Site_Fw_A	DMZ_In_A	StrongEncryption		Originally created...
3	on	Network_dmz1	Site_Fw_A	Lan_in_A	StrongEncryption		Originally created...
4	on	Network_dmz1	Site_Fw_A	DMZ_In_A	StrongEncryption		Originally created...

J'active le keep-alive :

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	Network_in	Site_Fw_B	Lan_in_B	StrongEncryption	30	Originally created...
2	on	Network_in	Site_Fw_B	DMZ_In_B	StrongEncryption	30	Originally created...
3	on	Network_dmz1	Site_Fw_B	Lan_in_B	StrongEncryption	30	Originally created...
4	on	Network_dmz1	Site_Fw_B	DMZ_In_B	StrongEncryption	30	Originally created...

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	Network_in	Site_Fw_A	Lan_in_A	StrongEncryption	30	Originally created...
2	on	Network_in	Site_Fw_A	DMZ_In_A	StrongEncryption	30	Originally created...
3	on	Network_dmz1	Site_Fw_A	Lan_in_A	StrongEncryption	30	Originally created...
4	on	Network_dmz1	Site_Fw_A	DMZ_In_A	StrongEncryption	30	Originally created...

N'ayant pas fonction j'ai tout fusionné en une seule politique (ne pas faire attention au profil de chiffrement c'est le screen de la question 7, car je n'ai pas le screen original de la politique) :

SITE À SITE (GATEWAY-GATEWAY) MOBILE - UTILISATEURS NOMADES

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	GRP_NET_IN_DM	Site_Fw_A	GRP_NET_IN_DM perso		30	Originally created...

Je regarde les tunnels négociés :

MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

POLITIQUES

Type	État	Extrémité de trafic locale	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic distante
Type : Tunnels site à site (4)							
	OK	Network_in	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	Lan_in_B
	OK	Network_in	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	DMZ_in_B
	OK	Network_dmz1	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	Lan_in_B
	OK	Network_dmz1	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	DMZ_in_B
Type : Politiques d'exception (bypass) (1)							
Bypass		rfc5735_loopback	localhost		localhost		any

- Je désactive la règle de filtrage Pass any any any et j'ajoute les règles autorisant les réseaux du site distant à joindre à pinguer vos réseaux locaux et à joindre vos serveurs FTP et WEB (je le fais sur les deux firewalls) :

Inoming traffic from IPSec (contient 4 règles, de 3 à 6)

3	on	passer	Lan_in_B DMZ_in_B	Network_in Network_dmz1	Any	icmp	IPS	Créée le 2025-10-06 12:51:05, par admin (192.168.1.2)
4	on	passer	Lan_in_B DMZ_in_B	srv_ftp_priv		ftp	IPS	Créée le 2025-10-06 12:51:05, par admin (192.168.1.2) - Mise à j...

via Tunnel VPN IPsec

on	passer	Network_in	srv_ftp_priv	ftp	IPS	
on	passer	Network_in	srv_ftp_priv	Any	icmp (requête Echc	IPS

Inoming traffic from IPSec (contient 5 règles, de 3 à 7)

3	on	passer	DMZ_In_A Lan_in_A via Tunnel VPN IPsec	Network_in Network_dr	Any	icmp (requête Echc	IPS
4	on	passer	DMZ_In_A Lan_in_A via Tunnel VPN IPsec	srv_ftp_priv	ftp	IPS	
5	on	passer	Network_in	srv_ftp_priv	ftp	IPS	
6	on	passer	Network_in	srv_ftp_priv	Any	IPS	
7	off	passer	Any	Any	Any	IPS	

FW Administration from Admin PC (contient 1 règles, de 8 à 8)

4	on	passer	DMZ_in_B via Tunnel VPN IPsec	sr	ftp	IPS	
5	on	passer	Network_in	sr	ftp	IPS	
6	on	passer	Network_in	sr	Any	icmp (requête Echc	IPS
7	off	passer	Any	Any	Any	IPS	

FW Administration from Admin PC (contient 1 règles, de 8 à 8)

Inoming traffic from IPSec (contient 4 règles, de 3 à 6)

3	on	passer	Lan_in_ DMZ_in_	Network_ Network_	Any	icmp (requête Echc	IPS	Créée le 2...
4	on	passer	Lan_in_ DMZ_in_	srv_ftp_	ftp	IPS	Créée le 2...	

via Tunnel VF

- Pour tester tous ca je ping l'entreprise A de B :

```
user@client-training:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=3.12 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=3.66 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=3.69 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=3.68 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 3.119/3.539/3.692/0.253 ms
user@client-training:~$
```

➤ Je rajoute sur les deux firewalls les règles de pour le web :

Inoming traffic from IPSec (contient 7 règles, de 3 à 9)									
3	<input type="checkbox"/>	on	passer	Lan_in_B DMZ_In_B via Tunnel VPN IPsec	Network_in Network_dmz1	* Any	icmp (requête Echc	IPS	
4	<input type="checkbox"/>	on	passer	Lan_in_B DMZ_In_B via Tunnel VPN IPsec	srv_ftp_priv	ftp		IPS	
5	<input type="checkbox"/>	on	passer	Lan_in_B DMZ_In_B via Tunnel VPN IPsec	srv_web_priv	http		IPS	
6	<input type="checkbox"/>	on	passer	Network_in	srv_ftp_priv	ftp		IPS	
7	<input type="checkbox"/>	on	passer	Network_in	srv_ftp_priv	* Any	icmp (requête Echc	IPS	
8	<input type="checkbox"/>	on	passer	Network_in	srv_web_priv	* Any	HTTP	IPS	
9	<input type="checkbox"/>	off	passer	* Any	* Any	* Any		IPS	

  

Inoming traffic from IPSec (contient 7 règles, de 3 à 9)									
3	<input type="checkbox"/>	on	passer	DMZ_In_A Lan_in_A via Tunnel VPN IPsec	Network_in Network_dr	* Any	icmp (requête Echc	IPS	
4	<input type="checkbox"/>	on	passer	DMZ_In_A Lan_in_A via Tunnel VPN IPsec	srv_ftp_priv	ftp		IPS	
5	<input type="checkbox"/>	on	passer	DMZ_In_A Lan_in_A via Tunnel VPN IPsec	srv_web_priv	http		IPS	
6	<input type="checkbox"/>	on	passer	Network_in	srv_ftp_priv	ftp		IPS	
7	<input type="checkbox"/>	on	passer	Network_in	srv_ftp_priv	* Any	icmp (requête Echc	IPS	
8	<input type="checkbox"/>	on	passer	Network_in	srv_web_priv	* Any	HTTP	IPS	
9	<input type="checkbox"/>	off	passer	* Any	* Any	* Any		IPS	

  

FW Administration from Admin PC (contient 1 règles, de 10 à 10)									
10	<input type="checkbox"/>	on	passer						

➤ Puis de A je ping B et vice-versa :

```
user@client-training:~$ ping 172.16.2.12
PING 172.16.2.12 (172.16.2.12) 56(84) bytes of data.
64 bytes from 172.16.2.12: icmp_seq=1 ttl=64 time=3.40 ms
64 bytes from 172.16.2.12: icmp_seq=2 ttl=64 time=4.06 ms
64 bytes from 172.16.2.12: icmp_seq=3 ttl=64 time=2.15 ms
64 bytes from 172.16.2.12: icmp_seq=4 ttl=64 time=3.27 ms
^C
--- 172.16.2.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 2.146/3.219/4.060/0.688 ms
user@client-training:~$
```

```

user@client-training:~$ ping 172.16.1.12
PING 172.16.1.12 (172.16.1.12) 56(84) bytes of data.
64 bytes from 172.16.1.12: icmp_seq=1 ttl=64 time=2.84 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=13.5 ms
^C
--- 172.16.1.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 2.836/8.171/13.507/5.336 ms
user@client-training:~$ █

```

- Je crée 2 profils de chiffrements IKE phase 1 et 2 :

## VPN / VPN IPSEC

TIQUE DE CHIFFREMENT - TUNNELS    CORRESPONDANTS    IDENTIFICATION    **PROFILS DE CHIFFREMENT** >

+ Ajouter    Actions

**IKE (5)**

- StrongEncryption
- GoodEncryption
- Mobile
- DR
- perso**

**IPsec (5)**

- StrongEncryption
- GoodEncryption
- Mobile
- DR
- perso

**PROFIL IKE : PERSO**

Général

Commentaire:

Diffie-Hellman: **DH15 MODP Group (3072-bits)**

Durée de vie maximum (en secondes): **21600**

**PROPOSITIONS**

+ Ajouter    X Supprimer    Monter    Descendre

	Chiffrement		Authentification	
	Algorithme	Force	Algorithme	Force
1	<b>aes</b>	<b>256</b>	<b>sha2_512</b>	<b>512</b>

< TIQUE DE CHIFFREMENT - TUNNELS    CORRESPONDANTS    IDENTIFICATION    **PROFILS DE CHIFFREMENT** >

**+ Ajouter**    **≡ Actions**

IKE (5)

- StrongEncryption
- GoodEncryption
- Mobile
- DR
- perso
- IPsec (5)**
- StrongEncryption
- GoodEncryption
- Mobile
- DR
- perso**

**PROFIL IPSEC : PERSO**

**Général**

Commentaire:

Perfect Forward Secrecy (PFS):

Durée de vie maximum (en secondes):

**PROPOSITIONS D'AUTHENTIFICATION**

**+ Ajouter**    **X Supprimer**

	Algorithme	Force
1	hmac_sha512	512

**PROPOSITIONS DE CHIFFREMENT**

**+ Ajouter**    **X Supprimer**

	Algorithme	Force
1	aes	256

VÉRIFICATION DE LA POLITIQUE

➤ J'applique mes profils de chiffrement sur mon VPN, puis je vérifie que tout fonctionne :

< **POLITIQUE DE CHIFFREMENT - TUNNELS**    CORRESPONDANTS    IDENTIFICATION    PROFILS DE CHIFFREMENT >

**IPsec 01 (01)**    **≡ Actions**    **Deactivate policy**

**SITE À SITE (GATEWAY-GATEWAY)**    MOBILE - UTILISATEURS NOMADES

Q Entrer un filtre...    **+ Ajouter**    **X Supprimer**    **↑ Monter**    **↓ Descendre**    **Couper**    **Copier**

	Etat	Réseau local	Correspond...	Réseau dist...	Profil de chi...	Keepalive	Commentai...
1	<input checked="" type="checkbox"/> on	GRP_NET_ Site_Fw_B	GRP_NET_ Site_Fw_B	GRP_NET_ Site_Fw_B	perso	30	Originally cr...
2	<input type="checkbox"/> off	Network_ir Site_Fw_B	Network_ir Site_Fw_B	Lan_in_B	StrongEncrypti		Originally cr...
3	<input type="checkbox"/> off	Network_ir Site_Fw_B	Network_ir Site_Fw_B	DMZ_In_B	StrongEncrypti		Originally cr...
4	<input type="checkbox"/> off	Network_d Site_Fw_B	Network_d Site_Fw_B	Lan_in_B	StrongEncrypti		Originally cr...
5	<input type="checkbox"/> off	Network_d Site_Fw_B	Network_d Site_Fw_B	DMZ_In_B	StrongEncrypti		Originally cr...

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 ECRITURE LOGS : ACCÈS RESTREINT ?

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

IPsec 01 (01) Actions Deactivate policy

SITE À SITE (GATEWAY-GATEWAY) MOBILE - UTILISATEURS NOMADES

Entrer un filtre... + Ajouter X Supprimer Monter Descendre Couper Copier Coller Afficher les

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	GRP_NET_IN_DM	Site_Fw_A	GRP_NET_IN_DM	perso	30	Originally created...
2	off	Network_in	Site_Fw_A	Lan_in_A	StrongEncryption		Originally created...
3	off	Network_in	Site_Fw_A	DMZ_In_A	StrongEncryption		Originally created...
4	off	Network_dmz1	Site_Fw_A	Lan_in_A	StrongEncryption		Originally created...
5	off	Network_dmz1	Site_Fw_A	DMZ_In_A	StrongEncryption		Originally created...

➤ Je ping de A vers B et vice-versa pour vérifier que tout fonctionne :

```

user@client-training: ~
user@client-training: ~ 80x24
user@client-training:~$ ping 172.16.2.11
PING 172.16.2.11 (172.16.2.11) 56(84) bytes of data.
64 bytes from 172.16.2.11: icmp_seq=1 ttl=64 time=3.90 ms
64 bytes from 172.16.2.11: icmp_seq=2 ttl=64 time=4.75 ms
64 bytes from 172.16.2.11: icmp_seq=3 ttl=64 time=5.07 ms
^C
--- 172.16.2.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 3.902/4.573/5.065/0.497 ms
user@client-training:~$

```

```

user@client-training: ~
user@client-training: ~ 80x24
user@client-training:~$ ping 172.16.1.12
PING 172.16.1.12 (172.16.1.12) 56(84) bytes of data.
64 bytes from 172.16.1.12: icmp_seq=1 ttl=64 time=9.13 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=10.5 ms
64 bytes from 172.16.1.12: icmp_seq=3 ttl=64 time=3.32 ms
^C
--- 172.16.1.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 3.315/7.653/10.511/3.118 ms
user@client-training:~$

```

- Je réalise l'interconnexion de ces mêmes réseaux, mais en configurant des tunnels basés sur des VTI, avec du routage statique :
- Je crée les VTI de A et B :

## 🏠 RÉSEAU / INTERFACES VIRTUELLES

INTERFACES IPSEC (VTI)   INTERFACES GRE   LOOPBACK

Rechercher  + Ajouter X Supprimer | 👁 Vérifier l'utilisation

État	Nom ↑	Adresse IPv4	Masque IPv4	Commentaire
🟢 Activé	VTI_to_B	192.168.120.0	255.255.255.254	

## 🏠 RÉSEAU / INTERFACES VIRTUELLES

INTERFACES IPSEC (VTI)   INTERFACES GRE   LOOPBACK

Rechercher  + Ajouter X Supprimer | 👁 Vérifier l'utilisation

État	Nom ↑	Adresse IPv4	Masque IPv4	Commentaire
🟢 Activé	VTI_to_A	192.168.120.1	255.255.255.254	

- Je créer les routes statiques (en créant au préalable l'objet IP\_VTI\_\*) :

## 🏠 RÉSEAU / ROUTAGE

IPV4 ROUTING   DYNAMIC ROUTING   IPV4 REVERSE ROUTING

General

Default gateway:

STATICS ROUTES

Rechercher...  + Ajouter X Supprimer

État	Host / Network / Group	Interface	Addressing plan	Gateway	Comment
🟢 on	Lan_in_B	🏠 VTI_to_B	192.168.2.0/24	IP_VTI_B	

Nom de l'objet: IP\_VTI\_B  
Adresse IP: 192.168.120.1

ROUTES STATIQUES

Rechercher...  + Ajouter X Supprimer

État	Réseau de destination (obj...)	Interface	Plan d'adressage	Passerelle	Commentaire
🟢 on	Lan_in_A	🏠 VTI_to_A	192.168.1.0/24	IP_VTI_A	

Nom de l'objet: IP\_VTI\_A  
Adresse IP: 192.168.120.0

➤ J'ajoute les règles de filtrages adaptées :

Incoming traffic from IPsec (contient 6 règles, de 4 à 9)							
4	<input checked="" type="checkbox"/>	on	passer	Lan_in_B DMZ_in_B interface: VTL_to_B	Network_In Network_dmz1	Any icmp (requête Ech...	Créée le 2025-10-06 12:51:05, par admin (192.168.1.2)
5	<input checked="" type="checkbox"/>	on	passer	Lan_in_B DMZ_in_B interface: VTL_to_B	srv_ftp_priv	ftp	Créée le 2025-10-06 12:51:05, par admin (192.168.1.2) - Mise à j...
6	<input checked="" type="checkbox"/>	on	passer	Lan_in_B DMZ_in_B interface: VTL_to_B	srv_web_priv	http	Créée le 2025-10-06 12:51:05, par admin (192.168.1.2) - Mise à j...

  

4	<input checked="" type="checkbox"/>	on	passer	DMZ_In_A Lan_in_A interface: VTL_to_A	Network_In Network_dmz1	Any icmp (requête Ech...	Créée le 2025-10-06 13:07:53, par admin (192.168.2.2)
5	<input checked="" type="checkbox"/>	on	passer	DMZ_In_A Lan_in_A interface: VTL_to_A	srv_ftp_priv	ftp	Créée le 2025-10-06 13:07:53, par admin (192.168.2.2) - Mise à j...
6	<input checked="" type="checkbox"/>	on	passer	DMZ_In_A Lan_in_A interface: VTL_to_A	srv_web_priv	http	Créée le 2025-10-06 13:07:53, par admin (192.168.2.2) - Mise à j...

➤ Je regarde que mes tunnels sont bien fonctionnels :

MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

POLITIQUES

Type	État	Extrémité de trafic locale	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic distante
Type : Tunnels site à site (1)							
<input checked="" type="checkbox"/>	OK	Firewall_VTL_to_B	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	IP_VTL_B
Type : Politiques d'exception (bypass) (1)							

  

MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

POLITIQUES

Type	État	Extrémité de trafic locale	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic distante
Type : Tunnels site à site (1)							
<input checked="" type="checkbox"/>	OK	Firewall_VTL_to_A	Firewall_out	192.36.253.20	Fw_A	192.36.253.10	IP_VTL_A
Type : Politiques d'exception (bypass) (1)							

➤ Et enfin je test de me connecter de A sur b.net et de B vers a.net :

Not secure | b.net

SNV4

Welcome to the www.b.net lab server!

If you expected to reach your WEBMAIL, click [I wanted to reach my WEBMAIL](#).

You won't find anything really useful here, just a bunch of RFCs... Feel free to read them, you might find some interesting informations there.

- [RFC 791](#) Internet Protocol
- [RFC 792](#) Internet Control Message Protocol
- [RFC 793](#) Transmission Control Protocol
- [RFC 821](#) Simple Mail Transfer Protocol
- [RFC 894](#) A Standard for the Transmission of IP Datagrams over Ethernet Networks
- [RFC 959](#) File Transfer Protocol (FTP)
- [RFC 1321](#) The MDS Message-Digest Algorithm
- [RFC 1323](#) TCP Extensions for High Performance
- [RFC 1436](#) The Internet Gopher Protocol
- [RFC 1945](#) Hypertext Transfer Protocol -- HTTP/1.0
- [RFC 2428](#) FTP Extensions for IPv6 and NATs
- [RFC 2616](#) Hypertext Transfer Protocol -- HTTP/1.1
- [RFC 2617](#) HTTP Authentication: Basic and Digest Access Authentication
- [RFC 2818](#) HTTP over TLS
- [RFC 3330](#) Special-Use IPv4 Addresses
- [RFC 3659](#) Extensions to FTP
- [RFC 3977](#) Network News Transfer Protocol (NNTP)
- [Little Red King - A Pleasant Sunset](#) Free CC Licenced MP3 from Opsound.org
- [Virus Test files](#) The official EICAR files for download
- [Logs](#) Collected syslog logs

Not secure | a.net

SNV4

Welcome to the www.a.net lab server!

If you expected to reach your WEBMAIL, click [I wanted to reach my WEBMAIL](#).

You won't find anything really useful here, just a bunch of RFCs... Feel free to read them, you might find some interesting informations there.

- [RFC 791](#) Internet Protocol
- [RFC 792](#) Internet Control Message Protocol
- [RFC 793](#) Transmission Control Protocol
- [RFC 821](#) Simple Mail Transfer Protocol
- [RFC 894](#) A Standard for the Transmission of IP Datagrams over Ethernet Networks
- [RFC 959](#) File Transfer Protocol (FTP)
- [RFC 1321](#) The MDS Message-Digest Algorithm
- [RFC 1323](#) TCP Extensions for High Performance
- [RFC 1436](#) The Internet Gopher Protocol
- [RFC 1945](#) Hypertext Transfer Protocol -- HTTP/1.0
- [RFC 2428](#) FTP Extensions for IPv6 and NATs
- [RFC 2616](#) Hypertext Transfer Protocol -- HTTP/1.1
- [RFC 2617](#) HTTP Authentication: Basic and Digest Access Authentication
- [RFC 2818](#) HTTP over TLS
- [RFC 3330](#) Special-Use IPv4 Addresses
- [RFC 3659](#) Extensions to FTP
- [RFC 3977](#) Network News Transfer Protocol (NNTP)
- [Little Red King - A Pleasant Sunset](#) Free CC Licenced MP3 from Opsound.org
- [Virus Test files](#) The official EICAR files for download
- [Logs](#) Collected syslog logs

## Quiz :

Q1– IPsec utilise TCP pour négocier la connexion, puis se envoie les données chiffrées grâce à UDP :

B. Faux

Q2–SHA1 est un algorithme de hachage sûr pour les tunnels VPN :

B. Faux

Q3–Les VTI font partie du standard IKEv2 et ne sont pas disponibles sur IKEv1 :

B. Faux

Q4–Un tunnel IPsec garantit :

A. L'authentification

C. L'intégrité

D. La confidentialité

E. L'anti-rejeu

Q5–L'option keepalive permet au pare-feu de détecter des coupures de connexion :

B. Faux

Q6– La négociation d'un tunnel IPsec est initiée seulement s'il y a des données à envoyer dans le tunnel :

A. Vrai

Q7– Sans VTI, il est impossible de faire fonctionner deux tunnels entre les mêmes réseaux simultanément (pour un besoin de redondance par exemple) :

A. Vrai

Q8– Une route statique est nécessaire pour que le firewall puisse envoyer les paquets dans un tunnel IPsec :

B. Vrai seulement avec des VTI