

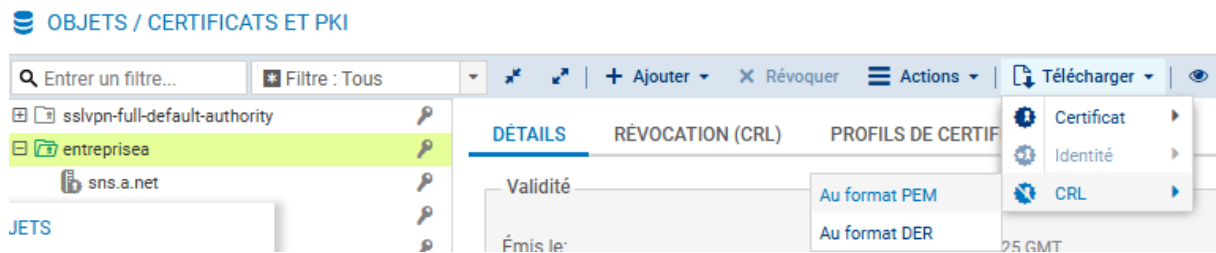
Lab13 : VPN IPsec Site à Site avec certificat

Table des matières

Lab13 : VPN IPsec Site à Site avec certificat 1

NICOLAU Noah

- Nous téléchargeons le certificat de l'autorité de certification pour l'importer sur le SNS de B.



- Nous créons l'identité serveur de b.

CRÉER UNE IDENTITÉ SERVEUR

OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Nom de domaine qualifié (FQDN):

Identifiant:

✗ ANNULER

⏪ PRÉCÉDENT

⏩ SUIVANT

- Nous mettons comme parents l'autorité de certification de l'entreprise a.

CRÉER UNE IDENTITÉ SERVEUR

OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Sélectionnez l'autorité parente

Autorité parente:

Mot de passe de la CA:

Attributs de l'autorité

Organisation (O):

Unité d'organisation (OU):

Ville (L):

État (ST):

Pays (C):

CRÉER UNE IDENTITÉ SERVEUR

OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Validité (jours):

Type de clé:

Taille de clé (bits):

CRÉER UNE IDENTITÉ SERVEUR

AJOUT D'ALIAS - ASSISTANT DE CRÉATION



+ Ajouter × Supprimer ↑ Monter ↓ Descendre

URI (address)

× ANNULER << PRÉCÉDENT >> SUIVANT

CRÉER UNE IDENTITÉ SERVEUR

RÉSUMÉ

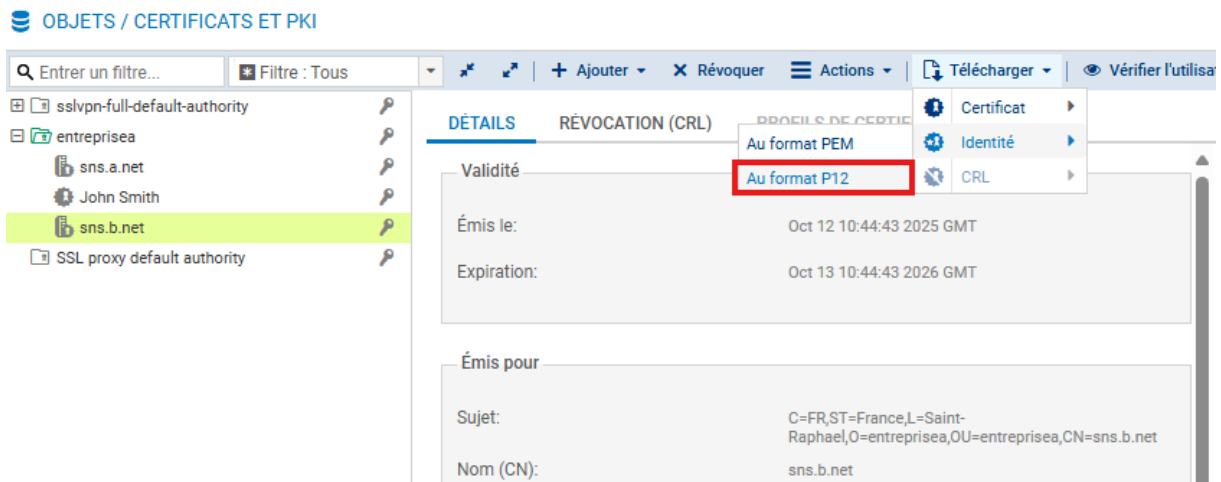
Terminez cet assistant afin de créer l'identité serveur ci-dessous

Nom:	sns.b.net
Identifiant:	sns.b.net
Autorité parente:	entreprisea
Organisation (O):	entreprisea
Unité d'organisation (OU):	entreprisea
Ville (L):	Saint-Raphael
État (ST):	France
Pays (C):	FR
Type de clé:	RSA
Taille de clé:	2048

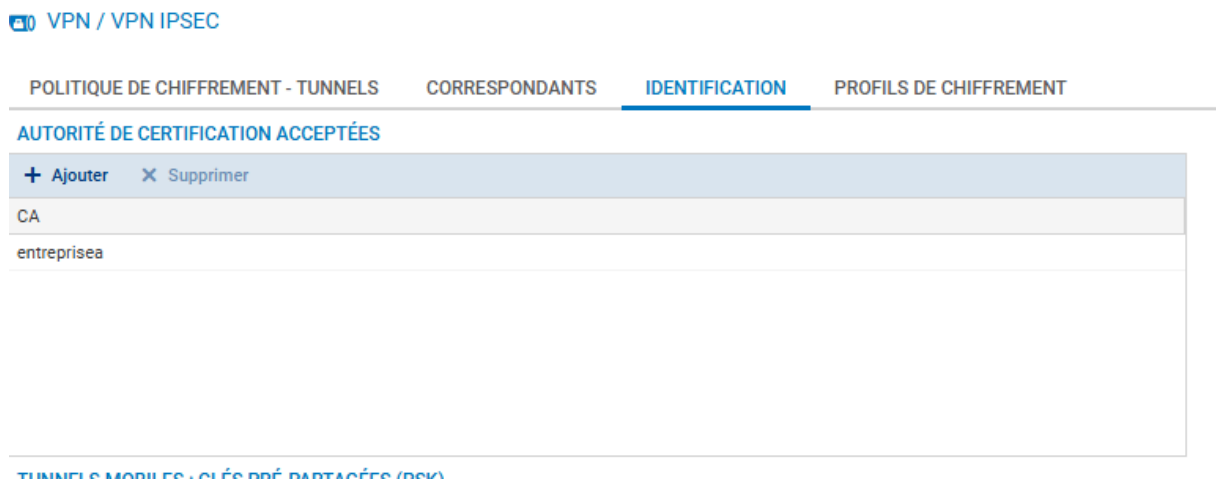
Valide jusque Tue Oct 13 2026 10:43:10 GMT+0200 (heure d'été d'Europe centrale) soit 365 jours

× ANNULER << PRÉCÉDENT ✓ TERMINER

- Nous téléchargeons le certificat de b pour lui remettre.



- Nous ajoutons l'autorité de certification dans les autorités de certification acceptées.



- Nous modifions le correspondant Site_Fw_B et ajoutons le certificat sns_a.net.

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrez un filtre...

- Passerelles distantes (1)
- Site_fw_b**
- Correspondants mobiles (1)
- nomade_entrepris...

SITE_FW_B

Général

Commentaire:

Passerelle distante: Fw_B

Adresse locale: Any

Profil IKE: IkePhase1

Version IKE: IKEv2

Identification

Méthode d'authentification: Certificat

Certificat: **entreprise:sns.a.net**

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

Clé pré-partagée (PSK): Éditer

- Nous vérifions la présence du tunnel VPN dans la politique de chiffrement.

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

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

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	Network_interna	Site_fw_b	Lan_in_B	IPSECPhase2	30	Originally created...

- Nous vérifions les règles de filtrage.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

Lab_9 Editer Exporter

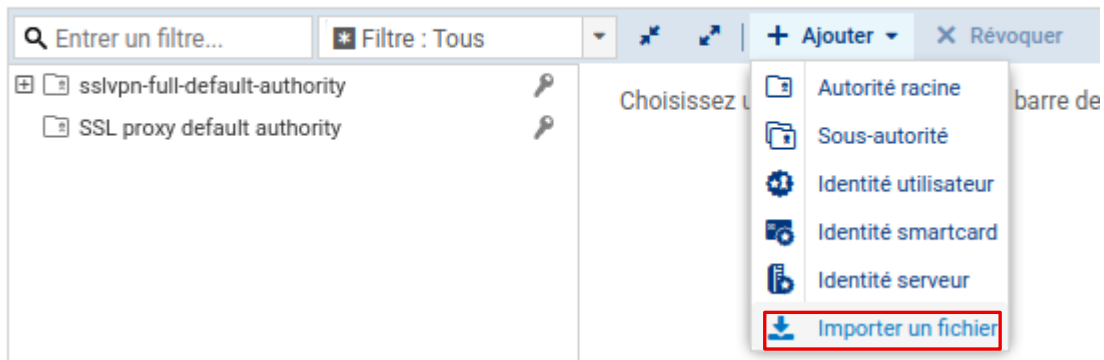
FILTRAGE NAT

Rechercher... + Nouvelle règle X Supprimer Monter Descendre Couper Copier Coller

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Comment...
1	off	passer	Any	Any	Any		IPS	Créée le 2...
Internal traffic to DMZ (contient 6 règles, de 2 à 7)								
Outgoing traffic (contient 14 règles, de 8 à 21)								
Incomming traffic (contient 6 règles, de 22 à 27)								
VPN IPSEC NOMADE (contient 4 règles, de 28 à 31)								
VPN IPSEC Site a Site (contient 2 règles, de 32 à 33)								
32	on	passer	Lan_in_f via Tunnel VP	srv_ftp_f	ftp		IPS	Créée le 2...
33	on	passer	Lan_in_f via Tunnel VP	srv_ftp_f	Any	icmp (requête Ech	IPS	Créée le 2...
IPSEC (contient 4 règles, de 34 à 37)								
VPN SSL (contient 3 règles, de 38 à 40)								

- Nous importons le certificat de l'identité serveur b sur le SNS b.

OBJETS / CERTIFICATS ET PKI



IMPORTER UN FICHIER DANS LA PKI

Fichier à importer: ...

Format du fichier: P12
 DER
 PEM

Mot de passe du fichier (si PKCS#12):

Éléments à importer: Tous
 Certificat(s)
 Clé(s) privée(s)
 CRL
 CA

Écraser le contenu existant dans la PKI

- Nous constatons que le certificat s'est bien importé.

OBJETS / CERTIFICATS ET PKI

The screenshot shows a web interface for managing certificates. On the left, a sidebar lists several objects: 'sslvpn-full-default-authority', 'entreprisea', 'sns.b.net' (highlighted in green), and 'SSL proxy default authority'. The main area is titled 'DÉTAILS' and shows the following information:

Validité	
Émis le:	Oct 12 10:44:43 2025 GMT
Expiration:	Oct 13 10:44:43 2026 GMT

Émis pour	
Sujet:	C=FR,ST=France,L=Saint-Raphael,O=entreprisea,OU=entreprisea,CN=sns.b.net
Nom (CN):	sns.b.net
Nom de l'organisation (O):	entreprisea
Nom de l'unité (OU):	entreprisea
Nom du lieu (L):	Saint-Raphael
Nom de l'état ou de la province (ST):	France
Pays (C):	FR
E-mail:	
Somme de contrôle:	769d5fb9

- Nous importons le certificat de l'autorité de certification.

The screenshot shows a form titled 'IMPORTER UN FICHIER DANS LA PKI'. The form contains the following fields and options:

- Fichier à importer: ...
- Format du fichier:
 - P12
 - DER
 - PEM
- Mot de passe du fichier (si PKCS#12):
- Éléments à importer:
 - Tous
 - Certificat(s)
 - Clé(s) privée(s)
 - CRL
 - CA
- Écraser le contenu existant dans la PKI

At the bottom, there are two buttons: 'ANNULER' (with a red X icon) and 'IMPORTER' (with a green checkmark icon).

- Nous constatons que cela a fonctionné.

OBJETS / CERTIFICATS ET PKI

Entrez un filtre... Filtre : Tous + Ajouter Révoquer Actions Télécharger Vérifier l'utilisation

sslvpn-full-default-authority entreprisea sns.b.net SSL proxy default authority

DÉTAILS **RÉVOCATION (CRL)** PROFILS DE CERTIFICATS

Validité

Dernière mise à jour: Oct 13 10:40:43 2025 GMT
Prochaine mise à jour: Nov 12 10:40:43 2025 GMT

POINTS DE DISTRIBUTION

+ Ajouter X Supprimer

URI (adresse)

CERTIFICATS RÉVOQUÉS

Numéro de série	Date de révocation	Motif de révocation
-----------------	--------------------	---------------------

- Nous ajoutons l'autorité de certification dans les autorités de certification acceptées.

VPN / VPN IPSEC

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

AUTORITÉ DE CERTIFICATION ACCEPTÉES

+ Ajouter X Supprimer

CA

entreprisea

VPN / VPN IPSEC

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

AUTORITÉ DE CERTIFICATION ACCEPTÉES

+ Ajouter X Supprimer

CA

C=FR ST=France L=Saint-Raphael O=entreprisea OU=entreprisea CN=entreprisea

- Nous modifions le correspondant IPsec et ajoutons le certificat sns_b.net.

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrer un filtre... ☰

Passerelles distantes (1)
Site_fw_a

SITE_FW_A

Général

Commentaire:

Passerelle distante: Fw_A

Adresse locale: Any

Profil IKE: IKEPhase1

Version IKE: IKEv2

Identification

Méthode d'authentification: **Certificat**

Certificat: C=FR ST=France L=Saint-Raphael O=entreprisea OU=entrepris

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

Clé pré-partagée (PSK): Éditer

- Nous vérifions la présence du tunnel VPN dans la politique de chiffrement.

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

IPsec 01 (01) ☰ Actions ℹ 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_internal	Site_fw_a	Lan_in_A	IPSECPhase2	30	Originally created...

- Nous ajoutons la machine srv_ftp_priv_A en tant qu'objet.

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Port

Nom de l'objet: srv_ftp_priv_A

Adresse IPv4: 172.16.1.12

Adresse MAC: 01:23:45:67:89:ab (Facultatif)

Résolution

Aucune (IP statique) Automatique

Commentaire:

- Nous configurons une règle de filtrage pour pouvoir se connecter en FTP au serveur intranet.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

Rechercher... | + Nouvelle règle | X Supprimer | ↑ ↓ ↕ ↗ ↘ | Couper | Copier | Coller |

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commenta...
VPN IPSEC Site a Site (contient 2 règles, de 1 à 2)								
1	on	passer	Network	srv_ftp_p	ftp		IPS	Créée le 20...
2	on	passer	Network	Any	Any	icmp (requête Echr	IPS	Créée le 20...

- Nous effectuons des tests pour vérifier le fonctionnement.

```

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=1.86 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=2.14 ms
64 bytes from 172.16.1.12: icmp_seq=3 ttl=64 time=1.41 ms
64 bytes from 172.16.1.12: icmp_seq=4 ttl=64 time=2.82 ms
64 bytes from 172.16.1.12: icmp_seq=5 ttl=64 time=5.00 ms
z64 bytes from 172.16.1.12: icmp_seq=6 ttl=64 time=6.38 ms

```

- Nous constatons que les tunnels sont opérationnels.

POLITIQUES

Type	État	Extrémité de trafic lo...	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic di...
Type : Tunnels site à site (5)							
↔	OK	Network_dmz1	Firewall_out	C=FR, ST=Franc...	Fw_B	%any	Lan_in_B
↔	OK	Network_in	Firewall_out	C=FR, ST=Franc...	Fw_B	%any	Lan_in_B
↔	OK	Net-SSLVPN_TCP	Firewall_out	C=FR, ST=Franc...	Fw_B	%any	Lan_in_B
↔	OK	Net-SSLVPN_UDP	Firewall_out	C=FR, ST=Franc...	Fw_B	%any	Lan_in_B
↔	OK	Firewall_VTL_to_A	Firewall_out	C=FR, ST=Franc...	Fw_B	%any	ip_VTL_B
Type : Tunnels mobiles (1)							
↔	OK	Network_dmz1		C=FR, ST=Franc...		%any	
Type : Politiques d'exemption (bypass) (1)							

- Nous vérifions les logs VPN.

LOG / VPN

30 derniers jours | Actualiser | Rechercher... | Recherche avancée

RECHERCHE DU - 13/09/2025 13:15:26 - AU - 13/10/2025 13:15:26

Enregistré à	Message	Utilisateur	Nom de la source	Réseau local	Nom de destinat
13/10/2025 13:08:41	IPSEC SA established		Anonymized	192.168.1.0/24	Fw_B
13/10/2025 13:08:41	Narrowing from 172...		Anonymized		Fw_B
13/10/2025 13:07:57	IPSEC SA established		Anonymized	192.168.120.0...	Fw_B