ARV : Administration de Réseau Virtuel

EOLE 2.5

création : Mai 2015 Version : révision : Avril 2018

EOLE 2.5

Version : révision : Avril 2018

Date : création : Mai 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Pour toute information concernant ce projet vous pouvez nous joindre :

- Par courrier électronique : eole@ac-dijon.fr
- Par FAX : 03-80-44-88-10
- Par courrier : EOLE-DSI - 2G, rue du Général Delaborde - 21000 DIJON
- Le site du Pôle national de compétences Logiciels Libres : http://eole.orion.education.fr

Table des matières

Chapitre 1

Présentation de ARV

ARV[p.46] est l'acronyme de : Administration de Réseaux Virtuels.

ARV permet de construire un modèle de configuration RVP[p.47]. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan[p.47].

http://www.strongswan.org/

ARV est pré-configuré dans le module Sphynx.

Le serveur Sphynx doit être enregistré sur Zéphir pour permettre de gérer les RVP des modules EOLE enregistrés sur Zéphir.

Un seul "Sphynx ARV" pourra gérer les RVP des modules Amon mais également d'autres "Sphynx distants".

ARV en mode certificats auto-signés ou certificats signés

Le Réseau Virtuel Privé[p.47] (RVP) est prévu pour fonctionner en mode PKI[p.47] :

- mode certificats auto signés (par CA locale) ;
- mode certificats signés (par CA externe).

Le concentrateur RVP (Sphynx) est pré-configuré pour fonctionner de cette façon.

Les connexions établies à l'aide de certificats auto signés et de certificats signés par une CA externe peuvent coexister sur ce serveur.

Le fonctionnement du concentrateur Sphynx en mode certificats signés nécessite comme pré-requis, un certificat délivré par l'Autorité de Certification (AC ou CA). Toute la gestion des certificats et des clefs nécessite une infrastructure de type RACINE[p.47] (chaque configuration établissement doit obtenir également un certificat).

Les éléments d'un Réseau Virtuel Privé

Un Réseau Virtuel Privé est composé de différents éléments :

- un **concentrateur RVP** :

  il permet la concentration des tunnels en provenance des établissements extérieurs (topologie en étoile) avant de les rediriger vers le sous réseau de concentration choisi ;

- le **pare-feu Amon** :

  point d'entrée dans le réseau établissement et point de sortie unique de l'établissement vers Internet (une extrémité du tunnel RVP) ;

- le **lien sécurisé** :

  lien entre un nœud de type pare-feu Amon et un concentrateur RVP, ce lien est sécurisé par des certificats SSL. Les tunnels passeront dans le lien sécurisé ;

- le **tunnel** :

  connexion au travers l'Internet permettant de relier deux réseaux locaux ;

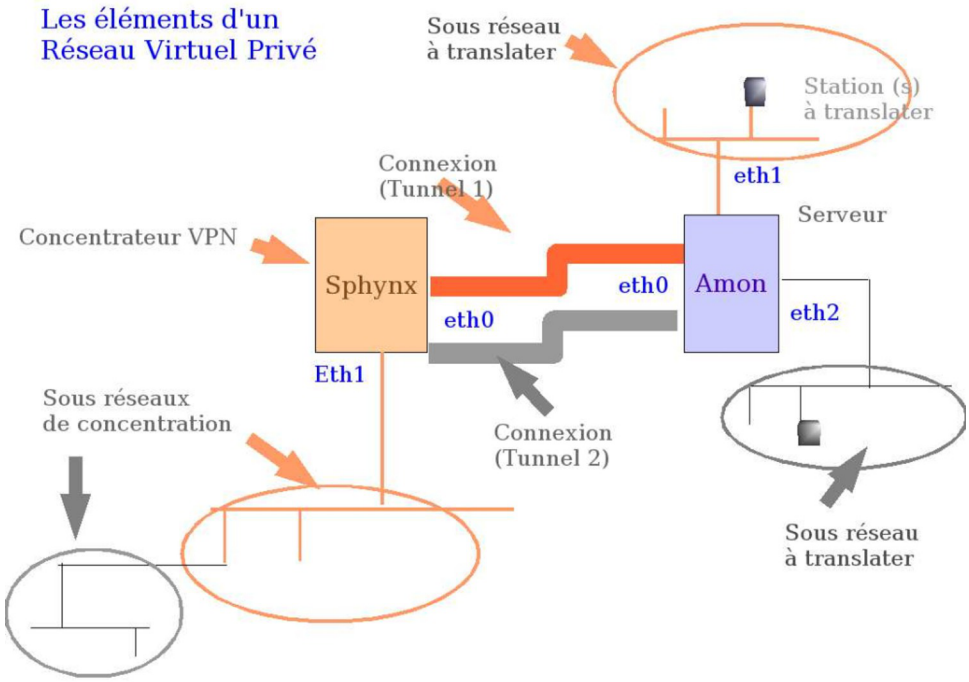
- le **réseau local** :

  situé derrière le pare-feu Amon (réseau établissement) ou derrière le concentrateur, il est composé de plusieurs sous-réseaux composés eux mêmes de stations.

La création de ce RVP permet donc de relier l'établissement à un ou plusieurs sous-réseaux des services académiques, mais également à plusieurs concentrateurs RVP et à plusieurs établissements.

Il est possible de choisir à l'intérieur de l'établissement la station, les stations du sous-réseau, le(s) sous-réseau(x) pouvant transiter au travers du tunnel ou des tunnels, et ainsi bénéficier des avantages du RVP (chiffrement des informations).

Le schéma ci-dessous récapitule de manière simple les différents composants d'un Réseau virtuel privé.



Les éléments d'un réseau virtuel privé

Serveurs impactés

Pour monter un tunnel vous devez intervenir sur les serveurs suivant : Sphynx, Amon, Zéphir (pour les utilisateurs du gestionnaire de parc). Vous devez également connaître les éléments des réseaux à relier.

C'est à dire :

- coté pare-feu Amon : la station, les sous-réseaux ou le réseau de l'établissement à translater dans le tunnel ;
- coté concentrateur : les sous-réseaux de concentration à atteindre.

Les tunnels

Le module Amon accepte de monter de 1 à n tunnels vers 1 ou n concentrateur RVP et vers 1 ou n Amon.

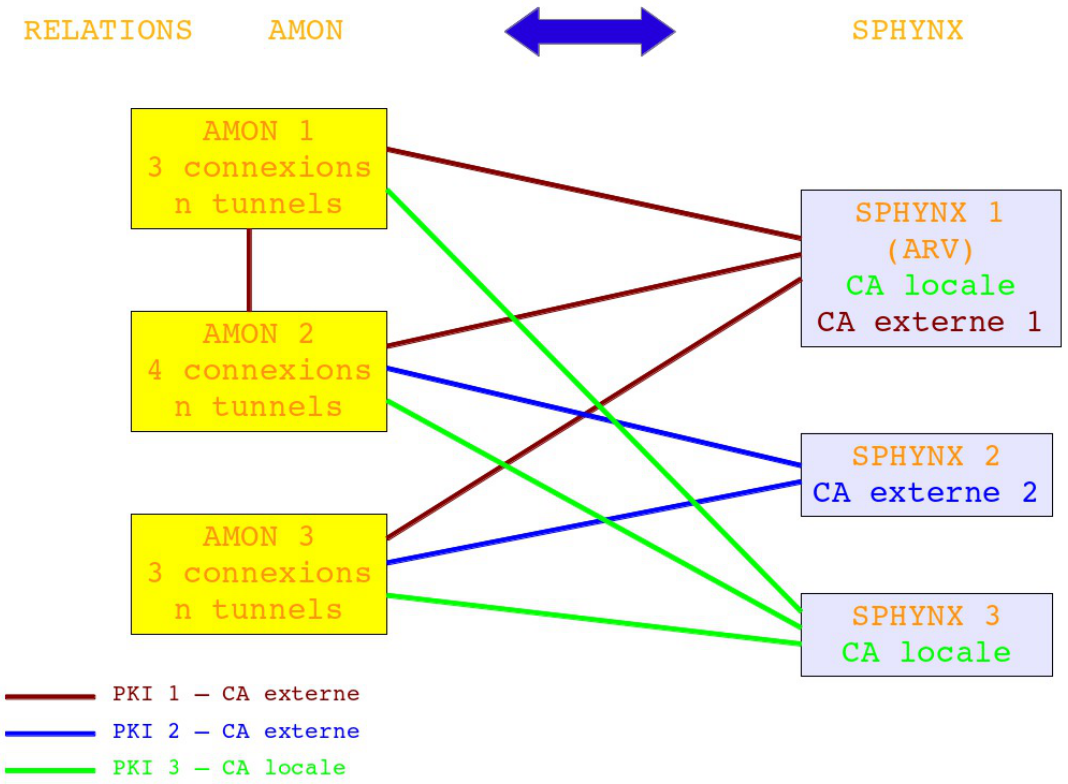
Avec ARV, il est possible de mélanger les modes.

On peut donc envisager, par exemple, d'avoir dans un établissement :

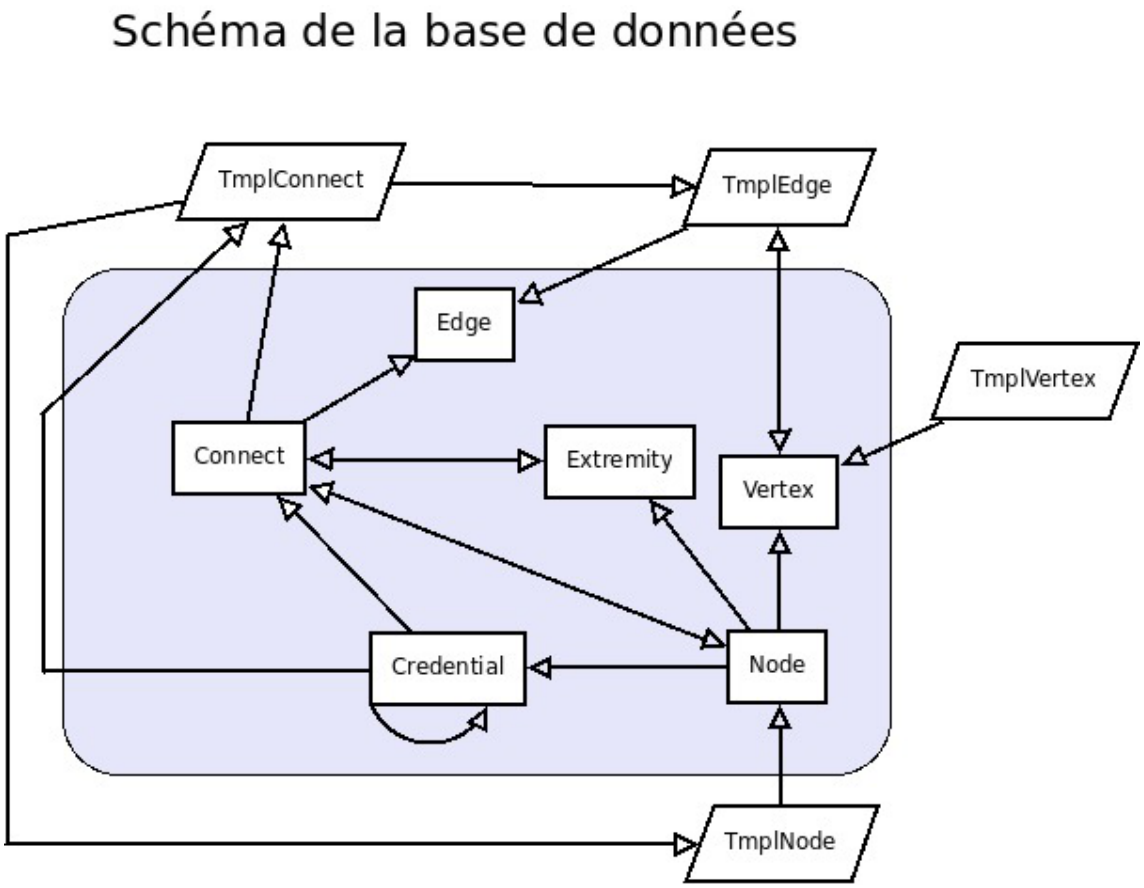
- un tunnel vers un serveur Sphynx académique protégeant les flux administratifs ;
- un tunnel faisant transiter certains flux vers un autre serveur Sphynx utilisant une CA différente ;
- un tunnel vers un autre site de son établissement connecté sur internet par un Amon.

Ces trois tunnels passeront dans trois liens sécurisés différents.

Les tunnels sont montés de façon permanente, une vérification automatique depuis l'extrémité établissement est mise en place. Elle permet de remonter le tunnel en cas de problème.

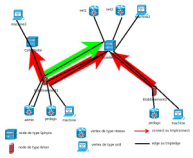


Les modèles

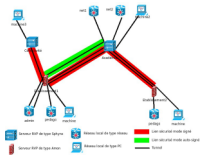


ARV est composé de deux vues :

- la vue abstraite, appelée modèle ;



- la vue concrète, avec les pare-feu Amon, les concentrateurs RVP, les liens sécurisés et les tunnels.



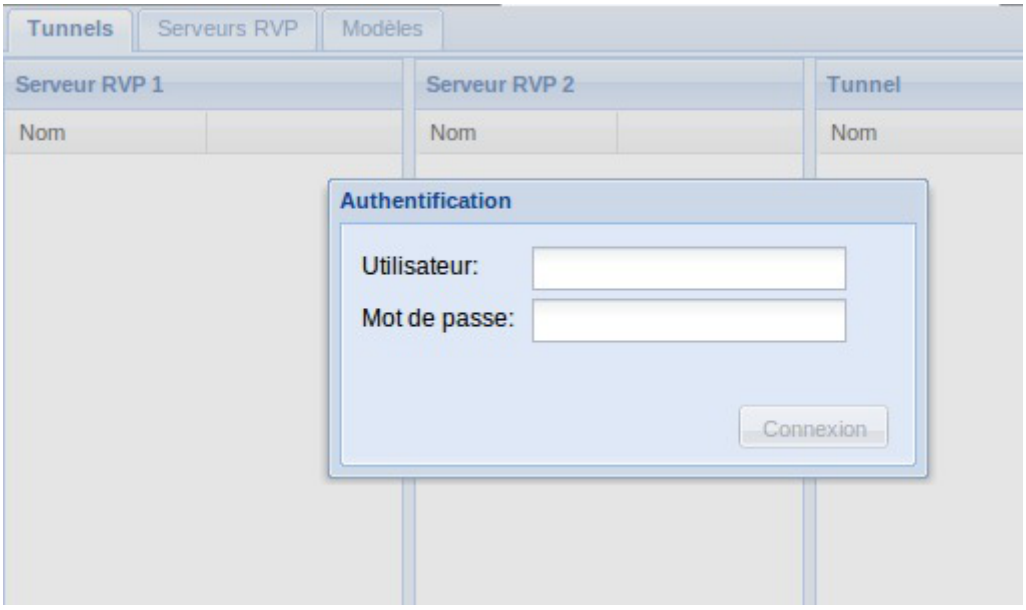
Un modèle est un squelette de réseau virtuel. Il permet de schématiser les relations entre les réseaux locaux de chaque serveur (Amon--concentrateur RVP et Amon--Amon). Chaque tunnel final sera basé sur ce modèle.

Chapitre 2

Présentation de l'interface

L'interface d'ARV est accessible via un navigateur web à l'adresse : `https://<IP Sphynx>:8088`

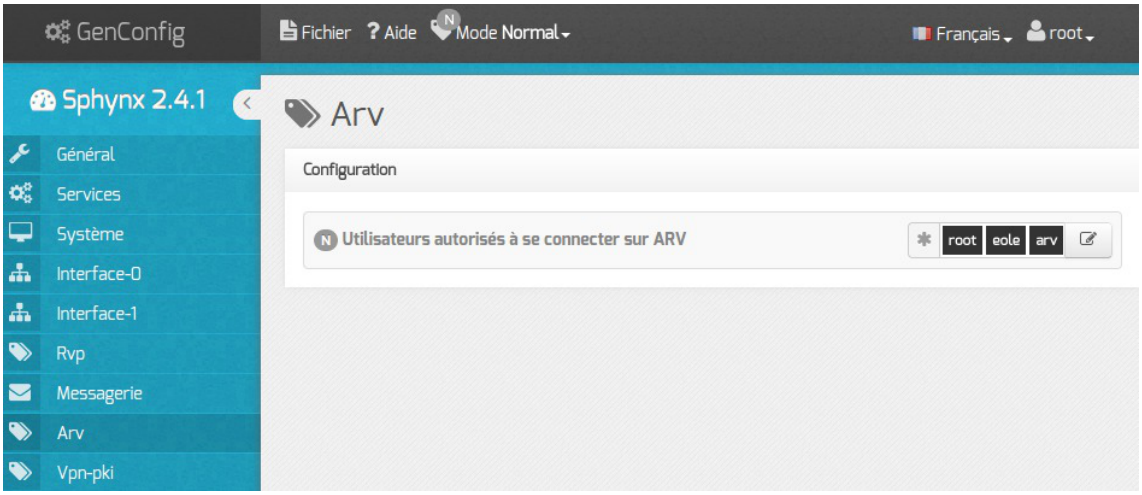
Elle nécessite une authentification.



Fenêtre d'authentification d'ARV

Les utilisateurs autorisés à se connecter sur ARV peuvent être des comptes systèmes locaux et des comptes Zéphir.

Pour qu'un compte puisse avoir accès à ARV, il faut impérativement les déclarer dans l'interface de configuration du module.



Gestion des utilisateurs autorisés à se connecter sur ARV

L'utilisation d'un compte Zéphir permet :

- de gérer les tunnels ;

- d'importer de Zéphir les serveurs de type Amon (Amon, AmonEcole, AmonHorus) et Sphynx enregistrés ;
- de générer les configurations RVP des tunnels modélisés sous forme d'archive ;
- d'envoyer sur le module Zéphir les archives RVP des serveurs ajoutés par importation.

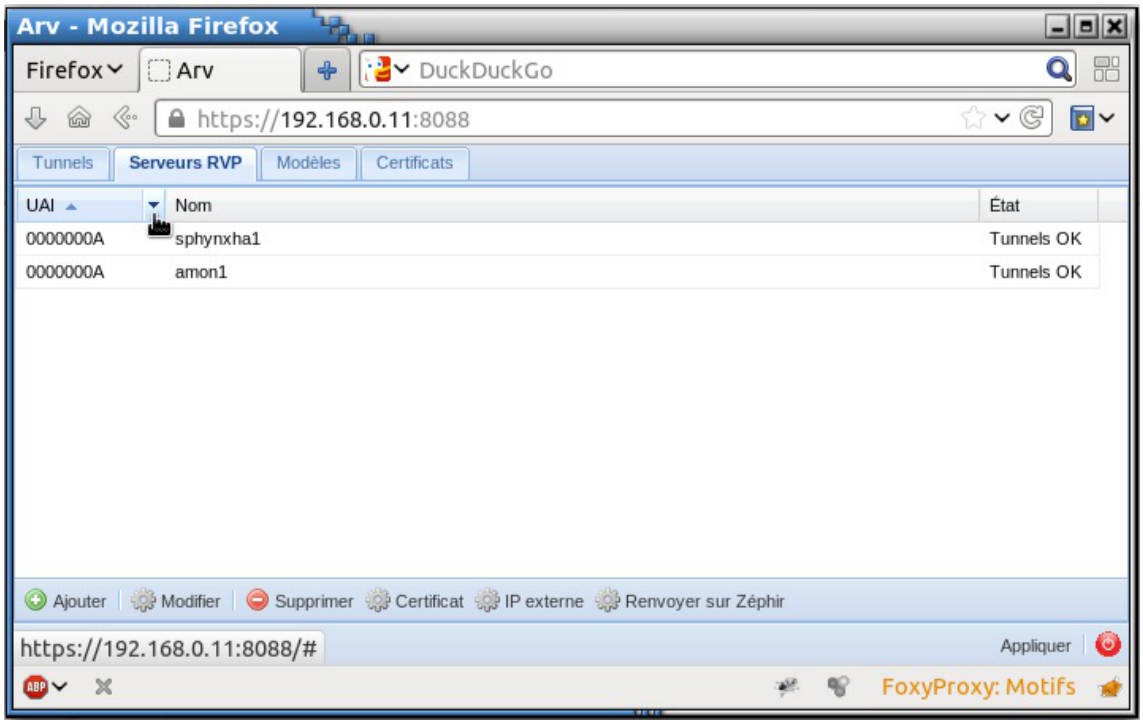
L'utilisation des comptes locaux (`root` et `eole` par défaut) permet :

- de gérer les tunnels ;
- de générer les configurations RVP des tunnels modélisés sous forme d'archive.

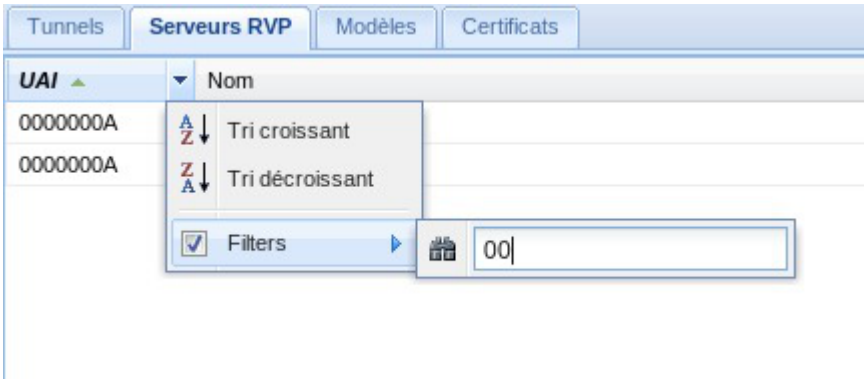
Les comptes Zéphir doivent avoir les droits en `Lecture` et `Configuration vpn`.

Sur certaines colonnes de l'application il est possible de trier ou de filtrer l'affichage.

Pour accéder à ces fonctionnalités il faut positionner le pointeur à la droite du titre de la colonne, une icône flèche en bas apparaît.



Un clique sur la flèche affiche les options de tri et éventuellement de filtrage.



La déconnexion se fait en cliquant sur le bouton rouge en bas à droite dans l'application.

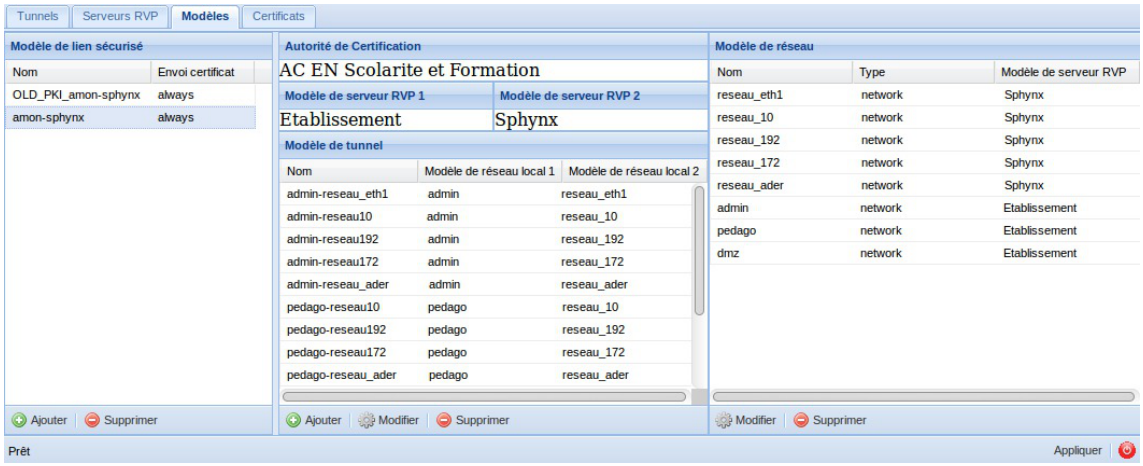
Bouton de déconnexion d'ARV

Chapitre 3

Modèles ARV

Ajout/Modification/Suppression d'un modèle de lien sécurisé

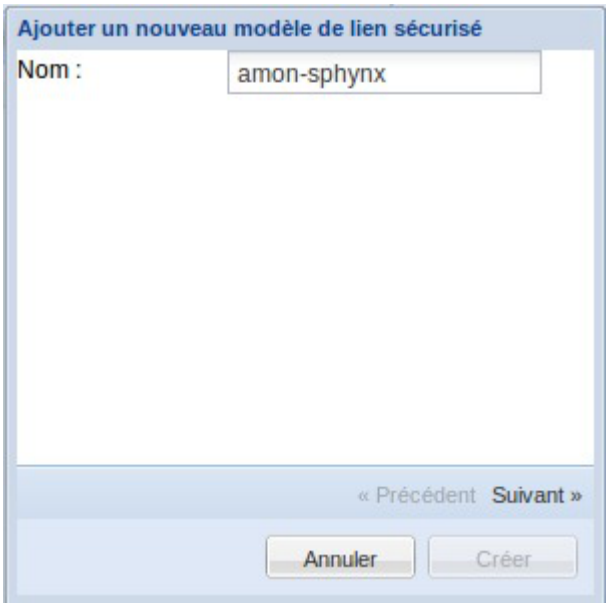
Pour ajouter, modifier ou supprimer un modèle de lien sécurisé, se rendre dans l'onglet `modèles` de la fenêtre principale de l'application web.



Fenêtre principale d'ARV avec l'onglet Modèles

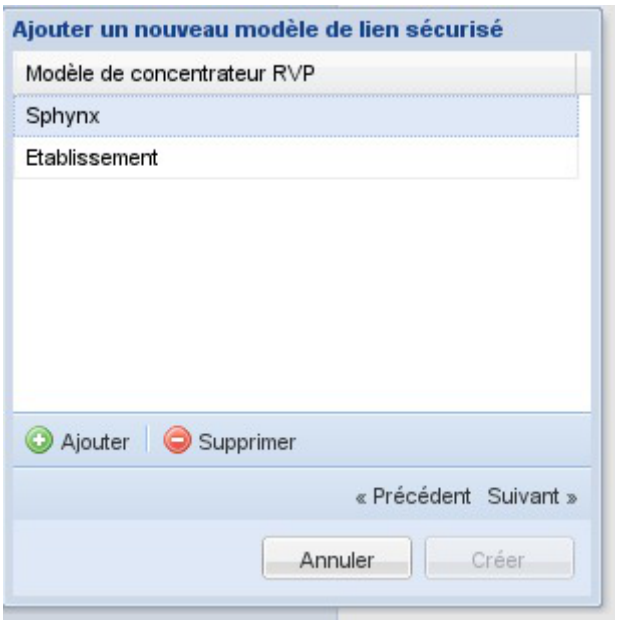
- Pour créer un nouveau modèle de lien sécurisé, cliquer sur le bouton `Ajouter` dans la colonne `modèle de lien sécurisé`.
- Pour modifier un modèle de lien sécurisé, il faut sélectionner le modèle voulu dans la colonne `modèle de lien sécurisé`. Vous pouvez ensuite `Ajouter` / `Modifier` / `Supprimer` des modèles de tunnel.
- Pour supprimer un modèle de lien, sélectionner le modèle voulu et cliquer sur le bouton `Supprimer` dans la colonne `modèle de lien sécurisé`. Ce modèle ne peut être supprimé que si il n'est plus utilisé.

Pour ajouter en modèle de lien sécurisé, commencer par lui donner un nom.



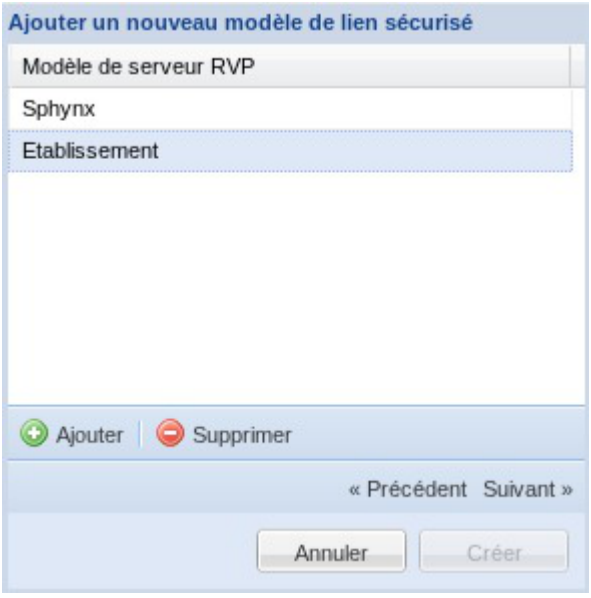
Nom du modèle de lien sécurisé

Choisir ensuite un modèle de serveur RVP source.



Modèle de concentrateur RVP source

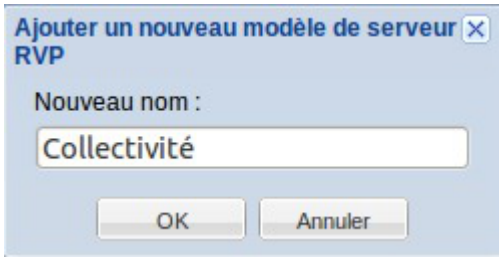
Et le modèle de serveur RVP de destination.



Modèle de concentrateur RVP destination

Notez qu'il est possible de construire des modèles de lien sécurisé de tout type (Etablissement-Sphynx, Etablissement-Etablissement, Sphynx-Sphynx).

Si vous voulez ajouter un modèle de serveur RVP, par exemple une collectivité locale, cliquer sur le bouton Ajouter et spécifier un nom.



Ajout d'un nouveau modèle de concentrateur RVP

Enfin, choisir l'autorité de certification et choisir si le certificat est envoyé ou non via le protocole IPsec.

Sélection de l'autorité de certification pour le modèle de lien sécurisé

Et cliquer sur Créer pour ajouter le modèle.

Le protocole IKEv2 ne supporte la fragmentation des paquets réseaux, ne jamais envoyer le certificat via le protocole IPsec permet de réduire la taille des paquets.

Ajout/Modification/Suppression d'un modèle de tunnel

Pour ajouter, modifier ou supprimer un modèle de tunnel, se rendre dans l'onglet modèles de la fenêtre principale de l'application web,et choisir un modèle de lien sécurisé.

- Pour ajouter un modèle de tunnel, cliquer sur le bouton Ajouter de la colonne Modèle de tunnel.
- Pour modifier un modèle de tunnel, il faut sélectionner le modèle voulu dans la colonne Modèle de tunnel et cliquer sur Modifier dans cette même colonne.

C'est ici qu'il sera possible d'Ajouter/Modifier/Supprimer des modèles de réseaux locaux.

- Pour supprimer un modèle de tunnel, il faut sélectionner le modèle voulu dans la colonne Modèle de tunnel et cliquer sur Supprimer dans cette même colonne. Ce modèle ne peut être supprimé que si il n'est plus utilisé.

La suppression d'un modèle de tunnel entraîne également la suppression des modèles de réseaux locaux non utilisés.

Pour ajouter un modèle de tunnel, commencer par lui donner un nom. C'est ce nom qui apparaîtra comme `child` lié à une `connexion` à l'exécution de la commande `ipsec statusall`.

Création d'un modèle de tunnel

Choisir, les modèles de réseaux locaux correspondants à chaque extrémité du tunnel et cliquer sur Créer.

Ajout/Modification/Suppression d'un modèle de réseau local

Un réseau local correspond à un nom et un type.

Il existe trois types de réseaux locaux :

- `IP` : adresse IP d'une machine isolée ;
- `réseau` : adresse réseau et adresse masque du réseau ;
- `plage` : plage d'adresses IP correspondant à des adresses de machines.

Pour pouvoir ajouter, modifier ou supprimer un modèle de réseau local, il faut ajouter ou modifier un modèle de tunnel.

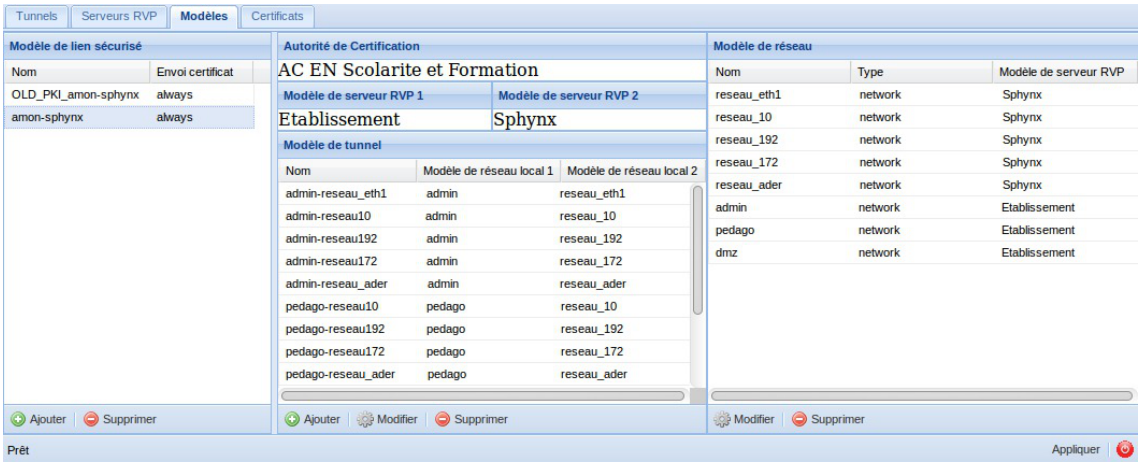
Création d'un modèle de tunnel

La modification d'un modèle de réseau local ne modifie pas les tunnels déjà créés.

- Pour ajouter un modèle de réseau local, cliquer sur le bouton Ajouter de la fenêtre d'ajout/modification de modèle de tunnel.
- Pour modifier un modèle de réseau local, il faut sélectionner le modèle voulu dans une des listes déroulantes et cliquer sur le bouton Modifier de la fenêtre d'ajout/modification de modèle de tunnel.
- Pour supprimer un modèle de réseau local, il faut sélectionner le modèle voulu dans une des listes déroulantes et cliquer sur le bouton Suppr. de la fenêtre d'ajout/modification de modèle de tunnel.Ce modèle ne peut être supprimé que si il n'est plus utilisé.

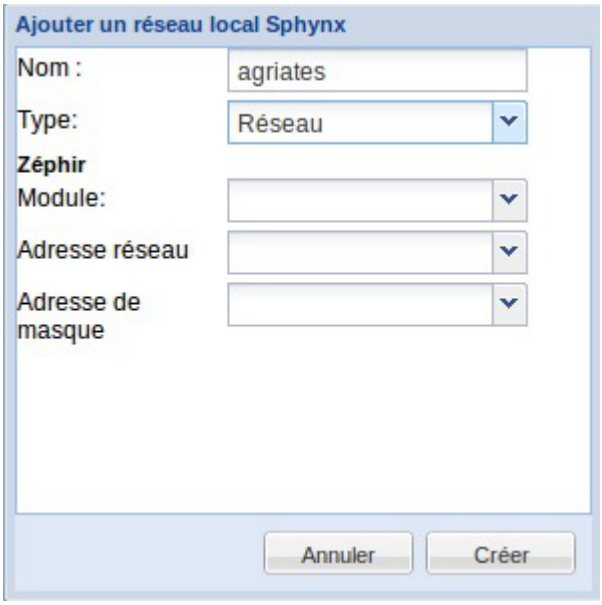
Il est également possible de modifier / supprimer les modèles de réseau dans la colonne de

droite de l'onglet Modèle.



Fenêtre principale d'ARV avec l'onglet Modèles

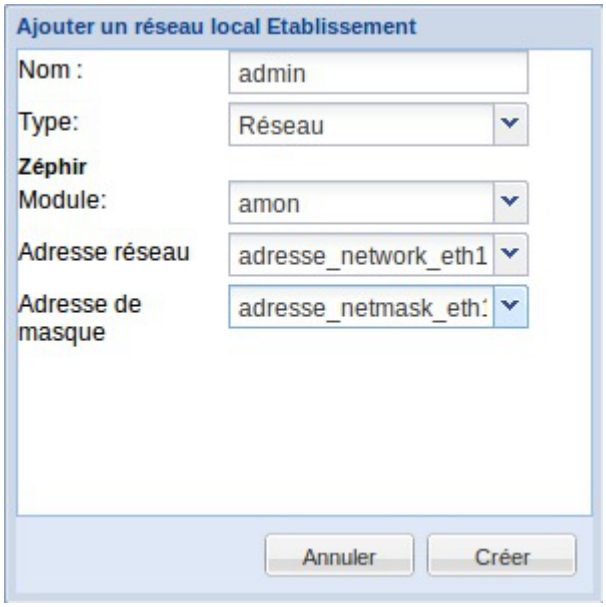
Pour ajouter un modèle de réseau local, commencer par lui donner un nom.



Création du modèle de réseau local net1

Pour faciliter la saisie des paramètres réseau, il est possible d'utiliser le serveur Zéphir.

Pour cela, indiquer le nom du module et les variables Creole correspondantes.



Création du modèle de réseau local Scribe

Il est possible d'utiliser des variables multivaluées qui peuvent être :

- sans index :
  - L'ensemble des valeurs de la variable multivaluée sera traité
  - Un tunnel sera créé pour chaque réseau de la liste

  Syntaxe : `adresse_network_vlan_eth1`
- avec index (`[n]`) :
  - Seule la valeur correspondant à l'index sera traitée
  - Un seul tunnel sera créé

  Syntaxe :

  `adresse_network_vlan_eth1[0]` et `adresse_netmask_vlan_eth1[0]` pour le premier vlan déclaré sur eth1 ;

  `adresse_network_vlan_eth1[1]` et `adresse_netmask_vlan_eth1[1]` pour le deuxième vlan déclaré sur eth1 ;

  [...]

  ou

  `alias_network_eth2[0]` et `alias_netmask_eth2[0]` pour le premier alias déclaré sur eth2 ;

  `alias_network_eth2[1]` et `alias_netmask_eth2[1]` pour le deuxième alias déclaré sur eth2 ;

  [...]

Si le modèle de réseau ne correspond pas à des variables Creole, il faut ne pas spécifier le nom du module et les adresses.

On peut toutefois spécifier des adresses IP si elles sont identiques sur tous les serveurs.

Puis cliquer sur `Créer`.

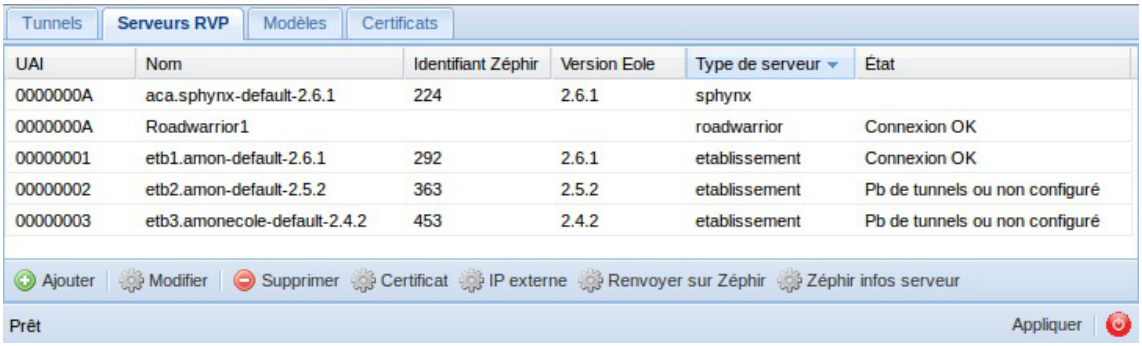
Si des modèles de sous réseau sont ajoutés, les valeurs correspondantes ne sont pas appliquées dans les serveurs RVP déjà existants dans la base ARV. Il faudra explicitement

> modifier chaque serveur dans l'onglet `Serveurs RVP` :
>
> - sélectionner un serveur ;
> - cliquer sur `Modifier` ;
> - cliquer sur `Recharger les valeurs du modèle`.
>
> Ce principe a été choisi pour pouvoir garder le contrôle des modifications.

Chapitre 4

Création d'un serveur RVP

La création d'un serveur est possible dans l'onglet Serveurs RVP.



Gestion des serveurs RVP

Selon le mode de connexion (compte Zéphir ou compte local) les informations présentes dans l'onglet varient. Avec le compte Zéphir l'identifiant Zéphir et la version d'EOLE apparaissent.

Pour créer un nouveau serveur RVP, il faut cliquer sur le bouton `Ajouter` dans l'onglet `Serveurs RVP`.

Il est possible de créer des serveurs RVP manuellement ou, si le serveur est enregistré sur le serveur Zéphir, de récupérer les informations depuis la base de données Zéphir.

Les renseignements d'un serveur RVP sont très importants et doivent être complétés en plusieurs étapes :

- Vérifier et renseigner les réseaux locaux utilisés, y compris sur Sphynx, ils ne sont pas tous renseignés automatiquement.
- Ajouter les certificats nécessaires à l'établissement des tunnels (auto-signés et signés par l'AC de Toulouse).
- Ajouter les adresses IP externes utilisées (y compris sur Sphynx).

La modification et la suppression d'un serveur RVP se fait en sélectionnant un serveur et en cliquant sur les boutons correspondants à l'action voulue.

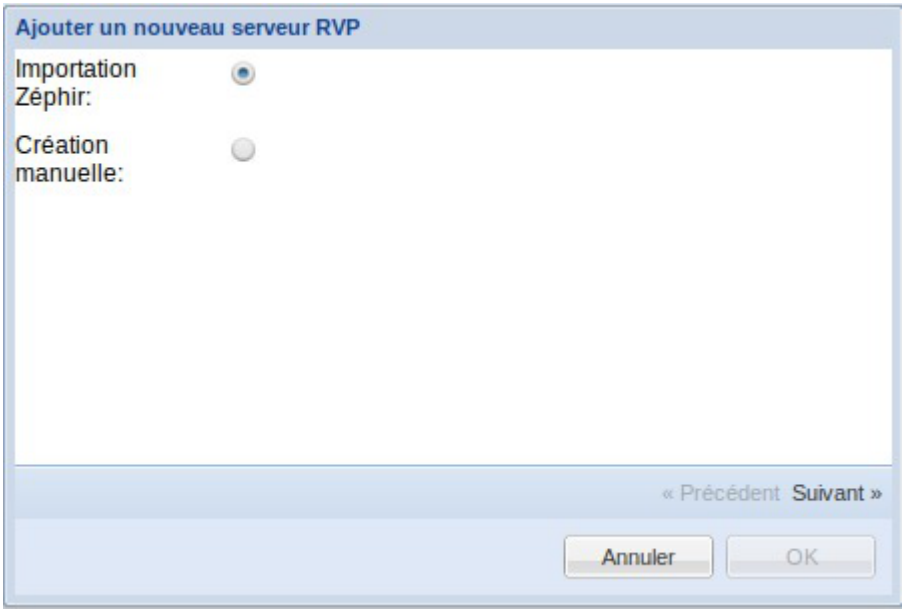
Toujours selon le mode de connexion (compte Zéphir ou compte local) les boutons `Renvoyer sur Zéphir` et `Zéphir infos serveur` sont disponibles ou grisés.

`Renvoyer sur Zéphir` permet de renvoyer une archive VPN déjà générée vers le serveur Zéphir.

`Zéphir infos serveur` permet de synchroniser l'identifiant Zéphir et la version d'EOLE d'un serveur créé manuellement. L'UAI et le nom dans ARV doivent correspondre à l'UAI et au libellé présent sur Zéphir.

1. Création manuelle d'un serveur RVP

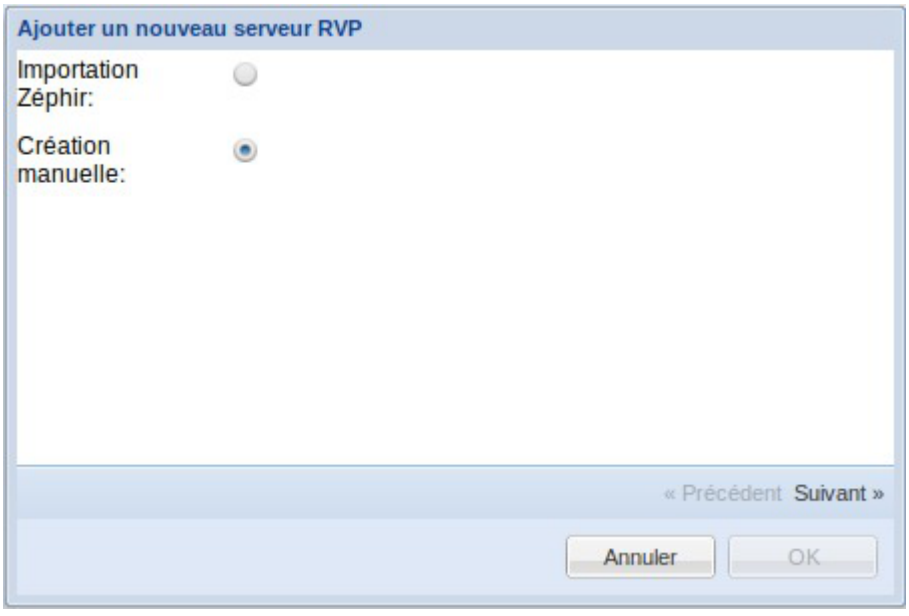
Dans le cas de la création manuelle du serveur RVP, il faut renseigner un nom, un identifiant (UAI, ex-RNE) et le type. Il existe deux types prédéfinis : Etablissement et Sphynx.



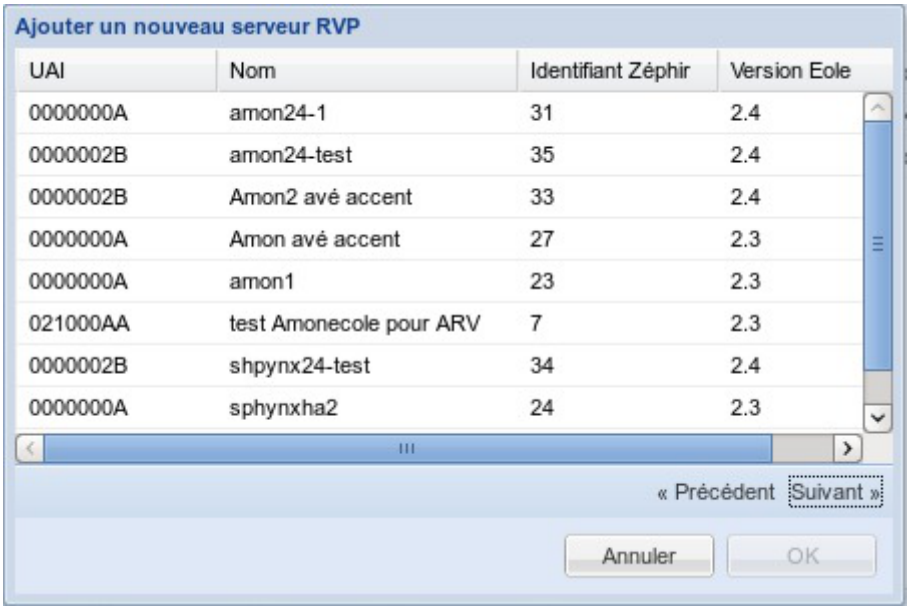
Configuration du concentrateur RVP manuelle

2. Création d'un serveur RVP par importation de Zéphir

Si ARV peut se connecter au serveur Zéphir, il est possible de rapatrier la liste des serveurs non présents dans ARV depuis la base de données Zéphir. Il suffit alors de sélectionner l'établissement à rapatrier.



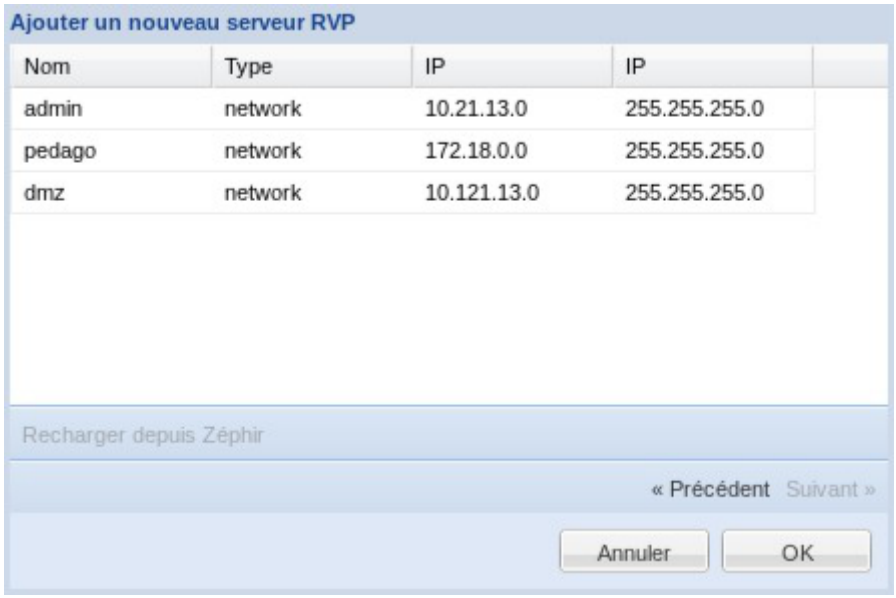
Ajouter un nouveau serveur RVP depuis Zéphir



Sélectionner un nouveau serveur RVP depuis Zéphir

Les valeurs correspondant aux variables indiquées dans le modèle de réseau local de l'établissement sont récupérées automatiquement sur Zéphir ainsi que l'identifiant Zéphir et la version d'EOLE.

Il sera possible de modifier un serveur RVP et de recharger les valeurs des variables depuis Zéphir.

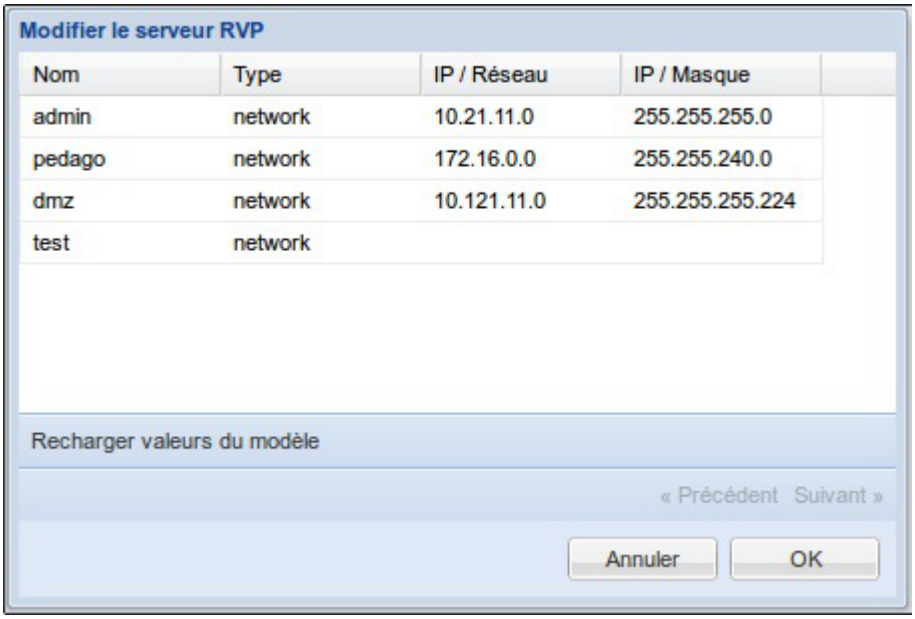


Les réseaux locaux sont automatiquement remplis en fonction du modèle défini

3. Création des réseaux locaux

Une fois le paramétrage du serveur RVP spécifié (par la méthode manuelle), il faut éventuellement renseigner les IP des réseaux locaux.

La liste des modèles de réseaux locaux est disponible dans la boite de dialogue suivante :



Spécification des IP des réseaux locaux du serveur RVP si le modèle de réseau local ne fait pas référence à des variables

Dans le cas où les réseaux locaux ne font pas référence à des variables Creole, il faut saisir les adresses IP manuellement.

Les adresses IP peuvent rester vides.

Un réseau non renseigné et non utilisé n'est pas bloquant.

Un réseau non renseigné utilisé dans un tunnel ne provoquera pas d'erreur dans ARV à la génération des bases ni de plantage de strongSwan. Le tunnel ne se montera pas et l'agent Zéphir du module Amon indiquera une erreur.

- Pour un modèle de type Réseau, la première colonne IP correspond à l'adresse réseau, la deuxième colonne correspond au masque de sous-réseau ;
- Pour un modèle de type Plage, la première colonne IP correspond à l'adresse du début de la plage, et la deuxième colonne correspond à l'adresse de fin de la plage ;
- Pour un modèle de type IP, la première colonne IP correspond à l'adresse de la machine, ne rien spécifier dans la deuxième colonne.

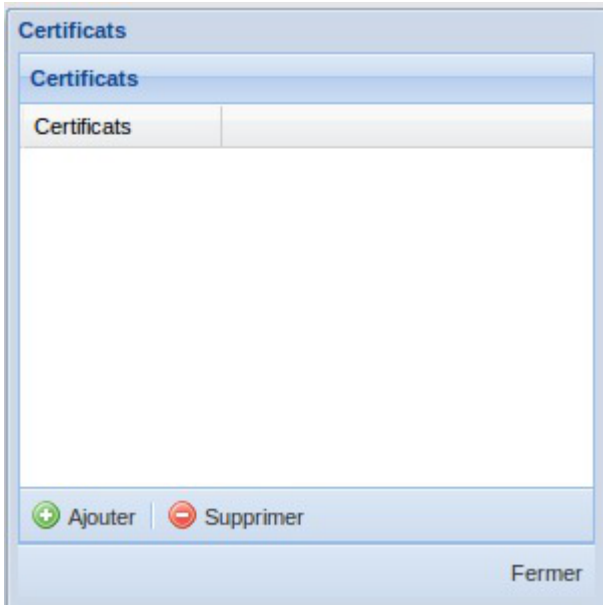
> Dans le cas de la méthode Zéphir, les adresses IP correspondant au modèle trouvées dans la base de données sont affichées. Ces adresses IP peuvent être modifiées à la création du réseau local. Si l'adresse IP est mise à jour dans Zéphir, la modification ne sera pas synchronisée avec ARV. Il est possible de les resynchroniser en cliquant sur `Recharger valeurs du modèle`.

4. Ajout des certificats

Il est nécessaire d'ajouter des certificats au serveur RVP.

Ce bouton permet d'ajouter des certificats au serveur RVP

Sélectionner le serveur RVP, cliquer sur Certificat puis sur Ajouter



Ajouter des certificats

Trois possibilités :

- vous possédez déjà les fichiers **clé privée** et **certificat** pour le serveur RVP, il faut ◉ Importer un certificat ;
- vous possédez un fichier au format PKCS12[p.46] qui contient le certificat et la clé privée, il faut ◉ Importer un fichier PKCS12 ;
- vous ne possédez pas de certificat pour le serveur RVP, il faut ◉ Générer un nouveau certificat

Importer un certificat

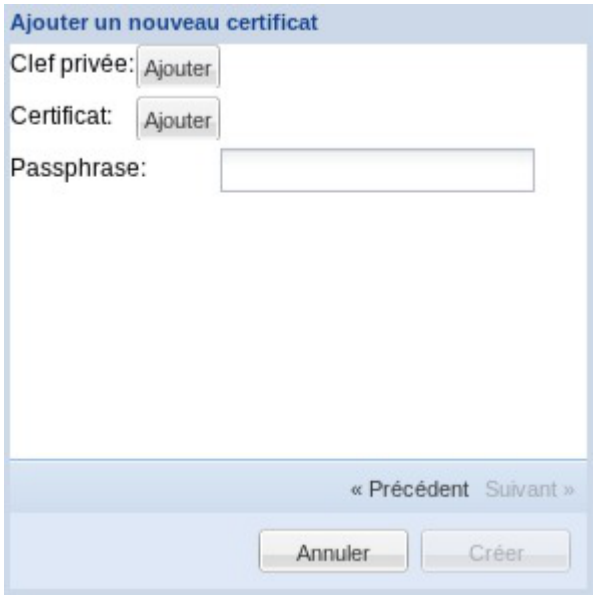
Importer un certificat

Pour importer un certificat, il faut ajouter la clé privée et le certificat du serveur signé par la CA (fichier avec l'extension `.pkcs7` ou `.p7`).

Le champ `Passphrase:` correspond au mot de passe qui protège la clé privée. Il n'est pas enregistré dans la base. Il permet d'extraire de la clé privée des informations nécessaires à la configuration.

Si il s'agit d'un certificat importé sur le serveur Sphynx-ARV, il servira à déchiffrer sa clé privée pour permettre l'activation du VPN.

Le mot de passe (phrase secrète) de la clé privée sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.



Importer une clé privée et un certificat un signé par la CA

Importer un fichier PKCS12

Cocher la case ◉ Importer un fichier PKCS12 pour insérer les fichiers certificat et clé privée dans la base ARV.

Importer un certificat PKCS12

Il reste à ajouter le fichier au format PKCS12 contenant le certificat ou toute la chaîne et la clé privée (fichier avec l'extension `.pkcs12` ou `.p12`).

Le mot de passe PKCS12 est celui qui a été utilisé pour générer le fichier PKCS12. Il permet d'extraire les certificats et la clé privée de ce fichier.des informations nécessaires à la configuration et de déchiffrer la clé privée du module Sphynx.

Le mot de passe permet de chiffrer la clé privée. Il sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.

Importer un certificat PKCS12 - Formulaire rempli

Générer un nouveau certificat

Cocher la case ◉ Générer un nouveau certificat pour utiliser des certificats autosignés ou créer un fichier de requête de certificat à fournir à une IGC.

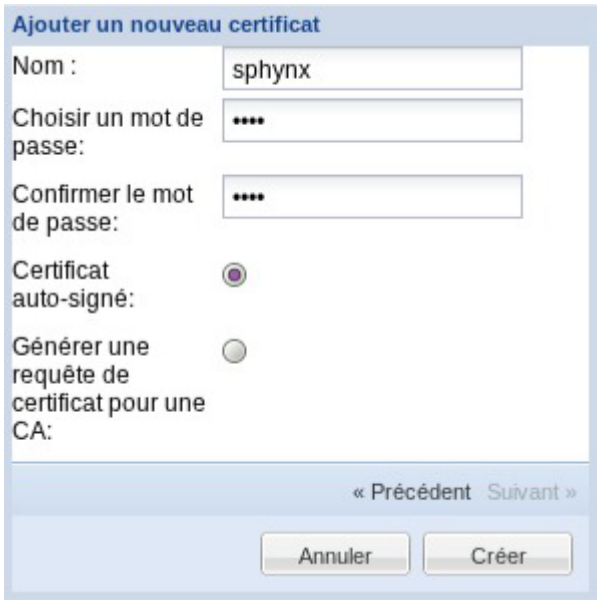
Générer un certificat autosigné ou importer les fichiers

Vous pouvez générer :

◉ Certificat auto-signé ;

◉ Générer une requête de certificat pour une CA externe.

Le fonctionnement en mode certificats auto-signés est un mode PKI mais avec une AC[p.46] (ou CA[p.46]) locale (sur Sphynx-ARV) qui signe le certificat généré.



Générer un certificat autosigné

Pour plus d'information sur l'option ◉ Générer une requête de certificat pour une CA externe il faut se référer à la partie de la documentation qui concerne la requête de certificat auprès de le l'IGC.

Voir aussi...

Requête de certificat auprès de l'IGC [p.26]

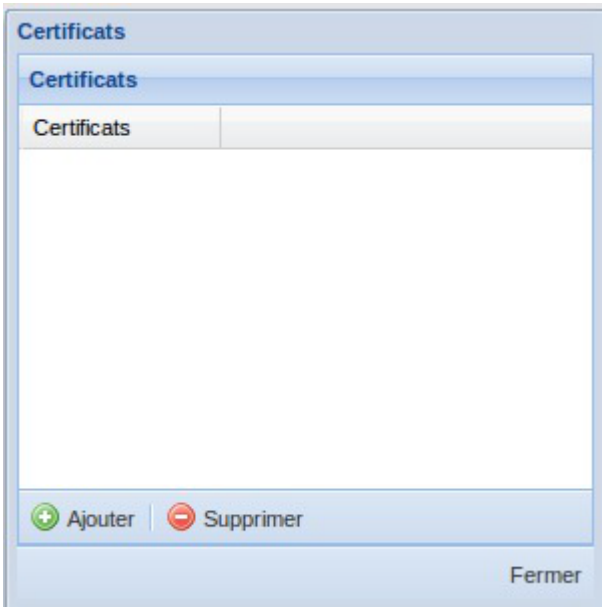
5. Requête de certificat auprès de l'IGC

Générer une requête de certificat pour une CA[p.46] génère une archive contenant la requête à envoyer à l'IGC[p.47].

Il faut se rendre dans l'onglet Serveurs RVP, sélectionner un serveur et enfin cliquer en bas sur le bouton Certificat.

Ce bouton permet d'ajouter des certificats au serveur RVP

Une fenêtre surgissante s'ouvre, cliquer alors sur le bouton Ajouter.



Ajouter des certificats

Choisir alors ◉ Générer un nouveau certificat et cliquer le bouton Suivant.

Générer un certificat autosigné ou importer les fichiers

Remplir les différents champs et sélectionner ◉ Générer une requête de certificat pour une CA .

La valeur du champ `Nom` est utilisée telle quelle dans le CN[p.46] du certificat.

Dans le cas où la PKI PNCN est utilisée, que la valeur du champ `Nom` soit saisie avec ou sans suffixe DNS, le CN sera forcé avec le suffixe saisi dans les paramètres de l'onglet `Général` de l'interface de configuration du module.

Exemples avec un suffixe ac-test.fr

Nom saisi	CN généré
certif	certif.ac-test.fr
certif.ac-test.fr	certif.ac-test.fr
certif.ac-test.fr.toto	certif.ac-test.fr.toto.ac-test.fr

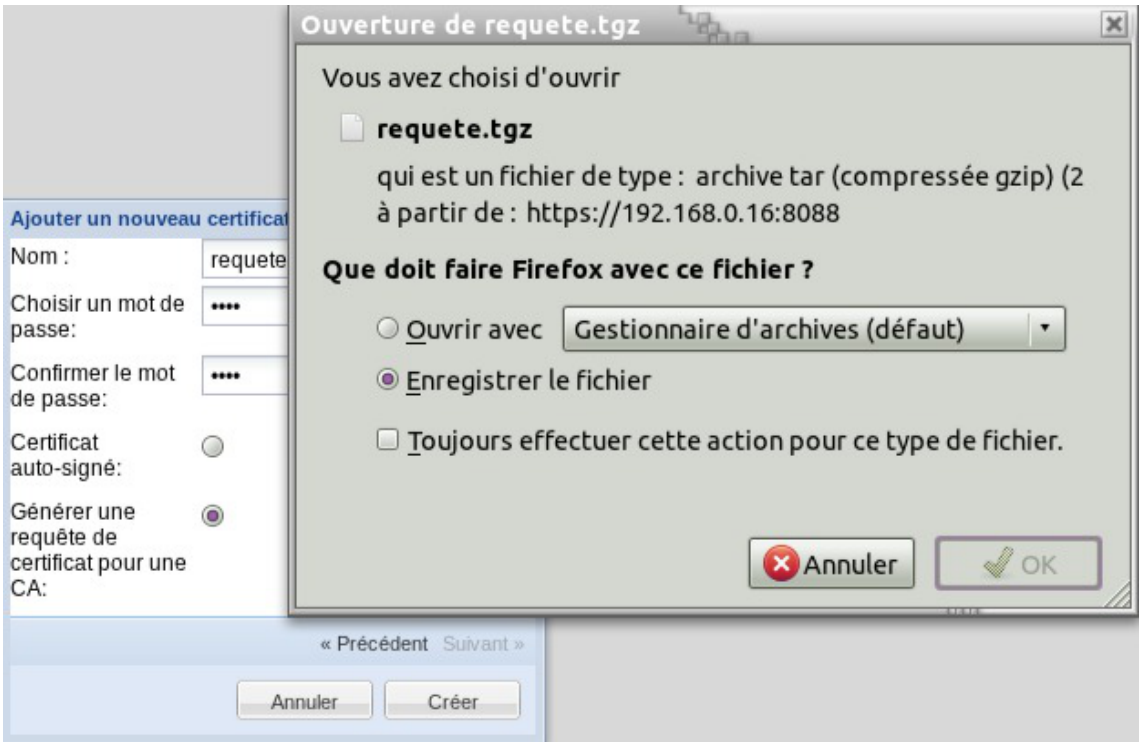
Valider en cliquant sur `Créer`.

Pensez à mémoriser le mot de passe (phrase secrète).

Le navigateur vous propose de télécharger une archive.

Elle contient la requête ainsi que la clé privée qui est associée au futur certificat signé par la CA.

Conserver précieusement cette archive, elle vous sera nécessaire pour un renouvellement de certificat.



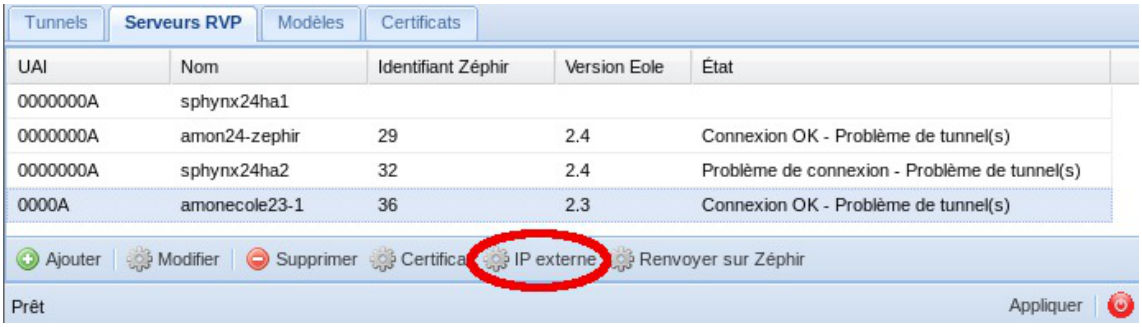
Requête de certificat à envoyer à l'IGC

Seul le fichier portant l'extension `.p10` est à envoyer à l'IGC après l'avoir extrait de l'archive.

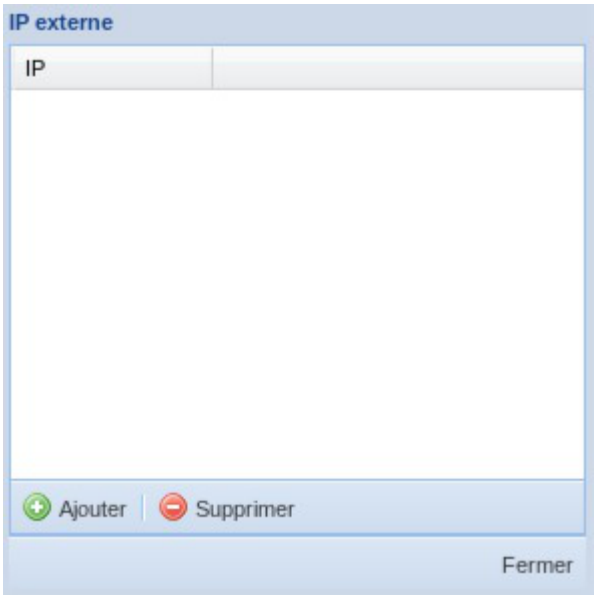
Il faudra par la suite importer la clé privée de cette archive ainsi que le certificat signé et renvoyé par l'IGC.

6. IP externes des serveurs RVP

Il est nécessaire de renseigner l'IP externe d'un serveur RVP.



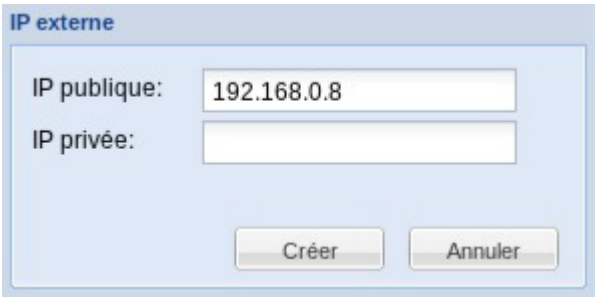
Il est possible de renseigner plusieurs IP externes (si IP aliasing).



L'IP publique est obligatoire. Elle concerne l'interface extérieure du module Amon.

Si le routeur est en bridge, il faut spécifier l'adresse IP attribuée à eth0 dans la zone `IP publique` et rien dans la zone `IP privée`.

Si votre routeur est en NAT, dans la zone `IP publique`, il faut spécifier l'adresse IP extérieure du routeur et dans la zone `IP privée`, l'adresse IP eth0 d'Amon.

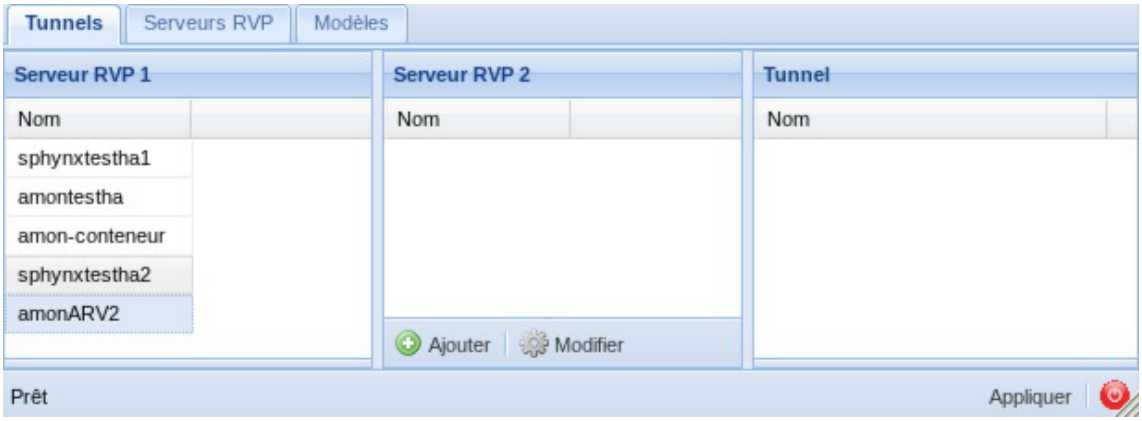


Chapitre 5

Création des tunnels

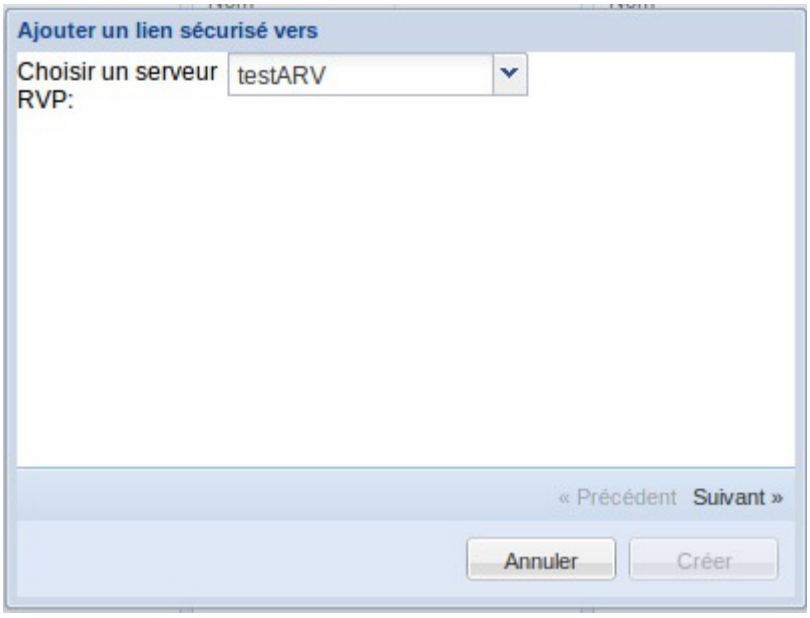
Création du lien sécurisé

La création de tunnels est possible entre deux serveurs RVP de même modèle (entre deux modules Amon ou deux modules Sphynx). La création des tunnels se fait dans l'onglet `Tunnels` de la fenêtre principale de l'application web.



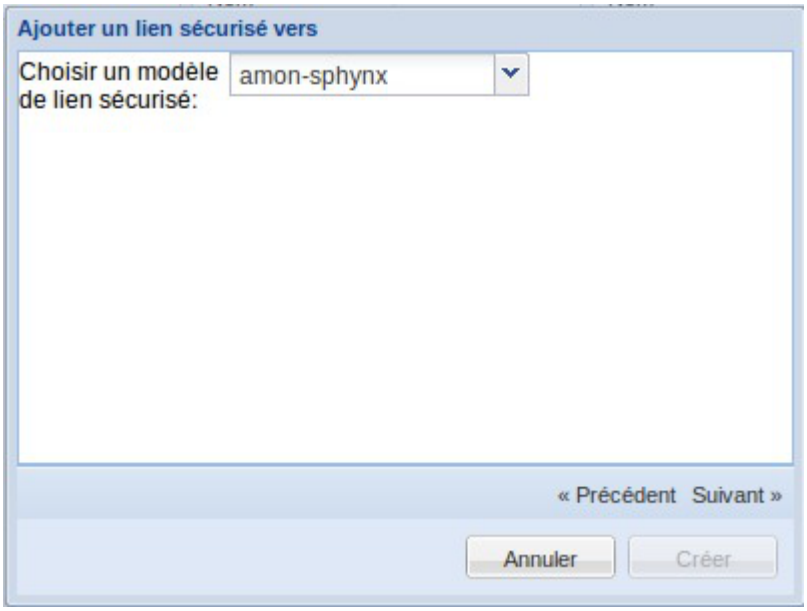
Fenêtre principale d'ARV avec l'onglet Tunnels

Pour pouvoir ajouter un tunnel entre deux réseaux locaux, il faut déjà créer un lien sécurisé entre deux serveurs RVP. Commencer par sélectionner le serveur RVP 1. Puis cliquer sur le bouton `Ajouter` de la colonne `Serveur RVP 2`. Choisir ensuite le serveur RVP 2 dans le menu déroulant suivant :



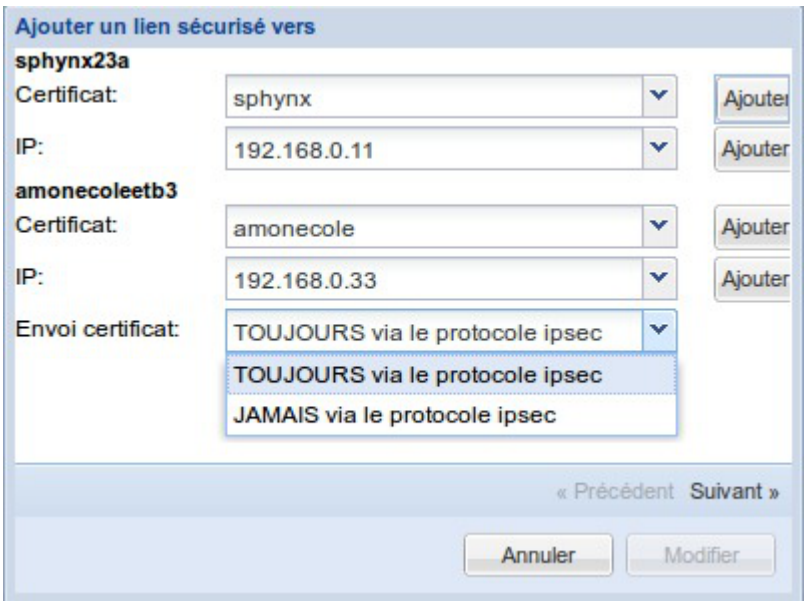
Choix du concentrateur RVP pour le lien sécurisé

Une fois les deux serveurs RVP sélectionnés, choisir le modèle de lien sécurisé voulu :



Choix du modèle de lien sécurisé

Puis choisir les IP et les certificats des deux serveurs RVP et la méthode d'envoi des certificats :



Choix des IP et certificats du lien sécurisé

Si besoin, ajouter l'IP et/ou un certificat d'un des deux serveurs RVP.

L'IP publique est obligatoire. Elle concerne à l'interface extérieure d'Amon (eth0).

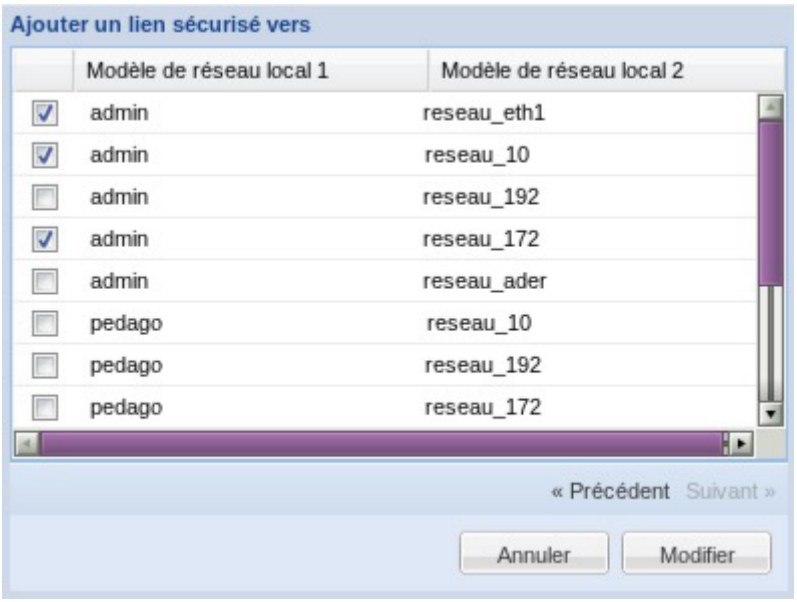
Si le routeur est en bridge, il faut spécifier l'adresse IP attribuée à eth0 dans la zone IP publique et rien dans la zone IP privée.

Si votre routeur est en NAT, dans la zone IP publique, il faut spécifier l'adresse IP extérieure du routeur et dans la zone IP privée, l'adresse IP eth0 d'Amon.

La méthode d'envoi du certificat pour la connexion choisi est celle du modèle utilisée. Il est possible de choisir une méthode différente pour chaque connexion.

Le protocole IKEv2 ne supporte la fragmentation des paquets réseaux, ne jamais envoyer le certificat via le protocole IPsec permet de réduire la taille des paquets.

Une fois le lien sécurisé paramétré, cocher les tunnels voulus (prédéfinis dans les modèles de liens et de tunnels).



Choix des tunnels

Gestion des translations

Si un réseau local possède le même adressage sur plusieurs Amon, il ne faut pas créer de tunnel mais utiliser un tunnel existant pour effectuer une translation. ARV n'implémente pas les translations dans un tunnel. Il faudra modifier le modèle ERA.

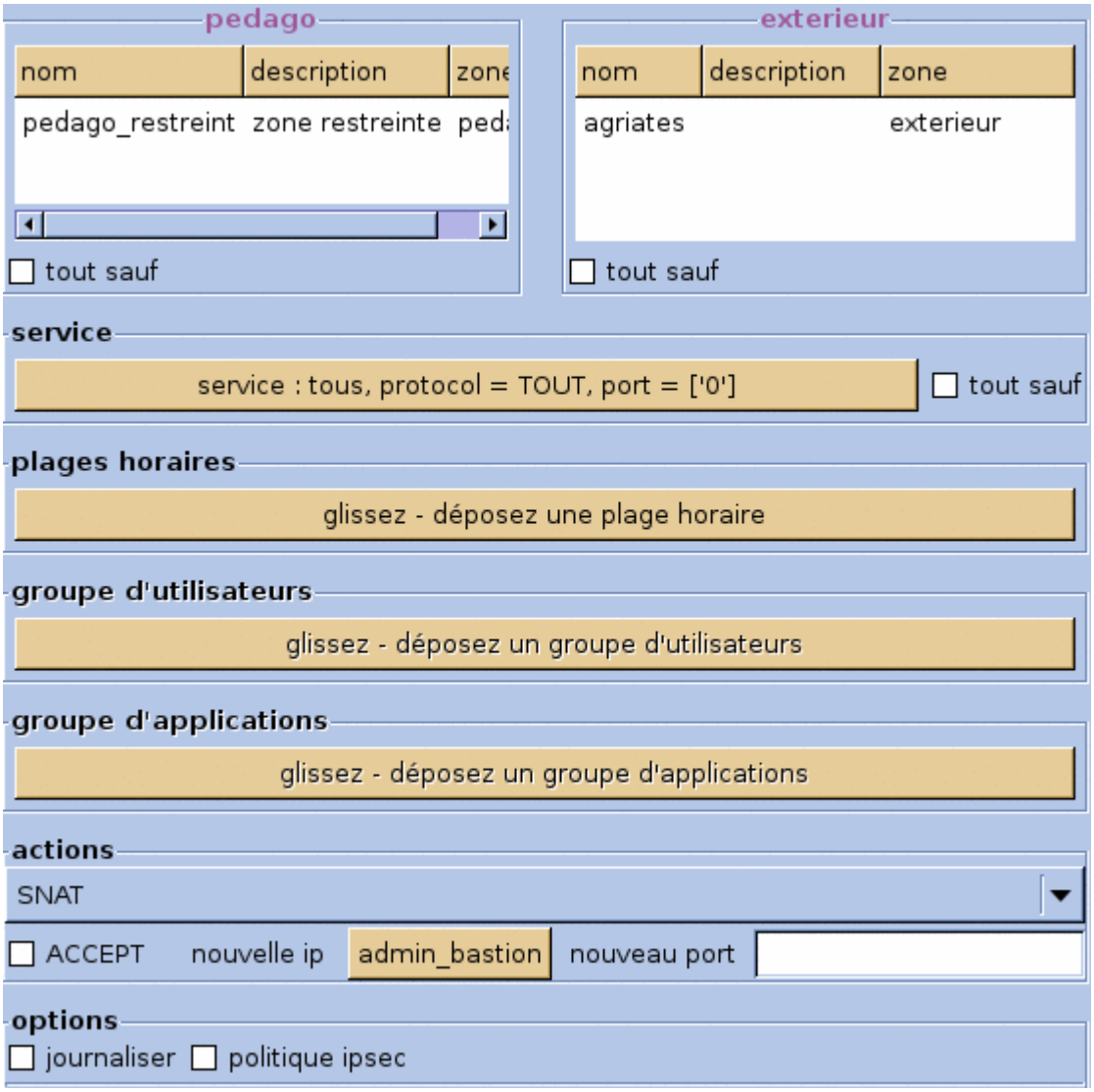
Par exemple :

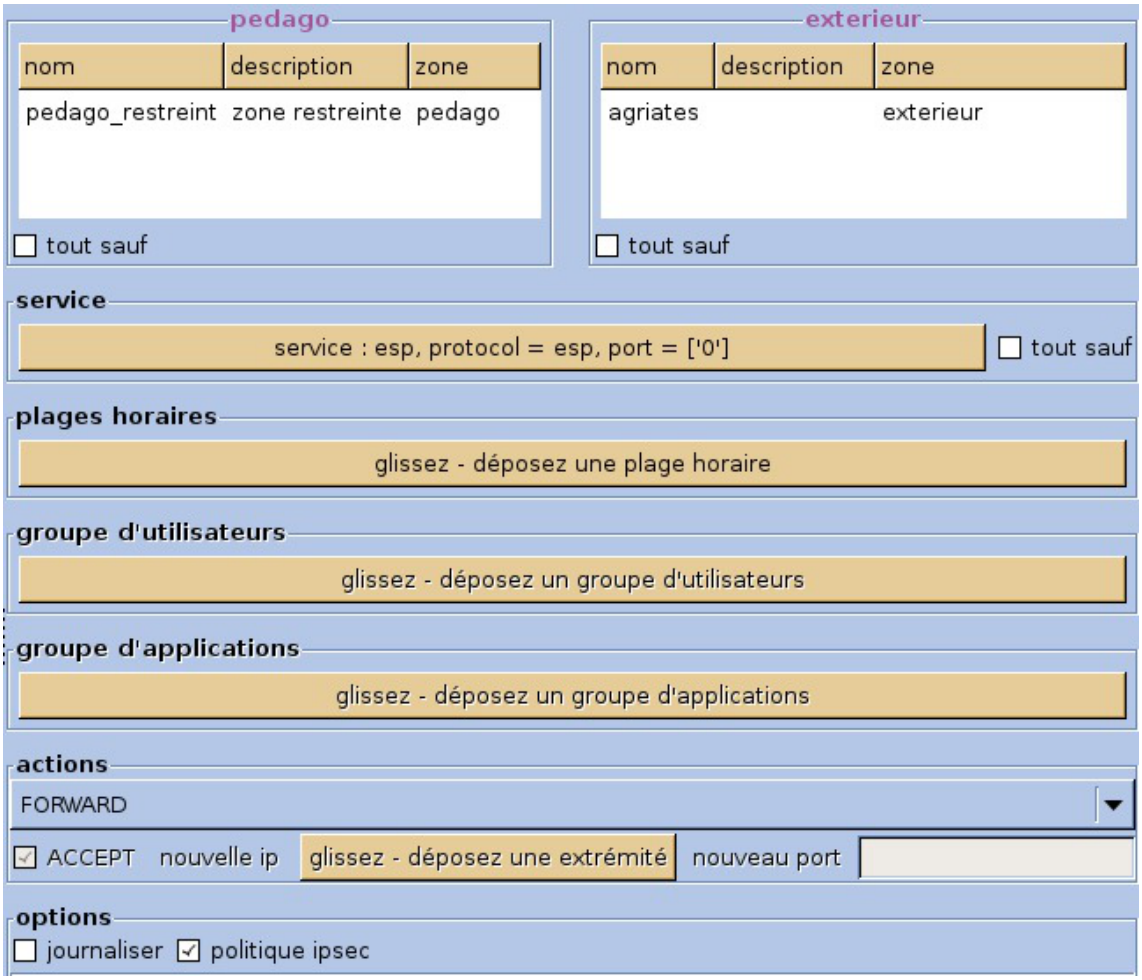
Si le réseau de l'interface eth2 est en 172.16.0.0/24 dans tous les établissements. Il sera impossible coté Sphynx d'établir des routes pour le même sous réseau vers plusieurs Amon. Il faudra donc translater ce réseau depuis l'Amon vers un tunnel existant.

On considère que le réseau eth1 (admin) est unique pour chaque Amon.

Il faut ensuite créer dans la zone `exterieur` les sous réseaux correspondant à l'intranet académique.

Les directives à ajouter dans ERA seront de ce type :





Il faudra ajouter autant de fois ces 2 directives que de réseaux de destination.

Ajout/Suppression d'un tunnel ou suppression de lien sécurisé

Pour supprimer ou modifier (ajout/suppression de tunnels) un lien sécurisé entre deux serveurs RVP, sélectionner le serveur RVP 1 et le serveur RVP 2 et cliquer sur `Modifier` dans la colonne `Serveur RVP 2` puis :

- Modification (ajout/suppression de tunnels) : Sélectionner le lien sécurisé à modifier et cliquer sur `Modifier`, cliquer sur `Suivant` et sélectionner ou désélectionner le/les tunnel(s).
- Suppression : Sélectionner le lien sécurisé à supprimer et cliquer sur `Supprimer`.

Chapitre 6

Génération des configurations IPsec

Opérations effectuées sur ARV

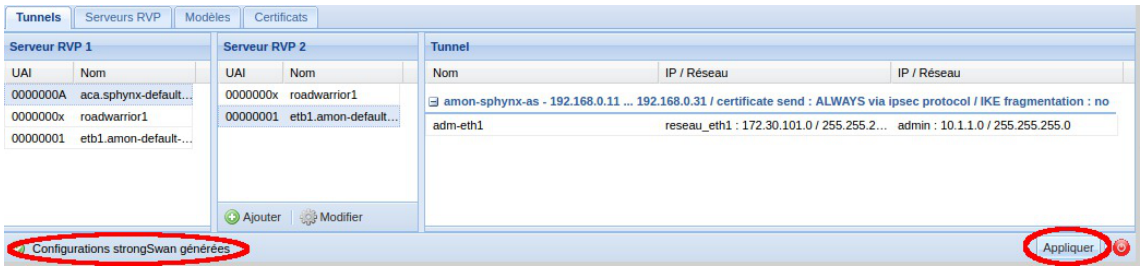
La génération des configurations IPsec pour strongSwan se fait en cliquant sur le bouton `Appliquer` en bas à droite de la fenêtre.

Quand les configurations strongSwan sont générées, la mention `Bases de données créées` ou `Configurations strongSwan générées` (selon le paramétrage du mode choisi dans l'onglet Rvp) s'affiche en bas à gauche de la fenêtre.

La configuration strongSwan du serveur Sphynx ARV est automatiquement mise à jour.

Les configurations strongSwan archivées des modules Amon et des modules Sphynx distants sont placées dans `/home/data/vpn/RNE/nom_serveur.tar.gz`.

Si on est connecté dans ARV avec un utilisateur Zéphir, les archives (Amon et Sphynx distants) sont également envoyées sur le module Zéphir.



Génération des configurations IPsec pour strongSwan

Chapitre 7

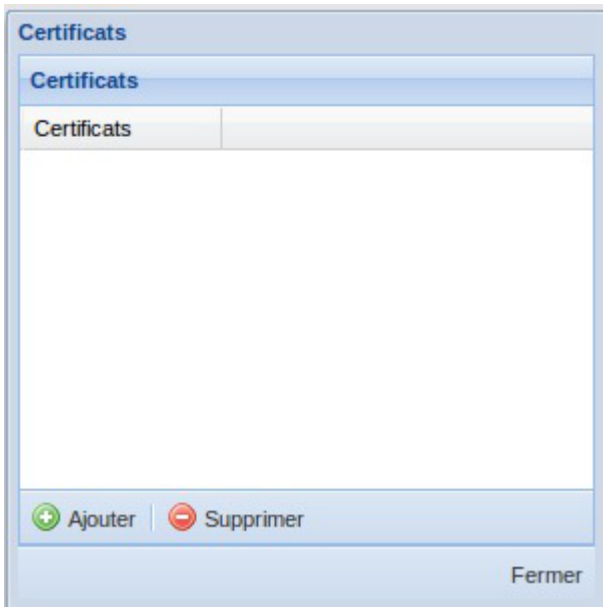
Gestion des certificats

1. Ajout des certificats

Il est nécessaire d'ajouter des certificats au serveur RVP.

Ce bouton permet d'ajouter des certificats au serveur RVP

Sélectionner le serveur RVP, cliquer sur Certificat puis sur Ajouter



Ajouter des certificats

Trois possibilités :

- vous possédez déjà les fichiers **clé privée** et **certificat** pour le serveur RVP, il faut ◉ Importer un certificat ;
- vous possédez un fichier au format PKCS12[p.46] qui contient le certificat et la clé privée, il faut ◉ Importer un fichier PKCS12 ;
- vous ne possédez pas de certificat pour le serveur RVP, il faut ◉ Générer un nouveau certificat

Importer un certificat

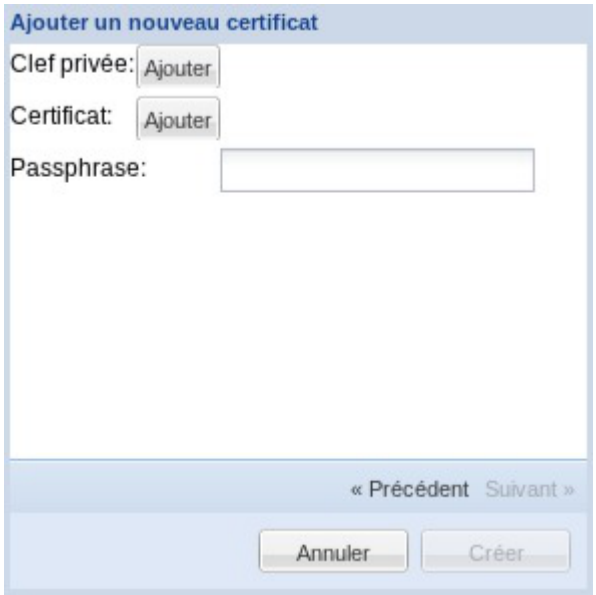
Importer un certificat

Pour importer un certificat, il faut ajouter la clé privée et le certificat du serveur signé par la CA (fichier avec l'extension `.pkcs7` ou `.p7`).

Le champ `Passphrase:` correspond au mot de passe qui protège la clé privée. Il n'est pas enregistré dans la base. Il permet d'extraire de la clé privée des informations nécessaires à la configuration.

Si il s'agit d'un certificat importé sur le serveur Sphynx-ARV, il servira à déchiffrer sa clé privée pour permettre l'activation du VPN.

Le mot de passe (phrase secrète) de la clé privée sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.



Importer une clé privée et un certificat un signé par la CA

Importer un fichier PKCS12

Cocher la case ◉ Importer un fichier PKCS12 pour insérer les fichiers certificat et clé privée dans la base ARV.

Importer un certificat PKCS12

Il reste à ajouter le fichier au format PKCS12 contenant le certificat ou toute la chaîne et la clé privée (fichier avec l'extension `.pkcs12` ou `.p12`).

Le mot de passe PKCS12 est celui qui a été utilisé pour générer le fichier PKCS12. Il permet d'extraire les certificats et la clé privée de ce fichier.des informations nécessaires à la configuration et de déchiffrer la clé privée du module Sphynx.

Le mot de passe permet de chiffrer la clé privée. Il sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.

Importer un certificat PKCS12 - Formulaire rempli

Générer un nouveau certificat

Cocher la case ◉ Générer un nouveau certificat pour utiliser des certificats autosignés ou créer un fichier de requête de certificat à fournir à une IGC.

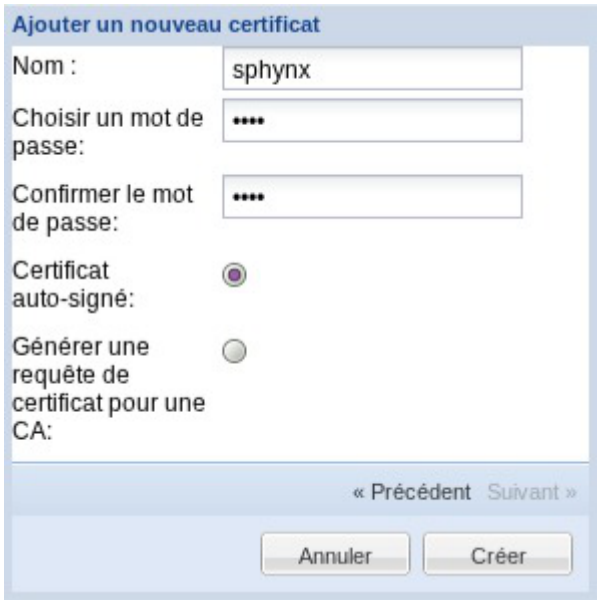
Générer un certificat autosigné ou importer les fichiers

Vous pouvez générer :

◉ Certificat auto-signé ;

◉ Générer une requête de certificat pour une CA externe.

Le fonctionnement en mode certificats auto-signés est un mode PKI mais avec une AC[p.46] (ou CA[p.46]) locale (sur Sphynx-ARV) qui signe le certificat généré.



Générer un certificat autosigné

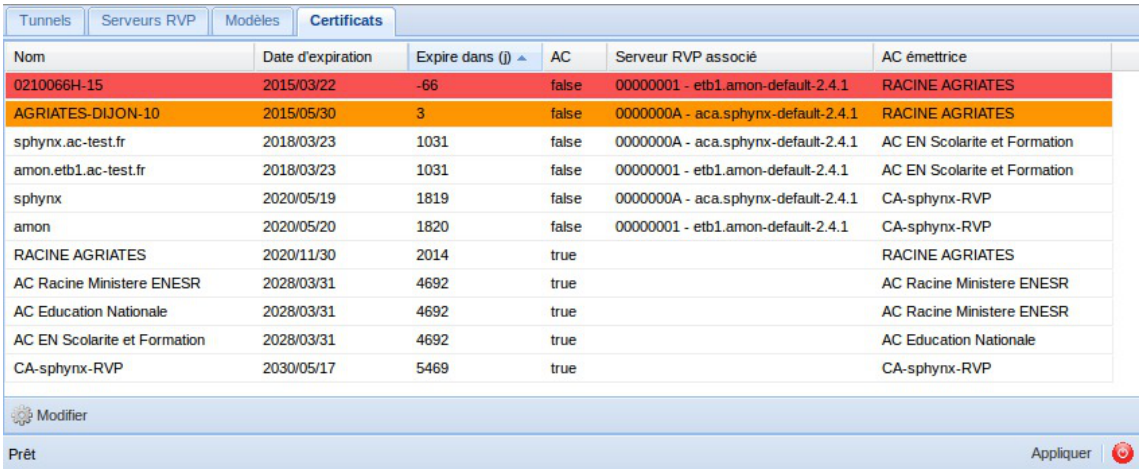
Pour plus d'information sur l'option ◉ Générer une requête de certificat pour une CA externe il faut se référer à la partie de la documentation qui concerne la requête de certificat auprès de le l'IGC.

Voir aussi...

Requête de certificat auprès de l'IGC [p.26]

2. Durée de vie d'un certificat

Les certificats sont utilisés par les serveurs Sphynx et Amon. Ces certificats délivrés par l'AC (Autorité de Certification) ont une durée de vie fixée à 5 ans pour les certificats RACINE[p.47]-AGRIATES[p.46].



Nom	Date d'expiration	Expire dans (j)	AC	Serveur RVP associé	AC émettrice
0210066H-15	2015/03/22	-66	false	00000001 - etb1.amon-default-2.4.1	RACINE AGRIATES
AGRIATES-DIJON-10	2015/05/30	3	false	0000000A - aca.sphynx-default-2.4.1	RACINE AGRIATES
sphynx.ac-test.fr	2018/03/23	1031	false	0000000A - aca.sphynx-default-2.4.1	AC EN Scolarite et Formation
amon.etb1.ac-test.fr	2018/03/23	1031	false	00000001 - etb1.amon-default-2.4.1	AC EN Scolarite et Formation
sphynx	2020/05/19	1819	false	0000000A - aca.sphynx-default-2.4.1	CA-sphynx-RVP
amon	2020/05/20	1820	false	00000001 - etb1.amon-default-2.4.1	CA-sphynx-RVP
RACINE AGRIATES	2020/11/30	2014	true		RACINE AGRIATES
AC Racine Ministere ENESR	2028/03/31	4692	true		AC Racine Ministere ENESR
AC Education Nationale	2028/03/31	4692	true		AC Racine Ministere ENESR
AC EN Scolarite et Formation	2028/03/31	4692	true		AC Education Nationale
CA-sphynx-RVP	2030/05/17	5469	true		CA-sphynx-RVP

Lorsqu'un certificat arrive en fin de vie, il est dit expiré et apparaît en rouge dans l'onglet `Certificats`.

Dans les 45 jours précédents son arrivée à expiration, il apparaît en orange.

La colonne `Serveur RVP associé` permet de savoir si un certificat est bien associé à un serveur RVP. Si ce n'est pas le cas, il s'agit d'une anomalie et le certificat peut être supprimé.

Les certificats de type CA (colonne CA à `true`) n'auront jamais de serveur RVP associé. Il ne doivent pas être supprimés.

3. Requête de certificat auprès de l'IGC

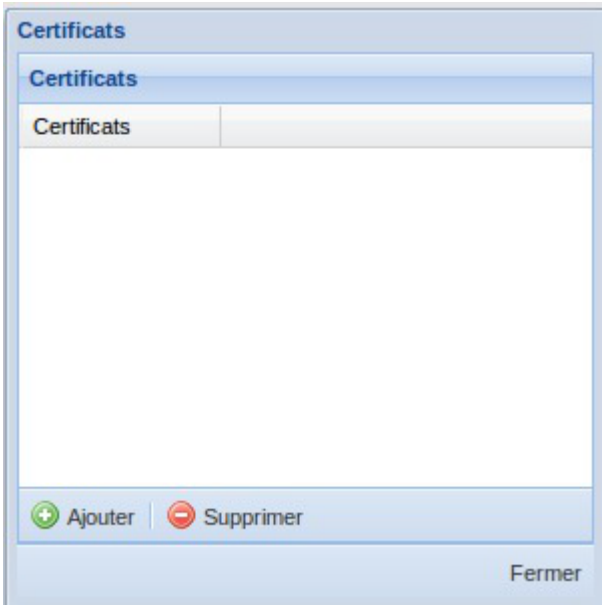
Générer une requête de certificat pour une CA[p.46] génère une archive contenant la requête à envoyer à l'IGC[p.47].

Il faut se rendre dans l'onglet `Serveurs RVP`, sélectionner un serveur et enfin cliquer en bas sur le bouton `Certificat`.

UAI	Nom	Identifiant Zéphir	Version Eole	État
0000000A	sphynx24ha1			
0000000A	amon24-zephir	29	2.4	Connexion OK - Problème de tunnel(s)
0000000A	sphynx24ha2	32	2.4	Problème de connexion - Problème de tunnel(s)
0000A	amonecole23-1	36	2.3	Connexion OK - Problème de tunnel(s)

Ce bouton permet d'ajouter des certificats au serveur RVP

Une fenêtre surgissante s'ouvre, cliquer alors sur le bouton `Ajouter`.



Ajouter des certificats

Choisir alors ◉ Générer un nouveau certificat et cliquer le bouton Suivant.

Générer un certificat autosigné ou importer les fichiers

Remplir les différents champs et sélectionner ◉ Générer une requête de certificat pour une CA.

La valeur du champ Nom est utilisée telle quelle dans le CN[p.46] du certificat.

Dans le cas où la PKI PNCN est utilisée, que la valeur du champ Nom soit saisie avec ou sans suffixe DNS, le CN sera forcé avec le suffixe saisi dans les paramètres de l'onglet Général de l'interface de configuration du module.

Exemples avec un suffixe ac-test.fr

Nom saisi	CN généré
certif	certif.ac-test.fr
certif.ac-test.fr	certif.ac-test.fr
certif.ac-test.fr.toto	certif.ac-test.fr.toto.ac-test.fr

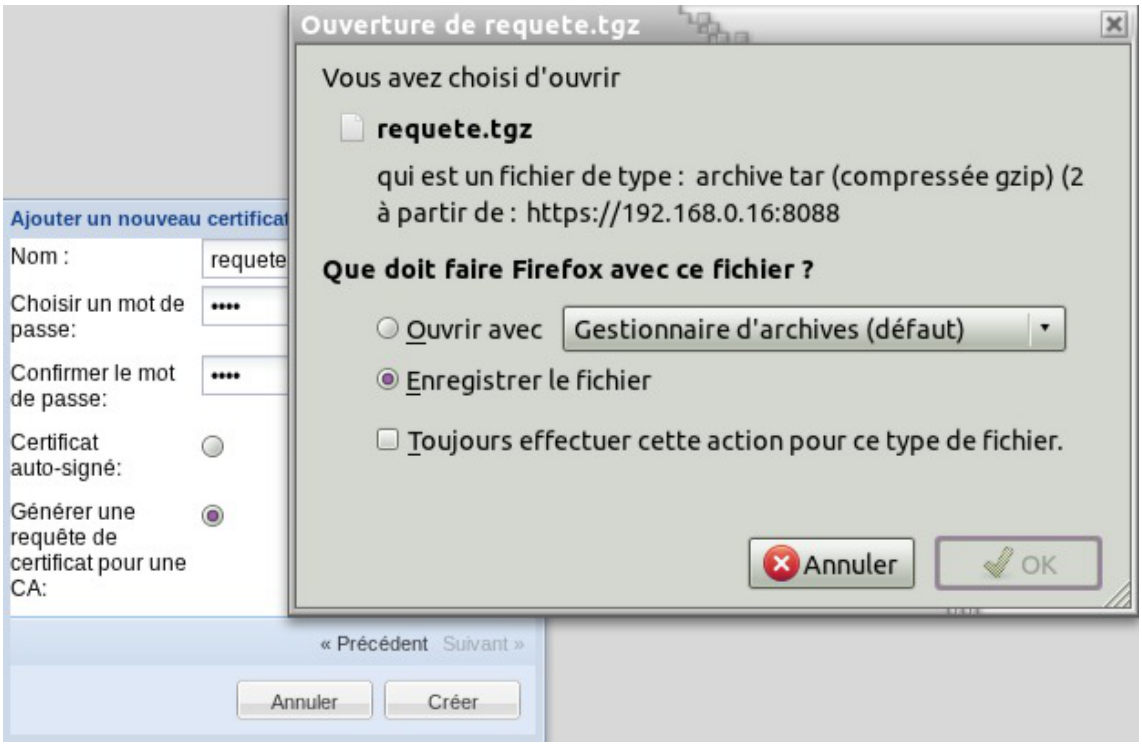
Valider en cliquant sur `Créer`.

Pensez à mémoriser le mot de passe (phrase secrète).

Le navigateur vous propose de télécharger une archive.

Elle contient la requête ainsi que la clé privée qui est associée au futur certificat signé par la CA.

Conserver précieusement cette archive, elle vous sera nécessaire pour un renouvellement de certificat.



Requête de certificat à envoyer à l'IGC

Seul le fichier portant l'extension `.p10` est à envoyer à l'IGC après l'avoir extrait de l'archive.

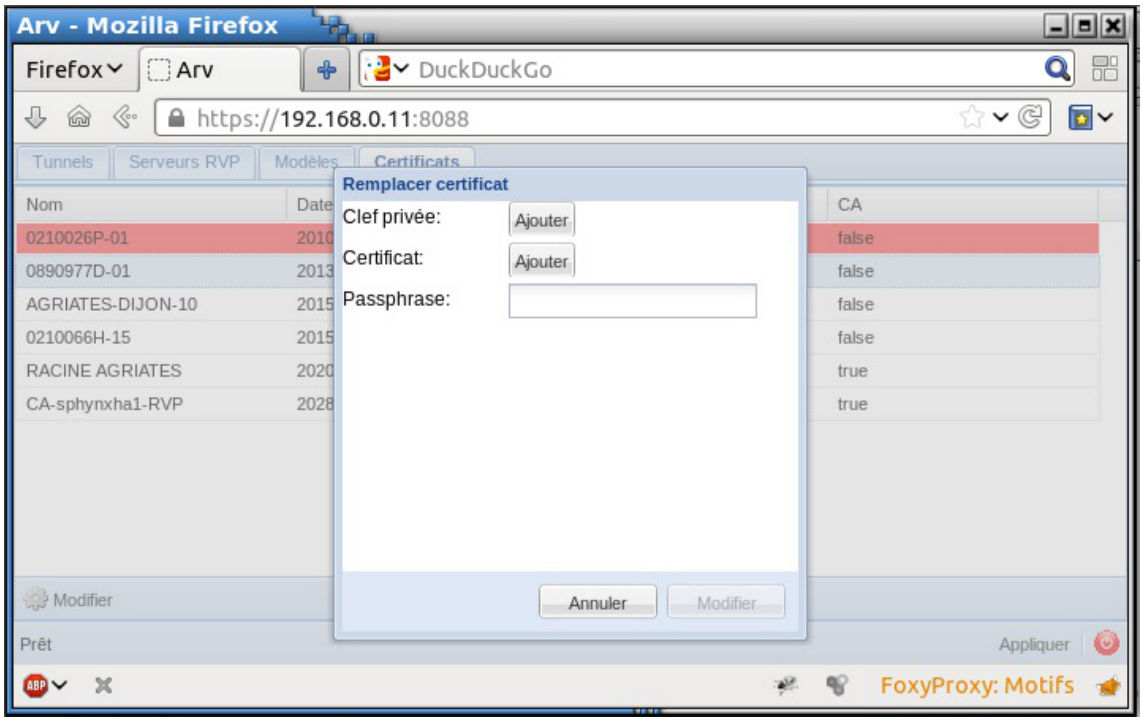
Il faudra par la suite importer la clé privée de cette archive ainsi que le certificat signé et renvoyé par l'IGC.

4. Prolongation d'un certificat existant

Pour prolonger la durée de vie du certificat il faut envoyer le fichier .p10 conservé dans l'archive de la requête précédente à l'IGC.

Une fois le certificat récupéré il faut le mettre à jour dans ARV.

Dans l'onglet `Certificats`, sélectionner le certificat concerné et cliquer sur le bouton `Modifier`



Dans la fenêtre surgissante :

- cliquer sur le bouton `Ajouter` de la ligne `Certificat` et choisir le nouveau fichier .pkcs7 renvoyé par l'IGC ;
- saisir le mot de passe dans le champs `Passphrase` ;
- cliquer sur `Modifier`.

La clé privé est conservée et le certificat est prolongé.

N'oubliez pas de refaire les configurations strongSwan dans ARV en cliquant sur le bouton `Appliquer`.

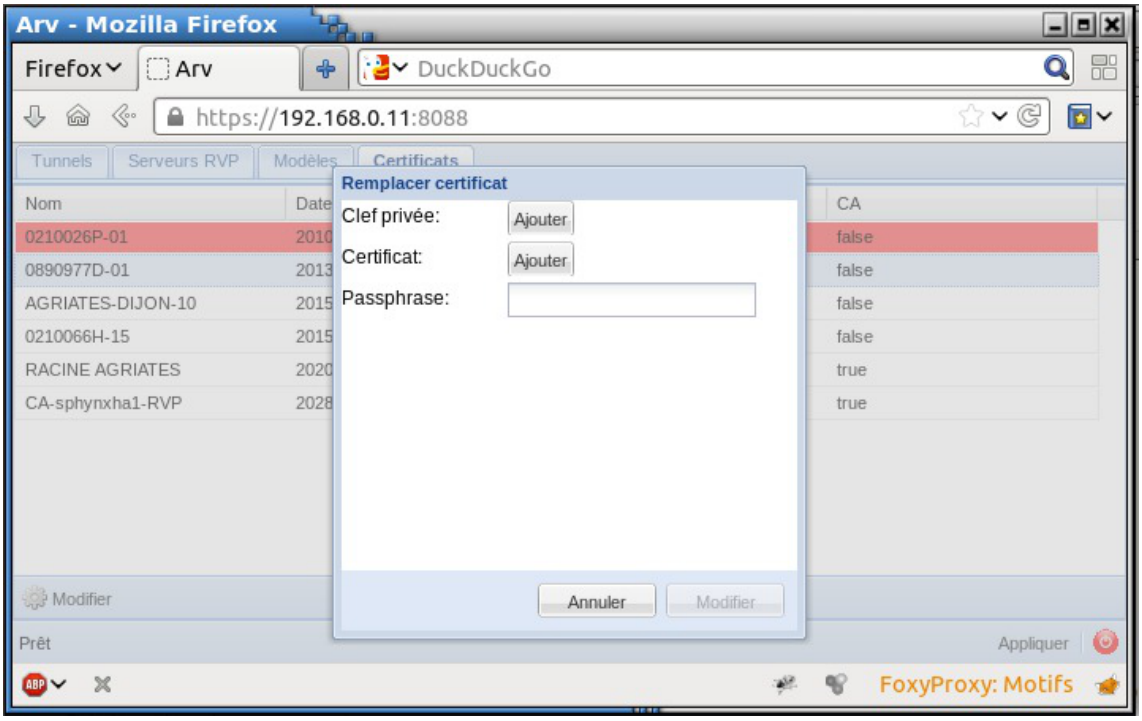
5. Remplacement d'un certificat existant

Pour remplacer un certificat il faut préalablement avoir fait une requête à l'IGC.

Dans l'archive issue de la requête à l'IGC se trouve la clé privée qu'il faut extraire.

Une fois le certificat récupéré auprès de l'IGC il faut mettre à jour dans ARV, le certificat et la clé privée.

Dans l'onglet `Certificats`, sélectionner le certificat concerné et cliquer sur le bouton `Modifier`.



Dans la fenêtre surgissante :

- cliquer sur le bouton Ajouter de la ligne Clef privée et choisir le fichier .pem extrait de l'archive ;
- cliquer sur le bouton Ajouter de la ligne `Certificat` et choisir le nouveau fichier .pkcs7 renvoyé par l'IGC ;
- saisir le mot de passe dans le champs `Passphrase` ;
- cliquer sur Modifier.

Le certificat et la clé privé sont remplacés.

N'oubliez pas de refaire les configurations strongSwan dans ARV en cliquant sur le bouton Appliquer.

Chapitre 8
Questions fréquentes propres à ARV

Pas de question fréquente pour le moment.

Glossaire

AGRIATES *= Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires*	De responsabilité partagée entre les collectivités locales et les académies, ces réseaux de concentration des établissements scolaires couvrent à ce jour l'ensemble de lycées et collèges et devraient s'étendre aux secteurs du primaire. L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE. Par extension, les applications AGRIATES sont les applications Intranet accessibles aux établissements connectés au réseau AGRIATES, à savoir essentiellement, mais pas uniquement, les applications internet à usage des services administratifs des établissements. RACINE-AGRIATES a pour objectif la fourniture d'un support sécurisé pour les échanges d'information (VPN) entre le réseau de l'administration des établissement et leur rectorat de rattachement. L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE. http://www.igc.education.fr/agriates/agriates.htm C'est à la fois une zone de confiance sur le réseau des rectorats et un ensemble de contraintes techniques auxquelles doivent répondre les dispositifs d'accès des établissements. RACINE-AGRIATES fait partie du projet réseau RACINE, dont l'objectif consiste à fournir un support sécurisé pour les échanges d'information (ou Réseau Virtuel Privé (RVP)) entre entités du ministère en s'appuyant sur des infrastructures réseau ouvertes. RACINE-AGRIATES a ainsi pour objectif la fourniture d'un support sécurisé pour les échanges d'information (RVP) entre le réseau de l'administration des établissements et leur rectorat de rattachement. RACINE-AGRIATES rassemble dans une même "zone de confiance" académique les établissements scolaires et les services académiques. Ce nouveau réseau privé virtuel sécurisé est l'Intranet académique.
ARV *= Administration de Réseaux Virtuels*	ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan. http://www.strongswan.org/
Autorité de Certification *= CA : Certification Authority*	AC est l'acronyme de Autorité de Certification. Une autorité de certification est une société ou un service administratif chargé de créer, de délivrer et de gérer des certificats électroniques.
CN *= Common Name*	Valeur permettant d'identifier le serveur dans le certificat.

PKCS12 *= Public Key Cryptographic Standards*	Utilisé pour signer et/ou chiffrer des messages dans le cadre d'une infrastructure à clés publiques. Sert également à la transmission de certificats. Source : http://fr.wikipedia.org/wiki/Public_Key_Cryptographic_Standards
PKI *= Public Key Infrastructure*	Une infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC) ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériel type HSM ou encore des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques. Une infrastructure à clés publiques délivre un ensemble de services pour le compte de ses utilisateurs. En résumé, ces services sont les suivants : • enregistrement des utilisateurs (ou équipement informatique) ; • génération de certificats ; • renouvellement de certificats ; • révocation de certificats ; • publication de certificats ; • publication des listes de révocation (comprenant la liste des certificats révoqués) ; • identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'ICP) ; • archivage, séquestre et recouvrement des certificats (option). Source de la définition : http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_public
RACINE *= Réseaux d'Accès et de Consolidation des INtranets de l'Éducation nationale*	Les réseaux RACINE (Réseaux d'Accès et de Consolidation des INtranets de l'Éducation nationale) sont des réseaux privés virtuels (RPV) qui ont pour objet d'offrir et garantir un environnement d'accès sécurisé aux systèmes d'information de l'Éducation nationale pour toute communauté d'utilisateurs " ayant droit " quel que soit le lieu où les utilisateurs exercent leurs activités professionnelles. http://www.igc.education.fr/IGC/IGC.htm L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE.
Réseau virtuel Privé *= RVP ou VPN (Virtual Private Network) en anglais*	Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.

strongSwan	strongSwan est une implémentation libre et complète de VPN IPsec pour le système d'exploitation Linux (noyaux Linux 2.6 et 3.x). L'objectif de ce projet est de proposer des mécanismes d'authentification forts. http://www.strongswan.org/