ARV : Administration de Réseau Virtuel

EOLE 2.5



création : Mai 2015 Version : révision : Avril 2018 Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

EOLE 2.5

révision : Avril 2018
création : Mai 2015
Pôle national de compétences Logiciels Libres
Équipe EOLE
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)
Cette documentation, rédigée par le Pôle national de compétences Logiciels Libres, est mise à disposition selon les termes de la licence :
Creative Commons Attribution - Partage dans les Mêmes Conditions 3.0 France (CC BY-SA 3.0 FR) : http://creativecommons.org/licenses/by-sa/3.0/fr/.
Vous êtes libres :
 de reproduire, distribuer et communiquer cette création au public ;
de modifier cette création.
Selon les conditions suivantes :
• Attribution : vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur

- de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggèrerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre);
 Partage des Conditions Initiales à l'Identique : si vous modifiez, transformez ou adaptez
- cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

À chaque réutilisation ou distribution de cette création, vous devez faire apparaître clairement au public les conditions contractuelles de sa mise à disposition. La meilleure manière de les indiquer est un lien vers cette page web.

Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits sur cette œuvre.

Rien dans ce contrat ne diminue ou ne restreint le droit moral de l'auteur ou des auteurs.

Cette documentation est basée sur une réalisation du Pôle national de compétences Logiciels Libres. Les documents d'origines sont disponibles sur le site.

EOLE est un projet libre (Licence GPL).

Il est développé par le Pôle national de compétences Logiciels Libres du ministère de l'Éducation nationale, rattaché à la Direction des Systèmes d'Information de l'académie de Dijon (DSI).

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	4
Chapitre 2 - Présentation de l'interface	8
Chapitre 3 - Modèles ARV	11
Chapitre 4 - Création d'un serveur RVP	18
1. Création manuelle d'un serveur RVP	19
2. Création d'un serveur RVP par importation de Zéphir	19
3. Création des réseaux locaux	20
4. Ajout des certificats	21
5. Requête de certificat auprès de l'IGC	26
6. IP externes des serveurs RVP	28
Chapitre 5 - Création des tunnels	30
Chapitre 6 - Génération des configurations IPsec	35
Chapitre 7 - Gestion des certificats	36
1. Ajout des certificats	36
2. Durée de vie d'un certificat	40
3. Requête de certificat auprès de l'IGC	40
4. Prolongation d'un certificat existant	43
5. Remplacement d'un certificat existant	43
Chapitre 8 - Questions fréquentes propres à ARV	45
Glossaire	46

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.





A 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



Schéma de la base de données

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 : <u>https://<IP Sphynx>:8088</u> Elle nécessite une authentification.

Tunnels Serveurs	RVP Modé	èles	
Serveur RVP 1		Serveur RVP 2	Tunnel
Nom		Nom	Nom
	Auth	entification	
	Uti	ilisateur:	Connexion
	Ean	âtra d'authantification d'A	DV

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.



L'utilisation d'un compte Zéphir permet :

• de gérer les tunnels ;

- A

- 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 (<u>root</u> et <u>eole</u> 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.

Arv - Mozilla Firefox	_ = ×
Firefox - Arv + Carve DuckDuckGo	Q =:
	☆ ~ @ ⊠~
Tunnels Serveurs RVP Modèles Certificats	
UAI A T Nom	État
0000000A sphynxha1	Tunnels OK
000000A amon1	Tunnels OK
🔾 Ajouter 🔅 Modifier 🤤 Supprimer 🎲 Certificat 🎲 IP externe 🌼 Renvoyer sur Zéphir	
https://192.168.0.11:8088/#	Appliquer 🥹
🐵 🗸 🦋 😵 Foxyl	Proxy: Motifs 🏾 🎓

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

A0000000	A ↓ Tri croissant		
A0000000	Z↓ Z↓ Tri décroissant		
	Filters	aa 00	

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



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.

Tunnels Serveurs RV	/P Modèles	Certificats							
Modèle de lien sécurisé		Auto	rité de Certificatio	on			Modèle de ré	seau	
Nom	Envoi certificat	AC I	EN Scolarit	te et Formati	ion		Nom	Туре	Modèle de serveur RVP
OLD_PKI_amon-sphynx	always	Mode	ele de serveur RVI	P1 Mo	dèle de	serveur RVP 2	reseau_eth1	network	Sphynx
amon-sphynx	always	Etal	blissement	Sp	hynx		reseau_10	network	Sphynx
		Modè	èle de tunnel				reseau_192	network	Sphynx
		Nom		Modèle de réseau	local 1	Modèle de réseau local 2	reseau_172	network	Sphynx
		admir	n-reseau eth1	admin		reseau eth1	reseau_ader	network	Sphynx
		admir	n-reseau10	admin		reseau_10	admin	network	Etablissement
		admir	n-reseau192	admin		reseau_192	pedago	network	Etablissement
		admir	n-reseau172	admin		reseau_172	dmz	network	Etablissement
		admir	n-reseau_ader	admin		reseau_ader			
		peda	go-reseau10	pedago		reseau_10			
		peda	go-reseau192	pedago		reseau_192			
		peda	go-reseau172	pedago		reseau_172			
		peda	go-reseau_ader	pedago		reseau_ader			
 Ajouter Supprim 	er	() A	jouter 🛛 🎲 Modifie	er 🛛 🥥 Supprimer			Modifier	Supprimer	
Prêt									Appliquer 🧿

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.

Ajouter un nouveau	modèle de lien sécurisé
Nom :	amon-sphynx
	« Précédent Suivant »
	Annuler Créer

Nom du modèle de lien sécurisé

Choisir ensuite un modèle de serveur RVP source.

Ajouter un nouveau modèle de lien sécurisé
Modèle de concentrateur RVP
Sphynx
Etablissement
Q Ajouter Q Supprimer
« Précédent Suivant »
Annuler

Modèle de concentrateur RVP source

Et le modèle de serveur RVP de destination.

Ajouter un nouveau moc	lèle de lien sécurisé
Modèle de serveur RVP	
Sphynx	
Etablissement	
🗿 Ajouter 🛛 🤤 Supprin	ner
	« Précédent Suivant »
(Annuler Créer

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.

Ajouter un nou RVP	iveau n	nodèle de s	erveur 🗙
Nouveau nor	n:		
Collectivit	é		
0	к	Annuler	

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.

Sélectionner une autorité de certification:	RACINE AGR	Ajouter
Certificat envoyé	TOUJOURS via le pro	otocole ips 💙
Certificat envoyé	TOUJOURS via le pro	otocole ipsec
Certificat envoyé	JAMAIS via le protoco	l ipsec
	« Précéd	ent Suivant

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 <u>child</u> lié à une <u>connexion</u> à l'exécution de la commande ipsec statusall.

Nom :	admin_eth1				
Nom du modèle du réseau local pour Etablissement:	admin	*	Modifier	Ajouter	Suppr
Nom du modèle du réseau local pour Sphynx:	reseau_eth1	~	Modifier	Ajouter	Suppr
			Annuler		réer

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.

Nom :	eth1-admin				
Nom du modèle du réseau local pour Sphynx:	reseau_eth1	~	Modifier	Ajouter	Suppr.
Nom du modèle du réseau local pour Etablissement:	admin	~	Modifier	Ajouter	Suppr.
		_			

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

Modèle de lien sécurisé		Autorité de Certificati	on		Modèle de réseau		
Nom	Envoi certificat	AC EN Scolari	te et Formatio	n	Nom	Туре	Modèle de serveur R
OLD_PKI_amon-sphynx	always	Modèle de serveur RV	P1 Modè	le de serveur RVP 2	reseau_eth1	network	Sphynx
amon-sphynx	always	Etablissement	Sph	nx	reseau_10	network	Sphynx
		Modèle de tunnel			reseau_192	network	Sphynx
		Nom	Modèle de réseau lo	cal 1 Modèle de réseau local 2	reseau_172	network	Sphynx
		admin-reseau eth1	admin	reseau eth1	reseau_ader	network	Sphynx
		admin-reseau10	admin	reseau_10	admin	network	Etablissement
		admin-reseau192	admin	reseau_192	pedago	network	Etablissement
		admin-reseau172	admin	reseau_172	dmz	network	Etablissement
		admin-reseau_ader	admin	reseau_ader			
		pedago-reseau10	pedago	reseau_10			
		pedago-reseau192	pedago	reseau_192			
		pedago-reseau172	pedago	reseau_172			
		pedago-reseau_ader	pedago	reseau_ader			
🔿 Aisutas 🗌 🦱 Cumuring	lor.	Aigutor Abodi	ior A Supprimor		Modifier 🔿 (Pupprimor	

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.

Type: Réseau V Zéphir Module: V
Zéphir Module:
lodule:
vilesse leseau
dresse de 🗸 🗸

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.

Type: Réseau Zéphir Module: amon Adresse réseau adresse_network_eth1
Zéphir Module: amon Adresse réseau adresse_network_eth1
Module: amon Non Adresse réseau adresse_network_eth1 Non
adresse réseau adresse_network_eth1
Adresse de adresse_netmask_eth: ************************************

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 (<u>[n]</u>):
 - Seule la valeur correspondant à l'index sera traitée
 - Un seul tunnel sera créé

Syntaxe :

<u>adresse_network_vlan_eth1[0]</u> et <u>adresse_netmask_vlan_eth1[0]</u> pour le premier vlan déclaré sur eth1 ;

<u>adresse_network_vlan_eth1[1]</u> et <u>adresse_netmask_vlan_eth1[1]</u> pour le deuxième vlan déclaré sur eth1 ;

[...]

```
ou
```

```
<u>alias_network_eth2[0]</u> et <u>alias_netmask_eth2[0]</u> pour le premier alias déclaré sur eth2;
<u>alias_network_eth2[1]</u> et <u>alias_netmask_eth2[1]</u> 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.

UAI	Nom	Identifiant Zéphir	Version Eole	Type de serveur 🔻	État
A000000	aca.sphynx-default-2.6.1	224	2.6.1	sphynx	
A000000	Roadwarrior1			roadwarrior	Connexion OK
0000001	etb1.amon-default-2.6.1	292	2.6.1	etablissement	Connexion OK
00000002	etb2.amon-default-2.5.2	363	2.5.2	etablissement	Pb de tunnels ou non configuré
0000003	etb3.amonecole-default-2.4.2	453	2.4.2	etablissement	Pb de tunnels ou non configuré

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.

Ajouter un nou	veau serveur RVP
Importation Zéphir:	۲
Création manuelle:	
	« Précédent Suivant »
	Annuler OK

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 nou	veau serveur RVP
Importation Zéphir:	•
Création manuelle:	۲
	« Précédent Suivant »
	AnnulerOK

Ajouter un nouveau serveur	RVP depuis Zephir	
u serveur RVP		
Nom	Identifiant Zéphir	Version Eole
amon24-1	31	2.4
amon24-test	35	2.4
Amon2 avé accent	33	2.4
Amon avé accent	27	2.3 =
amon1	23	2.3
test Amonecole pour ARV	7	2.3
shpynx24-test	34	2.4
sphynxha2	24	2.3
Ш		>
	« Pré	cédent Suivant »
	Annuler	ок
	Ajouter un nouveau serveur serveur RVP Nom amon24-1 amon24-test Amon 2 avé accent Amon avé accent amon1 test Amonecole pour ARV shpynx24-test sphynxha2 III	Nom Identifiant Zéphir amon24-1 31 amon24-test 35 Amon2 avé accent 33 Amon avé accent 27 amon1 23 test Amonecole pour ARV 7 sphynxha2 24 (* Pré

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.

Ajouter un no	uveau serveur RVP		
Nom	Туре	IP	IP
admin	network	10.21.13.0	255.255.255.0
pedago	network	172.18.0.0	255.255.255.0
dmz	network	10.121.13.0	255.255.255.0
Recharger de	puis Zéphir		
			« Précédent Suivant »
			Annuler OK

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 :

Sélectionner un nouveau serveur RVP depuis Zéphir

Modifier le ser	veur RVP			
Nom	Туре	IP / Réseau	IP / Masque	
admin	network	10.21.11.0	255.255.255.0	
pedago	network	172.16.0.0	255.255.240.0	
dmz	network	10.121.11.0	255.255.255.224	
test	network			
Bacharara val				
Recharger var	eurs du modele			
			« Précédent Suivant »	
			Annuler OK	

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.

UAI	Nom	Identifiant Zéphir	Version Eole	État
A000000	sphynx24ha1			
A0000000	amon24-zephir	29	2.4	Connexion OK - Problème de tunnel(s)
A0000000	sphynx24ha2	32	2.4	Problème de connexion - Problème de tunnel(s)
0000A	amonecole23-1	36	2.3	Connexion OK - Problème de tunnel(s)
🗿 Ajouter 👯	🎉 Modifier 📔 🤤 Supprin	ier 🌼 Certificat 🎲 IP	externe 🌼 Renv	oyer sur Zéphir
Drāt		\sim		Appliquer

Ce bouton permet d'ajouter des certificats au serveur RVP

Sélectionner le serveur RVP, cliquer sur Certificat puis sur Ajouter

Certificats	
Certificats	
Certificats	
Ainster Summing	
Ajouter Supprimer	

Trois possibilités :

- vous possédez déjà les fichiers clé privée et certificat pour le serveur RVP, il faut
 Importer un ertificat ;
- 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 O Générer un nouveau certificat

Ajouter un nouv	eau certificat	
Importer un certificat:	۲	
Importer un fichier PKCS12:	0	
Générer un nouveau certificat:	•	
	« Précédent	Suivant »
	Annuler	Créer
lr	nporter 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 <u>Passphrase</u>: 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.

Ajouter un n	ouveau certificat
Clef privée:	Ajouter
Certificat:	Ajouter
Passphrase	:
	« Précédent Suivant »
	Annuler Créer

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.

Ajouter un nouv	eau certificat	
Importer un certificat:	•	
Importer un fichier PKCS12:	۲	
Générer un nouveau certificat:	•	
	« Précédent	Suivant »
	Annuler	Créer
Import	tor up cortificat DI/CC10	

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.

Ajouter un nouv	eau certificat	
Fichier PKCS12:	Ajouter	
Mot de passe PKCS12:	•••••	
Choisir un mot de passe:	•••••	
Confirmer le mot de passe:	•••••	
	« Précédent	Suivant »
	Annuler	Créer

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.

Ajouter un nouv	eau certificat
Importer un certificat:	0
Importer un fichier PKCS12:	0
Générer un nouveau certificat:	۲
	« Précédent Suivant »
	Annuler Créer

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.

Ajouter un nouveau	u certificat
Nom :	sphynx
Choisir un mot de passe:	••••
Confirmer le mot de passe:	••••
Certificat auto-signé:	۲
Générer une requête de certificat pour une CA:	
	« Précédent Suivant »
	Annuler Créer

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.

UAI	Nom	Identifiant Zéphir	Version Eole	État
A0000000	sphynx24ha1			
A0000000	amon24-zephir	29	2.4	Connexion OK - Problème de tunnel(s)
A0000000	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.

Certificats	
Certificats	
Certificats	
Ajouter Supprimer	

Ajouter des certificats

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

Ajouter un nouv	eau certificat
Importer un certificat:	0
Importer un fichier PKCS12:	•
Générer un nouveau certificat:	۲
	« Précédent Suivant »
	Annuler Créer
Générer un certific	sat autosigné ou importer les fichiers

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

La valeur du champ <u>Nom</u> 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 <u>Nom</u> 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).

Ajouter un nouveau	ı certificat
Nom :	sphynx
Choisir un mot de passe:	•••••
Confirmer le mot de passe:	•••••
Certificat auto-signé:	0
Générer une requête de certificat pour une CA:	۲
	« Précédent Suivant »
	Annuler Créer

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.

		Ouverture de reque	te.tgz	×
		Vous avez choisi d'o	ouvrir	
		requete.tgz		
		qui est un fichier de type : archive tar (compressée gzip		
Ajouter un nouveau	u certificat	a partir de : htt	ps://192.168.0.16:8088	
Nom :	requete	Que doit faire Fire	fox avec ce fichier ?	
Choisir un mot de passe:	••••	○ <u>O</u> uvrir avec	Gestionnaire d'archives (défaut)	
Confirmer le mot de passe:		. ● <u>E</u> nregistrer l	e fichier	
Certificat auto-signé:	•	□ <u>T</u> oujours eff	ectuer cette action pour ce type de fichier.	
Générer une requête de certificat pour une CA:	۲		SAnnuler 🖉 OK	
		« Précédent Suivant »		
	Ar	nuler Créer		

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.

UAI	Nom	Identifiant Zéphir	Version Eole	État
A000000	sphynx24ha1			
A000000	amon24-zephir	29	2.4	Connexion OK - Problème de tunnel(s)
A000000	sphynx24ha2	32	2.4	Problème de connexion - Problème de tunnel(s)
0000A	amonecole23-1	36	2.3	Connexion OK - Problème de tunnel(s)

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

Pexterne	
IP	
Ajouter Supprimer	
	Fermer

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 <u>IP publique</u> et rien dans la zone <u>IP privée</u>.

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

	192.100.0.0	
privée:		
	L	

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.

Serveur RVP 1	Serveur RVP 2	Tunnel
Nom	Nom	Nom
sphynxtestha1		
amontestha		
amon-conteneur		
sphynxtestha2		
amonARV2		
	Ajouter Modifier	

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 :

	2111		110111
Ajouter un lien sécu	risé vers		
Choisir un serveur	testARV	~	
RVP:			
		α.	Précédent Suivant »
		Annular	Créer
		Annuel	Creer

Choix du concentrateur RVP pour le lien sécurisé

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

Ajouter un lien sécu	risé vers	
Choisir un modèle de lien sécurisé:	amon-sphynx	
		« Précédent Suivant »
		Annuler Créer

Choix du modèle de lien sécurisé

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

		-
sphynx	*	Ajouter
192.168.0.11	~	Ajouter
amonecole	*	Ajouter
192.168.0.33	*	Ajouter
TOUJOURS via le protocole ipsec	~	
TOUJOURS via le protocole ipsec		
JAMAIS via le protocole ipsec		
« Préci	édent a	Suivant »
	sphynx 192.168.0.11 amonecole 192.168.0.33 TOUJOURS via le protocole ipsec TOUJOURS via le protocole ipsec JAMAIS via le protocole ipsec	sphynx 192.168.0.11 amonecole 192.168.0.33 TOUJOURS via le protocole ipsec TOUJOURS via le protocole ipsec JAMAIS via le protocole ipsec JAMAIS via le protocole ipsec

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).

Ajout	er un lien sécurisé vers				
	Modèle de réseau local 1	Modèle de réseau local 2			
1	admin	reseau_eth1			
V	admin	reseau_10			
	admin	reseau_192			
V	admin	reseau_172			
	admin	reseau_ader			
	pedago	reseau_10			
	pedago	reseau_192			
	pedago	reseau_172			
4					
		« Précédent Suivant »			
		Annuler Modifier			

Choix des tunnels

- <u> Gestion</u> 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 :

	—pedago—		_				exterieu	ır
nom	descript	ion zo	ne		nom	des	cription	zone
pedago_rest	treint zone re	streinte pe	di		agriates			exterieur
•			•					
🗌 tout sauf					🗌 tout sau	uf		
service								
	service : tou	is, protocol	= то	зu	JT, port = ['0']		🗌 🗌 tout saut
plages hora	aires							
	gl	issez - dép	osez	u	ne plage ho	orair	е	
groupe d'ut	tilisateurs—							
	glissez - déposez un groupe d'utilisateurs							
groupe d'a	pplications-							
	glisse	z - dépose	z un	g	roupe d'app	olicat	ions	
actions								
SNAT								•
ACCEPT	nouvelle ip	admin_ba	stion		nouveau p	ort		
options								
🗌 journaliser	· 🗌 politique i	psec						

Version : révision : Avril 2018

	-pedago				exte	rieur —	
nom	description	zone	nom	d	lescription	zone	
pedago_restreint	zone restreinte	pedago	agriat	es		exterieur	
🗌 tout sauf			🗌 tou	t sauf			· · · · · · · · · · · · · · · · · · ·
service							
	service : es	p, protocol =	= esp, port =	= ['0']			🗌 tout sauf
plages horaires							
	glis	ssez - dépos	ez une plag	e hor	aire		
groupe d'utilisa	teurs						
	glisse	z - déposez (un groupe d	d'utilis	ateurs		
groupe d'applic	ations						
	glisse:	z - déposez u	un groupe d	appli	cations		
FORWARD							 ▼
ACCEPT nouve	elle ip <mark>glissez</mark> -	déposez une	e extrémité	nou	iveau port		
options							
ijournaliser 🗹 p	oolitique ipsec						

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 <u>Bases de données créées</u> ou <u>Configurations strongSwan générées</u> (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.

Serveur R\	veur RVP 1 Serveur RVP 2		Tunnel			
UAI	Nom	UAI	Nom	Nom	IP / Réseau	IP / Réseau
A0000000	aca.sphynx-default	0000000x	roadwarrior1	🖃 amon-sphynx-as - 192.	168.0.11 192.168.0.31 / certificate send : ALWAYS	via ipsec protocol / IKE fragmentation : no
x0000000	roadwarrior1	00000001	etb1.amon-default	adm-eth1	reseau eth1 : 172 30 101 0 / 255 255	2 admin : 10 1 1 0 / 255 255 255 0
00000001	etb1.amon-default					
		Ajoute	r 💮 Modifier			

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.

UAI	Nom	Identifiant Zéphir	Version Eole	État
A0000000	sphynx24ha1			
A0000000	amon24-zephir	29	2.4	Connexion OK - Problème de tunnel(s)
A0000000	sphynx24ha2	32	2.4	Problème de connexion - Problème de tunnel(s)
0000A	amonecole23-1	36	2.3	Connexion OK - Problème de tunnel(s)
Aiguter	🚳 Modifier 🔰 🦳 Supprin	er to Certificat	externe 📸 Renv	over sur Zénhir

Ce bouton permet d'ajouter des certificats au serveur RVP

Sélectionner le serveur RVP, cliquer sur Certificat puis sur Ajouter

Certificats	
Certificats	
Certificats	
Aigutar A Supprimer	
Supprimer	
	Fermer

Ajouter des certificats

Trois possibilités :

- vous possédez déjà les fichiers clé privée et certificat pour le serveur RVP, il faut
 Importer un ertificat ;
- 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 O Générer un nouveau certificat

Ajouter un nouv	eau certificat
Importer un certificat:	۲
Importer un fichier PKCS12:	•
Générer un nouveau certificat:	•
	« Précédent Suivant »
	Annuler Créer
lr	nporter 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 <u>Passphrase</u>: 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.

Ajouter un n	ouveau certificat
Clef privée:	Ajouter
Certificat:	Ajouter
Passphrase	:
_	
	« Précédent Suivant »
	Annuler Créer

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.

Ajouter un nouv	eau certificat	
Importer un certificat:	0	
Importer un fichier PKCS12:	۲	
Générer un nouveau certificat:	•	
	« Précédent	Suivant »
	Annuler	Créer
Impor	ter 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.

Ajouter un nouve	eau certificat	
Fichier PKCS12:	Ajouter	
Mot de passe PKCS12:	•••••	
Choisir un mot de passe:	•••••	
Confirmer le mot de passe:	•••••	
	« Précédent	Suivant »
	Annuler	Créer

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.

Ajouter un nouv	eau certificat
Importer un certificat:	0
Importer un fichier PKCS12:	0
Générer un nouveau certificat:	۲
	« Précédent Suivant »
	Annuler

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.

Ajouter un nouveau	u certificat
Nom :	sphynx
Choisir un mot de passe:	••••
Confirmer le mot de passe:	••••
Certificat auto-signé:	۲
Générer une requête de certificat pour une CA:	
	« Précédent Suivant »
	Annuler Créer

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 (i)	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 <u>Serveur RVP associé</u> 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 <u>true</u>) 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.

0000000A sphynx24ha1 0000000A amon24-zephir 29	2.4 Conservice OK Brahlème de hener(e)
0000000A amon24-zephir 29	2.4 Connection OK Deablished do transmite)
	2.4 Connexion OK - Probleme 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.

Certificats	
Certificats	
Certificats	
Ainstea 🛛 🙈 Comminger	
Supprimer	
	Ferme

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

Ajouter un nouv	eau certificat
Importer un certificat:	0
Importer un fichier PKCS12:	0
Générer un nouveau certificat:	۲
	« Précédent Suivant »
	Annuler Créer

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 <u>Nom</u> 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).

Ajouter un nouveau	u certificat
Nom :	sphynx
Choisir un mot de passe:	•••••
Confirmer le mot de passe:	•••••
Certificat auto-signé:	0
Générer une requête de certificat pour une CA:	۲
	« Précédent Suivant »
	Annuler Créer

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.

		Ouverture de reque	te.tgz	×
		Vous avez choisi d'o	ouvrir	
Ajouter un nouveau Nom :	a certificat requete	requete.tgz qui est un fichie à partir de : htt Que doit faire Fire	er de type : archive tar (compressée gzip) (2 :ps://192.168.0.16:8088 fox avec ce fichier ?	
Choisir un mot de passe:	••••	○ <u>O</u> uvrir avec	Gestionnaire d'archives (défaut)	
Confirmer le mot de passe:		. ● <u>E</u> nregistrer l	e fichier	
Certificat auto-signé:	0	□ <u>T</u> oujours effe	ectuer cette action pour ce type de fichier.	
Générer une requête de certificat pour une CA:	۲		S Annuler V OK	
		« Précédent Suivant »		_
	Ar	nuler Créer		

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

Arv - Mozilla Firefox	200		- • ×
Firefox 🗸 🗍 Arv	🕨 🔁 Duck Du	JckGo	Q ::
	168.0.11:8088		☆~@ ◙~
Tunnels Serveurs RVP Modèl	Certificats	at	
Nom Dat	Clef privée:	Ajouter	CA
0210026P-01 201	Cortificat		false
0890977D-01 201	3 Ceruncal.	Ajouter	false
AGRIATES-DIJON-10 201	5 Passphrase:		false
0210066H-15 201	5		false
RACINE AGRIATES 202	a		true
CA-sphynxha1-RVP 202	в		true
🔅 Modifier		Annuler Modifier	
Prêt	L]	Appliquer 🧿
		<u>1</u>	📽 FoxyProxy: Motifs 🌸

Dans la fenêtre surgissante :

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

Arv - Mozilla Firefo	ox 🖣	ha			- • ×
Firefox Y Arv	4	🛛 🔁 🖌 Duck 🛙	DuckGo		Q =:
🕹 📾 🖑 🔒 https	://192.1	68.0.11:8088			ଳ କା ଳ (ଅକ
Tunnels Serveurs RVP	Modèles	Certificats Remplacer certif	icat		
Nom	Date	Clef privée:	Aiouter		CA
0210026P-01	2010	oler philes.	Ajouter		false
0890977D-01	2013	Certificat:	Ajouter		false
AGRIATES-DIJON-10	2015	Passphrase:			false
0210066H-15	2015				false
RACINE AGRIATES	2020				true
CA-sphynxha1-RVP	2028				true
Street Modifier			Annuler	odifier	
Prêt					Appliquer 🛛 🧿
@ ∽ 🗶				- 1 98. (😵 FoxyProxy: Motifs 💣

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 <u>Certificat</u> et choisir le nouveau fichier .pkcs7 renvoyé par l'IGC ;
- saisir le mot de passe dans le champs <u>Passphrase</u>;
- 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.

DKOC10	
= 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/