Connection Management Center 1.2

Guide de référence

Dernière mise à jour : 6 mai 2024
Référence du document : 20240506_RG_CMC_1.2_FR_1.0

www.thegreenbow.com

TheGreenBow est un nom commercial déposé.

Microsoft, Windows 10 et Windows 11 sont soit des marques déposées, soit des marques commerciales de Microsoft Corp. aux États-Unis et/ou dans d'autres pays.

Linux® est une marque déposée par Linus Torvalds aux États-Unis et dans d'autres pays.

Ubuntu et le logo Ubuntu logo sont soit des marques déposées, soit des marques commerciales de Canonical Group Ltd. au Royaume-Uni, d'autres pays, ou les deux.

Red Hat, Red Hat Enterprise Linux, le logo Red Hat, le logo Shadowman, CentOS, JBoss, OpenShift, Fedora, le logo Infinity, et RHCE sont des marques déposées de Red Hat, Inc. aux États-Unis et dans d'autres pays.

Debian est une marque déposée de Software in the Public Interest, Inc. aux États-Unis, gérée par le projet Debian.

Apple, le logo Apple, iPhone, iOS, Mac et macOS sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays et régions.

Android, Google Chrome, Google Play et le logo Google Play sont des marques commerciales de Google, LLC.

HashiCorp, le logo HashiCorp, Consul, Nomad, Terraform et Vault sont des marques de HashiCorp Inc. déposées aux États-Unis et dans d'autres pays.

D'autres marques de commerce appartenant à des tiers et mentionnées dans ce document demeurent la propriété intellectuelle de ces tiers.

Toutes les informations fournies sont sujettes à modification à tout moment et sans préavis.

Malgré tous les soins apportés à la réalisation de ce document et à sa mise à jour régulière, des erreurs peuvent s'être glissées dans les informations présentées. Si vous en constatez n'hésitez pas à nous le faire savoir en nous contactant, nous procéderons aux rectifications correspondantes.

Table des matières

1 Introduction 1
2 Page Créer un / Modifier le tunnel IKEv2 2
2.1 Introduction 2
2.2 Onglet PASSERELLE DISTANTE 2
2.2.1 Bloc d'identification 3
2.2.2 Bloc Passerelle distante 3
2.2.3 Bloc Durée de vie 5
2.2.4 Bloc Dead Peer Detection (DPD) 5
2.2.5 Bloc Cryptographie 7
2.3 Onglet AUTHENTIFICATION DU CLIENT 8
2.3.1 Introduction 8
2.3.2 Sous-onglet CLÉ PARTAGÉE 9
2.3.3 Sous-onglet CERTIFICAT 11
2.3.4 Sous-onglet EAP 16
2.4 Onglet CHILD SA 18
2.4.1 Bloc Cryptographie 18
2.4.2 Bloc Durée de vie 20
2.4.3 Bloc Réseau 20
2.5 Onglet AUTHENTIFICATION DE LA PASSERELLE 24
2.5.1 Bloc Identité (Remote ID) 24
2.5.2 Bloc CA de confiance 25
2.5.3 Bloc Options 26
2.6 Onglet AVANCÉ 28
2.6.1 Bloc Protocole IKE 28
2.6.2 Bloc Test de trafic dans le tunnel 30
2.6.3 Bloc Autres 31
3 Page Créer un / Modifier le tunnel OpenVPN 33
3.1 Introduction 33
3.2 Onglet PASSERELLE DISTANTE 33
3.2.1 Bloc d'identification 34
3.2.2 Bloc Passerelle distante 34
3.2.3 Bloc Options d'établissement du tunnel 35
3.2.4 Bloc Renégociation 36

3.2.5 Bloc Dead Peer Detection (DPD) 37
3.2.6 Bloc Autres 38
3.3 Onglet AUTHENTIFICATION DU CLIENT 39
3.3.1 Bloc Authentification initiale (TLS) 39
3.3.2 Bloc Type de stockage 40
3.3.3 Bloc Préciser l'objet du certificat 40
3.3.4 Bloc Certificat PKCS #12 41
3.3.5 Bloc Authentification supplémentaire 42
3.4 Onglet AUTHENTIFICATION DE LA PASSERELLE 43
3.4.1 Bloc Identité (Remote ID) 43
3.4.2 Bloc CA de confiance 43
3.5 Onglet TRAFIC 44
3.5.1 Bloc Suite de sécurité du trafic 44
3.5.2 Bloc Extra HMAC (TLS-Auth) 46
3.6 Onglet AVANCÉ 47
3.6.1 Bloc Options du tunnel 47
3.6.2 Bloc Test de trafic dans le tunnel 49
3.6.3 Bloc Autres 49
4 Page Créer une / Modifier la connexion 52
4.1 Introduction 52
4.2 Bloc d'identification 52
4.3 Paramètres avancés d'une connexion classique 54
4.3.1 Présentation 54
4.3.2 Bloc Mode GINA 55
4.3.3 Bloc Tunnel de repli 55
4.3.4 Bloc Mode d'ouverture automatique 57
4.4 Paramètres avancés d'une connexion TrustedConnect 57
4.4.1 Présentation 57
4.4.2 Bloc Mode GINA 58
4.4.3 Bloc Always-On 59
4.4.4 Bloc Détection de réseau de confiance (TND) 60
4.4.5 Bloc Détection de portail captif 64
5 Page Créer une / Modifier la configuration 66
5.1 Introduction 66
5.2 Onglet GÉNÉRAL 66
5.2.1 Bloc d'identification 66

5.2.2 Bloc Connexions 67
5.3 Onglet MODE FILTRANT 68
5.3.1 Présentation 68
5.3.2 Bloc Mode filtrant 68
5.3.3 Boîte de dialogue Créer une règle 69
6 Gestion des certificats 72
6.1 Introduction 72
6.2 Certificat utilisateur 73
6.2.1 Généralités 73
6.2.2 Options spécifiques 73
6.2.3 Stockage des certificats 75
6.2.4 Importation de certificats dans la configuration VPN 76
6.2.5 Utilisation de certificats sur carte à puce ou sur token 77
6.2.6 Utilisation de certificats du magasin de certificats de l'OS 78
6.3 Certificat de la passerelle VPN 79
6.3.1 Généralités 79
6.3.2 Contraintes relatives à l'extension Key Usage 80
6.3.3 Contraintes relatives à l'extension Extended Key Usage 80
6.4 Restriction du téléchargement des CRL 81
6.4.1 Introduction 81
6.4.2 Blocage du téléchargement de la CRL de validation du certificat utilisateur 81
6.4.3 Limitation du téléchargement de la CRL de validation du certificat passerelle 82
6.5 Autorités de certification 82
6.5.1 Généralités 82
6.5.2 Importation d'une autorité de certification 83
6.5.3 Mode IPsec DR 83
7 Gestion des paramètres dynamiques 84
7.1 Généralités 84
7.2 Utilisation des paramètres 85
7.2.1 local_subnet 85
7.2.2 nonce_size 85
7.2.3 local_virtual_network_size 86
7.2.4 user_cert_dnpattern 86
7.2.5 user_cert_keyusage 86
7.2.6 reader_pattern 87
7.2.7 MachineStore 87

7.2.8 enable_OCSP ... 87
7.2.9 check_user_crl ... 88
7.2.10 crl_cache_duration ... 88
7.2.11 allow_server_extra_keyusage ... 89
7.2.12 allow_server_and_client_auth ... 90
7.2.13 sha2_in_cert_req ... 90
7.2.14 Method14_RSASSA_PKCS1 ... 90
7.2.15 Method1_PKCS1v15_Scheme ... 91
7.2.16 use_method_214 ... 91
7.2.17 user_smartcard_tip ... 91

8 Gestion du Panneau TrustedConnect ... 93

8.1 Présentation ... 93
8.2 Always-On ... 93
8.2.1 Principe et fonctionnement ... 93
8.2.2 Configuration de Always-On ... 94
8.3 Détection du réseau de confiance (TND) ... 94
8.3.1 Principe et fonctionnement ... 94
8.3.2 Configuration de TND ... 96
8.4 Scripts ... 97

9 Automatisation ... 98

9.1 Introduction ... 98
9.2 Passerelle redondante ... 98
9.2.1 Présentation ... 98
9.2.2 Configuration d'une passerelle redondante ... 99
9.3 Tunnel de repli ... 99
9.3.1 Présentation ... 99
9.3.2 Configuration d'un tunnel de repli ... 99
9.4 Mode d'ouverture automatique ... 100
9.4.1 Présentation ... 100
9.4.2 Configuration des modes d'ouverture automatique ... 100
9.5 Scripts ... 100
9.5.1 Présentation ... 100
9.5.2 Configuration des scripts ... 101
9.6 Mode GINA ... 102
9.6.1 Présentation ... 102
9.6.2 Configuration du mode GINA ... 103

9.6.3 Utilisation du mode GINA ... 104
9.7 Partage de bureau distant ... 105
9.7.1 Présentation ... 105
9.7.2 Configuration du partage de bureau distant ... 105
10 IPv4 et IPv6 ... 106
11 Recommandations de sécurité ... 107
11.1 Hypothèses ... 107
11.1.1 Profil et responsabilités des administrateurs ... 107
11.1.2 Profil et responsabilités de l'utilisateur ... 107
11.1.3 Respect des règles de gestion des éléments cryptographiques ... 107
11.2 Configuration VPN ... 108
11.2.1 Données sensibles dans la configuration VPN ... 108
11.2.2 Authentification de l'utilisateur ... 108
11.2.3 Authentification de la passerelle VPN ... 109
11.2.4 Protocole ... 109
11.2.5 Mode « tout dans le tunnel » et « split tunneling » ... 109
11.2.6 Mode GINA ... 109
11.2.7 Recommandations de l'ANSSI ... 110
12 Contact ... 111
12.1 Information ... 111
12.2 Commercial ... 111
12.3 Support ... 111
13 Annexes ... 112
13.1 Architecture sécurisée ... 112
13.2 Notions élémentaires de cryptographie ... 114
13.2.1 Algorithmes SHA, RSA, ECDSA et ECSDSA ... 114
13.2.2 Accès aux certificats ... 115
13.2.3 Déterminer le type de conteneur d'un certificat ... 117
13.2.4 Format des certificats ... 117
13.2.5 Méthodes d'authentification des certificats ... 123

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2024-05-06	Toutes	Version provisoire	BB

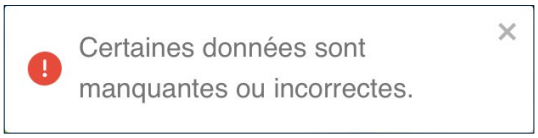
1 Introduction

Ce guide est destiné aux administrateurs du Connection Management Center (CMC).

Il suppose que le logiciel est déjà installé et s'utilise conjointement avec le « Guide de l'administrateur » du CMC. En effet, il décrit de manière détaillée les différents champs sur les pages et les onglets de configuration VPN (chapitres 2, 3, 4 & 5) et apporte des informations complémentaires relatives à la gestion des certificats (chapitre 6), la gestion des paramètres dynamiques (chapitre 7), la gestion **du Panneau TrustedConnect** du Client VPN Windows Enterprise (chapitre 8), les options d'automatisation (chapitre 9) et le choix IPv4/IPv6 (chapitre 10). Il présente en outre des recommandations de sécurité (chapitre 11), l'architecture sécurisée du CMC (section 13.1) et des notions élémentaires de cryptographie (section 13.2).

Le « Guide de l'administrateur » du CMC, quant à lui, définit quelques notions fondamentales et présente l'interface du CMC pour en faciliter la prise en main, puis il décrit les principales procédures d'administration du CMC, de gestion des configurations VPN, de gestion des licences et de supervision. Il comporte également quelques procédures de maintenance courante.

De manière générale, tous les champs de l'interface du CMC pourvus d'un astérisque doivent être remplis. Si vous tentez d'enregistrer un objet (tunnel, connexion ou configuration) sans avoir rempli tous les champs obligatoires, les champs concernés sont mis en évidence par leur coloration en rouge et un message correspondant s'affiche en haute à droite de l'écran :



Pour faciliter le travail de configuration, des encadrés de compatibilité indiquent les systèmes d'exploitation et, le cas échéant, les versions des Clients VPN TheGreenBow pour lesquels les options et paramètres peuvent être utilisés :

Compatibilité : , , ,

Le CMC est prévu pour fonctionner avec les Clients VPN TheGreenBow suivants :

- Client VPN Windows Enterprise v7.2 et supérieur,
- Client VPN macOS v2.2 et supérieur,
- Client VPN Android v6.2 et supérieur,
- Client VPN Linux v3.2 et supérieur.

2 Page Créer un / Modifier le tunnel IKEv2

2.1 Introduction

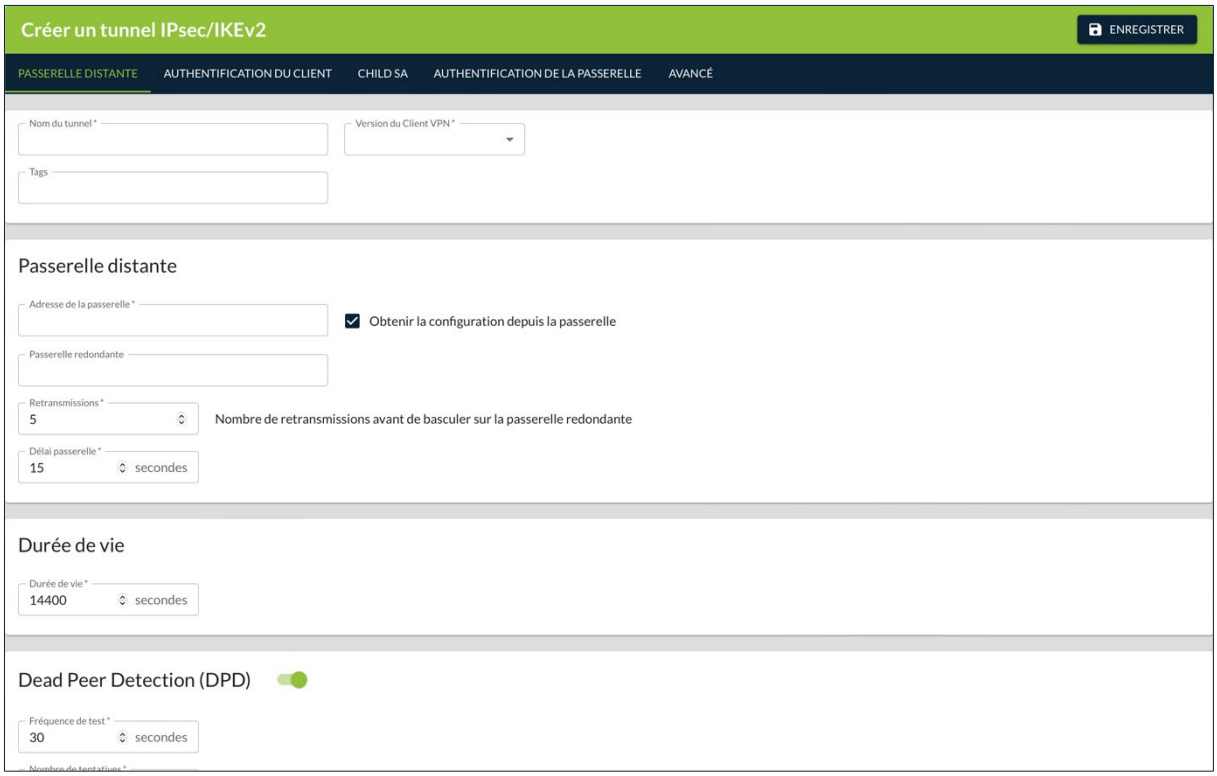
Les champs figurant sur les pages **Créer un tunnel IKEv2** et **Modifier le tunnel IKEv2** sont identiques. Ils sont donc décrits de façon commune ci-dessous. Cas pages comportent chacune les cinq onglets suivants :

- **PASSERELLE DISTANTE**, voir 2.2
- **AUTHENTIFICATION DU CLIENT**, voir 2.3
- **CHILD SA**, voir 2.4
- **AUTHENTIFICATION DE LA PASSERELLE**, voir 2.5
- **AVANCÉ**, voir 2.6

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour comprendre les différences entre les protocoles IPsec/IKEv2 et OpenVPN.

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour comprendre les notions de tunnel, connexion et configuration telles qu'elles sont utilisées chez TheGreenBow.

2.2 Onglet PASSERELLE DISTANTE



2.2.1 Bloc d'identification

Compatibilité : Windows, macOS, Android, Linux

Le premier bloc de l'onglet n'a pas de titre et sert à identifier le tunnel.

Nom du tunnel

Nom attribué au tunnel.

Longueur max. : 50

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

Ce champ doit être obligatoirement renseigné.

Version du Client VPN

Version du Client VPN TheGreenBow pour laquelle le tunnel est créé.

Les informations protocolaires d'un tunnel sont spécifiques à une version donnée des Clients VPN TheGreenBow. Le tunnel peut donc être utilisé avec n'importe quel Client VPN d'un niveau de version donné, p. ex. le Client VPN Windows Enterprise v7.4, le Client VPN macOS v2.4 et le Client VPN Android v6.4.

Ce champ doit être obligatoirement renseigné.

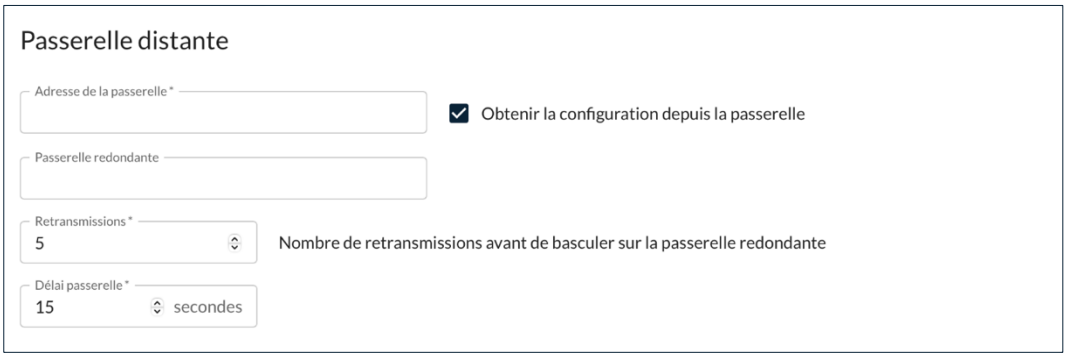
Tags

Tags destinés à faciliter le filtrage des tunnels dans la liste des tunnels.

Vous pouvez saisir n'importe quel type de caractère. Appuyez ensuite sur Entrée pour former le tag. Saisissez autant de tags que nécessaire.

2.2.2 Bloc Passerelle distante

Compatibilité : Windows, macOS, Android, Linux



Adresse de la passerelle

Adresse IP (IPv6 ou IPv4) ou adresse DNS de la passerelle VPN distante.

Ce champ doit être obligatoirement renseigné.

Obtenir la configuration depuis la passerelle

Cette option (aussi appelée « Configuration Payload » ou encore « Mode CP ») permet au Client VPN de récupérer depuis la passerelle VPN toutes les informations utiles à la connexion VPN :

- adresse du Client VPN,
- adresse réseau distant,
- masque réseau,
- adresses DNS.

Elles sont renseignées dynamiquement au cours de l'ouverture du tunnel, avec les valeurs envoyées par la passerelle VPN dans l'échange Mode CP.

Cette case est cochée par défaut. Lorsqu'elle est décochée, ces informations doivent être saisies manuellement au niveau des **Sélecteurs de trafic** dans le bloc **Réseau** sur l'onglet **CHILD SA** (voir 2.4.3.1 Sous-bloc Sélecteurs de trafic).

Le Mode CP permet à la passerelle de configurer jusqu'à 16 sous-réseaux. Si plus de 16 sous-réseaux sont configurés par la passerelle, seuls les 16 premiers seront pris en compte.

Passerelle redondante

Définit l'adresse d'une passerelle VPN de secours sur laquelle le Client VPN bascule lorsque la passerelle VPN initiale est indisponible ou inaccessible.

L'adresse de la passerelle VPN redondante peut être une adresse IP ou DNS.

Ce champ est facultatif.

⚠ La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction **Tunnel de repli**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé.

☞ Pour une description détaillée de cette fonction, reportez-vous à la section 9.2 Passerelle redondante.

Retransmissions

Nombre de retransmissions de messages protocolaires IKE avant échec.

Valeur par défaut : 5.

Ce champ doit être obligatoirement renseigné.

Délai passerelle

Délai entre chaque retransmission.

Valeur par défaut : 15.

Ce champ doit être obligatoirement renseigné.

2.2.3 Bloc Durée de vie

Compatibilité : , , ,

Durée de vie

Durée de vie de la phase IKE Authentication.

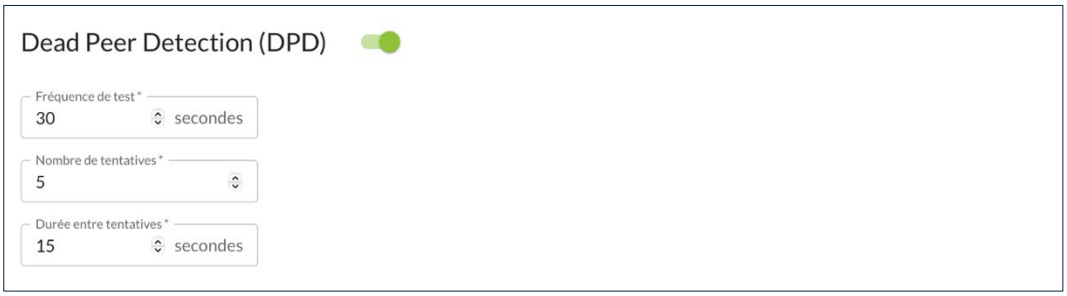
La durée de vie est exprimée en secondes.

Sa valeur par défaut est de 14 400 secondes (4 h).

Ce champ doit être obligatoirement renseigné.

2.2.4 Bloc Dead Peer Detection (DPD)

La fonction Dead Peer Detection (DPD) est activée par défaut.



Si vous ne souhaitez pas utiliser la fonction Dead Peer Detection (DPD) et que vous voulez masquer les champs correspondants, actionnez le bouton bascule à droite du nom du bloc pour la désactiver. Dans ce cas, le client VPN ne pourra pas déterminer si la passerelle est disponible.

Fréquence de test

La fonction DPD (Dead Peer Detection) permet au Client VPN de détecter que la passerelle VPN devient inaccessible ou inactive.

La période de vérification est la période entre deux envois de messages de vérification DPD, exprimée en secondes.

Ce champ doit être obligatoirement renseigné.

La fonction de DPD est active à l'ouverture du tunnel (après la phase d'authentification). Associé à une passerelle redondante, le DPD permet au Client VPN de basculer automatiquement d'une passerelle à l'autre sur indisponibilité de l'une ou l'autre.

Nombre de tentatives

Nombre d'essais infructueux consécutifs avant de déclarer que la passerelle VPN est injoignable.

Ce champ doit être obligatoirement renseigné.

Durée entre tentatives

Intervalle entre les messages DPD lorsqu'aucune réponse n'est reçue de la passerelle VPN, exprimé en secondes.

Ce champ doit être obligatoirement renseigné.

2.2.5 Bloc Cryptographie

Compatibilité : , , ,

Chiffrement

Algorithme de chiffrement négocié au cours de la phase d'authentification :

- Automatique[1],
- AES CBC (128, 192, 256),
- AES CTR (128, 192, 256),
- AES GCM (128, 192, 256).

Ce champ doit être obligatoirement renseigné.

Intégrité

Algorithme d'intégrité négocié au cours de la phase d'authentification :

- Automatique[2],
- SHA2 256,
- SHA2 384,
- SHA2 512.

Ce champ doit être obligatoirement renseigné.

[1] **Automatique** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.
[2] idem

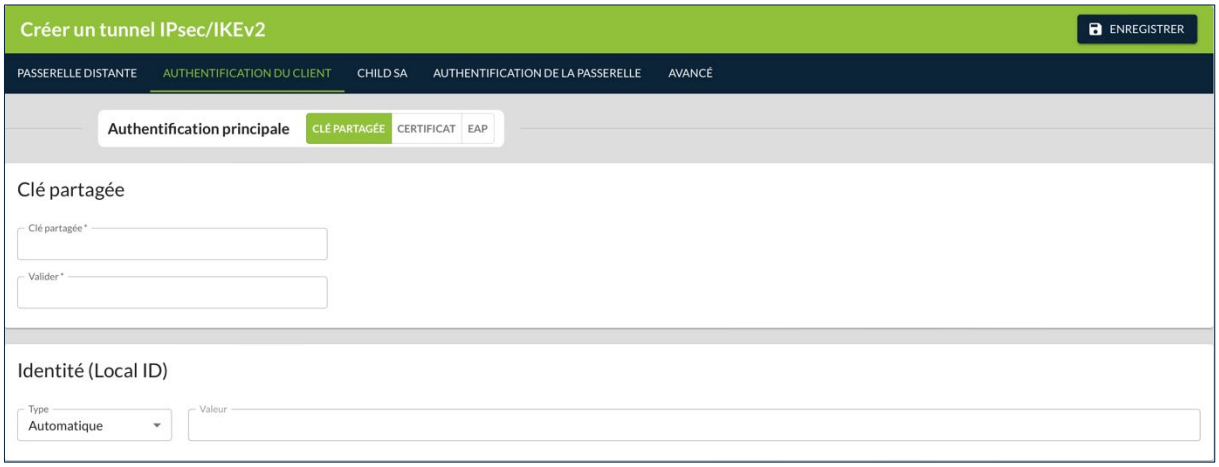
Diffie-Hellman

Longueur de la clé Diffie-Hellman:

- Automatique[1],
- DH14 (MODP 2048),
- DH15 (MODP 3072),
- DH16 (MODP 4096),
- DH17 (MODP 6144),
- DH18 (MODP 8192),
- DH19 (ECP 256),
- DH20 (ECP 384),
- DH21 (ECP 521),
- DH28 (BrainpoolP256r1).

Ce champ doit être obligatoirement renseigné.

2.3 Onglet AUTHENTIFICATION DU CLIENT



2.3.1 Introduction

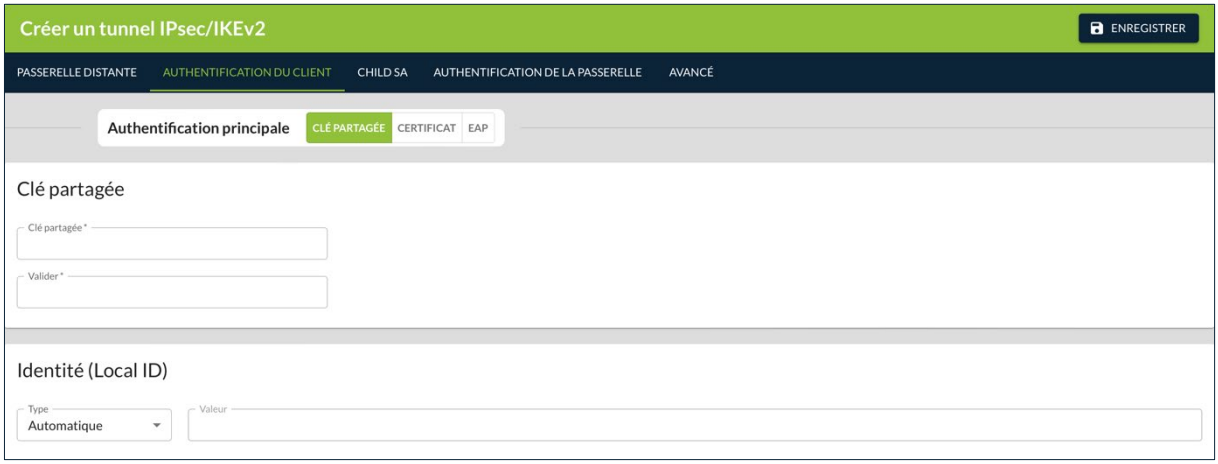
Cet onglet contient les trois sous-onglets suivants qui s'affichent en fonction de l'**Authentification principale** sélectionnée :

- **CLÉ PARTAGÉE**, voir 2.3.2
- **CERTIFICAT**, voir 2.3.3
- **EAP**, voir 2.3.4

Il s'ouvre par défaut sur le sous-onglet **CLÉ PARTAGÉE** lors de la création d'un tunnel. Lorsque le tunnel est ouvert en modification, l'onglet s'ouvre sur le sous-onglet configuré précédemment.

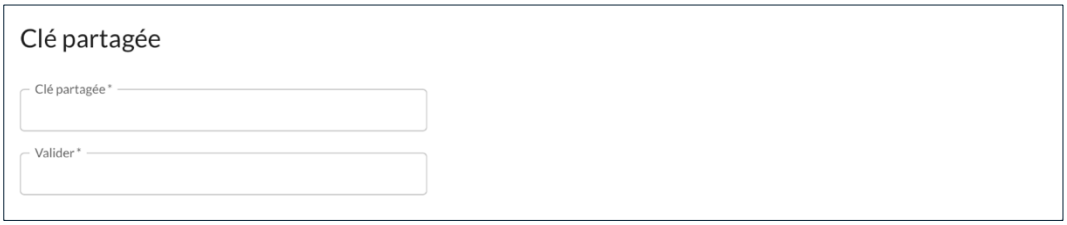
[1] **Automatique** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.

2.3.2 Sous-onglet CLÉ PARTAGÉE



2.3.2.1 Bloc Clé partagée

Compatibilité : , , ,



Clé partagée

Mot de passe ou clé partagée par la passerelle distante.

Ce champ doit être obligatoirement renseigné.

La clé partagée (preshared key) est un moyen simple de configurer un tunnel VPN. Elle apporte toutefois moins de souplesse dans la gestion de la sécurité que l'utilisation de certificats.
Voir le chapitre 11 Recommandations de sécurité.

Valider

Confirmation du mot de passe ou de la clé partagée par la passerelle distante.

Ce champ doit être obligatoirement renseigné.

2.3.2.2 Bloc Identité (Local ID)

Compatibilité : , , ,

Type

Type d'identifiant de la phase d'authentification que le Client VPN envoie à la passerelle VPN distante (Local ID).

Suivant le type sélectionné, cet identifiant peut être :

- Automatique : une fois le certificat sélectionné, le type de d'identifiant du tunnel passe automatiquement à **DER ASN1 DN**, et le sujet du certificat est utilisé par défaut comme valeur de cet identifiant
- Adresse IPV4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 195.100.205.101
- DNS : un nom de domaine (type = FQDN), p. ex. gw.mondomaine.net
- KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123456
- Email : une adresse e-mail (type = USER FQDN), p. ex. support@thegreenbow.com
- Adresse IPV6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3
- DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) ; ce champ est automatiquement renseigné avec le sujet d'un certificat X.509 lorsque le tunnel est associé à un certificat utilisateur (cf. chapitre 6 Gestion des certificats)

Depuis la version x.3 des Clients VPN TheGreenBow, vous pouvez sélectionner le type **DNS** ou **Email** dans la liste déroulante **Type**, afin d'affecter automatiquement à l'identifiant une valeur de DNS ou d'e-mail récupérée du certificat.

Si vous choisissez le type **DNS**, la valeur de l'identifiant prendra automatiquement la valeur du champ `dNSName` du nom alternatif du sujet du certificat (`SubjAltName`). Si ce champ n'est pas renseigné (absence de `SubjAltName` dans le certificat ou absence de `dNSName` dans le `SubjAltName`), c'est la valeur `CN` du sujet du certificat qui est reprise. Si cette dernière valeur n'est pas non plus présente, aucun certificat n'est admissible pour configurer le tunnel et la montée du tunnel échoue.

Si vous choisissez le type **Email**, la valeur de l'identifiant prendra automatiquement la valeur du champ `rfc822Name` du nom alternatif du sujet du certificat (`SubjAltName`). Si ce champ n'est pas renseigné (absence de `SubjAltName` dans le certificat ou absence de `rfc822Name` dans le

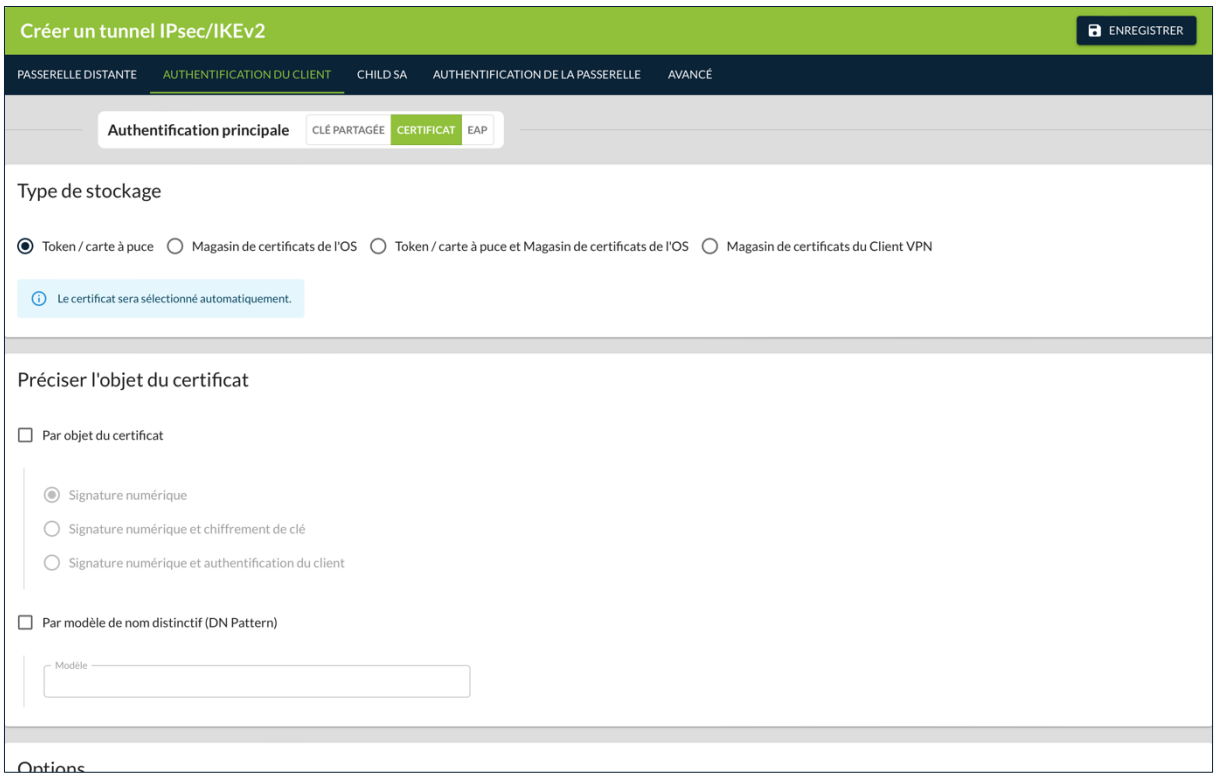
`SubjAltName`), c'est la valeur `Email` du sujet du certificat qui est reprise. Si cette dernière valeur n'est pas non plus présente, aucun certificat n'est admissible pour configurer le tunnel et la montée du tunnel échoue.

Valeur

La valeur associée au type sélectionné dans la liste déroulante.

Ce champ doit être obligatoirement renseigné si le type sélectionné est différent de la valeur par défaut **Automatique**.

2.3.3 Sous-onglet CERTIFICAT



2.3.3.1 Bloc Type de stockage

Compatibilité : , , , (voir notes pour les limitations)

Indique l'emplacement où est stocké le certificat :

- Token / carte à puce
- Magasin de certificats de l'OS
- Token / carte à puce et Magasin de certificats de l'OS[1]
- Magasin de certificats du Client VPN[2]

Dans les trois premiers cas, le certificat sera sélectionné automatiquement. Si vous sélectionnez l'option **Magasin de certificat du Client VPN**, le bloc **Préciser l'objet du certificat** est remplacé par le bloc **Certificat PKCS #12**, voir 2.3.3.3 Bloc Certificat PKCS #12.

2.3.3.2 Bloc Préciser l'objet du certificat

Compatibilité : ,

Ce bloc s'affiche uniquement pour les types de stockage suivants :

- **Token / carte à puce**
- **Magasin de certificats de l'OS**
- **Token / carte à puce et Magasin de certificats de l'OS**

[1] Cette option est uniquement disponible pour les clients de version 7.4 / 2.4 / 6.4 et 7.5 / 2.5 / 6.5.
[2] Correspond à l'enregistrement du certificat dans la configuration VPN.

Par objet du certificat

Lorsque la case est cochée, le certificat est sélectionné en fonction de son champ « key usage » :

- Signature numérique : sélection du certificat par le champ « key usage » dont la valeur de l'attribut `digitalSignature=1`.
- Signature numérique et chiffrement de clé : sélection du certificat par le champ « key usage » dont la valeur des attributs `digitalSignature=1` et `keyEncipherment=1`.
- Signature numérique et authentification du client : sélection du certificat par les champ « key usage » et « extended key usage » dont la valeur des attributs `digitalSignature=1` et `id-kp-clientAuth=1`.

Par modèle de nom distinctif (DN Pattern)

Lorsque la case est cochée, le Client VPN recherche, sur token, carte à puce et dans le magasin de certificats de l'OS, le certificat dont le sujet contient le texte renseigné dans le champ **Modèle**.

2.3.3.3 Bloc Certificat PKCS #12

Compatibilité : ,

Ce bloc s'affiche uniquement si vous avez sélectionné l'option **Magasin de certificats du Client VPN** dans le bloc **Type de stockage** (cf. 2.3.3.1 Bloc Type de stockage).

Le certificat utilisateur est envoyé par le Client VPN à la passerelle pour qu'elle puisse authentifier l'utilisateur.

Pour ajouter un certificat, cliquez sur le bouton **+ IMPORTER UN CERTIFICAT**, puis suivez les instructions à l'écran.

☞ Pour une description détaillée de la procédure d'importation et de suppression d'un certificat PKCS #12, reportez-vous au « Guide de l'administrateur » du CMC.

Lorsque l'importation a réussi, le certificat est ajouté à la liste des certificats importés dans la configuration avec son nom commun, l'autorité de certification qui l'a délivré et la date d'expiration.

2.3.3.4 Bloc Options

Compatibilité :

Vérifier le certificat client par rapport à la CRL

Lorsque cette option est sélectionnée, le Client VPN vérifie la liste des certificats révoqués (CRL ou *Certificate Revocation List* en anglais) du certificat de la passerelle VPN, ainsi que celle de chaque certificat de la chaîne de certification jusqu'au certificat racine.

Le certificat racine et les certificats intermédiaires doivent être importés dans la configuration ou accessibles dans le magasin de certificats de l'OS. De même, les CRL doivent être accessibles, soit dans le magasin de certificats de l'OS, soit téléchargeables.

Il est possible de vérifier la révocation du certificat de la passerelle à l'aide du protocole de vérification de certificat en ligne en mode agrafage (OCSP ou *Online Certificate Status Protocol* en anglais). Pour cela, il convient d'ajouter le paramètre dynamique `enable_OCSP` défini à la valeur `true` (voir le chapitre 7 Gestion des paramètres dynamiques).

2.3.3.5 Bloc Identité (Local ID)

Compatibilité :

Type

Type d'identifiant de la phase d'authentification que le Client VPN envoie à la passerelle VPN distante (Local ID).

Suivant le type sélectionné, cet identifiant peut être :

- Automatique : une fois le certificat sélectionné, le type de d'identifiant du tunnel passe automatiquement à **DER ASN1 DN**, et le sujet du certificat est utilisé par défaut comme valeur de cet identifiant
- Adresse IPV4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 195.100.205.101
- DNS : un nom de domaine (type = FQDN), p. ex. gw.mondomaine.net
- KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123456
- Email : une adresse e-mail (type = USER FQDN), p. ex. support@thegreenbow.com
- Adresse IPV6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3
- DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) ; ce champ est automatiquement renseigné avec le sujet d'un certificat X.509 lorsque le tunnel est associé à un certificat utilisateur (cf. chapitre 6 Gestion des certificats)

2.3.3.6 Ajouter une deuxième authentification

Le bouton bascule permet d'activer la combinaison des deux authentifications par certificat puis par EAP. Le mode EAP (Extensible Authentication Protocol) permet d'authentifier l'utilisateur grâce à un couple identifiant/mot de passe.

Le Client VPN prend en charge la double authentification « certificat puis EAP », mais il ne prend pas en charge la double authentification « EAP puis certificat ».

2.3.3.7 Bloc EAP

Compatibilité : , ,

Popup EAP

Quand la case **Popup EAP** est cochée, une fenêtre demande à l'utilisateur de saisir son identifiant /mot de passe à chaque ouverture du tunnel.

Lorsque la case **Popup EAP** est décochée, l'identifiant et le mot de passe EAP sont mémorisés dans la configuration VPN en les renseignant dans les champs **Identifiant** et **Mot de passe**.

Il est recommandé de garder la case **Popup EAP** cochée (cf. chapitre 11 Recommandations de sécurité).

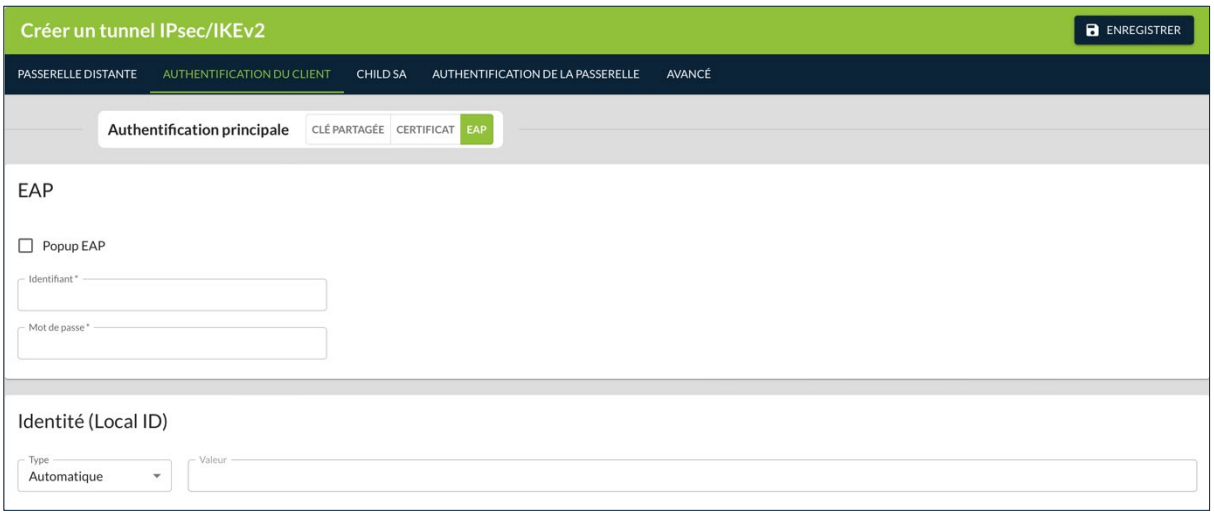
Identifiant

Lorsque la case **Popup EAP** est décochée, ce champ doit être obligatoirement renseigné. Il sert à stocker l'identifiant dans la configuration VPN.

Mot de passe

Lorsque la case **Popup EAP** est décochée, ce champ doit être obligatoirement renseigné. Il sert à stocker le mot de passe dans la configuration VPN.

2.3.4 Sous-onglet EAP



2.3.4.1 Bloc EAP

Compatibilité : , , ,

Popup EAP

Quand la case **Popup EAP** est cochée, une fenêtre demande à l'utilisateur de saisir son identifiant /mot de passe à chaque ouverture du tunnel.

Lorsque la case **Popup EAP** est décochée, l'identifiant et le mot de passe EAP sont mémorisés dans la configuration VPN en les renseignant dans les champs **Identifiant** et **Mot de passe**.

Il est recommandé de garder la case **Popup EAP** cochée (cf. chapitre 11 Recommandations de sécurité).

Identifiant

Lorsque la case **Popup EAP** est décochée, permet de stocker l'identifiant dans la configuration VPN.

Mot de passe

Lorsque la case **Popup EAP** est décochée, permet de stocker le mot de passe dans la configuration VPN.

2.3.4.2 Bloc Identité (Local ID)

Compatibilité : , , ,

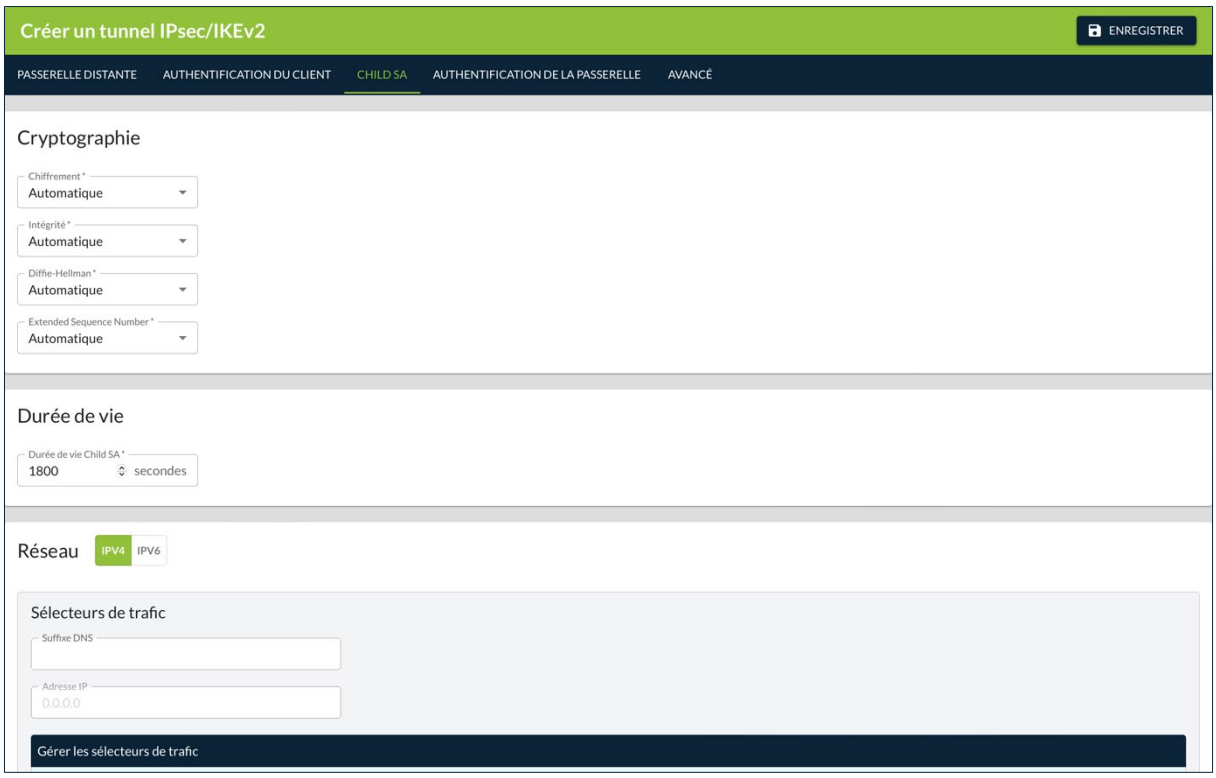
Type

Type d'identifiant de la phase d'authentification que le Client VPN envoie à la passerelle VPN distante (Local ID).

Suivant le type sélectionné, cet identifiant peut être :

- Automatique : une fois le certificat sélectionné, le type de d'identifiant du tunnel passe automatiquement à **DER ASN1 DN**, et le sujet du certificat est utilisé par défaut comme valeur de cet identifiant
- Adresse IPV4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 195.100.205.101
- DNS : un nom de domaine (type = FQDN), p. ex. gw.mondomaine.net
- KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123456
- Email : une adresse e-mail (type = USER FQDN), p. ex. support@thegreenbow.com
- Adresse IPV6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3
- DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) ; ce champ est automatiquement renseigné avec le sujet d'un certificat X.509 lorsque le tunnel est associé à un certificat utilisateur (cf. chapitre 6 Gestion des certificats)

2.4 Onglet CHILD SA



2.4.1 Bloc Cryptographie

Compatibilité : , , ,

Chiffrement

Algorithme de chiffrement négocié au cours de la phase IPsec :

- Auto[1],
- AES CBC (128, 192, 256),
- AES CTR (128, 192, 256),
- AES GCM (128, 192, 256).

Intégrité

Algorithme d'intégrité négocié au cours de la phase IPsec :

- Auto[2],
- SHA2 256,
- SHA2 384,
- SHA2 512.

Diffie-Hellman

Longueur de la clé Diffie-Hellman :

- Auto[3],
- DH14 (MODP 2048),
- DH15 (MODP 3072),
- DH16 (MODP 4096),
- DH17 (MODP 6144),
- DH18 (MODP 8192),
- DH19 (ECP 256),
- DH20 (ECP 384),
- DH21 (ECP 521),
- DH28 (EC-BP 256).

[1] **Auto** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.
[2] idem
[3] idem

Extended Sequence Number

Permet l'usage de numéros de séquence étendus de taille 64 bits (cf. RFC 4304) :

- Auto[1],
- Non,
- Oui.

Il est recommandé d'activer le mode ESN.

2.4.2 Bloc Durée de vie

Compatibilité : , , ,

Durée de vie Child SA

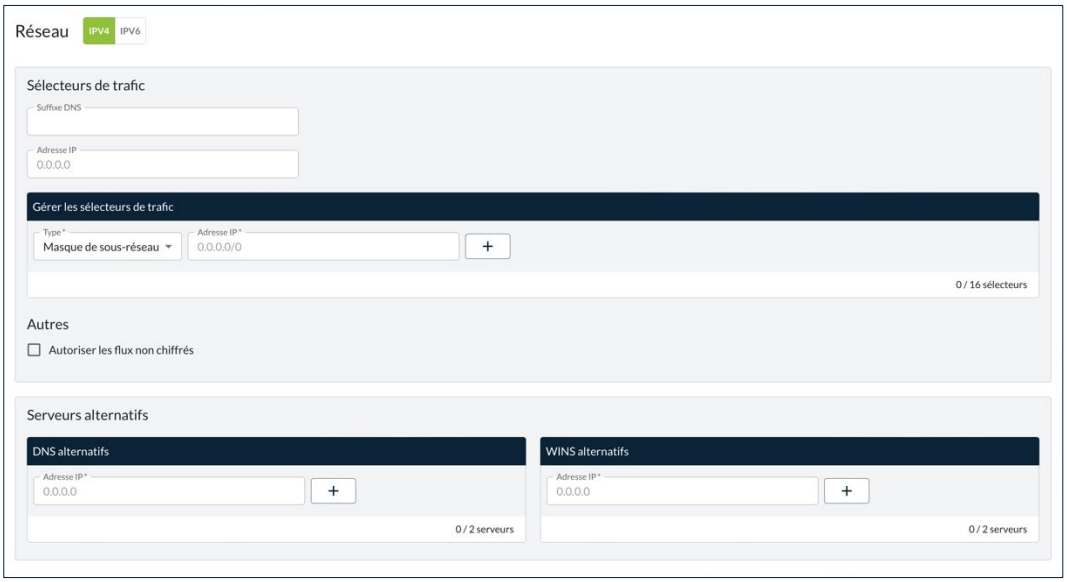
Durée en secondes entre deux renégociations.

La valeur par défaut pour la durée de vie Child SA est de 1 800 s (30 min).

2.4.3 Bloc Réseau

Compatibilité : , , ,

[1] **Auto** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.



Ce bloc contient deux onglets : IPv4 et IPv6. La seule différence réside dans le format de l'adresse dans les champs **Adresse IP**.

Lorsque l'option **Obtenir la configuration depuis la passerelle** est activée sur l'onglet **PASSERELLE DISTANTE**, il convient de la désactiver pour spécifier manuellement les sélecteurs de trafic.

2.4.3.1 Sous-bloc Sélecteurs de trafic

Si l'option **Obtenir la configuration depuis la passerelle** est activée sur l'onglet **PASSERELLE DISTANTE**, vous ne pouvez pas spécifier manuellement les sélecteurs de trafic.

Suffixe DNS

Suffixe de domaine à ajouter à chaque nom de machine, par exemple : `mozart.dev.thegreenbow`.

Ce paramètre est optionnel. Lorsqu'il est spécifié, le Client VPN essaye de traduire l'adresse de la machine sans ajouter le suffixe DNS. Puis, si la

traduction échoue, il ajoute le suffixe DNS et essaye à nouveau de traduire l'adresse.

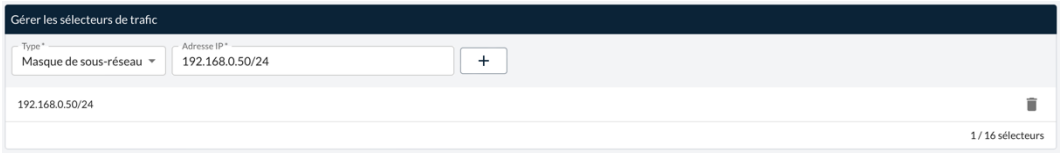
Adresse IP

Adresse IP « virtuelle » du terminal, tel qu'il sera « vu » sur le réseau distant.

Techniquement, c'est l'adresse IP source des paquets IP transportés dans le tunnel IPsec.

Pavé Gérer les sélecteurs de trafic

Si l'extrémité du tunnel est un réseau ou un terminal, sélectionnez **Masque de sous-réseau**, renseignez l'**Adresse IP**, puis cliquez sur le bouton [+] :



Vous pouvez également sélectionner **Plage**, définir l'**Adresse de début** et l'**Adresse de fin**, puis cliquez sur le bouton [+] :

Vous pouvez ajouter jusqu'à 16 sélecteurs de trafic.

La fonction **Ouvrir automatiquement ce tunnel sur détection de trafic** permet d'ouvrir automatiquement un tunnel sur détection de trafic vers l'une des adresses de la plage d'adresses spécifiée (moyennant le fait que cette plage d'adresses soit aussi autorisée dans la configuration de la passerelle VPN, voir section 4.3.4 Bloc Mode d'ouverture automatique).

Configuration « tout le trafic dans le tunnel VPN »

Il est possible de configurer le Client VPN pour que l'intégralité du trafic sortant du poste passe dans le tunnel VPN. Pour réaliser cette fonction, indiquez comme **Adresse IP** `0.0.0.0/0`.

☞ De nombreux guides de configuration du Client VPN avec différentes passerelles VPN sont disponibles sur le site web TheGreenBow : https://thegreenbow.com/fr/support/guides-dintegration/passerelles-vpn-compatibles/.

Section Autres

Autoriser les flux non chiffrés

Cette option est décochée par défaut. Dans ce cas, seul le trafic passant dans le tunnel est autorisé.

L'option de configuration **Autoriser les flux non chiffrés** réduit « l'étanchéité » du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction induit des risques de flux entrants qui pourraient transiter hors du tunnel VPN.

Il est recommandé de ne pas autoriser les flux non chiffrés.

Associée à la configuration « Passer tout le trafic dans le tunnel » (voir la section 2.4.3.1 Sous-bloc Sélecteurs de trafic), le blocage des flux non chiffrés (case décochée) permet de garantir une étanchéité totale du poste, dès lors que le tunnel VPN est ouvert.

Ce mode est recommandé.

2.4.3.2 Sous-bloc Serveur alternatifs

Si l'option **Obtenir la configuration depuis la passerelle** est activée sur l'onglet **PASSERELLE DISTANTE**, les serveurs alternatifs sont désactivés.

Table des adresses IP des serveurs DNS (2 maximum) et WINS (2 maximum) accessibles sur le réseau distant. Les adresses IP seront des adresses IPv4 ou IPv6 suivant le type de réseau choisi dans le bloc **Réseau**.

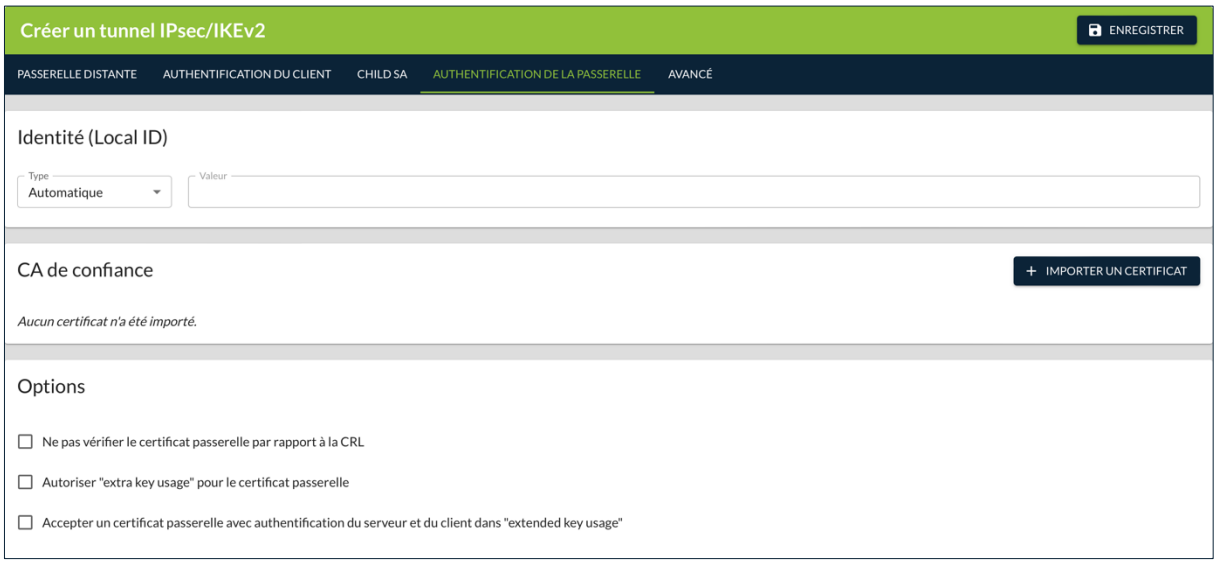
Pavé DNS alternatifs

Pour ajouter un serveur DNS alternatif, saisissez l'adresse IP dans le champ prévu à cet effet, puis cliquez sur le bouton [+].

Pavé WINS alternatifs

Pour ajouter un serveur WINS alternatif, saisissez l'adresse IP dans le champ prévu à cet effet, puis cliquez sur le bouton [+].

2.5 Onglet AUTHENTIFICATION DE LA PASSERELLE



2.5.1 Bloc Identité (Remote ID)

Compatibilité : , , ,

Type

Type d'identifiant de la phase d'authentification que le Client VPN s'attend à recevoir de la passerelle VPN distante (Remote ID).

Suivant le type sélectionné, cet identifiant peut être :

- Automatique : adresse de la passerelle
- Adresse IPV4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 80.2.3.4
- DNS : un nom de domaine (type = FQDN), p. ex. routeur.mondomaine.com
- Email : une adresse e-mail (type = USER FQDN), p. ex. admin@mondomaine.com
- Adresse IPV6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3
- DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN)
- KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123abc

⚠ Pour des raisons de sécurité, ce paramètre est obligatoire depuis la version 6.8 du Client VPN Windows Enterprise.

Valeur

Valeur attribuée au **Type**.

2.5.2 Bloc CA de confiance

Compatibilité : , , ,

Lorsque le Client VPN est configuré pour vérifier les certificats passerelle, les autorités de certification (CA) doivent être également accessibles.

☞ Pour plus d'informations sur la gestion des certificats, reportez-vous au chapitre 6 Gestion des certificats.

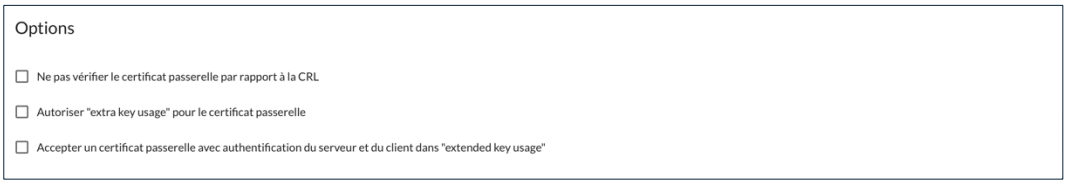
Pour importer un certificat, cliquez sur le bouton **+ IMPORTER UN CERTIFICAT**, puis suivez les instructions à l'écran.

☞ Pour une description détaillée de la procédure d'importation et de suppression d'un certificat de CA, reportez-vous au « Guide de l'administrateur » du CMC.

Lorsque l'importation a réussi, le certificat est ajouté à la liste des certificats importés dans la configuration avec son nom commun, l'autorité de certification qui la délivré et la date d'expiration.

2.5.3 Bloc Options

Compatibilité : ,



Ne pas vérifier le certificat passerelle par rapport à la CRL

Cette option empêche le téléchargement de la CRL de validation du certificat utilisateur.

☞ Pour en savoir davantage sur la liste de révocation de certificats (*Certificate Revocation List* ou CRL), reportez-vous à la section 6.4 Restriction du téléchargement des CRL.

Autoriser "extra key usage" pour le certificat passerelle

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Key Usage. Elle doit :

- être présente,
- être marquée comme critique et
- contenir uniquement les valeurs `digitalSignature` et/ou `nonRepudation`.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout en activant cette option.

Dans cette configuration, le certificat sera également validé si l'extension Key Usage contient l'une des combinaisons de valeurs suivantes :

- `digitalSignature` + `keyEncipherment` + `keyAgreement`
- `digitalSignature` + `keyAgreement`
- `nonRepudiation` + `keyEncipherment`
- `nonRepudiation` + `keyEncipherment` + `keyAgreement`
- `nonRepudiation` + `keyAgreement`
- `keyEncipherment`
- `keyEncipherment` + `keyAgreement`

De plus, dans cette configuration l'extension Key Usage peut être marquée comme non critique.

Conformément aux exigences de sécurité, la valeur `keyEncipherment` de l'extension Key Usage a été rendue obsolète et remplacée par la valeur `nonRepudiation`, qui est désormais acceptée par défaut Cependant, la version 7.5 du Client VPN Windows Enterprise continue d'accepter la valeur `keyEncipherment` sans l'utilisation du paramètre dynamique `allow_extra_keyusage`.

Il est recommandé de préférer la valeur `nonRepudiation` de l'extension Key Usage à la valeur `keyEncipherment`.

Accepter un certificat passerelle avec authentification du serveur et du client dans "extended key usage"

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Extended Key Usage. Cette dernière peut être absente ou présente. Si elle est présente, elle doit :

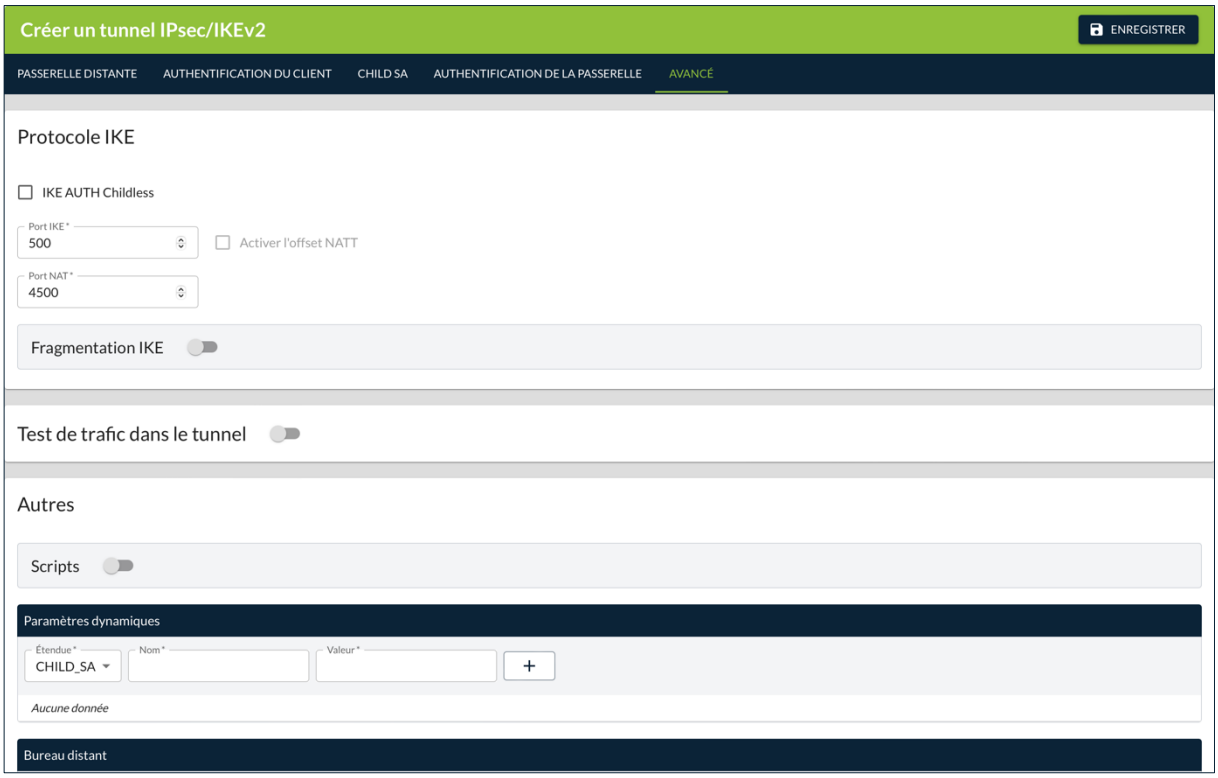
- être marquée comme non-critique et
- uniquement contenir les valeurs suivantes :
  - `id-kp-serverAuth` ou
  - `id-kp-serverAuth` + `id-kp-ipsecIKE`.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en activant cette option.

Dans cette configuration, le certificat sera également validé si l'extension Extended Key Usage contient l'une des combinaisons de valeurs suivantes :

- `id-kp-ServerAuth` + `id-kp-ClientAuth` ou
- `id-kp-serverAuth` + `id-kp-ClientAuth` + `id-kp-ipsecIKE`.

2.6 Onglet AVANCÉ



2.6.1 Bloc Protocole IKE

Compatibilité : , , ,

IKE AUTH Childless

Lorsque ce mode est activé, le Client VPN tentera d'effectuer l'initiation des échanges IKE sans création de Child SA, conformément au RFC 6023.

Ce mode est recommandé.

Port IKE

Les échanges IKE Init (pendant la phase d'authentification IKE) s'effectuent sur le protocole UDP, en utilisant par défaut le port 500. Le paramétrage du port IKE permet de passer les équipements réseau (pare-feux, routeurs) qui filtrent ce port 500.

Ce champ doit être obligatoirement renseigné. Sa valeur par défaut est le port 500. Sa valeur doit être comprise entre 1 et 65535.

La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Auth sur un port différent de 500.

Activer l'offset NATT

Lorsque le port IKE est différent de 500, il peut être nécessaire de cocher cette option pour que la passerelle accepte la connexion. La case à cocher est grisée tant que la valeur par défaut de 500 n'est pas modifiée.

Port NAT

Les échanges IKE Auth, les échanges IKE Child SA et le trafic IPsec s'effectuent sur le protocole UDP, en utilisant par défaut le port 4500. Le paramétrage du port NAT permet de passer les équipements réseau (pare-feux, routeurs) qui filtrent ce port 4500.

Ce champ doit être obligatoirement renseigné. Sa valeur par défaut est le port 4500. Sa valeur doit être comprise entre 1 et 65535.

La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Child SA sur un port différent de 4500.

Fragmentation IKE

Cliquez sur le bouton bascule **Fragmentation IKE** pour activer la fragmentation des paquets IKEv2 conformément à la RFC 7383. Le champ **Taille des fragments** s'affiche.

Cette fonction permet d'éviter que les paquets IKEv2 ne soient fragmentés par le réseau IP traversé.

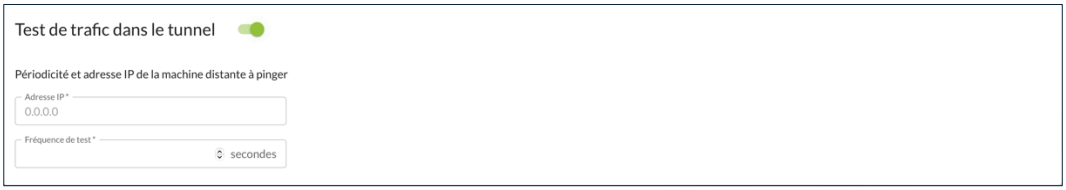
En général, il convient de spécifier une taille de fragment inférieure de 200 octets à la MTU de l'interface physique, par exemple 1300 octets dans le cas d'une MTU classique de 1500 octets.

Dès lors que la fragmentation IKE est activée, ce champ doit être obligatoirement renseigné. Sa valeur doit être comprise entre 200 et 9216 octets.

2.6.2 Bloc Test de trafic dans le tunnel

Compatibilité :

Cliquez sur le bouton bascule **Test de trafic dans le tunnel** pour vérifier régulièrement la connectivité au réseau distant. Si la connectivité est perdue, le Client VPN ferme automatiquement le tunnel puis tente de le rouvrir. Les champs **Adresse IP** et **Fréquence de test** s'affichent.



Adresse IP

Le champ **Adresse IP** est l'adresse d'une machine située sur le réseau distant, censée répondre aux « ping » envoyés par le Client VPN. S'il n'y a pas de réponse au « ping », la connectivité est considérée comme perdue.

Dès lors que le test de trafic dans le tunnel est activé, ce champ doit être obligatoirement renseigné.

Si le tunnel est configuré en IPv4 (bouton dans le bloc **Réseau** de l'onglet **CHILD SA**, voir section 2.4.3 Bloc Réseau), c'est le champ IPv4 qui est présenté. Si le tunnel est configuré en IPv6, c'est le champ IPv6 qui est présenté.

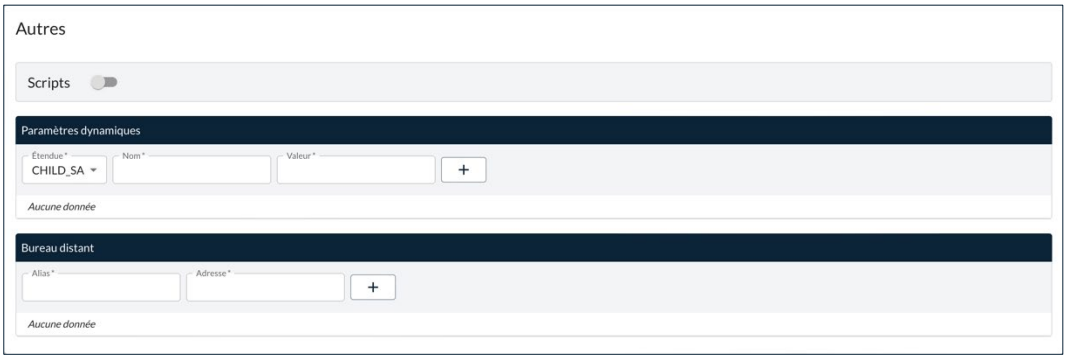
Fréquence de test

Le champ **Fréquence de test** indique la période, exprimée en secondes, entre chaque « ping » émis par le Client VPN à destination de la machine dont l'adresse IP est spécifiée au-dessus.

Dès lors que le test de trafic dans le tunnel est activé, ce champ doit être obligatoirement renseigné. Sa valeur doit être comprise entre 1 et 65535.

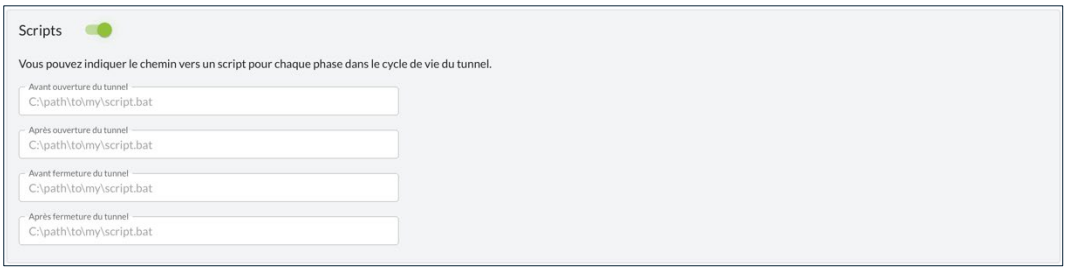
2.6.3 Bloc Autres

Compatibilité : ,



2.6.3.1 Scripts

Cliquez sur le bouton bascule **Scripts** pour indiquer le chemin vers des scripts configurables exécutés dans les différentes phase du cycle de vie d'un tunnel VPN. Les champs **Avant ouverture du tunnel**, **Après ouverture du tunnel**, **Avant fermeture du tunnel** et **Après fermeture du tunnel** s'affichent.



Saisissez le chemin vers le script à exécuter pour la phase correspondante.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à a section 9.5 Scripts.

2.6.3.2 Paramètres dynamiques

Le Client VPN Windows Enterprise permet si besoin de configurer des paramètres dynamiques additionnels au niveau de la configuration IKE Auth ou Child SA

☞ Pour en savoir davantage sur l'utilisation des paramètres dynamiques, reportez-vous au chapitre 7 Gestion des paramètres dynamiques.

2.6.3.3 Bureau distant

Alias

Nom est utilisé pour identifier la connexion dans les différents menus du Client VPN.

Adresse

Adresse IP ou nom Windows du poste distant.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à la section 9.7 Partage de bureau distant.

3 Page Créer un / Modifier le tunnel OpenVPN

3.1 Introduction

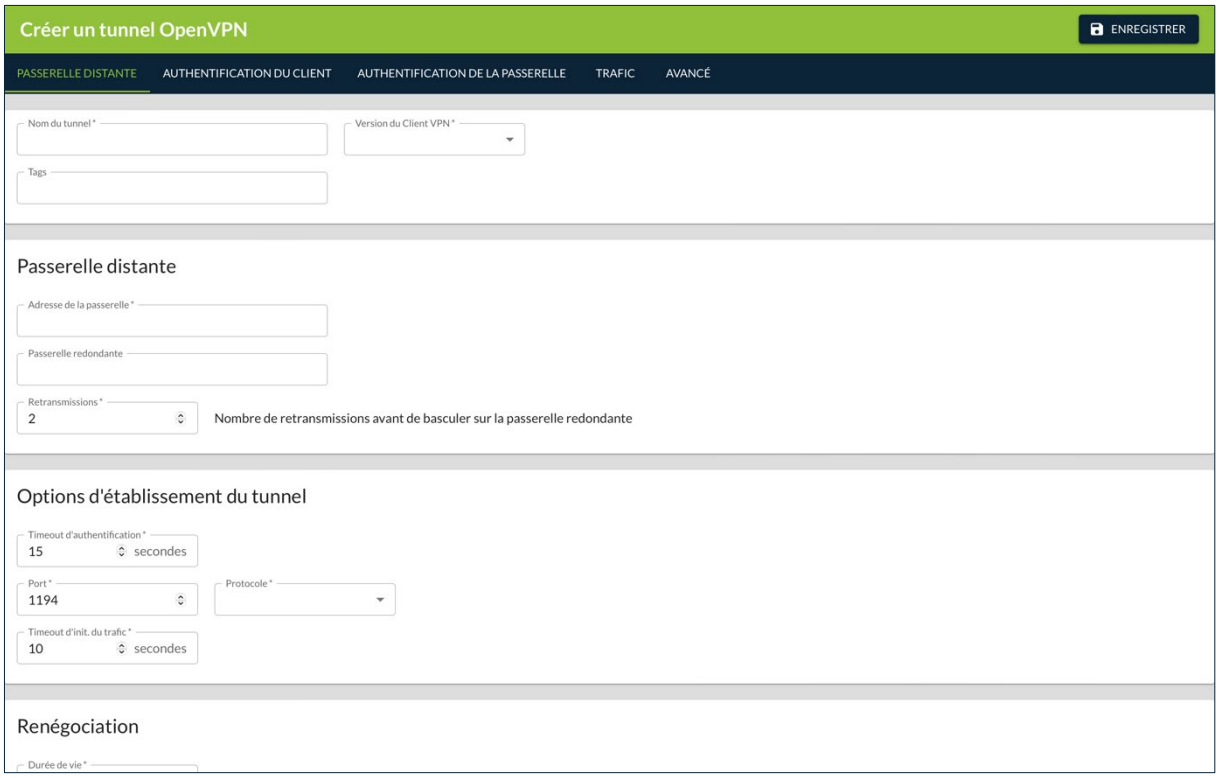
Les champs figurant sur les pages **Créer un tunnel OpenVPN** et **Modifier le tunnel OpenVPN** sont identiques. Ils sont donc décrits de façon commune ci-dessous. Ces pages comportent chacune les cinq onglets suivants :

- **PASSERELLE DISTANTE**, voir 3.2
- **AUTHENTIFICATION DU CLIENT**, voir 3.3
- **AUTHENTIFICATION DE LA PASSERELLE**, voir 3.4
- **TRAFIC**, voir 3.5
- **AVANCÉ**, voir 3.6

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour comprendre les différences entre les protocoles IPsec/IKEv2 et OpenVPN.

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour comprendre les notions de tunnel, connexion et configuration telles qu'elles sont utilisées chez TheGreenBow.

3.2 Onglet PASSERELLE DISTANTE



3.2.1 Bloc d'identification

Compatibilité : Windows, macOS, Android, Linux

Le premier bloc de l'onglet n'a pas de titre et sert à identifier le tunnel.

Nom du tunnel

Nom attribué au tunnel.

Longueur max. : 50

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

Ce champ doit être obligatoirement renseigné.

Version du Client VPN

Version du Client VPN TheGreenBow pour laquelle le tunnel est créé.

Le tunnel peut donc être utilisé avec n'importe quel Client VPN d'un niveau de version donné, p. ex. le Client VPN Windows Enterprise v7.4, le Client VPN macOS v2.4 et le Client VPN Android v6.4.

Ce champ doit être obligatoirement renseigné.

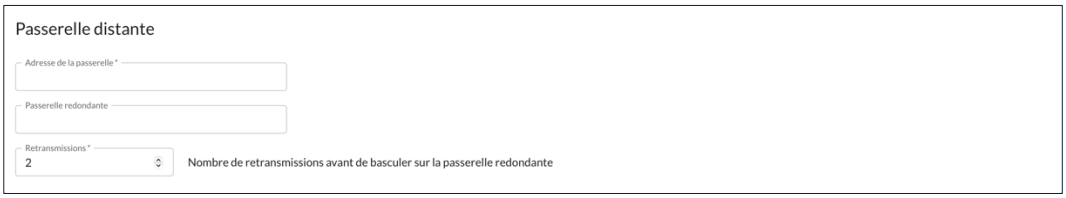
Tags

Tags destinés à faciliter le filtrage des tunnels dans la liste des tunnels.

Vous pouvez saisir n'importe quel type de caractère. Appuyez ensuite sur Entrée pour former le tag. Saisissez autant de tags que nécessaire.

3.2.2 Bloc Passerelle distante

Compatibilité : Windows, macOS, Android, Linux



Adresse de la passerelle

Adresse IP (IPv6 ou IPv4) ou adresse DNS de la passerelle VPN distante.

Ce champ doit être obligatoirement renseigné.

Passerelle redondante

Définit l'adresse d'une passerelle VPN de secours sur laquelle le Client VPN bascule lorsque la passerelle VPN initiale est indisponible ou inaccessible.

L'adresse de la passerelle VPN redondante peut être une adresse IP ou DNS.

Ce champ est facultatif.

⚠ La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction **Tunnel de repli**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé.

☞ Pour une description détaillée de cette fonction, reportez-vous à la section 9.2 Passerelle redondante.

Retransmissions

Nombre de retransmissions de messages protocolaires IKE avant échec.

Ce champ doit être obligatoirement renseigné.

3.2.3 Bloc Options d'établissement du tunnel

Compatibilité : , , ,

Timeout d'authentification

Délai d'établissement de la phase d'authentification au bout duquel on considère que le tunnel ne s'ouvrira pas. À échéance de ce timeout, le tunnel est fermé.

Ce champ doit être obligatoirement renseigné. Sa valeur par défaut est de 15 secondes.

Port

Numéro du port utilisé pour l'établissement du tunnel.

Ce champ doit être obligatoirement renseigné. Par défaut, le port est configuré à 1194.

Protocole

Sélection du protocole à utiliser. Généralement, le tunnel utilise UDP.

Ce champ doit être obligatoirement renseigné.

Timeout d'init. du trafic

Phase d'établissement du tunnel : délai au bout duquel, si toutes les étapes n'ont pas été établies, le tunnel est fermé.

Ce champ doit être obligatoirement renseigné. Sa valeur par défaut est de 10 secondes.

3.2.4 Bloc Renégociation

Compatibilité : , , ,

Les clés peuvent être renégociées sur échéance de 3 critères (qui peuvent être combinés) :

- durée de vie, exprimée en secondes dans le champ **Durée de vie** ;
- quantité de trafic, exprimée en Ko dans le champ **Octets** ;
- quantité de paquets, exprimée en nombre de paquets dans le champ **Paquets**.

Si plusieurs critères sont configurés, les clés sont renégociées sur échéance du premier critère vérifié.

3.2.5 Bloc Dead Peer Detection (DPD)

Compatibilité : , , ,

La fonction DPD (Dead Peer Detection) permet aux deux extrémités du tunnel de vérifier mutuellement leur présence.

La fonction de DPD est active une fois le tunnel ouvert. Associé à une passerelle redondante, le DPD permet au Client VPN de basculer automatiquement d'une passerelle à l'autre sur indisponibilité de l'une ou l'autre.

Ping passerelle

Période exprimée en seconde d'envoi par le Client VPN d'un « ping » vers la passerelle. Cet envoi permet à la passerelle de déterminer que le Client VPN est toujours présent.

Ce champ doit être obligatoirement renseigné. Sa valeur par défaut est de 0 secondes.

Détection de la passerelle

Sous-bloc qui comporte un champ **Délai** et deux boutons radio permettant de définir l'action à exécuter lorsqu'une inactivité de la passerelle est détectée.

Délai

Durée en secondes à l'issue de laquelle, si aucun « ping » n'a été reçu de la passerelle, celle-ci est considérée comme indisponible.

Sur détection d'inactivité

Lorsque la passerelle est détectée comme indisponible (c'est-à-dire à la fin du **Délai** de détection de la passerelle), choisissez si le Client VPN doit **Fermer le tunnel** ou tenter de **Rouvrir le tunnel**.

3.2.6 Bloc Autres

Compatibilité : , , ,

Explicit exit

Cette option est cochée par défaut. Elle configure le Client VPN pour envoyer une trame spécifique de clôture du tunnel VPN à la passerelle, quand on ferme le tunnel.

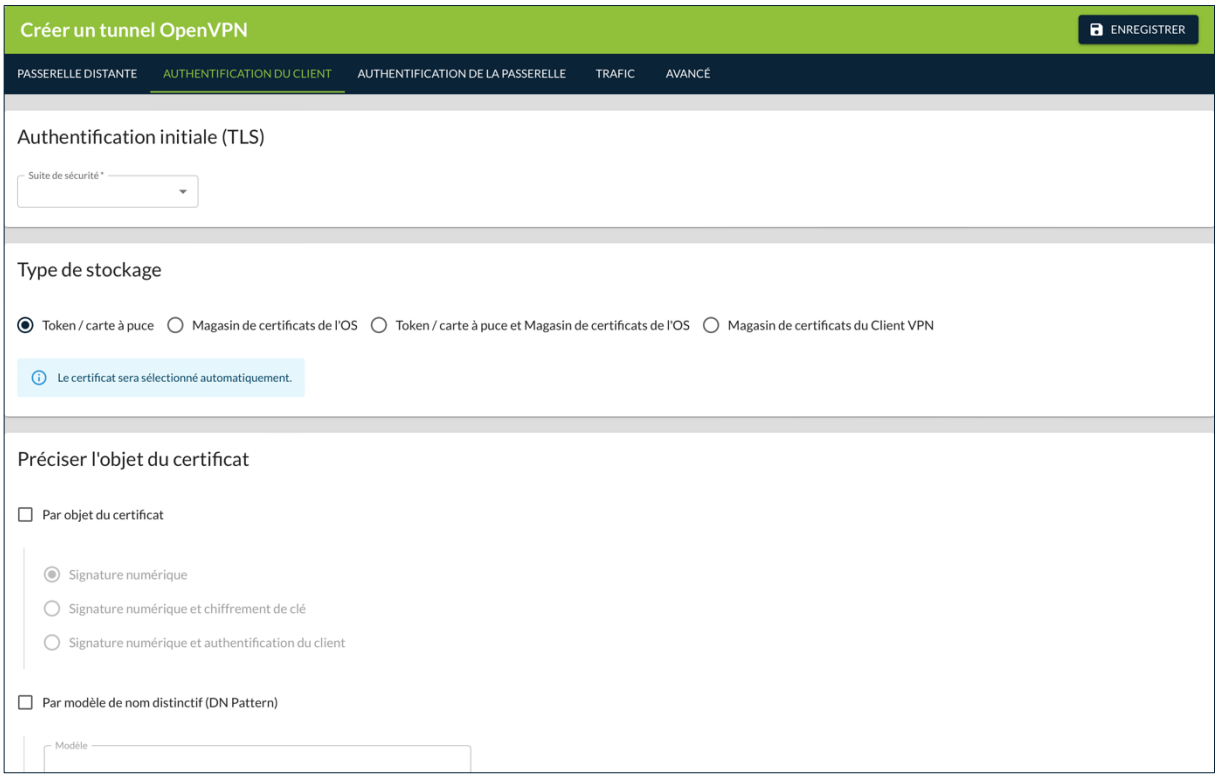
Si cette option n'est pas cochée, la passerelle utilise le DPD pour fermer le tunnel de son côté, ce qui est moins performant.

Vérification des options de la passerelle

Cette liste déroulante permet de définir le niveau de cohérence entre les paramètres du tunnel VPN et ceux de la passerelle (algorithmes de chiffrement, compression, etc.).

- **Appliquer** : Réglage par défaut. Les paramètres de la passerelle sont appliqués.
- **Oui** : La cohérence est vérifiée sur l'ensemble des paramètres VPN. Le tunnel VPN ne peut s'ouvrir si un paramètre diffère.
- **Non** : La cohérence n'est pas vérifiée avant ouverture du tunnel. Le tunnel VPN tente de s'ouvrir, quitte à ce qu'aucun trafic ne puisse passer parce que certains paramètres sont incohérents.
- **Simple** : La cohérence entre le Client VPN et la passerelle n'est vérifiée que sur les paramètres essentiels.

3.3 Onglet AUTHENTIFICATION DU CLIENT



3.3.1 Bloc Authentification initiale (TLS)

Compatibilité : , , ,

Cette liste déroulante permet de configurer le niveau de sécurité de la phase d'authentification dans l'échange SSL :

- **Automatique** : toutes les suites cryptographiques (sauf nulle) sont proposées à la passerelle qui décide de la meilleure suite à utiliser.
- **Basse** : seules les suites cryptographiques « basses » sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement de 128 bits.
- **Normale** : seules les suites cryptographiques normales sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement supérieurs ou égaux à 128 bits.
- **Haute** : suite TLS 1.3 négociée avec la passerelle, incluant :
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256

3.3.2 Bloc Type de stockage

Compatibilité : , , , (voir notes pour les limitations)

Indique l'emplacement où est stocké le certificat :

- Token / carte à puce
- Magasin de certificats de l'OS
- Token / carte à puce et Magasin de certificats de l'OS[1]
- Magasin de certificats du Client VPN[2]

Dans les trois premiers cas, le certificat sera sélectionné automatiquement. Si vous sélectionnez l'option **Magasin de certificat du Client VPN**, le bloc **Préciser l'objet du certificat** est remplacé par le bloc **Certificat PKCS #12**, voir 2.3.3.3 Bloc Certificat PKCS #12.

3.3.3 Bloc Préciser l'objet du certificat

Compatibilité : ,

[1] Cette option est uniquement disponible pour les clients de version 7.4 / 2.4 / 6.4 et 7.5 / 2.5 / 6.5.
[2] Correspond à l'enregistrement du certificat dans la configuration VPN.

Par objet du certificat

Lorsque la case est cochée, le certificat est sélectionné en fonction de son champ « key usage » :

- Signature numérique : sélection du certificat par le champ « key usage » dont la valeur de l'attribut `digitalSignature=1`.
- Signature numérique et chiffrement de clé : sélection du certificat par le champ « key usage » dont la valeur des attributs `digitalSignature=1` et `keyEncipherment=1`.
- Signature numérique et authentification du client : sélection du certificat par les champ « key usage » et « extended key usage » dont la valeur des attributs respectifs `digitalSignature=1` et `id-kp-clientAuth=1`.

Par modèle de nom distinctif (DN Pattern)

Lorsque la case est cochée, le Client VPN recherche, sur token, carte à puce et dans le magasin de certificats de l'OS, le certificat dont le sujet contient le texte renseigné dans le champ **Modèle**.

3.3.4 Bloc Certificat PKCS #12

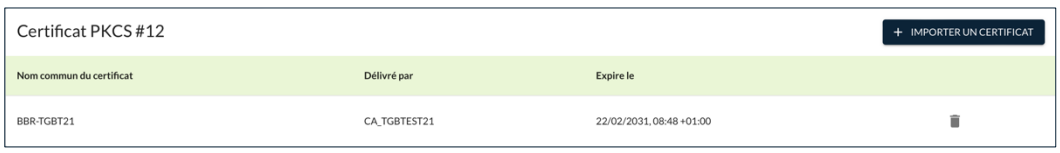
Compatibilité : , , ,

Ce bloc s'affiche, si vous avez sélectionné l'option **Magasin de certificats du Client VPN** dans le bloc Type de stockage (cf. 3.3.2 Bloc Type de stockage).

Cliquez sur le bouton **+ IMPORTER UN CERTIFICAT**, puis suivez les instructions à l'écran.

☞ Pour une description détaillée de la procédure d'importation d'un certificat de CA, reportez-vous au « Guide de l'administrateur » du CMC.

Lorsque l'importation a réussi, le certificat est ajouté à la liste des certificats importés dans la configuration avec son nom commun, l'autorité de certification qui la délivré et la date d'expiration.



3.3.5 Bloc Authentification supplémentaire

Compatibilité : , , ,

Cette option apporte un niveau de sécurité supplémentaire en demandant à l'utilisateur la saisie d'un identifiant / mot de passe à chaque ouverture du tunnel.

Popup à l'ouverture du tunnel

Lorsque cette option est cochée, l'identifiant et le mot de passe seront demandés à l'utilisateur à chaque ouverture du tunnel. Lorsqu'elle est décochée, l'identifiant et le mot de passe doivent être saisis ici de manière permanente. L'utilisateur n'aura alors pas besoin de les saisir à chaque ouverture du tunnel.

Il est recommandé de garder la case **Popup à l'ouverture du tunnel cochée** (cf. chapitre 11 Recommandations de sécurité).

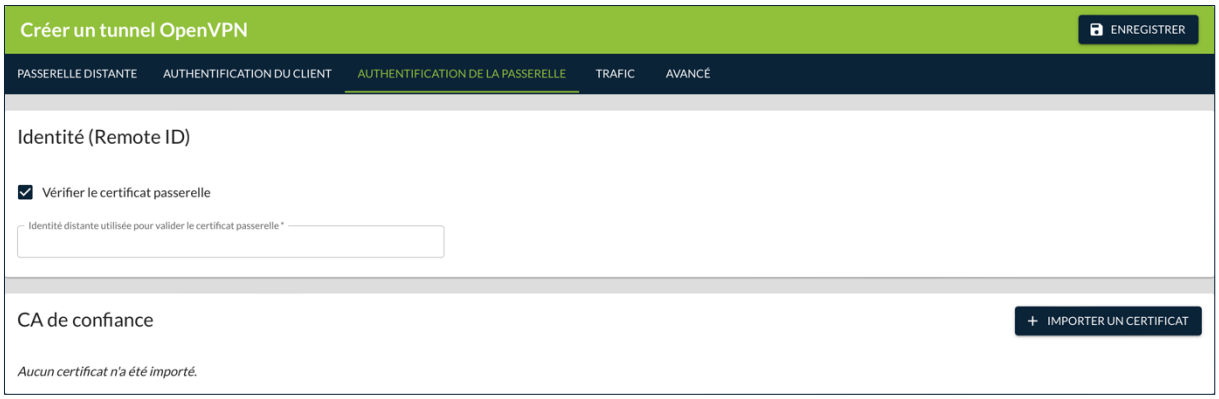
Identifiant

Lorsque la case **Popup à l'ouverture du tunnel** est décochée, ce champ doit être obligatoirement renseigné. Il sert à stocker l'identifiant dans la configuration VPN.

Mot de passe

Lorsque la case **Popup à l'ouverture du tunnel** est décochée, ce champ doit être obligatoirement renseigné. Il sert à stocker le mot de passe dans la configuration VPN.

3.4 Onglet AUTHENTIFICATION DE LA PASSERELLE



3.4.1 Bloc Identité (Remote ID)

Compatibilité : , , ,

Vérifier le certificat passerelle

Cette option est cochée par défaut. Elle spécifie le niveau de contrôle appliqué au certificat de la passerelle.

Lorsqu'elle est cochée, la validité du certificat est vérifiée sur la base du champ **Identité utilisée pour valider le certificat passerelle**, qui doit être obligatoirement renseigné. Il s'agit du sujet du certificat de la passerelle.

Lorsqu'elle est décochée, la validité du certificat n'est pas vérifiée.

3.4.2 Bloc CA de confiance

Compatibilité : , , ,

Lorsque le Client VPN est configuré pour vérifier les certificats passerelle, les autorités de certification (CA) doivent être également accessibles.

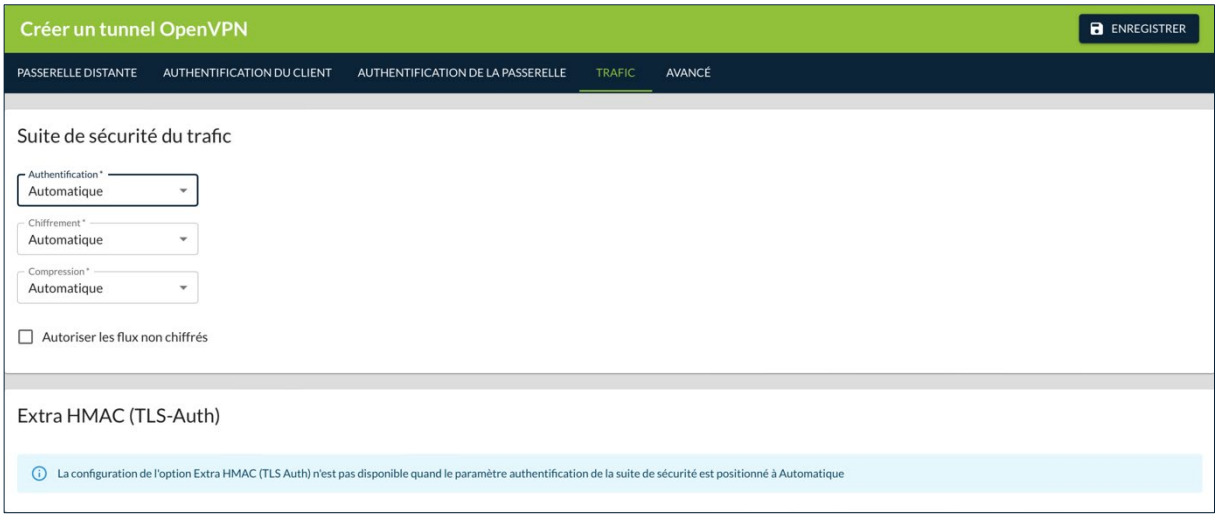
☞ Pour plus d'informations sur la gestion des certificats passerelle, reportez-vous à la section 6.3 Certificat de la passerelle VPN.

Pour importer un certificat, cliquez sur le bouton **+ IMPORTER UN CERTIFICAT**, puis suivez les instructions à l'écran.

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour une description détaillée de la procédure d'importation et de suppression d'un certificat de CA.

Lorsque l'importation a réussi, le certificat est ajouté à la liste des certificats importés dans la configuration avec son nom commun, l'autorité de certification qui la délivré et la date d'expiration.

3.5 Onglet TRAFIC



3.5.1 Bloc Suite de sécurité du trafic

Compatibilité : , , ,

Authentification

Algorithme d'authentification négocié pour le trafic :

- Automatique[1],
- SHA-256,
- SHA-384,
- SHA-512.

Si vous souhaitez activer l'option **Extra HMAC** (cf. 3.5.2 Bloc Extra HMAC (TLS-Auth)), l'algorithme d'authentification ne peut être **Automatique**. Il doit être configuré explicitement, et doit être identique à celui choisi côté passerelle.

Chiffrement

Algorithme de chiffrement du trafic :

- Automatique[2],
- AES CBC 128,
- AES CBC 192,
- AES CBC 256.

Compression

Compression du trafic :

- Auto[3],
- LZ0,
- Non,
- LZ4.

Autoriser les flux non chiffrés

Lorsque cette option est décochée, seul le trafic passant dans le tunnel est autorisé. L'option de configuration **Autoriser les flux non chiffrés** réduit « l'étanchéité » du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction induit des risques de flux entrants qui pourraient transiter hors du tunnel VPN.

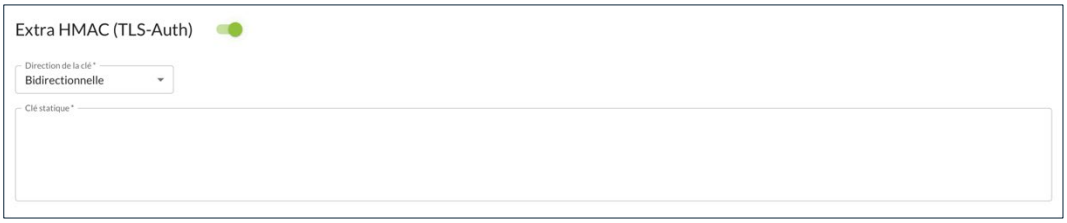
Il est recommandé de ne pas autoriser les flux non chiffrés.

[1] **Automatique** signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.
[2] idem
[3] idem

3.5.2 Bloc Extra HMAC (TLS-Auth)

Compatibilité : , , ,

Cliquez sur le bouton bascule **Extra HMAC (TLS-Auth)** pour ajouter un niveau d'authentification aux paquets échangés entre le Client VPN et la passerelle VPN. Les champs **Direction de la clé** et **Clé statique** s'affichent :



Pour être opérationnelle, cette option doit aussi être configurée sur la passerelle (sur une passerelle, cette option est souvent appelée « TLS-Auth »)

Direction de la clé

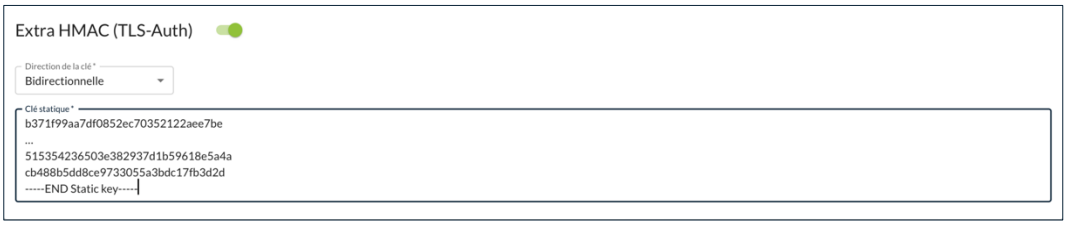
Sélectionnez la **Direction de la clé** :

- **BiDir** : La clé spécifiée est utilisée dans les deux sens (mode par défaut).
- **Client** : La direction de la clé à configurer sur la passerelle doit être **Serveur**.
- **Serveur** : La direction de la clé à configurer sur la passerelle doit être **Client**.

Clé statique

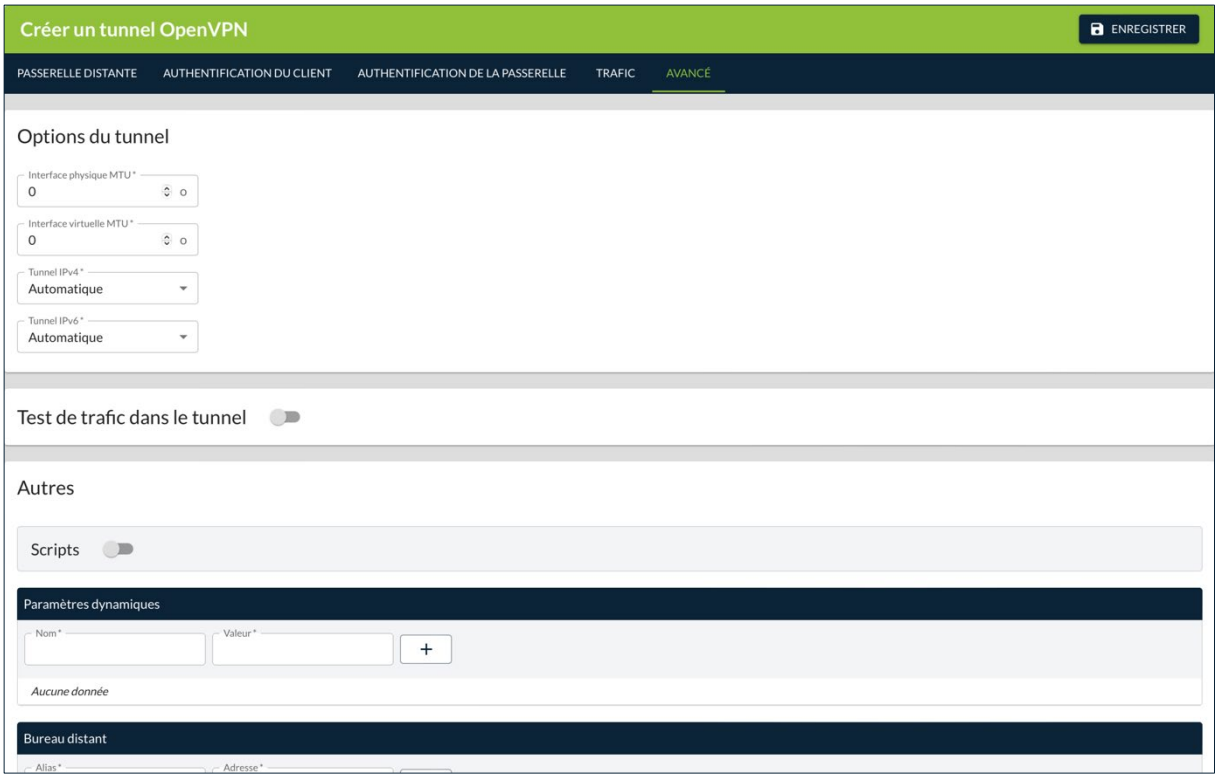
Quand cette option est sélectionnée, une clé doit être saisie dans le champ situé en dessous de la case cochée. Cette clé doit être saisie à l'identique sur la passerelle. C'est une suite de caractères hexadécimaux, dont le format est le suivant :

```
-----BEGIN Static key-----
362722d4fbff4075853fbe6991689c36
b371f99aa7df0852ec70352122aee7be
...
515354236503e382937d1b59618e5a4a
cb488b5dd8ce9733055a3bdc17fb3d2d
-----END Static key-----
```



La configuration de l'option **Extra HMAC (TLS Auth)** n'est pas disponible quand le paramètre **Authentification** de la suite de sécurité est positionné à **Automatique** (cf. 3.5.1 Bloc Suite de sécurité du trafic).

3.6 Onglet AVANCÉ



3.6.1 Bloc Options du tunnel

Compatibilité : , , ,

Interface physique MTU

Taille maximale des paquets OpenVPN.

Permet de spécifier une taille de paquet de telle sorte que les trames OpenVPN ne soient pas fragmentées au niveau réseau.

Par défaut, la MTU spécifiée est à 0, ce qui signifie que le logiciel prend la valeur de la MTU de l'interface physique.

Ce champ doit être obligatoirement renseigné. Sa valeur doit être comprise entre 0 et 32 767.

Interface virtuelle MTU

Par défaut, la MTU de l'interface virtuelle est à 0, ce qui signifie que le logiciel prend la valeur de la MTU de l'interface physique.

Il est recommandé de configurer une valeur de MTU pour l'interface virtuelle qui est inférieure à celle pour l'interface physique.

Ce champ doit être obligatoirement renseigné. Sa valeur doit être comprise entre 0 et 32 767.

Tunnel IPv4

Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv4 :

- **Automatique** : Accepte ce qui est envoyé par la passerelle.
- **Activé** : Vérifie que ce qui est envoyé par la passerelle correspond au comportement configuré. Si ce n'est pas le cas, un message d'alerte est affiché dans la **Console** et le tunnel ne se monte pas.
- **Désactivé** : Ignore ce qui est envoyé par la passerelle.

Vérifier que les deux choix **Tunnel IPv4** et **Tunnel IPv6** ne sont pas tous deux sur **Désactivé**.

Tunnel IPv6

Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv6 :

- **Automatique** : Accepte ce qui est envoyé par la passerelle.
- **Activé** : Vérifie que ce qui est envoyé par la passerelle correspond au comportement configuré. Si ce n'est pas le cas, un message d'alerte est affiché dans la **Console** et le tunnel ne se monte pas.
- **Désactivé** : Ignore ce qui est envoyé par la passerelle.

Vérifier que les deux choix **Tunnel IPv4** et **Tunnel IPv6** ne sont pas tous deux sur **Désactivé**.

3.6.2 Bloc Test de trafic dans le tunnel

Compatibilité : ,

Cliquez sur le bouton bascule **Test de trafic dans le tunnel** pour vérifier l'état de la connexion. Les champs **Adresse IP** et **Fréquence de test** s'affichent :

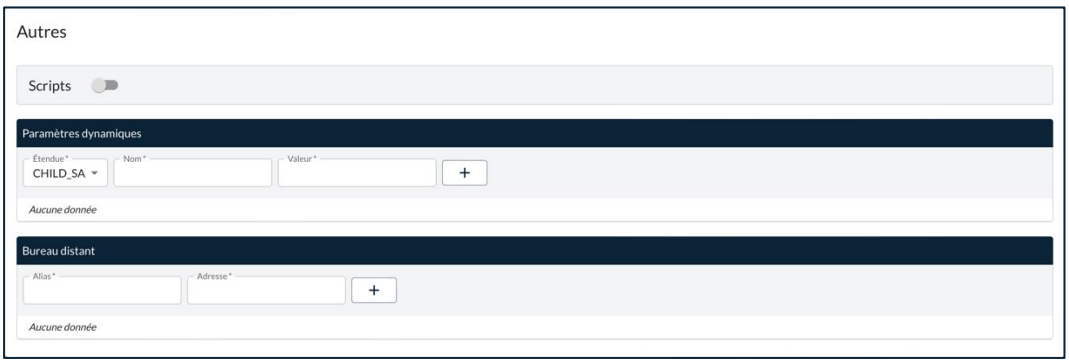
Si ces champs sont renseignés, le Client VPN tente de faire un « ping » sur ces adresses après ouverture du tunnel VPN. L'état de la connexion (réponse au ping ou absence de réponse au ping) est affiché dans la **Console**.

Il n'est pas obligatoire de renseigner les deux champs.

Aucune action particulière n'est faite s'il n'y a pas de réponse au « ping ».

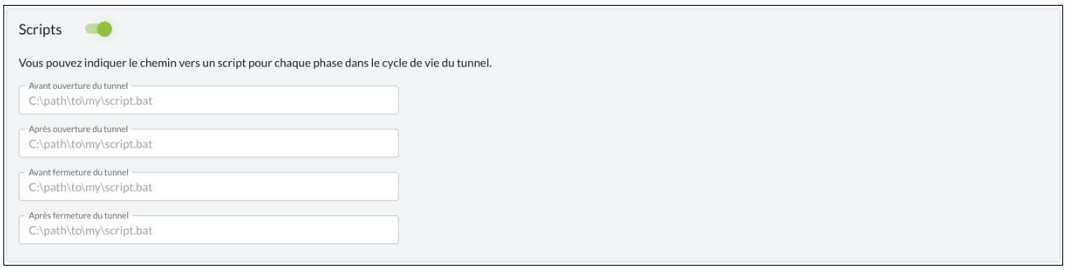
3.6.3 Bloc Autres

Compatibilité : ,



3.6.3.1 Scripts

Cliquez sur le bouton bascule **Scripts** pour indiquer le chemin vers des scripts configurables exécutés dans les différentes phase du cycle de vie d'un tunnel VPN. Les champs **Avant ouverture du tunnel**, **Après ouverture du tunnel**, **Avant fermeture du tunnel** et **Après fermeture du tunnel** s'affichent.



Saisissez le chemin vers le script à exécuter pour la phase correspondante.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à a section 9.5 Scripts.

3.6.3.2 Paramètres dynamiques

Compatibilité : ,

Le Client VPN Windows Enterprise permet si besoin de configurer des paramètres dynamiques additionnels au niveau de la configuration TLS.

☞ Pour en savoir davantage sur l'utilisation des paramètres dynamiques, reportez-vous au chapitre 7 Gestion des paramètres dynamiques.

3.6.3.3 Bureau distant

Compatibilité :

Alias

Nom est utilisé pour identifier la connexion dans les différents menus du Client VPN.

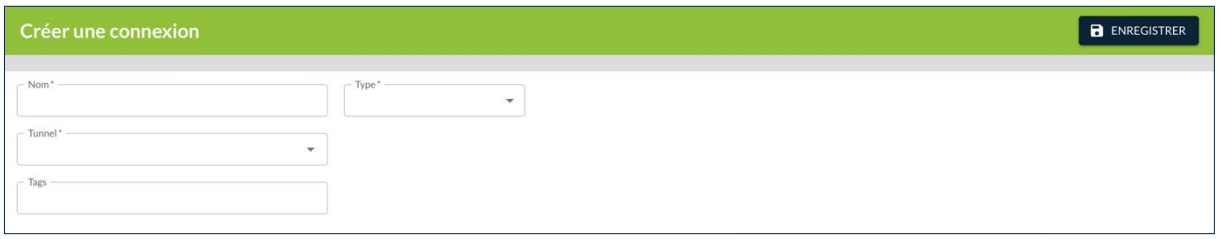
Adresse

Adresse IP ou nom Windows du poste distant.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à la section 9.7 Partage de bureau distant.

4 Page Créer une / Modifier la connexion

4.1 Introduction



Les blocs et champs figurant sur les pages **Créer une connexion** et **Modifier la connexion** sont identiques. Ils sont donc décrits de façon commune ci-dessous. De plus, ils varient en fonction d'un choix fondamental opéré à la création de la connexion et qui ne peut plus être modifié une fois la connexion créée, à savoir le **Type** de connexion : **Classique** ou **TrustedConnect**.

⚠ Les connexions de type TrustedConnect sont uniquement compatibles avec le Client VPN Windows Enterprise.

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour comprendre les notions de tunnel, connexion et configuration telles qu'elles sont utilisées chez TheGreenBow.

4.2 Bloc d'identification

Compatibilité : , , ,

Le premier bloc de la page n'a pas de titre et sert à identifier la connexion et définir son type.

Nom

Nom attribué à la connexion.

Longueur max. : 50

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

Ce champ doit être obligatoirement renseigné.

Type

Liste déroulante définissant le type de connexion. Une fois que la connexion a été enregistrée, le type ne peut plus être modifié. Les blocs affichés dans la section Paramètres avancés de la page **Créer une connexion** varient en fonction du type sélectionné. Les deux types disponibles sont les suivants :

- Classique,
- TrustedConnect.

⚠ Les connexions de type TrustedConnect sont uniquement compatibles avec le Client VPN Windows Enterprise.

Tunnel

Liste déroulante contenant tous les tunnels définis dans le CMC triés dans l'ordre de création. Dans la liste, le nom est suivi du type de protocole (IPsec/IKEv2 ou OpenVPN) et de la version des Clients VPN indiqués entre parenthèses.

Le pictogramme 👁 **Afficher le tunnel** à droite du champ **Tunnel** permet d'ouvrir le tunnel sélectionné en modification. Vous pouvez ainsi consulter les paramètres configurés, voire les modifier.

⚠ Lorsque vous cliquez sur le pictogramme 👁 **Afficher le tunnel**, le tunnel s'ouvre dans le même onglet de votre navigateur. Si vous êtes en train de créer une connexion, ouvrez le tunnel dans un nouvel onglet. Si vous ouvrez le tunnel dans le même onglet et que vous utilisez le bouton retour de votre navigateur, les données saisies seront perdues.

Connexion de remédiation

Compatibilité : v7.5

Cette case à cocher s'affiche dès lors que vous avez sélectionné un tunnel qui prend en charge cette fonctionnalité. Elle sert à définir la connexion que vous êtes en train de configurer comme une connexion de remédiation.

Lorsque le Secure Connection Agent (SCA) détecte une quasi-conformité, une connexion de remédiation sera ouverte si elle a été configurée.

⚠ La case **Connexion de remédiation** ne doit être cochée que pour une seule connexion. Si la case **Connexion de remédiation** est cochée pour plusieurs connexions, il est impossible de savoir quelle connexion sera utilisée.

☞ Reportez-vous au « Guide de l'administrateur » du SCA pour une description détaillée de cette fonctionnalité.

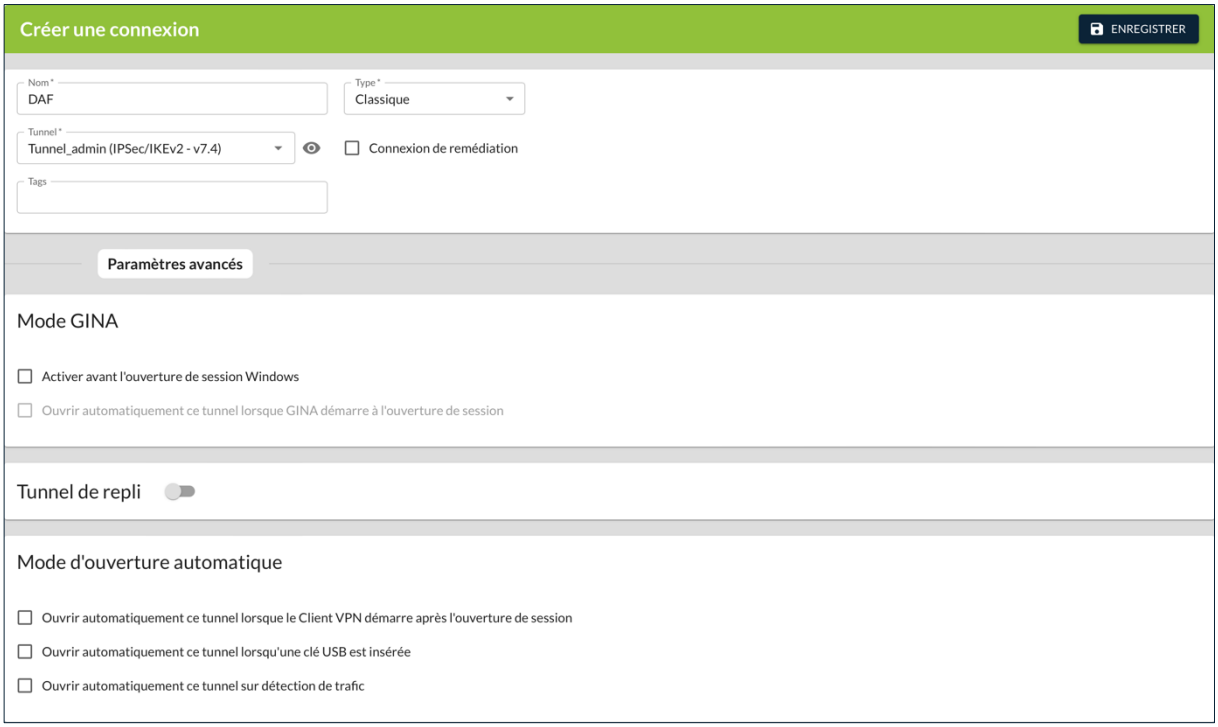
Tags

Tags destinés à faciliter le filtrage des connexions dans la liste des connexions.

Vous pouvez saisir n'importe quel type de caractère. Appuyez ensuite sur Entrée pour former le tag. Saisissez autant de tags que nécessaire.

4.3 Paramètres avancés d'une connexion classique

4.3.1 Présentation



Lorsque le **Type** de la connexion est défini sur **Classique**, la section **Paramètres avancés** de la page **Créer une / Modifier la connexion** comporte les trois blocs suivants décrits dans les sections ci-dessous :

- Mode GINA, voir 4.3.2
- Tunnel de repli, voir 4.3.3
- Mode d'ouverture automatique, voir 4.3.4

4.3.2 Bloc Mode GINA

Compatibilité :

Activer avant l'ouverture de session Windows

Cette option indique que la connexion VPN peut être ouverte avant l'ouverture de session Windows : elle apparaît dans la fenêtre des connexions GINA.

Ouvrir automatiquement ce tunnel lorsque GINA démarre à l'ouverture de session

Quand cette option est cochée, le tunnel s'ouvre automatiquement avant l'ouverture de session Windows. Cette option est active si l'option **Activer avant l'ouverture de session Windows** est sélectionnée.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à la section 9.6 Mode GINA.

4.3.3 Bloc Tunnel de repli

Compatibilité :

Le Client VPN Windows Enterprise implémente une fonction de tunnel de repli (*fallback tunnel* en anglais) qui permet de tenter automatiquement l'ouverture d'un tunnel alternatif lorsque l'ouverture du premier tunnel échoue.

⚠ La fonction **Tunnel de repli** ne doit pas être configurée conjointement avec la fonction **Passerelle redondante**. Il convient de choisir soit l'une ou l'autre, faute de quoi la Client VPN pourrait adopter un comportement non déterminé.

Actionnez le bouton bascule à droite du nom du bloc pour activer le mode **Tunnel de repli** et afficher les champs correspondants.

Repli vers le tunnel

La liste déroulante présente les tunnels vers lequel le logiciel peut basculer automatiquement si le tunnel en cours d'édition est indisponible.

Message à afficher

Comme cette fonction peut passer automatiquement d'un tunnel à un autre, le second étant par exemple moins sécurisé que le premier, il est possible de saisir un message d'avertissement à l'utilisateur, qui lui sera délivré à chaque bascule vers le tunnel de repli.

Nombre d'essais

Le nombre d'essais est enregistré de façon à éviter les boucles de bascules sans fin (un tunnel 1 qui se replie sur un tunnel 2 qui se replie sur un tunnel 1).

Ce champ doit être obligatoirement renseigné. Sa valeur doit être comprise entre 0 et 255.

Autoriser l'utilisateur à refuser ce repli

Permet de configurer la fonction de repli de sorte que ce soit l'utilisateur qui décide de passer d'un tunnel à l'autre.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à la section 9.3 Tunnel de repli.

4.3.4 Bloc Mode d'ouverture automatique

Compatibilité :

Ouvrir automatiquement ce tunnel lorsque le Client VPN démarre après l'ouverture de session

Le tunnel s'ouvre automatiquement au démarrage du Client VPN après l'ouverture de session.

Ouvrir automatiquement ce tunnel lorsqu'une clé USB est insérée

Si le tunnel est configuré avec un certificat contenu sur une carte à puce ou un token, il est ouvert automatiquement sur insertion de cette carte à puce ou token.

Ouvrir automatiquement ce tunnel sur détection de trafic

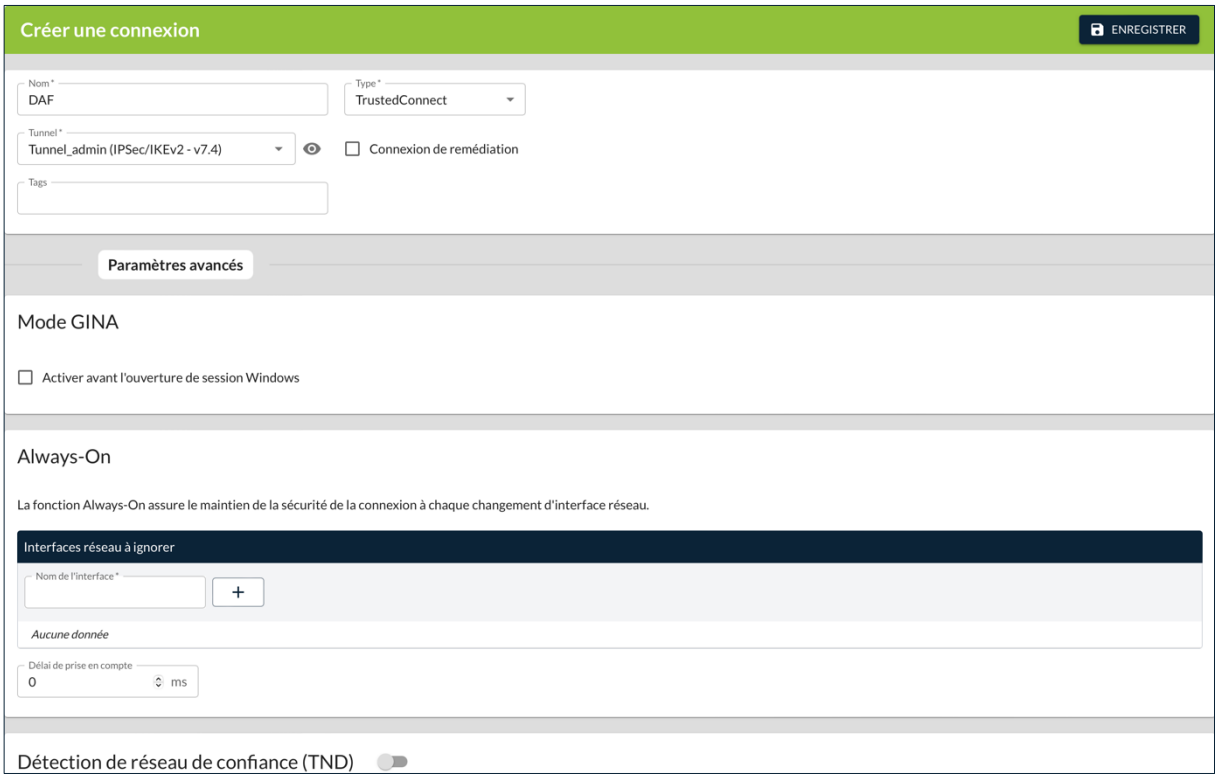
Le tunnel s'ouvre automatiquement sur détection de trafic à destination d'une adresse IP faisant partie du réseau distant.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à la section 9.4 Mode d'ouverture automatique.

4.4 Paramètres avancés d'une connexion TrustedConnect

4.4.1 Présentation

Compatibilité :



Lorsque le **Type** de la connexion est défini sur **TrustedConnect**, la section **Paramètres avancés** de la page **Créer une** / **Modifier la connexion** comporte les quatre blocs suivants décrits dans les sections ci-dessous :

- Mode GINA, voir section 4.4.2
- Always-On, voir section 4.4.3
- Détection de réseau de confiance (TND), voir section 4.4.4
- Détection de portail captif, voir section 4.4.5

⚠ Les connexions de type TrustedConnect sont uniquement compatibles avec le Client VPN Windows Enterprise.

4.4.2 Bloc Mode GINA

Compatibilité :

Activer avant l'ouverture de session Windows

Cette option indique que la connexion VPN peut être ouverte avant l'ouverture de session Windows : elle apparaît dans la fenêtre des connexions GINA.

☞ Pour en savoir davantage sur l'utilisation de cette fonctionnalité, reportez-vous à la section 9.6 Mode GINA.

4.4.3 Bloc Always-On

Compatibilité :

La fonctionnalité **Always-On** est activée dès lors que le **Panneau TrustedConnect** est utilisé pour ouvrir un tunnel VPN. Elle peut être configurée pour exclure certaines interfaces réseau de la reconnexion automatique du tunnel VPN.

⚠ La fonction Always-On associée au mode TrustedConnect du Client VPN Windows Enterprise, ne doit pas être confondue avec la fonction VPN permanent du Client VPN Android. En effet, cette dernière ne peut pas être définie dans une configuration VPN et doit être activée directement sur le terminal mobile.

Interfaces réseau à ignorer

Il est possible d'exclure des interfaces réseaux du monitoring de Always-On. L'exclusion d'une interface se fait sur la base de sa propriété **description** (visible par ipconfig /all).

La valeur de ce paramètre doit contenir une partie ou la totalité du champ **description** de l'interface réseau à exclure. Si la valeur est partielle, alors toute interface dont le champ **description** contient la valeur définie, sera exclue du monitoring.

Les valeurs de ce paramètre ne sont pas sensibles à la casse (toutes les chaînes de caractères sont converties en minuscules avant la comparaison).

Pour ajouter une interface à ignorer, il suffit de saisir la valeur dans le champ **Nom de l'interface**, puis de cliquer sur le bouton +. La valeur est ajoutée à la liste des interfaces à ignorer.

Pour retirer une valeur de la liste des interfaces à ignorer, il suffit de cliquer sur le pictogramme **Supprimer**.

Délai de prise en compte

Le temps de prise en compte d'une nouvelle interface réseau varie suivant les systèmes. S'il est trop long, il peut interférer avec le mécanisme TND, ce qui peut aboutir au fait que le Client VPN essaye d'établir une connexion VPN alors que le poste est connecté au réseau de confiance.

Pour éviter ce problème, ce paramètre permet de retarder le déclenchement du mécanisme TND (voir section suivante).

Il est exprimé en millisecondes. Si la valeur par défaut doit être modifiée, il est recommandé de spécifier une valeur supérieure ou égale à 3000 ms.

Par défaut, la valeur vaut 0 et le mécanisme TND est lancé immédiatement, ce qui convient dans la majorité des cas observés.

4.4.4 Bloc Détection de réseau de confiance (TND)

Compatibilité :

Actionnez le bouton bascule à droite du nom du bloc pour activer le mode **Détection de réseau de confiance (TND)** et afficher les champs correspondants.

Cette fonctionnalité consiste à détecter si le poste est connecté au réseau de l'entreprise (réseau de confiance) ou non. Lorsque le Client VPN détecte que le poste n'est pas sur le réseau de l'entreprise, le tunnel prédéfini est ouvert automatiquement.

☞ Pour en savoir davantage sur ce mode, reportez-vous à la section 8.3 Détection du réseau de confiance (TND).

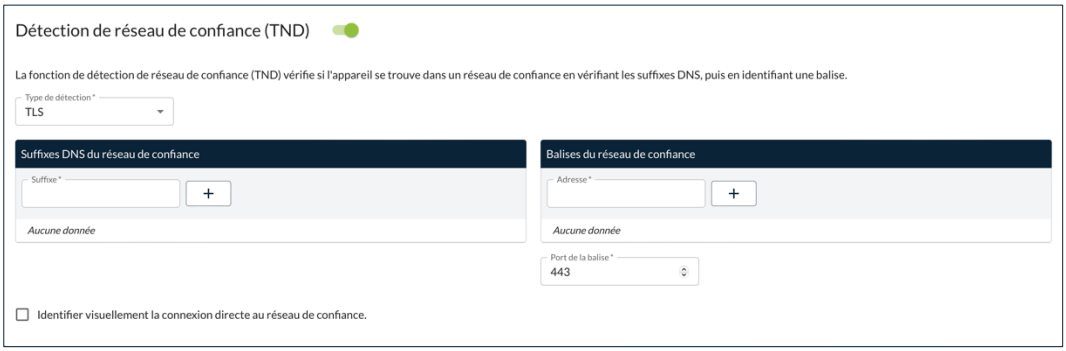
Type de détection

Liste déroulante destinée à la sélection du type de détection :

- TLS
- LDAPS[1]
- LDAP[2]
- AD seul[3]

Les champs à renseigner s'adaptent en fonction du type sélectionné.

Voici les options pour le type de détection **TLS** :



Suffixes DNS du réseau de confiance

Ce paramètre définit la liste des suffixes DNS de confiance. Il peut contenir plusieurs suffixes DNS.

Pour cela, entrez le nom du suffixe à ajouter, puis cliquez sur le bouton **+** à droit du champ de saisie. Répétez l'opération autant de fois que nécessaire.

Balises du réseau de confiance

Ce paramètre définit la liste des adresses IP (ou noms DNS) des serveurs de confiance à utiliser.

Cette liste peut contenir plusieurs adresses IP (ou noms DNS) de serveurs de confiance. Le Client VPN teste alors successivement toutes les adresses IP (ou noms DNS) et tous les certificats associés à chaque serveur, jusqu'à en trouver un accessible et valide.

[1] Uniquement disponible à partir de la version 7.5 du Client VPN Windows Enterprise.
[2] idem
[3] idem

Les adresses IP (ou noms DNS) de la liste doivent être séparées par une virgule, sans espace.

Il n'est pas nécessaire de faire précéder l'adresse IP (ou le nom DNS) du préfixe `https://`.

⚠ Par défaut, le **Panneau TrustedConnect** tente de se connecter à la page `/index.html`. Si celle-ci n'existe pas sur le serveur, celui-ci ne peut pas servir de balise.

Port des balises

Ce paramètre définit le port à utiliser pour joindre les serveurs de confiance.

Il n'est possible de configurer qu'un seul port, qui sera utilisé pour toutes les adresses IP (ou noms DNS).

Si ce paramètre n'est pas configuré, le Client VPN utilise par défaut le port 443.

Voici les options pour le type de détection **LDAPS** :

Noms de domaines

Ce paramètre définit la liste des noms de domaines de confiance. Il peut contenir plusieurs noms de domaines.

Pour cela, entrez le nom du domaine à ajouter, puis cliquez sur le bouton **+** à droit du champ de saisie. Répétez l'opération autant de fois que nécessaire.

Les noms de domaines sont insensibles à la casse.

Port LDAP

Ce paramètre définit le port à utiliser pour joindre le serveur LDAP sécurisé.

Il n'est possible de configurer qu'un seul port, qui sera utilisé pour tous les noms de domaines.

La valeur par défaut est 636.

Voici les options pour le type de détection **LDAP** :

Noms de domaines

Ce paramètre définit la liste des noms de domaines de confiance. Il peut contenir plusieurs noms de domaines.

Pour cela, entrez le nom du domaine à ajouter, puis cliquez sur le bouton **+** à droit du champ de saisie. Répétez l'opération autant de fois que nécessaire.

Les noms de domaines sont insensibles à la casse.

Port LDAP

Ce paramètre définit le port à utiliser pour joindre le serveur LDAP sécurisé.

Il n'est possible de configurer qu'un seul port, qui sera utilisé pour tous les noms de domaines.

La valeur par défaut est 389.

Voici les options pour le type de détection **AD seul** :

Noms de domaines

Ce paramètre définit la liste des noms de domaines de confiance. Il peut contenir plusieurs noms de domaines.

Pour cela, entrez le nom du domaine à ajouter, puis cliquez sur le bouton **+** à droite du champ de saisie. Répétez l'opération autant de fois que nécessaire.

Les noms de domaines sont insensibles à la casse.

Identifier visuellement la connexion directe au réseau de confiance

Cette option ajoute un repère visuel au **Panneau TrustedConnect** pour indiquer que le Client VPN est connecté au réseau de confiance.

Si la case est cochée, l'icône en barre des tâches et la couleur du rond dans le panneau est bleue lorsque la machine est connectée au réseau de confiance et verte lorsqu'un tunnel est ouvert.

Si la case est décochée, l'icône en barre des tâches et le rond dans le panneau reste vert dans les deux cas. Aucune distinction n'est faite entre le réseau de confiance et un tunnel ouvert.

4.4.5 Bloc Détection de portail captif

Actionnez le bouton bascule à droite du nom du bloc pour activer le mode **Détection de portail captif** et afficher les champs correspondants.

Le logiciel TheGreenBow Client VPN Windows Enterprise contient une fonctionnalité avancée appelée Détection de portail captif (ou CPD pour *Captive Portal Detection*) qui détecte automatiquement la présence d'un portail captif pour la connexion à internet.

☞ Reportez-vous au « Guide d'utilisation du Mode filtrant » pour une description détaillée de cette fonctionnalité.

URL

Adresse du serveur web qui sera utilisé pour réaliser la détection.

Port

Port à utiliser pour accéder au serveur web utilisé pour réaliser la détection.

Le port doit être différent de 443. Seul HTTP est possible.

Code d'état HTTP

Code retour différent attendu par le Client VPN Windows Enterprise, pour éviter le cas d'un portail captif qui répondrait avec ce code retour HTTP 204.

Contenu du corps HTML

Contenu attendu dans la réponse du serveur web utilisé pour la détection.

Délai

Temps en secondes accordé à l'utilisateur pour s'identifier sur le portail captif.

Par défaut : 180 s

Minimum : 10 s

Maximum : 600 s

Navigateur personnalisé

Facultatif : chemin vers le navigateur à utiliser pour la détection, si le navigateur par défaut ne doit pas être utilisé.

Arguments du navigateur

Facultatif : arguments à indiquer au navigateur lors de son lancement.

5 Page Créer une / Modifier la configuration

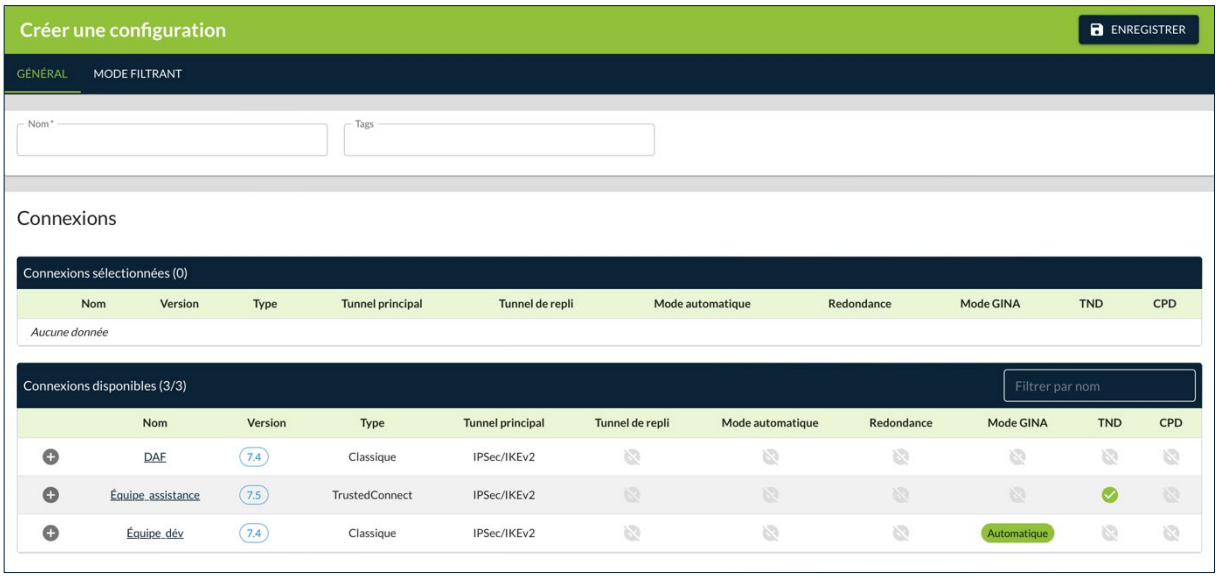
5.1 Introduction

Les blocs et champs figurant sur les pages **Créer une configuration** et **Modifier la configuration** sont identiques. Ils sont donc décrits de façon commune ci-dessous. Ces pages comportent chacune les deux onglets suivants :

- **GÉNÉRAL**, voir 5.2
- **MODE FILTRANT**, voir 5.3

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour comprendre les notions de tunnel, connexion et configuration telles qu'elles sont utilisées chez TheGreenBow.

5.2 Onglet GÉNÉRAL



5.2.1 Bloc d'identification

Compatibilité : , , ,

Le premier bloc de la page n'a pas de titre et sert à identifier la configuration.

Nom

Nom attribué à la configuration.

Longueur max. : 50

Seuls les caractères alphanumériques non accentués et les caractères de soulignement sont autorisés.

Ce champ doit être obligatoirement renseigné.

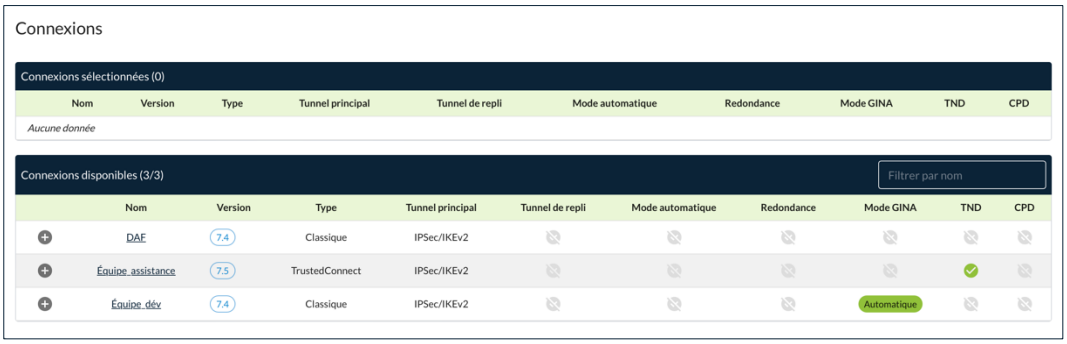
Tags

Tags destinés à faciliter le filtrage des configurations dans la liste des configurations.

Vous pouvez saisir n'importe quel type de caractère. Appuyez ensuite sur Entrée pour former le tag. Saisissez autant de tags que nécessaire.

5.2.2 Bloc Connexions

Compatibilité : Windows, macOS, Android, Linux



Ce bloc est constitué des deux listes suivantes :

- Connexions sélectionnées
- Connexions disponibles

Signification des pictogrammes :

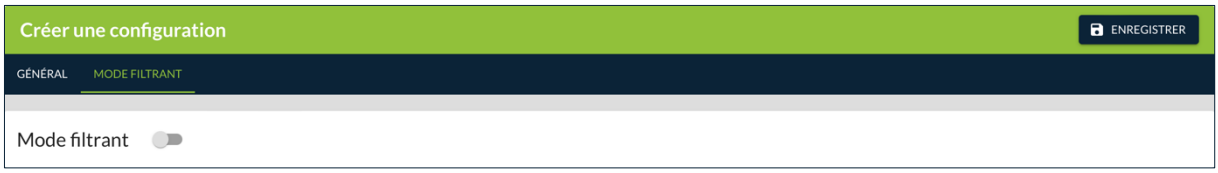
- Ajouter la connexion à la configuration
- La connexion n'est pas compatible avec les connexions sélectionnées
- Griffe de déplacement d'une connexion

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour savoir comment utiliser ces listes.

5.3 Onglet MODE FILTRANT

5.3.1 Présentation

Compatibilité :



Le **Mode filtrant** du Client VPN Windows Enterprise est une fonction de filtrage des flux entrants et sortants du poste. Il est activé dès lors que le Client VPN Windows Enterprise ne se trouve pas sur le réseau de confiance. Par conséquent, il est uniquement disponible avec le **Panneau TrustedConnect**.

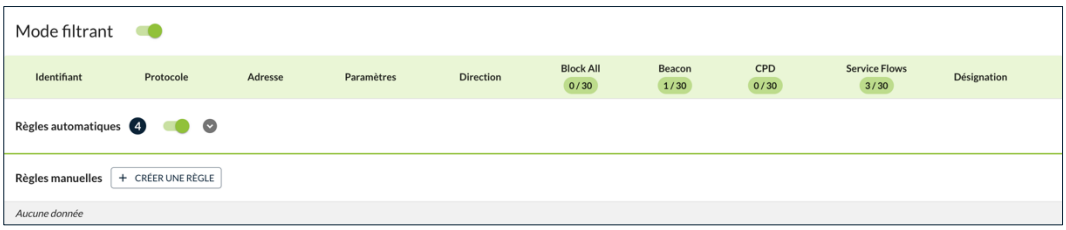
La configuration du **Mode filtrant** est uniquement disponible lorsqu'au moins une connexion **TrustedConnect** est sélectionnée. Ce mode n'est pas disponible pour les connexions classiques.

☞ Reportez-vous au « Guide d'utilisation du Mode filtrant » pour une description détaillée de cette fonctionnalité.

5.3.2 Bloc Mode filtrant

Compatibilité :

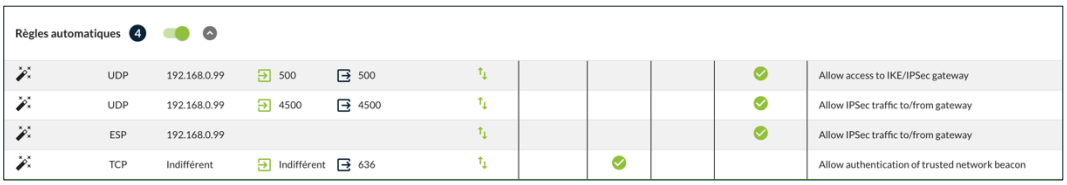
Actionnez le bouton bascule à droite du nom du bloc **Mode filtrant** pour activer le mode et afficher les champs correspondants.



Section Règles automatiques

Certaines règles sont créées automatiquement sur la base des informations de la ou des connexions TrustedConnect sélectionnées. Elles sont activées par défaut, Vous pouvez les désactiver en actionnant le bouton bascule) droite du titre de la section.

Pour afficher les règles et leurs paramètres, cliquez sur le pictogramme **Afficher**.



Aucune autre action n'est possible sur ces règles automatiques.

Section Règles manuelles

Pour ajouter une règle, cliquez sur le bouton **+ CRÉER UNE RÈGLE**, puis renseignez les informations dans la boîte de dialogue qui s'affiche en fonction de vos besoins.

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour une description détaillée de la procédure.

5.3.3 Boîte de dialogue Créer une règle

Cette boîte de dialogue s'affiche après avoir cliqué sur le bouton **+ CRÉER UNE RÈGLE** dans la section **Règles manuelles** du bloc **Mode filtrant** dans l'onglet **MODE FILTRANT**.

Désignation

Désignation attribuée à la règle manuelle constituée d'une chaîne de caractères libre, sans espace, à l'exclusion de `DYN_RULES` qui est réservé à TheGreenBow.

Autoriser dans le contexte

Sélection des contextes dans lesquels la règle est autorisée :

- Block All
- Beacon
- CPD
- Service Flows

☞ Reportez-vous au « Guide d'utilisation du Mode filtrant » pour une description détaillée de ces contextes.

Direction

Direction dans laquelle s'applique la règle du point de vue du poste de travail :

- Descendant
- Ascendant
- Les deux

Adresse

Adresse à laquelle s'applique la règle. Il peut s'agir d'un nom de domaine pleinement qualifié (FQDN), une adresse IP ou * pour toute adresse.

Protocole

Protocole auquel s'applique la règle. L'une des valeurs suivantes est à sélectionner dans la liste déroulante :

- ICMP
- TCP
- UDP
- ESP
- ALL pour tout protocole

Si le protocole **ICMP** est sélectionné, les champs **Code** et **Type** s'affichent et doivent être renseignés.

Si le protocole **TCP**, **UDP** ou **ALL** est sélectionné, les champs **Port source** et le **Port de destination** s'affichent et doivent être renseignés.

☞ Reportez-vous au « Guide d'utilisation du Mode filtrant » pour une description détaillée des valeurs à renseigner dans ces champs.

6 Gestion des certificats

6.1 Introduction

Les Clients VPN TheGreenBow offrent un ensemble de fonctions permettant l'exploitation de certificats de toute nature, issus de PKI / IGC de tout type et stockés sur des supports de toute nature : carte à puce, token, magasin de certificats, fichier de configuration.

Les Clients VPN TheGreenBow implémentent en particulier les facilités suivantes :

- sélection automatique du support à utiliser parmi plusieurs ;
- accès aux cartes à puce et aux tokens en PKCS #11 et CNG[1] ;
- sélection multicritère des certificats à utiliser en fonction du sujet et du key usage ;
- gestion des certificats côté utilisateur (côté client VPN), comme des certificats de la passerelle VPN, incluant la gestion des dates de validité, des chaînes de certification, des certificats racines, intermédiaires et des CRL ;
- gestion des autorités de certification (Certificate Authority : CA) ;
- possibilité de préconfigurer tous les paramètres PKI / IGC pour une prise en compte automatique lors de l'installation.

Les Clients VPN TheGreenBow apportent des fonctions de sécurité supplémentaires sur la gestion des PKI / IGC comme l'ouverture et la fermeture automatique du tunnel sur insertion et extraction de carte à puce et de token, ou encore la possibilité de configurer l'interface PKI / IGC dans l'installeur du logiciel de façon à automatiser le déploiement.

La liste des cartes à puce et des tokens compatibles avec les Clients VPN TheGreenBow est disponible sur le site TheGreenBow à l'adresse : https://thegreenbow.com/fr/support/guides-dintegration/tokens-vpn-compatibles/.

La configuration et la caractérisation des certificats peut être effectuée dans :

1. l'onglet **AUTHENTIFICATION DU CLIENT** du tunnel concerné (IPsec/IKEv2 ou OpenVPN) ;
2. l'onglet **AUTHENTIFICATION DE LA PASSERELLE** du tunnel concerné (IPsec/IKEv2 ou OpenVPN) ;
3. un fichier de configuration des lecteurs de cartes à puce et tokens appelé `vpnconf.ini` (cf. « Guide de déploiement » du Client VPN Windows Enterprise).

[1] Client VPN Windows Enterprise uniquement.

Les types de certificat suivants sont pris en charge :

- RSASSA-PKCS1-v1.5 avec SHA-2 (uniquement si le paramètre dynamique correspondant est configuré, cf. section 13.2.5 Méthodes d'authentification des certificats)
- RSASSA-PSS avec SHA-2 (uniquement si le paramètre dynamique correspondant est configuré, cf. section 13.2.5 Méthodes d'authentification des certificats)
- ECDSA « secp256r1 » avec SHA-2 (256 bits)
- ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits)

☞ Pour en savoir davantage sur les méthodes d'authentification et la cryptographie utilisées dans les Clients VPN TheGreenBow, consultez la section 13.2 Notions élémentaires de cryptographie dans l'annexe.

6.2 Certificat utilisateur

6.2.1 Généralités

Le certificat utilisateur est envoyé par le Client VPN à la passerelle pour qu'elle puisse authentifier l'utilisateur.

Il doit se conformer aux contraintes suivantes (recommandations de sécurité de l'ANSSI) :

- L'extension Key Usage doit être présente, marquée comme critique, et contenir uniquement la valeur `digitalSignature`.
- L'extension Extended Key Usage doit être présente, marquée comme non-critique, et uniquement contenir la valeur `id-kp-clientAuth`.

Si ces contraintes ne sont pas respectées, le Client VPN affichera un avertissement dans la **Console** mais n'empêchera pas la communication avec la passerelle. Celle-ci devrait néanmoins refuser l'authentification du Client VPN.

6.2.2 Options spécifiques

Compatibilité : Windows v7.4 & v7.5

Deux options peuvent être définies dans le CMC pour les Clients VPN Windows Enterprise de version 7.4 et supérieure. Elles sont définies au niveau de la charge utile d'authentification IKE_AUTH et s'appliquent à un tunnel donné.

L'onglet **AUTHENTIFICATION DU CLIENT** du tunnel IPsec/IKEv2 ou OpenVPN présente le bloc **Préciser l'objet du certificat** avec les options **Par objet du certificat** et **Par modèle de nom distinctif (DN Pattern)**.

☞ Pour une description détaillée de ce bloc, voir la section 2.3.3.2 pour un tunnel IPsec/IKEv2 ou la section 3.3.3 pour un tunnel OpenVPN.

Dans le Client VPN Windows Enterprise, ces options sont définies sous forme de paramètres dynamiques (`user_cert_dnpattern` et `user_cert_keyusage`). Avant cela, la configuration s'effectuait au moyen de propriétés MSI définies au moment de l'installation du Client VPN. alors Les propriétés MSI s'appliquent à l'ensemble des tunnels, alors que les paramètres dynamiques du Client VPN s'appliquent à un tunnel donné, comme les options du CMC.

6.2.2.1 Option Par objet du certificat

Cette option correspond aux paramètres dynamiques `user_cert_keyusage` et `allow_server_and_client_auth`. Elle permet de sélectionner un certificat en fonction de son champ « key usage » :

Case non cochée

Pas de sélection du certificat par le champ « key usage ».

Signature numérique

Sélection du certificat par le champ « key usage » dont la valeur de l'attribut `digitalSignature=1`.

Signature numérique et chiffrement de la clé

Sélection du certificat par le champ « key usage » dont la valeur des attributs `digitalSignature=1` et `keyEncipherment=1`.

Signature numérique et authentification du client

Signature numérique et authentification du client : sélection du certificat par les champ « key usage » et « extended key usage » dont la valeur des attributs respectifs `digitalSignature=1` et `id-kp-clientAuth=1`.

6.2.2.2 Option Par modèle de nom distinctif (DN Pattern)

Cette option correspond au paramètre dynamique `user_cert_dnpattern` et permet de caractériser le certificat à utiliser. Lorsqu'il est défini, le Client VPN Windows Enterprise recherche, sur token, carte à puce et dans le magasin de certificats Windows, le certificat dont le sujet contient la chaîne de caractères spécifiée dans le champ **Modèle**.

Quand cette option n'est pas activée, le Client VPN recherche le premier certificat conforme aux autres caractéristiques configurées.

6.2.3 Stockage des certificats

Le CMC permet d'affecter un certificat utilisateur à un tunnel VPN. Il ne peut y avoir qu'un seul certificat par tunnel, mais chaque tunnel peut avoir son propre certificat.

Le CMC propose plusieurs options pour sélectionner le certificat utilisateur depuis différentes sources.

L'onglet **AUTHENTIFICATION DU CLIENT** du tunnel IPsec/IKEv2 ou OpenVPN présente le bloc **Type de stockage** avec les options suivantes :

- Token / carte à puce
- Magasin de certificats de l'OS
- Token / carte à puce et Magasin de certificats de l'OS[1]
- Magasin de certificats du Client VPN

[1] Uniquement disponible pour le Client VPN Windows Enterprise v7.4 ou v7.5.

☞ Pour une description détaillée de ce bloc, voir la section 2.3.3.1 pour un tunnel IPsec/IKEv2 ou la section 3.3.2 pour un tunnel OpenVPN.

Dans les trois premiers cas, la sélection du certificat s'effectue de manière automatique. L'option **Magasin de certificats du Client VPN** permet d'importer le certificat dans la configuration VPN.

Si vous choisissez l'option **Token / carte à puce et Magasin de certificats de l'OS**, le logiciel va d'abord chercher le certificat utilisateur sur un token / une carte à puce. S'il n'en trouve pas, il va poursuivre la recherche dans le magasin de certificats de l'OS.

Pour les options **Token / carte à puce** et **Token / carte à puce et Magasin de certificats de l'OS**, si vous utilisez plusieurs lecteurs de tokens / cartes à puce vous devez configurer le paramètre dynamique `reader_pattern` pour spécifier le lecteur à partir duquel le certificat doit être sélectionné (voir section 7.2.6 reader_pattern). Comme valeur du paramètre, indiquez le nom du lecteur (p. ex. `NEOWAVE`) ou `Virtual` s'il s'agit d'un module de plateforme sécurisée (TPM ou *Trusted Platform Module*).

Depuis la version 7.5 du Client VPN Windows Enterprise, en présence de plusieurs cartes à puce du même fabricant utilisant des lecteurs identiques, le paramètre dynamique `user_smartcard_tip` peut être défini au niveau IKE Auth à une valeur au choix, qui sera affichée lors de la demande du mot de passe pour identifier de manière univoque chaque carte à puce (voir section 7.2.17 user_smartcard_tip).

Si vous avez précédemment importé un certificat dans la configuration et que vous décidez de choisir la sélection automatique, aucun avertissement ne s'affiche pour vous indiquer que le certificat sera supprimé de la configuration lorsque vous la sauvegarderez.

6.2.4 Importation de certificats dans la configuration VPN

Le CMC permet d'importer dans la configuration VPN des certificats utilisateurs au format PEM/PFX ou PKCS #12. L'intérêt de cette solution, moins sécurisée que l'utilisation du magasin de certificats de l'OS, d'une carte à puce ou d'un token, est de faciliter le transport des certificats.

Cette solution présente l'avantage de regrouper le certificat (propre à un utilisateur) et la configuration VPN (a priori générique) dans un fichier unique, facile à transmettre vers le poste utilisateur et à importer dans le Client VPN.

Néanmoins, l'inconvénient de transporter les certificats dans une configuration VPN est que chaque configuration devient alors propre à

chaque utilisateur. Cette solution, n'est donc pas préconisée pour un déploiement conséquent.

L'importation des certificats utilisateurs s'effectue au niveau du bloc **Certificat PKCS #12** de l'onglet **AUTHENTIFICATION DU CLIENT**.

☞ Pour une description détaillée de ce bloc, voir la section 2.3.3.3 pour un tunnel IPsec/IKEv2 ou la section 3.3.4 pour un tunnel OpenVPN.

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour une description détaillée de la procédure d'importation.

⚠ Dès lors qu'un certificat est importé dans une configuration VPN, il est fortement recommandé lors de l'exportation du fichier de configuration, de le protéger par un mot de passe, pour éviter que le certificat ne soit visible en clair. Actuellement, le CMC ne permet pas de le faire. Pour cela, il faut exporter la configuration VPN, l'importer dans un Client VPN TheGreenBow et l'exporter avec un protection par mot de passe.

6.2.5 Utilisation de certificats sur carte à puce ou sur token

Lorsqu'un tunnel VPN est configuré pour exploiter un certificat stocké sur carte à puce ou sur token, le code PIN d'accès à cette carte à puce ou token est demandé à l'utilisateur à chaque ouverture du tunnel.

Si la carte à puce n'est pas insérée, ou si le token n'est pas accessible, le tunnel ne s'ouvre pas.

Si le certificat trouvé ne remplit pas les conditions configurées, le tunnel ne s'ouvre pas.

Si le code PIN présenté est erroné, le Client VPN avertit l'utilisateur, qui a habituellement trois essais consécutifs avant blocage de la carte à puce ou du token.

Le Client VPN Windows Enterprise implémente un mécanisme de détection automatique de l'insertion d'une carte à puce. Ainsi, les tunnels associés au certificat contenu sur la carte à puce sont montés automatiquement à l'insertion de cette carte à puce. Réciproquement, l'extraction de la carte à puce ferme automatiquement tous les tunnels associés.

☞ Pour savoir comment mettre en œuvre cette fonction, voir la section 4.3.4 Bloc Mode d'ouverture automatique.

Depuis la version x.4 des Clients VPN TheGreenBow, une option permet de sélectionner automatiquement le certificat depuis un token /une carte à puce, le magasin de certificats Windows ou les deux (voir la section 6.2.3 Stockage des certificats).

Depuis la version x.5 des Clients VPN TheGreenBow, en présence de plusieurs cartes à puce identiques utilisant des lecteurs identiques, le paramètre dynamique `user_smartcard_tip` peut être défini à une valeur au choix permettant d'identifier de manière univoque chaque carte à puce (voir section 7.2.17 user_smartcard_tip).

6.2.6 Utilisation de certificats du magasin de certificats de l'OS

6.2.6.1 Caractéristiques requises

En vue d'offrir une granularité plus fine dans la configuration du choix de magasin de certificats à utiliser, depuis la version x.5 des Clients VPN TheGreenBow, ce choix n'est plus opéré au niveau du poste, mais à celui du tunnel.

Pour qu'un certificat du magasin de certificats Windows soit identifié par le Client VPN Windows Enterprise, il doit respecter les caractéristiques suivantes :

- Le certificat doit être certifié par une autorité de certification (ce qui exclut les certificats auto-signés).
- Par défaut, le certificat doit être situé dans le magasin de certificats « Personnel » (il représente l'identité personnelle de l'utilisateur qui veut ouvrir un tunnel VPN vers son réseau d'entreprise). Pour utiliser le magasin de certificats machine de Windows, il convient d'ajouter le paramètre dynamique `MachineStore` défini à la valeur `true` (voir section 7.2.7 MachineStore).

Pour gérer les certificats dans le magasin de certificats Windows, Microsoft propose en standard l'outil de gestion `certmgr.msc`. Pour exécuter cet outil, aller dans le menu **Démarrer** de Windows, puis dans le champ **Rechercher les programmes et fichiers**, entrer `certmgr.msc`.

6.2.6.2 Importation de certificats en fonction du type de magasin

Lors de l'importation de certificats dans le magasin de certificats Windows , il convient de spécifier le type de magasin utilisé (utilisateur ou machine) dans la

ligne de commande. Ci-dessous, vous trouverez des exemples de ligne de commande avec les options à préciser.

- Magasin utilisateur :

```
certutil -csp KSP -user -importpfx CertFileName.p12
```

- Magasin machine :

```
certutil -csp KSP -importpfx CertFileName.p12
```

Dans les lignes de commande, l'option `-user` de la commande `certutil` sert à spécifier le magasin utilisateur. Lorsqu'elle est omise, le magasin machine est utilisé par défaut.

Depuis la version x.4 des Clients VPN TheGreenBow, une option permet de sélectionner automatiquement le certificat depuis un token /une carte à puce, le magasin de certificats Windows ou les deux (voir la section 6.2.3 Stockage des certificats).

6.3 Certificat de la passerelle VPN

6.3.1 Généralités

Il est recommandé de forcer les Clients VPN TheGreenBow à vérifier la chaîne de certification du certificat reçu de la passerelle VPN (comportement par défaut).

☞ Voir section 2.5.3 Bloc Options.

Cela nécessite d'importer le certificat racine et tous les certificats de la chaîne de certification (l'autorité de certification racine et les autorités de certification intermédiaires) dans le fichier de configuration.

Tant que l'option **Ne pas vérifier le certificat passerelle par rapport à la CRL** reste décochée, le Client VPN utilisera aussi la liste des certificats révoqués (CRL ou *Certificate Revocation List* en anglais) des différentes autorités de certification.

Si ces CRL sont absentes du magasin de certificats, ou si ces CRL ne sont pas téléchargeables à l'ouverture du tunnel VPN, le Client VPN ne sera pas en mesure de valider le certificat de la passerelle.

La vérification de chaque élément de la chaîne implique :

- la vérification de la date d'expiration du certificat,
- la vérification de la date de début de validité du certificat,
- la vérification des signatures de tous les certificats de la chaîne de certificats (y compris le certificat racine, certificats intermédiaires et le certificat du serveur),
- la vérification des CRL de tous les émetteurs de certificats de la chaine de confiance.

Depuis la version 7.5 du Client VPN Windows Enterprise, il est possible de vérifier la révocation du certificat de la passerelle à l'aide du protocole de vérification de certificat en ligne en mode agrafage (OCSP ou *Online Certificate Status Protocol* en anglais). Pour cela, il convient d'ajouter le paramètre dynamique `enable_OCSP` défini à la valeur `true` (voir section **Error! Reference source not found. Error! Reference source not found.**).

6.3.2 Contraintes relatives à l'extension Key Usage

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Key Usage. Elle doit :

- être présente,
- être marquée comme critique et
- contenir uniquement les valeurs `digitalSignature` et/ou `nonRepudation`.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le paramètre dynamique `allow_server_extra_keyusage` défini à la valeur `true` (voir section 7.2.11 allow_server_extra_keyusage).

6.3.3 Contraintes relatives à l'extension Extended Key Usage

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Extended Key Usage. Cette dernière peut être absente ou présente. Si elle est présente, elle doit :

- être marquée comme non-critique et
- uniquement contenir les valeurs suivantes :
  - `id-kp-serverAuth` ou
  - `id-kp-serverAuth` + `id-kp-ipsecIKE`.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le

paramètre dynamique `allow_server_and_client_auth` défini à la valeur `true` (voir section 7.2.12 allow_server_and_client_auth).

6.4 Restriction du téléchargement des CRL

6.4.1 Introduction

Une liste de révocation de certificats (*Certificate Revocation List* ou CRL) contient l'ensemble des certificats qui ne sont plus valables (date de validité expirée, perte ou compromission de la clé privée associée au certificat, changement d'un champ relatif au titulaire, etc.) et qui ne sont donc plus dignes de confiance.

Les CRL sont définies dans les normes RFC 5280 et RFC 6818.

Les CRL sont publiées par les autorités de certification (CA) et les infrastructures de gestion de clés (IGC ou *Public Key Infrastructure* – PKI).

Dans certains cas, ces listes peuvent être relativement volumineuses (plusieurs Mo). Leur téléchargement peut donc prendre du temps et par conséquent ralentir le temps d'ouverture d'un tunnel lorsqu'un grand nombre d'utilisateurs contacte le serveur HTTP en même temps.

Le CMC met à disposition deux paramètres dynamiques décrits ci-dessous pour accélérer le temps d'ouverture d'un tunnel. Ces paramètres fonctionnent de manière indépendante et peuvent être associés.

Le premier paramètre dynamique, nommé `check_user_crl`, empêche le téléchargement de la CRL de validation du certificat utilisateur. Le second, nommé `crl_cache_duration`, limite le téléchargement de la CRL de validation du certificat passerelle.

6.4.2 Blocage du téléchargement de la CRL de validation du certificat utilisateur

Par défaut, lorsque le Client VPN vérifie le certificat utilisateur (p. ex. parce qu'il dépend d'une CA connue), il vérifie également la CRL pour savoir si ce certificat est toujours valide. Si le certificat n'est pas valide, un simple avertissement est consigné dans la **Console**. En fin de compte, c'est la passerelle qui va décider si le certificat utilisateur peut être accepté ou non.

Afin d'empêcher le téléchargement de la CRL et donc accélérer le temps d'ouverture d'un tunnel, vous pouvez ajouter le paramètre dynamique `check_user_crl` défini à la valeur `false` (voir section 7.2.9 check_user_crl). Dans ce cas, la vérification de la CRL n'est pas effectuée pour le certificat utilisateur. C'est la passerelle qui se charge d'effectuer cette vérification.

6.4.3 Limitation du téléchargement de la CRL de validation du certificat passerelle

Si vous souhaitez limiter le nombre de fois qu'une CRL est téléchargée pour la validation du certificat de la passerelle sans pour autant empêcher son téléchargement – toujours en vue d'accélérer le temps d'ouverture d'un tunnel –, vous pouvez ajouter le paramètre dynamique `crl_cache_duration` défini à une valeur correspondant au nombre d'heures pendant lequel la CRL est mise en cache (voir section 7.2.10 crl_cache_duration).

6.5 Autorités de certification

6.5.1 Généralités

Lorsqu'un Client VPN TheGreenBow est configuré pour vérifier les certificats passerelle, les autorités de certification (CA) doivent être également accessibles.

La CA racine de la passerelle doit obligatoirement être importée dans la configuration.

Si la passerelle n'est pas configurée pour envoyer les CA, alors il est également nécessaire d'importer les CA intermédiaires dans la configuration.

Depuis la version x.3 des Clients VPN TheGreenBow, il est possible de créer des configurations avec plus de trois autorités de certification (CA).

Les types de CA intermédiaires prises en charge sont :

- RSASSA-PKCS1-v1.5 avec SHA-2
- RSASSA-PSS avec SHA-2
- ECDSA « secp256r1 » avec SHA-2
- ECDSA « BrainpoolP256r1 » avec SHA-2

Les types de CA racine prises en charge sont :

- RSASSA-PKCS1-v1.5 avec SHA-2
- RSASSA-PSS avec SHA-2
- ECDSA « secp256r1 » avec SHA-2
- ECDSA « BrainpoolP256r1 » avec SHA-2

Pour des raisons de sécurité, l'utilisation du magasin de certificats de l'OS pour accéder aux CA n'est pas autorisé.

6.5.2 Importation d'une autorité de certification

L'importation des certificats de CA s'effectue au niveau du bloc **CA de confiance** de l'onglet **AUTHENTIFICATION DE LA PASSERELLE**.

☞ Pour une description détaillée de ce bloc, voir la section 2.5.2 pour un tunnel IPsec/IKEv2 ou la section 3.4.2 pour un tunnel OpenVPN.

☞ Reportez-vous au « Guide de l'administrateur » du CMC pour une description détaillée de la procédure d'importation.

6.5.3 Mode IPsec DR

Pour pouvoir utiliser les Clients VPN TheGreenBow en mode IPsec DR, l'une des exigences du référentiel IPsec DR de l'ANSSI est que la valeur `Certification Auhtority` dans la charge utile de demande de certificat (CERTREQ payload) est une liste concaténée de condensats SHA-2 des clés publiques des autorités de certification de confiance.

Depuis la version x.5 des Clients VPN TheGreenBow, le Client VPN détecte automatiquement le format (SHA-1 ou SHA-2) en fonction de la longueur de la charge utile de demande de certificat [CERTREQ] qu'il reçoit de la passerelle. Cette sélection automatique est uniquement effectuée si le paramètre dynamique `sha2_in_cert_req` n'est pas présent.

Si vous souhaitez sélectionner le format manuellement, vous pouvez ajouter le paramètre dynamique `sha2_in_cert_req` défini à la valeur `true` pour SHA-2 ou à la valeur `false` pour SHA-1 (voir section 7.2.13 sha2_in_cert_req).

ℹ Si la longueur ne permet pas de déterminer le format, SHA-1 est privilégié. Face à une passerelle configurée en mode IPsec DR, il convient donc d'utiliser le paramètre dynamique `sha2_in_cert_req` pour exclure toute ambiguïté.

☞ Pour savoir comment configurer le Client VPN Windows Enterprise en vue de l'utiliser avec une passerelle configurée en mode IPsec DR, consultez le guide de configuration « Client VPN et IPsec DR » disponible sur le site TheGreenBow.

7 Gestion des paramètres dynamiques

7.1 Généralités

Le CMC permet si besoin de configurer des paramètres dynamiques additionnels sur l'onglet **AVANCÉ** d'un tunnel IPsec/IKEv2 ou OpenVPN.

Le tableau suivant énumère les paramètres dynamiques documentés dans le présent guide et précise leur utilisation ainsi que leur étendue :

Paramètre	Utilisation	Étendue
`local_subnet`	Spécifier l'adresse IP de l'interface réseau (voir 7.2.1)	IKE Auth
`nonce_size`	Spécifier la taille du nonce pour les passerelles IPsec DR (voir 7.2.2)	IKE Auth
`local_virtual_network_size`	Spécifier la taille du réseau local virtuel (voir 7.2.3)	Child SA
`user_cert_dnpattern`	Sélectionner un certificat en fonction de son sujet (voir 7.2.4)	IKE Auth et TLS
`user_cert_keyusage`	Sélectionner un certificat en fonction de son champ « key usage » (voir 7.2.5)	IKE Auth et TLS
`reader_pattern`	Sélectionner le lecteur de tokens / cartes à puce à utiliser pour la sélection automatique du certificat utilisateur (voir 7.2.6)	IKE Auth et TLS
`MachineStore`	Définir le magasin de certificats à utiliser au niveau tunnel (voir 7.2.7)	IKE Auth et TLS
`enable_OCSP`	Activer le protocole de vérification de certificat en ligne (OCSP ou *Online Certificate Status Protocol* en anglais, voir 7.2.8)	IKE Auth et TLS
`check_user_crl`	Empêcher le chargement de la CRL pour le certificat utilisateur (voir 7.2.9)	IKE Auth et TLS
`crl_cache_duration`	Limiter le chargement de la CRL pour le certificat de la passerelle (voir7.2.10)	IKE Auth et TLS
`allow_server_extra_keyusage`	Valider le certificat même s'il ne se conforme pas aux contraintes relatives à l'extension Key Usage (voir 7.2.11)	IKE Auth et TLS
`allow_server_and_client_auth`	Valider le certificat même s'il ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage (voir 7.2.12)	IKE Auth et TLS
`sha2_in_cert_req`	Utiliser l'algorithme de hachage SHA-2 dans la charge utile de demande de certificat (voir 7.2.13)	IKE Auth et TLS
`Method14_RSASSA_PKCS1`	Employer d'autres méthodes d'authentification des certificats (voir 7.2.14)	IKE Auth

Paramètre	Utilisation	Étendue
`Method1_PKCS1v15_Scheme`	Employer d'autres méthodes d'authentification des certificats (voir 7.2.15)	IKE Auth
`use_method_214`	Employer la méthode 214 ou la méthode 14 pour l'authentification des certificats utilisateurs Brainpool (voir 7.2.16)	IKE Auth
`user_smartcard_tip`	Afficher un message personnalisé dans la fenêtre popup de demande du code PIN (voir 7.2.17)	IKE Auth et TLS

Dans certaines circonstances, le support TheGreenBow peut vous proposer d'ajouter d'autres paramètres dynamiques (Nom, Valeur), non documentés dans le présent guide, qui permettront de gérer des cas d'usage particuliers, soit sur la version du logiciel installée, soit sur des patches qui vous seront fournis.

7.2 Utilisation des paramètres

7.2.1 local_subnet

Compatibilité :

Lorsque l'interface réseau possède plusieurs adresses IP, vous pouvez spécifier l'adresse à l'aide du paramètre dynamique `local_subnet`.

Seules les adresses IPv4 sont prises en charge. Le format de l'adresse à renseigner comme valeur du paramètre dynamique est le suivant : `aaa.bbb.ccc.ddd/xx`.

Si le masque de sous-réseau est omis en ne renseignant que `aaa.bbb.ccc.ddd`, l'adresse correspondra à `aaa.bbb.ccc.ddd/32`.

7.2.2 nonce_size

Compatibilité : , , ,

Si vous utilisez une passerelle IPsec DR, il convient d'ajouter le paramètre dynamique `nonce_size` et de le définir à la valeur 16. En effet, ces passerelles ne prennent pas en charge de nonce avec une taille différente.

7.2.3 local_virtual_network_size

Compatibilité : Windows

La taille par défaut du réseau local virtuel est 24. Pour utiliser un réseau local d'une autre taille (p. ex. 32), il convient d'ajouter le paramètre dynamique `local_virtual_network_size` défini à la valeur souhaitée (valeurs possibles : 1 à 32).

7.2.4 user_cert_dnpattern

Compatibilité : Windows

Le paramètre dynamique `user_cert_dnpattern` permet de caractériser le certificat à utiliser. Lorsqu'il est défini, le Client VPN Windows Enterprise recherche, sur token, carte à puce et dans le magasin de certificats Windows, le certificat dont le sujet contient `[texte]`.

Quand ce paramètre dynamique n'est pas défini, le Client VPN recherche le premier certificat conforme aux autres caractéristiques configurées.

Le CMC propose l'option **Par modèle de nom distinctif (DN Pattern)** en lieu et place de ce paramètre dynamique. Il convient donc de privilégier cette option plutôt que d'utiliser le paramètre dynamique.

☞ Pour une description détaillée de cette option, voir la section 6.2.2.2 Option Par modèle de nom distinctif (DN Pattern).

7.2.5 user_cert_keyusage

Compatibilité : Windows

Le paramètre dynamique `user_cert_keyusage` permet de sélectionner un certificat en fonction de son champ « key usage » :

0 ou non défini	Pas de sélection du certificat par le champ « key usage ».
1	Sélection du certificat par le champ « key usage » dont la valeur de l'attribut `digitalSignature=1`.
2	Sélection du certificat par le champ « key usage » dont la valeur des attributs `digitalSignature=1` et `keyEncipherment=1`.

Le CMC propose l'option **Par objet du certificat** en lieu et place de ce paramètre dynamique. Il convient donc de privilégier cette option plutôt que d'utiliser le paramètre dynamique.

☞ Pour une description détaillée de cette option, voir la section 6.2.2.1 Option Par objet du certificat.

7.2.6 reader_pattern

Compatibilité : ,

Pour les options **Token / carte à puce** et **Token / carte à puce et Magasin de certificats de l'OS** du bloc **Type de stockage**, si vous utilisez plusieurs lecteurs de tokens / cartes à puce vous devez configurer le paramètre dynamique `reader_pattern` pour spécifier le lecteur à partir duquel le certificat doit être sélectionné. Comme valeur du paramètre, indiquez le nom du lecteur (p. ex. `NEOWAVE`) ou `Virtual` s'il s'agit d'un module de plateforme sécurisée (TPM ou *Trusted Platform Module*).

☞ Pour une description détaillée de ces options, voir la section 6.2.3 Stockage des certificats.

7.2.7 MachineStore

Compatibilité :

Par défaut, le certificat utilisateur doit être situé dans le magasin de certificats « Personnel » (il représente l'identité personnelle de l'utilisateur qui veut ouvrir un tunnel VPN vers son réseau d'entreprise). Pour utiliser le magasin de certificats machine de Windows, il convient d'ajouter le paramètre dynamique `MachineStore` défini à la valeur `true`.

☞ Pour en savoir davantage sur l'utilisation de ce type de certificat, voir la section 6.2.6 Utilisation de certificats du magasin de certificats de l'OS.

7.2.8 enable_OCSP

Compatibilité : ,

Depuis la version x.5 des Clients VPN TheGreenBow, il est possible de vérifier la révocation du certificat de la passerelle à l'aide du protocole de vérification

de certificat en ligne en mode agrafage (OCSP ou *Online Certificate Status Protocol* en anglais). Pour cela, il convient d'ajouter le paramètre dynamique `enable_OCSP` défini à la valeur `true`.

☞ Pour en savoir davantage sur l'utilisation de ce type de certificat, voir la section 6.3 Certificat de la passerelle VPN.

7.2.9 check_user_crl

Compatibilité : Windows

Pour empêcher le téléchargement de la CRL et donc accélérer le temps d'ouverture d'un tunnel, vous pouvez ajouter le paramètre dynamique `check_user_crl` défini à la valeur `false`.

Dans ce cas, la vérification de la CRL n'est pas effectuée pour le certificat utilisateur. C'est la passerelle qui se charge d'effectuer cette vérification.

☞ Pour en savoir davantage sur le téléchargement de la liste de révocation de certificats, voir la section 6.4 Restriction du téléchargement des CRL.

7.2.10 crl_cache_duration

Compatibilité : Windows

Si vous souhaitez limiter le nombre de fois qu'une CRL est téléchargée pour la validation du certificat de la passerelle sans pour autant empêcher son téléchargement – toujours en vue d'accélérer le temps d'ouverture d'un tunnel –, vous pouvez ajouter le paramètre dynamique `crl_cache_duration` défini à une valeur correspondant au nombre d'heures pendant lequel la CRL est mise en cache.

Lorsque la valeur du paramètre est égale à zéro, la mise en mémoire cache de la CRL est désactivée. La durée de la mise en cache est limitée à sept jours, soit 168 heures. Toute valeur supérieure à 168 sera considérée comme égale au maximum de sept jours.

Lorsque le paramètre dynamique est configuré avec une valeur différente de zéro, la CRL est stockée dans une mémoire cache et un délai d'expiration correspondant au nombre d'heures configuré est fixé pour cette CRL. Tant que le délai n'est pas écoulé, la CRL dans la mémoire cache est utilisée et aucun téléchargement n'est effectué. Lorsque le délai est écoulé, la CRL est téléchargée et mise à jour dans la mémoire cache.

☞ Pour en savoir davantage sur le téléchargement de la liste de révocation de certificats, voir la section 6.4 Restriction du téléchargement des CRL.

7.2.11 allow_server_extra_keyusage

Compatibilité : Windows, macOS

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Key Usage mentionnées à la section 6.3.2, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le paramètre dynamique `allow_server_extra_keyusage` défini à la valeur `true`.

Dans cette configuration, le certificat sera également validé si l'extension Key Usage contient l'une des combinaisons de valeurs suivantes :

- `digitalSignature` + `keyEncipherment` + `keyAgreement`
- `digitalSignature` + `keyAgreement`
- `nonRepudiation` + `keyEncipherment`
- `nonRepudiation` + `keyEncipherment` + `keyAgreement`
- `nonRepudiation` + `keyAgreement`
- `keyEncipherment`
- `keyEncipherment` + `keyAgreement`

De plus, dans cette configuration l'extension Key Usage peut être marquée comme non critique.

Conformément aux exigences de sécurité, la valeur `keyEncipherment` de l'extension Key Usage a été rendue obsolète et remplacée par la valeur `nonRepudiation`, qui est désormais acceptée par défaut Cependant, la version 7.5 du Client VPN Windows Enterprise continue d'accepter la valeur `keyEncipherment` sans l'utilisation du paramètre dynamique `allow_extra_keyusage`.

Il est recommandé de préférer la valeur `nonRepudiation` de l'extension Key Usage à la valeur `keyEncipherment`.

☞ Pour en savoir davantage sur ces contraintes, voir la section 6.3.2 Contraintes relatives à l'extension Key Usage.

7.2.12 allow_server_and_client_auth

Compatibilité : ,

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le paramètre dynamique `allow_server_and_client_auth` défini à la valeur `true`.

Dans cette configuration, le certificat sera également validé si l'extension Extended Key Usage contient l'une des combinaisons de valeurs suivantes :

- `id-kp-ServerAuth` + `id-kp-ClientAuth` ou
- `id-kp-serverAuth` + `id-kp-ClientAuth` + `id-kp-ipsecIKE`.

☞ Pour en savoir davantage sur ces contraintes, voir la section 6.3.3 Contraintes relatives à l'extension Extended Key Usage.

7.2.13 sha2_in_cert_req

Compatibilité : ,

Si vous souhaitez sélectionner manuellement le format de la liste concaténée de condensats des clés publiques des autorités de certification de confiance dans la charge utile de demande de certificat (CERTREQ payload), vous pouvez ajouter le paramètre dynamique `sha2_in_cert_req` défini à la valeur `true` pour SHA-2 ou à la valeur `false` pour SHA-1.

Si la longueur ne permet pas de déterminer le format, SHA-1 est privilégié. Face à une passerelle configurée en mode IPsec DR, il convient donc d'utiliser le paramètre dynamique `sha2_in_cert_req` pour exclure toute ambiguïté.

☞ Pour en savoir davantage sur cette exigence du référentiel IPsec DR de l'ANSSI, voir la section 6.5.3 Mode IPsec DR.

7.2.14 Method14_RSASSA_PKCS1

Compatibilité : ,

Dans le cas où la passerelle ne prend pas en charge la méthode 14 avec la signature `RSASSA-PSS`, il est possible de configurer le Client VPN pour

employer la méthode 14 avec la signature `RSASSA-PKCS1-v1_5`, en ajoutant le paramètre dynamique `Method14_RSASSA_PKCS1` défini à la valeur `true` ou `yes`.

☞ Pour en savoir davantage sur les méthodes d'authentification des certificats, voir la section 13.2.5 Méthodes d'authentification des certificats.

7.2.15 Method1_PKCS1v15_Scheme

Compatibilité : ,

Dans le cas où la passerelle ne prend pas non plus en charge la méthode 14 avec la signature `RSASSA-PKCS1-v1_5`, il est possible de configurer le Client VPN pour employer la méthode 1 avec signature numérique RSA et SHA-2, en ajoutant le paramètre dynamique `Method1_PKCS1v15_Scheme` défini à la valeur `04` (SHA-256), `05` (SHA-384) ou `06` (SHA-512). Toute autre valeur sera rejetée par le Client VPN.

☞ Pour en savoir davantage sur les méthodes d'authentification des certificats, voir la section 13.2.5 Méthodes d'authentification des certificats.

7.2.16 use_method_214

Compatibilité : ,

Lorsque le Client VPN doit créer une signature pour un certificat utilisateur de type Brainpool, la méthode d'authentification 14 est utilisée par défaut, ce qui convient pour une passerelle ne fonctionnant pas en mode DR. Si ce type de certificat doit être utilisé avec une passerelle fonctionnant en mode DR, il convient d'ajouter le paramètre dynamique `use_method_214` défini à la valeur `true`. L'algorithme d'empreinte numérique NID_sha256, NID_sha384 ou NID_sha512 est utilisé pour signer selon la taille de la clef.

☞ Pour en savoir davantage sur les méthodes d'authentification des certificats, voir la section 13.2.5 Méthodes d'authentification des certificats.

7.2.17 user_smartcard_tip

Compatibilité :

Depuis la version 7.5 du Clients VPN Windows Enterprise, en présence de plusieurs cartes à puce identiques utilisant des lecteurs identiques, le

paramètre dynamique `user_smartcard_tip` peut être défini à une valeur au choix permettant d'identifier de manière univoque chaque carte à puce.

☞ Pour en savoir davantage sur l'utilisation d'un certificat sur carte à puce ou token, voir la section 6.2.5 Utilisation de certificats sur carte à puce ou sur token.

8 Gestion du Panneau TrustedConnect

8.1 Présentation

Compatibilité :

Le **Panneau TrustedConnect** permet d'ouvrir une connexion VPN de manière automatisée en dehors du réseau de confiance et de garder la connexion ouverte en cas de changement d'interface réseau.

Pour être prise en compte, cette connexion VPN doit respecter les conditions suivantes :

1. La connexion VPN doit être la première connexion VPN définie dans le **Panneau des Connexions**. Pour configurer cette première connexion, reportez-vous à la section Créer une configuration du « Guide de l'administrateur » du CMC.
2. Le tunnel VPN doit être configuré en IPsec/IKEv2.

Les fonctions suivantes du **Panneau TrustedConnect** sont configurables :

- Exclusion d'interfaces réseau d'Always-On
- Détection du réseau de confiance (TND)
- Gestion de l'extraction des tokens ou des cartes à puce
- Gestion des scripts liés au tunnel VPN
- Minimisation de l'IHM
- Purge des fichiers de logs

8.2 Always-On

8.2.1 Principe et fonctionnement

La fonctionnalité **Always-On**, toujours active avec le **Panneau TrustedConnect**, assure le maintien de la sécurité de la connexion à chaque changement d'interface réseau.

Les type d'interfaces réseaux pris en charge sont les suivants :

- Adaptateur virtuel (ex : vmware)
- Wi-Fi
- Ethernet
- Modem USB (type smartphone)
- Modem Bluetooth (type smartphone)

Les évènements réseau déclenchant la reconnexion automatique du tunnel (et la détection du réseau de confiance, le cas échéant), sauf exclusion explicite (voir section 8.2.2 Configuration de Always-On) sont les suivants :

- Connexion à un réseau (adresses APIPA ignorées)
- Déconnexion d'un réseau
- Un adaptateur change d'adresse IP ou passage DHCP à statique et vice versa
- ipconfig /release
- ipconfig /renew
- Passage en mode avion

8.2.2 Configuration de Always-On

La fonctionnalité **Always-On** est activée dès lors que le **Panneau TrustedConnect** est utilisé pour ouvrir un tunnel VPN. Elle peut être configurée pour exclure certaines interfaces réseau de la reconnexion automatique du tunnel VPN.

Dans le CMC, la configuration des paramètres de la fonctionnalité **Always-On** s'effectue dans le bloc **Always-On** des **Paramètres avancés** d'une connexion de type **TrustedConnect**.

☞ Pour une description détaillée de ce bloc, voir la section 4.4.3 Bloc Always-On.

8.3 Détection du réseau de confiance (TND)

8.3.1 Principe et fonctionnement

8.3.1.1 Généralités

Cette fonctionnalité consiste à détecter si le poste est connecté au réseau de l'entreprise (réseau de confiance) ou non.

Lorsque le Client VPN détecte que le poste n'est pas sur le réseau de l'entreprise, le tunnel prédéfini est ouvert automatiquement. Ce document fait référence à cette fonctionnalité sous le terme TND (Trusted Network Detection).

Le **Panneau TrustedConnect** utilise l'une des deux méthodes suivantes pour détecter si le poste se trouve sur un réseau de confiance ou non par l'association de la détection :

1. d'un suffixe DNS de confiance et de la vérification de l'accès à un serveur web de confiance ainsi que de la validité de son certificat (cf. section 8.3.1.2 Méthode HTTPS) ;
2. d'un serveur Active Directory (AD) et la présence d'un nom de domaine dans une liste de domaines de confiance (cf. section 8.3.1.3 Méthode AD).

Si le Mode filtrant est actif, il convient de configurer la TND tel que décrit dans le « Guide d'utilisation du Mode filtrant » disponible sur le site TheGreenBow.

8.3.1.2 Méthode HTTPS

La méthode HTTPS se déroule en deux étapes :

1. Vérification que l'un des suffixes DNS des interfaces réseau présentes sur le poste fait partie de la liste des suffixes DNS de confiance (liste configurée dans le logiciel, cf. ci-dessous).
2. Accès automatique en HTTPS à un serveur web de confiance, et vérification de la validité de son certificat.

Les deux étapes sont obligatoires et doivent être associées pour détecter que le poste se trouve sur un réseau de confiance. Pour cela, le Client VPN teste en premier lieu la présence d'un suffixe DNS de confiance :

- s'il n'en trouve pas, le Client VPN ne poursuit pas le test, et conclut que le poste n'est pas connecté au réseau de confiance ;
- s'il en trouve un, il poursuit la séquence de test en vérifiant l'accès au serveur de confiance et la validité de son certificat.

Au premier serveur de confiance accessible dont le certificat est valide, le Client VPN conclut que le poste est connecté au réseau de confiance.

Dans tous les autres cas énumérés ci-dessous, le Client VPN conclut que le poste n'est pas connecté au réseau de confiance, et tente alors automatiquement d'ouvrir la connexion VPN configurée :

- aucun suffixe DNS trouvé dans la liste des suffixes DNS de confiance,
- liste des suffixes DNS de confiance vide,
- liste d'URL de serveurs de confiance vide,
- aucun serveur de confiance accessible, ou aucun n'ayant de certificat valide.

Pour activer la fonctionnalité de détection du réseau de confiance (TND), les paramètres suivants doivent donc être configurés :

- une liste de suffixes DNS,
- une liste d'URL de serveurs de confiance.

Sur certains postes, lors de l'apparition d'une interface réseau, un délai de quelques secondes est nécessaire avant que l'interface ne soit prête à émettre. Pour pallier ce délai, le paramètre **Délai de prise en compte** est disponible dans le bloc **Always-On** (voir section 4.4.3 Bloc Always-On).

8.3.1.3 Méthode AD

Cette méthode de détection de réseaux de confiance (TND), introduite avec la version 7.5 du Client VPN Windows Enterprise, permet d'exploiter la connexion à Active Directory (AD) pour déterminer si le poste se trouve sur un réseau de confiance. Cette méthode se décline en trois variantes :

- **AD seul** : vérifie si le poste est intégré à un domaine et, si c'est le cas, le nom du domaine est vérifié par rapport à une liste de noms de domaines de confiance[1] ;
- **LDAP** : comme **AD seul**, plus validation par la connexion à un service d'annuaire LDAP ;
- **LDAPS** : comme **AD seul**, plus validation sécurisée par la connexion à un service d'annuaire LDAPS.

En mode GINA, le poste sera déclaré comme n'étant pas sur un réseau de confiance tant qu'il n'a pas ouvert de session Windows.

8.3.2 Configuration de TND

Dans le CMC, la configuration des paramètres de la fonctionnalité **Trusted Network Detection** s'effectue dans le bloc **Détection de réseau de confiance (TND)** des **Paramètres avancés** d'une connexion de type **TrustedConnect**.

☞ Pour une description détaillée de ce bloc, voir la section 4.4.4 Bloc Détection de réseau de confiance (TND).

[1] Si la liste est vide, tout domaine est accepté.

8.4 Scripts

Le **Panneau TrustedConnect** exécute les scripts liés à l'ouverture et à la fermeture d'un tunnel. Pour configurer cette fonctionnalité, reportez-vous à la section 9.5 Scripts.

9 Automatisation

9.1 Introduction

Les Clients VPN TheGreenBow permettent d'associer des automatismes à chaque tunnel VPN :

- mise en place d'une passerelle redondante (voir 9.2),
- bascule vers un tunnel de repli (fallback tunnel, voir 9.3),
- ouverture automatique du tunnel suivant différents critères (voir 9.4),
- exécution de scripts à différentes étapes de l'ouverture ou de la fermeture du tunnel (voir 9.5),
- mode GINA (voir 9.6),
- partage de bureau distant (voir 9.7).

Ces automatismes sont disponibles pour tout type de tunnel : IPsec/IKEv2 et OpenVPN.

9.2 Passerelle redondante

9.2.1 Présentation

Compatibilité : ,

Les Clients VPN TheGreenBow permettent la gestion d'une passerelle VPN redondante.

Associée au paramétrage du DPD (Dead Peer Detection), cette fonction permet au Client VPN de basculer automatiquement sur la passerelle redondante dès que la passerelle principale est détectée comme étant injoignable ou indisponible.

En effet, sur perte d'un pair, si une passerelle redondante est configurée, le tunnel tente de se rouvrir automatiquement. Il est possible de configurer une passerelle redondante identique à la passerelle principale pour profiter de ce mode de réouverture automatique sans avoir réellement deux passerelles.

L'algorithme de prise en compte de la passerelle redondante est le suivant :

- Le Client VPN contacte la passerelle initiale pour ouvrir le tunnel VPN.
- Si le tunnel ne peut être ouvert au bout de N tentatives, le Client VPN contacte la passerelle redondante.

Le même algorithme s'applique à la passerelle redondante :

- Si la passerelle redondante est indisponible, le Client VPN tente d'ouvrir le tunnel VPN avec la passerelle initiale.

Le Client VPN n'essaye pas de contacter la passerelle redondante si la passerelle initiale est accessible mais qu'il y a des incidents d'ouverture du tunnel.

Le Client VPN n'essaye pas de contacter la passerelle redondante si la passerelle initiale est inaccessible à cause d'un problème de résolution DNS.

9.2.2 Configuration d'une passerelle redondante

La configuration d'une passerelle redondante s'effectue au niveau du bloc **Passerelle distante** de l'onglet **PASSERELLE DISTANTE**.

☞ Pour une description détaillée de ce bloc, voir la section 2.2.2 pour un tunnel IPsec/IKEv2 ou la section 3.2.2 pour un tunnel OpenVPN.

La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction **Tunnel de repli**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé.

9.3 Tunnel de repli

9.3.1 Présentation

Compatibilité :

Le Client VPN Windows Enterprise implémente une fonction de tunnel de repli (fallback tunnel) qui permet de tenter automatiquement l'ouverture d'un tunnel alternatif lorsque l'ouverture du premier tunnel échoue.

9.3.2 Configuration d'un tunnel de repli

Dans le CMC, cette fonction se configure dans le bloc **Tunnel de repli** d'une connexion classique indépendamment du fait que le tunnel soit IPsec/IKEv2 ou OpenVPN.

☞ Pour une description détaillée de ce bloc, voir la section 4.3.3 Bloc Tunnel de repli.

⚠ La fonction **Tunnel de repli** ne doit pas être configurée conjointement avec la fonction **Passerelle redondante**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé.

9.4 Mode d'ouverture automatique

9.4.1 Présentation

Compatibilité : Windows

Le CMC permet de configurer l'ouverture automatique d'un tunnel dans les cas suivants :

- lorsque le Client VPN démarre,
- lorsqu'un clé USB est insérée,
- sur détection de trafic.

9.4.2 Configuration des modes d'ouverture automatique

Dans le CMC, cette fonction se configure dans le bloc **Mode d'ouverture automatique** d'une connexion classique indépendamment du fait que le tunnel soit IPsec/IKEv2 ou OpenVPN.

☞ Pour une description détaillée de ce bloc, voir la section 4.3.4 Bloc Mode d'ouverture automatique.

9.5 Scripts

9.5.1 Présentation

Compatibilité : Windows

Le CMC permet d'indiquer le chemin vers des scripts configurables exécutés dans les différentes phase du cycle de vie d'un tunnel VPN :

- avant ouverture du tunnel,
- après ouverture du tunnel,
- avant fermeture du tunnel,
- après fermeture du tunnel.

Les lignes de commande peuvent être :

- l'appel à un fichier « batch », par exemple : `C:\vpn\batch\script.bat`
- l'exécution d'un programme, par exemple : `C:\Windows\notepad.exe`
- l'ouverture d'une page web, par exemple : `https://mon.site`
- etc.

Les applications sont nombreuses :

- création d'un fichier sémaphore lorsque le tunnel est ouvert, de telle sorte qu'une application tierce puisse détecter le moment où le tunnel est ouvert ;
- ouverture automatique d'un serveur intranet de l'entreprise, une fois le tunnel ouvert ;
- nettoyage ou vérification d'une configuration avant l'ouverture du tunnel ;
- vérification du poste (anti-virus mis à jour, versions correctes des applications, etc.) avant l'ouverture du tunnel ;
- nettoyage automatique (suppression des fichiers) d'une zone de travail sur le poste avant fermeture du tunnel ;
- application de comptabilisation des ouvertures, fermetures et durées des tunnels VPN ;
- modification de la configuration réseau, une fois le tunnel ouvert, puis restauration de la configuration réseau initiale après fermeture du tunnel ;
- etc.

Les scripts ne sont pas configurables pour un tunnel configuré en mode GINA. Les champs de saisie sont désactivés.

9.5.2 Configuration des scripts

Dans le CMC, les scripts se configurent dans le bloc **Autres** sur l'onglet **AVANCÉ** d'un tunnel IPsec/IKEv2 ou OpenVPN.

☞ Pour une description détaillée de ce bloc, voir la section 2.6.3.1 pour un tunnel IPsec/IKEv2 ou la section 3.6.3.1 pour un tunnel OpenVPN.

9.6 Mode GINA

9.6.1 Présentation

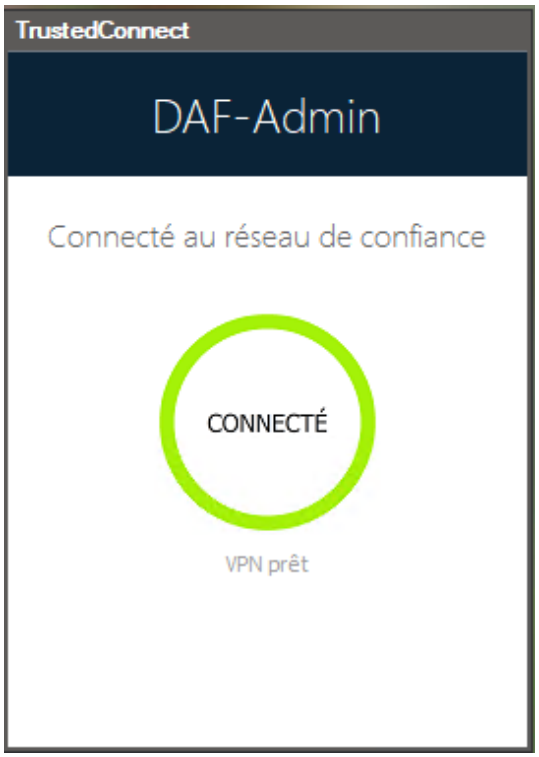
Compatibilité :

Le mode GINA permet d'ouvrir des connexions VPN avant l'ouverture d'une session Windows.

Cette fonction permet par exemple d'établir une connexion sécurisée vers un serveur de gestion des droits d'accès de façon à obtenir les droits d'accès au poste utilisateur avant l'ouverture de la session utilisateur.

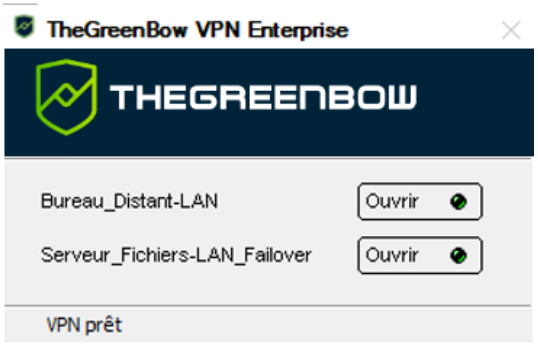
Lorsqu'un tunnel est configuré « en mode GINA », deux cas se présentent :

1. Si le mode de démarrage du Client VPN est configuré en mode **TrustedConnect** (voir section 4.2 Bloc d'identification), alors le **Panneau TrustedConnect** est affiché sur l'écran d'ouverture de session Windows et le Client VPN tente de se connecter automatiquement au réseau de confiance.



À partir de la version 7.4 du Client VPN Windows Enterprise, si l'option permettant de choisir la connexion dans le **Panneau TrustedConnect** a été activée à l'aide de la propriété MSI `DIALERBEHAVIOR` lors de l'installation du Client VPN (voir le « Guide de déploiement » du Client VPN Windows Enterprise), l'utilisateur peut choisir la connexion avant l'ouverture de la session Windows (voir le « Guide de l'administrateur » du Client VPN Windows Enterprise).

2. Sinon, une fenêtre d'ouverture de tunnel similaire au **Panneau des Connexions** est affichée sur l'écran d'ouverture de session Windows. Elle permet d'ouvrir manuellement ou automatiquement un tunnel VPN.



Depuis la version 7.5 du Client VPN Windows Enterprise, le comportement du mode GINA s'adapte en fonction du niveau de conformité détecté par le Secure Connection Agent (SCA), qui détermine si un poste doit être autorisé à accéder au réseau de l'entreprise (voir le « Guide de l'administrateur » du SCA).

Cas d'usage particulier

Si vous souhaitez utiliser plusieurs tunnels, dont un pour le mode GINA et un autre pour la connexion de l'utilisateur en mode TrustedConnect après l'ouverture de la session Windows, le tunnel utilisateur doit être le premier de la liste des connexions.

Ainsi, le tunnel GINA sera ouvert au démarrage du poste, puis une transition vers le tunnel utilisateur sera opérée lors de l'ouverture de la session Windows. De même, une transition du tunnel utilisateur vers le tunnel GINA sera effectuée lorsque l'utilisateur ferme sa session Windows.

9.6.2 Configuration du mode GINA

Dans le CMC, la configuration d'une connexion VPN en mode GINA s'effectue dans le bloc **Mode GINA** d'une connexion classique ou

TrustedConnect indépendamment du fait que le tunnel soit IPsec/IKEv2 ou OpenVPN.

☞ Pour une description détaillée de ce bloc, voir la section 4.3.2 pour une connexion classique ou la section 4.4.2 pour une connexion TrustedConnect.

9.6.3 Utilisation du mode GINA

Lorsque la connexion VPN est configurée en mode GINA, la fenêtre d'ouverture des tunnels GINA est affichée sur l'écran d'ouverture de session Windows. Le tunnel VPN s'ouvre automatiquement s'il est configuré dans ce sens.

Un tunnel associé à une connexion VPN en mode GINA peut parfaitement mettre en œuvre une authentification EAP (l'utilisateur doit alors entrer son identifiant / mot de passe), ou une authentification par certificat (l'utilisateur doit alors entrer le code PIN d'accès à la carte à puce).

Considération de sécurité

Un tunnel configuré en mode GINA peut être ouvert avant l'ouverture de la session Windows, donc par n'importe quel utilisateur du poste. Il est donc fortement recommandé de configurer une authentification forte par certificat, et si possible sur support amovible.

ℹ Pour que l'option **Ouvrir automatiquement ce tunnel sur détection de trafic** (voir section 4.3.4 Bloc Mode d'ouverture automatique) soit opérationnelle après ouverture de la session Windows, l'option **Peut être ouvert avant le logon Windows** ne doit pas être cochée.

⚠ Limitation : Les scripts ne sont pas disponibles pour les tunnels VPN en mode GINA.

⚠ Il est impossible d'utiliser en mode GINA une connexion VPN dont le tunnel est configuré avec un certificat stocké dans le magasin de certificats utilisateur de Windows. En effet, le mode GINA est exécuté avant qu'un utilisateur Windows ne soit identifié (hors de toute session utilisateur). Le logiciel ne peut tout simplement pas identifier le certificat de l'utilisateur dans le magasin de certificats machine de Windows.

9.7 Partage de bureau distant

Compatibilité :

9.7.1 Présentation

L'ouverture d'une session « Remote Desktop » (partage de bureau distant) au travers d'internet sur un ordinateur Windows distant nécessite habituellement l'établissement d'une connexion sécurisée, ainsi que la saisie des paramètres de connexions (adresse de l'ordinateur distant, etc.).

Le Client VPN Windows Enterprise permet de simplifier et de sécuriser automatiquement l'ouverture d'une session « Remote Desktop » : en un seul clic, la connexion VPN s'établit avec le poste distant et la session RDP (Remote Desktop Protocol) est automatiquement ouverte sur ce poste distant.

9.7.2 Configuration du partage de bureau distant

Dans le CMC, le partage de bureau distant se configure dans le bloc **Autres** sur l'onglet **AVANCÉ** d'un tunnel IPsec/IKEv2 ou OpenVPN.

☞ Pour une description détaillée de ce bloc, voir la section 2.6.3.3 pour un tunnel IPsec/IKEv2 ou la section 3.6.3.3 pour un tunnel OpenVPN.

10 IPv4 et IPv6

Les Clients VPN TheGreenBow prennent en charge les protocoles IPv4 et IPv6, que ce soit pour la communication avec la passerelle ou pour la communication sur le réseau distant. Les Clients VPN permettent de combiner l'utilisation d'IPv4 et IPv6, par exemple pour établir une connexion IPv4 sécurisée dans un tunnel VPN transporté sur IPv6.

Le choix IPv4/IPv6 se fait soit d'après l'adresse IP si elle est numérique, soit d'après la résolution DNS. Dans ce dernier cas, la résolution du nom de la passerelle fournit soit une adresse IP soit IPv4, soit IPv6, soit les deux. Si les deux adresses sont fournies, l'adresse IPv4 est privilégiée.

Pour les tunnels IPsec/IKEv2, la configuration du protocole IPv4 ou IPv6 s'effectue dans le bloc **Réseau** de l'onglet **CHILD SA**.

☞ Pour une description détaillée de ce bloc, voir la section 2.4.3 Bloc Réseau.

Le protocole IP configuré par le bouton **IPv4/IPv6** est exactement le protocole utilisé sur le réseau distant.

Le choix IPv4 ou IPv6 s'applique à l'ensemble des sous-blocs du bloc **Réseau**.

11 Recommandations de sécurité

11.1 Hypothèses

Afin de garantir un niveau de sécurité approprié, les conditions de mise en œuvre et d'utilisation suivantes doivent être respectées.

11.1.1 Profil et responsabilités des administrateurs

L'administrateur système et réseau et l'administrateur sécurité chargés respectivement de l'administration du système et de la définition des politiques de sécurité VPN sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et les procédures d'administration.

L'administrateur sécurité s'assure régulièrement que la configuration du produit est conforme à celle qu'il a mise en place et effectue les mises à jour requises le cas échéant.

La fonction de journalisation du produit est activée et correctement configurée. Les administrateurs sont responsables de la consultation régulière des journaux.

11.1.2 Profil et responsabilités de l'utilisateur

L'utilisateur du logiciel est une personne non hostile et formée à son utilisation. En particulier, l'utilisateur exécute les opérations dont il a la charge pour le bon fonctionnement du produit et ne divulgue pas les informations utilisées pour son authentification auprès de la passerelle VPN.

11.1.3 Respect des règles de gestion des éléments cryptographiques

Les bi-clés et les certificats utilisés pour ouvrir le tunnel VPN sont gérés (génération, révocation) par une autorité de certification de confiance qui garantit le respect des règles dans la gestion de ces éléments cryptographiques et plus particulièrement les recommandations issues de [RGS_B1] et [RGS_B2].

11.2 Configuration VPN

11.2.1 Données sensibles dans la configuration VPN

Il est recommandé de ne mémoriser aucune donnée sensible dans le fichier de configuration VPN.

À ce titre, il est recommandé de ne pas utiliser les facilités suivantes offertes par le logiciel :

- Ne pas utiliser le mode EAP (mot de passe / login) seul, mais uniquement en combinaison avec un certificat,
- Dans le cas où EAP est utilisé, ne pas mémoriser le login / mot de passe EAP dans la configuration VPN (fonction décrite à la section 2.3.4),
- Ne pas importer de certificat dans la configuration VPN (fonction décrite à la section 6.2.4), et privilégier l'utilisation de certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows,
- Ne pas utiliser le mode « Clé partagée » (fonction décrite à la section 2.3.2) et privilégier le mode « Certificat » avec des certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows,
- Ne pas diffuser la configuration VPN en clair, c'est-à-dire non protégée par un mot de passe (fonction décrite à la section).

11.2.2 Authentification de l'utilisateur

Les fonctions d'authentification de l'utilisateur proposées par le CMC sont décrites ci-dessous, de la plus faible à la plus forte.

En particulier, il est à noter qu'une authentification par clé partagée (preshared key), si elle est facile à mettre en œuvre, permet néanmoins à tout utilisateur ayant accès au poste, de monter un tunnel, sans vérification d'authentification.

Type d'authentification de l'utilisateur	Force
Clé partagée	faible
EAP	
Popup EAP	
Certificat mémorisé dans la configuration VPN	
Certificat dans le magasin de certificats de l'OS	
Certificat sur carte à puce ou sur token	forte

11.2.3 Authentification de la passerelle VPN

Il est recommandé de mettre en œuvre la vérification du certificat de la passerelle VPN, tel que décrit à la section 6.3 Certificat de la passerelle VPN.

Il est recommandé de ne pas configurer le Client VPN pour valider les certificats non conformes aux contraintes relatives aux extensions Extended Key Usage et Key Usage (ne pas utiliser les paramètres dynamiques `allow_server_and_client_auth` et `allow_server_extra_keyusage`).

11.2.4 Protocole

Il est recommandé de ne configurer que des tunnels IPsec/IKEv2 (et pas OpenVPN).

11.2.5 Mode « tout dans le tunnel » et « split tunneling »

Il est recommandé de configurer le tunnel VPN en mode « tout le trafic dans le tunnel » avec le mode « bloquer les flux non chiffrés » (split tunneling) activé.

☞ Voir les sections 2.4.3.1 et 2.6.2.

11.2.6 Mode GINA

Il est recommandé d'associer une authentification forte à tout tunnel en mode GINA.

11.2.7 Recommandations de l'ANSSI

Les recommandations décrites ci-dessus peuvent être complétées par le document de configuration IPsec rédigé par l'ANSSI : Recommandations de sécurité relatives à IPsec pour la protection des flux réseau.

12 Contact

12.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur le site : https://thegreenbow.com/.

12.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

12.3 Support

Le site TheGreenBow propose plusieurs pages concernant le support technique des logiciels :

Aide en ligne

https://thegreenbow.com/fr/support/assistance/

FAQ

https://thegreenbow.com/fr/faq/

Formulaire de contact

Le support technique est accessible via un formulaire disponible sur le site TheGreenBow à l'adresse : https://thegreenbow.com/fr/support/assistance/support-technique/.

13 Annexes

13.1 Architecture sécurisée

Dans une démarche de sécurisation dès la conception[1], le CMC a été conçu comme un boîtier applicatif[2] basé sur des microservices sans état[3] gérés par un orchestrateur permettant de garantir une haute disponibilité.

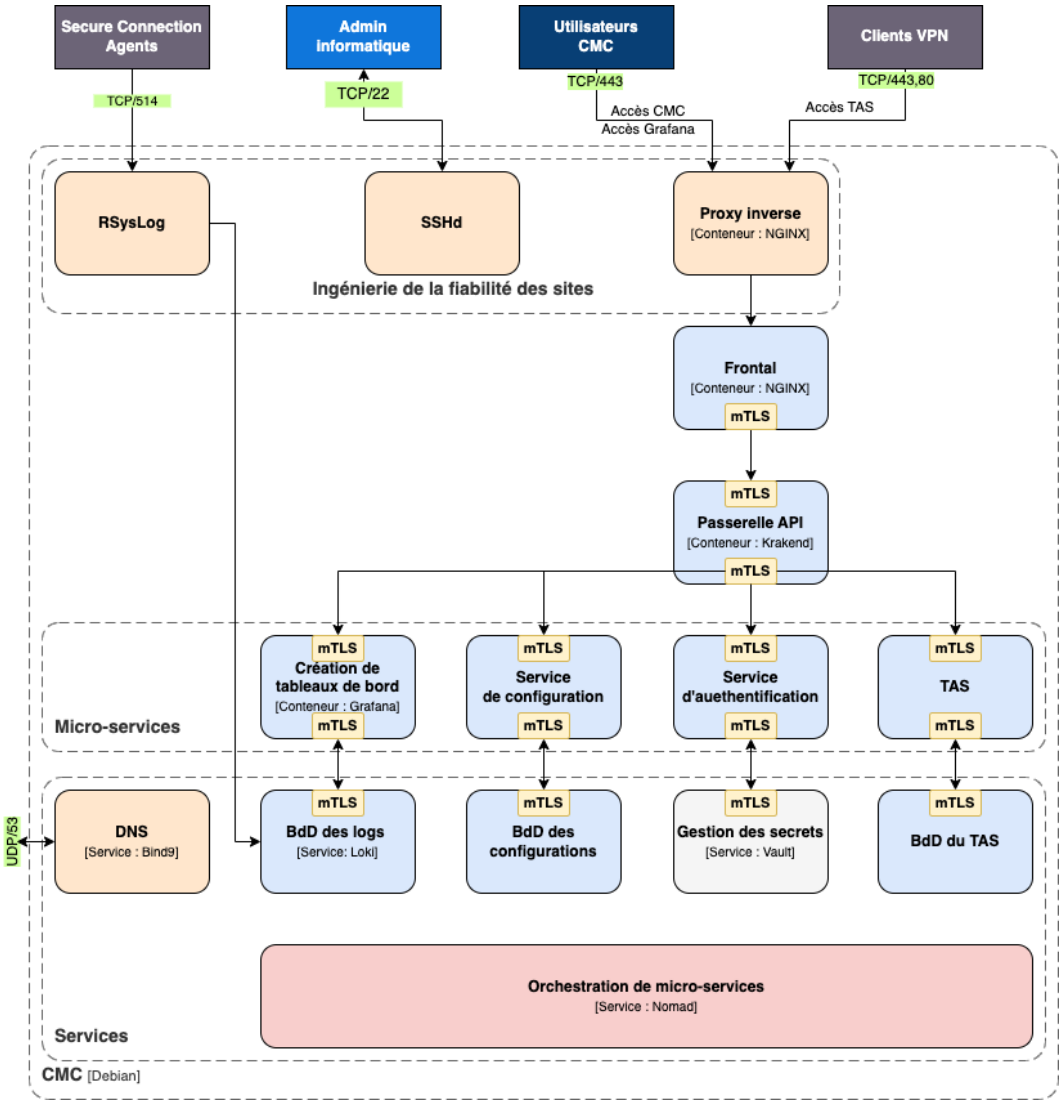
Les services ainsi exposés sur le réseau de l'entreprise sont sécurisés au moyen de certificats pouvant s'intégrer dans la PKI de l'entreprise. Toutes les informations échangées sont chiffrées.

Fonctionnellement, le CMC communique avec les utilisateurs (RSSI, administrateurs…) au travers d'un frontal web, et avec les clients VPN au travers d'un proxy inversé pour authentifier et filtrer les appels.

De la même manière que pour ses clients VPN, TheGreenBow suit les CVE afin de faire les mises à jour de sécurité nécessaires dans les plus brefs délais.

[1] *Security by design* en anglais
[2] *Software appliance* en anglais
[3] *Stateless* en anglais

Le schéma suivant présente une architecture simplifiée du CMC :



La partie supérieure du schéma montre que le CMC interagit à la fois avec des logiciels (SCA et Clients VPN) et des humains (administrateur informatique, utilisateurs du CMC).

Le CMC est constitué de plusieurs couches, dont :

- une couche de fiabilité (SRE),
- un frontal,
- une couche de micro-services,
- une couche de services avec un orchestrateur de micro-services.

13.2 Notions élémentaires de cryptographie

13.2.1 Algorithmes SHA, RSA, ECDSA et ECSDSA

Les signatures numériques font généralement intervenir deux algorithmes différents :

- un algorithme de hachage (SHA ou *secure hash algorithm*) et
- un algorithme de signature (RSA : initiales des trois inventeurs, ECDSA : *elliptic curve digital signature algorithm* ou ECSDSA : *elliptic curve Schnorr digital signature algorithm*).

La force du chiffrement RSA dépend de la taille de la clé utilisée. Dès lors que la taille est doublée, l'opération de déchiffrage va demander une puissance de traitement six à sept fois supérieure.

Selon l'ANSSI et le NIST, la taille de clé minimale recommandée est de 2048 bits.

Les algorithmes de hachage peuvent subir deux types d'attaques :

- la collision et
- la pré-image.

Une collision a lieu lorsque deux fichiers différents produisent le même condensat et qu'il est donc possible de substituer l'un pour l'autre.

La pré-image consiste à déterminer la valeur d'un fichier à partir de son condensat. Une pré-image secondaire consiste à produire à partir du condensat une valeur différente que celle à l'origine du hachage.

Selon l'ANSSI, la famille de fonctions de hachage SHA-1 n'est plus conforme à son référentiel général de sécurité et il convient par conséquent d'utiliser la famille SHA-2. Le NIST encourage de la même manière les agences fédérales étatsuniennes d'abandonner le SHA-1 au profit du SHA-2.

Les règles appliquées par le Client VPN Windows Enterprise suivent les recommandations de l'ANSSI et du NIST. Toutefois, si la PKI implémentée ne répond pas à ces exigences, il est possible de débrider le logiciel à l'aide de paramètres dynamiques.

On trouve plusieurs notations pour les algorithmes de la famille SHA-2. Par exemple, SHA-2 (256 bits) s'écrit aussi SHA-256, SHA-2 (384 bits) s'écrit aussi SHA-384 et ainsi de suite.
Il en va de même pour les courbes elliptiques. Par exemple, pour secp256r1 on parle aussi de « courbe P-256 », pour secp384r1 de « courbe P-384 » et pour secp521r1 de « courbe P-521 ».

13.2.2 Accès aux certificats

13.2.2.1 CSP, CNG et PKCS #11 : quelles différences ?

La gestion des certificats sous Windows fait intervenir différents logiciels et normes pour leur stockage, que ce soit dans un magasin de certificats, sur un token ou sur une carte à puce.

Les certificats stockés sur des cartes à puce ou tokens sont généralement copiés dans le magasin de certificats de l'utilisateur actuel, lorsque la carte est insérée dans le lecteur ou que le token est connecté à l'ordinateur.

CSP, CNG et PKCS #11 sont des notions connexes qui font toutes appel à des interfaces de programmation d'application (API) pour la gestion des certificats, mais la technologie mise en œuvre est différente dans chaque cas.

13.2.2.2 CSP et KSP

Sous Windows, la gestion des certificats faisait traditionnellement appel à des fournisseurs de services cryptographiques ou *Cryptographic Service Providers* (CSP) en anglais. Les CSP servent notamment à créer, stocker et accéder aux clés cryptographiques.

Aujourd'hui, il existe une nouvelle génération de modules logiciels indépendants appelés fournisseurs de stockage de clés ou *Key Storage Providers* (KSP) en anglais. Un KSP sert à créer, supprimer, exporter, importer, ouvrir et stocker des clés.

13.2.2.3 CAPI et CNG

L'évolution des normes de sécurité a conduit Microsoft à rendre obsolète l'API associée à ces CSP, appelée Cryptography API (CryptoAPI ou CAPI). Celle-ci a été remplacée par Cryptography API: Next Generation (CNG), dans laquelle les fournisseurs cryptographiques sont dissociés des fournisseurs de clés.

C'est pourquoi les versions 7.2 et supérieures du Client VPN Windows Enterprise ne prennent pas en charge les CSP et que seule l'API CNG est prise en charge par cette version. Il convient donc de s'assurer que le certificat est importé dans le magasin de certificats Windows avec la bonne bibliothèque (cf. section 13.2.3 Déterminer le type de conteneur d'un certificat ci-dessous).

13.2.2.4 Magasin machine et magasin utilisateur

Par ailleurs, il convient de savoir qu'il existe deux magasins de certificats sous Windows :

- le magasin machine, disponible pour tous les utilisateurs d'une machine, et
- le magasin utilisateur, uniquement disponible pour l'utilisateur actuel d'une machine.

Dans les lignes de commande, l'option `-user` de la commande `certutil` sert à spécifier le magasin utilisateur. Lorsqu'elle est omise, le magasin machine est utilisé par défaut.

13.2.2.5 PKCS #11

Enfin, en cryptographie, il existe des normes de cryptographie à clé publique ou *Public Key Cryptography Standards* (PKCS) en anglais. Il s'agit d'un ensemble de spécifications conçues par la société RSA Security.

La norme PKCS #11 fournit des applications avec une méthode d'accès aux périphériques matériels (cartes à puce ou tokens), indépendamment du type d'appareil. Elle comporte donc une API servant d'interface générique à un pilote de périphérique prenant en charge la norme PKCS #11. Cette API est prise en charge par les deux versions 6.8x et 7.x du Client VPN Windows Enterprise dès lors qu'un middleware correspondant est installé.

13.2.2.6 Synthèse

En résumé, il existe donc plusieurs types de middleware d'accès aux certificats stockés sur token, sur carte à puce et dans un magasin de certificats (`certmgr.msc`) :

- **CSP** pour **C**ryptographic **S**ervice **P**rovider (déprécié au profit de CNG) : pris en charge jusqu'à la version 6.8x.
- **CNG** pour **C**ryptography API: **N**ext **G**eneration : seule API prise en charge dans les versions 7.x. Dans le cas présent, il est nécessaire d'importer le certificat dans le magasin Windows avec la bonne bibliothèque.
- **PKCS #11** pour **P**ublic-**K**ey **C**ryptography **S**tandards : pris en charge par les deux versions 6.8x et 7.x.

13.2.3 Déterminer le type de conteneur d'un certificat

CSP et CNG sont des middlewares Microsoft. Sous Windows, les certificats sont stockés dans des conteneurs de type CNG ou de type CSP.

Pour connaître le conteneur des certificats dans le magasin de certificats, le token ou la carte à puce, vous pouvez lister les certificats contenus dans le magasin (utilisateur ou machine). Les informations retournées indiquent le type de fournisseur à partir duquel vous pouvez déduire le type de conteneur (CSP ou CNG). Ce dernier vous permet ensuite de déterminer la compatibilité du certificat avec les versions 7.2 et supérieures du Client VPN Windows Enterprise.

- Pour lister les certificats contenus dans le magasin utilisateur, exécutez la commande suivante :

```
certutil -verifystore -user My
```

- Pour lister les certificats contenus dans le magasin machine, exécutez la commande suivante :

```
certutil -verifystore My
```

À partir des informations retournées, vous pouvez déterminer le type de conteneur de la manière suivante. Si le fournisseur est :

- Microsoft Smart Card Key Storage Provider, le conteneur est de type CNG (compatible avec les versions 7.2 et supérieures) ;
- Microsoft Base Smart Card Crypto Provider, le conteneur est de type CSP (non compatible avec les versions 7.2 et supérieures).

Pour les certificats faisant appel au middleware PKCS #11, le type de conteneur est indifférent étant donné qu'il est compatible avec les deux versions du Client VPN Windows Enterprise.

13.2.4 Format des certificats

À partir de la version 7 du Client VPN Windows Enterprise, le format des certificats doit respecter une taille de clé et un algorithme de hachage précis.

Obligatoire

- Longueur de clé (en bits) : dans le cas des certificats RSA, la taille doit être de 2048 ou plus
- Algorithme de prise d'empreinte (ou *digest algorithm*) : doit être SHA-256, SHA-384 ou SHA-512

Optionnel

La vérification de la CRL du certificat utilisateur.

Depuis la version 7.5 du Client VPN Windows Enterprise, il est possible de vérifier la révocation du certificat de la passerelle à l'aide du protocole de vérification de certificat en ligne en mode agrafage (OCSP ou *Online Certificate Status Protocol* en anglais). Pour cela, il convient d'ajouter le paramètre dynamique `enable_OCSP` défini à la valeur `true` (voir section **Error! Reference source not found. Error! Reference source not found.**).

13.2.4.1 Certificat passerelle

Partie Key Usage extension

- doit être présente,
- doit être marquée comme critique et
- ne doit contenir que les valeurs `digitalSignature` et/ou `nonRepudiation`.

☞ Si ce n'est pas le cas, référez-vous au paramètre dynamique `allow_server_extra_keyusage` décrit à la section 6.3.2 Contraintes relatives à l'extension Key Usage.

Conformément aux exigences de sécurité, la valeur `keyEncipherment` de l'extension Key Usage a été abandonnée au profit de la valeur `nonRepudiation`. Cependant, la version 7.5 du Client VPN Windows Enterprise continue d'accepter la valeur `keyEncipherment` sans l'utilisation du paramètre dynamique `allow_extra_keyusage`.

Il est recommandé de préférer la valeur `nonRepudiation` de l'extension Key Usage à la valeur `keyEncipherment`.

Partie Extended Key Usage extension

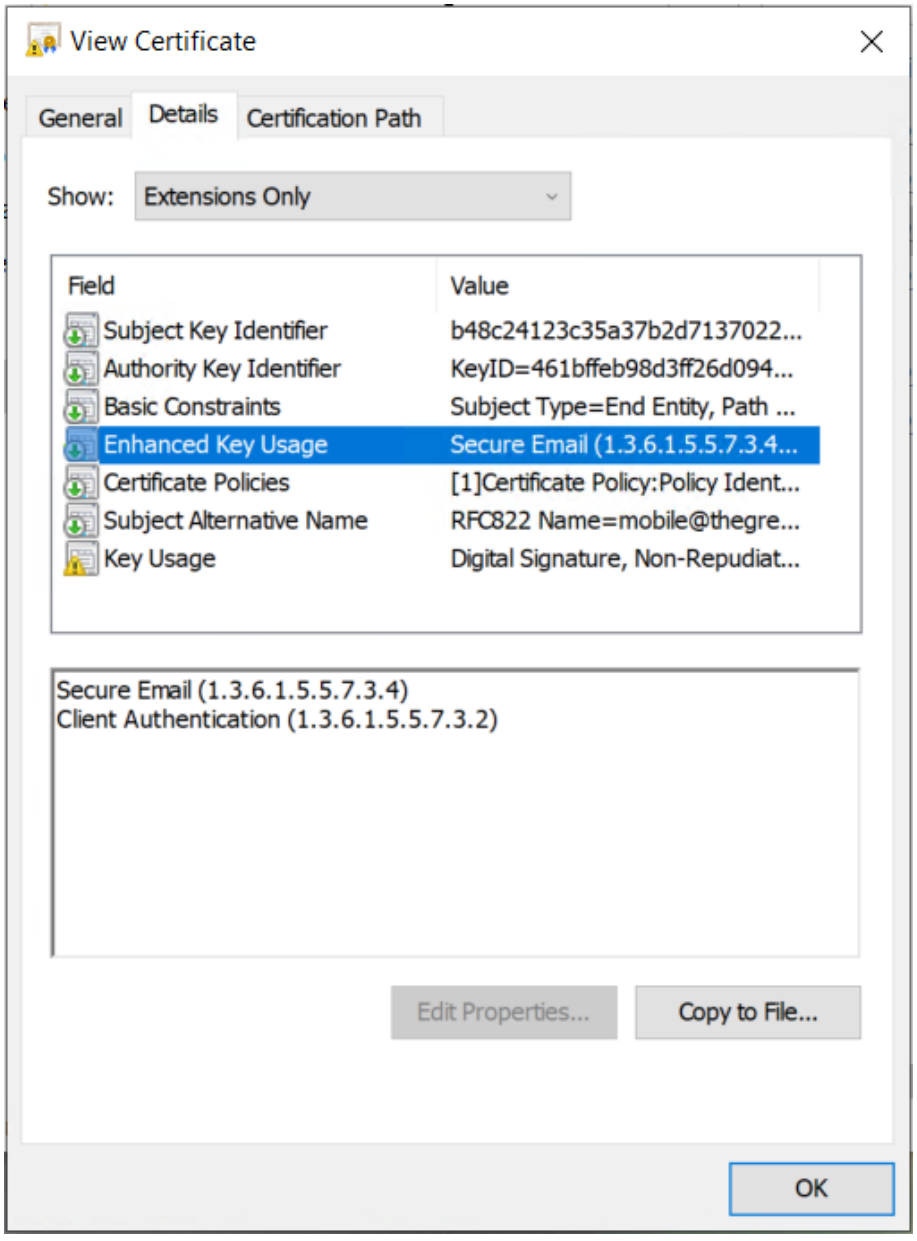
- peut être absente ou présente,
- si elle est présente, elle doit :
  - doit être marquée comme non-critique et
  - uniquement contenir les valeurs suivantes :
    - `id-kp-serverAuth` ou
    - `id-kp-serverAuth` et `id-kp-ipsecIKE`.

☞ Si ce n'est pas le cas, référez-vous au paramètre dynamique `allow_server_and_client_auth` décrit à la section 6.3.3 Contraintes relatives à l'extension Extended Key Usage.

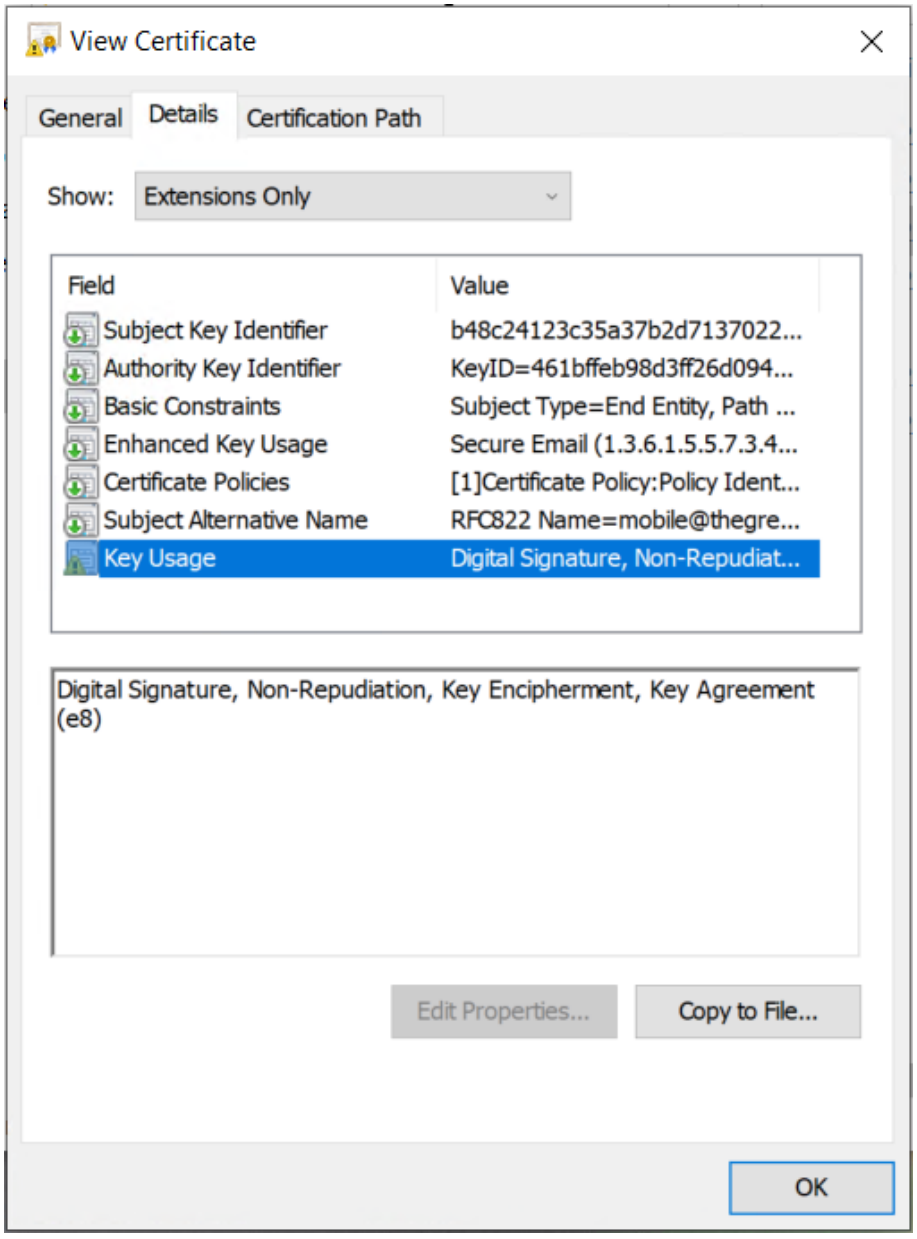
13.2.4.2 Exemple de certificat sous Windows

Dans une PKI Windows, voici la relation entre un certificat et les extensions :

- Extended Key Usage :



- Key Usage :


View Certificate
General
Details
Certification Path
Show:
Extensions Only
Field
Value
Subject Key Identifier
b48c24123c35a37b2d7137022...
Authority Key Identifier
KeyID=461bffeb98d3ff26d094...
Basic Constraints
Subject Type=End Entity, Path ...
Enhanced Key Usage
Secure Email (1.3.6.1.5.5.7.3.4...
Certificate Policies
[1]Certificate Policy:Policy Ident...
Subject Alternative Name
RFC822 Name=mobile@thegre...
Key Usage
Digital Signature, Non-Repudiat...
Digital Signature, Non-Repudiation, Key Encipherment, Key Agreement (e8)
Edit Properties...
Copy to File...
OK

13.2.4.3 Exemple de log d'un certificat

Les extensions sont présentes dans un log de certificat (fichier `tgbikeng.log`) :

```
20220826 17:20:23:953    Local0.Info         [11204]
X509v3 extensions
20220826 17:20:23:956    Local0.Info         [11204]
Basic constraints :
20220826 17:20:23:960    Local0.Info         [11204]
CA:FALSE
20220826 17:20:23:965    Local0.Info         [11204]
Netscape Certificate comment :
20220826 17:20:23:968    Local0.Info         [11204]
TheGreenBow PKI generated server certificate
20220826 17:20:23:971    Local0.Info         [11204]
Subject key identifier :
20220826 17:20:23:974    Local0.Info         [11204]
FB:D6:5A:EF:FE:1B:DC:68:90:66:B9:D7:47:45:EA:B5:86:97:4
A:B3
20220826 17:20:23:978    Local0.Info         [11204]
Authority key identifier :
20220826 17:20:23:981    Local0.Info         [11204]
keyIdentifier:
6F:6D:B8:A5:0B:EA:64:82:2E:B4:5F:0A:35:53:8B:80:05:4C:7
B:0E
20220826 17:20:23:984    Local0.Info         [11204]
authorityCertIssuer: C = FR, ST = Ile-de-France, L =
Paris, O = TheGreenBow, OU = QA40, CN = Root CA
20220826 17:20:23:988    Local0.Info         [11204]
authorityCertSerialNumber: 10:00
20220826 17:20:23:990    Local0.Info         [11204]
Key usage : critical
20220826 17:20:23:995    Local0.Info         [11204]
Digital signature
20220826 17:20:24:000    Local0.Info         [11204]
Extended key usage :
20220826 17:20:24:003    Local0.Info         [11204]
Server authentication
```

13.2.4.4 Certificat utilisateur

Dans le cas d'un certificat utilisateur, il peut il y avoir des avertissements, mais il n'est pas nécessaire de débrider le Client VPN. Les messages sont affichés dans la **Console**.

13.2.5 Méthodes d'authentification des certificats

Le Client VPN Windows Enterprise prend en charge les méthodes d'authentification des certificats suivantes :

- Méthode 1 : signature numérique RSA avec SHA-2 [RFC 7296]
- Méthode 9 : ECDSA « secp256r1 » avec SHA-2 (256 bits) sur la courbe P-256 [RFC 4754]
- Méthode 10 : ECDSA « secp384r1 » avec SHA-2 (384 bits) sur la courbe P-384 [RFC 4754]
- Méthode 11 : ECDSA « secp521r1 » avec SHA-2 (512 bits) sur la courbe P-521 [RFC 4754]
- Méthode 14 : signature numérique RSASSA-PSS, RSASSA-PKCS1-v1_5 et Brainpool avec SHA-2 (256/384/512 bits) [RFC 7427]
- Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) sur la courbe BrainpoolP256r1 (uniquement disponible avec des passerelles prenant en charge cette méthode)

Par défaut, la méthode d'authentification utilisée pour les certificats de type RSA (RSASSA-PSS ou RSASSA-PKCS1-v1_5) est la méthode 14 avec signature RSASSA-PSS. Si la passerelle / le pare-feu utilise la méthode 14 avec la signature RSASSA-PKCS1-v1.5, le Client VPN va rejeter le certificat, avec le message suivant dans la **Console** :

```
RSASSA-PKCS1-v1_5 signature scheme not supported with
authentication method 14
```

Dans le cas où la passerelle ne prend pas en charge la méthode 14 avec la signature `RSASSA-PSS`, il est possible de configurer le Client VPN pour employer la méthode 14 avec la signature `RSASSA-PKCS1-v1_5`, en ajoutant le paramètre dynamique `Method14_RSASSA_PKCS1` défini à la valeur `true` ou `yes` (voir section 7.2.14 Method14_RSASSA_PKCS1).

Dans le cas où la passerelle ne prend pas non plus en charge la méthode 14 avec la signature `RSASSA-PKCS1-v1_5`, il est possible de configurer le Client VPN pour employer la méthode 1 avec signature numérique RSA et SHA-2, en ajoutant le paramètre dynamique `Method1_PKCS1v15_Scheme` défini à la valeur `04` (SHA-256), `05` (SHA-384) ou `06` (SHA-512) (voir section 7.2.15 Method1_PKCS1v15_Scheme). Toute autre valeur sera rejetée par le Client VPN.

La méthode d'authentification utilisée pour les certificats de type ECDSA (courbes elliptiques) dépend de la courbe elliptique utilisée dans le certificat : ECDSA avec SHA-256 sur la courbe P-256, ECDSA avec SHA-384 sur le courbe P-384, ECDSA avec SHA-512 sur la courbe P-521 ou ECDSA avec SHA-256 sur la courbe BrainpoolP256r1.

Lorsque le Client VPN doit créer une signature pour un certificat utilisateur de type Brainpool, la méthode d'authentification 14 est utilisée par défaut, ce qui

convient pour une passerelle ne fonctionnant pas en mode DR. Si ce type de certificat doit être utilisé avec une passerelle fonctionnant en mode DR, il convient d'ajouter le paramètre dynamique `use_method_214` défini à la valeur `true` (voir section 7.2.16 use_method_214). L'algorithme d'empreinte numérique NID_sha256, NID_sha384 ou NID_sha512 est utilisé pour signer selon la taille de la clef.

L'utilisation de l'algorithme SHA-1 dans les signatures numériques n'est pas possible.

Les certificats RSA avec une clé de taille inférieure à 2048 bits seront refusés par le Client VPN Windows Enterprise.

Les certificats ECDSA avec une clé de taille inférieure à 256 bits seront refusés par le Client VPN Windows Enterprise.

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com