Windows Enterprise VPN Client 7.5

Notes de version

Dernière mise à jour : 15 novembre 2024
Référence du document : 20241115_RN_VPE_7.5_FR_1.2

www.thegreenbow.com

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2024-01-22	Toutes	Version initiale	FB, FG, BB
1.1	2024-05-23	3 & 4.1	Mise à jour pour le build 007	BB
1.2	2024-11-15	3 & 4.1	Mise à jour pour le build 109	BB

1 Préambule

Les présentes notes de version apportent une description détaillée des fonctionnalités, améliorations, correctifs, problèmes connus et limitations des différentes versions du Client VPN Windows Enterprise.

Le nom du produit a évolué à plusieurs reprises au fil des ans. Le produit était notamment désigné par les noms suivants :

- Client VPN TheGreenBow ;
- Client VPN TheGreenBow IPsec.

2 Évolutions majeures de la version 7

2.1 Prise en charge de Windows 11

La version 64 bits de Windows 11 est désormais prise en charge sur les processeurs x86-64.

2.2 Fin de la prise en charge de Windows 7 32/64 bits, Windows 8 32/64 bits et Windows 10 32 bits

Cette version du logiciel est uniquement compatible avec Windows 10 & 11 64 bits sur processeurs x86-64. Si vous avez besoin d'un Client VPN pour Windows 7 32/64 bits, Windows 8 32/64 bits ou Windows 10 32 bits, veuillez utiliser la version 6.64 du logiciel.

2.3 Compatibilité des fichiers de configuration

⚠ Les fichiers de configuration VPN issus de versions précédentes du logiciel ne peuvent pas être importés dans la nouvelle version. Lors d'une mise à jour d'une version précédente, l'installateur de la nouvelle version convertit et importe automatiquement la configuration existante.

Ne désinstallez donc pas la version précédente avant de lancer l'installateur de la nouvelle version.

2.4 Vérification du certificat de la passerelle

Par défaut, le certificat de la passerelle est systématiquement vérifié à l'ouverture d'un tunnel. Il peut être nécessaire d'importer la chaîne complète des autorités de certification (CA) de la passerelle, soit dans le magasin Windows, soit dans le fichier de configuration VPN.

Il est également possible (mais non recommandé) de modifier ce comportement par défaut (menu **Options** > **Options PKI**).

2.5 Fin de prise en charge des algorithmes « faibles »

Pour des raisons de sécurité, cette version ne prend plus en charge les algorithmes suivants : DES, 3DES, MD-5, SHA-1, DH 1-2, DH 5. Si une

configuration antérieure comporte l'un de ces algorithmes, l'installeur les convertira en « auto » (négociation automatique avec la passerelle).

Dans le cas où la passerelle prend uniquement en charge ces algorithmes, la connexion avec cette version du logiciel sera impossible.

3 Client VPN Windows Enterprise 7.5 build 109

Fonctionnalités, améliorations, correctifs et problèmes connus depuis la version 7.5.007 :

3.1 Fonctionnalités

- [Version personnalisée] La prise en charge de l'absence de groupe DH dans la proposition a été réintroduite au niveau IKE.

3.2 Améliorations

- Le code d'erreur présenté dans les logs lors d'un problème d'activation donne désormais plus de détails sur les causes de l'erreur.
- Le délai d'attente de téléchargement de la CRL a été porté de 30 secondes à 60 secondes pour une meilleure gestion des connexions mobiles.
- [Version personnalisée] La saisie des données d'accès dans la fenêtre pop-up EAP peut désormais se faire en caractères chinois.
- [Version personnalisée] La case à cocher **Remédiation** a été supprimée de cette version, car présente à tort.

3.3 Correctifs

- Correction d'un problème où les codes d'erreurs générés lors de la vérification d'une signature ECDSA n'étaient pas gérés correctement ni détaillés de manière suffisamment explicite dans les logs.
- Correction d'un problème où le fonctionnement en mode TrustedConnect, en association avec le mode GINA, le Mode filtrant et la propriété MSI `IKESTART`, ne permettait pas d'ouvrir le tunnel.
- Correction d'un problème où la renégociation `IKE_AUTH` pouvait provoquer la génération d'un code d'erreur 13 avec TrustedConnect.
- Correction d'un problème où la renégociation de la phase `CHILD_SA` échouait lorsque celle-ci était initiée par la passerelle.

3.4 Problèmes connus

- Les options **Bloquer les flux non chiffrés** et **Tout le trafic dans le tunnel** ne sont pas compatibles avec les tunnels OpenVPN transportés sur TCP.
- Lors de la reprise après une mise en veille, le tunnel n'est plus ouvert et il est impossible de le rouvrir. Soit la réinitialisation de l'IKE n'a pas

fonctionné ou une erreur d'interface se produit après la réinitialisation de l'IKE.

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2
- 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 la Client VPN pourrait adopter un comportement non déterminé.
- Lors d'une migration d'une version antérieure à une version plus récente, il est recommandé d'effectuer le déploiement avec une configuration créée avec la version à déployer plutôt que de laisser le Client VPN utiliser la configuration antérieure, en particulier pour éviter des problèmes avec les changements du format de la configuration liés à la sélection automatique des certificats sur cartes à puce et dans le magasin Windows.
- Une erreur de code PIN peut se produire lorsque la sélection automatique du certificat est activée.

4 Versions précédentes

4.1 Client VPN Windows Enterprise 7.5 build 007

Fonctionnalités, améliorations, correctifs et problèmes connus depuis la version 7.5.006 :

4.1.1 Fonctionnalités

- [Version personnalisée] Le logo d'une version personnalisée a été mis à jour pour correspondre à la nouvelle charte graphique.

4.1.2 Améliorations

- Pour des raisons de sécurité, les certificats PKCS #12 chiffrés avec l'algorithme RC2 ne peuvent plus être importés.

4.1.3 Correctifs

- Correction d'un problème où le Mode filtrant ne pouvait pas être activé au démarrage (IKESTART = 1).
- [Version personnalisée] Correction d'un problème où la liste de trafic sélecteurs (TSr) n'était pas correctement gérée lors de la renégociation Child SA.
- [Version personnalisée] Correction d'un problème d'ouverture d'un tunnel configuré avec un chiffrement AES-CTR.
- [Version personnalisée] Correction d'un problème où la méthode 14 était utilisée à la place de la méthode 214 lorsqu'un tunnel est configuré avec Brainpool.
- [Version personnalisée] Correction d'un problème où le mode GINA ne fonctionnait pas avec le **Panneau des Connexions** une fois le produit activé.

4.1.4 Problèmes connus

- Les options **Bloquer les flux non chiffrés** et **Tout le trafic dans le tunnel** ne sont pas compatibles avec les tunnels OpenVPN transportés sur TCP.
- Lors de la reprise après une mise en veille, le tunnel n'est plus ouvert et il est impossible de le rouvrir. Soit la réinitialisation de l'IKE n'a pas fonctionné ou une erreur d'interface se produit après la réinitialisation de l'IKE.

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2
- 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 la Client VPN pourrait adopter un comportement non déterminé.
- Lors d'une migration d'une version antérieure à une version plus récente, il est recommandé d'effectuer le déploiement avec une configuration créée avec la version à déployer plutôt que de laisser le Client VPN utiliser la configuration antérieure, en particulier pour éviter des problèmes avec les changements du format de la configuration liés à la sélection automatique des certificats sur cartes à puce et dans le magasin Windows.
- Une erreur de code PIN peut se produire lorsque la sélection automatique du certificat est activée.

4.2 Client VPN Windows Enterprise 7.5 build 006

Fonctionnalités, améliorations, correctifs et problèmes connus depuis la version 7.4.018 :

4.2.1 Fonctionnalités

- Le Client VPN permet désormais d'utiliser l'Active Directory (AD) pour la détection de réseaux de confiance (TND).
- Le Client VPN adapte le comportement du **Panneau des Connexions** et du **Panneau TrustedConnect** 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.
- Le Client VPN est désormais en mesure de transférer des traces d'audit vers le Connection Management Center (CMC) lorsqu'il est associé au module complémentaire Secure Connection Agent (SCA).
- Respect des recommandations de l'ANSSI pour assurer la compatibilité avec les passerelles fonctionnant en mode « IPsec DR strict », notamment par l'utilisation de l'algorithme de hachage SHA-2 dans la charge utile de demande de certificat.
- Il est désormais possible d'indiquer le navigateur internet à utiliser pour la détection de portail captif (CPD) et d'ajouter une ligne de commande, par exemple, en vue de désactiver le proxy pour sécuriser la connexion.
- Tous les composants du Client VPN reposant sur OpenSSL ont été migrés à la version 3.0.
- Le **Panneau TrustedConnect** et le **Panneau des Connexions** gèrent désormais la conformité des terminaux de manière dynamique en fonction de l'état du SCA.

4.2.2 Améliorations

- Amélioration de la granularité dans la configuration du choix de certificat : il est désormais possible d'indiquer l'emplacement du certificat (magasin utilisateur ou magasin machine) au niveau du tunnel.
- Automatisation du choix du certificat quel que soit le support, y compris en présence de plusieurs tokens et cartes à puce.
- Ajout d'un paramètre dynamique permettant d'activer le protocole de vérification de certificat en ligne (OCSP).
- Prise en charge par défaut des certificats utilisateur sur courbe Brainpool utilisant la méthode 14 et ajout d'un paramètre dynamique permettant de définir la méthode 214 comme méthode par défaut lorsque le mode DR est requis.
- Les nouvelles exigences de l'ANSSI relatives aux extensions Key Usage et Extended Key Usage ont été appliquées.
- L'algorithme de hachage (SHA-1 ou SHA-2) est désormais sélectionné automatiquement pour la charge utile de demande de certificat (CERTREQ).
- Ajout d'un paramètre dynamique permettant de configurer la taille du réseau virtuel local.
- Ajout d'une case à cocher **Remédiation** permettant d'indiquer que cette connexion peut être utilisée pour la remédiation.
- Meilleure gestion des paquets fragmentés.
- Pour améliorer la sécurité du produit, la fonctionnalité Mode USB a été retirée.

4.2.3 Correctifs

- Correction d'un problème où le **Panneau TrustedConnect** permettait d'ouvrir plusieurs tunnels simultanément, dont un en mode GINA.
- Correction d'un problème qui entraînait le blocage du poste (BSOD) lorsque le Client VPN était arrêté puis relancé successivement à de nombreuses reprises.
- Correction d'un problème qui entraînait le blocage du poste (BSOD) lors de la réception de paquets UDP incorrects.
- Correction d'un problème où une carte à puce n'était pas détectée après un temps d'inactivité du gestionnaire de cartes à puce.
- Correction d'un problème où les entrées DNS renseignées sur une interface physique n'étaient pas restaurées.
- Correction d'un problème où la présence d'un fichier temporaire créé à la suite d'une fin anormale du programme empêchait le démarrage du mode GINA.
- Correction d'un problème où la saisie d'un code PIN incorrect, lorsque le mode filtrant et la détection de portail captif (CPD) étaient activés, empêchait l'ouverture d'un tunnel lors de toute tentative ultérieure de saisie du bon code PIN.
- Correction d'un problème où le message IKEAuth était incomplet.

- Correction d'un problème où la détection du réseau de confiance (TND) tournait en boucle dans le **Panneau TrustedConnect** en l'absence de certificat valide au lieu de générer une erreur.
- Correction d'un problème de dépassement de mémoire tampon en présence d'un nom de serveur syslog trop long.
- Correction d'un problème où il n'y avait plus de trafic lorsqu'un tunnel était en configuré en IPv4 dans IPv6.
- Correction d'un problème où un seul réseau distant était configuré au moment de la renégociation de la phase Child SA pour un tunnel comportant plusieurs réseaux distants.
- Correction d'un problème où les scripts n'étaient pas exécutés de manière systématique à l'ouverture d'un tunnel.
- Correction d'un problème où les horodatages n'étaient pas synchrones.
- Correction d'un problème où la configuration du Mode filtrant était inopérante.
- Résolution d'un problème de trafic, lorsque le pilote VPN a été mis à jour automatiquement par Windows.
- [Version personnalisée] En raison de la génération insatisfaisante des propositions de suites d'algorithmes, l'option **Auto** a été supprimée des listes déroulantes de sélection des algorithmes.
- [Version personnalisée] Correction d'un problème où la mise en forme de la charge utile SA était incorrecte en mode « Full IPsec DR ».
- [Version personnalisée] Correction d'un problème où la configuration avec le protocole EAP n'était pas possible.

4.2.4 Problèmes connus

- Lors de la reprise après une mise en veille, le tunnel n'est plus ouvert et il est impossible de le rouvrir. Soit la réinitialisation de l'IKE n'a pas fonctionné ou une erreur d'interface se produit après la réinitialisation de l'IKE.
- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2
- 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 la Client VPN pourrait adopter un comportement non déterminé.
- Lors d'une migration d'une version antérieure à une version plus récente, il est recommandé d'effectuer le déploiement avec une configuration créée avec la version à déployer plutôt que de laisser le Client VPN utiliser la configuration antérieure, en particulier pour éviter des problèmes avec les changements du format de la configuration liés à la sélection automatique des certificats sur cartes à puce et dans le magasin Windows.
- Une erreur de code PIN peut se produire lorsque la sélection automatique du certificat est activée.

4.3 Client VPN Windows Enterprise 7.4 build 018

Correctifs, limitations et problèmes connus depuis la version 7.4.016 :

4.3.1 Correctifs

- Correction d'un problème avec OpenVPN où la validation du certificat de la passerelle était désactivée par défaut.
- Correction d'un problème où la modification d'un port de balise TND n'était pas prise en compte.

4.3.2 Limitations

- Mode USB : la configuration spécifique à une machine a été désactivée dans cette version.
- L'utilisation d'IPv4 au sein d'une connexion IPv6 ne fonctionne pas avec toutes les configurations.

4.3.3 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.4 Client VPN Windows Enterprise 7.4 build 016

Fonctionnalités, améliorations, correctifs, limitations et problèmes connus depuis la version 7.3.007 :

4.4.1 Fonctionnalités

- Le **Panneau TrustedConnect** gère désormais plusieurs connexions, y compris en mode GINA et lorsque le Mode filtrant est actif.
- Les demandes d'activation par le TAS sont étalées jusqu'à 90 jours avant la fin de l'abonnement afin d'éviter une surcharge du serveur TAS lorsqu'un grand nombre de licences doivent être renouvelées à la même date.
- Prise en charge de la sélection automatique du certificat utilisateur indépendamment de son support : token / carte à puce ou magasin de certificats Windows.

4.4.2 Améliorations

- La fenêtre de la **Console** disponible à partir du **Panneau TrustedConnect** adopte désormais le même comportement que celle disponible à partir du **Panneau des Connexions** :
  - l'option peut être activée ou désactivée dans le menu contextuel du **Panneau TrustedConnect** ;
  - le même raccourci clavier Ctrl+Alt+T pour activer ou désactiver la journalisation est disponible ;
  - un message dans la fenêtre de la **Console** indique désormais si la journalisation est activée ou désactivée, et une icône pour ouvrir le dossier où sont stockés les logs s'affiche lorsque la journalisation est activée.
- Les licences peuvent désormais être activées sur le serveur TAS après l'expiration de la période d'essai ou de l'abonnement lorsque `NoActivWin` et `AutoActiv` sont activés.
- À la suite des modifications que l'ANSSI a apportées à la [RFC 7296] en lien avec la conformité IPsec DR, la charge utile de demande de certificat doit dorénavant utiliser SHA-2 au lieu de SHA-1 pour les versions personnalisées du logiciel exécutées en mode IPsec DR (nécessite la configuration d'un paramètre dynamique).
- Harmonisation du comportement entre les tunnels SSL/OpenVPN et IKEv2 qui utilisent un certificat client ayant un champ *key usage* incorrect ou une CA manquante : un avertissement s'affiche, mais il est toujours possible d'ouvrir le tunnel.
- Amélioration de la gestion des tunnels OpenVPN sans certificat : la configuration SSL peut toujours être importée, aucune erreur n'est générée dans la **Console** et il est toujours possible d'ouvrir le tunnel.
- Mise à jour d'OpenSSL à la version 1.1.1t.
- Les messages d'avertissement et les codes d'erreur ont été harmonisés entre le **Panneau des Connexions**, le **Panneau TrustedConnect** et le panneau affiché sur l'écran d'ouverture de session Windows lorsque le mode GINA est activé.
- [Version personnalisée] Le tunnel s'ouvre désormais automatiquement lorsqu'une passerelle redondante est définie et que la passerelle principale envoie une demande de suppression (DELETE) suivie d'une demande de création (CREATE).
- [Version personnalisée] Le réseau virtuel est forcé à 32 lorsque le mode CP n'est pas utilisé.

4.4.3 Correctifs

- Correction d'un problème où la génération d'une charge utile d'authentification échouait lors de l'utilisation d'un certificat chargé automatiquement dans le magasin de certificats Windows lors de

l'insertion d'une carte à puce ou d'un token, mais dont la clé privée reste sur la carte à puce ou le token.
- Correction d'un problème où l'onglet **Certificat** n'était plus mis à jour lors de l'insertion ou du retrait d'un token ou d'une carte à puce.
- Dans le cadre de l'utilisation de plusieurs cartes à puce, correction d'un problème où un tunnel était fermé de manière inopinée lors du retrait d'une carte à puce qui n'est pas utilisée avec le Client VPN.
- Correction d'un problème où l'installation du Client VPN était abandonnée sous Windows 11.
- En présence d'une passerelle redondante, la taille du SPI dans la proposition SA_INIT est définie à 8 au lieu de 0 lorsque le Client VPN bascule sur la passerelle redondante.
- Correction d'un problème où l'anneau indicateur de l'état de connexion du **Panneau TrustedConnect** restait gris pendant et après la détection d'un réseau de confiance (TND).
- Correction d'un problème où un tunnel qui n'utilise pas de token était fermé lors du retrait d'un token.
- Correction d'un problème où un tunnel ne se fermait pas côté client lorsqu'une passerelle envoie des demandes de suppression (DELETE) et ne répond plus.
- Correction d'un problème où un tunnel ne s'ouvrait pas lorsque le code PIN correct est saisi après une première saisie d'un code PIN incorrect.
- Correction d'un problème où le Client VPN ne demandait pas explicitement le code PIN lorsqu'une carte à puce est retirée puis réinsérée.
- Correction d'un problème où une réinitialisation IKE était déclenchée lors de l'insertion d'une carte à puce lorsque la CPD est activée.
- Correction d'un problème où l'écriture et la suppression des clefs `path` et `ngpath` était possible à l'aide d'un outil d'exploitation des vulnérabilités.
- Correction d'un problème où un nom de serveur syslog trop long entraînait un dépassement de mémoire tampon.
- [Version personnalisée] Correction d'un problème où une erreur de « format incompatible » se produisait lors de la récupération d'une configuration à partir d'un ancien modèle de passerelle.
- [Version personnalisée] Correction d'un problème où le Client VPN n'acceptait pas un fichier de configuration provenant d'un nouveau modèle de passerelle qui prend en charge les algorithmes de signature SHA-2.
- [Version personnalisée] Correction d'un problème où le Client VPN n'acceptait pas un certificat auto-signé ou un certificat utilisé par les deux points de terminaison distant et local.
- [Version personnalisée] L'algorithme de hachage SHA-1 a été réintroduit pour prendre en charge les équipements plus anciens.
- [Version personnalisée] Correction d'un problème où le **Panneau de Configuration** restait accessible depuis l'icône en barre des tâches alors que l'option **Restreindre l'accès du panneau de configuration aux administrateurs** était activée.

- [Version personnalisée] Le schéma de signature RSASSA-PKCS1-V1_5 a été rétabli en tant que schéma par défaut pour prendre en charge des équipements plus anciens.

4.4.4 Limitations

- Mode USB : la configuration spécifique à une machine a été désactivée dans cette version.
- L'utilisation d'IPv4 au sein d'une connexion IPv6 ne fonctionne pas avec toutes les configurations.

4.4.5 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.5 Client VPN Windows Enterprise 7.3 build 007

Fonctionnalités, améliorations, correctifs, limitations et problèmes connus depuis la version 7.2.008 :

4.5.1 Fonctionnalités

- Ajout d'une fenêtre **Console** au **Panneau TrustedConnect**.
- Permet l'ouverture d'un tunnel dans le **TrustedConnect Panel** même en cas de détection d'un réseau de confiance.
- Le **Panneau TrustedConnect** peut désormais être relancé automatiquement après avoir quitté l'application ou en cas d'arrêt inopiné.
- La CRL peut désormais être téléchargée dans une mémoire cache et un délai d'expiration peut être défini pour la CRL en mémoire cache.

4.5.2 Améliorations

- Prise en charge de plusieurs adresses IP source sur l'interface réseau.
- Le nombre de règles du Mode filtrant a été augmenté de 12 à 30.
- Le Local ID peut désormais être rempli automatiquement avec le DNS ou une adresse e-mail en plus de l'objet du certificat.
- Les mots de passe servant à chiffrer des configurations exportées doivent désormais se conformer aux recommandations de l'ANSSI, c'est-à-dire être composés d'au moins 16 caractères dans un alphabet de 90 symboles, dont au moins un caractère en majuscule, un en minuscule et un caractère spécial.

- Le Client VPN accepte désormais la valeur `id-kp-ipsecIKE` dans l'extension *Extended Key Usage* (EKU) pour un certificat de passerelle VPN.
- Meilleure prise en charge des passerelles IPsec DR :
  - la renégociation des clés de la *Child SA* demande désormais le même *TS* que celui de la *SA* d'origine ;
  - la taille *NONCE* est de 16 octets lorsque *PRF_HMAC_SHA2_256* est utilisé.
- Meilleure prise en charge des tokens / cartes à puce :
  - la fenêtre de saisie du code PIN précise désormais la carte à puce / le token concerné ;
  - PKCS#11 ne provoque plus l'arrêt inopiné du Client VPN avec les lecteurs CNG ;
  - un tunnel n'est plus fermé lorsqu'un token non relatif au tunnel est extrait.

4.5.3 Correctifs

- Les champs DSCP sont désormais gérés correctement dans les paquets ESP créés.
- Le Client VPN ne s'arrête plus de manière inopinée à la sortie du mode veille.
- Le module d'activation lit désormais tous les fichiers `tgbcode` et utilise celui disposant de la date de renouvellement la plus récente.
- Correction d'un problème où la **Console** n'enregistrait plus de logs quand l'utilisateur quittait son poste de travail ou verrouillait sa session.
- Correction d'un problème où le serveur d'activation retournait un message d'erreur injustifié.
- Correction d'un problème où le tunnel s'arrêtait avec le message d'erreur « unsupported payload 53 for this exchange ».
- Correction d'un problème d'ouverture du menu contextuel pour Windows en mode tablette.

4.5.4 Limitations

- Mode USB : la configuration spécifique à une machine a été désactivée dans cette version.

4.5.5 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.6 Client VPN Windows Enterprise 7.2 build 008

Fonctionnalités, améliorations, correctifs, limitations et problèmes connus depuis la version 6.87.109 :

4.6.1 Fonctionnalités

- Mise en œuvre des principes d'un accès réseau à vérification systématique (ou Zero Trust Network Access – ZTNA) pour une meilleure protection du poste de travail.
- Ajout d'une fonction de filtrage des flux de données associée à la détection de portail captif.
- Introduction d'un nouvel algorithme : Diffie-Hellman 28 (BrainpoolP256r1).
- Introduction de la méthode d'authentification de certificat ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits).
- Utilisation par défaut de la méthode d'authentification de certificat 14 RSASSA-PSS avec tous les certificats RSA.
- La vérification de la CRL du certificat utilisateur est désormais optionnelle.
- Forçage du mode d'encapsulation UDP pour IKEv2.
- L'interface utilisateur permet désormais d'ajouter plus de 3 CA.
- Augmentation à 16 du nombre de sous-réseaux pris en charge.
- Possibilité d'augmenter ou de réduire la hauteur de la fenêtre du **Panneau des Connexions**.

4.6.2 Améliorations

- Amélioration de la stabilité du module IKE.
- Meilleure performance du chiffrement AES-GSM.
- Mise à jour de la palette de couleurs utilisée pour l'interface utilisateur et les bitmaps conformément à la nouvelle charte graphique.
- Suppression d'algorithmes considérés comme faibles pour SSL/OpenVPN : MD5, SHA1, TLS suite de sécurité « low », BF-CBC.
- Suppression d'algorithmes considérés comme faibles pour IKEv2 : DES, 3DES, MD5/PRF_HMAC_MD, SHA1/PRF_HMAC_SHA1, SHA2/PRF_HMAC_SHA2_224, DH 1 (modp768), DH 2 (modp1024), DH 5 (modp1536).
- IKEv1 a été supprimé.
- Rejet des certificats RSA dont la taille de la clé est inférieure à 2048 bits.
- Rejet des certificats ECDSA dont la taille de la clé est inférieure à 256 bits.
- Ajout aux propriétés MSI d'informations relatives à la version du logiciel.
- Mise à jour d'OpenSSL à la version 1.1.1l.

- Les nouvelles cartes à puce Gemalto Safenet sont désormais détectées automatiquement.
- La fenêtre popup glissante en barre des tâches est désormais désactivée par défaut.
- Mise à jour de la bibliothèque LZ4 à la version 1.9.3 pour OpenVPN.
- L'interface utilisateur permet désormais l'ajout de CA uniquement dans la boîte de dialogue de **Gestion des CA**.
- Conformément aux règles de l'ANSSI, les extensions *KeyUsage* des certificats utilisateur et passerelle sont désormais vérifiées.
- Toutes les CA d'un fichier P12 sont désormais importées dans la configuration VPN.
- Utilisation de HMAC 256 au lieu du hachage SHA-2 (256 bits) pour la signature du fichier de configuration VPN.
- Les mots de passe servant à chiffrer des configurations exportées doivent désormais être composés d'au moins 16 caractères.

4.6.3 Correctifs

- Correction des blocages qui surviennent lorsque la langue arabe ou grecque est sélectionnée.
- Correction de problèmes rares liés à l'affichage de l'état TrustedConnect.
- Les utilisateurs peuvent désormais refuser l'utilisation d'un tunnel de repli même si aucun message ne s'affiche.
- Correction de certains problèmes avec le Mode filtrant.
- Correction d'un problème de fragmentation IKEv2 lors de l'utilisation d'AES-GCM.
- Diverses améliorations cosmétiques et de stabilité.

4.6.4 Limitations

- Mode USB : la configuration spécifique à une machine a été désactivée dans cette version.

4.6.5 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.7 Client VPN Windows Enterprise 6.87 build 109

Correctifs et problèmes connus depuis la version 6.87.108 :

4.7.1 Correctifs

- Correction de divers problèmes de stabilité liés à TrustedConnect.
- Dans le cadre de l'utilisation de plusieurs cartes à puce, correction d'un problème où un tunnel était fermé de manière inopinée lors du retrait d'une carte à puce qui n'est pas utilisée avec le Client VPN.
- Correction de problèmes liés au Mode filtrant de TrustedConnect lors du passage à un adaptateur réseau USB-C.

4.7.2 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.8 Client VPN Windows Enterprise 6.87 build 108

Améliorations, correctifs et problèmes connus depuis la version 6.87.001 :

4.8.1 Améliorations

- Prise en charge de cartes à puce / tokens multiples avec CNG.
- Mise à jour d'OpenSSL vers la version 1.1.1n pour augmenter le niveau de sécurité.
- Le **Panneau des Connexions** s'affiche désormais automatiquement au démarrage.

4.8.2 Correctifs

- Correction d'un problème qui empêchait la fermeture du Client VPN dans de rares cas.
- Récupération des codes PIN stockés en mémoire cache désormais possible lors d'une reconnexion après le verrouillage de la session.
- Correction d'un problème avec les certificats RSA/SHA512.
- Correction de rares cas d'arrêt inopiné du **Panneau des Connexions** lors de la fermeture.
- Correction d'un problème de DPD après une retransmission.
- Correction d'un problème survenant lorsqu'une suppression (DELETE) n'est pas suivie d'une réception (RECV) et provoque une erreur en mode TrustedConnect.
- La CA ne disparaît plus après avoir décoché la fenêtre popup EAP.

- Correction d'un problème de détection du réseau de confiance (TND).
- Correction d'un problème avec le Local ID lors de l'authentification.
- Correction de problèmes d'activation lors de la mise à jour.
- L'activation en https est désormais opérationnelle.
- Comprend un correctif de sécurité destiné à empêcher le débordement du tampon lors d'une réponse du serveur d'activation.
- Application de modifications DNS sur l'interface physique après un changement d'adresse IP virtuelle lors de la renégociation des clés SA Auth.
- Reconnexion automatique de la fonction Always-On à un réseau Wi-Fi ayant un SSID différent.
- Les clés en base de registre du pilote par défaut sont désormais définies lors de la mise à jour.
- Correction d'un problème avec les clés Yubikey 5 NFC.
- Correction d'une incompatibilité de la licence sauvegardée lors de la mise à jour.
- Correction de l'erreur inattendue « Code 103: erreur de DNS ».
- Correction de l'option *VPNLogPurge*.

4.8.3 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.9 Client VPN Windows Enterprise 6.87 build 001

Fonctionnalités, améliorations, correctifs et problèmes connus depuis la version 6.86.015 :

4.9.1 Fonctionnalités

- La sélection automatique du certificat utilisateur est désormais disponible individuellement pour chaque tunnel.
- La propriété MSI `TOKENOUTHANDLE` (initialement conçue pour TrustedConnect) peut désormais être utilisée pour le **Panneau des Connexions**.

4.9.2 Améliorations

- Ajout d'une propriété MSI permettant d'éviter l'analyse du répertoire `ProgramData` dans son intégralité.
- Ajout d'un paramètre dynamique permettant de choisir le type d'interface réseau virtuelle (publique ou privée).

4.9.3 Correctifs

- Correction de la syntaxe non valide lors de l'envoi de propositions de chiffrement en mode automatique OpenVPN.
- Correction d'un problème de déconnexion via le Wi-Fi avec TrustedConnect.
- Correction de problèmes de mise en cache du code PIN avec les tokens et cartes à puce SafeNet.
- Correction d'un problème survenant lors de l'utilisation de la propriété MSI `SIGNFILE =1`.
- Les propriétés MSI `CERT` et `OSACERT` peuvent désormais être utilisées indifféremment afin de spécifier un certificat pour le TAS.
- Correction d'un problème où TrustedConnect ne parvenait pas à authentifier l'extrémité distante.
- Correction d'un problème de fragmentation IKEv2 lors de l'utilisation d'AES-GCM.
- Correction d'un problème de fragmentation IKEv2 lors de la retransmission de paquets perdus.
- Correction d'un problème dans le **Panneau des Connexions** qui fermait le tunnel uniquement la première fois qu'un jeton est extrait.
- L'ensemble des fichiers `tgbcode *.dat` et `tgbparam*.dat` est désormais copié lors d'une mise à jour.
- Correction d'un problème avec `OSACheck` et désactivation de `OSACheck` lors de la désinstallation.
- Correction d'un problème où le fichier de licence était supprimé lors de la mise à jour de la version 6.6x à la version 6.86 avec une nouvelle licence.
- Correction d'un problème où TrustedConnect restait bloqué à l'état « Connexion en cours ».
- Correction d'un problème qui empêchait la libération d'une licence sur le TAS lors de la désinstallation du Client VPN.
- Les fichiers de configuration Cisco (.pcf) ne sont plus pris en charge et ne sont plus proposés dans la fenêtre de l'explorateur de fichiers de configuration.
- Correction d'un problème survenant lors de la lecture du sujet d'un certificat codé en BMPString.

4.9.4 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.10 Client VPN Windows Enterprise 6.86 build 015

Fonctionnalités, améliorations, correctifs et problèmes connus depuis la version 6.85.007 :

4.10.1 Fonctionnalités

- Les administrateurs peuvent désormais désactiver les repères visuels bleu ou vert permettant d'identifier la connexion directe au réseau de confiance.

4.10.2 Améliorations

- Mise à jour d'OpenSSL à la version 1.1.1l.
- Les fichiers de configuration à partir de la version 2.4.7 d'OpenVPN sont désormais pris en charge.
- L'activation silencieuse peut désormais être effectuée même après l'expiration de la période d'essai.

4.10.3 Correctifs

- TrustedConnect : Correction d'un problème où le Mode filtrant pouvait être désactivé en cas d'erreur de connexion.
- TrustedConnect : Correction d'un problème où le tunnel était parfois indiqué comme étant fermé alors qu'il était ouvert.
- TrustedConnect : Correction d'un problème où le code 9 (aucune réponse de la passerelle) était affiché après le renouvellement de la clé alors que le trafic circulait toujours.
- TrustedConnect : Le panneau se ferme désormais correctement lorsque la fenêtre « À propos » est ouverte.
- Correction d'un problème où une socket était parfois créée sur le port 500/4500 alors qu'elle n'était pas requise.
- L'ACL des données d'activation est désormais correctement restauré lors d'une mise à jour à partir d'anciennes versions.
- Correction de problèmes de codage de caractères spéciaux lors d'une mise à jour à partir d'anciennes versions.
- Correction d'un problème où il était impossible de réinstaller les anciennes versions du logiciel si l'installation MSI échouait.
- L'activation de la licence est désormais réinitialisée correctement après une désinstallation.
- Correction d'un problème rare où les fenêtres d'activation s'affichaient après une activation silencieuse.
- Les licences existantes sont désormais correctement prises en compte lors d'une mise à jour à partir d'anciennes versions.

- La propriété MSI `VPNLOGPURGE` est désormais correctement prise en compte.
- La configuration du middleware PKCS#11 pour les lecteurs de cartes à puce / tokens est désormais correctement définie lors d'une mise à jour à partir d'anciennes versions.
- Le tunnel se ferme désormais lorsqu'un lecteur de cartes à puce / token est retiré.
- Correction d'un problème avec la mise à jour silencieuse lorsque le fichier `%TEMP%\vpncfg.bak` était présent.
- Les propriétés MSI `NOPINCODE`, `SIGNFILE` et `TOKENOUTHANDLE` sont désormais gérées correctement.
- Ajout de certaines traductions manquantes.
- L'option **Bloquer les flux non chiffrés** est décochée par défaut pour IKEv1 (comme pour IKEv2).
- Le fichier `VpnConf.ini` est désormais conservé lors d'une mise à jour.

4.10.4 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.11 Client VPN Windows Enterprise 6.85 build 007

Fonctionnalités, améliorations, correctifs et problèmes connus depuis la version 6.64.003 :

4.11.1 Fonctionnalités

- Nouvel installeur MSI.
- Nouvelle interface utilisateur TrustedConnect.
- Mise à jour logicielle silencieuse à partir des éditions précédemment installées, y compris la récupération de la licence, de la politique de sécurité VPN et des paramètres d'installation.
- Mode Always-On configurable.
- Mode de détection du réseau de confiance (TND) configurable.
- Ajout de la prise en charge de l'API Microsoft CNG.
- Ajout de la prise en charge de la RFC 4304 Extended Sequence Number (ESN).
- Ajout de la prise en charge de la RFC 6023 (Childless IKE Initiation).
- Ajout de la prise en charge de l'authentification des certificats à l'aide de SHA-2 (Méthode 9) [RFC 4754].
- Ajout de la prise en charge de l'authentification des certificats à l'aide de RSA (Méthode 14) [RFC 7427].
- Importation de certificats au format PKCS#12 depuis la ligne de commande.

- L'accès à la politique de sécurité VPN est restreint à l'administrateur Windows (le mot de passe spécifique n'est plus nécessaire).
- Ajout de la prise en charge de la compression Lz4 pour OpenVPN/SSL.

4.11.2 Améliorations

- Mise à jour de la bibliothèque SSL à la version 1.1.1.i.
- Le DNS est demandé de manière explicite (pour la compatibilité avec les passerelles Fortinet).
- Compilé pour Windows 10 64 bits.
- Chiffrement des politiques de sécurité VPN à l'aide de SHA-2.
- Suppression des algorithmes plus faibles (DES, 3DES, SHA, MD5, DH 1-2, DH 5).
- Après connexion à une passerelle redondante, le Client VPN tente de revenir à la passerelle principale à la prochaine ouverture du tunnel.
- Reconnexion automatique au retour du mode veille.

4.11.3 Correctifs

- Le tunnel se ferme désormais lorsqu'un lecteur de cartes à puce est retiré.

4.11.4 Problèmes connus

- L'assistant de création d'un tunnel SSL s'ouvre par défaut sur la création d'un tunnel IKEv2

4.12 Client VPN TheGreenBow 6.64 build 003

Correctifs depuis la version 6.64.002 :

4.12.1 Correctifs

- [Spécifique au partenaire] Assistant d'activation : le lien **Buy a license** est mort.

4.13 Client VPN TheGreenBow 6.64 build 002

Correctifs depuis la version 6.64.001 :

4.13.1 Correctifs

- L'utilisation de réseaux multiples sur plusieurs tunnels ne fonctionne pas correctement sur une seule adresse IP virtuelle.
- DistVPN devrait pouvoir gérer plusieurs fournisseurs de DLL PKCS11.
- Pas de trafic avec AESGCM pour certaines tailles de paquets.

4.14 Client VPN TheGreenBow 6.64 build 001

Fonctionnalités, améliorations et correctifs depuis la version 6.63.005 :

4.14.1 Fonctionnalités

- Désactivation de l'exécution du script (spécifique au partenaire).
- Mise à jour d'OpenSSL à la version 1.1.1.
- IKEv2 Multiple Phase 2.

4.14.2 Améliorations

- Possibilité de modifier les coordonnées de la fenêtre GINA, ainsi que le mode « premier plan ».

4.14.3 Correctifs

- L'itinérance Winstore avec *keyusage* et *dnpattern* ne fonctionne pas correctement.
- Il est possible d'ouvrir un tunnel EAP Multiple Auth sans certificat.
- Erreur « Absence de socket » après retour de veille/hibernation.
- TgbLogonUI : Lors de la renégociation, l'état affiché pour le tunnel IKEV2 Auth n'est pas correct.
- Certificat non pris en compte lors de l'importation de la configuration (spécifique au partenaire).

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com