Client VPN Windows Enterprise

Guide d'utilisation du Mode filtrant

Dernière mise à jour : 15 janvier 2024
Référence du document : 20240115_FM_VPE_7.5_FR_1.0

www.thegreenbow.com

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2024-01-15	Toutes	Version initiale	ALP, BB

1 Introduction

1.1 Présentation

Le logiciel TheGreenBow Client VPN Windows Enterprise contient des fonctionnalités avancées appelées Mode filtrant et Détection de portail captif (ou CPD pour *Captive Portal Detection*) prévues pour un usage spécifique et qu'il convient d'ajouter lors de l'installation du logiciel avant de pouvoir les utiliser.

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**.

Le filtrage des flux est associé aux différents états du Client VPN Windows Enterprise.

Ainsi, par défaut, le Mode filtrant est en mode « tout bloqué » et n'autorise que les flux strictement nécessaires au bon fonctionnement du poste ainsi qu'à la bonne exécution des différents états du Client VPN Windows Enterprise.

De ce fait, le Mode filtrant est associé à la fonction CPD qui détecte automatiquement la présence d'un portail captif pour la connexion à internet.

Si le poste de travail est derrière un portail captif, le logiciel se met en attente pendant 3 minutes (valeur par défaut), le temps pour l'utilisateur de s'authentifier sur ce portail captif. Dès que ce dernier s'est authentifié, le poste est connecté à internet, le Client VPN Windows Enterprise établit alors automatiquement et immédiatement la connexion VPN.

Pour tester si le poste est derrière un portail captif, le Client VPN Windows Enterprise tente de se connecter à un serveur web prédéfini. Si la réponse à cette tentative de connexion n'est pas celle attendue par le Client VPN Windows Enterprise, il en conclut que le poste est derrière un portail captif.

Pour limiter les cas de « faux-positifs » (un portail captif répondrait comme un serveur web de test), il est possible de caractériser le code retour HTTP et/ou les données que le Client VPN Windows Enterprise attend de la part du serveur web en réponse à sa requête.

Il existe également un Mode filtrant restreint et permanent qui est actif y compris lorsque le Client VPN n'est pas lancé (cf. chapitre 5 Contextes et états du Panneau TrustedConnect).

Ce guide spécifique est un complément au Guide de l'administrateur et au Guide de déploiement du Client VPN Windows Enterprise. Il est destiné aux

administrateurs système qui souhaitent mettre en place ces fonctionnalités avancées pour leurs utilisateurs.

⚠ Le Mode filtrant ne saurait en aucun cas remplacer un pare-feu sur le poste de travail configuré avec cette fonctionnalité du Client VPN Windows Enterprise.

1.2 Références

Ce document fait référence aux documents suivants :

- Guide d'utilisation du Mode filtrant du Client VPN Windows Enterprise (ce document)
- Guide de l'administrateur du Client VPN Windows Enterprise
- Guide de déploiement du Client VPN Windows Enterprise

Vous trouverez les dernières versions de ces documents sur la page Documentations produits sur notre site à l'adresse : https://www.thegreenbow.com/fr/support/documentations-produits/.

2 Ajout du Mode filtrant

2.1 Introduction

Pour pouvoir l'utiliser, le Mode filtrant doit être ajouté lors de l'installation du Client VPN Windows Enterprise. La fonctionnalité de Détection de portail captif (CPD) est indissociable du Mode filtrant. Elle est donc ajoutée en même temps que ce dernier.

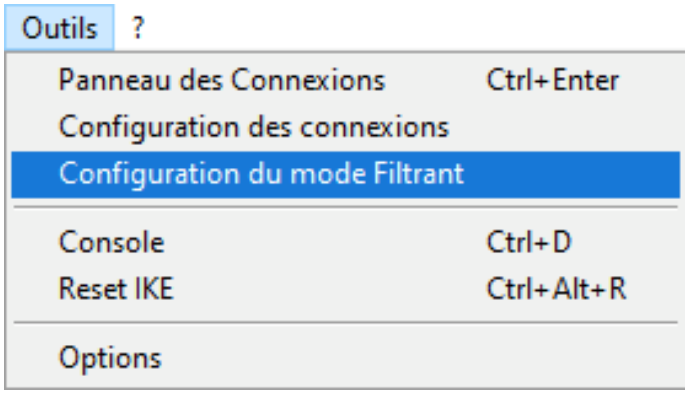
Si vous avez déjà installé le Client VPN Windows Enterprise, vous devez le désinstaller puis le réinstaller pour ajouter cette fonctionnalité.

L'ajout du Mode filtrant peut se faire de deux manières :

- soit en passant une propriété de l'installeur MSI en ligne de commande,
- soit en ajoutant une entrée dans le fichier `vpnsetup.ini`.

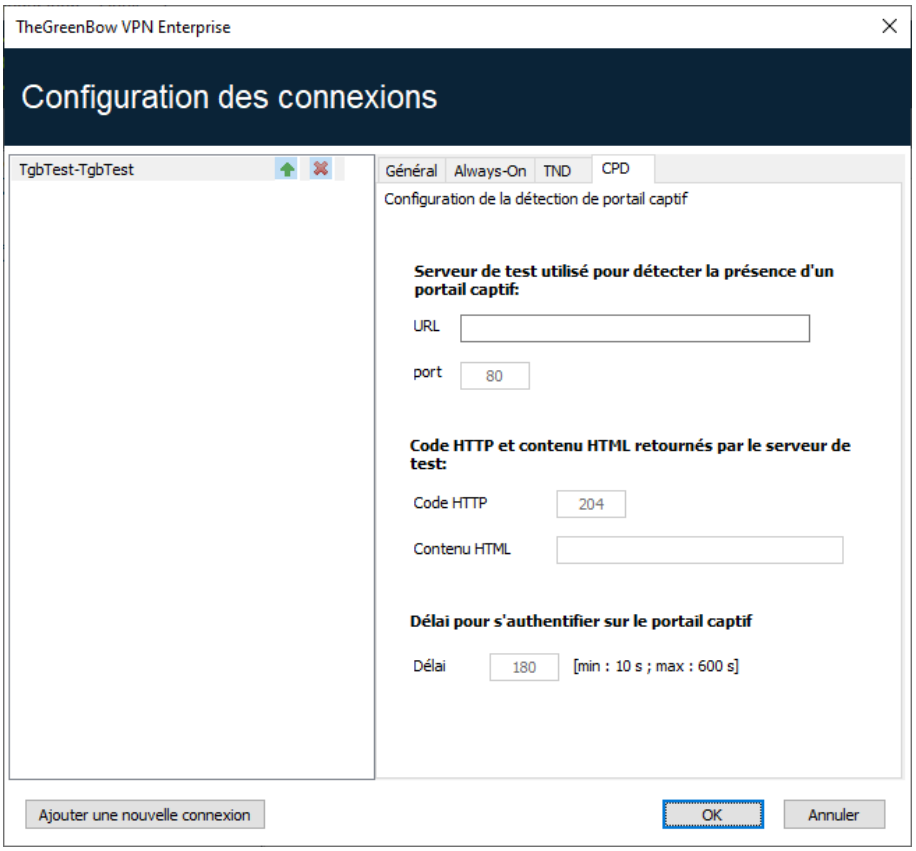
☞ Pour plus de détails sur l'utilisation des propriétés de l'installeur MSI et l'ajout d'une entrée dans le fichier `vpnsetup.ini`, reportez-vous au Guide de déploiement du Client VPN Windows Enterprise.

L'ajout de la fonctionnalité Mode filtrant et CPD lors de l'installation fait apparaître une entrée supplémentaire dans le menu **Outils**, appelée **Configuration du mode Filtrant** :



☞ Voir le chapitre 3 Configuration du Mode filtrant pour savoir comment configurer le Mode filtrant.

De plus, un onglet **CPD** vient s'ajouter à la fenêtre de **Configuration des Connexions** et se présente comme suit :



☞ Voir le chapitre 4 Configuration de la Détection de portail captif pour savoir comment configurer la Détection de portail captif.

2.2 Propriété NETPARAMS de l'installeur MSI

La propriété de l'installeur MSI à passer en ligne de commande pour ajouter le Mode filtrant et la Détection de portail captif s'appelle `NETPARAMS`. Étant donné que le Mode filtrant s'utilise uniquement avec le **Panneau TrustedConnect**, il convient de passer cette propriété avec la propriété `USEDIALERBYDEFAULT` qui lance le **Panneau TrustedConnect** automatiquement au démarrage de la session Windows.

La propriété `NETPARAMS` s'utilise de la même manière que les autres propriétés décrites dans le Guide de déploiement du Client VPN Windows Enterprise et peut être associée à ces dernières.

Le tableau suivant récapitule la syntaxe à respecter et l'usage de la propriété :

Syntaxe :	`NETPARAMS=1`
Usage :	Cette propriété permet d'ajouter la fonctionnalité spécifique Mode filtrant. Elle doit obligatoirement être utilisée avec la propriété `USEDIALERBYDEFAULT`. Elle ajoute en outre l'option **Configuration du mode Filtrant** au menu **Outils** du **Panneau de Configuration**, ainsi que l'onglet **CPD** à la fenêtre de **Configuration des Connexions**.
Exemple :	`msiexec /i "[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi" USEDIALERBYDEFAULT=1 NETPARAMS=1`

2.3 Propriété IKESTART de l'installeur MSI

La propriété de l'installeur MSI à passer en ligne de commande pour ajouter le Mode filtrant restreint et permanent s'appelle `IKESTART`.

Elle s'utilise de la même manière que les autres propriétés décrites dans le Guide de déploiement du Client VPN Windows Enterprise et peut être associée à ces dernières.

Syntaxe :	`IKESTART=1`
Usage :	Cette propriété permet d'ajouter un Mode filtrant restreint et permanent. Elle doit obligatoirement être utilisée avec les propriétés `USEDIALERBYDEFAULT` et `NETPARAMS`.
Exemple :	`msiexec /i "[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi" USEDIALERBYDEFAULT=1 NETPARAMS=1 IKESTART=1`

Le fait que le contexte `RESTRICTED` soit appliqué lorsque le **Panneau TrustedConnect** n'est pas en cours d'exécution est une fonction configurable par une propriété de l'installeur MSI ou un paramètre dans le fichier d'installation `vpnsetup.ini`. Il convient donc de faire ce choix lors de l'installation (cf. chapitre 5 Contextes et états du Panneau TrustedConnect).

2.4 Fichier vpnsetup.ini

L'ajout du Mode filtrant peut être configuré dans le fichier `vpnsetup.ini` qui accompagne l'installeur du Client VPN Windows Enterprise.

Pour cela, il suffit de définir le paramètre `UseDialerByDefault` dans la section `[Dialer]` ainsi que le paramètre `NetParams` et, le cas échéant, le

paramètre `IkeStart` dans la section `[AddRegKey]` du fichier `vpnsetup.ini` de la façon suivante :

```
[Dialer]
UseDialerByDefault=1

[AddRegKey]
NetParams=1
IkeStart=1
```

☞ Se reporter au Guide de déploiement du Client VPN Windows Enterprise pour plus de détails sur le fichier `vpnsetup.ini`.

2.5 Retrait du Mode filtrant

Pour retirer le Mode filtrant du Client VPN Windows Enterprise et ne plus afficher l'option **Configuration du mode Filtrant** du menu **Outils**, il convient de désinstaller le logiciel et de le réinstaller sans cette fonctionnalité avancée.

3 Configuration du Mode filtrant

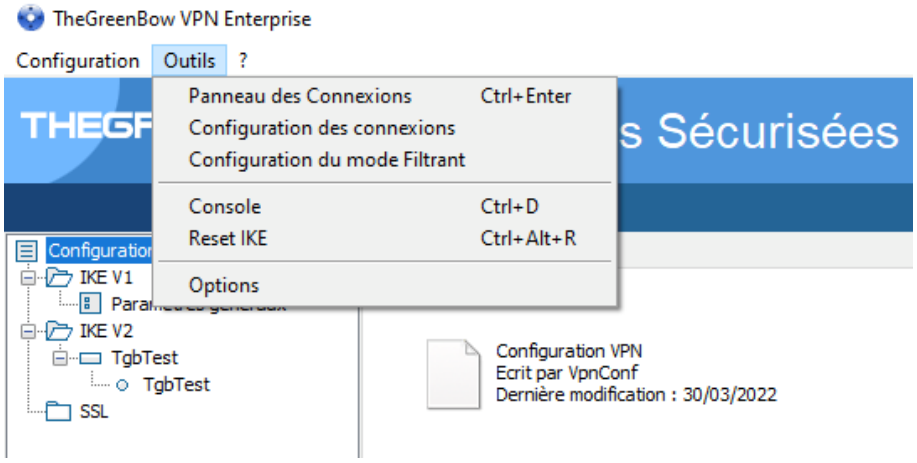
3.1 Introduction

La configuration du Mode filtrant est contenue dans le fichier de configuration VPN. Elle bénéficie ainsi des mécanismes de protection de ce fichier (chiffrement, authenticité et intégrité), et bénéficie aussi des facilités de déploiement et/ou de modification à distance.

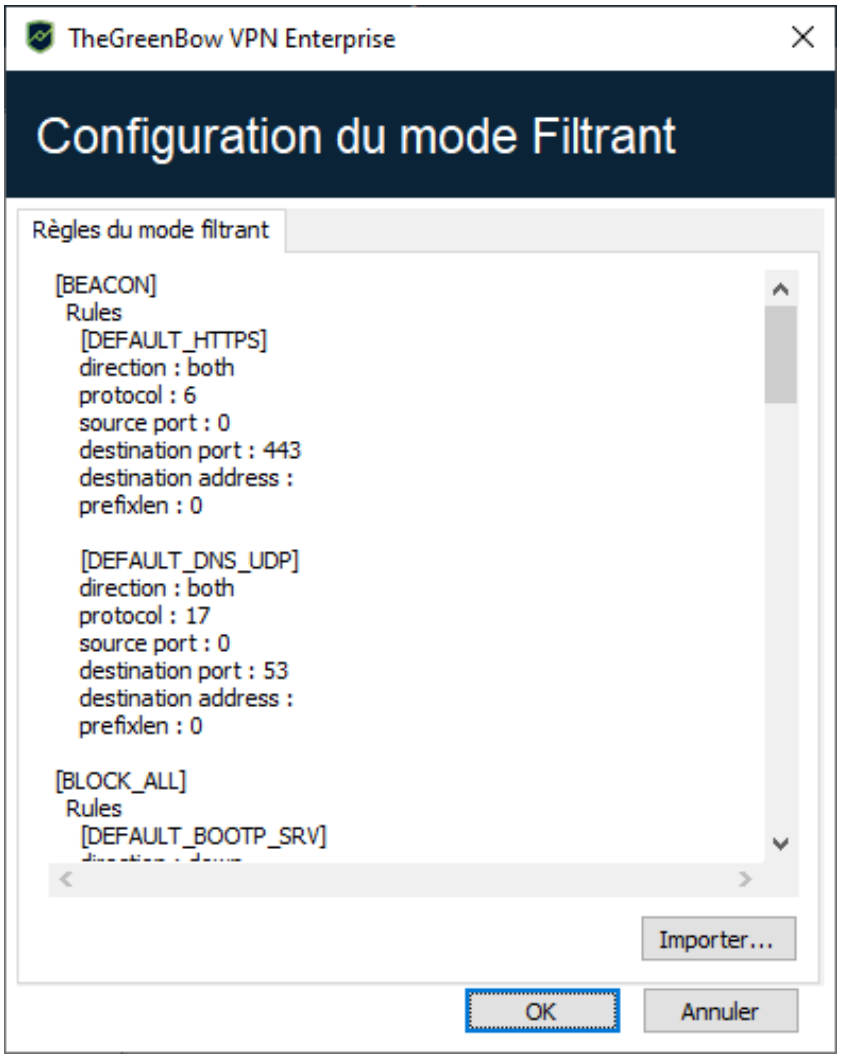
La configuration du Mode filtrant s'effectue ainsi via les étapes suivantes :

1. Rédaction des règles de filtrage dans un fichier texte (cf. section 6.2 Exemple de fichier de règles du Mode filtrant dans l'annexe).
2. Import de ce fichier texte dans la configuration VPN (la cohérence syntaxique de ce fichier est vérifiée au moment de l'import, cf. section 3.3 Vérification de la configuration importée ci-dessous).

L'import du fichier de configuration des règles de filtrage est proposé dans la fenêtre de **Configuration du mode Filtrant** accessible par le menu **Outils** > **Configuration du mode Filtrant** du **Panneau de Configuration** du Client VPN Windows Enterprise.



La fenêtre de **Configuration du mode Filtrant** se présente comme suit :



La dernière version du Client VPN Windows Enterprise permet de configurer tous les filtres de chaque état du **Panneau TrustedConnect**.

Dans la suite de ce document, les termes « contexte » et « filtre » signifient la même chose. Un contexte est un groupe de règles.

3.2 Format du fichier de configuration des règles du Mode filtrant

Le fichier de configuration des règles du Mode filtrant est un fichier XML constitué de deux sections principales :

1. la définition de toutes les règles de filtrage,
2. la définition des contextes.

La syntaxe d'un fichier de configuration des règles est la suivante :

```
<filter_mode>
     <rules>
          <rule ...>règle 1</rule>
          <rule ...>règle 2</rule>
          <rule ...>règle 3</rule>
     </rules>
     <ruleset>
          <block_all>contexte block_all</block_all>
          <beacon>contexte beacon</beacon>
          <cpd>contexte cpd</cpd>
          <service_flows>contexte
service_flows</service_flows>
     </ruleset>
</filtermode>
```

La syntaxe d'une règle est la suivante :

```
<rule name="DNS_UDP" direction = "DOWN">
     <protocol>17</protocol>
     <src_port>ALL</src_port>
     <dst_port>53</dst_port>
     <dst_addr>ALL</dst_addr>
     <prefix_len>0</prefix_len>
</rule>
```

Les paramètres du fichier de configuration des règles du Mode filtrant sont les suivants :

`name`	Chaîne de caractères libre, sans espace, à l'exclusion de `DYN_RULES` qui est réservé à TheGreenBow
`direction`	`BOTH`, `DOWN` ou `UP` : direction du point de vue du poste de travail
`protocol`	Entier parmi la liste suivante : 0, 1, 6, 17, 50 (respectivement : all, ICMP, TCP, UDP, ESP)
`src_port`, `dst_port`[1]	Entier compris entre 0 et 65535 0 ou `ALL` signifient « tous les ports »
`icmp_code`[2]	Entier compris entre 0 et 15 ou mot clé `ALL` qui signifie « tous les codes ICMP »

[1] `src_port` et `dst_port` doivent obligatoirement être spécifiés si `protocol` est différent de 1 (ICMP)
[2] `icmp_code` doit obligatoirement être spécifié si `protocol` est égal à 1 (ICMP)

`icmp_type`[1]	Entier compris entre 0 et 18 ou mot clé `ALL` qui signifie « tous les types ICMP »
`dst_addr`	Peut prendre l'une des valeurs suivantes : • une adresse IPv4 en notation décimale pointée, • une URI (ex. : www.thegreenbow.com), • 0 ou `ALL` qui signifient « toutes les adresses IP autorisées ».
`prefix_len`	Définit le masque réseau. Si `dst_addr` est de type IPv4 : entier compris entre 0 et 32. Si `dst_addr` est de type URI, la valeur de `prefix_len` n'est pas utilisée, `prefix_len` est calculé dynamiquement.

La syntaxe d'un contexte est la suivante :

```
<block_all>
     <rule_add>BOOTP_SRV</rule_add>
     <rule_add>BOOTP_CLIENT</rule_add>
     <rule_add>DNS_UDP</rule_add>
     <rule_add>DNS_TCP</rule_add>
     <rule_add>ICMP</rule_add>
</block_all>
```

Les contextes suivants sont configurables :

- `BLOCK_ALL`,
- `BEACON`,
- `CPD`,
- `SERVICE_FLOWS`.

Les contextes suivants ne sont pas configurables :

- `RESTRICTED` si le client VPN est installé avec `IKESTART=1`,
- `ALLOW_ALL` si le mode filtrant n'est pas actif.

⚠ Dès qu'au moins une règle de filtrage est indiquée dans un contexte donné, elle annule et remplace toutes les règles par défaut de ce contexte.

[1] `icmp_type` doit obligatoirement être spécifié si `protocol` est égal à 1 (ICMP)

⚠ Il est fortement recommandé d'activer les deux protocoles DNS et DHCP dans les contextes `BLOCK_ALL` et `SERVICE_FLOWS`.

3.3 Vérification de la configuration importée

La cohérence syntaxique de la configuration du Mode filtrant est vérifiée au moment où elle est importée.

Si une erreur est détectée, elle est affichée dans la fenêtre de **Configuration du mode Filtrant**.

Les cohérences syntaxiques vérifiées au moment de l'import de la configuration du Mode Filtrant sont les suivantes :

- aucun contexte ne contient plus de 30 règles ;
- les noms des contextes sont :
  - `BLOCK_ALL`,
  - `BEACON`,
  - `CPD` ou
  - `SERVICE_FLOWS` ;
- chaque contexte n'est défini qu'une seule fois (il n'y a pas deux contextes portant le même nom) ;
- chaque contexte contient au moins une règle ;
- toute règle spécifiée dans un contexte existe dans la liste des règles définies ;
- les champs `name`, `direction`, `protocol`, `dst_addr` sont spécifiés et non vides ;
- si `protocol = 1` (ICMP) les champs `icmp_code` et `icmp_type` sont spécifiés et non vides ;
- si `protocol` est différent de 1 (ICMP), les champs `dst_port` et `src_port` sont spécifiés et non vides ;
- le champ `prefix_len` est spécifié, si le champ `dst_addr` est une adresse IP ;
- si le champ `dst_addr` est un URI, le champ `prefix_len` est supprimé ;
- le format de `dst_addr` (adresse IPv4 ou URI) est correct ;
- la valeur de `prefix_len` est cohérente avec la famille de l'adresse IP :
  - si `dst_addr` est de type IPv4, `prefix_len` est compris entre 0 et 32 ;
  - si `dst_addr` est à `0` ou `ALL`, `prefix_len` n'est pas pris en compte ;
- `direction` est l'une des trois valeurs : `DOWN`, `UP` ou `BOTH` ;
- `protocol` est l'une des valeurs suivantes : 0, 1, 6, 17, 50 (respectivement : all, ICMP, TCP, UDP, ESP) ;

- les ports destination et source sont un entier compris entre 0 et 65535 ou le mot-clé `ALL` ;
- la valeur de `icmp_code` est un entier compris entre 0 et 15 ou le mot-clé `ALL` ;
- la valeur de `icmp_type` est un entier compris entre 0 et 18 ou le mot-clé `ALL`.

3.4 Réinitialisation du Mode filtrant

TheGreenBow fournit à titre d'exemple le fichier de configuration du Mode filtrant par défaut (cf. section 6.1 Règles de filtrage par défaut du Mode filtrant dans l'annexe).

La configuration par défaut du Mode filtrant peut être réinitialisée en important un fichier de configuration « vide ».

Un fichier de configuration « vide » doit respecter la syntaxe suivante :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<tgbconfig>
     <dialer_params>
          <filter_mode>
          </filter_mode>
     </dialer_params>
</tgbconfig>
```

3.5 Limitations actuelles

Les contextes `ALLOW_ALL` et `RESTRICTED` ne sont pas configurables.

Un contexte peut contenir au maximum 30 règles.

Lorsque le **Panneau TrustedConnect** n'est pas actif (avant d'avoir démarré ou après avoir été arrêté le logiciel), s'il est appliqué (`IKESTART=1`), le contexte `RESTRICTED` n'est pas configurable (et autorise uniquement DHCP, DNS/UDP, DNS/TCP).

Le protocole IPv6 n'est pas encore pris en charge.

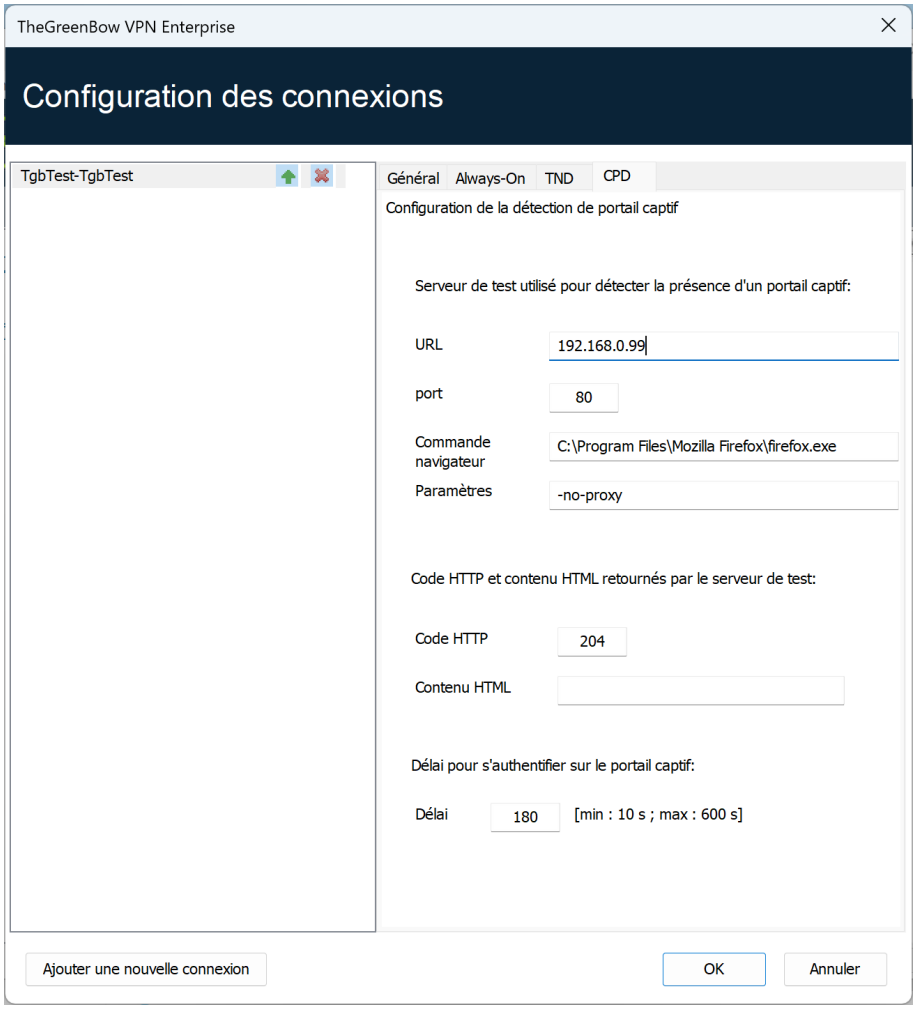
4 Configuration de la Détection de portail captif

La configuration de la Détection de portail captif s'effectue dans l'onglet **CPD** de la fenêtre de **Configuration des Connexions**.

Pour accéder à l'onglet **CPD**, sélectionnez l'option de menu **Outils** > **Configuration des connexions**, puis sélectionnez l'onglet **CPD**.

4.1 Onglet CPD de la fenêtre Configuration des Connexions

L'onglet **CPD** de la fenêtre de **Configuration des Connexions** se présente comme suit :



Son utilisation est simple et intuitive :

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.

Commande navigateur	Facultatif : chemin vers le navigateur à utiliser pour la détection, si le navigateur par défaut ne doit pas être utilisé
Paramètres	Facultatif : paramètres à indiquer au navigateur lors de son lancement
Code 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 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

4.2 Entrées de journalisation associées à la Détection de portail captif

Les entrées de journalisation suivantes relatives à la fonctionnalité de Détection de portail captif peuvent s'afficher dans la **Console** :

Workstation is behind a captive portal	Indique que le poste de travail est derrière un portail captif.
Workstation is not behind a captive portal	Indique que le poste de travail n'est pas derrière un portail captif.
Captive portal login timeout	Indique que le portail captif n'a pas été ouvert dans les 3 minutes (valeur par défaut) suivant la détection.

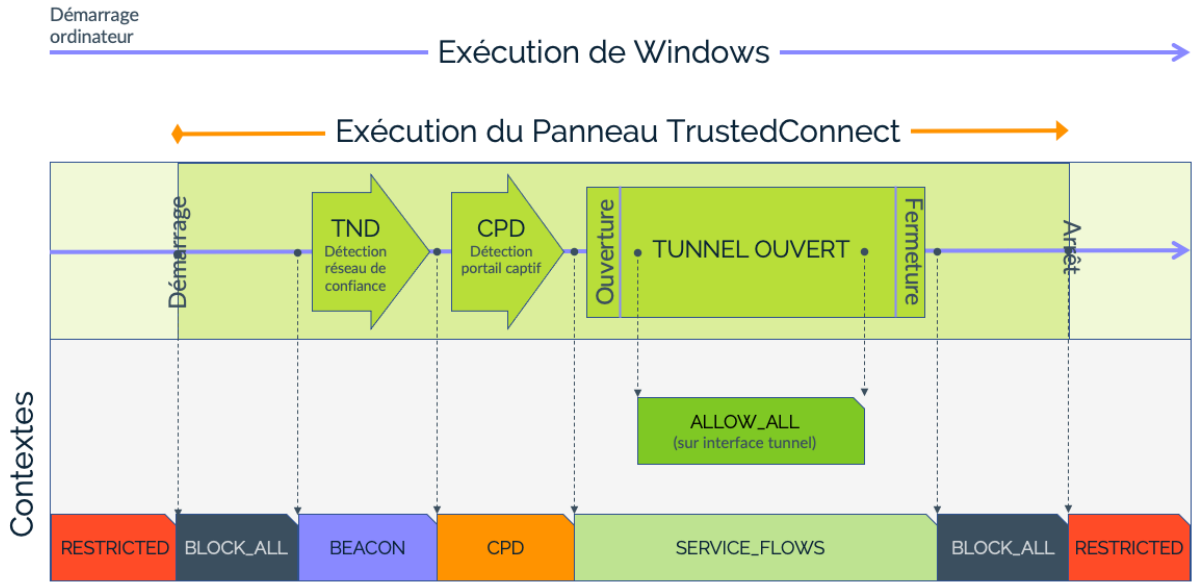
☞ Pour savoir comment afficher la **Console**, reportez-vous au Guide de l'administrateur du Client VPN Windows Enterprise.

5 Contextes et états du Panneau TrustedConnect

5.1 Introduction

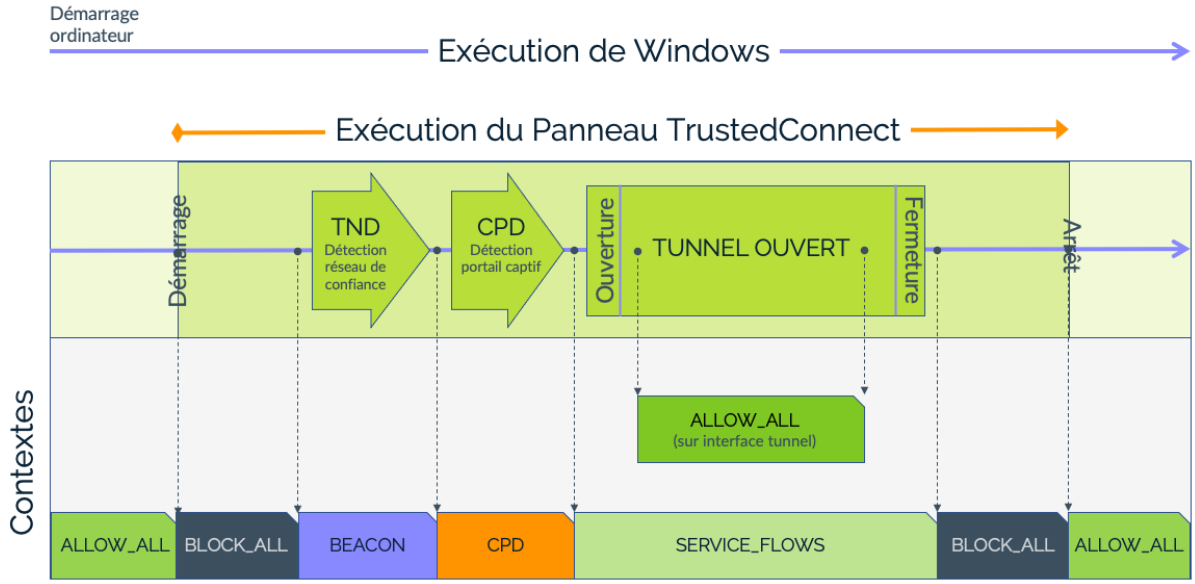
Les schémas ci-dessous représentent les différents états possibles du **Panneau TrustedConnect** et les contextes associés à ces différents états.

Si les propriétés `NETPARAMS=1` et `IKESTART=1` ont été configurées, le Mode filtrant restreint et permanent est actif depuis le démarrage du poste jusqu'à son arrêt, y compris pendant les périodes de mise en veille.



Autrement, si seule la propriété `NETPARAMS=1` a été configurée, le Mode filtrant n'est actif que lorsque le Client VPN est ouvert.

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 (cf. « Guide de déploiement »), l'utilisateur peut choisir la connexion après avoir fermé le tunnel (cf. « Guide de l'administrateur »).



5.2 Contexte BLOCK_ALL

Le contexte `BLOCK_ALL` est appliqué sur toutes les interfaces réseau tant que le **Panneau TrustedConnect** n'a pas démarré la détection du réseau de confiance (TND), dès que le tunnel est fermé ou si le tunnel est en erreur.

Pour bloquer tout trafic lorsque le **Panneau TrustedConnect** n'est pas en cours d'exécution, il convient d'utiliser le contexte `RESTRICTED` (cf. section 5.7 Contexte RESTRICTED).

5.3 Contexte BEACON

Le contexte `BEACON` est appliqué au moment où le **Panneau TrustedConnect** exécute le mécanisme TND.

Il est appliqué tour à tour sur chaque interface réseau dont le suffixe DNS est considéré de confiance.

5.4 Contexte CPD

Le contexte `CPD` est appliqué lorsque le **Panneau TrustedConnect**, après avoir détecté que le poste n'est pas connecté au réseau de confiance, exécute le mécanisme de détection de portail captif.

Le contexte `CPD` est appliqué à l'interface utilisée pour ouvrir la connexion VPN.

Le contexte `CPD` reste appliqué pendant un maximum de 3 minutes (laps de temps par défaut donné à l'utilisateur pour s'authentifier).

Dès que l'utilisateur s'est authentifié, le **Panneau TrustedConnect** ouvre la connexion VPN et applique les contextes `SERVICE_FLOWS` et `ALLOW_ALL` (cf. ci-dessous) aux interfaces réseau concernées.

À l'inverse, si l'utilisateur ne s'est pas authentifié à la fin des 3 minutes (valeur par défaut), le **Panneau TrustedConnect** applique le contexte `BLOCK_ALL`.

5.5 Contexte SERVICE_FLOWS

Le contexte `SERVICE_FLOWS` est appliqué à l'interface réseau utilisée pour établir et maintenir la connexion VPN.

Le contexte est constitué des règles de filtrages qui autorisent les protocoles nécessaires à l'ouverture de la connexion VPN (ISAKMP, ESP, etc.) et également nécessaires à son maintien (DHCP, DNS, par exemple).

Le contexte `SERVICE_FLOWS` s'applique à l'interface réseau physique sur laquelle est ouverte la connexion VPN.

5.6 Contexte ALLOW_ALL

Le contexte `ALLOW_ALL` est appliqué à l'interface réseau connectée au réseau de confiance.

Cette interface réseau peut être soit une interface physique lorsque le poste est connecté directement sur le réseau de confiance (en Ethernet, par exemple), soit une interface virtuelle lorsque le poste est connecté au réseau de confiance au travers de la connexion VPN.

Ce contexte autorise tous les flux sur l'interface réseau concernée.

Ce contexte peut aussi être appliqué à une interface réseau (physique ou virtuelle) que l'administrateur a décidé d'exclure des interfaces traitées par le **Panneau TrustedConnect**. Ce traitement spécifique est configurable à l'installation comme décrit dans la section dédiée à la fonction Always-On dans le Guide de l'administrateur du Client VPN Windows Enterprise.

Ce contexte n'est pas configurable (cf. section 3.5 Limitations actuelles ci-dessus).

5.7 Contexte RESTRICTED

Le contexte `RESTRICTED` est appliqué à toutes les interfaces réseau tant que le **Panneau TrustedConnect** n'est pas lancé, et dès qu'il est quitté.

Les règles de filtrage actives dans ce contexte sont les suivantes :

- DHCP :
  - DEFAULT_BOOTP_SRV
  - DEFAULT_BOOTP_CLIENT
- DNS :
  - DEFAULT_DNS_UDP
  - DEFAULT_DNS_TCP

⚠ Ce contexte n'est disponible que si la propriété `IKESTART=1` a été configurée lors de l'installation du logiciel (cf. section 2.3 Propriété IKESTART de l'installeur MSI ci-dessus).

ℹ Ce contexte n'est pas configurable (cf. section 3.5 Limitations actuelles ci-dessus).

5.8 Règles de filtrage par défaut

Par défaut (lorsqu'aucune règle de filtrage spécifique n'est configurée), le Mode filtrant est constitué des règles de filtrage suivantes :

Contexte	Règles par défaut
BLOCK_ALL	Autorise uniquement DHCP, DNS/UDP
BEACON	Autorise uniquement HTTPS, DNS/UDP, DNS/TCP
CPD	Autorise uniquement HTTP, HTTPS, DNS/UDP, DNS/TCP
SERVICE_FLOWS	Autorise uniquement DHCP, DNS/UDP, DNS/TCP, ISAKMP, ESP, ESP/NAT-T, HTTPS
ALLOW_ALL	Autorise tous les flux
Si IKESTART=1	
RESTRICTED	Autorise uniquement DHCP, DNS/UDP, DNS/TCP

6 Annexe

6.1 Règles de filtrage par défaut du Mode filtrant

Les règles de filtrage par défaut du Mode filtrant sont reproduites ci-dessous :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<tgbconfig>
  <dialer_params>
    <filter_mode>
    <rules>
      <rule name="DEFAULT_HTTPS" direction="BOTH">
        <protocol>6</protocol>
        <src_port>ALL</src_port>
        <dst_port>ALL</dst_port>
     <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_DNS_UDP" direction="BOTH">
        <protocol>17</protocol>
        <src_port>ALL</src_port>
        <dst_port>53</dst_port>
     <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_BOOTP_SRV" direction="DOWN">
        <protocol>17</protocol>
        <src_port>ALL</src_port>
        <dst_port>67</dst_port>
     <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_BOOTP_CLIENT" direction="UP">
        <protocol>17</protocol>
        <src_port>68</src_port>
        <dst_port>0</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_HTTP" direction="BOTH">
        <protocol>6</protocol>
        <src_port>ALL</src_port>
        <dst_port>80</dst_port>
        <dst_addr>ALL</dst_addr>
      </rule>
      <rule name="DEFAULT_ISAKMP" direction="BOTH">
        <protocol>17</protocol>
        <src_port>ALL</src_port>
        <dst_port>500</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
```

```
      <rule name="DEFAULT_ESP" direction="BOTH">
        <protocol>50</protocol>
        <src_port>ALL</src_port>
        <dst_port>ALL</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_ESP_NATT" direction="BOTH">
        <protocol>17</protocol>
        <src_port>ALL</src_port>
        <dst_port>4500</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
    </rules>
    <rulesets>
      <block_all>
        <rule_add>DEFAULT_BOOTP_SRV</rule_add>
        <rule_add>DEFAULT_BOOTP_CLIENT</rule_add>
        <rule_add>DEFAULT_DNS_UDP</rule_add>
      </block_all>
      <beacon>
        <rule_add>DEFAULT_HTTPS</rule_add>
        <rule_add>DEFAULT_DNS_UDP</rule_add>
      </beacon>
      <cpd>
        <rule_add>DEFAULT_HTTP</rule_add>
        <rule_add>DEFAULT_DNS_UDP</rule_add>
      </cpd>
      <service_flows>
        <rule_add>DEFAULT_BOOTP_SRV</rule_add>
        <rule_add>DEFAULT_BOOTP_CLIENT</rule_add>
        <rule_add>DEFAULT_DNS_UDP</rule_add>
        <rule_add>DEFAULT_ISAKMP</rule_add>
        <rule_add>DEFAULT_ESP</rule_add>
        <rule_add>DEFAULT_ESP_NATT</rule_add>
      </service_flows>
    </rulesets>
  </filter_mode>
  </dialer_params>
</tgbconfig>
```

6.2 Exemple de fichier de règles du Mode filtrant

Cet exemple de fichier comporte les règles suivantes :

- La règle `BEACON` sert à autoriser la détection du réseau de confiance en utilisant le protocole TCP vers le port de destination 443 et l'adresse IP de destination `www.thegreenbow.com` quel que soit le port source :
  - `protocol` : 6
  - `src_port` : ALL
  - `dst_port` : 443
  - `dst_addr` : www.thegreenbow.com
- La règle `CPDWEB` sert à autoriser la détection du portail captif en utilisant le protocole TCP vers le port de destination 80 et l'adresse IP de destination `detectportal.firefox.com` quel que soit le port source :
  - `protocol` : 6
  - `src_port` : 0
  - `dst_port` : 80
  - `dst_addr` : detectportal.firefox.com
- La règle `BOOTP_SRV` sert à autoriser le protocole UDP vers le serveur sur le port de destination 67 quel que soit le port source et l'adresse IP de destination afin de permettre l'utilisation du protocole DHCP :
  - `protocol` : 17
  - `src_port` : 0
  - `dst_port` : 67
  - `dst_addr` : 0
- La règle `BOOTP_CLIENT` sert à autoriser le protocole UDP venant du serveur vers le port source 68 quel que soit le port de destination et l'adresse IP de destination afin de permettre l'utilisation du protocole DHCP :
  - `protocol` : 17
  - `src_port` : 68
  - `dst_port` : 0
  - `dst_addr` : 0
- La règle `DNS_UDP` sert à autoriser le protocole UDP vers le port de destination 53 quel que soit le port source et l'adresses IP de destination afin de permettre l'utilisation du service DNS :
  - `protocol` : 17
  - `src_port` : 0
  - `dst_port` : 53
  - `dst_addr` : 0

- La règle `DNS_TCP` sert à autoriser le protocole TCP vers le port de destination 53 quel que soit le port source et l'adresses IP de destination afin de permettre l'utilisation du service DNS :
  - `protocol` : 6
  - `src_port` : 0
  - `dst_port` : 53
  - `dst_addr` : 0
- La règle `ICMP` sert à autoriser tous les codes ICMP pour tous les types ICMP sur toutes les adresses de destination afin de permettre le ping :
  - `icmp_type` : ALL
  - `icmp_code` : ALL
  - `dst_addr` : ALL
- La règle `CRLOCSP_TCP` sert à autoriser le protocole TCP vers le port de destination 80 et l'adresse IP de destination `ocsp.sectigo.com` quel que soit le port source afin de permettre l'interfaçage avec OSCP :
  - `protocol` : 6
  - `src_port` : 0
  - `dst_port` : 80
  - `dst_addr` : ocsp.sectigo.com
- La règle `NETBIOS_NAME` sert à autoriser le protocole UDP vers le port de destination 137 quel que soit le port source et l'adresse IP de destination afin de permettre la résolution de noms de machines via NetBIOS :
  - `protocol` : 17
  - `src_port` : 0
  - `dst_port` : 137
  - `dst_addr` : 0
- La règle `NETBIOS_DGRAM` sert à autoriser le protocole UDP vers le port de destination 138 quel que soit le port source et l'adresse IP de destination afin de permettre l'utilisation du protocole NetBIOS (partage de fichiers, imprimantes, etc. sous Windows) :
  - `protocol` : 17
  - `src_port` : 0
  - `dst_port` : 138
  - `dst_addr` : 0

- La règle `HTTPS` sert à autoriser le protocole TCP vers le port de destination 443 quel que soit le port source et l'adresse IP de destination afin de permettre la navigation web en mode sécurisé :
  - `protocol` : 6
  - `src_port` : ALL
  - `dst_port` : 443
  - `dst_addr` : ALL
- La règle `HTTP` sert à autoriser le protocole TCP vers le port de destination 443 quel que soit le port source et l'adresse IP de destination afin de permettre la navigation web en mode non sécurisé :
  - `protocol` : 6
  - `src_port` : ALL
  - `dst_port` : 443
  - `dst_addr` : ALL
- La règle `ISAKMP` sert à autoriser le protocole UDP à partir du port source 500 vers le port de destination 500 et l'adresse IP de destination `tgbtest.dyndns.org` afin de permettre l'établissement d'un tunnel IPsec :
  - `protocol` : 17
  - `src_port` : 500
  - `dst_port` : 500
  - `dst_addr` : tgbtest.dyndns.org
- La règle `ESP` sert à autoriser le protocole ESP vers tous les ports de destination quel que soit le port source et l'adresse IP de destination afin de permettre l'établissement d'un tunnel IPsec :
  - `protocol` : 50
  - `src_port` : ALL
  - `dst_port` : ALL
  - `dst_addr` : 0
- La règle `ESP-NATT` sert à autoriser le protocole UDP à partir du port source 4500 vers le port de destination 4500 et l'adresse IP de destination `tgbtest.dyndns.org` afin de permettre l'établissement d'un tunnel IPsec :
  - `protocol` : 17
  - `src_port` : 4500
  - `dst_port` : 4500
  - `dst_addr` : tgbtest.dyndns.org

Ces règles sont utilisées de la manière suivante dans les différents contextes :

- Le contexte `BLOCK_ALL` bloque toutes les communications autres que celles répondant aux règles définies ici tant que le **Panneau TrustedConnect** n'est pas lancé et dès qu'il est quitté :
  - `BOOTP_SRV`
  - `BOOTP_CLIENT`
  - `DNS_UDP`
  - `DNS_TCP`
  - `ICMP`
- Le contexte `BEACON` autorise toutes les communications répondant aux règles suivantes pour permettre la détection du réseau de confiance :
  - `DNS_UDP`
  - `DNS_TCP`
  - `BEACON`
  - `CRLOCSP_TCP`
- Le contexte `CPD` autorise toutes les communications répondant aux règles suivantes pour permettre la détection du portail captif :
  - `DNS_UDP`
  - `DNS_TCP`
  - `CPDWEB`
  - `HTTPS`
- Le contexte `SERVICE_FLOWS` autorise toutes les communications répondant aux règles suivantes pour permettre d'établir la connexion VPN :
  - `BOOTP_SRV`
  - `BOOTP_CLIENT`
  - `DNS_UDP`
  - `DNS_TCP`
  - `ISAKMP`
  - `ESP`
  - `ESP-NATT`

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<tgbconfig>
  <dialer_params>
    <filter_mode>
      <rules>
        <rule name="BEACON" direction="BOTH">
          <protocol>6</protocol>
          <src_port>ALL</src_port>
          <dst_port>443</dst_port>
          <dst_addr>www.thegreenbow.com</dst_addr>
        </rule>
        <rule name="CPDWEB" direction="BOTH">
          <protocol>6</protocol>
          <src_port>0</src_port>
          <dst_port>80</dst_port>
          <dst_addr>detectportal.firefox.com</dst_addr>
        </rule>
        <rule name="BOOTP_SRV" direction="DOWN">
          <protocol>17</protocol>
          <src_port>0</src_port>
          <dst_port>67</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="BOOTP_CLIENT" direction="UP">
          <protocol>17</protocol>
          <src_port>68</src_port>
          <dst_port>0</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="DNS_UDP" direction="BOTH">
          <protocol>17</protocol>
          <src_port>0</src_port>
          <dst_port>53</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="DNS_TCP" direction="BOTH">
          <protocol>6</protocol>
          <src_port>0</src_port>
          <dst_port>53</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="ICMP" direction="BOTH">
          <protocol>1</protocol>
          <icmp_type>ALL</icmp_type>
          <icmp_code>ALL</icmp_code>
          <dst_addr>ALL</dst_addr>
        </rule>
```

```
    <rule name="CRLOCSP_TCP" direction="BOTH">
      <protocol>6</protocol>
      <src_port>0</src_port>
      <dst_port>80</dst_port>
      <dst_addr>ocsp.sectigo.com</dst_addr>
    </rule>
    <rule name="NETBIOS_NAME" direction="BOTH">
      <protocol>17</protocol>
      <src_port>0</src_port>
      <dst_port>137</dst_port>
      <dst_addr>0</dst_addr>
    </rule>
    <rule name="NETBIOS_DGRAM" direction="BOTH">
      <protocol>17</protocol>
      <src_port>0</src_port>
      <dst_port>138</dst_port>
      <dst_addr>0</dst_addr>
    </rule>
    <rule name="HTTPS" direction="BOTH">
      <protocol>6</protocol>
      <src_port>ALL</src_port>
      <dst_port>443</dst_port>
      <dst_addr>ALL</dst_addr>
    </rule>
    <rule name="HTTP" direction="BOTH">
      <protocol>6</protocol>
      <src_port>ALL</src_port>
      <dst_port>80</dst_port>
      <dst_addr>ALL</dst_addr>
    </rule>
    <rule name="ISAKMP" direction="BOTH">
      <protocol>17</protocol>
      <src_port>500</src_port>
      <dst_port>500</dst_port>
      <dst_addr>tgbtest.dyndns.org</dst_addr>
    </rule>
    <rule name="ESP" direction="BOTH">
      <protocol>50</protocol>
      <src_port>ALL</src_port>
      <dst_port>ALL</dst_port>
      <dst_addr>0</dst_addr>
    </rule>
    <rule name="ESP-NATT" direction="BOTH">
      <protocol>17</protocol>
      <src_port>4500</src_port>
      <dst_port>4500</dst_port>
      <dst_addr>tgbtest.dyndns.org</dst_addr>
    </rule>
  </rules>
```

```
      <rulesets>
        <block_all>
          <rule_add>BOOTP_SRV</rule_add>
          <rule_add>BOOTP_CLIENT</rule_add>
          <rule_add>DNS_UDP</rule_add>
          <rule_add>DNS_TCP</rule_add>
          <rule_add>ICMP</rule_add>
        </block_all>
        <beacon>
          <rule_add>DNS_UDP</rule_add>
          <rule_add>DNS_TCP</rule_add>
          <rule_add>BEACON</rule_add>
          <rule_add>CRLOCSP_TCP</rule_add>
        </beacon>
        <cpd>
          <rule_add>DNS_UDP</rule_add>
          <rule_add>DNS_TCP</rule_add>
          <rule_add>CPDWEB</rule_add>
          <rule_add>HTTPS</rule_add>
        </cpd>
        <service_flows>
          <rule_add>BOOTP_SRV</rule_add>
          <rule_add>BOOTP_CLIENT</rule_add>
          <rule_add>DNS_UDP</rule_add>
          <rule_add>DNS_TCP</rule_add>
          <rule_add>ISAKMP</rule_add>
          <rule_add>ESP</rule_add>
          <rule_add>ESP-NATT</rule_add>
        </service_flows>
      </rulesets>
    </filter_mode>
  </dialer_params>
</tgbconfig>
```

6.3 Exemple de fichier de règles du Mode filtrant : Windows Remote Desktop

Cet exemple reprend les règles par défaut. Les modifications à apporter pour le faire fonctionner avec Windows Remote Desktop figurent en orange.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<tgbconfig>
  <dialer_params>
    <filter_mode>
      <rules>
        <rule name="RDP_SRV_TCP" direction="BOTH">
          <protocol>6</protocol>
          <src_port>3389</src_port>
          <dst_port>0</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="RDP_SRV_UDP" direction="BOTH">
          <protocol>17</protocol>
          <src_port>3389</src_port>
          <dst_port>0</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="DEFAULT_BOOTP_SRV"
direction="DOWN">
          <protocol>17</protocol>
          <src_port>0</src_port>
          <dst_port>67</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="DEFAULT_BOOTP_CLIENT"
direction="UP">
          <protocol>17</protocol>
          <src_port>68</src_port>
          <dst_port>0</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
        <rule name="DEFAULT_DNS_UDP" direction="BOTH">
          <protocol>17</protocol>
          <src_port>0</src_port>
          <dst_port>53</dst_port>
          <dst_addr>0</dst_addr>
        </rule>
```

```
      <rule name="DEFAULT_HTTPS" direction="BOTH">
        <protocol>6</protocol>
        <src_port>0</src_port>
        <dst_port>443</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_HTTP" direction="BOTH">
        <protocol>6</protocol>
        <src_port>0</src_port>
        <dst_port>80</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_ISAKMP" direction="BOTH">
        <protocol>17</protocol>
        <src_port>0</src_port>
        <dst_port>500</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_ESP" direction="BOTH">
        <protocol>50</protocol>
        <src_port>0</src_port>
        <dst_port>0</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
      <rule name="DEFAULT_ESP_NATT" direction="BOTH">
        <protocol>17</protocol>
        <src_port>0</src_port>
        <dst_port>4500</dst_port>
        <dst_addr>0</dst_addr>
      </rule>
    </rules>
    <rulesets>
      <beacon>
          <rule_add>RDP_SRV_TCP</rule_add>
          <rule_add>RDP_SRV_UDP</rule_add>
        <rule_add>DEFAULT_HTTPS</rule_add>
        <rule_add>DEFAULT_DNS_UDP</rule_add>
      </beacon>
      <block_all>
          <rule_add>RDP_SRV_TCP</rule_add>
          <rule_add>RDP_SRV_UDP</rule_add>
        <rule_add>DEFAULT_BOOTP_SRV</rule_add>
        <rule_add>DEFAULT_BOOTP_CLIENT</rule_add>
        <rule_add>DEFAULT_DNS_UDP</rule_add>
      </block_all>
```

```
        <cpd>
            <rule_add>RDP_SRV_TCP</rule_add>
            <rule_add>RDP_SRV_UDP</rule_add>
          <rule_add>DEFAULT_HTTP</rule_add>
          <rule_add>DEFAULT_DNS_UDP</rule_add>
        </cpd>
        <service_flows>
            <rule_add>RDP_SRV_TCP</rule_add>
            <rule_add>RDP_SRV_UDP</rule_add>
          <rule_add>DEFAULT_BOOTP_SRV</rule_add>
          <rule_add>DEFAULT_BOOTP_CLIENT</rule_add>
          <rule_add>DEFAULT_DNS_UDP</rule_add>
          <rule_add>DEFAULT_ISAKMP</rule_add>
          <rule_add>DEFAULT_ESP</rule_add>
          <rule_add>DEFAULT_ESP_NATT</rule_add>
        </service_flows>
      </rulesets>
    </filter_mode>
  </dialer_params>
</tgbconfig>
```

7 Contact

7.1 Information

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

7.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

7.3 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/.

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris — France

sales@thegreenbow.com

www.thegreenbow.com