Windows Enterprise VPN Client

Filtering Mode User's Guide

Latest update: 23 November 2022
Document reference number: 20221123_FM_VPE_7.3_EN_1.0

www.thegreenbow.com

Table of contents

1 Introduction 1
1.1 Overview 1
1.2 References 2
2 Adding the Filtering Mode 3
2.1 Introduction 3
2.2 MSI installer property NETPARAMS 4
2.3 MSI installer property IKESTART 5
2.4 vpnsetup.ini file 5
2.5 Removing the Filtering Mode 6
3 Configuring the Filtering Mode 7
3.1 Introduction 7
3.2 Format of the Filtering Mode rule configuration file 8
3.3 Verifying the imported configuration 11
3.4 Resetting the Filtering Mode 12
3.5 Current limitations 12
4 Configuring Captive Portal Detection 13
4.1 CPD tab of the Connections Configuration window 13
4.2 Log entries associated with Captive Portal Detection 14
5 Rulesets and states of TrustedConnect Panel 15
5.1 Introduction 15
5.2 BLOCK_ALL ruleset 16
5.3 BEACON ruleset 16
5.4 CPD ruleset 16
5.5 SERVICE_FLOWS ruleset 17
5.6 ALLOW_ALL ruleset 17
5.7 RESTRICTED ruleset 18
5.8 Default filtering rules 18

6 Appendix 19
6.1 Default filtering rules of the Filtering Mode 19
6.2 Sample rule file for the Filtering Mode 22
6.3 Sample rule file for the Filtering Mode: Windows Remote Desktop 30
7 Contact 34
7.1 Information 34
7.2 Sales 34
7.3 Support 34

Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2022-11-22	All	Initial draft	AL, BB

1 Introduction

1.1 Overview

TheGreenBow's Windows Enterprise VPN Client includes advanced features called Filtering Mode and Captive Portal Detection (CPD) that are intended for a specific usage, and which must be added when installing the software before they can be used.

The Filtering Mode in the Windows Enterprise VPN Client is a function used to filter the workstation's inbound and outbound data flows. It is enabled as soon as the Windows Enterprise VPN Client is not connected to a trusted network. Consequently, it is only available with the **TrustedConnect Panel**.

The data flows are filtered according to the various states of the Windows Enterprise VPN Client.

By default, the Filtering Mode works in "block all" mode and thus only allows data flows that are required for the proper operation of the workstation as well as for the proper execution of the Windows Enterprise VPN Client's various states.

Consequently, the Filtering Mode is associated with the CPD function, which automatically detects the presence of a captive portal when connecting to the internet.

If the workstation is behind a captive portal, the software is put on hold for 3 minutes (default value) to let the user authenticate on this captive portal. As soon as the user has authenticated, the workstation is connected to the internet, the Windows Enterprise VPN Client then automatically and immediately establishes the VPN connection.

To test if the workstation is behind a captive portal, the Windows Enterprise VPN Client tries to connect to a predefined web server. If the response to this connection attempt is not the one that the Windows Enterprise VPN Client expects, it concludes that the workstation is behind a captive portal.

To limit the cases of false positives (where a captive portal responds as a test web server), you can specify the HTTP return code and/or the data that the Windows Enterprise VPN Client should expect from the web server in response to its request.

A restricted and permanent Filtering Mode is also available. It is active even when the VPN Client is not running (refer to chapter 5 Rulesets and states of TrustedConnect Panel).

This specific guide is a supplement to the Windows Enterprise VPN Client Administrator's Guide and Deployment Guide. It is intended for system administrators who want to implement these advanced features for their users.

⚠ The Filtering Mode can in no way serve as a replacement for a firewall on a workstation that is configured with this feature of the Windows Enterprise VPN Client.

1.2 References

This document refers to the following documents:

- Windows Enterprise VPN Client Filtering Mode User's Guide (this document)
- Windows Enterprise VPN Client Administrator's Guide
- Windows Enterprise VPN Client Deployment Guide

You will find the latest versions of these documents on the Product Documentation page on our website at: https://www.thegreenbow.com/en/support/product-documentation/.

2 Adding the Filtering Mode

2.1 Introduction

To be able to use the Filtering Mode, it must be added when the Windows Enterprise VPN Client is installed. The Captive Portal Detection (CPD) feature is tied to the Filtering Mode. It is therefore added together with the Filtering Mode.

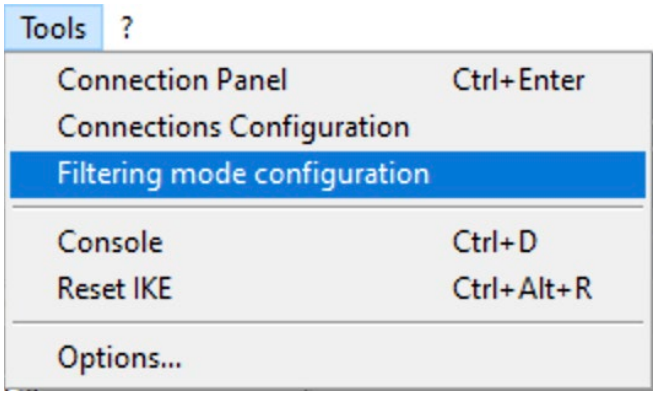
If you have already installed the Windows Enterprise VPN Client, you must uninstall it and then reinstall it to add this feature.

The Filtering Mode can be added in either of the following two ways:

- By passing a property to the MSI installer from the command line
- By adding an entry in the `vpnsetup.ini file`

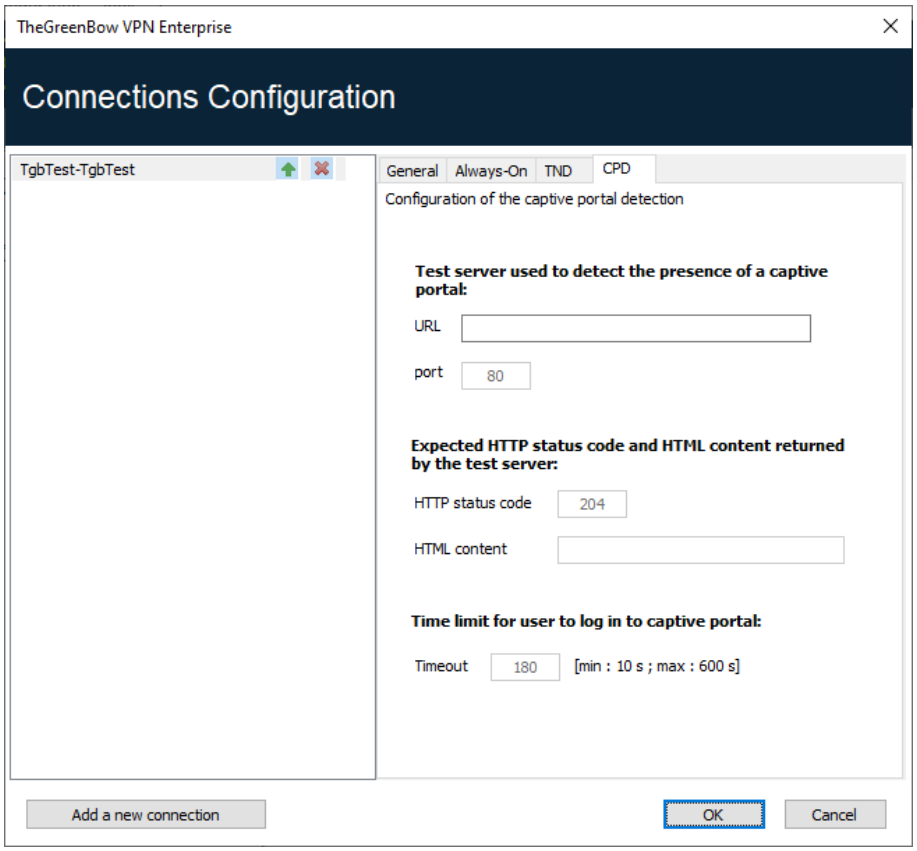
For more details on how to use the properties of the MSI installer and how to add an entry in the `vpnsetup.ini file`, refer to the Windows Enterprise VPN Client Deployment Guide.

When you add the Filtering Mode and CPD feature, an additional entry, called **Filtering mode configuration**, will appear in the **Tools** menu:



Refer to chapter 3 Configuring the Filtering Mode to find out how to configure the Filtering Mode.

A **CPD** tab will also be added to the **Connections Configuration** window, which will then appear as follows:



Refer to chapter 4 Configuring Captive Portal Detection to find out how to configure Captive Portal Detection.

2.2 MSI installer property NETPARAMS

The property to be passed to the MSI installer in the command line to add the Filtering Mode and CPD is called `NETPARAMS`. Since the Filtering Mode is only used with the **TrustedConnect Panel**, you must pass this property together with the `USEDIALERBYDEFAULT` property, which automatically starts the **TrustedConnect Panel** when the user logs on to Windows.

The `NETPARAMS` property is used in the same way as the other properties described in the Windows Enterprise VPN Client Deployment Guide and may be combined with these.

The following table provides a summary of the property's required syntax and usage:

Syntax:	`NETPARAMS=1`
Usage:	This property is used to add the special Filtering Mode feature. It must be used in combination with the `USEDIALERBYDEFAULT` property. It also adds the **Filtering mode configuration** option to the **Tools** menu in the **Configuration Panel**, as well as the **CPD** tab to the **Connections Configuration** window.
Example:	`msiexec /i "[download_directory]\TheGreenBow_VPN_ENTERPRISE.msi" USEDIALERBYDEFAULT=1 NETPARAMS=1`

2.3 MSI installer property IKESTART

The property to be passed to the MSI installer in the command line to add the restricted and permanent Filtering Mode is called `IKESTART`.

It is used in the same way as the other properties described in the Windows Enterprise VPN Client Deployment Guide and may be combined with these.

Syntax:	`IKESTART=1`
Usage:	This property is used to add a restricted and permanent Filtering Mode. It must be used in combination with the `USEDIALERBYDEFAULT` and `NETPARAMS` properties.
Example:	`msiexec /i "[download_directory]\TheGreenBow_VPN_ENTERPRISE.msi" USEDIALERBYDEFAULT=1 NETPARAMS=1 IKESTART=1`

The fact that the `RESTRICTED` ruleset is applied when the **TrustedConnect Panel** is not running is a feature that you can configure using an MSI installer property or a parameter in the `vpnsetup.ini` installation file. You must therefore make this choice during installation (see chapter 5 Rulesets and states of TrustedConnect Panel).

2.4 vpnsetup.ini file

You can configure the addition of the Filtering Mode in the `vpnsetup.ini file` to be used in combination with Windows Enterprise VPN Client installer.

To do this, simply define the `UseDialerByDefault` parameter in the `[Dialer]` section as well as the `NetParams` parameter and, where

appropriate, the `IkeStart` parameter in the `[AddRegKey]` section of the `vpnsetup.ini` file as follows:

```
[Dialer]
UseDialerByDefault=1

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

For more details on how to use the `vpnsetup.ini` file, refer to the Windows Enterprise VPN Client Deployment Guide.

2.5 Removing the Filtering Mode

To remove the Filtering Mode from the Windows Enterprise VPN Client and no longer show the **Filtering mode configuration** option in the **Tools** menu, you must uninstall the software and reinstall it without this advanced feature.

3 Configuring the Filtering Mode

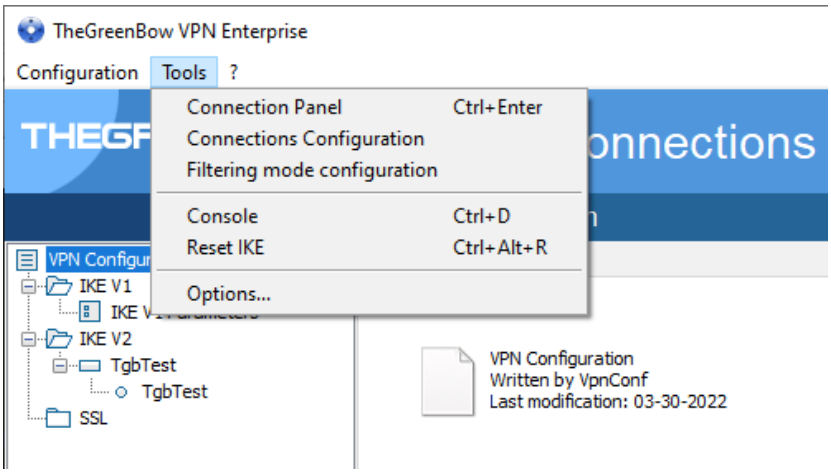
3.1 Introduction

The Filtering Mode's configuration is stored in the VPN configuration file. It thus benefits from the same mechanisms that protect this file (encryption, authenticity, and integrity), as well as the facilities for remote deployment and/or modification.

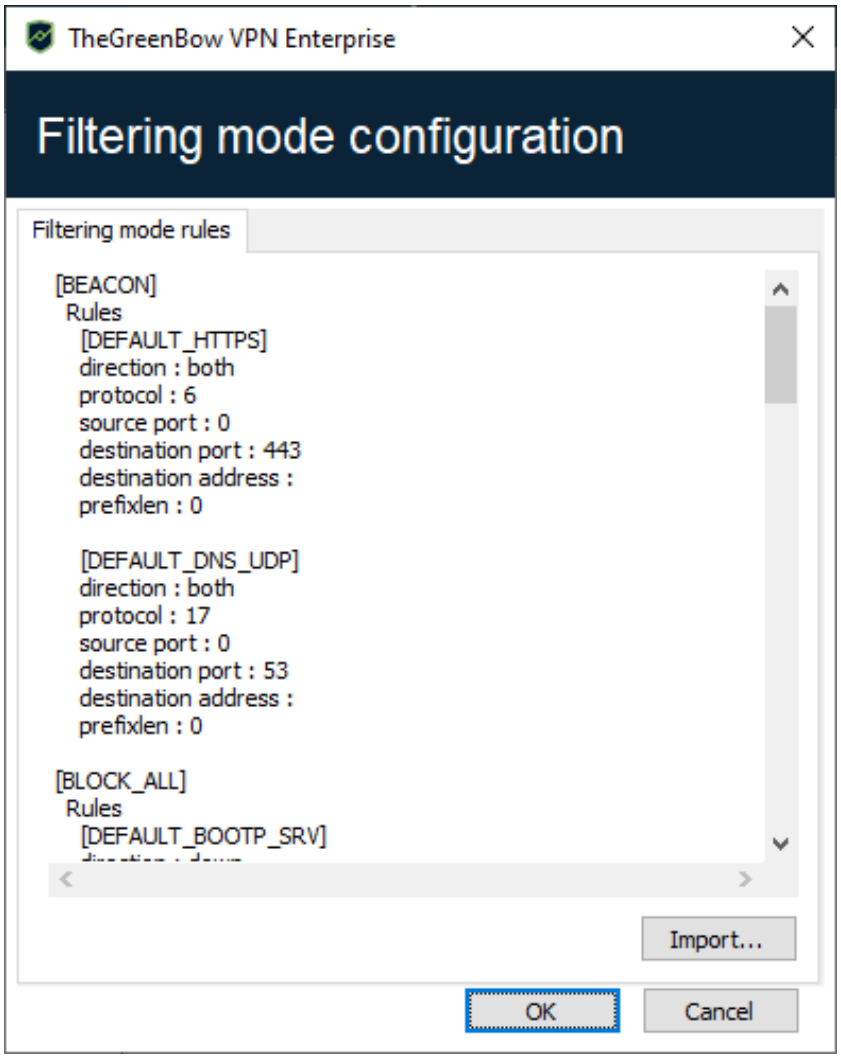
Follow the steps below to configure the Filtering Mode:

1. Edit the filtering rules in a text file (see section 6.2 Sample rule file in the appendix).
2. Import the text file into the VPN configuration (a check is performed during import to ensure that the file syntax is consistent, see section 3.3 Verifying the imported configuration below).

The **Filtering mode configuration** window includes an option to import the filtering rule configuration file. To access the window, in the Windows Enterprise VPN Client's **Configuration Panel**, choose the **Tools** > **Filtering mode configuration** menu option.



The **Filtering mode configuration** window appears as follows:



The latest version of the Windows Enterprise VPN Client allows you to configure all the filters for each state of the **TrustedConnect Panel**.

In the remainder of this document, the terms "ruleset" and "filter" mean the same thing. A ruleset is a set of rules.

3.2 Format of the Filtering Mode rule configuration file

The file used to configure the Filtering Mode's rules is an XML file containing two main sections:

1. The first defines all the filtering rules
2. The second defines the rulesets

The syntax of a rule configuration file is as follows:

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

The syntax of a rule is as follows:

```
<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>
```

The Filtering Mode rule configuration file uses the following parameters:

`name`	Any character string, excluding spaces as well as `DYN_RULES`, which is reserved for TheGreenBow
`direction`	`BOTH`, `DOWN` or `UP`: direction from the workstation's point of view
`protocol`	Integer from among the following: 0, 1, 6, 17, 50 (respectively: all, ICMP, TCP, UDP, ESP)
`src_port`, `dst_port`[1]	Integer between 0 and 65535 0 or `ALL` means "all ports"
`icmp_code`[2]	Integer between 0 and 15 or the keyword `ALL`, which means "all ICMP codes"

[1] `src_port` and `dst_port` must be specified if `protocol` is different from 1 (ICMP)
[2] `icmp_code` must be specified if `protocol` is equal to 1 (ICMP)

`icmp_type`[1]	Integer between 0 and 18 or the keyword `ALL`, which means "all ICMP types"
`dst_addr`	May be set to one of the following values: • An IPv4 address with a dotted decimal notation • An URI (e.g. www.thegreenbow.com) • 0 or `ALL`, which means "all authorized IP addresses"
`prefix_len`	Defines the network mask. If `dst_addr` is of type IPv4: integer between 0 and 32. If `dst_addr` is of type URI, the value of `prefix_len` is not used, `prefix_len` will be calculated dynamically.

The syntax of a ruleset is as follows:

```
<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>
```

The following rulesets can be configured:

- `BLOCK_ALL`
- `BEACON`
- `CPD`
- `SERVICE_FLOWS`

The following rulesets cannot be configured:

- `RESTRICTED` if the VPN client has been installed with `IKESTART=1`
- `ALLOW_ALL` if the filtering mode has not been enabled

As soon as at least one filtering rule is specified in any given ruleset, it overrides and replaces all default rules in that ruleset.

We strongly recommend that you enable both the DNS and DHCP protocols in the `BLOCK_ALL` and `SERVICE_FLOWS` rulesets.

[1] `icmp_type` must be specified if `protocol` is equal to 1 (ICMP)

3.3 Verifying the imported configuration

A syntactic consistency check is performed when the Filtering Mode configuration is imported.

If an error is detected, it will be shown in the **Filtering mode configuration** window.

The following aspects are verified during this check:

- No ruleset contains more than 30 rules
- Ruleset names are either of the following:
  - `BLOCK_ALL`
  - `BEACON`
  - `CPD`
  - `SERVICE_FLOWS`
- Each ruleset is defined only once (there are no two rulesets with the same name)
- Each ruleset contains at least one rule
- Any rule specified in a ruleset exists in the list of rules defined
- The fields `name`, `direction`, `protocol`, and `dst_addr` have been specified (not empty)
- If `protocol = 1` (ICMP) the `icmp_code` and `icmp_type` fields have been specified (not empty)
- If `protocol` is different from 1 (ICMP), the `dst_port` and `src_port` fields have been specified (not empty)
- The `prefix_len` field is specified, if the `dst_addr` field is an IP address
- If the `dst_addr` filed is an URI, the `prefix_len` field has been removed
- The format of `dst_addr` (IPv4 address or URI) is correct
- The value of `prefix_len` is consistent with the address family of the IP address:
  - If `dst_addr` is of type IPv4, `prefix_len` ranges from 0 to 32
  - If `dst_addr` is set to `0` or `ALL`, `prefix_len` will not be taken into consideration
- `direction` is set to one of the following three values: `DOWN`, `UP`, or `BOTH`
- `protocol` is set to one of the following values: 0, 1, 6, 17, 50 (respectively: all, ICMP, TCP, UDP, ESP)
- The destination and source ports are set to an integer between 0 and 65535 or the keyword `ALL`
- The value of `icmp_code` is set to an integer between 0 and 15 or the keyword `ALL`
- The value of `icmp_type` is set to an integer between 0 and 18 or the keyword `ALL`

3.4 Resetting the Filtering Mode

TheGreenBow provides the default Filtering Mode configuration file as an example (see section 6.1 Default filtering rules of the Filtering Mode in the appendix).

The default configuration of the Filtering Mode can be reset by importing an "empty" configuration file.

An "empty" configuration file must comply with the following syntax:

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

3.5 Current limitations

The `ALLOW_ALL` and `RESTRICTED` rulesets are not configurable.

A ruleset can contain no more than 30 rules.

When the **TrustedConnect Panel** is not active (before the software has been started or after it has been stopped), if it is applied (`IKESTART =1`), the `RESTRICTED` ruleset is not configurable (and only allows DHCP, DNS/UDP, DNS/TCP).

The IPv6 protocol is not yet supported.

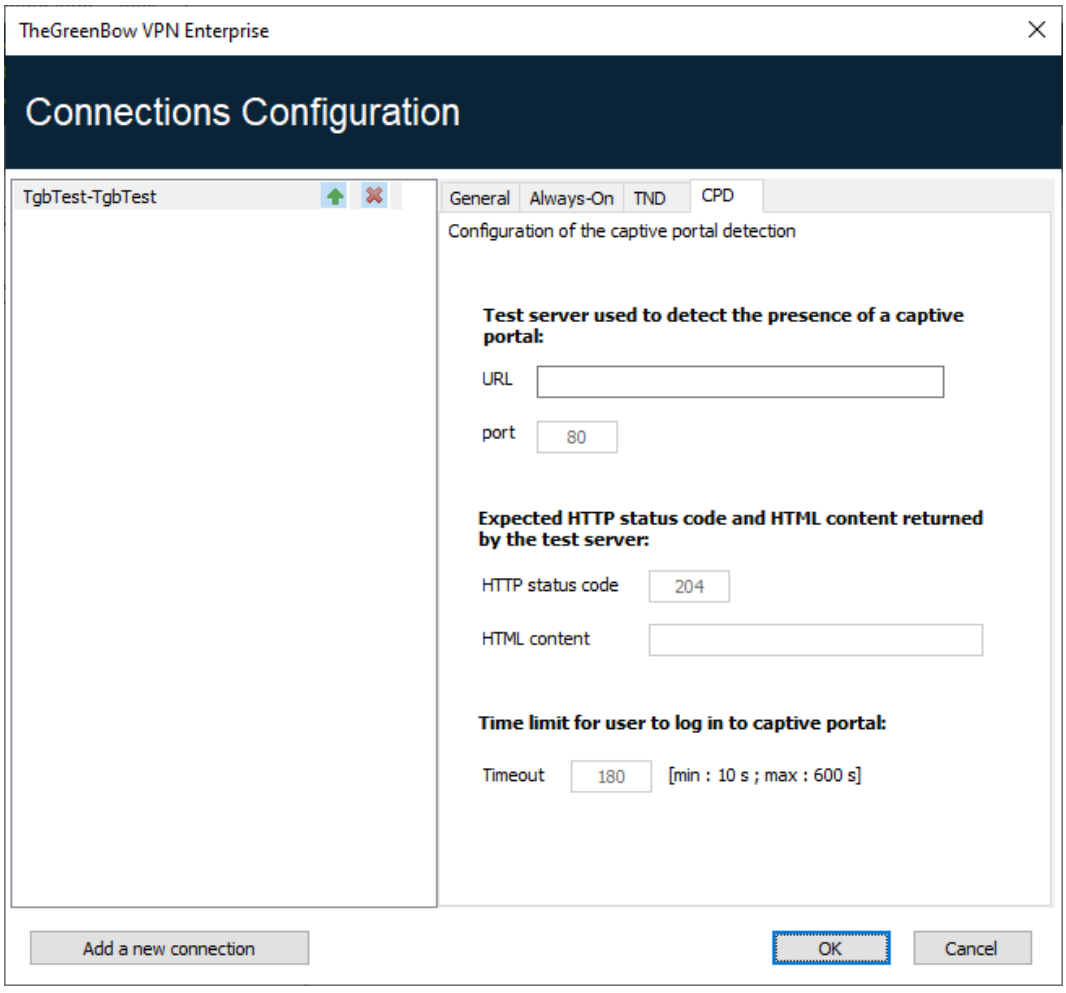
4 Configuring Captive Portal Detection

Use the **CPD** tab of the **Connections Configuration** window to configure Captive Portal Detection.

To access the **CPD** tab, from the **Tools** menu, choose **Connections Configuration**, and then select the **CPD** tab.

4.1 CPD tab of the Connections Configuration window

The **CPD** tab of the **Connections Configuration** window appears as follows:



It is simple and intuitive to use.

URL	Address of the web server that will be used to perform the detection
port	Port used to access the web server that will be used to perform the detection

HTTP status code	Different return code expected by the Windows Enterprise VPN Client, to avoid issues when a captive portal responds with the HTTP return code 204
HTML content	Content expected in the response of the web server used for detection
Timeout	Time in seconds allotted to the user to identify on the captive portal Default value: 180 s Minimum: 10 s Maximum: 600 s

4.2 Log entries associated with Captive Portal Detection

The following log entries pertaining to the Captive Portal Detection feature may appear in the **Console**:

Workstation is behind a captive portal	Indicates that the workstation is behind a captive portal.
Workstation is not behind a captive portal	Indicates that the workstation is not behind a captive portal.
Captive portal login timeout	Indicates that the captive portal has not been opened within 3 minutes (default value) following detection.

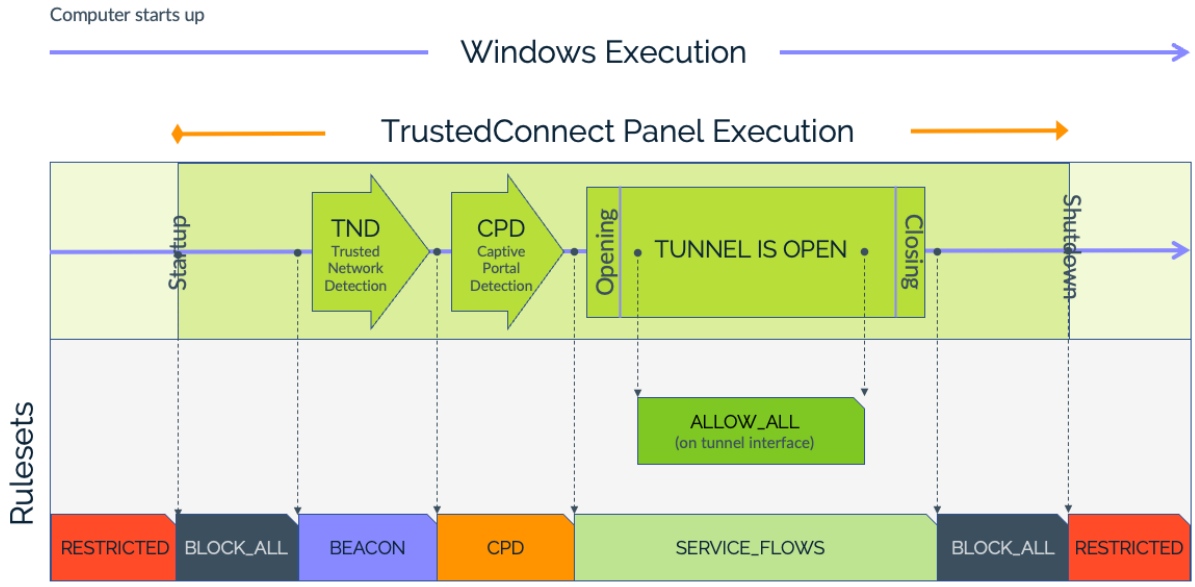
To find out how to display the **Console**, refer to the Windows Enterprise VPN Client Administrator's Guide.

5 Rulesets and states of TrustedConnect Panel

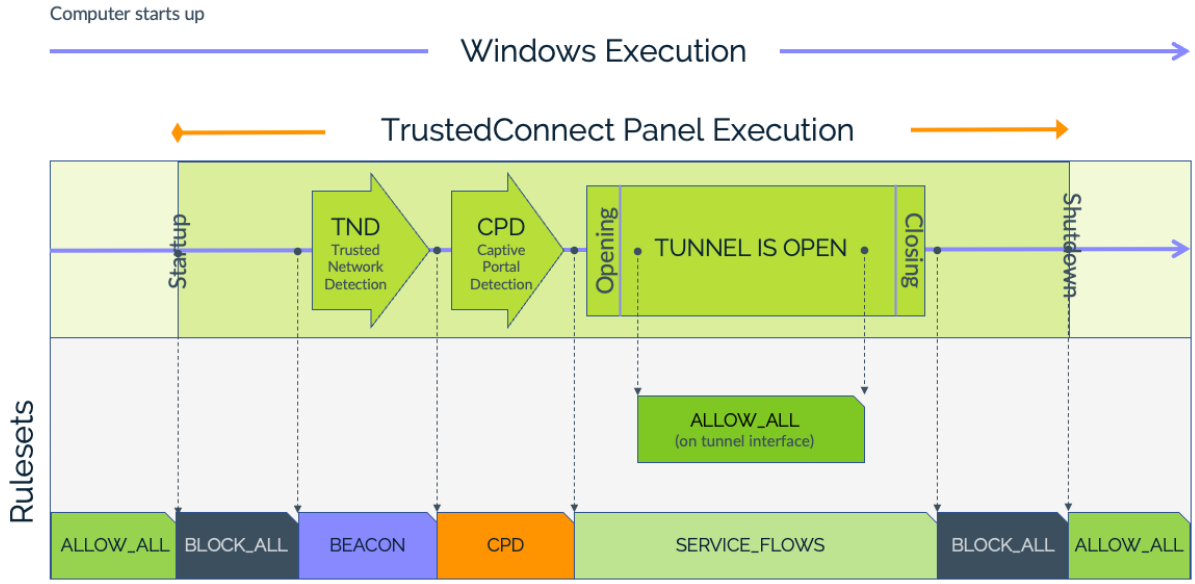
5.1 Introduction

The diagrams below show the various possible states of the **TrustedConnect Panel** and the rulesets associated with these different states.

If you configure the properties `NETPARAMS=1` and `IKESTART=1`, the restricted and permanent Filtering Mode will be enabled from the time the workstation is started until it is shut down, including when it is standing by.



Otherwise, if you only configure the property `NETPARAMS=1`, the Filtering Mode will only be enabled when the VPN Client is open.



5.2 BLOCK_ALL ruleset

The `BLOCK_ALL` ruleset is applied to all network interfaces while the **TrustedConnect Panel** has not started Trusted Network Detection (TND), as soon as the tunnel is closed, or if the tunnel has failed.

To block all traffic when the **TrustedConnect Panel** is not running, use the `RESTRICTED` ruleset (see section 5.7 RESTRICTED ruleset).

5.3 BEACON ruleset

The `BEACON` ruleset is applied when the **TrustedConnect Panel** is running the TND mechanism.

It is successively applied to each network interface whose DNS suffix is considered as trusted.

5.4 CPD ruleset

The `CPD` ruleset is applied when the **TrustedConnect Panel** is running the Captive Portal Detection mechanism, after having detected that the workstation is not connected to the trusted network.

The `CPD` ruleset is applied to the interface used to open the VPN connection.

The CPD ruleset remains applied for a maximum of 3 minutes (default time allotted to the user to authenticate).

As soon as the user has authenticated, the **TrustedConnect Panel** opens the VPN connection and applies the SERVICE_FLOWS and ALLOW_ALL rulesets (see below) to the network interfaces concerned.

Conversely, if the user has not authenticated within the allotted 3 minutes (default value), the **TrustedConnect Panel** applies the BLOCK_ALL ruleset.

5.5 SERVICE_FLOWS ruleset

The SERVICE_FLOWS ruleset is applied to the network interface used to establish and maintain the VPN connection.

The ruleset consists of filtering rules that allow the protocols required to open the VPN connection (ISAKMP, ESP, etc.) as well as those required to maintain it (e.g. DHCP, DNS).

The SERVICE_FLOWS ruleset applies to the physical network interface on which the VPN connection has been opened.

5.6 ALLOW_ALL ruleset

The ALLOW_ALL ruleset is applied to the network interface that is connected to the trusted network.

This network interface can be either a physical interface, when the workstation is directly connected to the trusted network (e.g. via Ethernet), or a virtual interface, when the workstation is connected to the trusted network via the VPN connection.

This ruleset allows all data flows on the relevant network interface.

This ruleset can also be applied to a (physical or virtual) network interface that the administrator has decided to exclude from the interfaces processed by the **TrustedConnect Panel**. You can configure this specific processing during installation, as specified in the section describing the Always-On function in the Windows Enterprise VPN Client Administrator's Guide.

This ruleset is not configurable (see section 3.5 Current limitations above).

5.7 RESTRICTED ruleset

The `RESTRICTED` ruleset is applied to all network interfaces while the **TrustedConnect Panel** is not running, i.e. before it is started and after it has been quit.

The following filtering rules are active in this ruleset:

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

This ruleset is only available if the property `IKESTART=1` has been configured when installing the software (see section 2.3 MSI installer property IKESTART above).

This ruleset is not configurable (see section 3.5 Current limitations above).

5.8 Default filtering rules

By default (when no specific filtering rules are configured), the Filtering Mode consists of the following filtering rules:

Ruleset	Default rules
BLOCK_ALL	Only allows DHCP, DNS/UDP
BEACON	Only allows HTTPS, DNS/UDP, DNS/TCP
CPD	Only allows HTTP, HTTPS, DNS/UDP, DNS/TCP
SERVICE_FLOWS	Only allows DHCP, DNS/UDP, DNS/TCP, ISAKMP, ESP, ESP/NAT-T, HTTPS
ALLOW_ALL	Allows all data flows
If IKESTART=1	
RESTRICTED	Only allows DHCP, DNS/UDP, DNS/TCP

6 Appendix

6.1 Default filtering rules of the Filtering Mode

The default filtering rules of the Filtering Mode are reproduced below:

```
<?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 Sample rule file for the Filtering Mode

This sample file contains the following rules:

- The `BEACON` rule is used to allow trusted network detection using the TCP protocol on destination port 443 and destination IP address `www.thegreenbow.com` regardless of the source port:
  - `protocol`: 6
  - `src_port`: ALL
  - `dst_port`: 443
  - `dst_addr`: www.thegreenbow.com
- The `CPDWEB` rule is used to allow captive portal detection using the TCP protocol on destination port 80 and destination IP address `detectportal.firefox.com` regardless of the source port:
  - `protocol`: 6
  - `src_port`: 0
  - `dst_port`: 80
  - `dst_addr`: detectportal.firefox.com
- The `BOOTP_SRV` rule is used to allow the UDP protocol directed towards the server on destination port 67 regardless of the source port and destination IP address to enable the use of the DHCP protocol:
  - `protocol`: 17
  - `src_port`: 0
  - `dst_port`: 67
  - `dst_addr`: 0
- The `BOOTP_CLIENT` rule is used to allow the UDP protocol coming from the server on source port 68 regardless of the destination port and destination IP address to enable the use of the DHCP protocol:
  - `protocol`: 17
  - `src_port`: 68
  - `dst_port`: 0
  - `dst_addr`: 0
- The `DNS_UDP` rule is used to allow the UDP protocol on destination port 53 regardless of the source port and destination IP address to enable the use of the DNS service:
  - `protocol`: 17
  - `src_port`: 0
  - `dst_port`: 53
  - `dst_addr`: 0

- The `DNS_TCP` rule is used to allow the TCP protocol on destination port 53 regardless of the source port and destination IP address to enable the use of the DNS service:
  - `protocol`: 6
  - `src_port`: 0
  - `dst_port`: 53
  - `dst_addr`: 0
- The `ICMP` rule is used to allow all ICMP codes for all ICMP types on all destination addresses to enable pinging:
  - `icmp_type`: ALL
  - `icmp_code`: ALL
  - `dst_addr`: ALL
- The `CRLOCSP_TCP` rule is used to allow the TCP protocol on destination port 80 and destination IP address `ocsp.sectigo.com` regardless of the source port to enable interaction with OSCP:
  - `protocol`: 6
  - `src_port`: 0
  - `dst_port`: 80
  - `dst_addr`: ocsp.sectigo.com
- The `NETBIOS_NAME` rule is used to allow the UDP protocol on destination port 137 regardless of the source port and destination IP address to enable machine name resolution via NetBIOS:
  - `protocol`: 17
  - `src_port`: 0
  - `dst_port`: 137
  - `dst_addr`: 0
- The `NETBIOS_DGRAM` rule is used to allow the UDP protocol on destination port 138 regardless of the source port and destination IP address to enable the use of the NetBIOS protocol (Windows file sharing, printers, etc.):
  - `protocol`: 17
  - `src_port`: 0
  - `dst_port`: 138
  - `dst_addr`: 0
- The `HTTPS` rule is used to allow the TCP protocol on destination port 443 regardless of the source port and destination IP address to enable secure web browsing:
  - `protocol`: 6
  - `src_port`: ALL
  - `dst_port`: 443
  - `dst_addr`: ALL

- The `HTTPS` rule is used to allow the TCP protocol on destination port 443 regardless of the source port and destination IP address to enable secure web browsing:
  - protocol: 6
  - `src_port`: ALL
  - `dst_port`: 443
  - `dst_addr`: ALL
- The `ISAKMP` rule is used to allow the UDP protocol from source port 500 to destination port 500 and destination IP address `tgbtest.dyndns.org` to enable the establishment of an IPsec tunnel:
  - `protocol`: 17
  - `src_port`: 500
  - `dst_port`: 500
  - `dst_addr`: tgbtest.dyndns.org
- The `ESP` rule is used to allow the ESP protocol on all destination ports regardless of the source port and destination IP address to enable the establishment of an IPsec tunnel:
  - `protocol`: 50
  - `src_port`: ALL
  - `dst_port`: ALL
  - `dst_addr`: 0
- The `ESP-NATT` rule is used to allow the UDP protocol from source port 4500 to destination port 4500 and destination IP address `tgbtest.dyndns.org` to enable the establishment of an IPsec tunnel:
  - `protocol`: 17
  - `src_port`: 4500
  - `dst_port`: 4500
  - `dst_addr`: tgbtest.dyndns.org

These rules are used in the following ways in the various rulesets:

- The `BLOCK_ALL` ruleset blocks all communications other than those that meet the rules defined here while the **TrustedConnect Panel** is not running, i.e. before it is started and after it has been quit:
  - `BOOTP_SRV`
  - `BOOTP_CLIENT`
  - `DNS_UDP`
  - `DNS_TCP`
  - `ICMP`

- The `BEACON` ruleset allows all communications that meet the following rules to enable trusted network detection:
  - `DNS_UDP`
  - `DNS_TCP`
  - `BEACON`
  - `CRLOCSP_TCP`
- The `CPD` ruleset allows all communications that meet the following rules to enable captive portal detection:
  - `DNS_UDP`
  - `DNS_TCP`
  - `CPDWEB`
  - `HTTPS`
- The `SERVICE_FLOWS` ruleset allows all communications that meet the following rules to enable the establishment of the VPN connection:
  - `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 Sample rule file for the Filtering Mode: Windows Remote Desktop

This sample file is based on the default rules. The required changes to make it work with Windows Remote Desktop are highlighted in 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

All the information on TheGreenBow products is available on our website: https://thegreenbow.com/.

7.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

7.3 Support

There are several pages related to the software's technical support on our website:

Online help

https://www.thegreenbow.com/en/support/online-support/

FAQ

https://www.thegreenbow.com/en/frequently-asked-questions/

Contact form

Technical support can be reached using the form on our website at the following address: https://www.thegreenbow.com/en/support/online-support/technical-support/.

Protect your connections
in any situation

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com