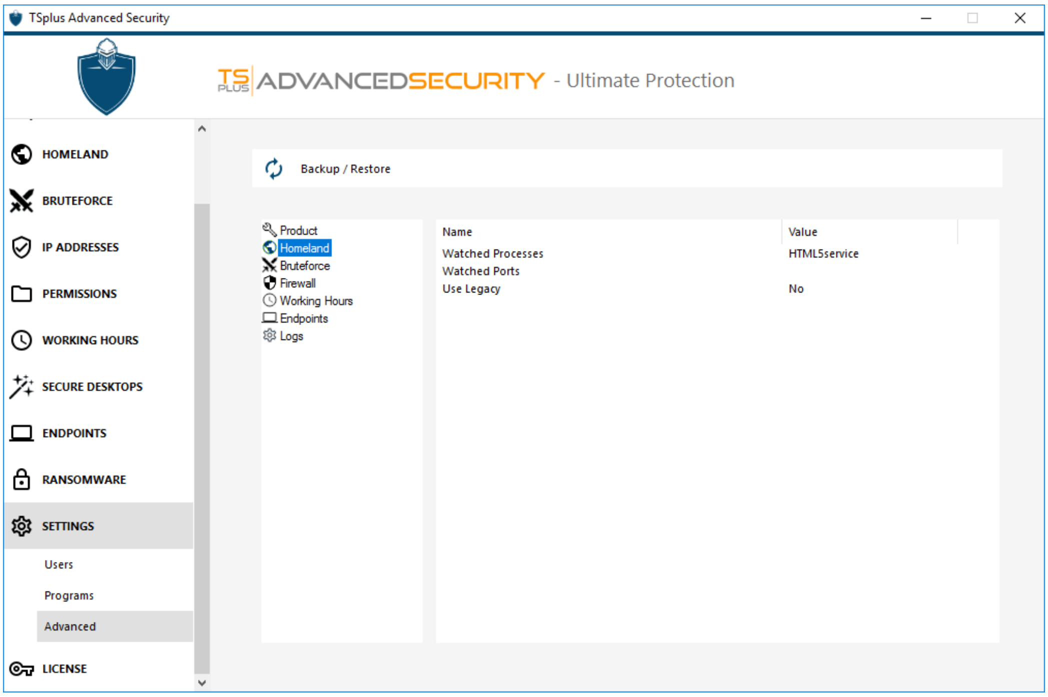
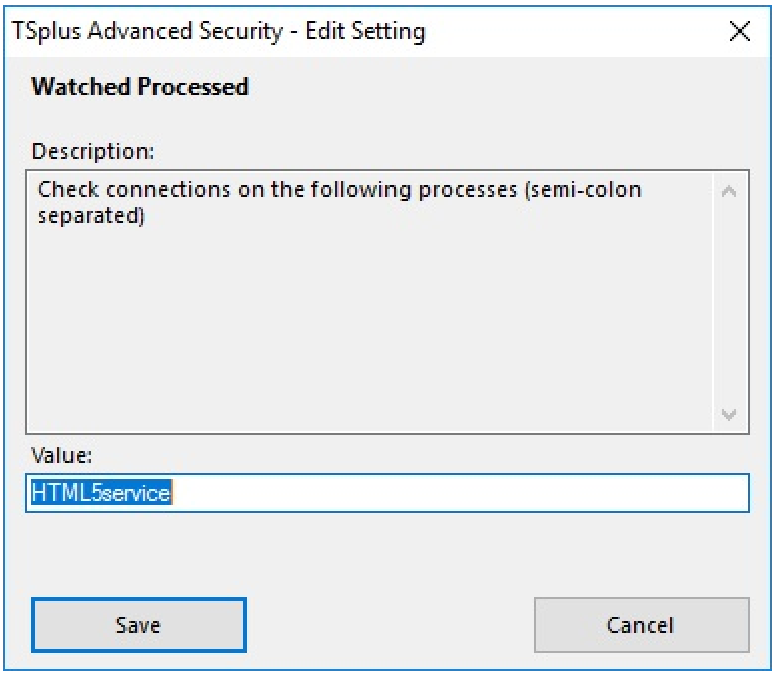
Advanced - Homeland Settings

The **Homeland tab** allows you to *add or remove Processes that are watched by the Homeland Protection feature*.



Name	Value
Watched Processes	HTML5service
Watched Ports	
Use Legacy	No


TSplus Advanced Security - Edit Setting

Watched Processed

Description:

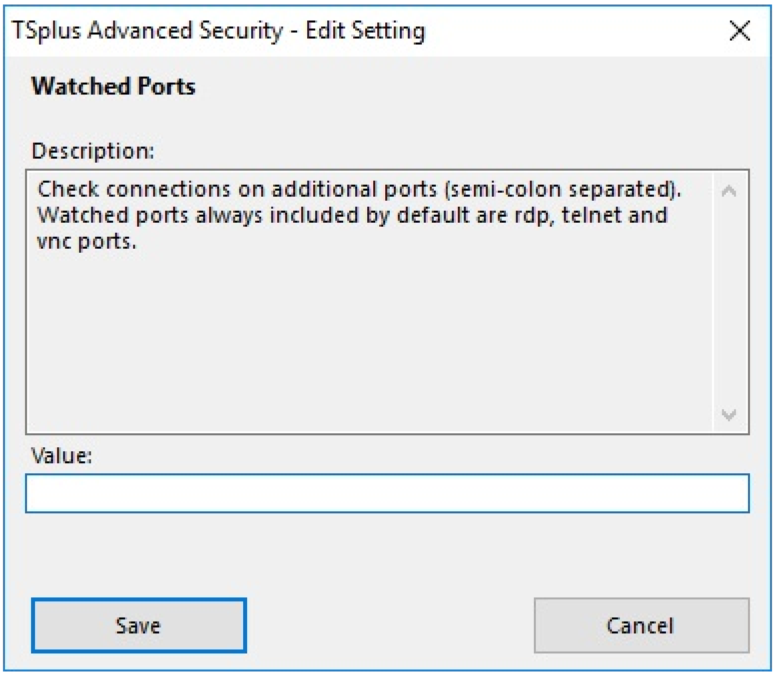
Check connections on the following processes (semi-colon separated)

Value:

HTML5service

By default, the HTML5 service is watched.

The **Watched Ports** settings allows you to add ports watched by the *Homeland Protection Feature*. By default, Homeland Access Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC. Homeland supports the following VNC providers: Tight VNC, Ultra VNC, Tiger VNC and Real VNC, which are not related whatsoever with TSplus.



TSplus Advanced Security - Edit Setting

Watched Ports

Description:

Check connections on additional ports (semi-colon separated). Watched ports always included by default are rdp, telnet and vnc ports.

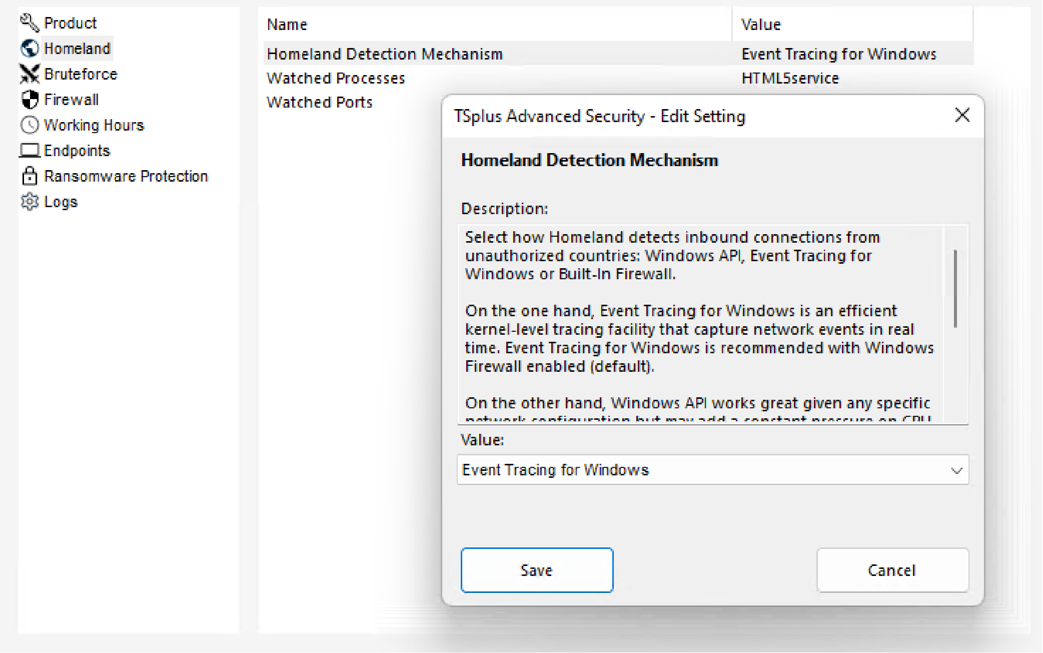
Value:

The **Homeland Detection Mechanism** setting defines how Homeland detects inbound connections from unauthorized countries, using one of the three differents detection mechanisms: - Windows API - Event Tracing for Windows - Built-In Firewall

On the one hand, Event Tracing for Windows is an efficient kernel-level tracing facility that capture network events in real time. Event Tracing for Windows is recommended with Windows Firewall enabled (default).

On the other hand, Windows API works great given any specific network configuration but may add a constant pressure on CPU depending on the amount of active connections. Please note that Windows API is not compatible with IPv6 yet.

Built-In Firewall enables user-mode capturing and dropping of network packets sent to the Windows network stack. When the Built-In Firewall is configured to block unwanted connections, it is recommended to use it to enforce Homeland's allowed countries.



Name	Value
Homeland Detection Mechanism	Event Tracing for Windows
Watched Processes	HTML5service
Watched Ports	

TSplus Advanced Security - Edit Setting

Homeland Detection Mechanism

Description:

Select how Homeland detects inbound connections from unauthorized countries: Windows API, Event Tracing for Windows or Built-In Firewall.

On the one hand, Event Tracing for Windows is an efficient kernel-level tracing facility that capture network events in real time. Event Tracing for Windows is recommended with Windows Firewall enabled (default).

On the other hand, Windows API works great given any specific

Value:

Event Tracing for Windows