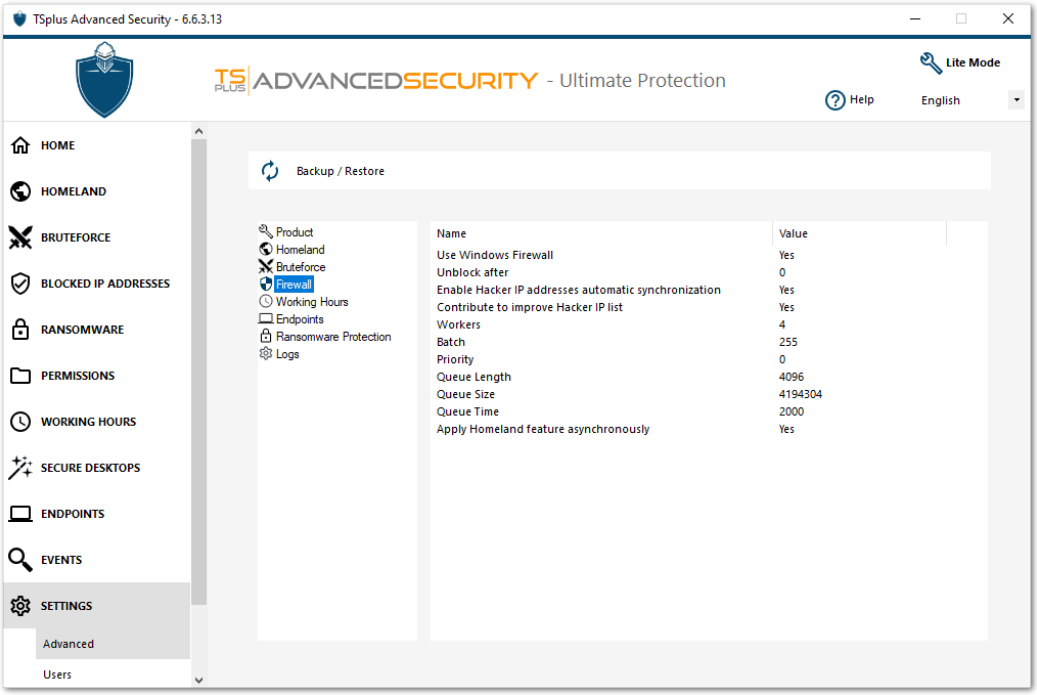
Advanced - Firewall Settings

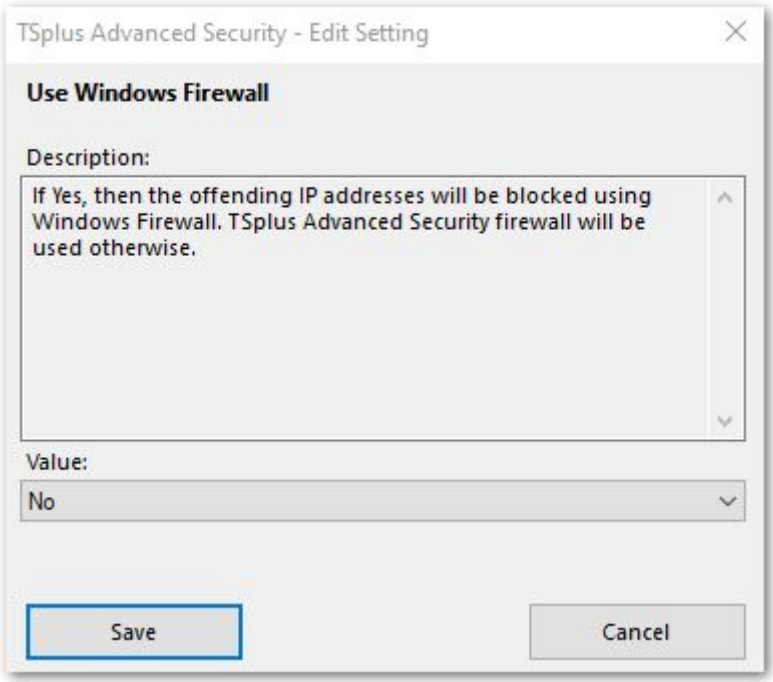
The **Firewall tab** allows you to activate the **Windows Firewall or deactivate it in favor of the TSplus Advanced Security built-in firewall**.

Since version 4.4, a built-in firewall is included in TSplus Advanced Security.

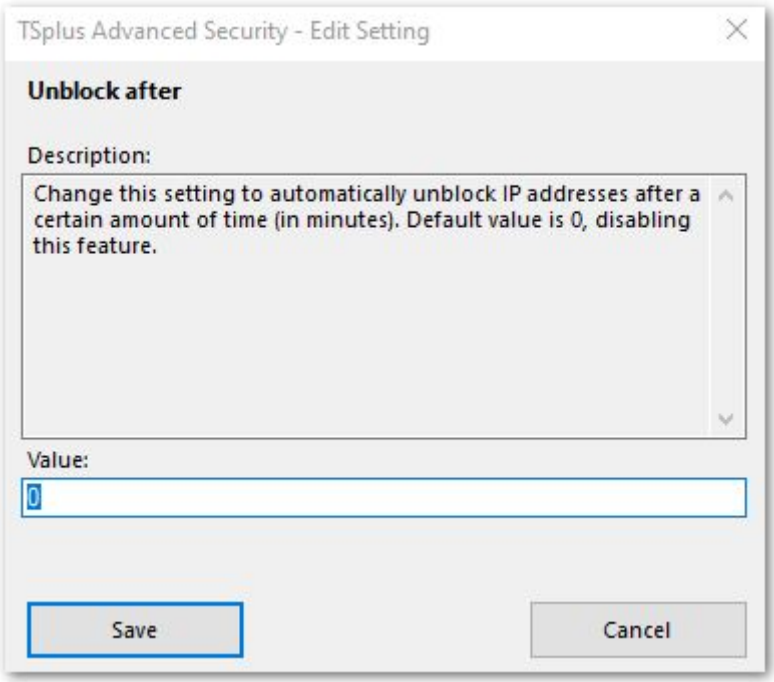
As a general guidance, if Windows Firewall is activated on your server, then you should use it to enforce TSplus Advanced Security rules (default). If you installed another firewall, then you must activate TSplus Advanced Security built-in firewall.



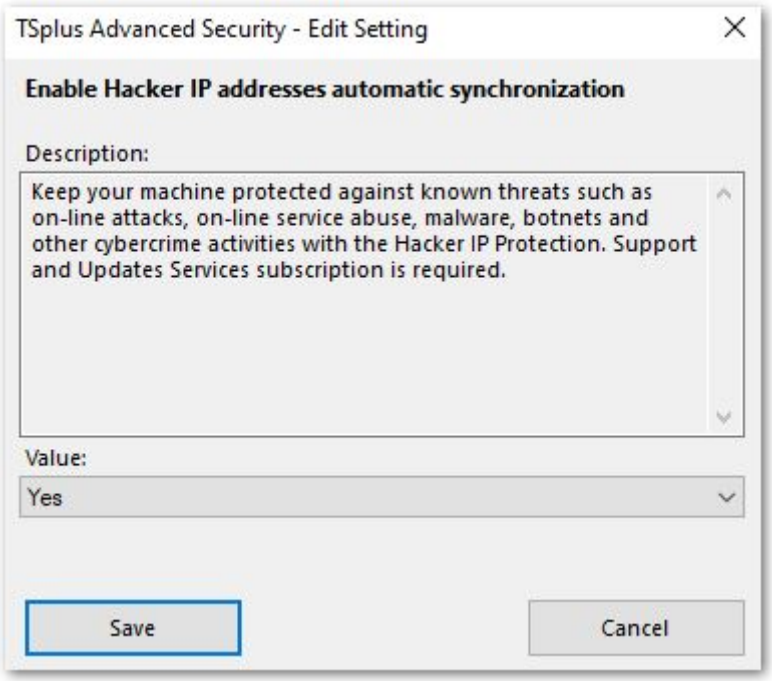
Use Windows Firewall
In order to activate the built-in firewall, go to Settings > Advanced > Product > Use Windows Firewall and set the value to: No
If Yes, then the offending IP addresses will be blocked using Windows Firewall.
TSplus Advanced Security firewall will be used otherwise.



Unblock after
Change this setting to automatically unblock IP addresses after a certain amount of time (in minutes). Default value is 0, disabling this feature.
Value: 0

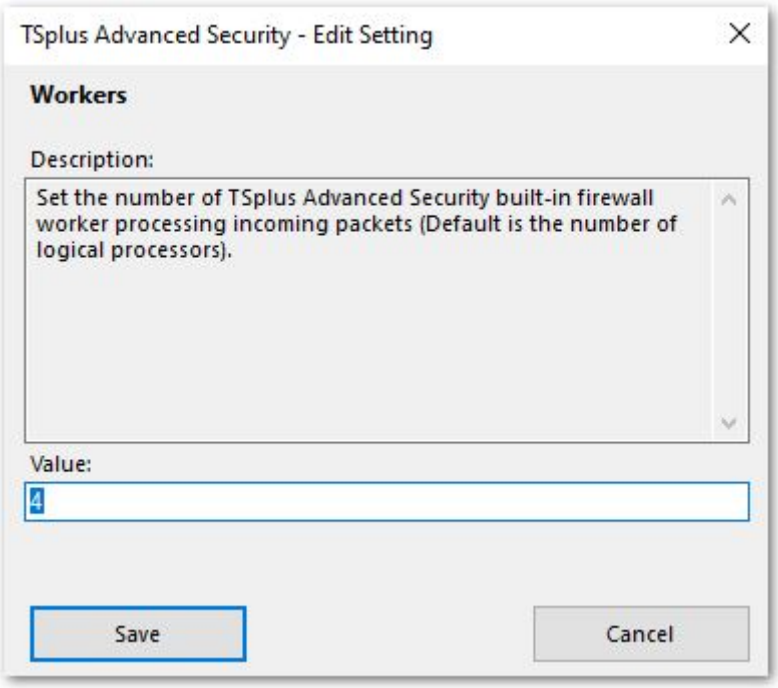


Enable Hacker IP addresses automatic synchronization
Keep your machine protected against known threats such as on-line attacks, on-line service abuse, malware, botnets and other electronic activities with the Hacker IP Protection. Support and Updates Services subscription is required.
Value: Yes

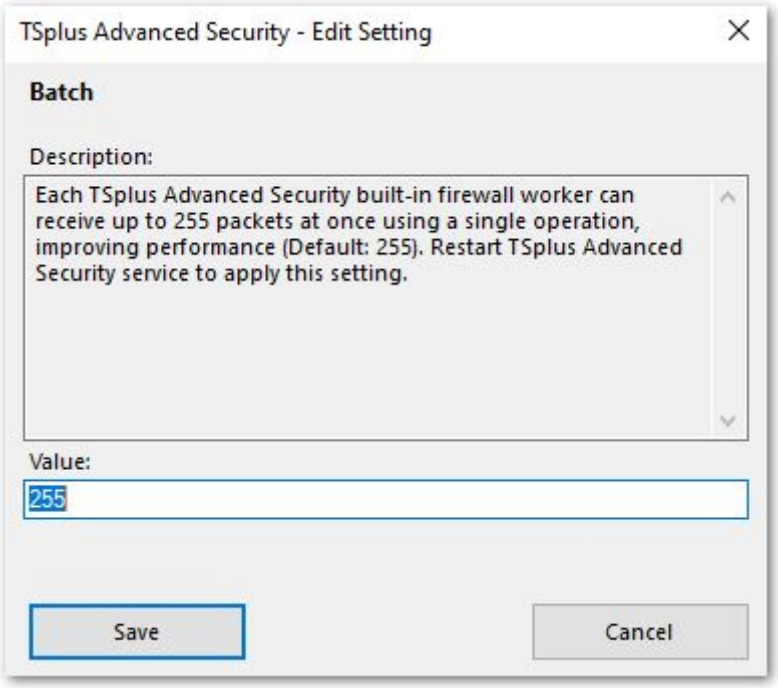


Contribute to improve Hacker IP list
Allow TSplus Advanced Security to send anonymous usage statistics to enhance protection against Hacker IP.
Value: Yes

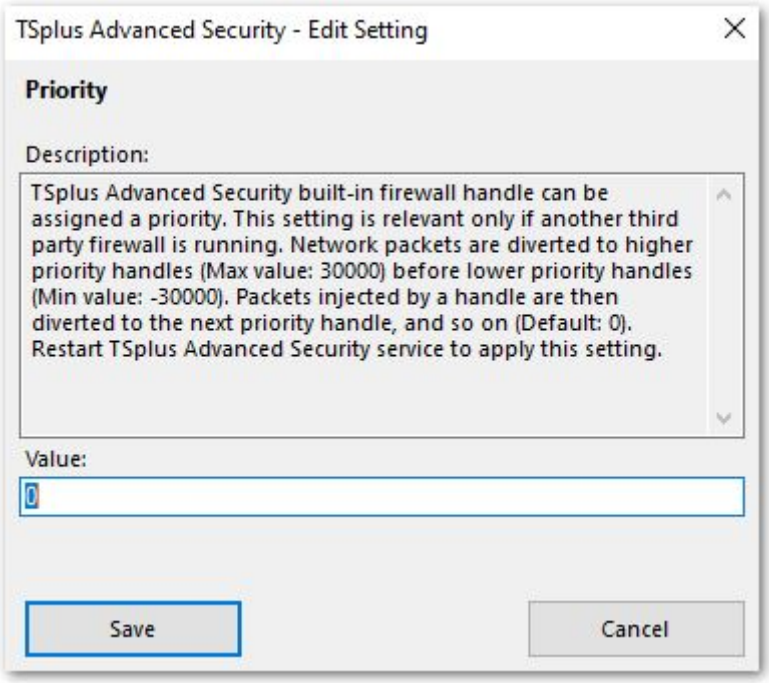
Workers
Set the number of TSplus Advanced Security built-in firewall worker processing incoming packets (Default is the number of logical processors).
Value: 4



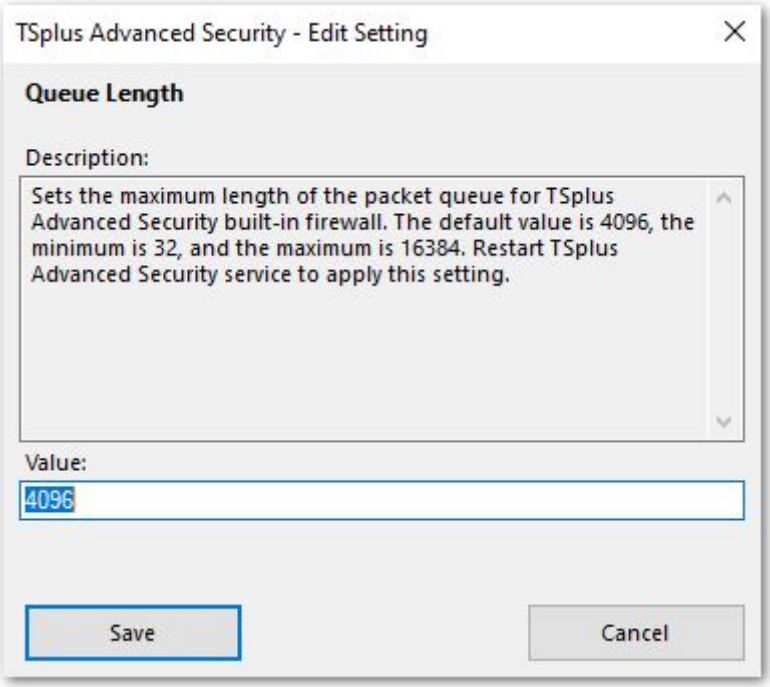
Batch
Each TSplus Advanced Security built-in firewall worker can receive up to 255 packets at once using a single operation, improving performance (Default: 255).
Restart TSplus Advanced security service to apply this setting.
Value: 255



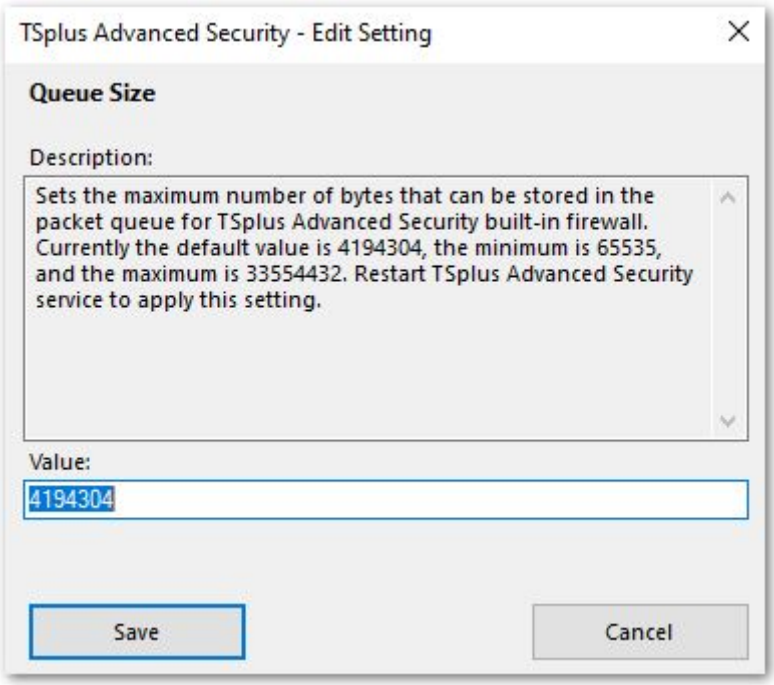
Priority
TSplus Advanced Security built-in firewall handle can be assigned a priority. This setting is relevant only if another third party firewall is running.
Network packets are diverted to higher priority handles (Max value: 30000) before lower priority handles (Min value: -30000). * Packets injected by a handle are then diverted to the next priority handle, and so on (Default: 0).
Restart TSplus Advanced Security service to apply this setting.
Value: 0



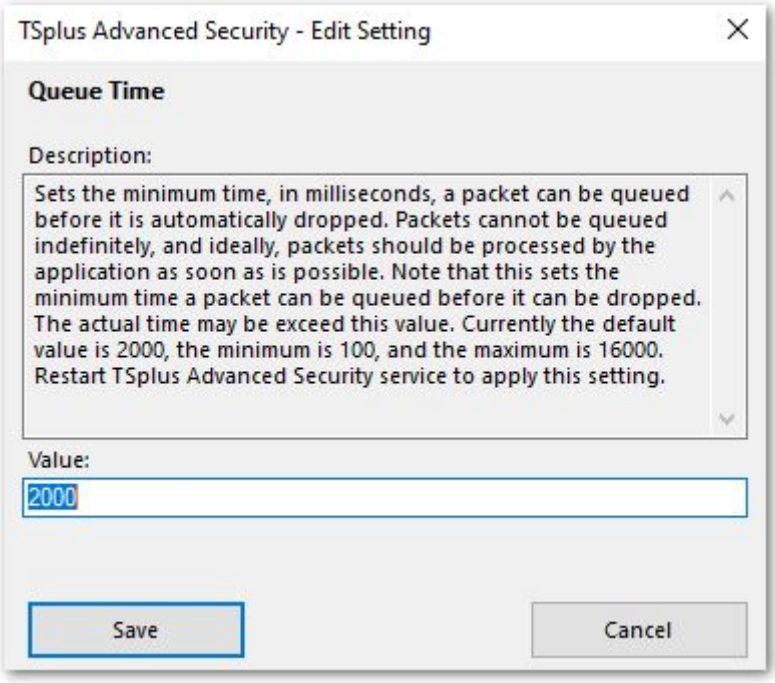
Queue Length
Sets the maximum length of the packet queue for TSplus Advanced security built-in firewall.
The default value is 4096, the minimum is 32, and the maximum is 16384.
Restart TSplus Advanced Security service to apply this setting.
Value: 4096



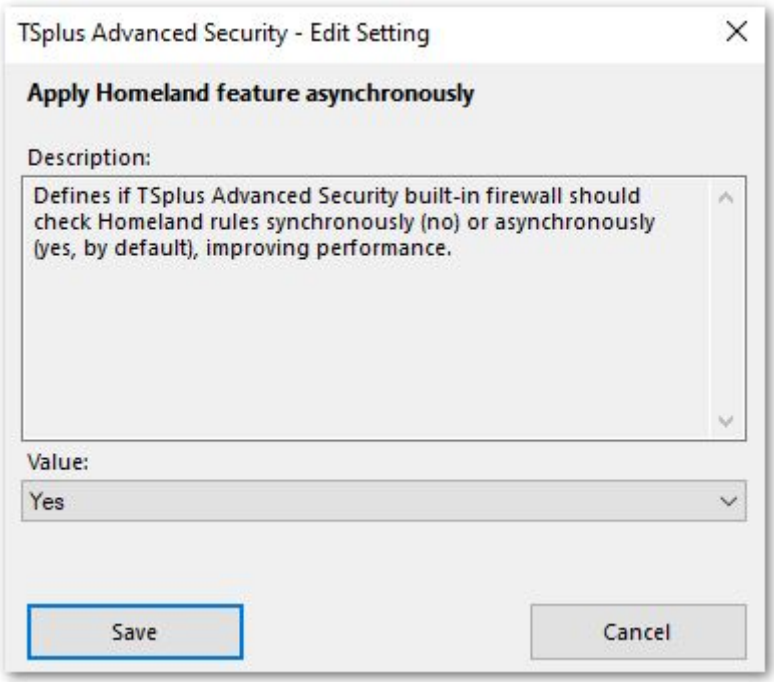
Queue Size
Sets the maximum number of bytes that can be stored in the packet queue for TSplus Advanced Security built-in firewall.
Currently the default value is 4194304, the minimum is 65535, and the maximum is 33554432.
Restart TSplus Advanced Security service to apply this setting.
Value: 4194304



Queue Time
Sets the minimum time, in milliseconds, a packet can be queued before it is automatically dropped.
Packets cannot be queued indefinitely, and ideally, packets should be processed by the application as soon as is possible.
Note that this sets the minimum time a packet can be queued before it can be dropped.
The actual time may exceed this value.
Currently the default value is 2000, the minimum is 100, and the maximum is 16000.
Restart TSplus Advanced Security service to apply this setting.
Value: 2000



Apply Homeland feature asynchronously
Defines if TSplus Advanced Security built-in firewall should check Homeland rules synchronously (no) or asynchronously (yes, by default), improving performance.
Value: Yes


TSplus Advanced Security - Edit Setting
Apply Homeland feature asynchronously
Description:
Defines if TSplus Advanced Security built-in firewall should check Homeland rules synchronously (no) or asynchronously (yes, by default), improving performance.
Value:
Yes
Save
Cancel