

How to block Psiphon 3

Users can use Psiphon to bypass restrictive policies configured on a Fortigate.

Psiphon is a circumvention system that uses a combination of secure communication and obfuscation technologies (VPN, SSH, and HTTP Proxy).

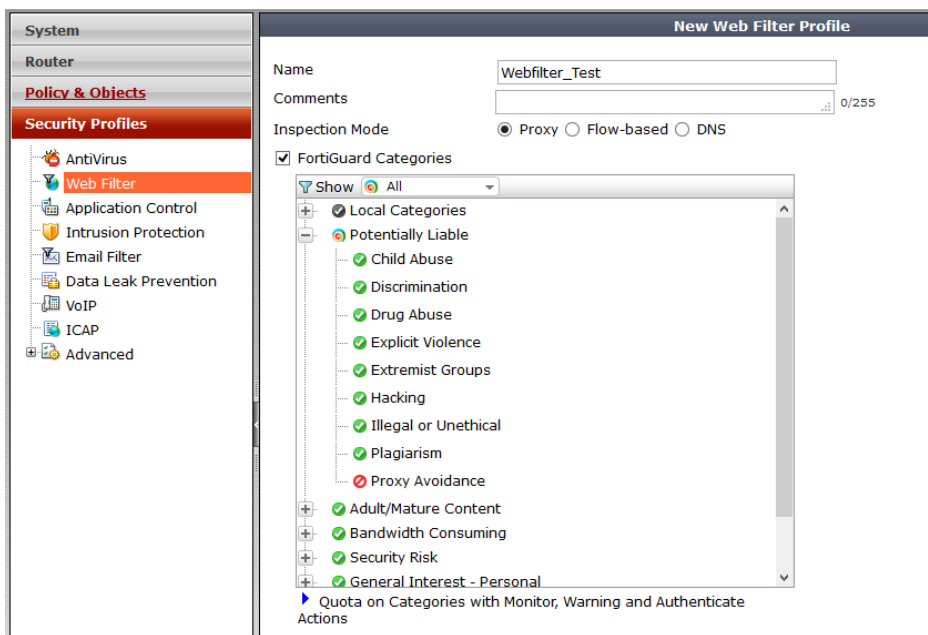
The Psiphon codebase is developed and maintained by Psiphon Inc which operates systems and technologies designed to assist users to bypass the content-filtering systems.

In this document we will show how to block Psiphon 3 as shown on a FortiGate running FortiOS 5.2.

Configuration Steps

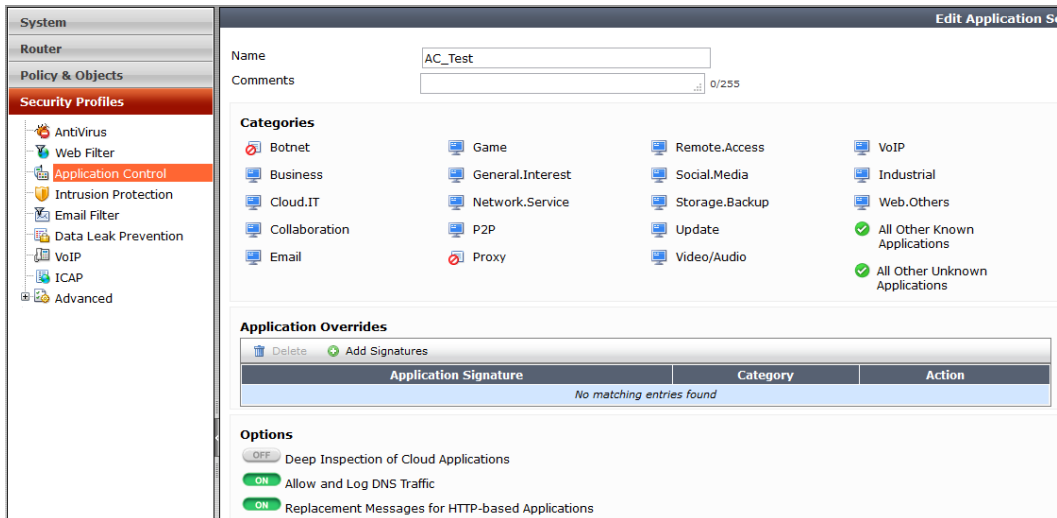
Step 1 -- Configure a WebFilter profile;

- Assign WebFilter_Test as a profile name.
- Enable Fortiguard Categories
- Go to Potentially Liable → Proxy Avoidance click right button and select Block



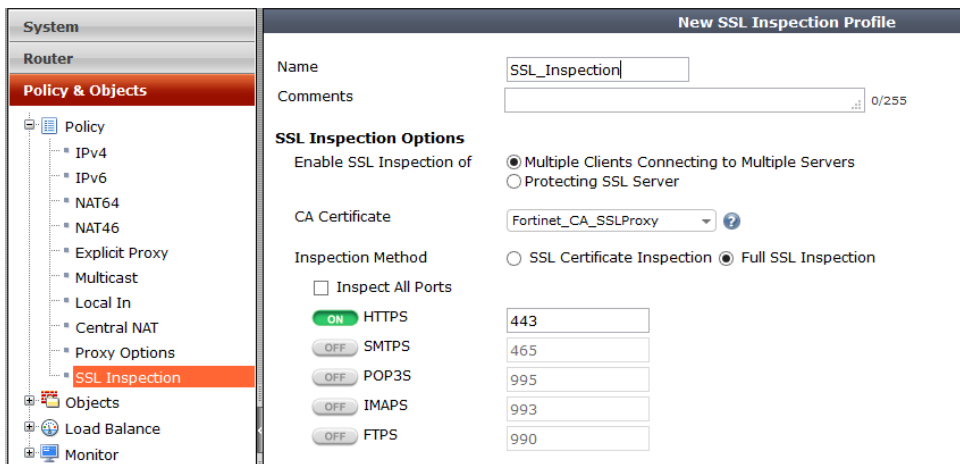
2) Configure an Application Control Sensor

- Assign sensor the name AC_Test
- Select Botnet and Proxy, right button and select Block



3) Configure an SSL Inspection profile which uses Full SSL Inspection (Or use the Factory default SSL profile “Deep-inspection”)

- Assign the profile the name SSL_Inspection
- Enable: HTTPS 443



4) Create a firewall policy and apply the security profiles defined in the previous three steps.

- Web Filter: WebFilter_Test
- Application Control: AC_Test
- SSL Inspection: SSL_Inspection

System

Router

Policy & Objects

- Policy
 - IPv4
 - IPv6
 - NAT64
 - NAT46
 - Explicit Proxy
 - Multicast
 - Local In
 - Central NAT
 - Proxy Options
 - SSL Inspection
- Objects
- Load Balance
- Monitor

Security Profiles

Incoming Interface: +

Source Address: +

Source User(s):

Source Device Type:

Outgoing Interface: +

Destination Address: +

Schedule:

Service: +

Action:

Firewall / Network Options

NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

Web Cache

WAN Optimization

Security Profiles

AntiVirus

Web Filter +

Application Control +

IPS

Email Filter

DLP Sensor

VoIP

ICAP

Proxy Options

SSL Inspection + ?

Verification:

- Open Psiphon in the Windows Laptop.
- Try connecting selecting any of the three options; SSH+, VPN and SSH
- Psiphon fails to connect.

