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 obsfucation 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 \rightarrow Proxy Avoidance click right button and select Block



2) Confgure an Application Control Sensor

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

System				Edit Application S
Router	Name	AC_Test		
Policy & Objects	Comments		0/255	
Security Profiles	Categories Ø Botnet Business Cloud.IT Collaboration Email	 Game General.Interest Network.Service P2P Proxy 	 Remote.Access Social.Media Storage.Backup Update Video/Audio 	 VoIP Industrial Web.Others All Other Known Applications All Other Unknown Applications
a Mavanced	Application Overrides			
	👕 Delete 🛛 Add Signa	atures		
	A	pplication Signature	Category	Action
		no ma	tening entries round	
	Options			
	Deep Inspection of	Cloud Applications		
	Allow and Log DNS	Traffic		
	Replacement Mess	ages for HTTP-based Applications		

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

System		New SSL Inspection Profile		
Router Policy & Objects	Name	SSL_Inspection		
Policy IPv4	SSL Inspection Options Enable SSL Inspection of	Multiple Clients Connecting to Multiple Servers Protecting SSL Server		
■ NAT64 ■ NAT46	CA Certificate	Fortinet_CA_SSLProxy		
 Explicit Proxy Multicast 	Inspection Method	\bigcirc SSL Certificate Inspection $\textcircled{\ensuremath{\mathbb{O}}}$ Full SSL Inspection		
Central NAT	TTPS	443		
Proxy Options	OFF SMTPS	465		
SSL Inspection	OFF POP3S	995		
🗂 Objects	OFF IMAPS	993		
🚯 Load Balance 🗐 Monitor	OFF FTPS	990		

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



Verification:

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

