

Configuring Fortigate for IPCS connections

To route inbound traffic from your iPCS Application or SSL Enabled PCS Phone / Navigate Software, you will need two things;

- 🕒 VIP (Virtual IP Object)
- 🕒 WAN to LAN IPv4 Policy

The VIP would normally be configured as follows;

The screenshot shows the configuration interface for a Virtual IP Object. The Name field is set to "iPCS Server TCP 5001". The Interface is set to "FIBRE WAN 1 (wan1)". The Type is set to "Static NAT". The External IP Address/Range is set to "WAN IP Address" and the Mapped IP Address/Range is set to "SSL Gateway IP Address". The Port Forwarding section is enabled, and the Protocol is set to "TCP". The External Service Port and Map to Port fields are both set to "5001". A red box highlights the port forwarding section, and a note says "Change to port 5000 if appropriate". The OK and Cancel buttons are visible at the bottom.

Name: iPCS Server TCP 5001
Comments: 25/255
Color: Change

Network

Interface: FIBRE WAN 1 (wan1)

Type: Static NAT

External IP Address/Range: WAN IP Address - WAN IP Address

Mapped IP Address/Range: SSL Gateway IP Address - SSL Gateway IP Address

Optional Filters:

Port Forwarding:

Protocol: **TCP** UDP SCTP ICMP

External Service Port: 5001 - 5001

Map to Port: 5001 - 5001

Change to port 5000 if appropriate

OK Cancel

Replace the fields containing WAN IP Address with the public IP address you are sending IPCS traffic to, and replace the field containing SSL Gateway IP Address, with your SSL Gateway IP address.

If you are using a different SSL Port than 5001, simply replace the External Service Port and Map to Port fields with your desired port number, for instance 5000.

Next, you will need a WAN to LAN IPv4 Policy, which would normally be configured as follows;

Edit Policy

Name: iPCS Inbound

Incoming Interface: SD-WAN **Interface bringing in your Internet connection**

Outgoing Interface: VOICE LAN (VoIP) **Interface routing to your SSL Gateway Server**

Source: WAN-SDWAN **Source Address Object to reflect where connections are coming from, for instance 0.0.0.0/0 which would be anywhere from the Internet, which is appropriate for iPCS connections.**

Destination: iPCS Server TCP 5001 **The VIP Object you just created**

Schedule: always

Service: ALL

Action: ACCEPT DENY LEARN IPsec

Firewall / Network Options

NAT: Do not enable NAT, as this is done via the VIP Object

Proxy Options: default

Security Profiles

AntiVirus:

Web Filter:

DNS Filter:

Application Control:

IPS:

Anti-Spam:

Web Application Firewall:

SSL Inspection:

Logging Options

Log Allowed Traffic: Security Events All Sessions

Comments: 0/1023

Enable this policy:

OK **Cancel**

For outbound traffic, you just need an IPv4 LAN to WAN Policy similar to the following;

Edit Policy

Name	iPCS Outbound
Incoming Interface	VOICE LAN (VoIP) Interface routing traffic from your SSL Gateway
Outgoing Interface	SD-WAN Interface connected to your Internet connection
Source	SSL Gateway Server IPv4 Address Object identifying your SSL Gateway Server
Destination	WAN-SDWAN IPv4 Address Object identifying anywhere on the Internet
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN <input type="checkbox"/> IPsec

Firewall / Network Options

NAT	<input checked="" type="checkbox"/>	Ensure NAT is enabled, and if you have multiple WAN IP addresses, that you use a Dynamic IP Pool to NAT to the correct IP address
IP Pool Configuration	Use Outgoing Interface Address <input type="checkbox"/> Use Dynamic IP Pool <input type="checkbox"/>	
Preserve Source Port	<input type="checkbox"/>	
Proxy Options	PRX default	

Security Profiles

AntiVirus	<input type="checkbox"/>
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>
Anti-Spam	<input type="checkbox"/>
Web Application Firewall	<input type="checkbox"/>
SSL Inspection	<input type="checkbox"/>

Logging Options

Log Allowed Traffic	<input type="checkbox"/> Security Events <input checked="" type="checkbox"/> All Sessions
Comments	<input type="text" value="Write a comment..."/> 0/1023
Enable this policy	<input checked="" type="checkbox"/>

OK **Cancel**

Fortigate - Disabling SIP ALG

The following documentation describes how SIP ALG can be disabled on a Fortigate UTM Appliance. This is applicable when forwarding SIP trunks to a SpliceCom SV1000.

1. Open the Fortigate CLI from the dashboard.
2. Enter the following commands in FortiGate's CLI:
3. **config system settings**
4. **set sip-helper disable**
5. **set sip-nat-trace disable**
6. reboot the device
7. Reopen CLI and enter the following commands – do not enter the text after //:
8. **config system session-helper**
9. **show** //locate the SIP entry, usually 12, but can vary.
10. **delete 12** //or the number that you identified from the previous command.
11. Disable RTP processing as follows:
12. **config voip profile**
13. **edit default**
14. **config sip**
15. **set rtp disable**
16. **end**
17. At the hash prompt, type in **config system settings** and press return.
18. Next, enter **set default-voip-alg-mode kernel-helper-based** and press return.
19. Next, type **end** and press return
20. Go back to the dashboard and backup the configuration
21. From the dashboard, select the option to reboot the Fortigate.
22. When the Fortigate boots back up, SIP ALG will be disabled.