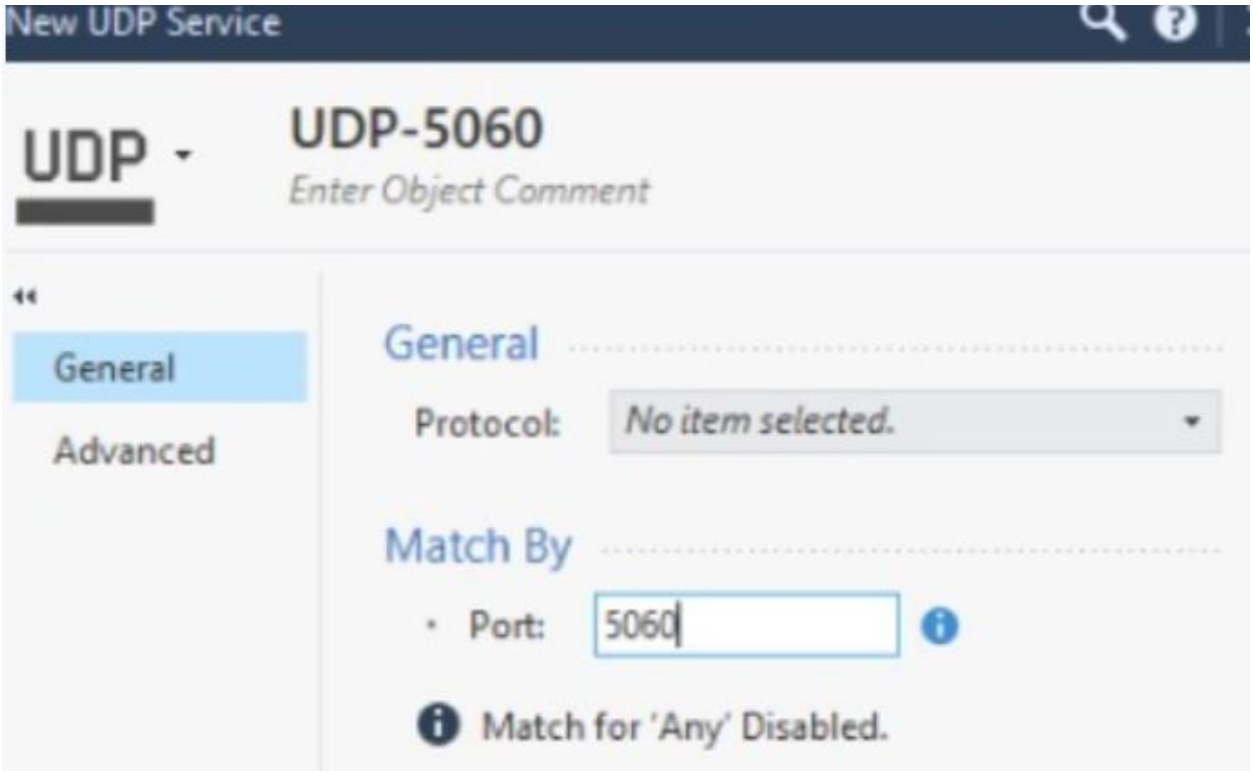
PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/

VOIP can cause a lot of troubles passing for firewalls, including Check Point that execute SecureXL, Deep Inspections. So during my jorney of 3 years working with Check Point I decide share my own tips that I set on my personal notes.

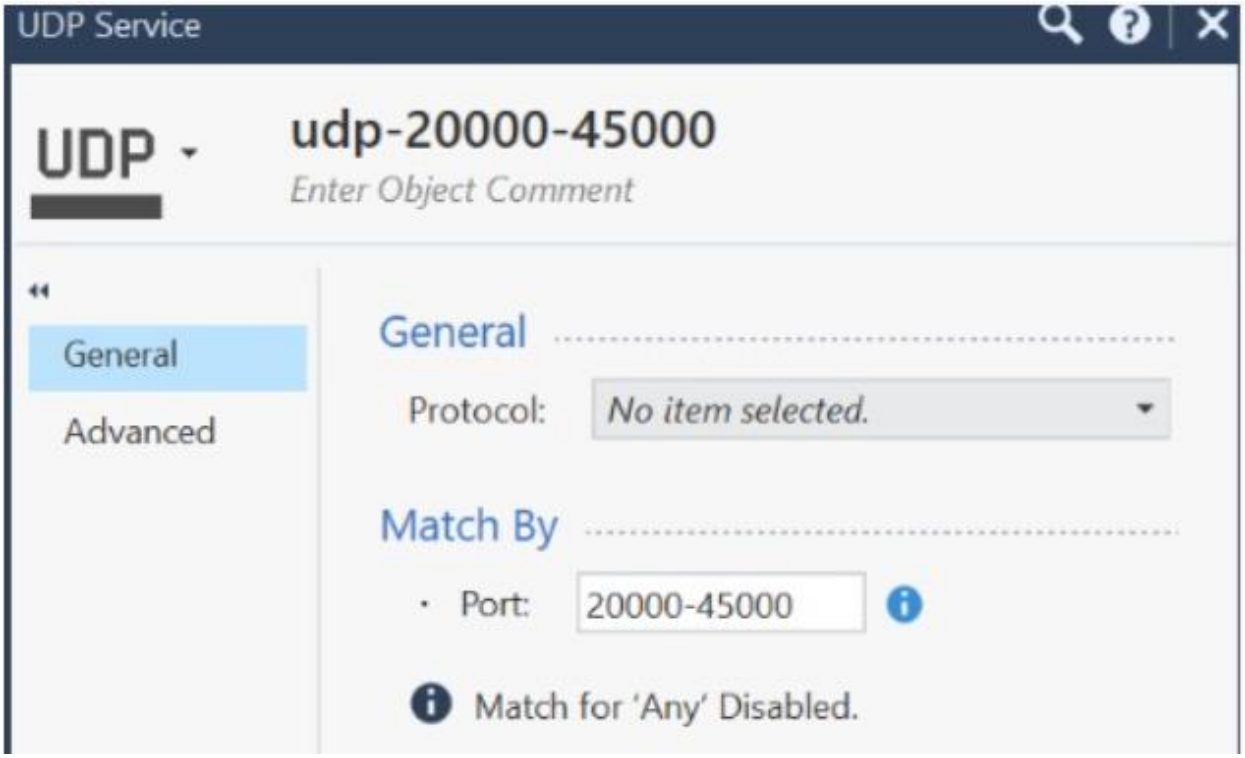
1 - The default Check Point objects can trigger deep inspection inspections (those marked with Protocol).

Create a new object with only the port specified, as shown in the example below, without selecting anything under General > Protocol.

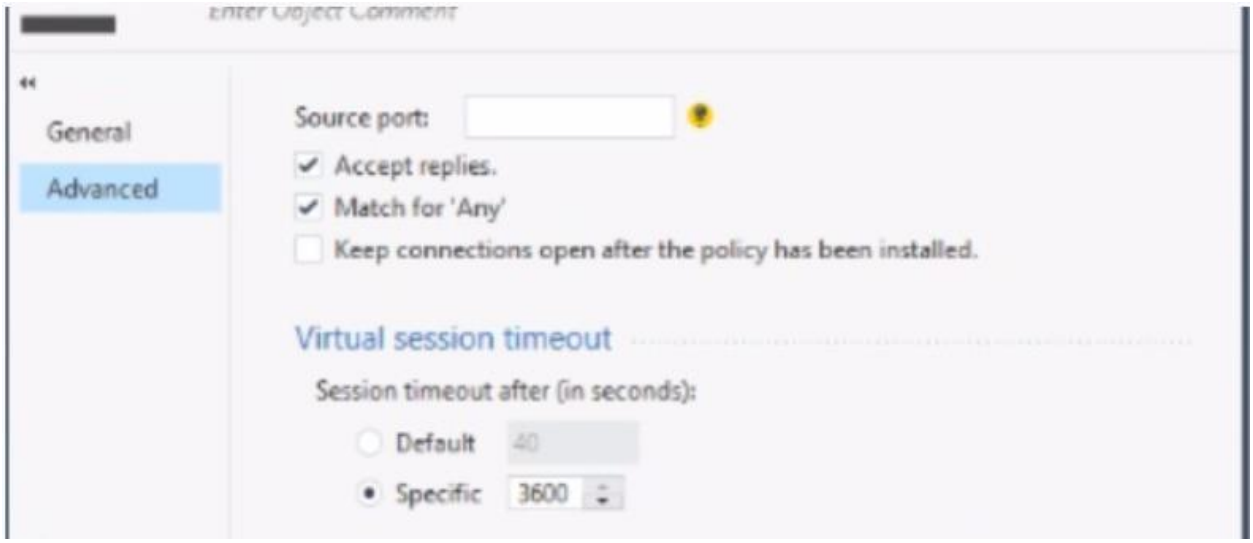


2- To pass voice via RTP, a range of high ports is used. Simply create the object and include the dash between the range. Also, make sure not to select Protocol in the General field.

PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/



3 - Increase the default session timout of some udp or tcp port can be necessary some times. For example for udp 5060 can be necessary have more than 40 seconds. Do this on Advanced inside your service object.

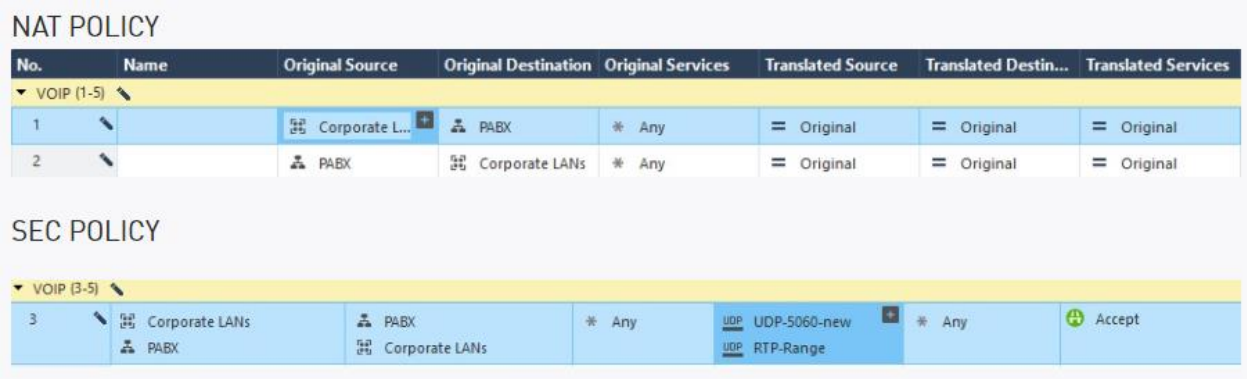


PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/

4 - It is common in VOIP to need to create bidirectional rules, especially for UDP traffic. So, if you are handling UDP voice traffic, or in large IPsec site-to-site scenarios where both sides need to send and receive traffic, create bidirectional NAT and security rules as shown in the example below:

Note: There are certain topologies where this may not be necessary, so evaluate your scenario using the VOIP Admin Guide for your version, and check the section "Important Information About Creating SIP Security Rules." link bellow:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_VoIP_AdminGuide/Topics-VOIPG/207846.htm



NOTE: NAT rules using masquerade types can cause issues; if possible, it's advisable to avoid them.

5 - Even after following all the steps, you may still encounter some cases of deep inspections. In such cases, it's worth creating fast_accel rules for the PBX IP. I usually make them bidirectional, as shown in the examples below:

SecureXL Fast Accelerator (fw fast_accel) for R80.20 and above

PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/

https://support.checkpoint.com/results/sk/sk156672

sk156672 shows examples of fast_accel rules.

NOTE: You need enable fast_accel first with **fw ctl fast_accel enable**

You can create the rule pointing to a network, in which case you need to include the subnet mask:

```
fw ctl fast_accel add 1.1.1.1 2.2.2.0/24 80 6
```

You can specify the network in either the source or destination. (to be bidirectional)

You can also create rules in the following ways:

```
fw ctl fast_accel add any 2.2.2.2 any any
```

```
fw ctl fast_accel add 2.2.2.2 any any any
```

Note: The rule name must use ONLY LETTERS and no special characters.

6 - In the PBX, configure NAT=yes.

This is necessary if there is NAT configuration in the VPN tunnel's phase 2 to resolve any overlap, or if you are hiding any network for any reason in phase 2. It is also applicable if you need to handle VOIP traffic outside of an IPsec site-to-site tunnel.

PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/

7 - If you continue to have difficulty establishing a UDP connection for SIP, consider switching to TCP on the PBX.

Also, check if the client can establish communication on TCP 5060 instead of UDP 5060, especially if the client does not have DTMF (Dual-Tone Multi-Frequency) activated in VOIP.

Add the line `transport=tcp` to the configuration.

NOTE: request for the VOIP team, bellow is just an example.

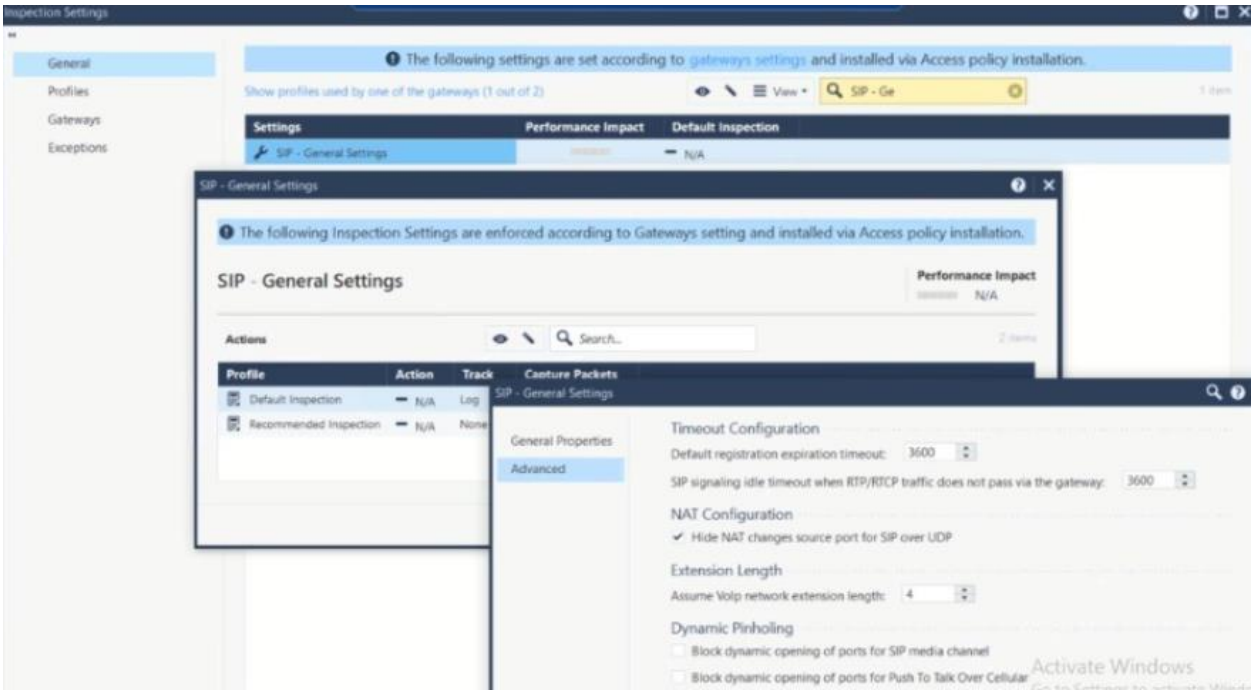
PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/

8 -

- VoIP SIP issues after upgrading Security Gateway to version R80.40 or higher with Hide NAT configured

https://support.checkpoint.com/results/sk/sk176286

PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/



9 - AS my last read the VOIP ATRG, and other references that Check Point have for VOIP, but my tips are here for all now.

Here are some useful resources for VOIP troubleshooting and configuration with Check Point:

- **ATR VOIP**: SK95369
- **SIP calls cannot be established after installing Check Point Security Gateway between SIP phones and SIP server**: SK113503
- **How to disable 'fw early SIP nat' chain / SIP inspection**: SK65072
- **Check Point Active Streaming (CPAS) and Passive Streaming Layer (PSL)**: SK44788
- **Important Information About Creating SIP Security Rules**: VoIP Admin Guide (including how to create rules)
- **Community Link with a good example of VOIP troubleshooting**: Community Example

PDF created by ISRAEL FERREIRA DA SILVA
Linkedin: https://www.linkedin.com/in/israel-ferreira-9a410bb5/

Best Regards