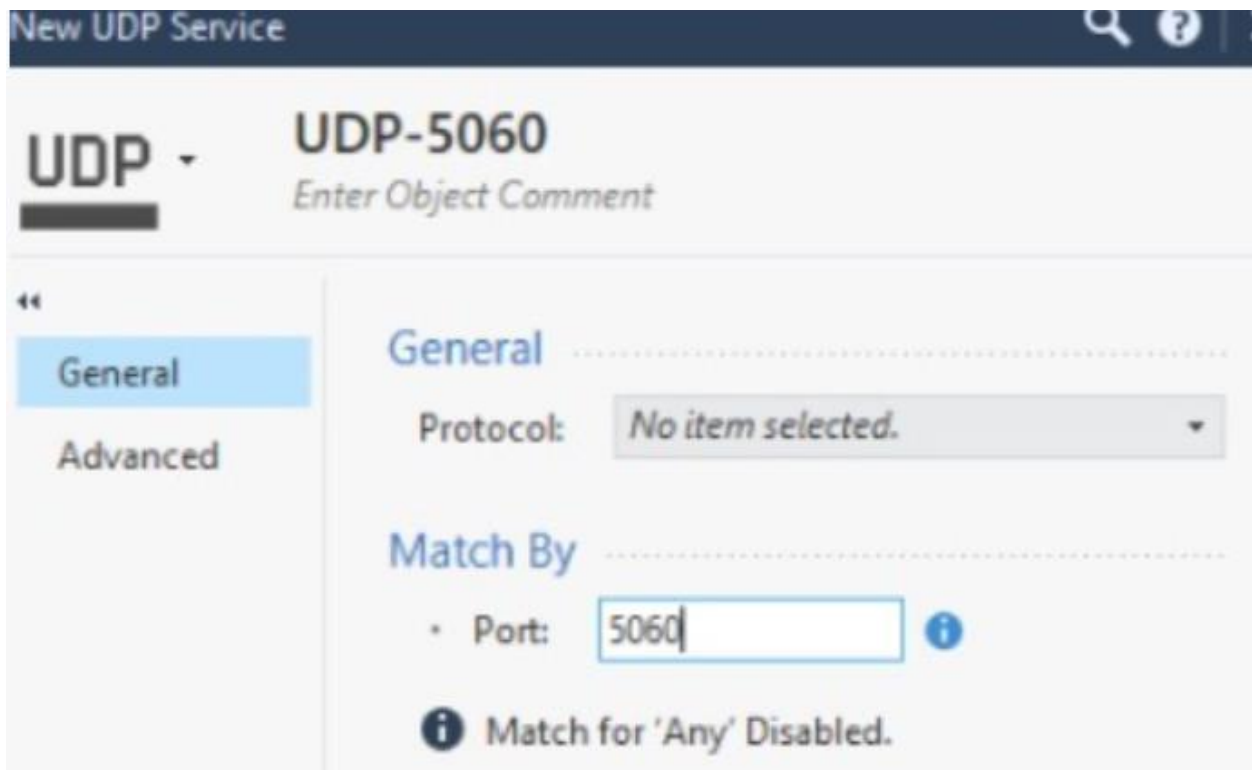


VOIP can cause a lot of troubles passing for firewalls, including Check Point that execute SecureXL, Deep Inspections. So during my journey of 3 years working with Check Point I decide share my own tips that I set on my personal notes.

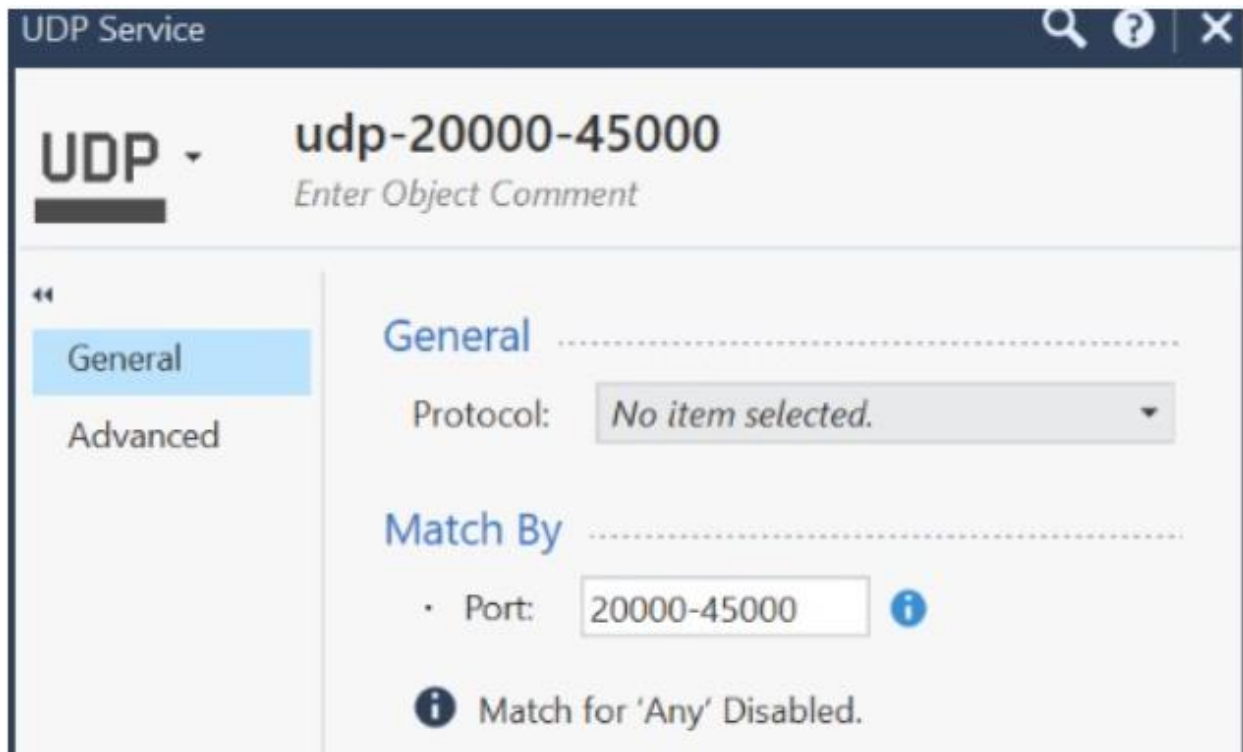
**1 - The default Check Point objects can trigger deep inspection inspections (those marked with Protocol).**

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

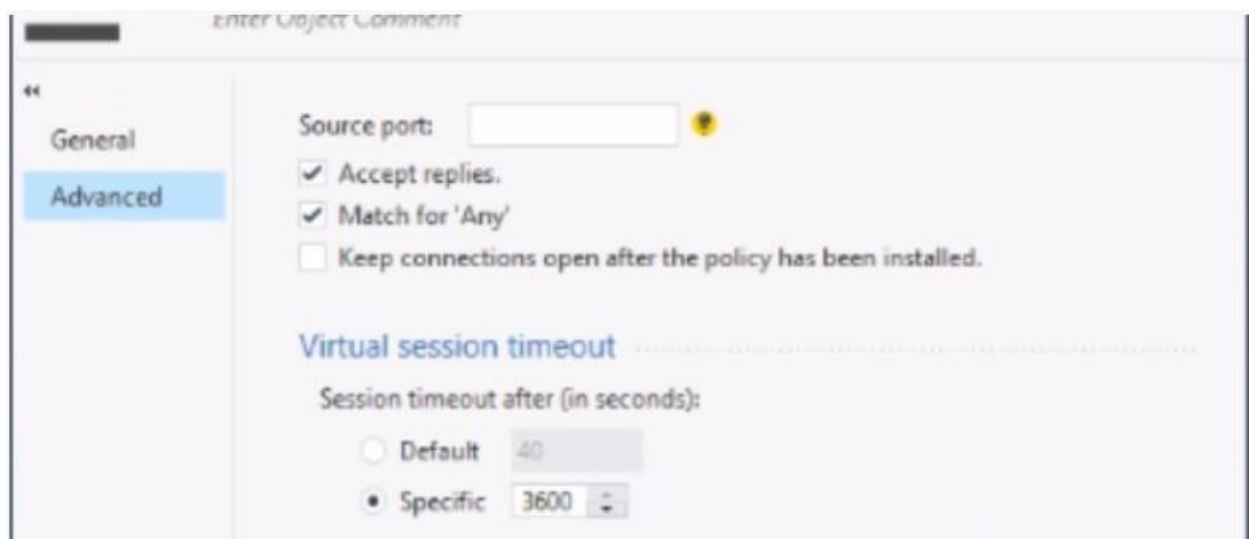


The screenshot shows the 'New UDP Service' configuration window in the Check Point management console. The title bar reads 'New UDP Service'. Below the title bar, the object name 'UDP' is selected from a dropdown menu, and the specific object name 'UDP-5060' is displayed. A text field for 'Enter Object Comment' is present. On the left side, there are two tabs: 'General' (which is active and highlighted in blue) and 'Advanced'. In the 'General' tab, the 'Protocol' field is a dropdown menu currently showing 'No item selected.'. Below this, the 'Match By' section has a 'Port' field with the value '5060' entered. An information icon (i) is next to the port field. At the bottom of the 'Match By' section, there is a message: 'Match for 'Any' Disabled.' with an information icon (i).

**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.**



**3 - Increase the default session timeout 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.**



**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 below:

[https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP\\_R81\\_VoIP\\_Admin\\_Guide/Topics-VOIPG/207846.htm](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_VoIP_Admin_Guide/Topics-VOIPG/207846.htm)

NAT POLICY							
No.	Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services
▼ VOIP (1-5)							
1		Corporate L...	PABX	* Any	= Original	= Original	= Original
2		PABX	Corporate LANs	* Any	= Original	= Original	= Original

SEC POLICY							
▼ VOIP (3-5)							
3	Corporate LANs PABX	PABX Corporate LANs	* Any	UDP-5060-new UDP RTP-Range	* Any	Accept	

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

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

sk156672 shows examples of fast\_accel rules.

```
[Expert@CPF01:0]# fw ctl fast_accel show_table
----- FIREWALL FAST ACCEL TABLE -----
#      Source IP      Destination IP      D-Port      Protocol      Hit count
-----
```

**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.



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.

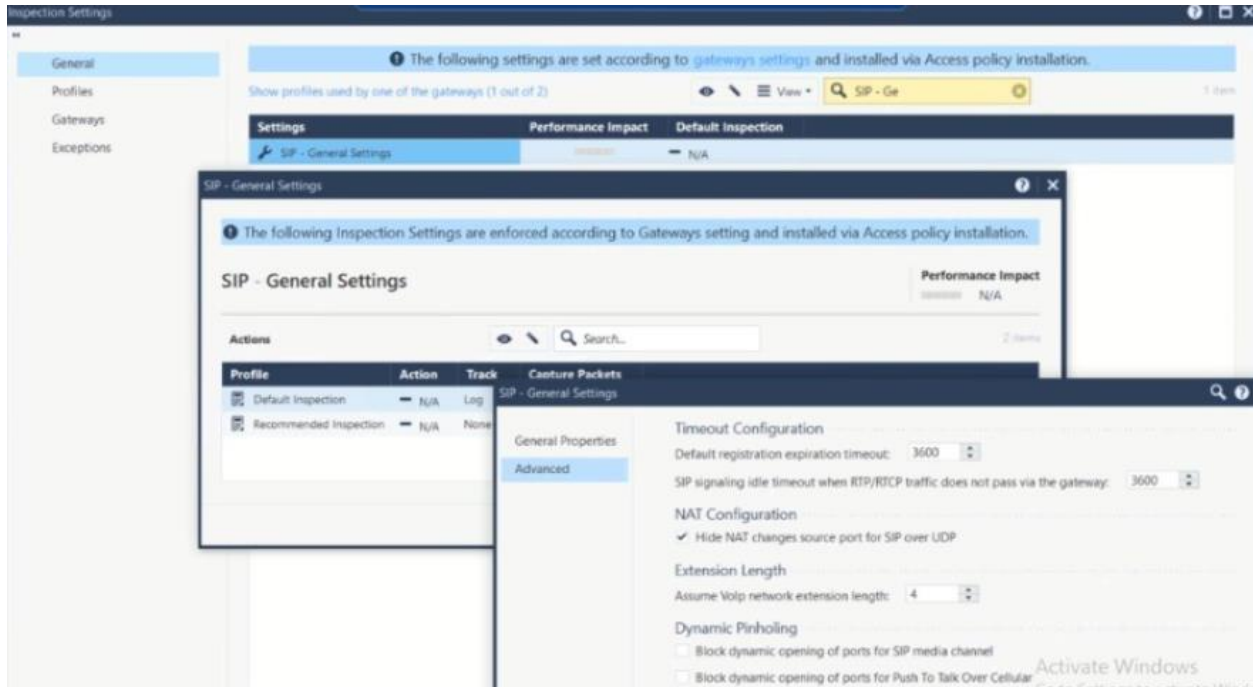
NOTE: request for the VOIP team, bellow is just an example.

The screenshot shows a configuration page for SIP. At the top, there are three tabs: 'Geral', 'Regras de Manipulação de Número Discado', and 'sip Configurações'. Under 'sip Configurações', there are two sub-tabs: 'Sainte' and 'Entrada'. The main content area is divided into two sections: 'Nome do Tronco' and 'Detalhes do PEER'. The 'Nome do Tronco' field contains the text 'epservice'. The 'Detalhes do PEER' section contains a list of configuration parameters: 'type=friend', 'host=10.190.0.97', 'fromdomain=10.190.0.97', 'disallow=all', 'allow=ulaw&alaw', 'qualify=no&yes', 'context=incoming', 'rtptimeout=600', 'insecure=invite.port', and 'nat=yes'. Below this list, the parameter 'transport=tcp' is also visible.

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>



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