

## How to configure VOIP with TWC/Spectrum

---

### Details on the TWC/Spectrum SIP implementation:

The Time Warner Cable Business Class (TWCBC) SIP Trunks product is an IP-based, voice only trunk that uses Session Initiation Protocol (SIP) to connect an IP PBX to the PSTN. The IP PBX uses SIP to exchange signaling information with the service provider and to deliver and receive voice in IP packets.

### WHAT IS THE PROBLEM?

The SIP device will initiate a connection over UDP-5060 to the external TWC/Spectrum SIP server

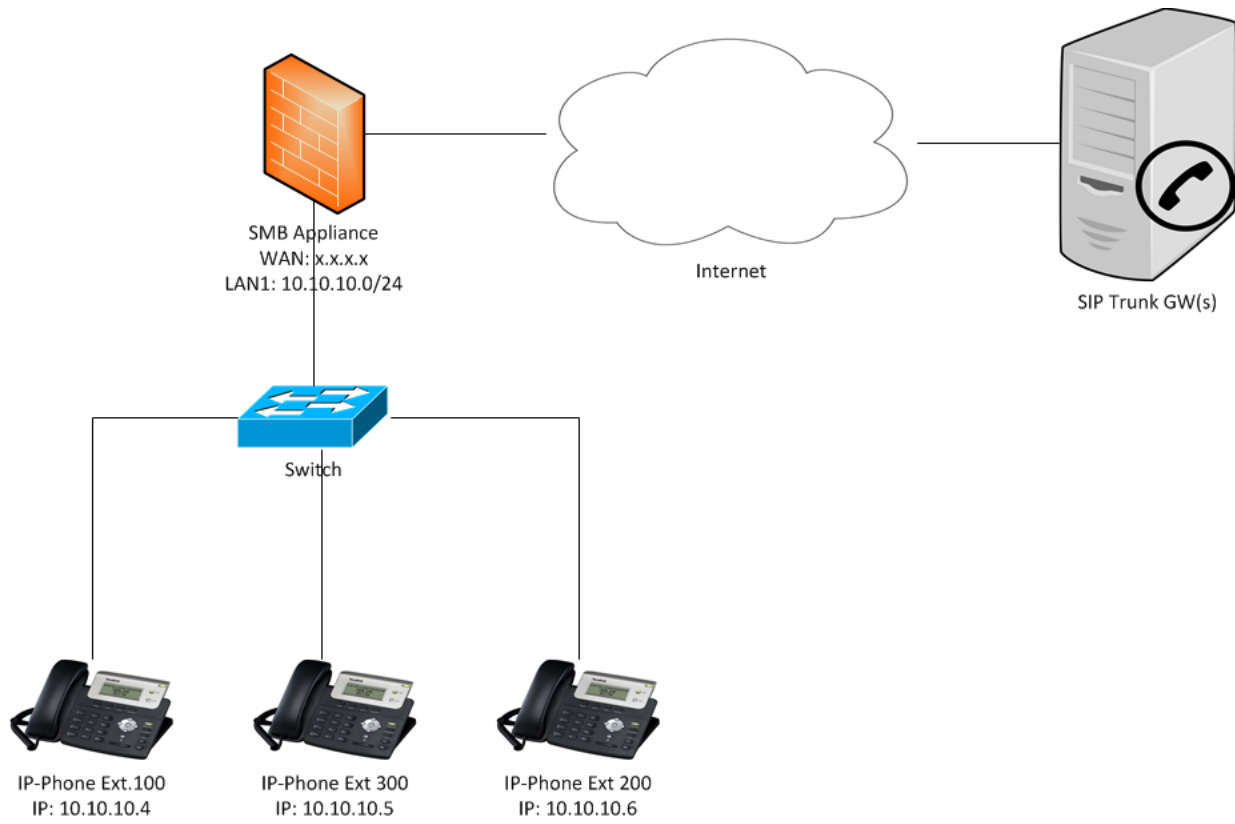
The device registers with the SIP server and negotiates a port specific to this device (note: this registration occurs every 30-180 seconds)

The SIP server will then use the negotiated port to communicate with the SIP device

**IMPORTANT NOTE:** the external SIP server then sends keep-alive packets to the SIP device. These keep alive packets are dropped (as they should be) by the firewall as out-of-state packets. This will break the connection and no calls will come into the SIP device. Calls to external systems make work, as the SIP device opens a new UDP connection.

# WHAT IS THE SOLUTION?

- Topology



- Configure the following:
  - VoIP Provider IP range (if it has several signaling IP ranges - configure them all as Network Objects, then assign them all to a new network object group, ex. VoIP-Provider)
  - Phones IP range (configure it as Network Object, ex. IP-Phones)
  - Create 1 Incoming Rule: From VoIP-Provider To IP-Phones at service SIP\_UDP (depends on the VoIP Provider Specification - this is the most common) action allow.

In Gaia Portal: Access Policy -> Policy, under 'Incoming, Internal and VPN traffic'

**Incoming, Internal and VPN traffic**

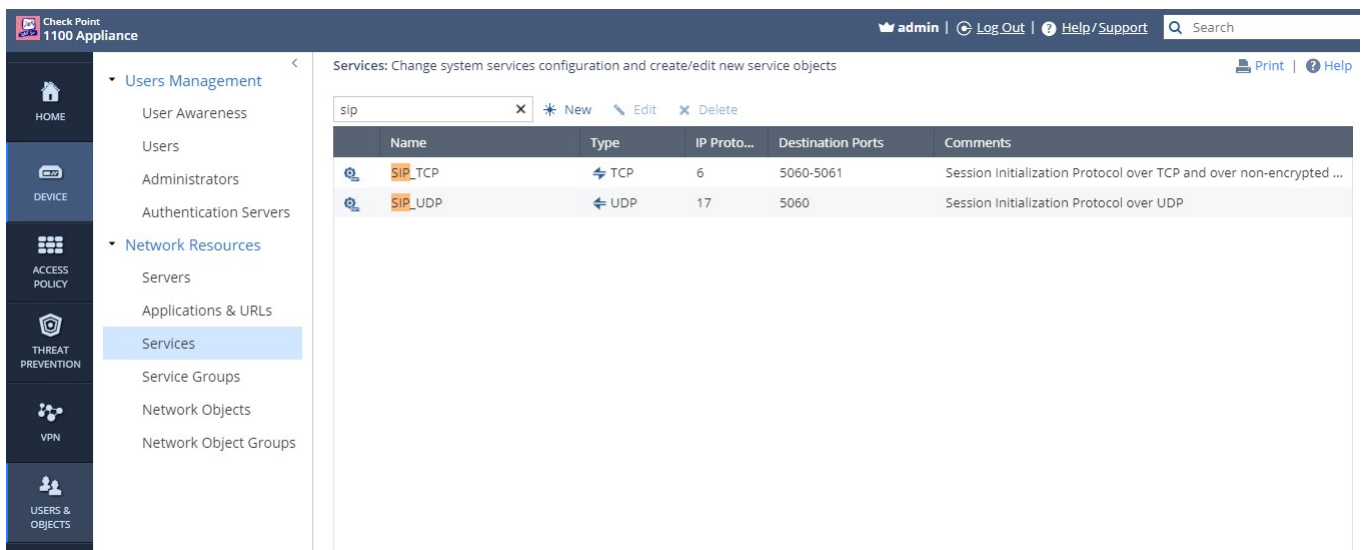
New Edit Delete Enable Clone

No.	Source	Destination	Service	Action	Log
Manual Rules					
1	VoIP-Provider	IP-Phones	SIP_UDP	Accept	Log

This is similar to the "fw early SIP nat chain" issue detailed in SK 65072.  
In order to disable early SIP inspection on Embedded GAIA:

Go to Users and Objects...Services...search for SIP\_UDP...Advanced tab...select "keep connections open after policy has been installed.

-- **And check the option box for 'disable inspection for this service'.**



Check Point 1100 Appliance | admin | Log Out | Help/Support | Search

Services: Change system services configuration and create/edit new service objects | Print | Help

sip [x] \* New Edit Delete

Name	Type	IP Proto...	Destination Ports	Comments
SIP_TCP	TCP	6	5060-5061	Session Initialization Protocol over TCP and over non-encrypted ...
SIP_UDP	UDP	17	5060	Session Initialization Protocol over UDP

Service

Advanced



**Note:** This is a system defined service. Some of the fields cannot be edited.

Name:

SIP\_UDP

Type:

UDP

Ports:

5060

Reset

Enter port numbers and/or port ranges separated by commas.  
For example: 1, 3, 5-8, 15

Comments:

Session Initialization Protocol over UDP



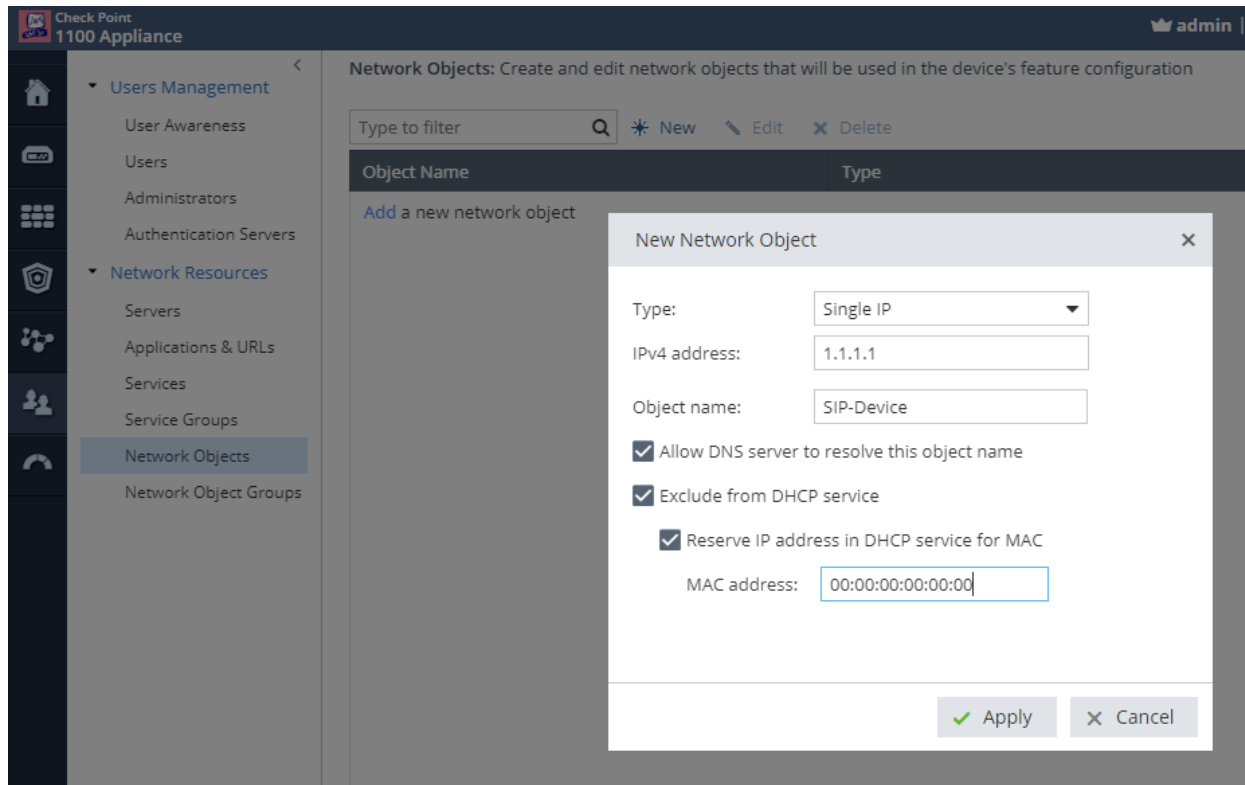
Disable inspection for this service

✓ Apply

✕ Cancel

Also note:

SIP devices may also need to be excluded from receiving a DHCP reservation. See below:



CONTACT US **Worldwide Headquarters** | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com  
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

