Oracle Contact Center Anywhere Network Setup

Definitions

Term	Definition
ALC	Lists that filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.
RTP	RTP is used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams (e.g., audio and video), RTCP is used to monitor transmission statistics and quality of service (QoS) and aids synchronization of multiple streams
SIP	Session Initiation Protocol
SIP ALG	This refers to a Firewall having the capability to do NAT using standard SIP protocols.
SIP Inspection	To support SIP calls through the security appliance, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well---known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user---data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

Overview

The type for voice is transferred as using the Real---Time Transport Protocol (RTP). The RTP download (“in”) stream are the voice packets sent from the Promero data center to the agent’s Softphone and the upstream or “out” packets that are sent from the agent’s Softphone to the Promero data center to be rebuilt and played back to the caller as the agent’s voice.

These are sent via the User Datagram Protocol (UDP) which is a faster and more efficient protocol (vs. TCP) for time---sensitive applications such as VoIP.

Firewall

Promero recommends that the Customer Firewall be configured to allow traffic using the TCP/ UDP ports listed below and source destination to or from any of Promero Data Center IP Address Ranges/Internet Domains listed below.

Promero IP Address Range

- 65.212.73.1-127
- 65.212.73.128-256

Promero Domain:

- www.promero.com
- Promero.com

SIP Firewall Note: Many firewalls with default inspect settings make changes to SIP/VoIP traffic. In most cases intrusive inspection by the Firewall changes the SIP VoIP traffic is unnecessary and may prevent VoIP from working correctly. Below is an example of SIP Inspection that should be turned off:

- SIP Inspection and Control
- SIP Access Layer Gateway (ALG)
- Strict Access Control List rules (ACL)

The customer's external Firewall, Session Border Controller (SBC), SIP Proxy and/or PC Firewall must have the following TCP/UDP ports open:

Port	TCP/UDP	Direction	Application
80	TCP	Outbound	HTTP
443	TCP	Outbound	HTTPS
5060	TCP/UDP	Inbound/Outbound	SIP
1024-65535	UDP	Inbound/Outbound	RTP

Figure 1

Checkpoint Specifics

1. Log into SmartDashboard as shown in Figure 1.

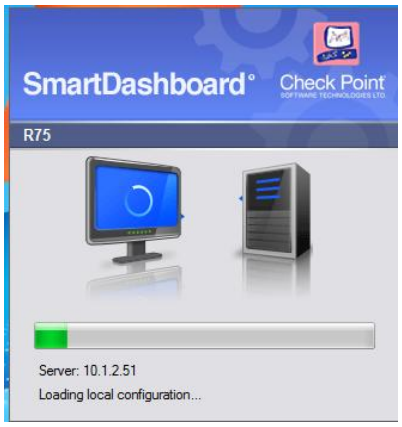


Figure 2

2. Select Manage then Services

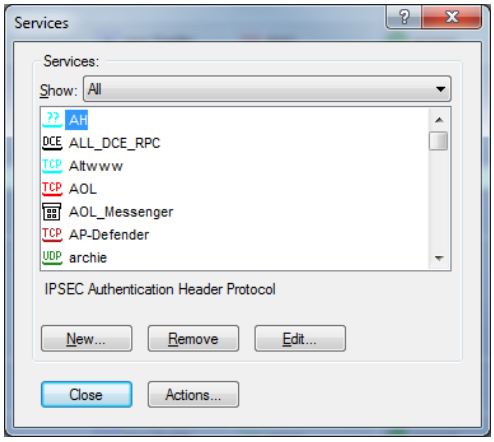


Figure 3

3. The first service to be added is SIP TCP.
4. Click New, TCP.
5. Name this Service something that is easily deciphered for example SIP5060T_No_Inspect

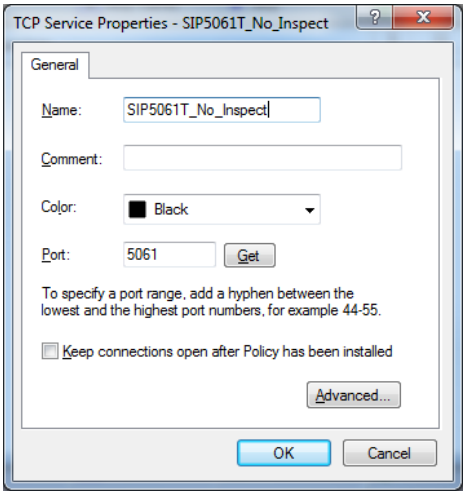
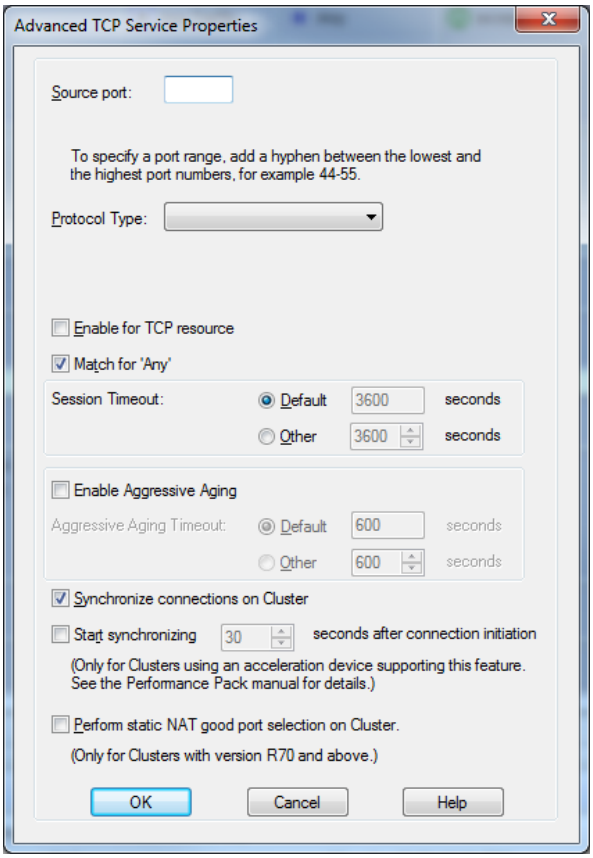


Figure 4

6. Specify Port 5060
7. Click Advanced.



a. Ensure the source port is empty
b. Ensure Match Any is enabled
c. Ensure Synchronize on Cluster is enabled
d. Click OK

8. Next add a Service for 5060 UDP, Manage Service, New, UDP
9. Name the Service something easy to decipher for example SIP5060U_No_Inspect

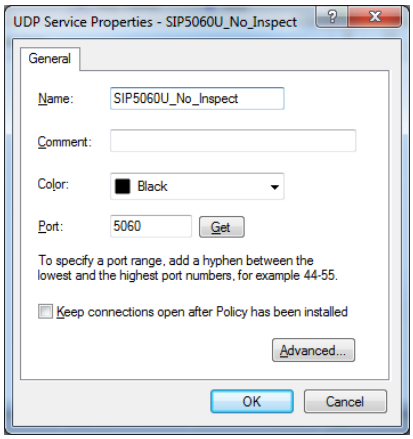


Figure 5

10. Click on Advanced

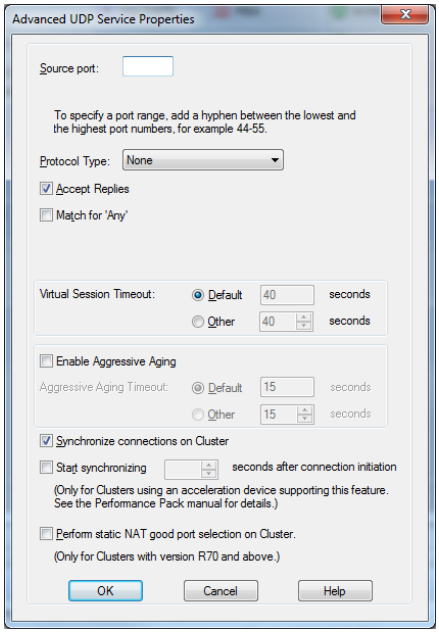


Figure 6

11. Configure as shown in Figure 5 above.
    a. Ensure the source port is empty
    b. Ensure Accept Replies is enabled
    c. Ensure Synchronize on Cluster is enabled
    d. Click OK
12. Next add a service for the RTP voice packets
13. Click on Manage, services, UDP

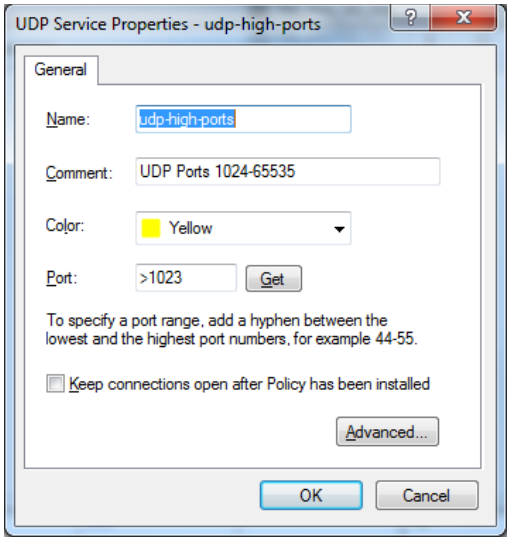


Figure 7

14. Name the service appropriately and enter the port range.
15. Click Advanced

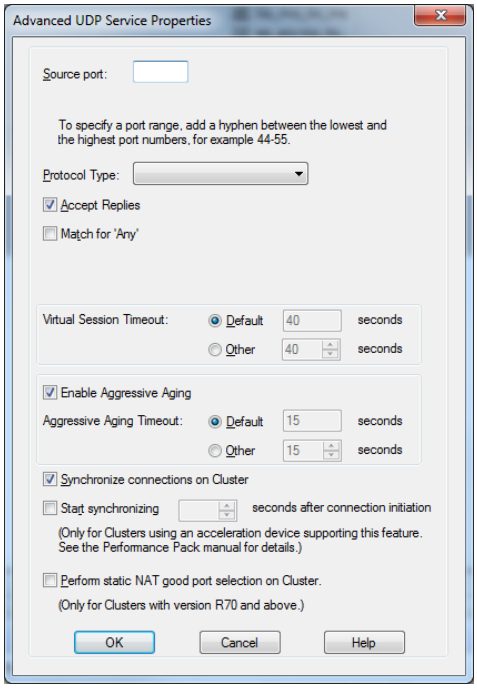


Figure 8

16. Make the selections as shown in Figure 7 above
17. Click OK
18. Next create a rule.
19. Add the 3 previous services to the rule
20. Set the action to Accept
21. Set logging for the rule
22. Add the Source and Destinations as defined on Page 2 of this document

23. Install the policy
24. Test SIP registration
25. Test SIP calls
26. If any difficulties are found, review the firewall logs in Checkpoint Tracker