Configuring the Sonicwall:

=====================

Since we don’t have a public IP to assign to the 3CX server, we will use a Many-to-One NAT configuration. In this scenario, the 3CX is reached via the Dell SonicWALL public IP address. (Hot Fix Required)

1. Create Services objects for TCP/UDP ports for which 3CX needs Port Forwarding

SecuredSIP (3CXSIPTLS) ports 5061 protocol: TCP

3CXRTP ports 9000-9255 protocol: UDP

3CX-TCP-5090 (3CXTUNNEL) ports 5090 protocol: TCP

3CX-UDP-5090 (3CXTUNNEL) ports 5090 protocol: UDP

3CXSIPUDP (3CXSIPUDP) ports 5060 protocol: UDP

MX\_SIP (3CXSIPTCP) ports 5060 protocol: TCP

SIP

SIP-TCP

1. Create the Service Group “3CX SIP Services“ (3CX Services) with all the above Service Objects as members
2. Create the Address Object “3CX SERVER” (3CX PBX) show the 3CX Phone System been located on the internal IP address XXX.XXX.XXX.XXX
3. Create NAT Policies for 3CX inbound and outbound connections
4. Add a NAT policy for outbound connections from the 3CX PBX

Original Source: 3CX SERVER (3CX PBX) or 3CXServer Private, 3CX-SSL Private, or 3CXSIP Private

Translate Source: WAN Interface IP

Original Destination: Any

Translate Destination: Original

Original Service: 3CXSIP services (Any)

Translate Service: Original

Inbound Interface: Any

Outbound Interface: X1 (replace X1 with the WAN Interface)

Enable NAT Policy: Checked

Edit the Advanced TAB and make sure check “Disable Source Port Remap”

1. Add a NAT policy for inbound connections to the 3CX PBX

Original Source: Any

Translate Source: Original

Original Destination: WAN Interface IP

Translate Destination: 3CX SERVER (3CX PBX), 3CXSIP Private or, or 3CXServer Private, 3CX-SSL Private,

Original Service: 3CXSIP Services (3CX Services)

Translate Service: Original

Inbound Interface: X1 (replace X1 with the WAN Interface) (Change this setting to Any If unmatched mapping error)

Outbound Interface: Any

Enable NAT Policy: Checked

Edit the Advanced TAB and make sure to check “Disable Source Port Remap”

1. Create the Firewall->Access Rule to allow access to the 3CX PBX direction WAN to LAN

Actions: Allow

From Zone: WAN

To Zone: LAN

Service: 3CXSIP Services (3CX Services)

Source: Any

Destination: WAN Interface IP

Users Allowed: All

Schedule: Always on

Comment: 3CX Inbound access

Enable logging: checked

Enable logging: checked

Allow Fragmented Packets: checked

Anything else: unchecked

1. Ensure that SIP Transformations and Consistent NAT are disabled

VOIP/Settings

General Setting -> Enable consistent NAT: unchecked

SIP Setting -> Enable SIP Transformations: unchecked

1. Run the 3CX Firewall Checker to validate the setup from the 3CX Phone System Management Console Settings >> Firewall Checker. All tested ports must return green / working.

Note- calls will be dropped for 5 minutes or until the firewall Checker finish.

References:

===================================================================================================================

<https://www.3cx.com/blog/voip-howto/3cx-firewall-checker-client/>

<https://www.3cx.com/blog/voip-howto/sonicwall-firewall-configuration/>

<https://www.3cx.com/docs/firewall-router-configuration-voip/>

<https://www.3cx.com/community/threads/unable-to-pass-firewall-check-v15-with-sonicwall.48270/#post-195190>

3CX Server

IP 192.168.0.100 XXX.XXX.XXX.XXX

webconsole: https://XXX.XXX.XXX.XXX:5001/

username: 192

password: <Password>

Office

Public IP XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX

Port Forwarding:

-Outgoing UDP 5060: Outgoing XXX.XXX.XXX.XXX:5060 UDP must be NAT to XXX.XXX.XXX.XXX:5060 UDP for packets the goes to the internet

-Incoming UDP 5060: Incoming to XXX.XXX.XXX.XXX:5060 UDP must be NAT to XXX.XXX.XXX.XXX:5060 UDP

-Port TCP 5061 if using secure SIP.

-Port UDP 9000-9255 for RTP.

-~~Port 9255-9500 for WebRTC~~ (Not installed in <ORGANIZATION>)

-~~Port 80 HTTP / 443 HTTPS for 3CXPhone Presence and HTTP provisioning.~~ (Not installed on <ORGANIZATION>)

WebRTC functionality

With the 3CX WebRTC Gateway feature you can share a WebRTC call link with anyone via chat or email allowing them to place a call from any open standards browser (Chrome, Firefox), directly to your extension,

without needing to install a client.

-Open ports 9255-9500