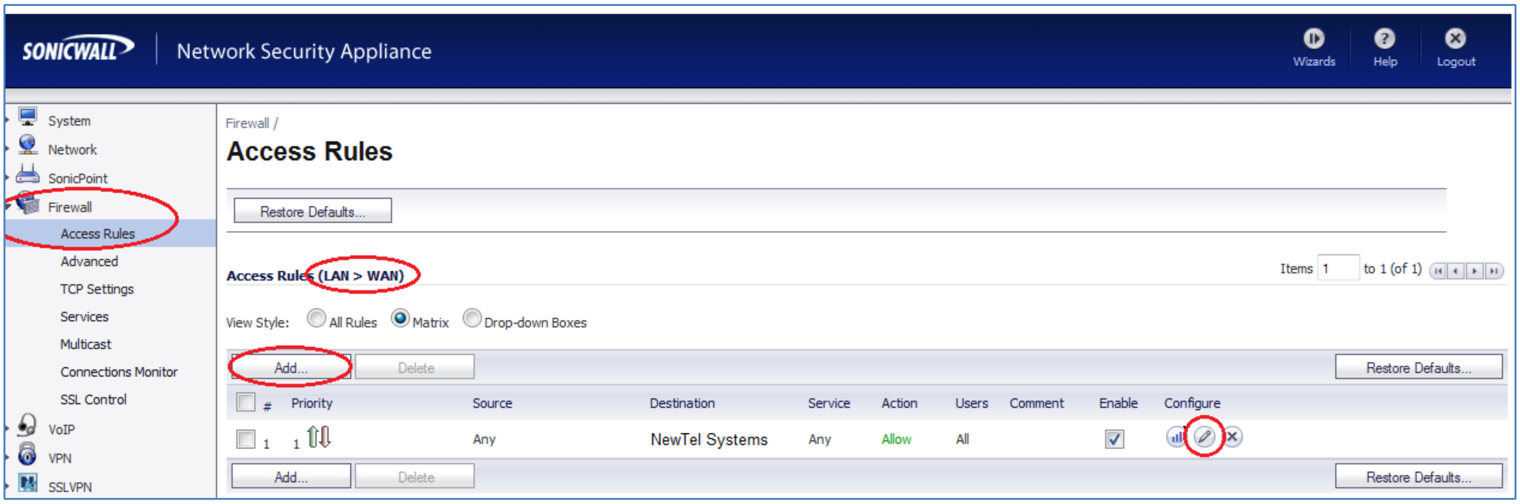
Sonicwall VoIP Setup Guide

1. Go to the Firewall Access Rule Menu and click “Add…” to add a new Rule



Access Rules

Access Rules (LAN > WAN)

Items 1 to 1 (of 1)

View Style: ○ All Rules ● Matrix ○ Drop-down Boxes

□ #	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
□ 1	1	Any	NewTel Systems	Any	Allow	All		☑	

2. Create a LAN -> WAN Rule. (Figure 1)
   ** NO WAN -> LAN RULES ARE NEEDED**

3. Create a new Address Object in the “***Destination***” selector. (As displayed in Figure 2)

4. Switch to the “***Advanced***“ tab of the new Access rule.

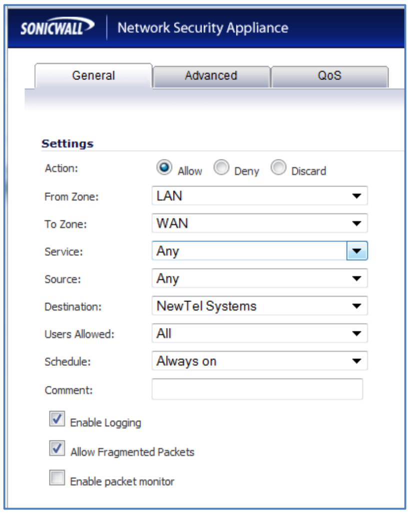
5. Modify the “***UDP Connection Inactivity Timeout***” and set it to 60 or above (preferably 120). The current setting of 30 is inadequately low and will cause the firewall NAT hole to close premature to our 50 second keepalive packets refreshing the NAT session. (See Figure 3 for reference)

6. You may choose to apply the DSCP and 802.1p QoS settings in the “***QoS***” tab. (As displayed in Figure 4)

7. Save the new Access Rule and ensure it appears above any other catch-all or conflicting rules.

8. To ensure the voice traffic is now flowing through the new rule you created, move your mouse over the 📊 icon. You do not have to click on it. If you configured and prioritized the rule correctly (and the phones are plugged in) you should see some traffic incrementing.

9. Ensure that under the “***VoIP Settings***” tab ***Consistent NAT*** is ENABLED and ***SIP Transformations*** are DISABLED. (As displayed in Figure 5). Phones should be rebooted if they were connected prior to disabling SIP Transformations.



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: LAN

To Zone: WAN

Service: Any

Source: Any

Destination: NewTel Systems

Users Allowed: All

Schedule: Always on

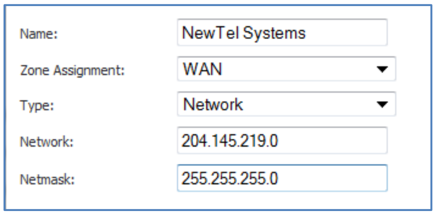
Comment:

☑ Enable Logging

☑ Allow Fragmented Packets

□ Enable packet monitor

Figure 1



Name: NewTel Systems

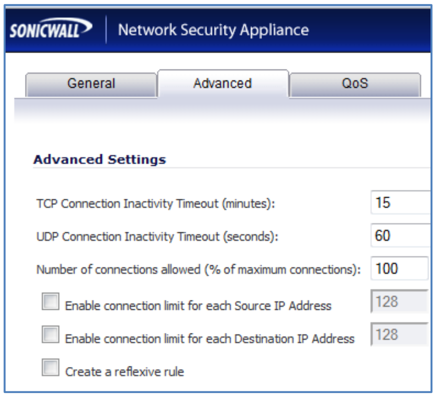
Zone Assignment: WAN

Type: Network

Network: 204.145.219.0

Netmask: 255.255.255.0

Figure 2



Advanced Settings

TCP Connection Inactivity Timeout (minutes): 15

UDP Connection Inactivity Timeout (seconds): 60

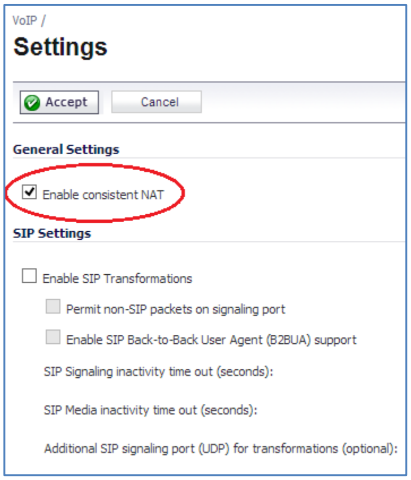
Number of connections allowed (% of maximum connections): 100

□ Enable connection limit for each Source IP Address 128

□ Enable connection limit for each Destination IP Address 128

□ Create a reflexive rule

Figure 3



Settings

General Settings

☑ Enable consistent NAT

SIP Settings

□ Enable SIP Transformations

□ Permit non-SIP packets on signaling port

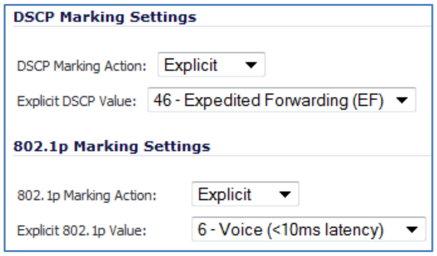
□ Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds):

SIP Media inactivity time out (seconds):

Additional SIP signaling port (UDP) for transformations (optional):

Figure 5



DSCP Marking Settings

DSCP Marking Action: Explicit

Explicit DSCP Value: 46 - Expedited Forwarding (EF)

802.1p Marking Settings

802.1p Marking Action: Explicit

Explicit 802.1p Value: 6 - Voice (<10ms latency)

Figure 4

** SIMPLE METHOD**

If you feel that you do not want to perform the above steps and prefer a simpler method. You may change the default “UDP Connection Inactivity Timeout” for the entire firewall as opposed to only voice traffic to NewTel. You would find this setting under the FIREWALL -> ADVANCED menu. This method is much simpler and perfectly secure. You must ensure that there is no default catch-all (ANY to ANY) LAN -> WAN rule that overrides this setting.