



SonicWALL Configuration for VoxEdge

Step 1:

Confirm with your ISP that their equipment does not have NAT enabled. Ensure that the NAT will be only done on the SonicWALL only.

Step 2:

Configure the SonicWALL's WAN and ensure that the network is working properly.

Step 3:

Check if IPS is enabled in 2 places

-Network → Zones → WAN zone and hit configure. "Enable IPS"

-Security Services → Intrusion Prevention and **uncheck** the "enable IPS"

If either is enable, please contact VoxEdge before continuing.

Step 4:

Create a new Address Object (not Address Group):

162.252.248.0/22 - the subnet mask of /22 is 255.255.252.0

Name the Address Object (in this example, "VoxEdge_VOIP_Server")

23.253.155.190/32 - the subnet mask of /32 is 255.255.255.255

Name the Address Object (in this example, "Provisioning_server")

Add Address Object - Google Chrome

https://192.168.10.1/addNetObjDlg.html

SONICWALL Network Security Appliance

Name: VoxEdge_VOIP_Server

Zone Assignment: WAN

Type: Network

Network: 162.252.248.0

Netmask: 255.255.252.0

Ready

Add Close



VoxEdge LLC
8 S. Forklanding Road
Maple Shade, NJ 08052
856.382.8100
www.VoxEdge.com

Step 5:

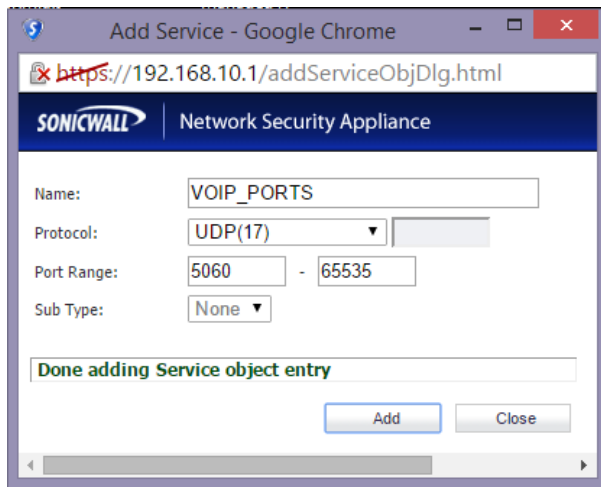
Create a new Service Object (not service group):

Enable ports 21, 22, 5060, 7000, and 16384 - 32768 for UDP traffic

Name the Service Object (in this example, "VOIP_PORTS")

Enable ports 21 and 22 for TCP traffic

Name the Service Object (in this example, "Device_provisioning")



Step 6:

Create 4 Firewall Access Rules:

Access Rule 1:

From LAN to WAN

Source - Any

Destination - VoxEdge_VOIP_Server

Service - VOIP_PORTS

Allow

Advanced Tab - Set UDP Timeout to 3600 seconds



VoxEdge LLC
8 S. Forklanding Road
Maple Shade, NJ 08052
856.382.8100
www.VoxEdge.com

A screenshot of a web browser window titled "Edit Rule - Google Chrome" showing the configuration page for a rule on a SonicWall Network Security Appliance. The URL in the address bar is <https://192.168.10.1/addRuleDlg.html?objTypes=63>. The page has a blue header with the SonicWall logo and "Network Security Appliance". Below the header are four tabs: "General", "Advanced", "QoS", and "Ethernet BWM". The "General" tab is selected. Under the "Settings" section, the "Action" is set to "Allow" (radio button selected). The "From Zone" is "LAN", "To Zone" is "WAN", "Service" is "VOIP_PORTS", "Source" is "Any", "Destination" is "VoxEdge_VOIP_Server", "Users Allowed" is "All", and "Schedule" is "Always on". There is a "Comment" text box. Below these are three checkboxes: "Enable Logging" (checked), "Allow Fragmented Packets" (checked), and "Enable packet monitor" (unchecked). At the bottom, there is a "Ready" status bar and three buttons: "OK", "Cancel", and "Help".

Access Rule 2:

From WAN to LAN

Source - VoxEdge_VOIP_Server

Destination - Any

Service - VOIP_PORTS

Allow

Advanced Tab - Set UDP Timeout to 3600 seconds



VoxEdge LLC
8 S. Forklanding Road
Maple Shade, NJ 08052
856.382.8100
www.VoxEdge.com

Add Rule - Google Chrome

<https://192.168.10.1/addRuleDlg.html?objTypes=63#>

SonicWall Network Security Appliance

General Advanced QoS Ethernet BWM

Settings

Action: ☒ Allow ☐ Deny ☐ Discard

From Zone: WAN

To Zone: LAN

Service: VOIP_PORTS

Source: VoxEdge_VOIP_Server

Destination: Any

Users Allowed: All

Schedule: Always on

Comment:

☒ Enable Logging

☒ Allow Fragmented Packets

☐ Enable packet monitor

Rule action done, please check rule table

Add Close Help

Access Rule 3:

From LAN to WAN

Source – Any

Destination - Provisioning_server

Service - Device_provisioning

Allow

Access Rule 4:

From WAN to LAN

Source - Provisioning_server

Destination – Any

Service - Device_provisioning

Allow