Endian Firewall – Getting SIP Phones To Work

There are a few things that need to be done on a new Endian Firewall (Community or UTM Appliance) installation in order to get it to play nice with SIP based voice over IP phones. If your phones are registering to an internal VoIP server you should not have any issues, however if your server or SIP provider are external to your network then some settings will need to be modified.

First in order to even get your phones to register to the external SIP provider or VoIP server you will need to disable the outbound firewall, or add rules to allow traffic over UDP port 5060 (SIP) and the UDP port range 10000:20000 (RTP). Once this is done you will notice that your SIP phones will register properly to the VoIP service and normal outbound and inbound calls will work properly. However if you try to dial another extension on your internal LAN the extension will ring and the call will be setup, but there will be no audio.

To understand why this issue occurs first we need to visualize what is happening when the first extension dials out to the second and what happens to the packet as it travels over the Internet. In very simple terms the packet leaves the first phone destined for the SIP provider or external VoIP server. Once it gets there the server attempts to establish the connection to the second extension which is located behind the same router/firewall as the first extension. Since both phones are located behind the same router they both appear to be coming from the same external IP address. The router does not understand where to send the packets from there since the packet header information only contains the public IP address, not the address of the phone it is destined for on the internal network. This is where port forwarding or NAT usually comes in and fixes the issue, but in normal practice this is a one to one relation and since you probably have many phones on your internal network it does not apply.

In order to fix the issue we need to allow the packets coming from and going to the phones on the internal network to still retain information that will allow them to be routed properly. To do this create two new rules in the firewall menu on the Endian under Port Forwarding/NAT. These rules need to be coming from the RED interface over the SIP and RTP ports destined for the entire LAN subnet not a single node like a normal port forwarding/NAT rule.

```
RED UDP 5060 -> 192.168.0.0/24 UDP 5060 #SIP
RED UDP 10000:20000 -> 192.168.0.0/24 UDP 10000:20000 #RTP
```

Once these rules are established you need to SSH into the Endian and modify some of the netfilter kernel modules to allow something called SIP Inspection so that the packets can be routed to the correct devices. SSH into your Endian and place the following script in /etc/cron.cyclic so that it is run every time the device is rebooted.

Name the script sip_fix and make sure you run the command

To make it executable.

Once this script is in place reboot your EFW and enjoy your now fully functional VoIP phones!