This HOWTO assumes that your UnifiedBX system is sitting behind a NATed firewall with no direct connection to the outside world and it is NOT in the DMZ zone. If you are relying on this article to set-up your system, DO NOT place your system on a public IP address or a DMZ zone. This article does not address the potential security implications involved in such a setup.

The four key considerations in setting up remote extensions are:

- 1. Ensure that your UnifiedBX is as secure as it can possibly be
- 2. Configure Asterisk so that it knows which IP addresses are inside your network and which ones are on the public internet
- 3. Forward the required ports from your firewall to your PBX
- 4. Configure the Extensions for External Use

In order to accomplish the above we need to apply some configuration information into UnifiedBX, some Asterisk configuration files and on your firewall/router.

Secure Your System

Anytime you access your PBX using a remote extension, you are exposing your PBX to the public internet. If you can access your system from the internet, so can anyone else. Before you begin, you might want to consider several security measures.

First, ensure that IPTables and Fail2Ban are installed and properly configured to protect Asterisk and UnifiedBX. Fail2Ban will temporarily ban any IP address that repeatedly attempts to connect to your PBX using the wrong password. This can effectively deter hackers, by making it take impossibly long to guess a password using brute force. Fail2Ban is already installed on the UnifiedBX distro, and can be configured from the System Administration module.

Second, make sure that all of your extensions are secured with a strong password. A strong password is composed of random letters (upper and lower case), numbers, and symbols, and is at least 15 characters long.

Third, you may wish to consider changing the default SIP Signaling Port from 5060 to an alternative. Port 5060 is widely used for VOIP services, and there are a number of hacking programs in the wild that scan for computers that have port 5060 open, and then attempt hack into any available PBX. If these hacking attacks succeed in obtaining a valid user/extension number and password, the hacker can use your system to place calls at your expense. Even if they don't succeed in obtaining a valid password, they can interfere with legitimate users (or crash asterisk) and thus cause your PBX to become inoperative.

In addition, Port 10000 is used for webmin (a tool that can be used to make substantial configuration changes on your machine using a web browser). If you have webmin on port 10000, either change webmin's default port to something else (such as 9001), or change the default RTP Media Ports from 10000-20000 to 10001-20000.

A range of 10000 ports available for RTP Media is often unnecessarily large for most small systems, because one call requires only 4 active ports. Thus, you might consider narrowing the range of ports used for RTP Media. If you do narrow the range, keep the range somewhere within 10000 to 20000 (i.e. don't select 43500 to 44500), as going outside this range can lead to call quality issues.

For all of these reasons, you may wish to change the default ports to alternative ports in order to enhance the security of your system.

To change the RTP Media Ports, you have to edit an Asterisk file from the command line. Open a command prompt on your machine (either by sitting in front of your machine or by using the UnifiedBX Java SSH module) and type the following:

cd /etc/asterisk

nano rtp.conf

In the file, you'll see the options for the low and high ports used by Asterisk. Change them to something that is still within the range of 10000 to 20000 (using ports outside this range can lead to call quality issues). At a minimum, change the lower port to start at 10001 if you use webmin.

When you're done, hit CTRL-O, hit ENTER, and then hit CTRL-X.

You now need to restart the amportal to get Asterisk to use the new ports. Type:

amportal stop

and then:

amportal start

Note: Whenever you restart amportal, you may lose Busy Lamp Fields until your phones re-register. Aastra phones default to a 3,600 second re-registration time, and so it could take up to an hour before these services come back. You can change the registration time by changing those settings in your phone's configuration settings, or simply reboot the phones to cause them to re-register immediately.

To change the SIP Signaling Port from the default of 5060, open your browser and access the UnifiedBX GUI. Click on "Tools," and then "Asterisk SIP Settings." If this module is not available on your installation of UnifiedBX, you can install it using the "Module Admin" module.

Scroll down to Advanced General Settings, and fill-in the desired port to the right of the Bind Port field. If the field is left blank, the UnifiedBX should default to port 5060. Click "Submit Changes" at the bottom of the screen, and then click the orange "Apply Configuration Changes" bar at the top of the screen.

Remember that if you change any of these default ports, you'll want to change the port forwarding on your router to match the correct ports. If you change your SIP signaling port, you'll need to change your phones to use the new port you selected instead of port 5060.

Tell Asterisk Which IPs are Internal and which IPs are Public

Unless you have your UnifiedBX on a public IP address (which is a very bad idea), then you need to tell UnifiedBX which IP addresses are internal addresses and which IP addresses are external, public IP addresses. It is important for UnifiedBX to have this information so that it can adjust the SIP headers to use your external IP address when it is contacting extensions outside of your local network.

Open your browser and access the UnifiedBX GUI. Click on "Tools," and then "Asterisk SIP Settings." If this module is not available on your installation of UnifiedBX, you can install it using the "Module Admin" module.

Under NAT Settings, click "Auto Configure." If UnifiedBX correctly enters your static IP address, your internal network address ending in .0 (i.e., 192.168.1.0), and your subnet (usually 255.255.255.0), then click "submit changes" and then click the orange bar to reload Asterisk.

If UnifiedBX doesn't accurately enter your static IP address and local address, enter them manually. If you have an IP address that never changes (i.e., a static IP addresss), you can select "Static IP," and enter the IP address into the "External IP" field. If your external IP address changes, you may wish to register for a Dynamic IP address (for example, using dyndns.org), and then select "Dynamic IP." Your internal IP address should be the IP address on the machines on your network, but ending in a zero. For example, if your PBX is 192.168.1.101, then you should enter 192.168.1.0 in the internal IP address field. Your subnet mask will probably be 255.255.255.0.

If you plan to connect to your PBX using a VPN from another network, click on the "Add Local Network Field," and enter the internal address used on that VPN (i.e., 192.168.2.0) along with the subnet mask (usually 255.255.255.0).

Forward the Required Ports from your Router to your PBX

You also have to forward some ports on your Firewall/Router, so that phones that are outside of your local network can reach the PBX through your router/firewall.

The default installation of UnifiedBX is configured to use UDP port 5060 as the SIP signaling port and UDP ports 10000-20000 as the RTP Media ports.

These ports must be forwarded to your UnifiedBX System using your router/firewall configuration. How to do this varies widely depending on the firewall or equipment that you are using. It is commonly referred to as Port Forwarding or maybe Destination NAT (DNAT). However it is referred, if we assume in this example that your UnifiedBX system has an internal IP address of 192.168.1.100, that you didn't change the default 5060 port, and that you changed the lower range of the RTP Media Port from 10000 to 10001, then you will want:

- UDP/5060 -> Forward to 192.168.1.100
- UDP/10000-20000 -> Forward to 192.168.1.100

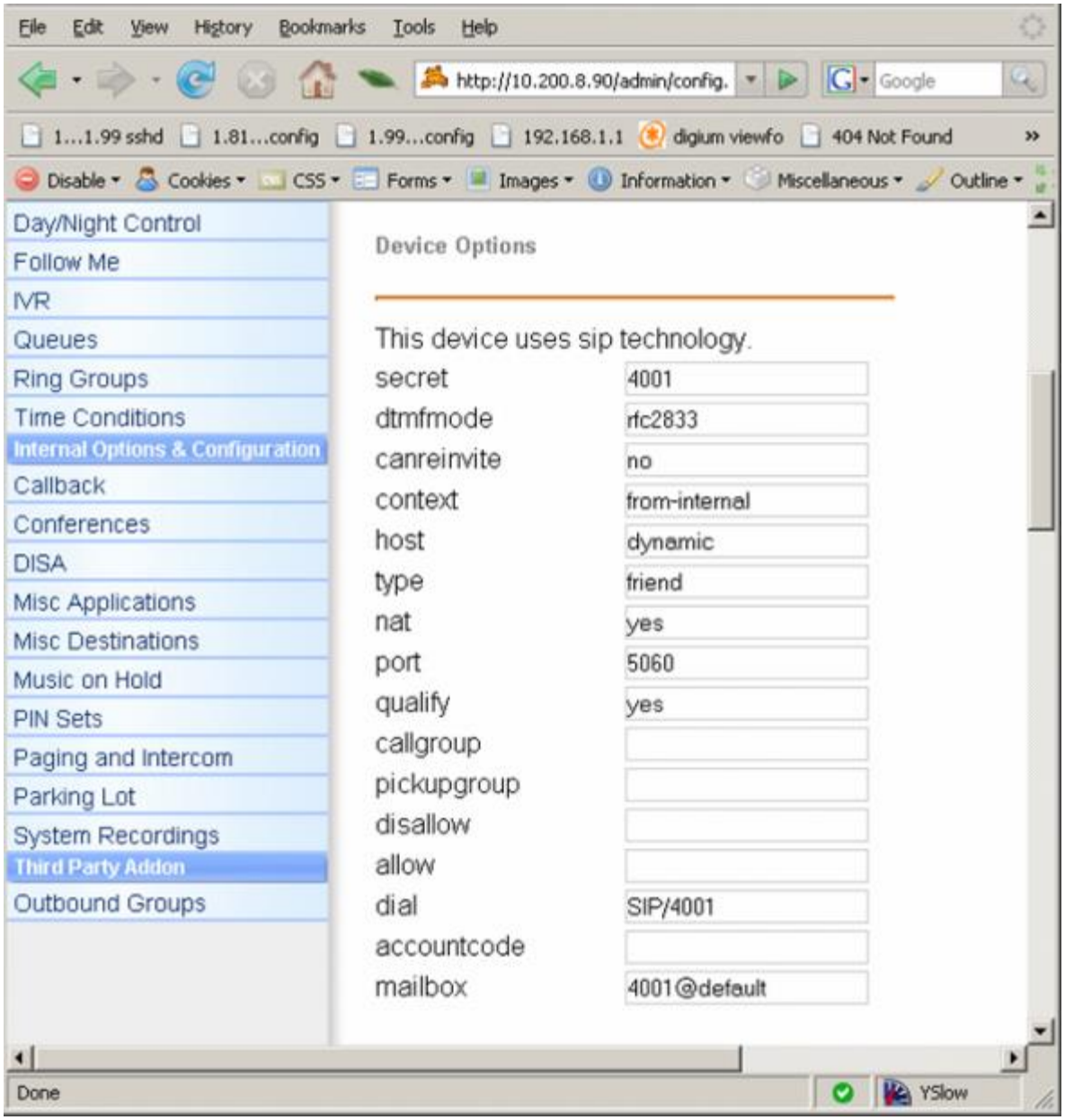
NEVER, EVER, EVER, EVER forward port 80 from your Router to your PBX. If you need remote access to UnifiedBX, the FOP, or the recording interface, set-up a VPN. You have been warned!

Configure Your Extensions for Remote Access

First, select a secure password. If you are making your system available over the internet, then anyone who has a valid extension password can connect to your system and make calls, unless you take action to lock the extensions down using the deny and permit fields (which can be used to limit access to certain extensions to local users).

Second, if possible, use the deny/permit fields in the Device/Extension modules to limit access to known IP addresses for every extension. For Devices/Extensions that don't need remote access, placing the entry "192.168.1.0/255.255.255.0" in the permit field should restrict access to your local network (change 192.168.1.0 to your internal IP addresses if they are different, but end in a .0). If you know the specific IP address from which you will access the remote Device/Extension, place it and the subnet mask in the permit field for the remote Device/Extension and subnet mask of 255.255.255.255 (not 255.255.255.0).

Third, you need to configure the remote Device/Extension with NAT enabled so that Asterisk knows this device is NATed and can apply the SIP rewriting rules that you previously configured above. Navigate to the desired extension and scroll down to the Device Options Section, it should look like:



Device Options - NAT

The configuration option nat must be set to yes, and you may want to set qualify to yes as well although not necessary.

With these steps, when properly configured, your external device should be able to communicate with your UnifiedBX server unless you have issues on the remote end where the device is located because of badly behaved Firewalls. The remote device should be configured to use your external IP address or domain name as specified above.