

Configuring an EdgeMarc for SIP trunking with an IP PBX

This document describes the steps needed to configure an IP PBX behind the EdgeMarc which is pointing to a SIP Trunk provider on the WAN.

Please note that this solution documents the basic configuration needed in the PBX and that the requirements of your specific SIP trunking environment may require modifications to the configuration steps provided in this document.

There are four modes of operations that are discussed in this article.

- A. The IP PBX has a static IP address and **is able** to send REGISTERS. It has to register a DID (usually the main trunk DID). Upon a successful registration, the SIP trunk provider will then route all numbers in that trunk group to the EdgeMarc WAN. The EdgeMarc will then forward all calls (using the dial rules) to the PBX defined in the Trunking page. **No Header Manipulation is needed.**
- B. The IP PBX has a static IP address but **is NOT able** to support REGISTERS. The SIP trunk provider doesn't need any Registrations and the provider statically assigns the EdgeMarc's WAN IP as the trusted IP to route calls to and accept calls from.
- C. The IP PBX has a static IP address but **is NOT able** to support REGISTERS. However, the SIP trunk provider requires a Registration and the EdgeMarc has to Register on behalf of the PBX. The EdgeMarc has to respond to any authentication challenge (401) from the SIP server and not pass in through to the LAN side PBX and the PBX doesn't support authentication.
- D. The IP PBX has a static IP address and **is able** to send REGISTERS. It has to register a DID (usually the main trunk DID). Upon a successful registration, the SIP trunk provider will then route all numbers in that trunk group to the EdgeMarc WAN. The EdgeMarc will then forward all calls (using the dial rules) to the PBX defined in the Trunking page. **Header Manipulation is needed.**

When to use B2BUA and when to use ALG Trunking ?

B2BUA is used when the EdgeMarc has to register on behalf of the PBX and/or Header Manipulation Rules (HMR) is required.

ALG (Trunking) is used when the EdgeMarc is just proxying the messages from the PBX and the PBX supports REGISTER messages. The ALG (Trunking) page also supports simple number manipulation rules.

Prerequisites and Assumptions:

SIP trunking information provided by the VoIP service provider:

- SIP server IP address or DNS name.
- Authentication-name and Password that the SIP Provider has given to register the SIP Trunk.

NOTE:

GUI screenshots in this article are based on VOS 14.6.0, other VOS version GUI interface may look different but the concepts are the same. For Scenario C and D, EdgeMarc should be on VOS 10.2.4 or higher.

Sample Network Diagram

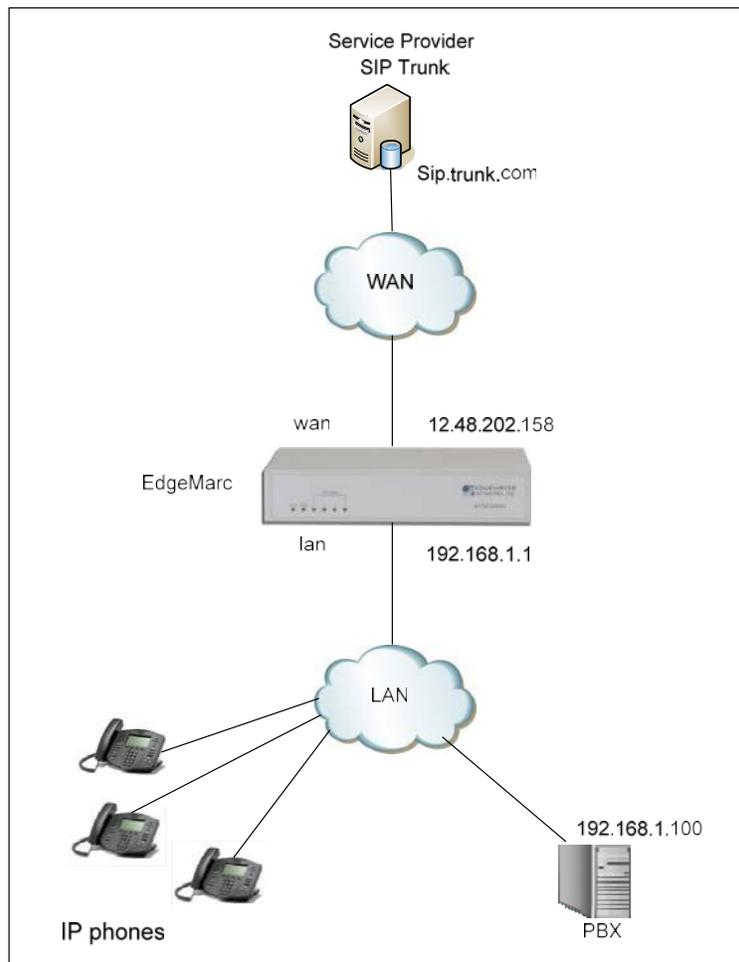


Figure 1: Network diagram

In this example, there is an IP PBX on the LAN side that is configured with 192.168.1.100 IP address and the EdgeMarc LAN IP is 192.168.1.1. The WAN interface IP address of the EdgeMarc is 12.48.202.158. The SIP/VoIP provider's SIP SERVER address is sip.trunk.com.

Configuring the EdgeMarc for Scenario A and B

The steps below assume you are starting from the factory default settings. Please refer to the EdgeMarc VOS user guide for more detailed information on the different configuration steps.

Configure the Network page

1. Connect and configure a PC to the LAN port on the EdgeMarc. By default, the EdgeMarc DHCP server is enabled. Your PC will pull an IP address.
If the PC doesn't get an IP, configure your PC NIC settings as follows:
IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Default gateway: 192.168.1.1
2. Log into the EdgeMarc by opening a web browser and entering <http://192.168.1.1>
Username: root
Password: default
3. Click on the "Network" link
4. Configure the LAN and WAN Interface Settings
In this example, the LAN IP is 192.168.1.1 and the WAN IP is 12.48.202.158
Set the Primary and Secondary DNS entres that the EdgeMarc will use in the DNS Server section.

The screenshot shows the 'Network' configuration page in the EdgeMarc web interface. On the left is a 'Configuration Menu' with options like Admin, Network, NAT, VLAN, WAN, etc. The main content area is titled 'Network' and contains several sections:

- LAN Interface Settings:** IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, IPv6 Address/Prefix: /, Enable VLAN support: , Default VLAN ID: 1.
- WAN Interface IPv6 Settings:** Select the type of IPv6 WAN Interface to use: Disabled, Static IP (ethernet), IPv6 in IPv4 Tunnel, VLAN.
- WAN Interface IPv4 Settings:** Select the type of IPv4 WAN Interface to use: Disabled, PPPoE, DHCP, Static IP, VLAN. IP Address: 12.48.202.158, Subnet Mask: 255.255.255.0.
- Network Settings:** Default Gateway: 12.48.202.1.
- DNS servers:** Note: In case of dynamic links, if the manual override checkbox is not checked the address provided will be used. Manually set DNS: . Primary DNS Server: 8.8.8.8, Secondary DNS Server: 4.2.2.2.

At the bottom are buttons for 'Submit', 'Reset', and 'Apply Later'.

Figure 2: Network page

5. Select “Submit” when done.

Configure the SIP Settings page

6. Next, click on the “VoIP” link

The screenshot shows the Edgewater Networks SIP Settings page. On the left is a Configuration Menu with a tree view. The 'SIP' link is highlighted with a red box. The main content area is titled 'SIP Settings' and contains the following fields and options:

- SIP Server Address:
- SIP Server Port:
- SIP Server Transport:
- Use Custom Domain:
- SIP Server Domain:
- List of SIP Servers:
- Enable Multi-homed Outbound Proxy Mode:
- Enable Transparent Proxy Mode:
- Limit Outbound to listed Proxies / SIP Servers:
- Limit Inbound to listed Proxies / SIP Servers:
- Include UPDATE In Allow:
- PRACK Support:

Below these settings is a section titled 'Allowed SIP Proxies' with a description: 'This is the list of proxies or registrars that are allowed when enabling the "Limit Outbound" (for transparent mode only) and "Limit Inbound" (for transparent as well as non-transparent mode) options. The SIP Server Address above is always included and does not have to be in this list.' It contains a table with the following structure:

List of SIP Proxies	
Select: All None	<input type="button" value="Delete"/>
<input type="text" value="SIP Proxy Address/FQDN"/>	
The list is currently empty	

At the bottom is an 'Add a new proxy' section with an 'IP Address/FQDN' field and 'Add' and 'Reset' buttons.

Figure 3: SIP page

7. Click on the “SIP” link

8. Configure “SIP Server Address” and “SIP Server Port”. The “SIP Server Address” is provided by the SIP service provider.

In this example, the SIP provider is ‘sip.trunk.com’

The SIP Server Port is usually port 5060, however, you may receive different instructions from your SIP provider. The EdgeMarc will forward all outbound calls to the SIP Server Address and Port. It will also expect to receive all inbound calls using the SIP Server Address and Port.

9. For security reasons, enable the “Limit Outbound to listed Proxies / SIP Servers” and “Limit Inbound to listed Proxies / SIP Servers” checkbox, This should be enabled by default.

Note: This means that the EdgeMarc will only process outbound / inbound SIP messages from SIP servers configured in the SIP settings and listed on the

Allowed SIP Proxies. This option will ensure that the EdgeMarc only forwards outbound / inbound SIP messages received from the IP PBX to the IP address configured in the SIP Server address and Allowed SIP Proxies field. This filtering feature is only one part of a multi-tiered security plan that should be implemented when using SIP trunking services. Other common techniques include configuring the IP PBX to restrict international dialing to authorized users, configuring passcodes for international dialing, disabling the ability to “zero” out of IVR or voicemail systems to place phone calls and restricting the use of the SIP trunk to only LAN side phones connected and registered to the IP PBX.

10. Select “**Submit**”

Configure the ALG Trunking Configuration

11. Select “VoIP -> ALG”

The screenshot displays the Edgewater Networks configuration interface for SIP Trunking. On the left is a Configuration Menu with options like Admin, Network, Users, Security, VoIP, H.323, MGCP, SIP, ALG (highlighted), B2BUA, SIP Routing, Media Server, Survivability, Clients List, Test UA, and VPN. The main content area is titled "ALG Trunking Configuration" and includes a "Help" link. A status bar at the top indicates "There are unapplied configuration changes: [Submit All] [Clear All]".

SIP Trunking Configuration
Configuration of SIP trunking devices.

SIP Trunking devices
A SIP trunking device can be a PSTN gateway, or similar device, that does not issue REGISTER messages. Calls will be forwarded to the device based on the dial-plan rules below.
If VLANs are enabled, the SIP trunking device needs to be in the same VLAN as defined in the VoIP ALG page.

SIP Trunking Devices				
Select: All None [Delete]				
	Address	Port	Name	Group
<input checked="" type="checkbox"/>	192.168.1.100	5060	PBX	

Add a trunking device
Action: Add new trunking device [v]
Name: []
Address: []
Port: 5060 []
[Commit] [Reset]

Header Transformation
These header transformation rules are applied to all SIP trunking devices. They define how specified SIP headers should be transformed when forwarding to the SIP Server.

From Header
Select the domain to use in From header when sending requests to the SIP Server:
 SIP Server Address (default)
 System WAN IP
[Commit] [Reset]

Rules
Rules are used to forward and/or modify incoming and outgoing calls. There are 3 types of rules:
- Inbound: from server to trunking device
- Outbound: from trunking device to server
- Redirect: from local phone to trunking device (w/o routing to server)
Outbound rules can match against and/or modify either the calling or called number. Inbound and redirect rules operate on the called number only. Stripped and added digits always apply to the left-most digits of the DID.

Dial Rules								
Select: All None [Delete]								
	Type	Mode	Party	PRJO	Pattern-match	Strip	Add	Trunking device
<input checked="" type="checkbox"/>	Inbound	Both			Default Rule			PBX (192.168.1.100:5060)

Add a rule
Action: Add new rule [v]
Type: Inbound [v]
Mode: Both [v]
Call Party: Called [v]
Default rule:
Priority:
Pattern-match (if not default): []
Strip digits: 0 []
Add string: []
Trunking device: PBX (192.168.1.100:5060) [v]
Note: "Use SIP proxy as secondary target" rule can be configured on the B2BUA page
[Commit] [Reset]

Figure 4: SIP Trunking devices page

13. Add the IP PBX as a SIP Trunking Device by configuring the “Name”, “Address”, and “Port”. The Address and Port need to match the IP address and SIP port configured in the IP PBX.
14. Select “Commit”
15. The IP PBX should appear in the SIP Trunking Devices table (as shown in Figure 4.)
16. On the same page, scroll down to the Dial Rules Section.
17. Select “Action - Add new rule”
18. Set “Type:” to “Inbound”

19. Select the “**Default Rule**” checkbox
20. Set the “**Trunking Device**” to be the name and IP address of the PBX.
21. Select “**Commit**”. The Dial Rules page should look like Figure 4.
This will create a routing rule that will direct ALL inbound calls received on the WAN interface of the EdgeMarc to the PBX.
22. When you are ready to apply the settings, click on the Submit All button on the blue bar at the top of the page.
23. Configure the rest of the EdgeMarc settings as per the manual.

Other settings on the EdgeMarc are optional for basic SIP trunking to operate, but we recommend configuring at least the following:

- Traffic Shaping and CAC: Adjust these values according to your WAN bandwidth.
- Syslogging and MOS monitoring to EdgeView e.g. Point the EdgeMarc to syslog to the EdgeView, to capture all the MOS scoring on the SIP trunking calls on the LAN and WAN side. This will allow you to “demarc” VoIP quality issue between LAN and WAN.

Configuring the PBX

24. On the PBX, configure the PBX SIP server setting to point to the LAN IP address of the EdgeMarc (192.168.1.1)
25. Disable the ‘Behind a NAT’ functionality on the PBX, if it is enabled.

Making and Receiving calls

- **Registration mode**

If the SIP trunk provider requires a registration from the PBX and PBX is capable to register, the registration sent by the PBX should be received on the LAN side of the EdgeMarc, processed by the ALG and will be forwarded out the WAN to the SIP trunk provider. As soon as it's registered, the PBX should be able to make calls. All inbound calls from the SIP trunk provider will be forwarded to the PBX (according to the Dial Rules – Fig 4).

- **Static mode**

If the PBX doesn't register, make sure that the SIP provider has statically assigned the WAN IP address of the EdgeMarc as a trusted IP address to send and receive calls from. All outbound calls from the PBX will be forwarded to the SIP Server from the WAN IP of the EdgeMarc. All inbound calls from the SIP trunk provider will be sent to the WAN IP of the EdgeMarc and will be forwarded to the PBX (according to the Dial Rules – Fig 4).

Configuring the EdgeMarc for Scenario C

Configure the EdgeMarc using the procedure listed in Step 1 – 10 above.

- C1. Select “**VoIP -> SIP -> B2BUA**” link.
- C2. Under the Trunking Devices section, add a trunking device.
- Name : PBX (as an example)
 - IP : 192.168.1.100
 - Port: 5060

Click on the “Update” button you should see the same ‘Trunking Devices’ table entry on Figure 5.

B2BUA Trunking Configuration [Help](#)

This page supports only IPv4 addressing.
In order for changes to this page to be applied, you must click the Submit button at the bottom of the page

Trunking Devices

Name	Address	Port	Group	Username	Registration Status
<input checked="" type="checkbox"/> PBX	192.168.1.100	5060			

New Entry

Name: Model:

IP: Transport:

Port:

Username: Password:

Figure 5: Defining the non-registering PBX in the B2BUA page

- C3. Next, you would need to define the DID / Authentication name and password that the SIP trunk provider is expecting. (*This is where you define what the EdgeMarc will register on behalf of the non-registering PBX*)

- Add the Username, Authentication-name and Password that the SIP Provider has given to register the SIP Trunk.
- Registrar - Choose Default SIP Proxy (B2BUA will use the SIP Server address configured on the ALG Page to register the AOR)
- Click on the “Update” button and you should see the same Credentials and Registration table entry on Figure 6.

Note: If the SIP server i authenticates every INVITE from the PBX, then you must set the ‘**Use as default**’ setting. Create another set of Credentials and check the ‘**Use as default**’ checkbox. The B2BUA will respond to any 401 challenge from the SIP server, instead of sending the 401 through to the PBX.

Credentials and Registration						
	AOR	Auth-User	Password	Registrar	Status	Transport
✘	4074017663	4074017663	is set	default		
✘	default	4074017663	is set			
New Entry						
Credentials						
Username:		<input type="text"/>		Auth-User: <input type="text"/>		
Edit Password:		<input checked="" type="checkbox"/>				
Password:		<input type="text"/>				
Confirm Password:		<input type="text"/>				
Use as default:		<input type="checkbox"/>				
Registrar						
<input checked="" type="radio"/> Don't Register						
<input type="radio"/> Default SIP Proxy						
Domain:		<input type="text"/>				
Address (optional):			<input type="text"/>		Port: <input type="text"/>	
Transport:		UDP ▾				
Register Options (Optional)						
Default Expires:		<input type="text"/> sec.		Renew interval: <input type="text"/> %		
<input type="button" value="Update"/>						

Figure 6: Information needed to register on behalf of the non-registering PBX.

C4. Next, you need to define the “Actions” for the Trunking Rules. Go to the Trunk section and add a “Action”. Below are two examples, one without Header Manipulation Rules (HMR) needed and the other with HMR.

Simple Action Rule with no Header Manipulation Rules.

In this example, an action was defined to route all incoming calls to the PBX.

- Name: incomingcalls (as an example)
- Send to: Select Trunking device “PBX” from the pull down menu (this is the device defined in Trunking Device on Figure 5)
- Click on the Update button and you should see the same ‘Actions’ table entry on Figure 7.

Actions						
	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
<input checked="" type="checkbox"/>	incomingcalls	<input checked="" type="checkbox"/>				
New Entry						
Name:	incomingcalls					
Send To:	<input checked="" type="radio"/> Trunking Device:		PBX ▼			
	<input type="radio"/> Client:		<input type="text"/>			
	<input type="radio"/> URI:		<input type="text"/>			
	<input type="radio"/> Response:		<input type="text"/>			
Prioritize:	<input type="checkbox"/>		Refer to Re-INVITE: <input type="checkbox"/>			
Serial Hunting:	<input type="text"/>		Add <input type="text"/>		Delete	
Header Manipulations:						
	Header			Value		
Header:	Request-URI ▼			Add		
Value:	<input type="text"/>					
Update						

Figure 7: Action rule with no HMR for call routing

- C6. Next, you need to define a matching pattern / rule for the calls.
 In this example, we are trying to define a default inbound rule that will route all incoming calls to the PBX (for more information on the options in the pull down menu, please refer to the *Help link* on the top right hand side of this page)
- Select a call direction: Inbound
 - Select “default”
 - For Action: select “incomingcalls” (which was the Action defined in Figure 7)
 - Click on the “Update” button and you should see the same Match table entry on the Figure 8.
- C7. Finally, click on the Submit button at the bottom of the page to submit all changes made on the B2BUA page.

Match									
	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
<input checked="" type="checkbox"/>	Inbound	BothModes	✓					Any	incomingcalls
New Entry									
	Direction:	Inbound ▾							
	Mode:	BothModes ▾							
	<input checked="" type="radio"/> default								
	<input type="radio"/> Pattern:	Called ▾							
	Called Party :	matches ▾							
	Calling Party:	matches ▾							
	Source:	Any ▾							
	Action:	incomingcalls ▾							
Update									

Figure 8: Defining a pattern match for the dialing rules

Configuring the EdgeMarc for Scenario D

Configure the EdgeMarc using the procedure listed in Steps 1 – 10 above. Next, follow the procedure outline in steps C1 – C3 above.

D1. Next, you need to define the “Actions” for the Trunking Rules. Go to the Trunk section and add a “Action”. In this example, an action was defined to route all incoming calls to the PBX and add Header Manipulation Rules to strip the leading 2 digits from the username in the Request URI and TO header.

- Name: incomingcalls (as an example)
- Send to: Select Trunking device “PBX” from the pull down menu (this is the device defined in Trunking Device on Figure 5)
- Put in the Header Manipulation Rules associated for the ‘incomingcalls’ Action. (*For more information on HMR rules, see the Help link on the top right hand corner of the page*)
- Click on the Update button and you should see the same ‘Actions’ and Header Manipulations table entry on Figure 9.

Actions

	Name	Send	Prio	Hunt	Header	Refer-To-ReINV
✘	incomingcalls	✓			✓	

New Entry

Name:

Send To: Trunking Device: Client:
 URI:
 Response:

Prioritize: Refer to Re-INVITE:

Serial Hunting:

Header Manipulations:

Header	Value
✘	Request-URI '<sip:' + substr(\$request.uri.user, 2, 0) + '@' + \$env.target_domain + '>'
✘	To '<sip:' + substr(\$to.uri.user, 2, 0) + '@' + \$env.target_domain + '>'

Header:

Value:

Figure 9: Action rule with HMR for call routing

- D5. Next, you need to define a matching pattern / rule for the calls. In this example, we are trying to define a default inbound rule that will route all incoming calls to the PBX
- Select a call direction: Inbound
 - Select “default”
 - For Action: select “incomingcalls” (which was the Action defined in Figure 9)
 - Click on the “Update” button and you should see the same Match table entry on the Figure 10.

Match									
	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
<input checked="" type="checkbox"/>	Inbound	BothModes	<input checked="" type="checkbox"/>					Any	incomingcalls
<i>New Entry</i>									
Direction: <input type="text" value="Inbound"/>									
Mode: <input type="text" value="BothModes"/>									
<input checked="" type="radio"/> default									
Pattern: <input type="text" value="Called"/>									
Called Party :				<input type="text" value="matches"/>	<input type="text"/>				
Calling Party:				<input type="text" value="matches"/>	<input type="text"/>				
Source: <input type="text" value="Any"/>									
Action: <input type="text" value="incomingcalls"/>									
<input type="button" value="Update"/>									

Figure 10: Defining a pattern match for the dialing rules.

- D6. Finally, click on the Submit All button to submit all changes made on the B2BUA page.

For advanced configurations and debugging, contact Edgewater Networks Technical Assistance Center at support@edgewaternetworks.com or call 408.351.7255.