

# <u>Goal</u>

Enable coexistence of a 3<sup>rd</sup>-party VPN / Firewall with an EdgeMarc appliance.

Describe characteristics and tradeoffs of different topologies.

Provide configuration information for the EdgeMarc.

## **Pre-Edgewater Configuration**

Assume the following configuration prior to installing the EdgeMarc appliance:



# <u>Solution</u>

Note: The descriptions below assume VOS v5.1 or later. Those configurations that do not utilize Proxy ARP will also work for older versions of VOS.

There are multiple ways to configure a VPN / firewall in conjunction with an EdgeMarc appliance. Each has various tradeoffs. The table below is a starting point to determine the appropriate configuration for your environment.

- EdgeMarc 200/250/4300/45XX/46XX/5300LF2
  - Non-VLAN-capable Ethernet switch
    - One public WAN IP range available.
      - Two Enet drops available per office/desk.

See *Sub-option A1: Split LAN Ethernets*, page 3. This offers full Plug 'n Dial for phones.

- One Enet drop available per office/desk.

See Sub-option A2: Single LAN Ethernet, using separate PC & Phone subnets, page 8. Phones must be manually configured in this layout. See Sub-option A3: Single LAN Ethernet, using the same PC & Phone subnet, page 9. Phones can share PCs' DHCP server

 Two (or more) public IP ranges. Want one (or more) subnets routed through the EdgeMarc to its LAN interface.

See Sub-option C1: VLAN-capable EdgeMarc, page 14.

- VLAN-capable Ethernet switch
  - One public WAN IP range available.
     See *Sub-option D1: VLAN-capable EdgeMarc*, page 20.
- EdgeMarc 4200/5300/6400
  - Non-VLAN-capable Ethernet switch
    - One public WAN IP range available.
      - Two Enet drops available per office/desk.
        - See Sub-option B1: Split LAN Ethernets, page 11.

This offers full Plug 'n Dial for phones.

- One Enet drop available per office/desk.
  - See Sub-option B2: One LAN Ethernet, page 13

This option isn't supported. See text for details.

- Two (or more) public IP ranges. Want one (or more) subnets routed through the EdgeMarc to its LAN interface.
  - Two Enet drops available per office/desk.

See Sub-option C2: Non-VLAN EdgeMarc, page 18

This configuration requires two Enet drops per office/desk.

- One Enet drop available per office/desk.

See Sub-option B2: One LAN Ethernet, page 13.

This option isn't supported. See text for details.

- VLAN-capable Ethernet switch
  - One public WAN IP range available.
    - See Sub-option D2: Non-VLAN EdgeMarc, page 26

## Option A: VLAN-capable Edgewater appliance, non-VLAN switches, one WAN subnet

Sub-option A1: Split LAN Ethernets



## **Characteristics**

- EdgeMarc provides NAT, Firewall and DHCP Plug 'n Dial to phones
- 3<sup>rd</sup>-party firewall provides NAT, Firewall and DHCP to PCs
- WAN interface has one free IP address:
  - The EdgeMarc is assigned one IP address from the WAN subnet
  - Other address(es), including the one already being used by the 3<sup>rd</sup>-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs
  - VLAN #2730 with private subnet for phones (associated with EM LAN port 4). This LAN uses standard 802.1 frames.
  - VLAN #2 with a public subnet for the 3<sup>rd</sup>-party VPN / Firewall device (associated with EM LAN port 3). This LAN uses standard 802.1 frames.

#### Limitations

- This configuration requires two drops per cube or office.
  - DHCP is used separately for PCs and Phones, requiring two broadcast domains. Two broadcast domains means two LANs.
- This configuration is only possible on Edgewater appliances that provide VLAN support (200/250/4300/4500/4600 Series EdgeMarcs).

## Implementation Steps

Utilizing the EdgeMarc GUI, follow the standard instructions (described in the user's guide) to enable the following on the EdgeMarc:

- 1. Enable Network with VLAN functionality
  - Set the four LAN ports to 802.1
  - Modify VLAN 2730 as: IP address: 10.10.10.1 with mask 255.255.255.0 Physical ports: 1, 2 and 4
  - Add a VLAN with: ID: 2 IP address: 10.0.0.1 with mask 255.255.255.0
  - $\circ$   $\,$  Associate VLAN 2 with LAN port 3  $\,$

When done, the VLAN screens should look similar to the following:

#### **VLAN Configuration Page:**

edgewater		V Confi	guration	Nucer to confidure \	<u>Hel</u>
Configuration Menu	<u>Creat</u>	e vlan   v	LAN Membership   <u>'</u>	VLAN Port	
Network     Subinterfaces	5 		VLAN Co	onfiguration	
VLAN Configuration	Select	: <u>All None</u>			Delete
<u>Configuration</u> <u>DHCP Relay</u>		VLAN ID	IP Address	Subnet Mask	Isolate VLAN
DHCP Server		2730	10.10.10.1	255.255.255.0	N
NAT     PPTP Server		2	10.0.0.1	255.255.255.0	N
<ul> <li><u>SIP UA</u></li> <li><u>Security</u></li> <li><u>Survivability</u></li> <li><u>Test UA</u></li> <li><u>Traffic Shaper</u></li> <li><u>VoIP ALG</u></li> <li><u>VoIP Traversal</u></li> <li><u>VPN</u></li> <li><u>WAN Link</u></li> <li><u>Redundancy</u></li> </ul>	Crea VLAN IP Ac Subr Isola Add	nte a nev N ID: ddress: et Mask: nte VLAN Reset	<b>v VLAN</b> from other VLA	Ns 🗖	

<pre>///edgewater</pre>	VLAN Port Membership	Help
Configuration Menu     Network     Subinterfaces     VLAN Configuration	VLAN Port Membership allows the user to as: VLAN.   <u>Create VLAN   VLAN Membership   VLAN Port</u>   VLAN ID: 2 -	sign ports as members of a
<u>WAN VLAN</u> <u>Configuration</u> <u>DHCP Relay</u>	VLAN Port Member	rship
DHCP Server     NAT	Port Number	Member
PPTP Server	1	
• <u>SIP UA</u>	2	
<u>Security</u>	3	
Survivability     Tost UA	4	
<ul> <li>Test DA</li> <li>Traffic Shaper</li> <li>VoIP ALG</li> <li>VoIP Traversal</li> <li>VPN</li> <li>WAN Link</li> <li>Redundancy</li> <li>System</li> </ul>	Submit Reset Apply Later	

## VLAN 2730 Port Membership:

edgewater	VLAN Port Membership	accian porte ac mombore of a
Configuration Menu • <u>Network</u> • <u>Subinterfaces</u> • VI AN Configuration	VLAN.	
WAN VLAN Configuration	VLAN Port Mem	bership
<ul> <li>DHCP Relay</li> <li>DHCP Server</li> </ul>	Select: <u>All None</u>	
NAT	Port Number	Member
PPTP Server	1	
SIP UA	2	
<u>Security</u>	3	
<ul> <li><u>Survivability</u></li> <li>Test UA</li> </ul>	4	
<ul> <li>Traffic Shaper</li> <li>VoIP ALG</li> <li>VoIP Traversal</li> </ul>	Submit Reset Apply Later	
• <u>VPN</u> WAN Link Redundancy		

#### **VLAN Port Configuration:**

Configuration Menu	VLAN Port Configuratic port.   <u>Create VLAN</u>   <u>VLAN Memi</u>	on allows the user to configur pership   <u>VLAN Port</u>	e VLAN s	settings pe	ər —
<ul> <li><u>Network</u></li> <li><u>Subinterfaces</u></li> </ul>	Port Number	Packet type		PVID	
<ul> <li>VLAN Configuration</li> <li>WAN VLAN</li> </ul>	1	Untagged Only	- 2	730	•
Configuration	2	Untagged Only	• 2	730	,
<u>DHCP Relay</u>	3	Untagged Only	<b>→</b> 2		-
NAT	4	Untagged Only	• 2	730	÷
SIP UA Security Survivability Test UA Traffic Shaper VoIP ALG VOIP Traversal VPN WAN Link Redundancy	Submit Reset Apply	Later			

- 2. Enable NAT
- 3. Enable ALG functionality
  - Specify VLAN 2730 for the ALG
- 4. Enable Traffic Shaping
- 5. Enable DHCP on VLAN #2730
- 6. Enable Firewall
- Enable System -> Proxy ARP Configure Proxy ARP so that the EdgeMarc bridges the external Firewall's IP address from the EM's WAN i/f to its LAN i/f.
  - VLAN 2 is associated with LAN Port 3
  - $\circ$  The IP address to be forwarded is 67.40.40.2/32
  - Bridge traffic back to the default gateway 67.40.40.1

When done, the Proxy ARP screen should look similar to the following:

## **PROXY ARP Page:**

edgewater	Proxy ARP					<u>Hel</u>
Configuration Menu Network DHCP Relay	Proxy ARP is used IP address or netw the firewall and N. using the address When configuring Proxy address with this syste configuring Proxy ARP.	to create a vork. Addres AT, allowing es. y ARP, the ups em's WAN MAC	bridge be ses and r complete tream route address. Fl	etween the WA networks that e unprotected r will need to reas ush the upstream	N and the L are bridged I access to th isociate the pro router's ARP ca	AN for an oypass e system oxied IP ache after
NAT	IP Address	Network N	lask (Bits)	Proxy on IF	Gateway	On IF
PTP Server	8 67.40.40.2	32		WAN	67.40.40.1	VLAN2
Test UA Traffic Shaper VoIP ALG VoIP Traversal VPN WAN Link Redundancy System • Backup / Restore • Clients List • Dynamic DNS • File Download • File Server Management Interface Network Information • Network Test Tools • Proxy ARP • RADIUS Settings	Network Mask (Bi Interface respond Gateway: On Interface: Add Clear Submit Reset	ts): ling to ARP: ApplyLater	32 WAN - 67.40.40.1 VLAN2	•		

Sub-option A2: Single LAN Ethernet, using separate PC & Phone subnets



#### **Characteristics**

- EdgeMarc provides NAT and Firewall to phones
- 3<sup>rd</sup>-party firewall provides NAT, Firewall and DHCP to PCs
- WAN interface has one free IP address:
  - The EdgeMarc is assigned one IP address from the WAN subnet
  - Other address(es), including the one already being used by the 3<sup>rd</sup>-party
     Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs
  - VLAN #2730 with private subnet for phones (associated with EM LAN port 4). This LAN uses standard 802.1 frames.
  - VLAN #2 with a public subnet for the 3<sup>rd</sup>-party VPN / Firewall device (associated with EM LAN port 3). This LAN uses standard 802.1 frames.

## Limitations

- DHCP and Plug 'n Dial not available for Phones
  - Phones must be manually configured with IP addresses in the 10.10.10.0 subnet and a SIP Proxy or MGCP Control Server address of the EdgeMarc.
- This configuration is only possible on Edgewater appliances that provide VLAN support, (200/250/4300/4500/4600 Series EdgeMarcs).

## Implementation Steps

Follow all the steps in Sub-option A1: Split LAN Ethernets, above, except:

• Skip step 5. Enable DHCP on VLAN #2730





## **Characteristics**

- EdgeMarc provides ALG functionality to phones
- 3<sup>rd</sup>-party firewall provides NAT, Firewall and DHCP to PCs and phones
  - Phones receive IP addresses from the same pool as PCs.
  - Default router for PC and phones is 3<sup>rd</sup>-party firewall
  - EdgeMarc is SIP Proxy or MGCP Control Server to phones
- WAN interface has one free IP address:
  - The EdgeMarc is assigned one IP address from the WAN subnet
  - Other address(es), including the one already being used by the 3<sup>rd</sup>-party
     Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs
  - VLAN #2730 with private subnet for phones, and shared by PCs (associated with EM LAN port 4). This LAN uses standard 802.1 frames.
  - VLAN #2 with a public subnet for the 3<sup>rd</sup>-party VPN / Firewall device (associated with EM LAN port 3). This LAN uses standard 802.1 frames.

## Limitations

• This configuration is only possible on Edgewater appliances that provide VLAN support, (200/250/4300/4500/4600 Series EdgeMarcs).

### **Implementation Steps**

Follow all the steps in Sub-option A1: Split LAN Ethernets, above, except:

- In step 1, VLAN #2730 uses subnet 192.168.1.0/24 and the EM is 192.168.1.254 in that subnet.
- Skip step 5, Enable DHCP on VLAN #2730.
   OR

Follow step 5, but disable DHCP on the 3<sup>rd</sup>-party firewall.

Note that phones expect a combination of DHCP Options 66, 150 and 151 for VoIP parameters. See Edgewater knowledgebase article: *90562* : *DHCP parameters supported by EdgeMarc*.

## Option B: Non-VLAN Edgewater appliance, non-VLAN switches, one WAN subnet

#### Sub-option B1: Split LAN Ethernets



## **Charocteristics**

- EdgeMarc provides NAT, Firewall and DHCP Plug 'n Dial to phones
- 3<sup>rd</sup>-party firewall provides NAT, Firewall and DHCP to PCs
- WAN interface has one free IP address:
  - The EdgeMarc is assigned one IP address from the WAN subnet
  - Other address(es), including the one already being used by the 3<sup>rd</sup>-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.

#### Limitations

- This configuration requires two drops per cube or office.
  - DHCP is used separately for PCs and Phones, requiring two broadcast domains. Two broadcast domains means two LANs.

#### **Implementation Steps**

Utilizing the EdgeMarc GUI, follow the standard instructions (described in the user's guide) to enable the following on the EdgeMarc:

- 1. Enable Network
  - WAN IP address 67.40.40.3
  - LAN IP address 10.10.10.1
- 2. Enable NAT
- 3. Enable ALG functionality
- 4. Enable Traffic Shaping
- 5. Enable DHCP
- 6. Enable Firewall
- 7. Enable System -> Proxy ARP

Configure Proxy ARP so that the EdgeMarc bridges the external Firewall's IP address from the EM's WAN i/f to its LAN i/f.

- The IP address to be forwarded is 67.40.40.2/32
- Bridge traffic back to the default gateway 67.40.40.1

When done, the Proxy ARP screen should look similar to the following:

redgewater	Proxy ARP					<u>Hel</u>
Configuration Menu	Proxy ARP is user IP address or net the firewall and I using the addres	d to create a work. Addres NAT, allowing ses. www.APP_the.ups	bridge be ses and r complete	etween the WA networks that e unprotected r will need to reas	N and the L are bridged b access to the	AN for ar oypass e system
<u>Network</u>	address with this sys	tem's WAN MAC	address. Fl	ush the upstream	router's ARP ca	iche after
DHCP Relay	configuring Proxy ARF	2.				
DHCP Server		Configui	red Prox	y ARP Entri	es	
NAL DDTD Server	IP Address	Network N	Aask (Bits)	Proxy on IF	Gateway	On IF
STD I IA	8 67.40.40.2	32		WAN	67.40.40.1	LAN
Security	Edit Proxy ARP	List				
Survivability	IP Address:		67.40.40.2			
Test UA	Network Mask (E	Bits):	32			
Traffic Shaper	Interface respon	ndina to ARP:	WAN -			
VoIP ALG	Gateway:		67,40,40,1			
VoIP Traversal	On Interface		LAN V			
VPN			1777777 A			
<u>VVAIN LINK</u> Redundancy	Add Clear					
System						
Backup / Restore	Submit Reset	Apply Later				
▶ <u>Clients List</u>						
Dynamic DNS     Eile Download						
▶ <u>File Server</u>						
Management						
Interface Network						
Information						
<u>Network Restart</u>						
Tools	-					
Proxy ARP						
<u>RADIUS Settings</u> Pabaat Sustam						



Edgewater does not recommend this design. With one LAN Ethernet and only one LAN on the EdgeMarc, broadcasts (such as ARPs) issued by the VPN/Firewall device on one of its interfaces will loop around and be heard on its other interface. Additionally, some models of firewalls will actually rebroadcast a message from one interface to the other, causing a packet storm.

Certain VPN/Firewall devices, such as the PIX, can handle this topology, but such devices are the exception.

## Option C: VLAN or Non-VLAN Edgewater appliance, non-VLAN switches, two WAN subnets





## **Characteristics**

- Create two LAN-side VLANs:
  - One VLAN with a public subnet for the 3<sup>rd</sup>-party VPN / Firewall device (associated with EM LAN port 3)
  - One VLAN with private subnet for phones (associated with EM LAN port 1)
- VPN / Firewall device provides DHCP, Firewall and NAT to PCs and servers
  - The VPN creates a third subnet (192.168.3.0, above), but it is ignored by the EdgeMarc and only used by the VPN and associated PCs.
- EdgeMarc provides Firewall and NAT to phones

## Limitations

- Plug 'n Dial not available for Phones
  - Phones must be manually configured with SIP Proxy or MGCP Control Server address.
- This configuration is only possible on Edgewater appliances that provide VLAN support (200/250/4300/4500/4600 Series EdgeMarcs).

#### Step 1

Utilizing the EdgeMarc GUI, follow the standard instructions (described in the user's guide) to enable the following on the EdgeMarc:

- 8. Enable Network with VLAN functionality
  - Set the four LAN ports to 802.1 (assuming the LAN Ethernet switch is not VLAN capable)
  - Modify VLAN 2730 as: IP address: 192.168.1.1 with mask 255.255.255.0 Physical ports: 1, 2 and 4
  - Add a VLAN with: ID: 2 IP address: 67.40.40.1 with mask 255.255.255.252
  - Associate VLAN 2 with LAN port 3

When done, the VLAN screen should look similar to the following:

#### VLAN Configuration Page:

edgewater	VLA	N Conf	iguration		Help
	VLAN	Configur	ration allows the	e user to configure VL	LAN support.
Configuration Menu	<u>Crea</u>	te VLAN   !	VLAN Membership   .	VLAN Port	
Network			VLAN Co	onfiguration	
<u>VLAN Configuration</u>	Selec	t: <u>All</u> <u>None</u>	6		Delete
<u>Configuration</u> DHCP Relay		VLAN ID	IP Address	Subnet Mask	Isolate VLAN
DHCP Server		2	67.40.40.1	255.255.255.252	N
<u>NAT</u> PPTP Server		2730	192.168.1.1	255.255.255.0	N
	Cre	ate a ne	w VLAN		
<u>security</u> Survivability	VLA	N ID:			
<u>est UA</u>	IP A	.ddress:			
raffic Shaper	Sub	het Mask			
OIP ALG	Icol	ato VLAN	I from other VI A		
PN			I II OITI OLI EI VLA ]		
<u>'AN Link</u>					
<u>edundancy</u>					
<u>ystem</u>					

edgewater	VLAN Port Membership	Help
Configuration Menu • Network • Subinterfaces • VLAN Configuration	VLAN Port Membership allows the user to assign VLAN.   Create VLAN   VLAN Membership   VLAN Port   VLAN ID: 2	n ports as members of a
Configuration	VLAN Port Membershi	р
DHCP Relay     DHCP Server	Select: All None	
• NAT	Port Number	Member
PPTP Server	1	
◆ <u>SIP UA</u>	2	
<ul> <li><u>Security</u></li> </ul>	3	
<u>Survivability</u> Tast LA	4	
<ul> <li><u>Iest DA</u></li> <li><u>Traffic Shaper</u></li> <li><u>VoIP ALG</u></li> <li><u>VOIP Traversal</u></li> <li><u>VPN</u></li> <li><u>WAN Link</u></li> <li><u>Redundancy</u></li> <li><u>System</u></li> </ul>	Submit Reset Apply Later	

## VLAN 2730 Port Membership:

edgewater	VLAN Port Membership	Help
Configuration Menu • <u>Network</u> • <u>Subinterfaces</u> • <u>VLAN Configuration</u>	VLAN Port Membership allows the user to assi VLAN.	gn ports as members of a
Configuration	VLAN Port Members	hip
DHCP Kerver     DHCP Server	Select: All None Port Number	Member
NAT     PPTP Server	1	
<u>SIP UA</u>	2	
<u>Security</u>	3	
<ul> <li>Survivability</li> <li>Test LIA</li> </ul>	4	
<ul> <li>Traffic Shaper</li> <li>VoIP ALG</li> <li>VOIP Traversal</li> <li>VPN</li> <li>WAN Link</li> <li>Redundancy</li> <li>System</li> </ul>	Submit Reset Apply Later	

<pre>// edgewater</pre>	VLAN Port Config	uration			<u>Help</u>
Configuration Menu	VLAN Port Configuratic port. 	n allows the user to configur	re VLAI	∖ settings pe	r
<ul> <li><u>Network</u></li> <li><u>Subinterfaces</u></li> </ul>	Port Number	Packet type		PVID	
<ul> <li>VLAN Configuration</li> <li>WAN VLAN</li> </ul>	1	Untagged Only	•	2730	-
Configuration	2	Untagged Only	•	2730	•
DHCP Relay     DHCP Server	3	Untagged Only	•	2	•
<u>NAT</u>	4	Untagged Only	•	2730	•
<ul> <li>PPTP Server</li> <li>SIP UA</li> <li>Security</li> <li>Survivability</li> <li>Test UA</li> <li>Traffic Shaper</li> <li>VoIP ALG</li> <li>VoIP Traversal</li> <li>VPN</li> <li>WAN Link</li> <li>Redundancy</li> <li>System</li> </ul>	Submit Reset Apply	Later			

- 9. Enable NAT
- 10. Enable ALG functionality
  - Specify VLAN 2730 for the ALG
- 11. Enable Traffic Shaping
- 12. **Disable** DHCP on both VLANs #2 and #2730
- 13. Enable Firewall

## **Step 2** Cofigure Pass-Through Rules for Public DMZ.

**Pass-Through Rules Page:** 

edgewater	Pass	s-Thro	ough	Rules				for a subset of			<u>Help</u>
Configuration Menu	When subnet	forwardir t. To add	ig a subi an addi	net, an IP tional IP a	address ne ddress to t	eds to b he syste	e assigned m, visit th	tor a subnet f to the system ie <u>Subinterface</u>	nom one interface to m to serve as the de <u>es</u> page.	fault rou	ter for the
Network	Add	a Pass	-Thro	iah Rule							
DHCP Relay DHCP Server	Proto	col:		agiri (ai	Any	-					
NAT	Inpu	t Interf	ace:		WAN						
PPTP Server	Sour	ce IP:									
SIP UA	Sour	ce Masl	<:								
Certificate Store	Cust	om Sou	irce Poi	rts:							
HTTPS	Outp	out Inte	rtace:		VLAN_2	•	-				
► MOTD	Dest	ination	IP:		67.40.40.0						
Pass-Through	Dest	ination	Mask:	n Dortou	255.255.25	5.252					
Session Management System Audit		et: Clea	r	on Ports:	Accept 👻						
▶ <u>User Management</u> Survivability						Pass-	Throug	h Rules			
Traffic Shaper VoIP ALG	Sele	ct: <u>All No</u>	ne							Action:	Delete
<u>VoIP Traversal</u> <u>VPN</u>		Proto	In Intf	Src IP	Src Mask	Src Ports	Out Intf	Dest IP	Dest Mask	Dest Ports	Target
WAN Link Redundancy		any	WAN	0.0.0.0	0.0.0.0	any	vlan_2	67.40.40.0	255.255.255.252	any	ACCEPT
Backup / Restore     Clients List     Dynamic DNS											



## **Characteristics**

- EdgeMarc provides DHCP, Firewall and NAT to phones
- VPN / Firewall provides DHCP, Firewall and NAT to PCs and servers

#### Limitations

• This configuration requires <u>two</u> Ethernet drops to each desk

#### Implementation Steps for the example

#### Step 1

Follow the standard instructions (described in the user's guide) to enable the following on the EdgeMarc:

- Enable NAT
- Enable ALG functionality
- Enable Traffic Shaping
- Enable DHCP
- Enable Firewall

## Pass-Through Rules Page:

edgewater	Pas	s-Thro	ough	Rules							He
Configuration Menu	Pass-" When the su	Through F forwardir Ibnet. To	Rules per ng a sub add an	rmits the fi net, an IP additional	rewall to fo address ne IP address	orward d eds to b to the s	ata traf e assigr ystem,	fic for a subne ned to the sys visit the <u>Subir</u>	et from one interface tem to serve as the <u>iterfaces</u> page.	e to anoti default i	ner. router for
<u>Network</u> DHCD Polov	Add	a Pass	-Thro	uah Rule	<u>.</u>						
DHCP Relay     DHCP Server	Prot	ocol:		3	Anv	-					
NAT	Inpu	it Interf	ace:		WAN	•					
PPTP Server	Sour	ce IP:	554989898998			0.04					
SIP UA	Sour	re Masl	C.								
Security	Cust	om Sol	irce Do	rte	-						
▶ <u>Certificate Store</u>	Outr	out Inte	rfaco:	103.	LAN	-1					
+HTTPS Configuration	Doct	ination	TD.		67.40.40.0	-	_				
• MOTD	Deat	ination	Moole		07.40.40.0	5 959	_				
Pass-Through	Dest		Mask.		200.200.20	9.292	_				
, Session	L	.om Des	sunatio	on Ports:							
Management	larg	et:			Accept 🔻						
System Audit     Trusted Hosts	Add	l Clea	r								
• User Management	38										
Survivability						Pass-T	hroud	h Rules			
<u>Test UA</u>								J			
Traffic Shaper     Vote ALG	Sele	ct: <u>All</u> <u>No</u>	ine							Action:	Delete
VoIP Traversal			In		Src	Src	Out			Dest	
VPN		Proto	Intf	Src IP	Mask	Ports	Intf	Dest IP	Dest Mask	Ports	Targe
<u>WAN Link</u> Redundancy		any WAN 0.0.0.0			0.0.0.0	any	LAN	67.40.40.0	255.255.255.252	any	ACCEP
System	<u> </u>	1		1	1			I	1		
Backup / Restore     Clients List											

## LAN sub-interface:

edgewater	Subinterfaces		Help
Configuration Menu	interface. After creating a LAN pass-through rule to permit IP the <u>Pass-Through Rules</u> page.	subinterface, it is often necessary to packets through the system. To conf	ies to a system ) configure a firewall igure pass-through, visit
Network	-		
Subinterfaces     VLAN Configuration     WAN VLAN     Configuration     DHCP Relay     DHCP Server     NAT     PPTP Server	Add a Subinterface: IP Address: 67.40.40.1 Netmask: 255.255.255.252 Interface: LAN • Add Clear		
<u>SIP UA</u>		Subinterfaces	
<u>Security</u> Survivability	Select: <u>All</u> <u>None</u>		Delete
Test UA	IP Address	Netmask	Interface
Traffic Shaper VoIP ALG VoIP Traversal	67.40.40.1	255.255.255.252	LAN
<u>VPN</u> WAN Link Redundancy			

## Option D: VLAN-capable Ethernet switch, VLAN or Non-VLAN Edgewater appliance

### Sub-option D1: VLAN-capable EdgeMarc



#### **Characteristics**

- EdgeMarc provides NAT, Firewall and DHCP Plug 'n Dial to phones
- 3<sup>rd</sup>-party firewall provides NAT, Firewall and DHCP to PCs
- WAN interface has at least one free IP address:
  - The EdgeMarc is assigned one IP address from the WAN subnet
  - Other address(es), including the one already being used by the 3<sup>rd</sup>-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs
  - VLAN #200 with private subnet for phones (associated with EM LAN port 2). This LAN uses 802.1q frames.
  - VLAN #2 with a public subnet for the 3<sup>rd</sup>-party VPN / Firewall device (associated with EM LAN port 3). This LAN uses standard 802.1 frames.

#### Limitations

• Requires VLAN-capable and CDP-capable Ethernet switch and phones.

#### **Implementation Steps**

Utilizing the EdgeMarc GUI, follow the standard instructions (described in the user's guide) to enable the following on the EdgeMarc:

- 1. Enable Network with VLAN functionality
  - Set LAN Port 2 to 802.1q framing. Set LAN Ports 1, 3 and 4 to 802.1 framing.
  - Leave VLAN 2730 as management port: IP Address: 192.168.1.1 with mask 255.255.255.0
  - Add a VLAN with: ID: 200 IP address: 10.10.10.1 with mask 255.255.255.0
  - Add a VLAN with: ID: 2 IP address: 10.0.0.1 with mask 255.255.255.0
  - Associate VLAN 2730 with LAN ports 1 and 4
  - Associate VLAN 200 with LAN port 2
  - Associate VLAN 2 with LAN port 3

When done, the VLAN screen should look similar to the following:

## VLAN Configuration Page:

	VLAN	l Configur	ation allows the	user to configure V	LAN suppo
onfiguration Menu	<u>Crea</u>	te VLAN   <u>V</u>	/LAN Membership   \	VLAN Port	
<u>Network</u> Subinterfaces			VLAN Co	nfiguration	
VLAN Configuration	Selec	t: <u>All None</u>	i.		Delete
Configuration DHCP Relay		VLAN ID	IP Address	Subnet Mask	Isolate VLAN
HCP Server		2	10.0.0.1	255.255.255.0	N
<u>AT</u> PTP Server		2730	192.168.1.1	255.255.255.0	N
IP UA		200	10.10.10.1	255.255.255.0	N
iest UA iest UA iraffic Shaper /oIP ALG /oIP Traversal /PN VAN Link Redundancy System Packup / Restore	Cre VLA IP A Sub Isol Add	ate a nev N ID: .ddress: net Mask: ate VLAN Reset	<b>v VLAN</b> from other VLAI	Ns 🗖	

edgewater	VLAN Port Membership	Help
Configuration Menu • Network • Subinterfaces • VLAN Configuration	VLAN Port Membership allows the user to as VLAN.   <u>Create VLAN   VLAN Membership   VLAN Port  </u> VLAN ID: 2	sign ports as members of a
Configuration	VLAN Port Membe	rship
DHCP Server	Select: <u>All None</u> Port Number	Member
<u>NAT</u> <u>PPTP Server</u>	1	
◆ <u>SIP UA</u>	2	
Security	3	
<ul> <li>Survivability</li> <li>Test UA</li> </ul>	4	
<ul> <li>Traffic Shaper</li> <li>VoIP ALG</li> <li>VoIP Traversal</li> <li>VPN</li> <li>WAN Link</li> <li>Redundancy</li> <li>System</li> </ul>	Submit Reset Apply Later	

## VLAN 2730 Port Membership:

edgewater	VLAN Port Membership	Hel
Networks	VLAN Port Membership allows the user to VLAN.	assign ports as members of a
Menu	<u>Create VLAN</u>   <u>VLAN Membership</u>   <u>VLAN Port</u>	
Network     Subinterfaces     VLAN Configuration     WAN VI AN	VLAN ID: 2730 -	
Configuration	VLAN Port Meml	pership
DHCP Relay	Select: <u>All None</u>	32
DHCP Server	Port Number	Member
PPTP Server	1	
SIP UA	2	
<u>Security</u>	3	
<ul> <li>Survivability</li> <li>Toot UA</li> </ul>	4	V
Traffic Shaper       VoIP ALG       VoIP Traversal       VPN       WAN Link       Redundancy       System	Submit Reset Apply Later	

edgewater	VLAN Port Membership	Hel
NETWORKS	VLAN Port Membership allows the user to	assign ports as members of a
Configuration Menu	Create VI AN 1 VI AN Memberchin 1 VI AN Port 1	
<ul> <li><u>Network</u></li> <li><u>Subinterfaces</u></li> </ul>		
<u>VLAN Configuration</u> <u>WAN VLAN</u> Configuration	VI AN Dort Mem	herchin
DHCP Relay	Select: All None	
DHCP Server	Port Number	Member
• <u>NAT</u>	1	
<u>PPTP Server</u>	-	
• <u>SIP UA</u>	2	<u>v</u>
<ul> <li><u>Security</u></li> <li>Survivebility</li> </ul>	3	
• <u>Survivability</u>	4	
<u>Traffic Shaper</u> Valle ALC	Submit Beset AnnlyLater	
<ul> <li>VOIP ALG</li> <li>VOID Travorcal</li> </ul>		
WAN Link		
Redundancy		
• <u>System</u>		
▶ Backup / Restore		
▶ <u>Clients List</u> ▶Dupamic DNC		

## VLAN Port Configuration:

edgewater	VLAN Port Config	uration	1.0.4		<u>Help</u>
Configuration Menu • Network	VLAN Port Configuratio port.   <u>Create VLAN</u>   <u>VLAN Memb</u>	pership   YLAN Port		n settings	; per
• <u>Subinterfaces</u>	Port Number	Packet type		PVII	)
► <u>VLAN Configuration</u> WAN VLAN	1	Untagged Only	•	2730	•
Configuration	2	Tagged Only	•	200	-
DHCP Relay     DHCP Server	3	Untagged Only	-	2	-
<u>NAT</u>	4	Untagged Only	•	2730	•
PPTP Server     SIP UA     Security     Survivability     Test UA     Traffic Shaper     VoIP ALG     VoIP Traversal     VPN	Submit Reset Apply	Later			5

- 2. Enable NAT
- 3. Enable ALG functionality
  o Specify VLAN 200 for the ALG
- 4. Enable Traffic Shaping

When done, the DHCP page should look similar to the following:

edgewater	DHCP Server	Help
Configuration Menu	DHCP IP Address Range	S
• <u>Network</u>	Select: <u>All None</u>	Delete
DHCP Relay     DHCP Server	Start IP Address End IP Ad	ddress
DHCP Leases     Vendor Specific     Configuration	10.10.10	10.10.10.200
<ul> <li><u>Configuration</u></li> <li><u>NAT</u></li> <li><u>PPTP Server</u></li> <li><u>SIP UA</u></li> <li><u>Security</u></li> <li><u>Survivability</u></li> <li><u>Test UA</u></li> <li><u>Traffic Shaper</u></li> <li><u>VOIP ALG</u></li> <li><u>VOIP Traversal</u></li> <li><u>VPN</u></li> <li><u>WAN Link</u></li> <li><u>Redundancy</u></li> <li><u>System</u></li> <li><u>Backup / Restore</u></li> <li><u>Clients List</u></li> <li><u>Dynamic DNS</u></li> </ul>	Add a DHCP range         Start IP Address:         End IP Address:         Add         Reset    Subnet: Subnet Mask: Enable DHCP Server: Lease Duration (Days): Time Offset, +/- hours (option 2): Primary DNS: Cases days DNO:	10.10.10.1 (VID=200) 255.255.255.0 7
File Download     File Server     Management     Interface     Network     Information	Secondary DNS: NTP Server Address (option 42): WINS Address (option 44): TFTP/FTP Server Name (option 66):	
Network Restart     Network Test     Tools     Proxy ARP	Boot File Name (option 67): VLAN ID Discovery (option 129): Option 150:	
RADIUS Settings     Reboot System     Route     Services	Option 159: Option 160:	
Configuration	Enable Vendor specific configuration (option 43):	

- 6. Enable Firewall
- 7. System -> Proxy ARP

Configure Proxy ARP so that the EdgeMarc bridges the external Firewall's IP address from the EM's WAN i/f to its LAN i/f.

- VLAN 2 is associated with LAN Port 3
- The IP address to be forwarded is 67.40.40.2/32
- Bridge traffic back to the default gateway 67.40.40.1

edgewater	Proxy ARP					пец
Configuration Menu • Network • DHCP Relay	Proxy ARP is used IP address or netw the firewall and N using the address When configuring Prox address with this syst configuring Proxy ARP.	to create a work. Addres AT, allowing es. y ARP, the ups em's WAN MAC	bridge be ses and r complete address. Fl	etween the WA networks that e unprotected r will need to reas ush the upstream	N and the L. are bridged b access to the sociate the pro- router's ARP ca	AN for an oypass e systems xied IP ache after
NAT	IP Address	Network N	lask (Bits)	Proxy on IF	Gateway	On IF
PPTP Server	8 67.40.40.2	32		WAN	67.40.40.1	VLAN2
Security Security Survivability Test UA Traffic Shaper VoIP ALG VoIP Traversal VPN WAN Link Redundancy System • Backup / Restore • Clients List • Dynamic DNS • File Download • File Server • Management Information • Network Restart • Network Test Tools • Proxy ARP	Edit Proxy ARP I IP Address: Network Mask (Bi Interface respond Gateway: On Interface: Add Clear	L <b>ist</b> its): ding to ARP: ApplyLater	67.40.40.2 32 WAN - 67.40.40.1 VLAN2			

## Sub-option D2: Non-VLAN EdgeMarc



#### **Characteristics**

- EdgeMarc provides NAT, Firewall and DHCP Plug 'n Dial to phones
- 3<sup>rd</sup>-party firewall provides NAT, Firewall and DHCP to PCs
- WAN interface has at least one free IP address:
  - The EdgeMarc is assigned one IP address from the WAN subnet
  - Other address(es), including the one already being used by the 3<sup>rd</sup>-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two Subnets (over one LAN segment)
  - Subnet 10.10.10.0/24 for phones (VLAN #200 within switch)
  - Proxy ARP subnet 67.40.40.2/32 for the 3<sup>rd</sup>-party VPN / Firewall device (VLAN #2 within switch).

#### Limitations

- Requires VLAN-capable and CDP-capable Ethernet switch and phones.
- VLANs #2 and #200 share Ethernet segment at EdgeMarc

#### **Implementation Steps**

Utilizing the EdgeMarc GUI, follow the standard instructions (described in the user's guide) to enable the following on the EdgeMarc:

- 1. Enable Network
  - WAN IP address 67.40.40.3
  - LAN IP address 10.10.10.1
- 2. Enable NAT
- 3. Enable ALG functionality
- 4. Enable Traffic Shaping
- 5. Enable DHCP
- 6. Enable Firewall
- 7. System -> Proxy ARP

Configure Proxy ARP so that the EdgeMarc bridges the external Firewall's IP address from the EM's WAN i/f to its LAN i/f.

- The IP address to be forwarded is 67.40.40.2/32
- Bridge traffic back to the default gateway 67.40.40.1

When done, the Proxy ARP screen should look similar to the following:

NETWORKS	Proxy ARP is used	d to create a	bridae be	etween the WA	N and the L	AN for ar
Configuration Menu	IP address or net the firewall and N using the address When configuring Pro-	work. Addres NAT, allowing ses. xy ARP, the ups	ses and r complet tream route	networks that e unprotected or will need to reas	are bridged l access to th sociate the pro	oypass e system oxied IP
DHCP Relay	configuring Proxy ARP			ush the upstream		
DHCP Server	IP Address	Configur	ed Prox	y ARP Entri	es Gateway	On IF
PPTP Server	67 40 40 2	37	nion (Dirio)		67.40.40.1	LAN
SIP UA	<b>5 1 1 1 1 1 1 1 1 1 1</b>			* ** **	01.10.10.1	C/114
Security	Edit Proxy ARP	List				
Survivability	IP Address:		67.40.40.2			
<u>Test UA</u>	Network Mask (E	Bits):	32			
Iraffic Shaper	Interface respon	ding to ARP:	WAN 👻			
VOIP ALG	Gateway:		67.40.40.1			
VolP Traversal	On Interface:		LAN 👻			
<u>WAN LINK</u> Redundancy	Add Clear					
System						
▶Backup / Restore	Submit Recet	Apply 1 stor				
▶ <u>Clients List</u>		Арріу Еслеі				
▶ <u>Dynamic DNS</u>						
▶ File Download						
▶ <u>File Server</u>						
Interface						
Network						
Information						
Network Test						
Tools						
Proxy ARP						

## **Option E – 3<sup>rd</sup>-party Firewall in front of Edgewater appliance**

## **Characteristics**

- External device provides port firewalling
- EdgeMarc provides Traffic Shaping (by having the servers, PCs and phones behind the EdgeMarc)
- EdgeMarc provides DHCP and NAT to PCs and phones
- EdgeMarc provides IP address passthrough from firewall to servers

#### Limitations

• This scenario is more complex than the above in that it requires the firewall to open ports necessary for VoIP protocol.

#### Diagram



## Step 1

Follow the standard instructions (described in user's guide) to enable the following on the EdgeMarc:

- 8. Enable NAT (all configs)
- 9. Enable ALG functionality (all configs)
- 10. Enable Traffic Shaping
- 11. Enable DHCP (all configs EXCEPT configuration B)
- 12. Enable Firewalling (all configs)

## **Step 2** Configure Pass-Through Rules for Public DMZ.

Pass-Through Rules Page:

Configuration Menu       When forwarding a subnet, an IP address needs to b the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the the subnet. To add an additional IP address to the Physical IP address to the the subnet. To add an additional IP address to the Physical IP address to the Physical IP address to the Input Interface:         MAI PPTP Server SIP UA       Source IP: Source IP: Source Mask:	pe assigi system,	ned to the sys visit the <u>Subin</u>	tem to serve as the <u>terfaces</u> page.	default r	outer for
Network     Add a Pass-Through Rule:       DHCP Relay     Protocol:     Any •       DHCP Server     Protocol:     May •       NAT     Input Interface:     WAN •       PPTP Server     Source IP:     Source Mask:	22	2			
DHCP Server     Protocol:     Any ▼       NAT     Input Interface:     WAN ▼       PPTP Server     Source IP:					
NAT     Input Interface:     WAN ▼       PPTP Server     Source IP:	22				
PPTP Server         Source IP:           SIP UA         Source Mask:					
SIP UA Source Mask:					
Custom Source Ports:					
Certificate Store Output Interface: LAN -					
Configuration Destination IP: 67.40.40.0					
MOTD Destination Mask: 255 255 240					
Rules Custom Destination Ports:					
Session Targot:					
Management Target.					
Trusted Hosts		5			
User Management					
Survivability Pass-1	Throug	gh Rules			
Select: All None				Action:	Delete
Proto In Src IP Src Src /PN	Intf	Dest IP	Dest Mask	Dest Ports	Target
WAN Link					_
Redundancy 🗌 any WAN 0.0.0.0 0.0.0.0 any	LAN	67.40.40.0	255.255.255.240	any	ACCEPT
System	- J	1		L	

#### LAN sub-interface Configuration:

edgewater	Subinterfaces	trator to accion additional ID addrocc	<u>Help</u>
Configuration Menu	interface. After creating a LAN : pass-through rule to permit IP p the <u>Pass-Through Rules</u> page.	subinterface, it is often necessary to ackets through the system. To confi	configure a firewall gure pass-through, visit
• <u>Network</u>	-		
Subinterfaces     VLAN Configuration     WAN VLAN     Configuration	Add a Subinterface: IP Address: 67.40.40.1		
DHCP Relay     DHCP Server     NAT	Interface: LAN - Add Clear		
PPTP Server     SIP UA		Subinterfaces	
Security     Survivebility	Select: <u>All None</u>		Delete
<ul> <li><u>Survivability</u></li> <li>Test UA</li> </ul>	IP Address	Netmask	Interface
Traffic Shaper	67.40.40.1	255.255.255.240	LAN
<u>VoIP ALG</u> <u>VoIP Traversal</u> VPN			
WAN Link     Redundancy			
System			

## Step 3

The Firewall *must* be configured to pass through VoIP protocols to the EdgeMarc. The firewall *can not* perform NAT, if it does it will break VoIP protocol.

Since the EdgeMarc is a VoIP proxy, all VoIP packets will have a source or destination IP address of the EdgeMarc's WAN interface. This can be used to help set up appropriately tight rules on the Firewall.

The Firewall must be opened for the following ports (to and from the EdgeMarc):

In all cases		
FTP	ТСР	21
HTTP	ТСР	80
RTP	UDP	16386:21785 <sup>*</sup>
SNMP	UDP	161
SSH	ТСР	22
Telnet	ТСР	23
TFTP	UDP	69
SNTP	ТСР	123
MGCP phones		
MGCP	UDP	2427, 2429, 2432, 2727
SIP phones		
SIP	UDP	5060

		plus any addl. ports
		specified on the VoIP ALG
		page
SIP, Media Server	ТСР	16386:16985
H.323 phones		
Q.931	ТСР	1720
RAS	UDP	1719
H.245	ТСР	14085:14385
Skinny (SCCP) phones		
Skinny	ТСР	2000

\*For EdgeMarc boxes supporting up to 300 simultaneous calls.

Copyright © 2004, Edgewater Networks, Inc. All rights reserved.