

## Goal

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

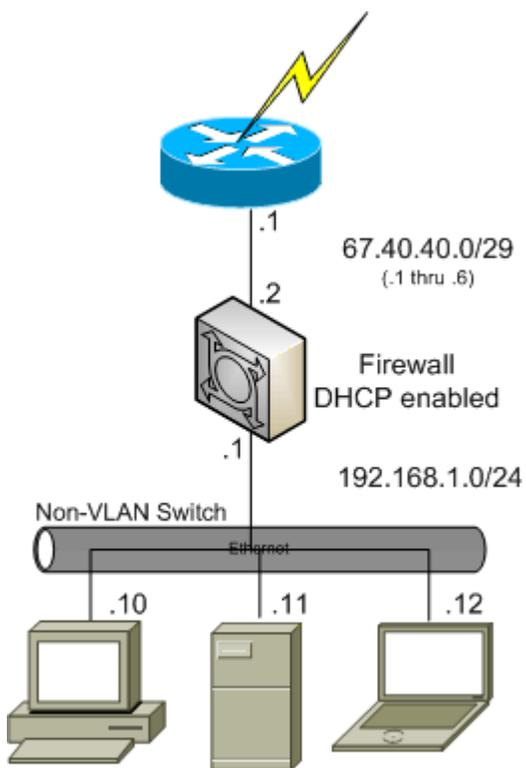
Describe characteristics and tradeoffs of different topologies.

Provide configuration information for the EdgeMarc.

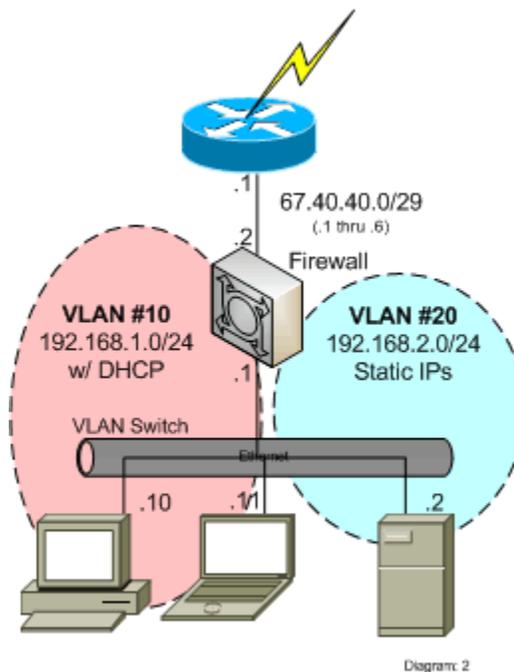
## Pre-Edgewater Configuration

Assume the following configuration prior to installing the EdgeMarc appliance:

### Non-VLAN-capable Ethernet switch



### VLAN-capable Ethernet switch



## Solution

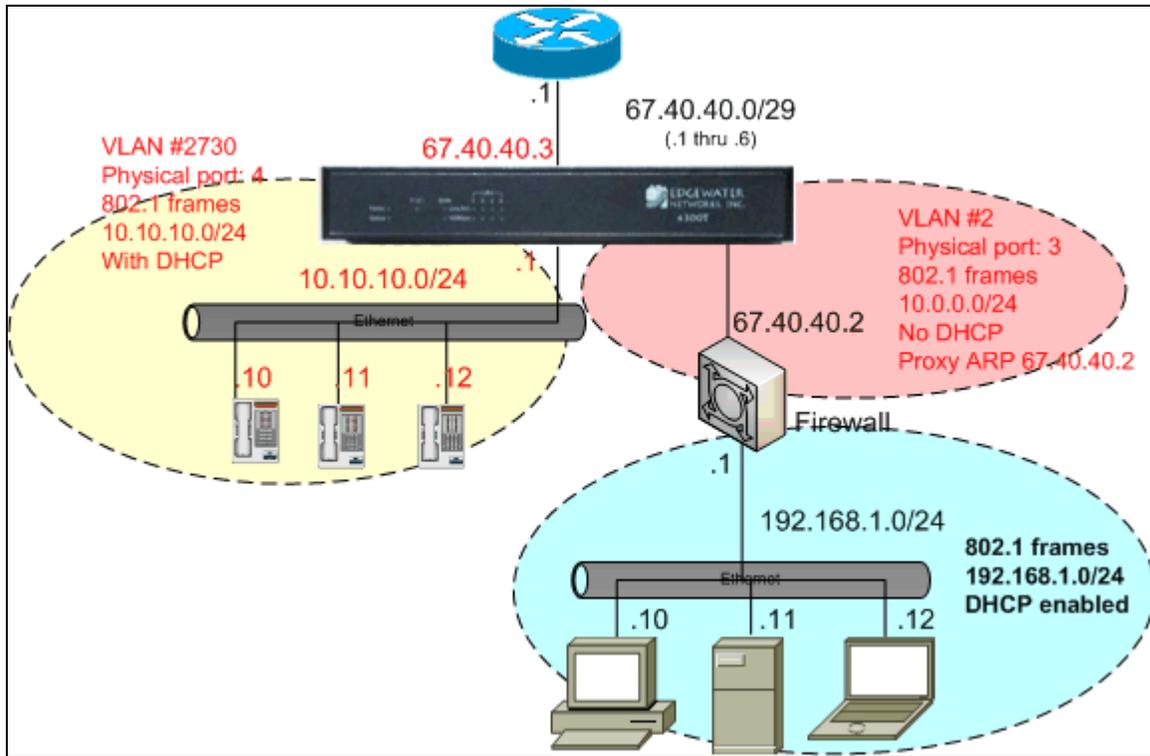
Note: The descriptions below assume VOS v5.1 or later. Those configurations that do not utilize Proxy ARP will also work for older versions of VOS.

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

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

### VLAN Configuration Page:

**edgewater NETWORKS** **VLAN Configuration** [Help](#)

VLAN Configuration allows the user to configure VLAN support.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN Configuration				
Select: <a href="#">All</a> <a href="#">None</a> <a href="#">Delete</a>				
	VLAN ID	IP Address	Subnet Mask	Isolate VLAN
<input type="checkbox"/>	2730	10.10.10.1	255.255.255.0	N
<input checked="" type="checkbox"/>	2	10.0.0.1	255.255.255.0	N

**Create a new VLAN**

VLAN ID:

IP Address:

Subnet Mask:

Isolate VLAN from other VLANs

[Add](#) [Reset](#)

**Configuration Menu**

- ◆ Network
  - ▶ Subinterfaces
  - ▶ VLAN Configuration
    - ▶ WAN VLAN Configuration
- ◆ DHCP Relay
- ◆ DHCP Server
- ◆ NAT
- ◆ PPTP Server
- ◆ SIP UA
- ◆ Security
- ◆ Survivability
- ◆ Test UA
- ◆ Traffic Shaper
- ◆ VoIP ALG
- ◆ VoIP Traversal
- ◆ VPN
  - WAN Link
  - Redundancy
- ◆ System

## VLAN 2 Port Membership:

**edgewater NETWORKS** **VLAN Port Membership** [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID: 2

VLAN Port Membership	
Select: <a href="#">All</a> <a href="#">None</a>	
Port Number	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>

## VLAN 2730 Port Membership:

**edgewater NETWORKS** **VLAN Port Membership** [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID: 2730

VLAN Port Membership	
Select: <a href="#">All</a> <a href="#">None</a>	
Port Number	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>

## VLAN Port Configuration:

**edgewater NETWORKS** **VLAN Port Configuration** [Help](#)

VLAN Port Configuration allows the user to configure VLAN settings per port.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

Port Number	Packet type	PVID
1	Untagged Only	2730
2	Untagged Only	2730
3	Untagged Only	2
4	Untagged Only	2730

**Configuration Menu**

- Network
  - Subinterfaces
  - VLAN Configuration
    - WAN VLAN Configuration
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- SIP UA
- Security
- Survivability
- Test UA
- Traffic Shaper
- VoIP ALG
- VoIP Traversal
- VPN
- WAN Link Redundancy
- System

2. Enable NAT
3. Enable ALG functionality
  - o Specify VLAN 2730 for the ALG
4. Enable Traffic Shaping
5. Enable DHCP on VLAN #2730
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.

- o VLAN 2 is associated with LAN Port 3
- o The IP address to be forwarded is 67.40.40.2/32
- o 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 NETWORKS** **Proxy ARP** [Help](#)

Proxy ARP is used to create a bridge between the WAN and the LAN for an IP address or network. Addresses and networks that are bridged bypass the firewall and NAT, allowing complete unprotected access to the systems using the addresses.

When configuring Proxy ARP, the upstream router will need to reassociate the proxied IP address with this system's WAN MAC address. Flush the upstream router's ARP cache after configuring Proxy ARP.

**Configured Proxy ARP Entries**

	IP Address	Network Mask (Bits)	Proxy on IF	Gateway	On IF
<input type="checkbox"/>	67.40.40.2	32	WAN	67.40.40.1	VLAN2

**Edit Proxy ARP List**

IP Address:

Network Mask (Bits):

Interface responding to ARP:

Gateway:

On Interface:

**Configuration Menu**

- [Network](#)
- [DHCP Relay](#)
- [DHCP Server](#)
- [NAT](#)
- [PPTP Server](#)
- [SIP UA](#)
- [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 Interface](#)
  - ▶ [Network Information](#)
  - ▶ [Network Restart](#)
  - ▶ [Network Test](#)
  - ▶ [Tools](#)
  - ▶ [Proxy ARP](#)
  - ▶ [RADIUS Settings](#)
  - ▶ [Reboot System](#)

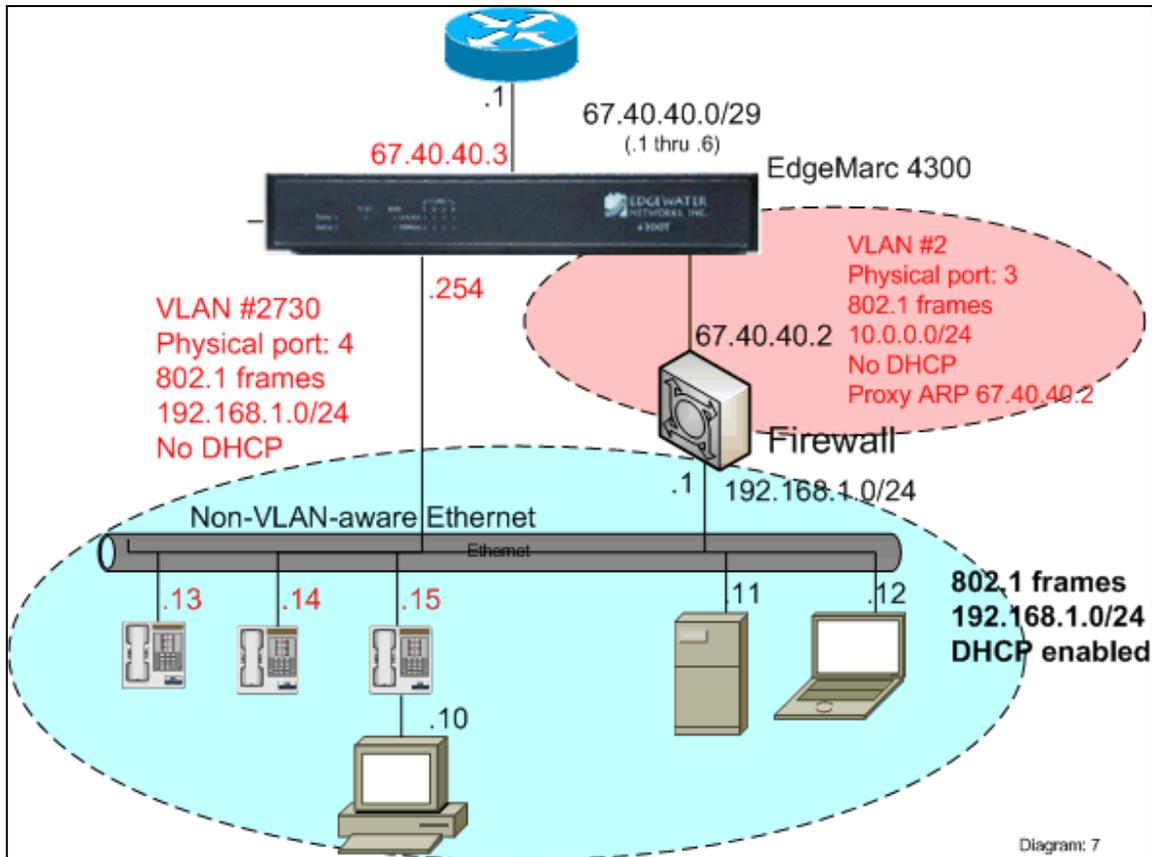


## Implementation Steps

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

- Skip step 5. Enable DHCP on VLAN #2730

## Sub-option A3: Single LAN Ethernet, using the same PC & Phone subnet



## 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.

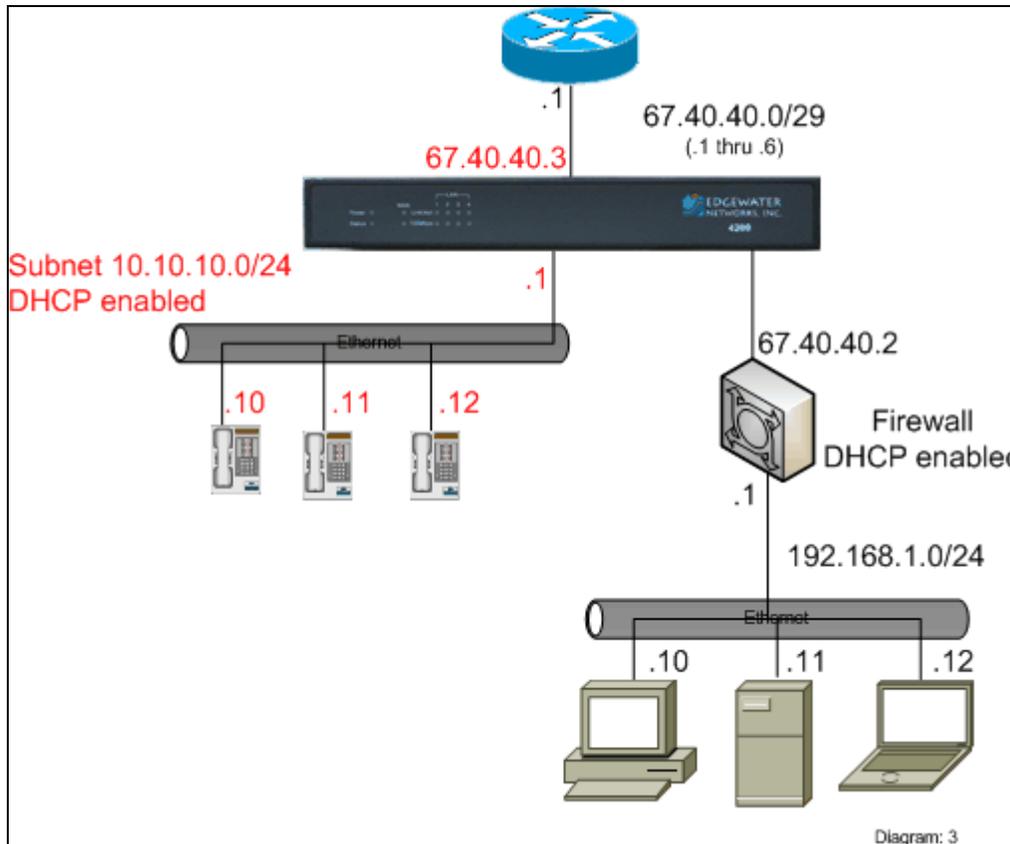
OR

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**



**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.

**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
  - o WAN IP address 67.40.40.3
  - o 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.

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

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

**edgewater NETWORKS** **Proxy ARP** [Help](#)

Proxy ARP is used to create a bridge between the WAN and the LAN for an IP address or network. Addresses and networks that are bridged bypass the firewall and NAT, allowing complete unprotected access to the systems using the addresses.

When configuring Proxy ARP, the upstream router will need to reassociate the proxied IP address with this system's WAN MAC address. Flush the upstream router's ARP cache after configuring Proxy ARP.

### Configured Proxy ARP Entries

	IP Address	Network Mask (Bits)	Proxy on IF	Gateway	On IF
<input type="checkbox"/>	67.40.40.2	32	WAN	67.40.40.1	LAN

#### Edit Proxy ARP List

IP Address:

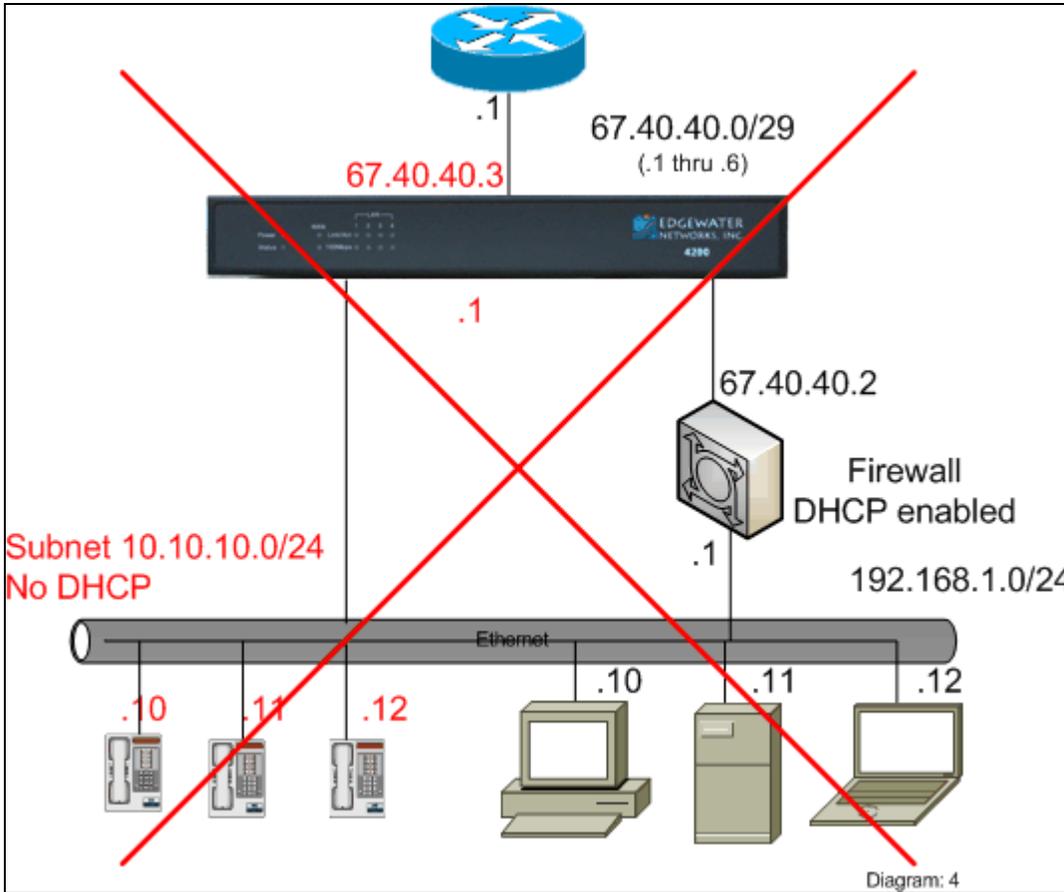
Network Mask (Bits):

Interface responding to ARP:

Gateway:

On Interface:

*Sub-option B2: One LAN Ethernet*

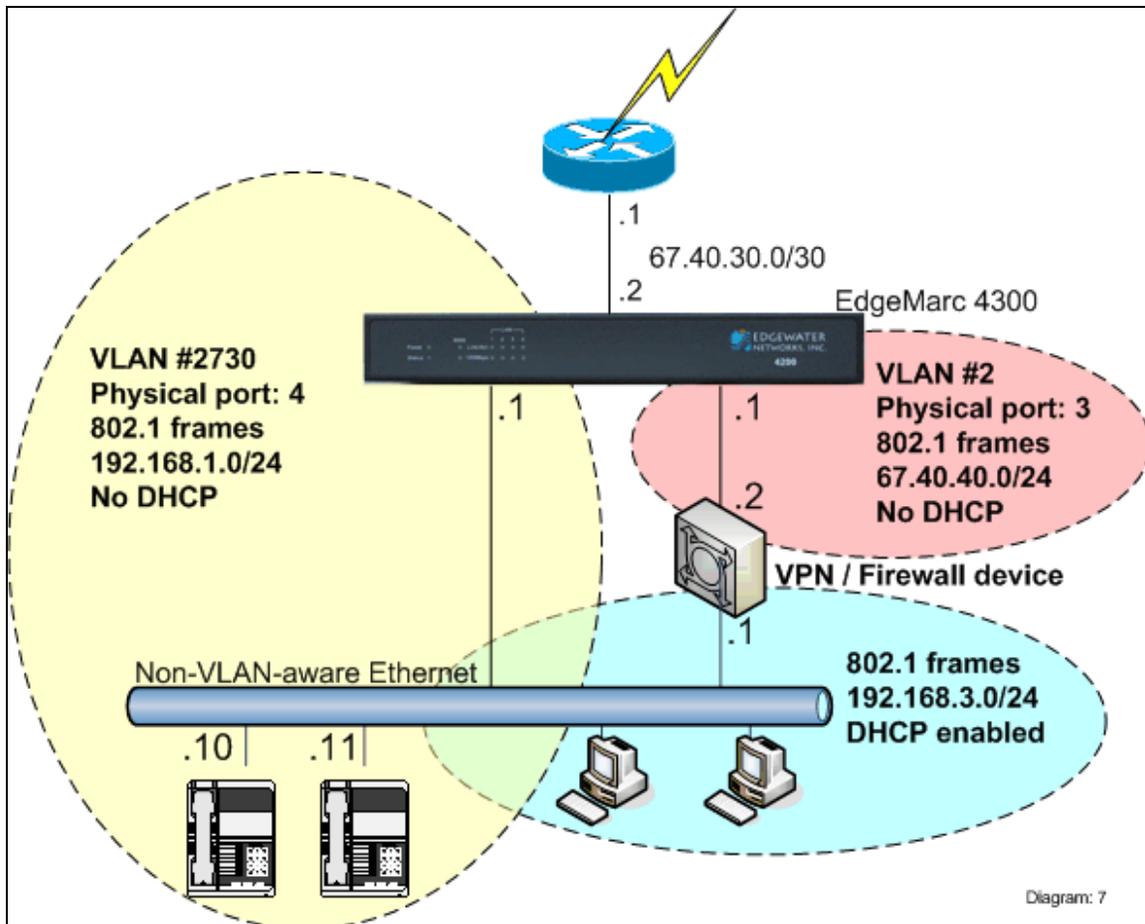


Edgewater does not recommend this design. With one LAN Ethernet and only one LAN on the EdgeMarc, broadcasts (such as ARPs) issued by the VPN/Firewall device on one of its interfaces will loop around and be heard on its other interface. Additionally, some models of firewalls will actually rebroadcast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

### Sub-option C1: VLAN-capable EdgeMarc



### 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).

## Implementation Steps for the example

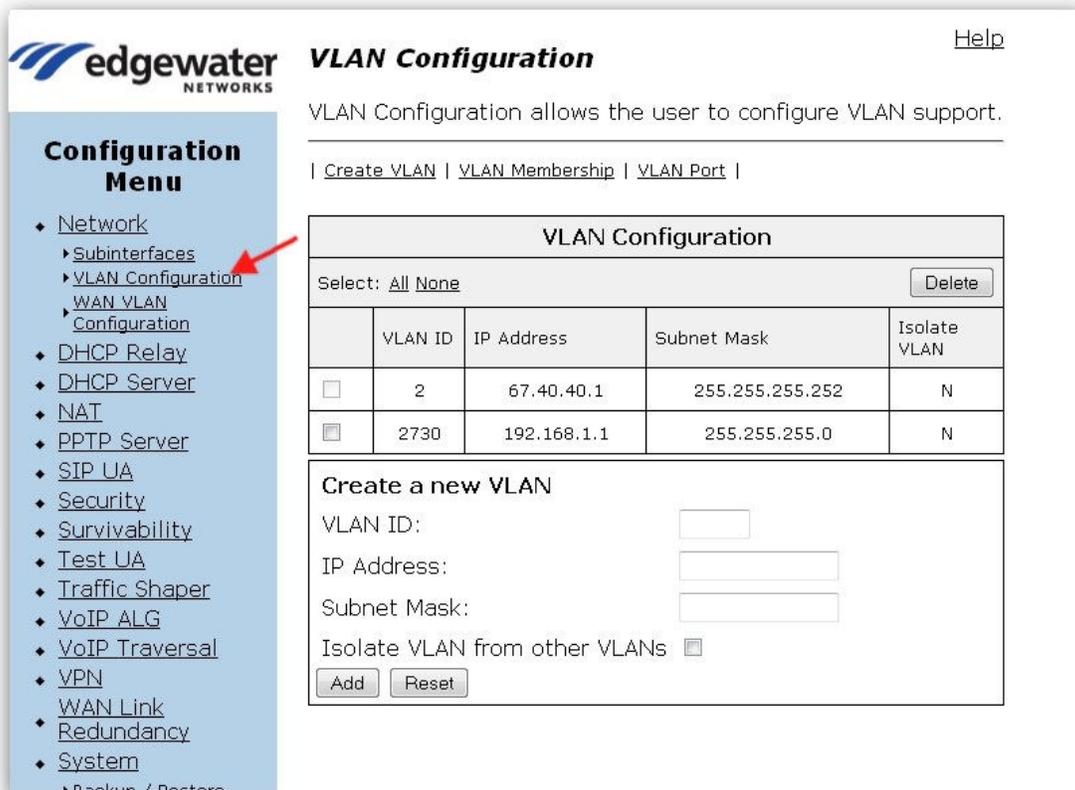
### Step 1

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

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

#### VLAN Configuration Page:



**edgewater NETWORKS** **VLAN Configuration** [Help](#)

VLAN Configuration allows the user to configure VLAN support.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN Configuration				
Select: All None <input type="button" value="Delete"/>				
	VLAN ID	IP Address	Subnet Mask	Isolate VLAN
<input type="checkbox"/>	2	67.40.40.1	255.255.255.252	N
<input checked="" type="checkbox"/>	2730	192.168.1.1	255.255.255.0	N

**Create a new VLAN**

VLAN ID:

IP Address:

Subnet Mask:

Isolate VLAN from other VLANs

## VLAN 2 Port Membership:

**edgewater NETWORKS** **VLAN Port Membership** [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

[Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID:

VLAN Port Membership	
Select: <a href="#">All</a> <a href="#">None</a>	
Port Number	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>

## VLAN 2730 Port Membership:

**edgewater NETWORKS** **VLAN Port Membership** [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

[Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID:

VLAN Port Membership	
Select: <a href="#">All</a> <a href="#">None</a>	
Port Number	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>

## VLAN Port Configuration:

**edgewater NETWORKS** **VLAN Port Configuration** [Help](#)

VLAN Port Configuration allows the user to configure VLAN settings per port.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

Port Number	Packet type	PVID
1	Untagged Only	2730
2	Untagged Only	2730
3	Untagged Only	2
4	Untagged Only	2730

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

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

### Pass-Through Rules Page:

**edgewater NETWORKS** **Pass-Through Rules** [Help](#)

Pass-Through Rules permits the firewall to forward data traffic for a subnet from one interface to another. When forwarding a subnet, an IP address needs to be assigned to the system to serve as the default router for the subnet. To add an additional IP address to the system, visit the [Subinterfaces](#) page.

**Add a Pass-Through Rule:**

Protocol:

Input Interface:

Source IP:

Source Mask:

Custom Source Ports:

Output Interface:

Destination IP:

Destination Mask:

Custom Destination Ports:

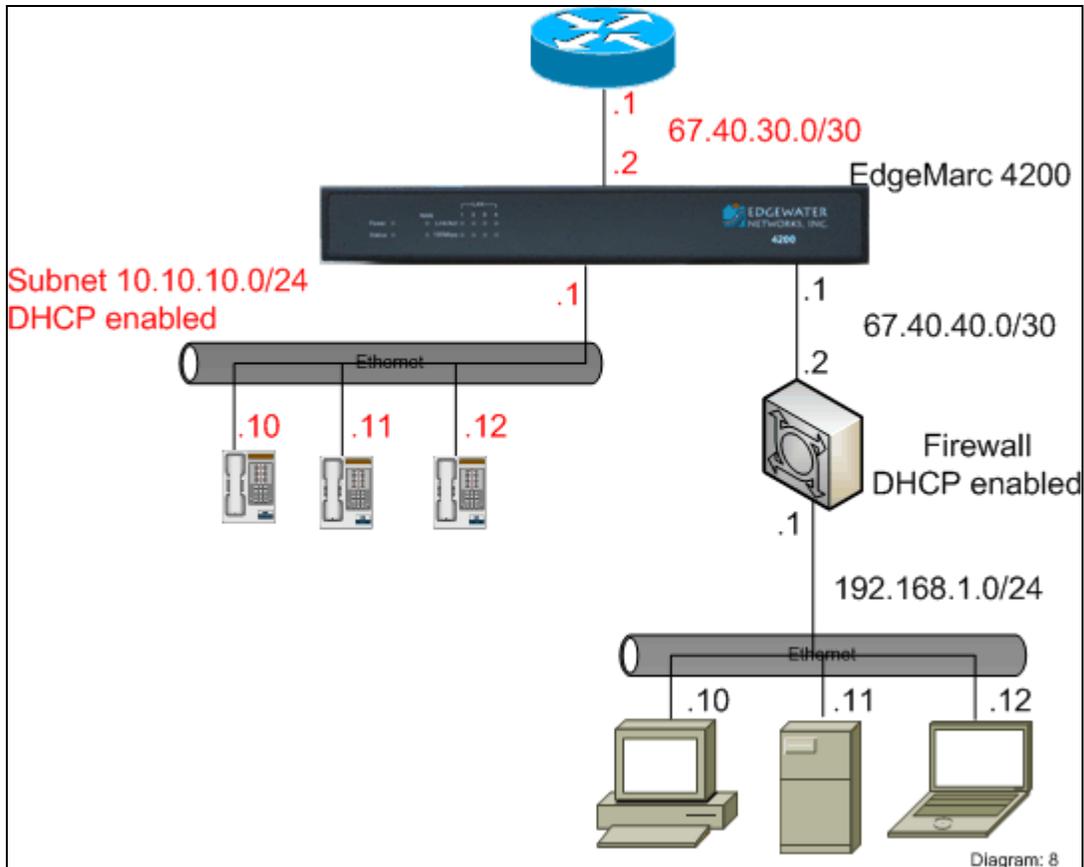
Target:

**Pass-Through Rules**

Select:  Action:

	Proto	In Intf	Src IP	Src Mask	Src Ports	Out Intf	Dest IP	Dest Mask	Dest Ports	Target
<input type="checkbox"/>	any	WAN	0.0.0.0	0.0.0.0	any	vlan_2	67.40.40.0	255.255.255.252	any	ACCEPT

## *Sub-option C2: Non-VLAN EdgeMarc*



### *Characteristics*

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

### *Limitations*

- This configuration requires two 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

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

### Pass-Through Rules Page:

**edgewater NETWORKS** **Pass-Through Rules** [Help](#)

Pass-Through Rules permits the firewall to forward data traffic for a subnet from one interface to another. When forwarding a subnet, an IP address needs to be assigned to the system to serve as the default router for the subnet. To add an additional IP address to the system, visit the [Subinterfaces](#) page.

**Add a Pass-Through Rule:**

Protocol: Any  
 Input Interface: WAN  
 Source IP:  
 Source Mask:  
 Custom Source Ports:  
 Output Interface: LAN  
 Destination IP: 67.40.40.0  
 Destination Mask: 255.255.255.252  
 Custom Destination Ports:  
 Target: Accept

Pass-Through Rules										
Select: <a href="#">All</a> <a href="#">None</a>										Action: <input type="button" value="Delete"/>
	Proto	In Intf	Src IP	Src Mask	Src Ports	Out Intf	Dest IP	Dest Mask	Dest Ports	Target
<input type="checkbox"/>	any	WAN	0.0.0.0	0.0.0.0	any	LAN	67.40.40.0	255.255.255.252	any	ACCEPT

### LAN sub-interface:

**edgewater NETWORKS** **Subinterfaces** [Help](#)

Subinterfaces allows an administrator to assign additional IP addresses to a system interface. After creating a LAN subinterface, it is often necessary to configure a firewall pass-through rule to permit IP packets through the system. To configure pass-through, visit the [Pass-Through Rules](#) page.

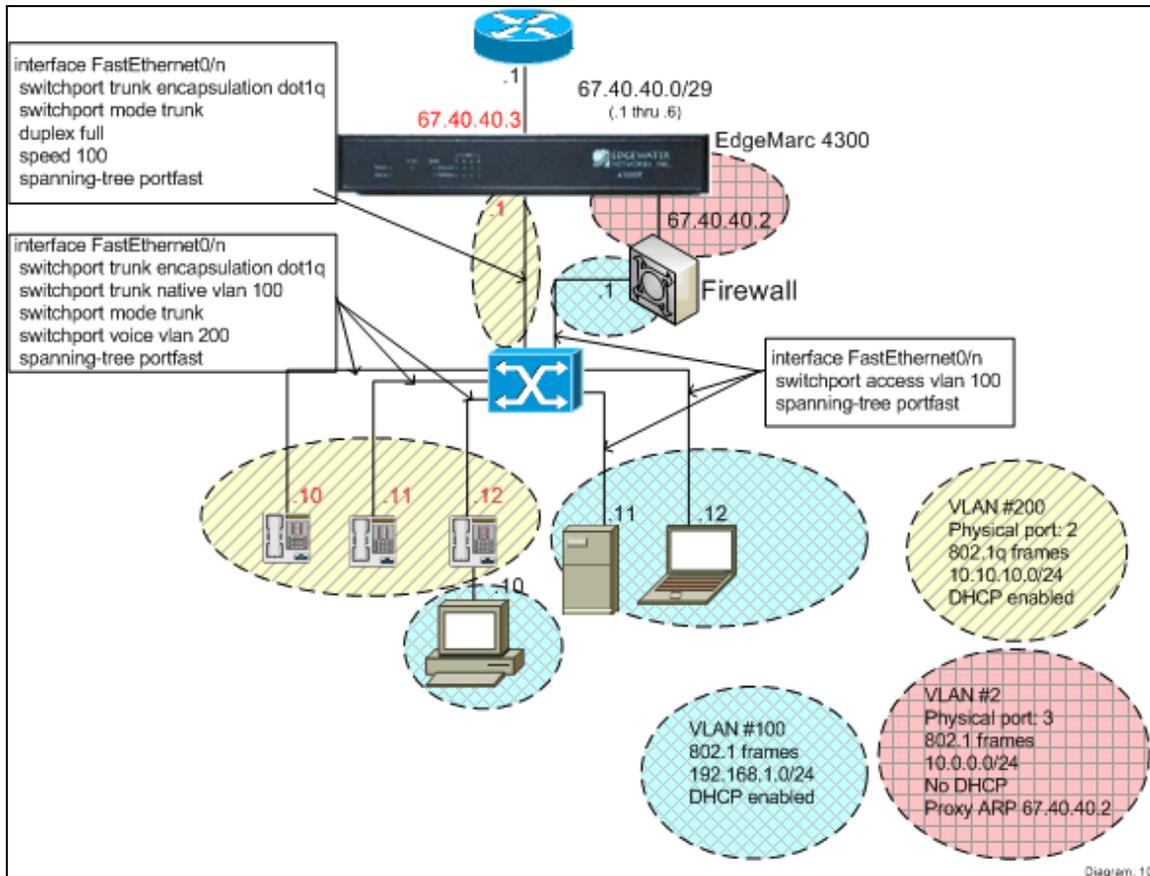
**Add a Subinterface:**

IP Address: 67.40.40.1  
 Netmask: 255.255.255.252  
 Interface: LAN

Subinterfaces			
Select: <a href="#">All</a> <a href="#">None</a>		<input type="button" value="Delete"/>	
	IP Address	Netmask	Interface
<input type="checkbox"/>	67.40.40.1	255.255.255.252	LAN

## 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.

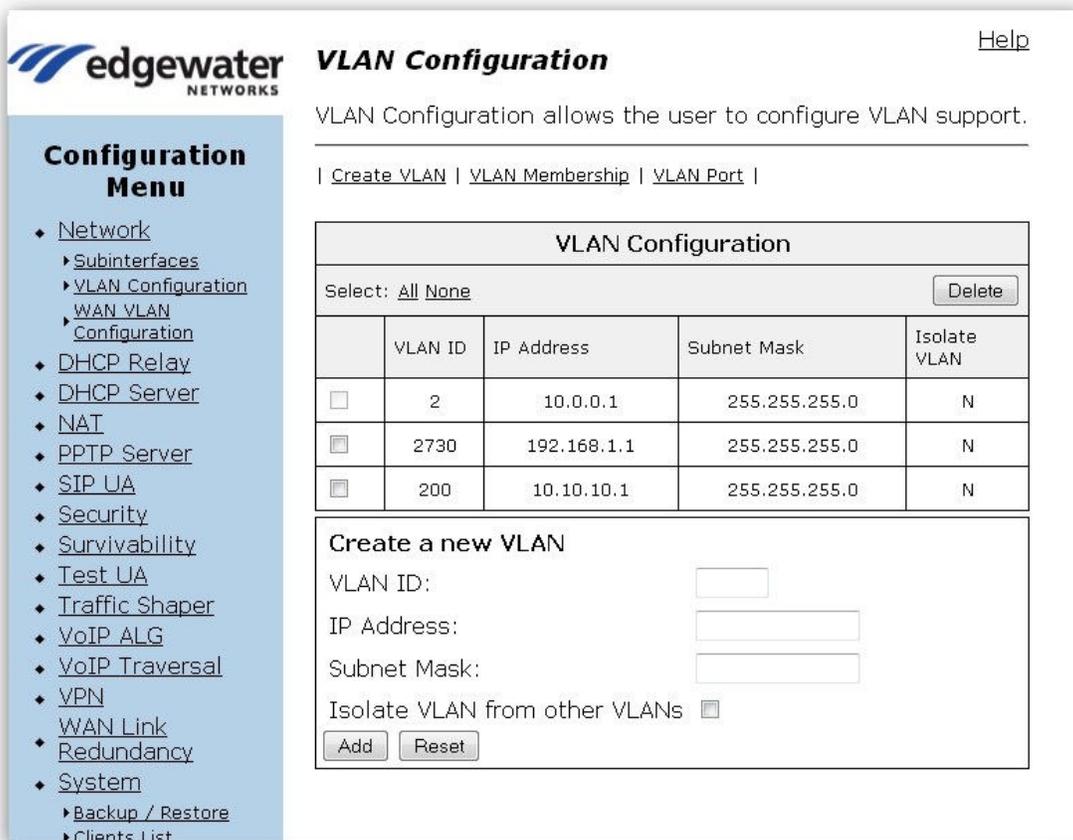
## Implementation Steps

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:



**edgewater NETWORKS** **VLAN Configuration** [Help](#)

VLAN Configuration allows the user to configure VLAN support.

[Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN Configuration				
Select: <a href="#">All</a> <a href="#">None</a> <a href="#">Delete</a>				
	VLAN ID	IP Address	Subnet Mask	Isolate VLAN
<input type="checkbox"/>	2	10.0.0.1	255.255.255.0	N
<input checked="" type="checkbox"/>	2730	192.168.1.1	255.255.255.0	N
<input checked="" type="checkbox"/>	200	10.10.10.1	255.255.255.0	N

**Create a new VLAN**

VLAN ID:

IP Address:

Subnet Mask:

Isolate VLAN from other VLANs

[Add](#) [Reset](#)

**Configuration Menu**

- ◆ [Network](#)
  - ▶ [Subinterfaces](#)
  - ▶ [VLAN Configuration](#)
    - ▶ [WAN VLAN Configuration](#)
- ◆ [DHCP Relay](#)
- ◆ [DHCP Server](#)
- ◆ [NAT](#)
- ◆ [PPTP Server](#)
- ◆ [SIP UA](#)
- ◆ [Security](#)
- ◆ [Survivability](#)
- ◆ [Test UA](#)
- ◆ [Traffic Shaper](#)
- ◆ [VoIP ALG](#)
- ◆ [VoIP Traversal](#)
- ◆ [VPN](#)
- ◆ [WAN Link](#)
- ◆ [Redundancy](#)
- ◆ [System](#)
  - ▶ [Backup / Restore](#)
  - ▶ [Clients List](#)

## VLAN 2 Port Membership:

**edgewater NETWORKS** **VLAN Port Membership** [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID: 2

VLAN Port Membership	
Select: <a href="#">All</a> <a href="#">None</a>	
Port Number	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>

## VLAN 2730 Port Membership:

**edgewater NETWORKS** **VLAN Port Membership** [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID: 2730

VLAN Port Membership	
Select: <a href="#">All</a> <a href="#">None</a>	
Port Number	Member
1	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>

## VLAN 200 Port Membership:

**edgewater NETWORKS** **VLAN Port Membership** [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID: 200

VLAN Port Membership	
Select: All None	
Port Number	Member
1	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>

**Configuration Menu**

- Network
  - Subinterfaces
  - VLAN Configuration
    - WAN VLAN
    - Configuration
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- SIP UA
- Security
- Survivability
- Test UA
- Traffic Shaper
- VoIP ALG
- VoIP Traversal
- VPN
- WAN Link
- Redundancy
- System
  - Backup / Restore
  - Clients List
  - Dynamic DNS

## VLAN Port Configuration:

**edgewater NETWORKS** **VLAN Port Configuration** [Help](#)

VLAN Port Configuration allows the user to configure VLAN settings per port.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

Port Number	Packet type	PVID
1	Untagged Only	2730
2	Tagged Only	200
3	Untagged Only	2
4	Untagged Only	2730

**Configuration Menu**

- Network
  - Subinterfaces
  - VLAN Configuration
    - WAN VLAN
    - Configuration
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- SIP UA
- Security
- Survivability
- Test UA
- Traffic Shaper
- VoIP ALG
- VoIP Traversal
- VPN

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

5. Enable DHCP on VLAN #200

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

The screenshot displays the Edgewater Networks DHCP Server configuration interface. On the left is a 'Configuration Menu' with categories like Network, DHCP Relay, DHCP Server, NAT, PPTP Server, SIP UA, Security, Survivability, Test UA, Traffic Shaper, VoIP ALG, VoIP Traversal, VPN, WAN Link, Redundancy, and System. The main area is titled 'DHCP Server' and contains a 'DHCP IP Address Ranges' table. The table has columns for 'Start IP Address' and 'End IP Address', with a single entry for 10.10.10.10 to 10.10.10.200. Below the table is a form to 'Add a DHCP range' with input fields for 'Start IP Address' and 'End IP Address', and 'Add' and 'Reset' buttons. Further down, there are settings for 'Subnet' (10.10.10.1), 'Subnet Mask' (255.255.255.0), 'Enable DHCP Server' (checked), 'Lease Duration (Days)' (7), 'Time Offset, +/- hours (option 2)', 'Primary DNS', 'Secondary DNS', 'NTP Server Address (option 42)', 'WINS Address (option 44)', 'TFTP/FTP Server Name (option 66)', 'Boot File Name (option 67)', 'VLAN ID Discovery (option 129)', 'Option 150', 'Option 159', 'Option 160', and 'Enable Vendor specific configuration (option 43)' (unchecked).

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.

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

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

**edgewater NETWORKS** **Proxy ARP** [Help](#)

Proxy ARP is used to create a bridge between the WAN and the LAN for an IP address or network. Addresses and networks that are bridged bypass the firewall and NAT, allowing complete unprotected access to the systems using the addresses.

When configuring Proxy ARP, the upstream router will need to reassociate the proxied IP address with this system's WAN MAC address. Flush the upstream router's ARP cache after configuring Proxy ARP.

**Configuration Menu**

- Network
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- SIP UA
- 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 Interface
  - Network Information
  - Network Restart
  - Network Test
  - Tools
  - Proxy ARP
  - RADIUS Settings
  - Reboot System

**Configured Proxy ARP Entries**

IP Address	Network Mask (Bits)	Proxy on IF	Gateway	On IF
67.40.40.2	32	WAN	67.40.40.1	VLAN2

**Edit Proxy ARP List**

IP Address:

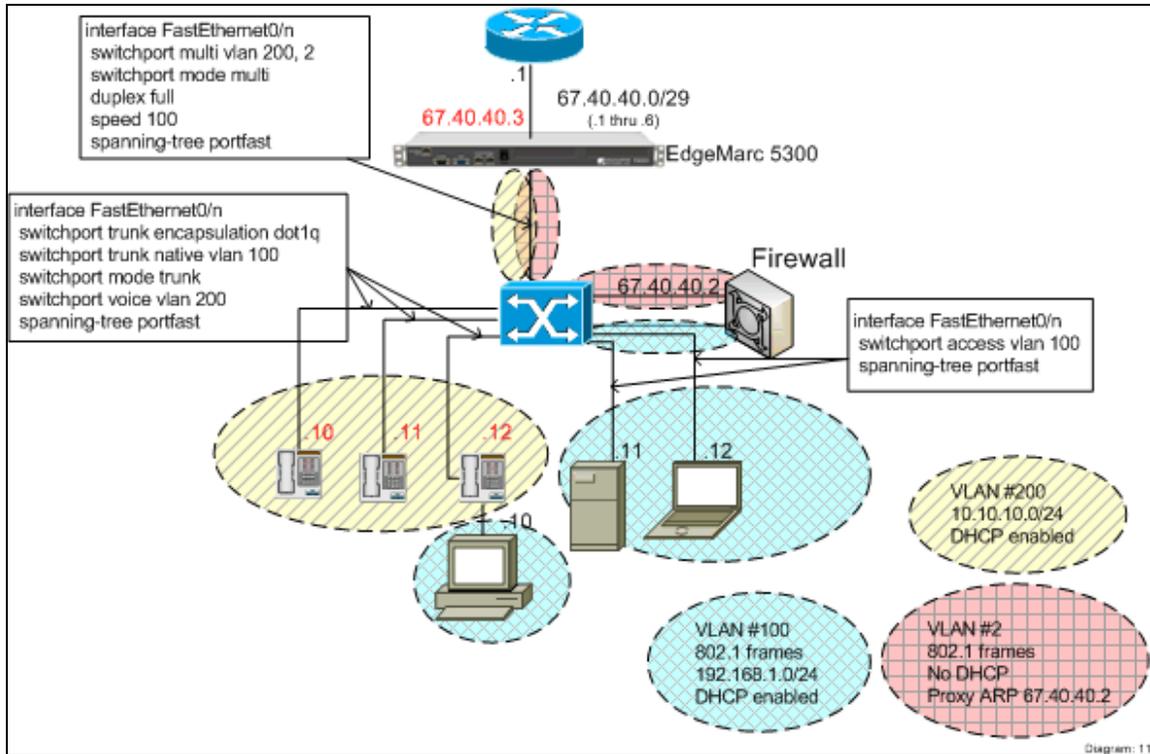
Network Mask (Bits):

Interface responding to ARP:

Gateway:

On Interface:

## 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
  - o WAN IP address 67.40.40.3
  - o 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.

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

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

**edgewater NETWORKS** **Proxy ARP** [Help](#)

Proxy ARP is used to create a bridge between the WAN and the LAN for an IP address or network. Addresses and networks that are bridged bypass the firewall and NAT, allowing complete unprotected access to the systems using the addresses.

When configuring Proxy ARP, the upstream router will need to reassociate the proxied IP address with this system's WAN MAC address. Flush the upstream router's ARP cache after configuring Proxy ARP.

### Configured Proxy ARP Entries

	IP Address	Network Mask (Bits)	Proxy on IF	Gateway	On IF
	67.40.40.2	32	WAN	67.40.40.1	LAN

#### Edit Proxy ARP List

IP Address:

Network Mask (Bits):

Interface responding to ARP:

Gateway:

On Interface:

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

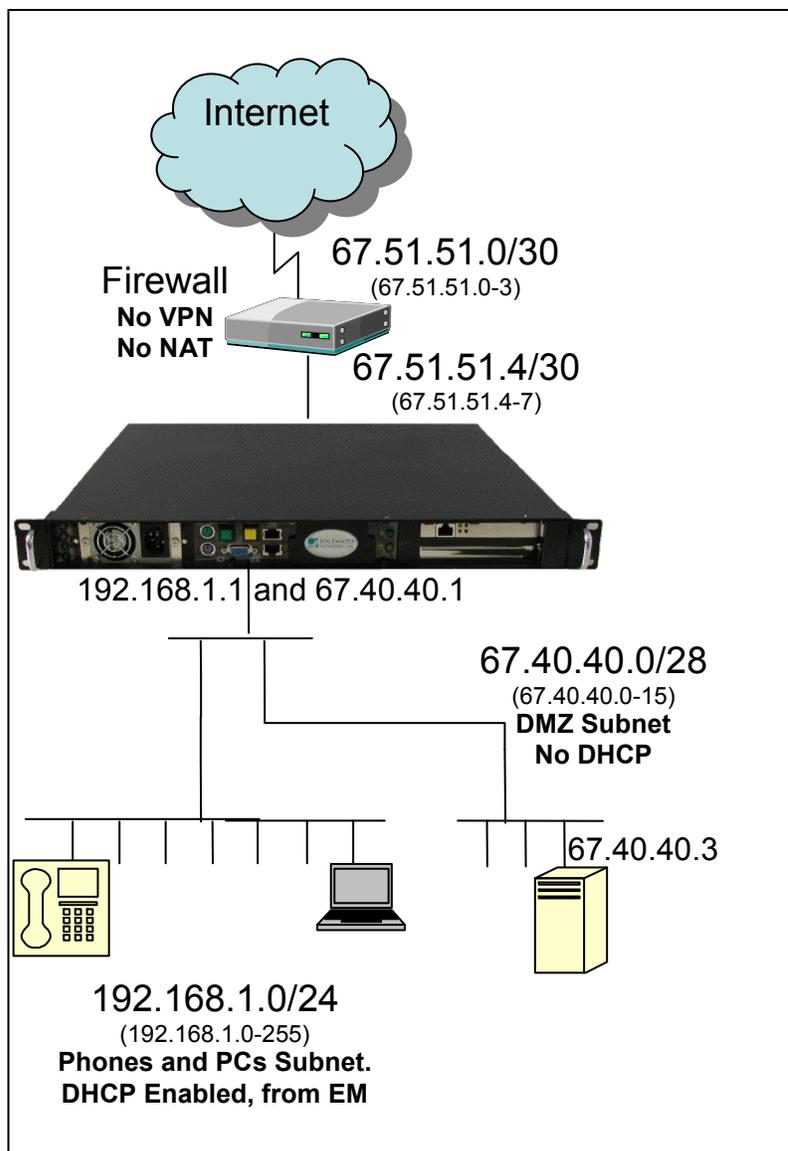
### Characteristics

- 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:

**edgewater NETWORKS** **Pass-Through Rules** [Help](#)

Pass-Through Rules permits the firewall to forward data traffic for a subnet from one interface to another. When forwarding a subnet, an IP address needs to be assigned to the system to serve as the default router for the subnet. To add an additional IP address to the system, visit the [Subinterfaces](#) page.

**Configuration Menu**

- Network
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- SIP UA
- Security
- ▶ Certificate Store
- ▶ HTTPS Configuration
- ▶ MOTD
- ▶ Pass-Through Rules
- ▶ Session Management
- ▶ System Audit
- ▶ Trusted Hosts
- ▶ User Management
- Survivability
- Test UA
- Traffic Shaper
- VoIP ALG
- VoIP Traversal
- VPN
- ▶ WAN Link
- ▶ Redundancy
- System
- ▶ Backup / Restore
- ▶ Clients List

**Add a Pass-Through Rule:**

Protocol: Any   
Input Interface: WAN   
Source IP:   
Source Mask:   
Custom Source Ports:   
Output Interface: LAN   
Destination IP: 67.40.40.0   
Destination Mask: 255.255.255.240   
Custom Destination Ports:   
Target: Accept

**Pass-Through Rules**

Select: All None Action:

	Proto	In Intf	Src IP	Src Mask	Src Ports	Out Intf	Dest IP	Dest Mask	Dest Ports	Target
<input type="checkbox"/>	any	WAN	0.0.0.0	0.0.0.0	any	LAN	67.40.40.0	255.255.255.240	any	ACCEPT

## LAN sub-interface Configuration:

**edgewater NETWORKS** **Subinterfaces** [Help](#)

Subinterfaces allows an administrator to assign additional IP addresses to a system interface. After creating a LAN subinterface, it is often necessary to configure a firewall pass-through rule to permit IP packets through the system. To configure pass-through, visit the [Pass-Through Rules](#) page.

**Configuration Menu**

- Network
  - ▶ Subinterfaces
  - ▶ VLAN Configuration
  - ▶ WAN VLAN Configuration
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- SIP UA
- Security
- Survivability
- Test UA
- Traffic Shaper
- VoIP ALG
- VoIP Traversal
- VPN
- WAN Link
- Redundancy
- System

**Add a Subinterface:**

IP Address: 67.40.40.1  
 Netmask: 255.255.255.240  
 Interface: LAN

Subinterfaces			
Select: All None			<input type="button" value="Delete"/>
	IP Address	Netmask	Interface
<input checked="" type="checkbox"/>	67.40.40.1	255.255.255.240	LAN

### 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	TCP	21
HTTP	TCP	80
RTP	UDP	16386:21785*
SNMP	UDP	161
SSH	TCP	22
Telnet	TCP	23
TFTP	UDP	69
SNTP	TCP	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	TCP	16386:16985
<b>H.323 phones</b>		
Q.931	TCP	1720
RAS	UDP	1719
H.245	TCP	14085:14385
<b>Skinny (SCCP) phones</b>		
Skinny	TCP	2000

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

---

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