

Cybersecurity Project Write-up

The aim of my cybersecurity end of semester project was to create a secure and reliable network which is designed based on the model of a small-to-medium business size. The project includes two physical locations, *Warszawa, Polska* and *Nottingham, UK*. The aim of the project is to demonstrate the types of network devices and configurations required in order to model a secure and reliable network for a small-to-medium business, plus demonstrate my own capabilities to design a network and implement security and reliability features.

My security design plan prior to the creation of the simulation was as follows:

- Dual WAN connections for ISP redundancy
- Dual edge firewalls running a Hot-standby redundancy protocol
- Firewall rules at the edge of the network to restrict what can enter and exit the network
- Site-to-Site VPN connection to allow secure connection between Polska and England sites
- DMZ connected to the firewalls to allow untrusted clients to reach publicly-accessible services, like a webserver or public DNS records
- Interior border gateway dynamic routing running in each site to automate route failure recovery
- Etherchannel connections to collapsed core switches for port failure redundancy
- VLAN segregation for each department to separate broadcast domains and reduce noise
- Core L3 switches running Hot-standby redundancy protocol to provide automatic failure recovery for default gateway devices

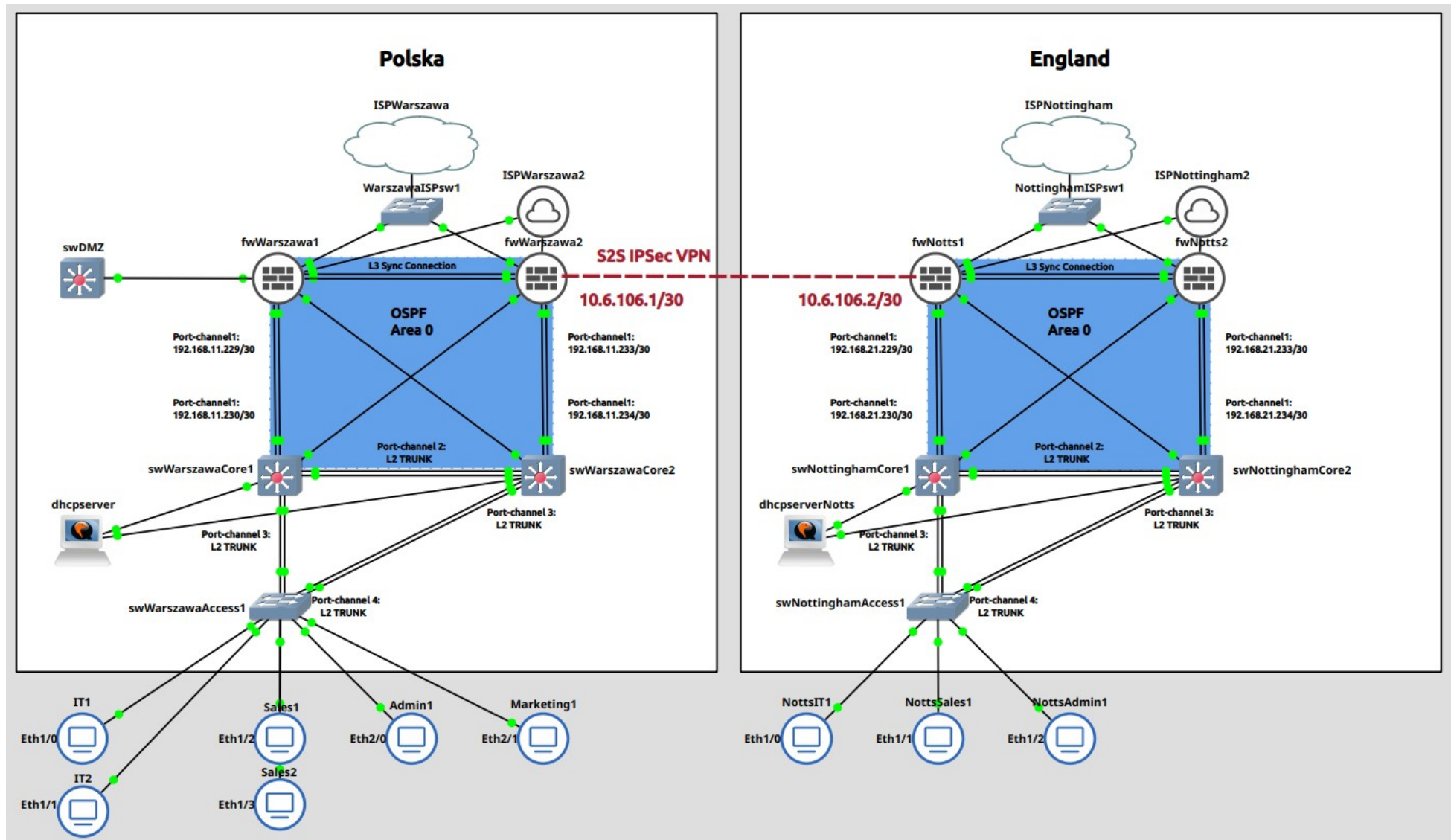
I managed to design the topology of the network, define the network addressing design and also implement the above reliability and security features. Please note that in this case, I consider reliability to also be security as it strengthens the “Availability” aspect of my network, which is one of the three core security fundamentals within the [CIA Security Triad](#).

Configuration files for each device will be bundled with the project for download, along with this documentation.

Table of Contents

Network Diagram.....	3
IP Addressing Scheme.....	4
Warszawa Site.....	4
Nottingham Site.....	6
Network Devices Used.....	9
Security Feature Configurations.....	10
Dual WAN connections for ISP redundancy.....	10
Dual edge firewalls running a Hot-standby redundancy protocol.....	11
Firewall rules at the edge of the network to restrict	11
Site-to-Site VPN connection	12
DMZ connected to the firewalls.....	13
Interior border gateway dynamic routing.....	14
Etherchannel connections to collapsed core switches for port failure redundancy.....	16
VLAN segregation for each department to separate broadcast domains and reduce noise.....	18
Core L3 switches running Hot-standby redundancy protocol.....	18

Network Diagram



IP Addressing Scheme

The below section shows the IP address schemes for the network, including the IP addresses for core network devices. Each site contained subnets to separate traffic for different teams/functions of the organisation. These functions are:

- IT
 - VLAN 10
- SALES
 - VLAN 11
- ADMIN
 - VLAN 12
- MARKETING
 - VLAN 13
- INFRASTRUCTURE
- SERVERS
 - VLAN 20
- DMZ

Warszawa Site

IT - 192.168.10.0/28 - VLAN 10

Net address: 192.168.10.0

First address: 192.168.10.1

Last address: 192.168.10.14

Broadcast address: 192.168.10.15

Core1 int: 192.168.10.2/28

Core2 int: 192.168.10.3/28

VRRP VIP: 192.168.10.1/28

Sales - 192.168.10.16/28 - VLAN 11

Net address: 192.168.10.16

First address: 192.168.10.17

Last address: 192.168.10.30

Broadcast address: 192.168.10.31

Core1 int: 192.168.10.18/28
Core2 int: 192.168.10.19/28
VRRP VIP: 192.168.10.17/28

Admin - 192.168.10.32/28 - VLAN 12

Net address: 192.168.10.32
First address: 192.168.10.33
Last address: 192.168.10.46
Broadcast address: 192.168.10.47

Core1 int: 192.168.10.34/28
Core2 int: 192.168.10.35/28
VRRP VIP: 192.168.10.33/28

Marketing - 192.168.10.48/28 - VLAN 13

Net address: 192.168.10.48
First address: 192.168.10.49
Last address: 192.168.10.62
Broadcast address: 192.168.10.63

Core1 int: 192.168.10.50/28
Core2 int: 192.168.10.51/28
VRRP VIP: 192.168.10.49/28

Infrastructure - 192.168.11.0/24

Net address: 192.168.11.0
First address: 192.168.11.1
Last address: 192.168.11.254
Broadcast address: 192.168.11.255

Core1-P2P-TO-FW1 – 192.168.11.228/30 - VLAN 14

Net address: 192.168.11.228
First address: 192.168.11.229
Last address: 192.168.11.230
Broadcast address: 192.168.11.231

Core1-BACKUP-TO-FW2 - 192.168.11.8/30

Net address: 192.168.11.8
First address: 192.168.11.9
Last address: 192.168.11.10
Broadcast address: 192.168.11.11

Core2-P2P-TO-FW2 – 192.168.11.232/30 - VLAN 14

Net address: 192.168.11.232

First address: 192.168.11.233

Last address: 192.168.11.234

Broadcast address: 192.168.11.235

Core2-BACKUP-TO-FW1 - 192.168.11.12/30

Net address: 192.168.11.12

First address: 192.168.11.13

Last address: 192.168.11.14

Broadcast address: 192.168.11.15

FW CARP SYNC - 192.168.11.16/30

Net address: 192.168.11.16

First address: 192.168.11.17

Last address: 192.168.11.18

Broadcast address: 192.168.11.19

Servers - 192.168.11.208/28 - VLAN 20

Net address: 192.168.11.208

First address: 192.168.11.209

Last address: 192.168.11.222

Broadcast address: 192.168.11.223

DMZ - 192.168.11.240/29

Net address: 192.168.11.240

First address: 192.168.11.241

Last address: 192.168.11.246

Broadcast address: 192.168.11.247

Nottingham Site

IT - 192.168.11.0/28 - VLAN 10

Net address: 192.168.11.0

First address: 192.168.11.1

Last address: 192.168.11.14

Broadcast address: 192.168.11.15

Core1 int: 192.168.11.2/28

Core2 int: 192.168.11.3/28
VRRP VIP: 192.168.11.1/28

Sales - 192.168.11.16/28 - VLAN 11
Net address: 192.168.11.16
First address: 192.168.11.17
Last address: 192.168.11.30
Broadcast address: 192.168.11.31

Core1 int: 192.168.11.18/28
Core2 int: 192.168.11.19/28
VRRP VIP: 192.168.11.17/28

Admin - 192.168.11.32/28 - VLAN 12
Net address: 192.168.11.32
First address: 192.168.11.33
Last address: 192.168.11.46
Broadcast address: 192.168.11.47

Core1 int: 192.168.11.34/28
Core2 int: 192.168.11.35/28
VRRP VIP: 192.168.11.33/28

Marketing - 192.168.11.48/28 - VLAN 13
Net address: 192.168.11.48
First address: 192.168.11.49
Last address: 192.168.11.62
Broadcast address: 192.168.11.63

Core1 int: 192.168.11.50/28
Core2 int: 192.168.11.51/28
VRRP VIP: 192.168.11.49/28

Infrastructure - 192.168.21.0/24
Net address: 192.168.21.0
First address: 192.168.21.1
Last address: 192.168.21.254
Broadcast address: 192.168.21.255

Core1-P2P-TO-FW1 – 192.168.21.228/30 - VLAN 14
Net address: 192.168.21.228
First address: 192.168.21.229

Last address: 192.168.21.230
Broadcast address: 192.168.21.231

Core1-BACKUP-TO-FW2 – 192.168.21.8/30

Net address: 192.168.21.8
First address: 192.168.21.9
Last address: 192.168.21.10
Broadcast address: 192.168.21.11

Core2-P2P-TO-FW2 - 192.168.21.232/30 - VLAN 14

Net address: 192.168.21.232
First address: 192.168.21.233
Last address: 192.168.21.234
Broadcast address: 192.168.21.235

Core2-BACKUP-TO-FW2 - 192.168.21.12/30

Net address: 192.168.21.12
First address: 192.168.21.13
Last address: 192.168.21.14
Broadcast address: 192.168.21.15

FW CARP SYNC - 192.168.21.16/30

Net address: 192.168.21.16
First address: 192.168.21.17
Last address: 192.168.21.18
Broadcast address: 192.168.21.19

Servers – 192.168.21.208/28 - VLAN 20

Net address: 192.168.21.208
First address: 192.168.21.209
Last address: 192.168.21.222
Broadcast address: 192.168.21.223

DMZ - 192.168.21.240/29

Net address: 192.168.21.240
First address: 192.168.21.241
Last address: 192.168.21.246
Broadcast address: 192.168.21.247

Network Devices Used

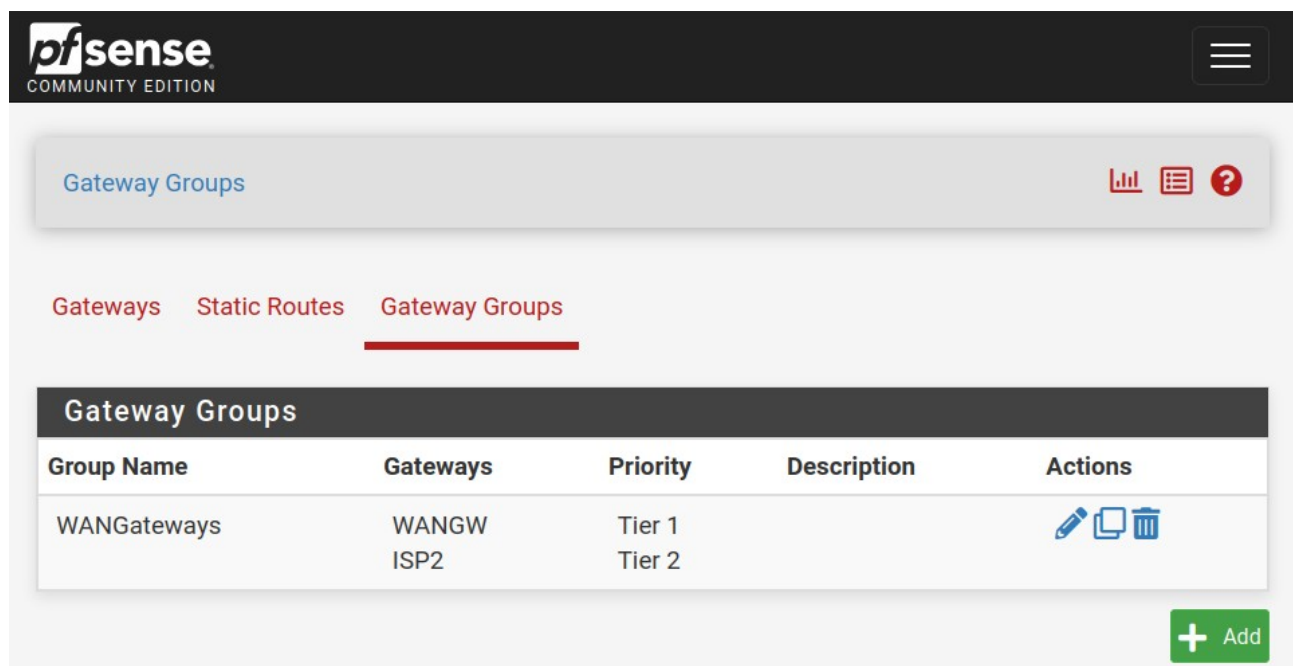
- **Firewalls**
 - PFSense Community edition
- **Core Switches**
 - L3 Cisco switch firmware
- **Access Switches**
 - L2 Cisco switch firmware
- **DHCP Servers**
 - Linux debian 6.1.0-28-amd64
- **Clients**
 - Linux tinycore 6.4

Security Feature Configurations




Dual WAN connections for ISP redundancy

The edge firewalls at each site are configured to utilise two different ISP connections – ISP1 is always used as the primary connection but if the connection to ISP1 is lost, ISP2 kicks in as the backup ISP. This ensures that upstream ISP failures do not cause downtime for the network.

These configurations are made on the **System > Routing > Gateway Groups** page, where the two ISPs can be set as a primary (tier 1) and secondary (tier 2) default gateway. Sample config below from **fwWarszawa1**:



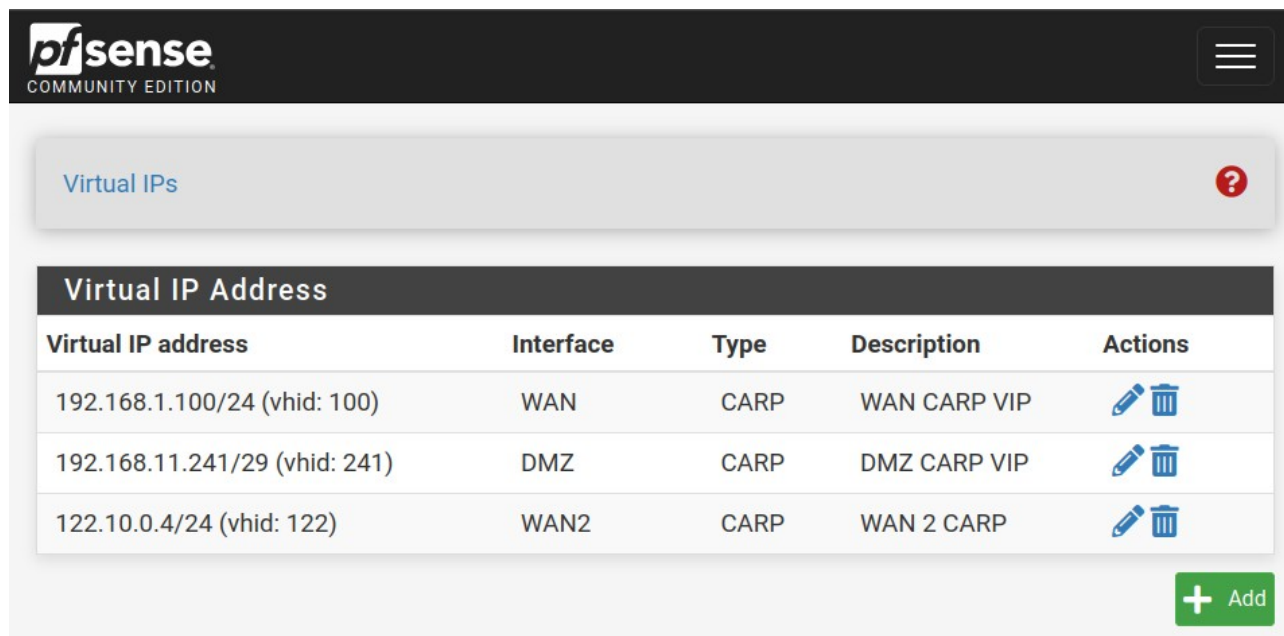
The screenshot shows the pfSense web interface. At the top is the 'pfSense COMMUNITY EDITION' header. Below it is a 'Gateway Groups' section with a title bar containing a bar chart icon, a list icon, and a help icon. Underneath are three tabs: 'Gateways', 'Static Routes', and 'Gateway Groups', with the last one being active and underlined. The main content area displays a table titled 'Gateway Groups'.

Group Name	Gateways	Priority	Description	Actions
WANGateways	WANGW ISP2	Tier 1 Tier 2		  

At the bottom right of the table area is a green button with a plus sign and the text 'Add'.

Dual edge firewalls running a Hot-standby redundancy protocol

The [Common Address Redundancy Protocol](#) (CARP) is used to configure a group of gateways under a single Virtual IP (VIP) address in order to provide automatic failover in the case of some kind of interface or device failure. In this project, CARP VIP's are assigned on the WAN, WAN 2 and DMZ (Warszawa only) interfaces. This configuration is made in the **Firewall > Virtual IPs** page. Sample config below from **fwWarszawa1**:



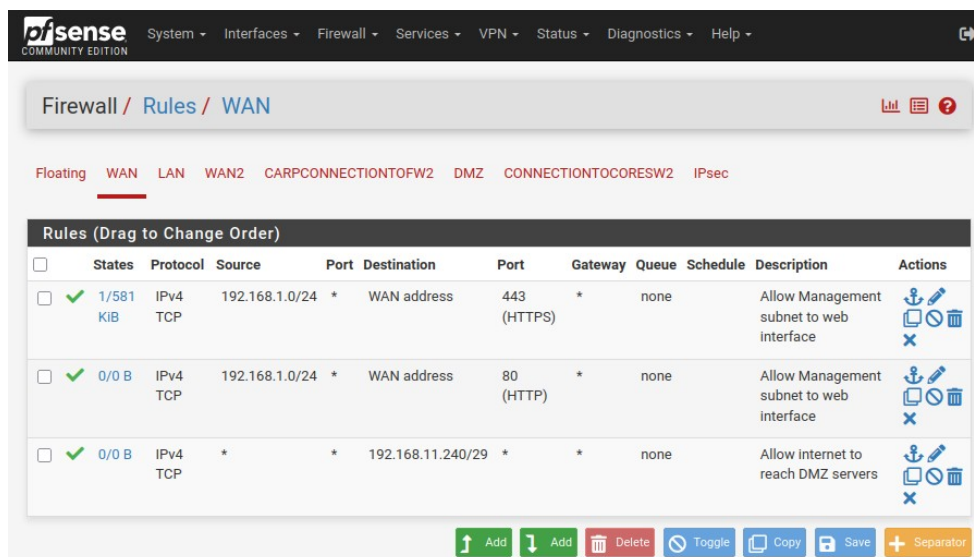
The screenshot shows the pfSense Community Edition interface. At the top, there's a navigation bar with the pfSense logo and a menu icon. Below it, a breadcrumb trail reads "Virtual IPs". A table titled "Virtual IP Address" lists three entries:

Virtual IP address	Interface	Type	Description	Actions
192.168.1.100/24 (vhid: 100)	WAN	CARP	WAN CARP VIP	
192.168.11.241/29 (vhid: 241)	DMZ	CARP	DMZ CARP VIP	
122.10.0.4/24 (vhid: 122)	WAN2	CARP	WAN 2 CARP	

At the bottom right of the table, there is a green "+ Add" button.

Firewall rules at the edge of the network to restrict what can enter and exit the network

Firewall rules are configured on each PfSense network edge firewall to control the flow of ingress and egress traffic on each interface (physical and virtual). These configurations are made from the **Firewall > Rules** page. Sample config below from **fwWarszawa1**:



The screenshot shows the pfSense Community Edition interface. At the top, there's a navigation bar with the pfSense logo and a menu icon. Below it, a breadcrumb trail reads "Firewall / Rules / WAN". A tabbed interface shows "Floating", "WAN", "LAN", "WAN2", "CARP CONNECTION TO FW2", "DMZ", "CONNECTION TO CORE SW2", and "IPsec". The "Rules (Drag to Change Order)" table lists three entries:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	1/581 KIB	IPv4 TCP	192.168.1.0/24	*	WAN address	443 (HTTPS)	*	none	Allow Management subnet to web interface	
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.1.0/24	*	WAN address	80 (HTTP)	*	none	Allow Management subnet to web interface	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.11.240/29	*	*	none	Allow internet to reach DMZ servers	

At the bottom, there is a row of buttons: "Add", "Add", "Delete", "Toggle", "Copy", "Save", and "Separator".





Site-to-Site VPN connection to allow secure connection between Polska and England sites





A site-to-site IPSEC VPN was configured between fwWarszawa1 & fwWarszawa2 → fwNotts1 & fwNotts2. This allowed clients between both geographical locations communicate with each other over a secure tunnel, without exposing sensitive business traffic to untrusted networks (such as the ISP networks and any hops between them.) The IPSEC VPN configuration is configured first, both IKE phase 1 & 2, and then static routes are created to specify which subnets should be routed over the secure tunnel. The configuration can be done from the **VPN > IPsec** page. These configurations are made from the **Firewall > Rules** page. Sample config below from **fwWarszawa1**:


VPN / IPsec / Tunnels


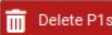
Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

IPsec Tunnels

	ID	IKE	Remote Gateway	Auth/ Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> 	1	V2	192.168.1.100 (WAN CARP VIP) 192.168.1.103	Mutual PSK	AES (256 bits)	SHA256	16 (4096 bit)	SecureConnectionS2S	  

	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/> 	1	vti	10.6.106.1/30	10.6.106.2	ESP	AES256-GCM (128 bits)		SecureConnectionS2S	  



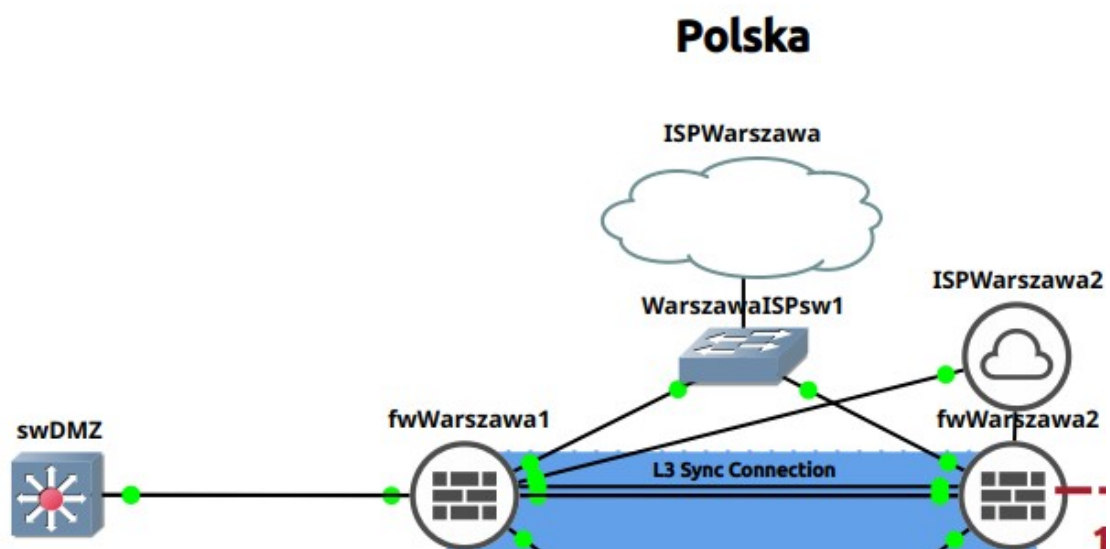
 

(**Note:** I have found the VPN performance within GNS3 to be sub-optimal – very often ping connections between clients hang for 5+ seconds, but connection can be tested and verified to be working.)

DMZ connected to the firewalls to allow untrusted clients to reach publicly-accessible services, like a webserver or public DNS records

A DMZ at the Warszawa site has been created so that publicly accessible services, such as a webserver or public DNS server, can be separated from the internal network. This means that untrusted devices, such as public clients, can access your public services but cannot communicate with your internal, private services. Since this is just a proof of concept I did not create a webserver or public DNS server (just an access switch is implemented currently), however I plan to do this in the future.

The PfSense firewalls control the flow of trusted and untrusted traffic. Some HTTP and HTTPS communications are allowed between the trusted clients and the DMZ for webserver access, but nothing else.



pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / DMZ

Floating WAN LAN WAN2 CARP CONNECTION TO FW2 **DMZ** CONNECTION TO CORE SW2 IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	192.168.11.240/29	*	! ClientVlans	*	none		Allow DMZ out to the internet	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.11.240/29	*	ClientVlans	443 (HTTPS)	none		Allow web traffic from DMZ to Client VLANs	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.11.240/29	*	ClientVlans	80 (HTTP)	none		Allow web traffic from DMZ to Client VLANs	
<input type="checkbox"/>	✓	0/892 B	IPv4 OSPF	DMZ subnets	*	DMZ address	*	none		Allow communication on the P2P link	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Interior border gateway dynamic routing running in each site to automate route failure recovery

The Open Shortest Path First (OSPF) protocol is used within the core network at each site in order to automate the sharing of routing information between the firewall and core switch devices, as well as to automate the failure recovery process when a device or link becomes unavailable.

If the main connection between core switch 1 and firewall 1 becomes unavailable or less desirable, the OSPF protocol will ensure that either core switch 2 or the backup link between core switch 1 and firewall 2 are used. This will all happen automatically without the need for administrator intervention.

On the PfSense firewalls, a package needs to be installed called “FRR”, which enables the OSPF protocol to be configured. OSPF can then be configured from the **Services > FRR Global/Zebra** and **Services > FRR OSPF** pages. A few pieces of configuration are displayed below for reference:

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / FRR / Global Settings ?

Global Settings Access Lists Prefix Lists Route Maps Raw Config [BFD] [BGP] [OSPF] [OSPF6] [RIP] Status

General Options

Enable ☒ Enable FRR

Default Router ID
Specify the default Router ID. RID is the highest logical (loopback) IP address configured on a router.
For more information on router identifiers see [wikipedia](#).
Per-daemon configuration will take precedence over this setting.

Master Password
Password to access the management daemons. Required.

Encrypt Password ☒ Enable password encryption service.










Ignore IPsec Restart ☐ Ignore IPsec restart events. When unchecked, IPsec VTI interfaces will be reset in FRR when IPsec restarts. This reset can prevent routes from becoming inactive in the routing table after interface events.


CARP Status IP
Used to determine the CARP status. When the CARP vhid is in BACKUP status, FRR will not be started.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / FRR / OSPF / Interfaces ?

OSPF Areas Interfaces Neighbors [Global Settings] [BFD] [BGP] [OSPF6] [RIP] Status

Interface	Description	Metric	Area	Authentication	
lan	p2p-to-switch1	10	0.0.0.0	digest	 
opt3	DMZ network		0.0.0.0	digest	 
opt4	p2p-to-switch2	100	0.0.0.0	digest	 
wan			0.0.0.0		 
					 Add

 Save

The below configuration is taken for the Cisco side is taken from **swWarszawaCore1**:

```
router ospf 1
router-id 1.1.1.1
area 0 authentication message-digest
passive-interface default
no passive-interface Ethernet1/3
no passive-interface Vlan14
```

```

interface Vlan14
  description P2P-FW1
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 7 10652D180547055E2B5A687F660B180B
  ip ospf network point-to-point
  ip ospf 1 area 0
  ip ospf cost 10

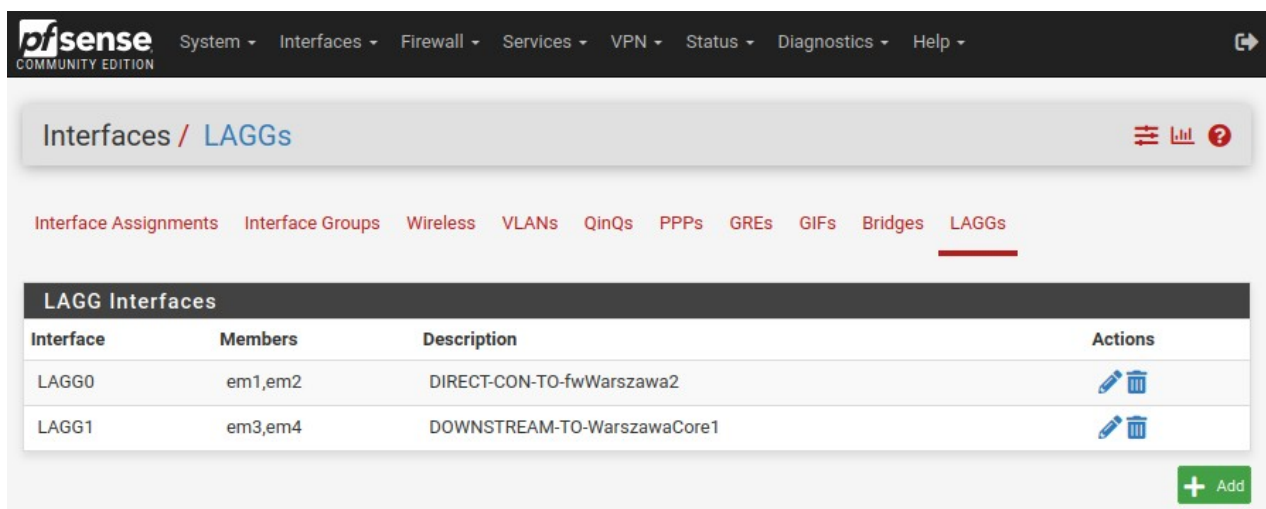
interface Vlan10
  description DEPARTMENT-IT
  ip ospf 1 area 0

```





Etherchannel connections to collapsed core switches for port failure redundancy

The core switches, access switches and primary firewall-to-core connections are all etherchannel connections, comprised of two Ethernet interfaces per bundle. The Link Aggregation Control Protocol (LACP) is used on both the PFSense and Cisco devices to create the logical interfaces between the devices. If a single Ethernet port fails on one of the devices, there is always a secondary interface that can still be used for traffic flow.

On the PFSense firewalls, LACP configuration can be made within the **Interfaces > Assignments > LAGGs** page:



The screenshot shows the PFSense web interface for the LAGGs configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Interfaces / LAGGs" and features a sidebar with various configuration options: Interface Assignments, Interface Groups, Wireless, VLANs, QinQs, PPPs, GREs, GIFs, Bridges, and LAGGs (which is currently selected). Below the sidebar, there is a table titled "LAGG Interfaces" with the following data:

Interface	Members	Description	Actions
LAGG0	em1,em2	DIRECT-CON-TO-fwWarszawa2	 
LAGG1	em3,em4	DOWNSTREAM-TO-WarszawaCore1	 

At the bottom right of the table, there is a green button with a plus sign and the text "Add".

For the Cisco devices, a sample of the LACP configuration has been placed below:

```
interface Port-channel1
  description P2P-FW1
  switchport access vlan 14
  switchport mode access
!
interface Port-channel2
  description ETH2/0,1/2-BONDED-TO-CORE2
  switchport trunk allowed vlan 1,10-14,20
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Port-channel3
  description ETH2,3-BONDED-TO-ACCESS1
  switchport trunk allowed vlan 1,10-13
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

Group	Port-channel	Protocol	Ports	
-----+-----+-----				
1	Po1 (SU)	LACP	Et0/0 (P)	Et0/1 (P)
2	Po2 (SU)	LACP	Et1/2 (P)	Et2/0 (P)
3	Po3 (SU)	LACP	Et0/2 (P)	Et0/3 (P)

VLAN segregation for each department to separate broadcast domains and reduce noise

The different teams/functions/departments within the network design from the “IP Addressing Schemes” (Page4) section have been separated into different VLANs so that their traffic can be more easily controlled. It also separates the L2 traffic between each department, ensuring the traffic from IT (who have more access to network systems for administration) does not leak into the broadcast domains of the Sales, Admin and Marketing department.

The following status of VLAN configuration has been taken from the **swWarszawaAccess1** device:

```
swWarszawaAccess1#sh vlan br
```

VLAN	Name	Status	Ports
1	default	active	Et2/2, Et2/3, Et3/0, Et3/1 Et3/2, Et3/3
10	IT	active	Et1/0, Et1/1
11	SALES	active	Et1/2, Et1/3
12	ADMIN	active	Et2/0
13	MARKETING	active	Et2/1

Core L3 switches running Hot-standby redundancy protocol to provide automatic failure recovery for default gateway devices

The core switches at each site are running the HSRP protocol to provide the same function as the CARP protocol on the Firewalls. It groups the core switch 1 & 2 gateways into a primary and secondary gateway for client devices within the network. It is configured for each VLAN in the network (each department), so that if core switch 1 goes down, the core switch 2 device will take over as the primary gateway for clients. The debian DHCP server is configured to provide the VIP (Group addr) seen below as the default-gateway IP for all clients in the network.

swWarszawaCore1:

```
interface Vlan10
description DEPARTMENT-IT
vrrp 10 ip 192.168.10.1
vrrp 10 priority 110
vrrp 10 authentication text ~'9e(y\
```

```
swWarszawaCore1#sh vrrp brief
```

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Vl10	10	110	3570		Y	Master	192.168.10.2	192.168.10.1

Vl111	11	110	3570	Y	Master	192.168.10.18	192.168.10.17
Vl112	12	110	3570	Y	Master	192.168.10.34	192.168.10.33
Vl113	13	110	3570	Y	Master	192.168.10.50	192.168.10.49
Vl120	20	110	3570	Y	Master	192.168.11.209	192.168.11.211

swWarszawaCore2:

```
interface Vlan10
  description DEPARTMENT-IT
  vrrp 10 ip 192.168.10.1
  vrrp 10 authentication text ~'9e(y\
```

```
swWarszawaCore2#sh vrrp brief
```

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Vl110	10	100	3609		Y	Backup	192.168.10.2	192.168.10.1
Vl111	11	100	3609		Y	Backup	192.168.10.18	192.168.10.17
Vl112	12	100	3609		Y	Backup	192.168.10.34	192.168.10.33
Vl113	13	100	3609		Y	Backup	192.168.10.50	192.168.10.49
Vl120	20	100	3609		Y	Backup	192.168.11.209	192.168.11.211