#### INSTITUTO TECNOLÓGICO DE CANCÚN

MODALIDAD: Individual

MECANISMOS: Banco de proyecto

TEMA: Control y Administración del Servidor Wifi del Instituto Tecnológico de Cancún.

NOMBRE: Catzin Escamilla Viviana Arely

NO. DE CONTROL: 11530310

CARRERA: Ingeniería en Sistema Computacionales

NOMBRE DE LA EMPRESA: Instituto Tecnológico de Cancún

## JUSTIFICACIÓN

La importancia del control y administración del servidor de internet inalámbrico es optimizar el acceso al servicio de internet para los alumnos y docentes del Instituto Tecnológico de Cancún, manteniendo una mejor administración del servidor para evitar el tráfico en la red, aprovechar el rendimiento del ancho de banda y establecer nuevos puntos de acceso para el flujo de la información cuando sea necesario y establecer una mayor seguridad.

## **OBJETIVOS**

**Objetivo General** 

Controlar el rendimiento de la red para los estudiantes, administrativos y docentes del Instituto Tecnológico de Cancún.

Objetivo Especifico

Describir los pasos existentes para llevar un mejor control y administración de la red wifi del Instituto Tecnológico de Cancún y poder aprovechar el rendimiento del ancho de banda de la red

Configurar en dado la ocasión el servicio de DHCP y verificar que funcione correctamente.

Implementación de vlan's para una mejor administración de forma segura y eficiente de la red.

## PROBLEMAS A RESOLVER PRIORIZANDOLO.

El Instituto Tecnológico de Cancún brinda el servicio de internet wifi a todos sus alumnos, docentes y personal administrativo, este servicio es difundido por medio de una red de puntos de acceso, los cuales están en ubicaciones cercanas donde los alumnos y docentes transitan.

El servicio de internet wifi es fácil de obtenerlo y cualquier persona ajena al instituto que entre puede obtenerlo daría mal uso a la red del instituto Tecnológico de Cancún. Por esta manera es que se crea la administración y control del servidor Pfsense para estar al tanto de reiniciar el sistema de red wifi o evitando el tráfico en la red.

De igual forma restringir a los alumnos y algunos docentes o administrativos páginas innecesarias, como lo son las páginas de películas, Facebook, YouTube, entre otros, para que así haya un mejor aprovechamiento de ancho de banda, ya que son cientos de alumno y docentes que hacen el uso de la red.

## PROCEDIMIENTO Y DESCRIPCIÓN DE AVTIVIDADES REALIZADAS

### 1. Recopilación de información actual

Actualmente el Instituto Tecnológico de Cancún utiliza un servidor llamado Pfsense, este nos ayuda a evitar el tráfico de red, aprovechar el ancho de banda de la red, da el servicio de DHCP, el balanceo de los enlaces para la red wifi y también cuenta con la opción de crear vlans y administrarlas para un mejor control, tener una mayor accesibilidad, entre otros.

El Pfsense es una distribución personalizada de FreeBSD (sistema Operativo) para usarlo en servicios de redes LAN y WAN tales como el firewall, enrutador, servidor de balanceo de cargas entre otros. Este servidor nos ofrece algunas funcionalidades:

Firewall: Es un dispositivo de seguridad de la red que monitorea el tráfico de red y decide si permite o bloquea tráfico.

State table: La tabla de estado del firewall mantiene informaciones de las conexiones abiertas.

Network Address Translation (NAT): Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

Portal cautivo: Es un programa o máquina de una red que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal

Servidor DNS: Usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres.

Servidor Proxy: Es un equipo informático que intercepta conexiones de red hechas desde un cliente a un servidor de destino.

Pfsense se puede configurar como un cortafuego permitiendo y denegando tráfico de redes tanto entrante como saliente a partir de una dirección, por ejemplo el

Instituto Tecnológico de Cancún tiene restringido algunas páginas para evitar el acceso a páginas innecesarias o dar mal uso al ancho de banda de la red.

## 2. Diagnóstico de la situación actual

Anteriormente existía un problema del amplio número de equipos que se conectaban a las redes por lo cual no era posible obtener el un buen control de las conexiones provocando la baja calidad del servicio de red. Para eso actualmente es utilizado un servidor proxy para filtrar y monitorear todo el tráfico en la red.

El desarrollo de servidor proxy consto de la instalación del servicio squid y squidguard dentro del servidor PfSense el cual se encarga del servicio de DHCP y Balanceo de carga dentro de la red inalámbrica pública del Instituto Tecnológico de Cancún.

Sen e	Tyston • Interfaces • Freevell •	Services + VPN +	Statue + D	tegnoeffice +	Bold +	1100 ÷.	18
Status / Se	rvices						0
Services							
Service	Description			Status		Actiona	
e-stap	ICAP Intelace for Squid and ClamAV in	dagration		0		C®	
cland	Clanvity Aminirus			0		C®	
should	OHCP Service			0		CONME	
dhamaaq	DNS Forwarder			0		C @ 2011	
døinger	Gateway Monitoring Daemon			0		C (8 = M =	
ntpd	NTP clock sync			0		C @ SIM T	
hispe	Squed Proxy Berver Service			0		CORME	
squidGuard	Proxy server filter Service			0		CO	

Ilustración 1.

Este servidor proxy instalado en el Pfsense ayudo mucho con la administración, porque ya es posible poder llegar a tener un mayor control del tráfico y con esto tiene una mejor administración de los recursos de seguridad en la red.

## 3. Administración y configuración del servidor Pfsense

Se llevara a cabo la administración y control del servidor Pfsense evitando la saturación de la red wifi pública del Instituto Tecnológico de Cancún, se enumera cada una de las actividades realizadas para el completo desarrollo del proyecto:

- 1. Resetear el pool de direcciones
- 2. Configuración del DHCP
- 3. Resetear el Pfsense
- 4. Crear Vlan

A continuación se explicara de manera más completa como se realizaron las actividades mencionadas anteriormente.

### 1. Resetear las direcciones

Iniciamos accediendo al servidor Pfsense

U Unit	× V Login	×		
€ C AN	a es seguro   https://172.168;0.	1		R 🕁 🗢 🧿
		<	<b>ense</b>	
			COMMUNITY EDITION	
		Login to pfSen	se	
		Username	Enter your upername.	
		Password	Enter your password	
			Login	



Colocamos el usuario y contraseña



Ilustración 3

Una vez dentro nos dirigiremos a la pestaña de diagnostics y de ahí a la opción de Edit file

Status / I	Dash	board							+ 0
Goteways					100	Traffic	Grepha		100
(fidearetes		RTT	RTTad	1.044	Blatun	WAN		• va/	(IN) . www.coutt
WANLDHOP 192.168.100.1		74.7010	3.600	0.0%	Outron				1.044
WAN2_0HCP 192.168.1.254		\$1.5mm	7.00%	0.0%	Orihom				1.004
Interfaces					100				h. sons
ALL WAR	-	1000hasarT <full< td=""><td>-diagram -</td><td>102.1</td><td>06.100.2</td><td></td><td></td><td></td><td>MAJ.</td></full<>	-diagram -	102.1	06.100.2				MAJ.
dia LAIN	+	1000breeT +full-	sharles-	172.1	168.0.1	43:07	49:20	#4.10	46:03
12. WANKS		1000kmmeT +full	-thogehise=	192.1	100.1.03	LAN			n 1010 Citer cited
System Info	rmat	ion:			100				Acc-01 (8 8)
Péarrie		O'Clience hick	ddumain						-1100
llystem		priservee Sectal 34419 Netypte Unity	972-460-11#7- # 10-37x59566	béab-#4a84 Stafffaan-Hof	234a673 0				-200#
BIOS		Vender: Dell & Version: 1.2.6 Reference Date	06/08/2015			43:02	49.30	44.10	-400h -5400h 45:01
Versilen		2.3.4 HELEAS built on Well M PrevBBD 10.3	R (1584) Any 00 15(22.11 RELEABE-p19	COT 2017		WANS	2	• 1911	040 0 000 0000 000
Platform		afflareau							1601
СРО Туре		tritul(III) Meterid 6 CPUIs: 1 pare	No CPU ES-260 Augustal + 6 por	0.v9 (j) 1.900 e(a)	Hz				404
									Alam

Ilustración 4

00800		VALUE	L PROVINCI	assuutes.	in the second	COMMANNESS.	AND READ OF	and the	10/3651-1	
COMMUNITY EDI	G System -	sitertaces +	Fireway -	ternices *	VPN +	statue -	Utagnostios +	0003 *	nep +	
Diagno	ostics / Edit	File								0
Advan	ed Users Only									
The capa	silities offered here c	an be dangerous. No s	iupport is availabl	le. Use them at you	r own riskt					
Save / I	oad a File from	n the Filesystem	,							
Puth to fi	a to be added									
Bloan	Browne 🖾 San							Þ	oTo Line #	

Ilustración 5

Una vez aquí colocaremos la dirección /var/dhcpd/var/db/dhcpd.leases~ para poder resetear el pool de las direcciones, damos clic en load y nos cargara las direcciones.



Una vez que nos haya aparecido se borra todas las direcciones, excepto la notas que contengan el siguiente símbolo #

NE :	× 9 😵 ITCSer	se/localdomain - 1 1	1	States and and	3.2	100	-			
C A No	es seguro   Hitter//1	72.168.0.1/dia <u>o_</u> ec	Riphp							
<b>Sen</b>	G System -	Interfaces +	Firmvall •	Services =	VPN =	Status +	Disgnantice +	Gold =	Help =	
Diagn	ostics / Edit F	ile								
Diagit		1973								
Advan	ced Users Only									
The capa	bilities offered here can	be dangerous. No s	upport is availab	le. Use them at yo	ur own risk!					
N. S.										
Save /	Load a File from	the Filesystem	Ě							
/ver/dhc	pd/var/db/dhopd leas	29~								
Riter	Birmane Bitane								oTo Line #	
(E) Low	a provide a provide								010 610 7	
# The T # This	ormat of this file lease file was wri	15 documented tten by Isc-dho	in the dhopd p-4.3.5	lesses(5) mar	iual page.					
			encrenen 16. il manada da							
# sutho	ring-byte-order en	try is generate le-endlag:	ed, DO NOT DE	LETE						
aucnur a	off-skied-prosts yarr	and and and a								

#### Ilustración 7

Después damos clic en save y borramos el ultimo símbolo de la dirección agregada en el campo de texto, así /var/dhcpd/var/db/dhcpd.leases y volvemos dar clic en load.



Una vez cargada se vuelve a borrar todas las direcciones y de nuevo le damos clic en save y listo, queda reseteado la red.



Ilustración 9

Eso nos ayuda para no tener saturada la red del Instituto Tecnológico de Cancún, ya que varios alumnos y docentes hacen uso de la red.

## 2. Configuración del DHCP en el Pfsense

A continuación, esta parte es configuración del DHCP.

DHCP es un protocolo internet usado para asignar lps de forma automatizada de un pool preconfigurado.

Abrimos el Pfsense y vamos al menú service y después a la opción DHCP Server y le damos clic.

Senne System	<ul> <li>Interfaces - Firewall -</li> </ul>	Services • VPN +	Statur +	Disgnostics -	Gold - Heip -	¢.			
Services / DHCP	Server / LAN	Captive Portal DHCP Relay DHCP Server				Co 🖬 🖬 O			
LAN WANZ		DHCPv6 Relay							
		DHCPx6 Server & RA							
Enable	Enable DHCP server on LAN inter	DNS Resolver							
BOOTP	I Ignore BOOTP queries	IGMP Proxy							
Deny unknown clients	Only the clients defined below will	Load Balancer	-ver.						
Ignore denied clients	<ul> <li>Denied clients will be ignored rath</li> <li>This option is not compatible with fail</li> </ul>	NTP PPPoE Server SNMP	when a Failover	Poor Ø addreas is	configured.				
Ignore client identifiers	If a client includes a unique identi This option may be useful when a cli enver behavior violates the official C	Squid Proxy Server Squid Reverse Proxy SmultiGuard Proxy Filter	ND will not be re est client identif	corded in its lease iers but the same !	nardware (MAC) address	a. Note that the resulting			
Subnet	172.168.0.0	UPpP & NAT-PMP							
Subnet mask	255 255 224 0	Wake-on-LAN							
Available range	172.168.0.1 - 172.168.31.254								
Bange	172.168.0.10		175	2.168.31.253					
	Prom		10						
Additional Pools									

Ilustración 10 Configuración del DHCP

Activamos el servicio marcando la opción Enable DHCP server on LAN interface

Escribimos el rango en que queremos sean repartidas las Ips. Estas Ips estarán asignadas dentro de la subred de la interfaz (172.168.0.0 con mascara 23). En este ejemplo activo from: 172.168.0.10 To: 172.168.31.253.

En la sección Servers podemos activar servidores WINS (servicio de resolución de nombres de Microsoft Windows Server), DNS servers.

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	8.8.8.8
	8.8.4.4
	DNS Server 3
	DNS Server 4
	Laws black to use the system datault DNS servers this interfand's ID if DNS Environder or Desolver is enabled, otherwise the servers confirmed on the

Ilustración 11 Activación de servidores WINS

En la sección Other Options podemos cambiar el Gateway, eso es en caso de que no sea la Ip de la interfaz, el Domain name servirá para activar el dominio de tu empresa en los equipos que se vayan conectando.

Other Options	
Gateway	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.
Domain name	The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here
Domain search list	The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default lease time	This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP	Leave blank to disable. Enter the Interface IP address of the other machine. Machines must be using CARP. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is < 20).
Static ARP	Enable Static ARP entries This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this interface.
Time format change	Change DHCP display lease time from UTC to local time By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.
Statistics graphs	Enable RRD statistics graphs Enable this to add DHCP leases statistics to the RRD graphs. Disabled by default.

Ilustración 12

Al igual que las opciones normales del DHCP server, no es obligatorio llenar todos los campos. Damos clic al botón save para terminar la asignación y guardar la configuración.

Default lease time (Seconds)	Used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time (Seconds)	This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Dynamic DNS	Chapting Advanced
NTP servers	Compling Advanced
TFTP servers	Elizabley Advanced
	图 Save

Ilustración 13

Una vez guardando los cambios y ya configurado, el DHCP estará funcionando en nuestro firewall. Este servicio lo podemos monitorear reiniciándolo, parándolo, mirando estadísticas o logs desde los botones de la esquina superior derecha.



#### 3. Reiniciar el Pfsense

El servidor de seguridad Pfsense puede ser reiniciado de forma segura y volver a un buen estado. Para eso, se realizó los siguientes pasos.

Una vez ya dentro del servidor Pfsense nos vamos en diagnostics y después a la opción Reboot. Nos aparecerá de esta forma como en l ilustración.



Ilustración 15

Después le damos clic en el botón rojo donde dice Reboot



Luego nos aparecerá un dialogo donde nos recalca que si estamos seguros de reiniciar el Pfsense y le damos aceptar, eso nos llevara algunos minutos para que se reinicie el Pfsense. Despues que se reinicie automáticamente nos mandara para iniciar de nuevo sesión en el Pfsense



Ilustración 17

El reinicio del Pfsense nos garantiza el funcionamiento correcto del servidor.

### 4. Creación de las vlan's en el Pfsense

Ingresamos al servidor web de nuestro PfSense. Una vez estando dentro nos vamos en la parte de interfaces y en la opción assign le damos clic.

Interfaces 🗸	Firewall 🗕	Services -	VPN			
(assign) LAN OPT1	\$	8	8			
JW.						
2.3.2-RELEASE (amd64) built on Tue Jul 19 12:44:43 CDT 2016 FreeBSD 10.3-RELEASE-p5 The system is on the latest version.						
Sense						
itel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz CPUs: 1 package(s) x 2 core(s)						
Day 04 Hours 40 Minutes 34 Seconds						
Aug 26 8:38:08 C	OT 2016					
	Interfaces   (assign) LAN OPT1 WAN W  C.2-RELEASE (am it on Tue Jul 19 1 eBSD 10.3-RELEA e system is on the Sense el(R) Core(TM)2 I CPUs: 1 package( Day 04 Hours 40 N Aug 26 8:38:08 C	Interfaces - Firewall - (assign) LAN OPT1 WAN W 3.2-RELEASE (amd64) itt on Tue Jul 19 12:44:43 CDT 20 eBSD 10.3-RELEASE-p5 e system is on the latest version. Sense el(R) Core(TM)2 Duo CPU E6750 CPUs: 1 package(s) x 2 core(s) Day 04 Hours 40 Minutes 34 Seco Aug 26 8:38:08 COT 2016	Interfaces  Firewall  Services   (assign) LAN OPT1 WAN WAN W  C  C  C  C  C  C  C  C  C  C  C  C			

Nos aparece un listado de las interfaces de red disponibles en el Pfsense, normalmente tendremos una WAN y una LAN. En este paso cree la vlan.

Interface Assignments Interface Groups Wi	reless VLANs QinQs PPPs GREs GIFs Bridges LAGGs	
Interface	Network port	
WAN	re0 (00:e0:4c:69:11.78) •	)
LAN	em0 (00:1c:c0:18:d0:ba) *	1 Delete
OPT1	re1 (00:e0.4c:69:11.ac) *	Delete
Available network ports:	ovpns1 (Soporte tecnico remoto) .	+ Add
Available network ports:	ovpris1 (Soporte tecnico remoto) •	+ Alt

llustración 19

Damos clic a la pestaña VLANs. Seguidamente agregamos la vlan dando clic al botón Add

Syste	m + Interfaces +	Frewall •	Services +	VPN -	Status +	Diagnostics	i = Gold	• Help •	. 🕪
Interfaces / VL	ANs								≅ lat 0
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs (	PPPs GREs	GIFs	Bridges	LAGGs	
VLAN Interfaces									
Interface	VLAN tag		Priority		Descrip	otion		Actions	
									+ 44

Ilustración 20

En la página que nos aparece escogemos Parent Interface se ingresa la LAN o la tarjeta que decidimos agregar.

En Vlan tag se agrega el número asignado a la vlan. En la opción vlan priority lo dejamos con el número que nos da por default, en la parte de descrption no es necesario agregar algo, en este caso se describió un comentario para que nos ayude a recordar la función de nuestra vlan. Y por último damos clic en save.

erfaces / VLAN	Ns / Edit			≅ lat
AN Configuration		_	_	_
Parent Interface	em0 (00.1c:c0.18:d0:ba) - Ian •			
	Only VLAN capable interfaces will be shown.			
VLAN Tag	2			
	B02.10 VLAN tag (between 1 and 4094).			
VLAN Priority	0			
324330337753	BD2.10 VLAN Priority (between 0 and 7).			
Description	Administración			
	A group description may be entered here for administrative reference (not parsed).			

Ilustración 21

Una vez creada la vlan nos aparecerá de esta

Synt	em • Interfaces •	Firewall + Services +	VPN + Status + D	iagnostics - Gold -	Help +	6
Interfaces / VL	ANs					≡ lat 0
Interface Assignments	Interface Groups	Wireless VLANs	QinQs PAPs GAEs	GIFs Bridges	LAGGs	
VLAN Interfaces						
Interface	VLAN tag	Priority	Description		Actions	
em0 (lan)	2		Administración		18	
						+ 4
0						

Ilustración 22

.

Seguidamente regresamos a la pestaña Interface Assignments. Paso seguido debemos agregar la vlan como una nueva interfaz de red. Damos clic en la caja desplegable de Available network Ports, elegimos nuestra recién vlan y damos clic al botón Add.

Interfaces / Inter	face Assignme	ents									IN O
Interface Assignments	Interface Groups	Wreless	VLANs	QuyQu	ppp <sub>1</sub>	GREN	GIFs	Bridges	LAGG6		
nterface		Network	k port								
WAN		re0 (0	-								
AN		em0 (	00:1c:c0:18:c	(ad 0t						Deine	
PT1		/e1 (0	0.e0.4c.69.1f	ac)						Delete	
vailable network ports:		VLAN	2 on em0 - la	an (Administr	ación)	<u> </u>				+ 44	

llustración 23

Ya tenemos nuestra vlan como una interfaz de red listada en las disponibles en pfSense

Interfaces / Inter	face Assignme	ents									[404]	
Interface has been added.												Cau -
Interface Assignments	Interface Groups	Witeless	VLANs	QinQs	ppps	GREs	OFs	Bridges	LAGGs			
nterface		Network	c port									
NAN		re0 (		)					•			
AN		erri0 (	00:1e:e0:18×	d0 be)						Coleta		
PT1		re1 (0	0.e0.4c.69.1	fine)						Delete		
0912		VLAN	2 on em0 - k	an (Administr	(norae					Delete		
wailable network north		owned	1./Soporte tr	enico remoti	01					F 1970		

Ilustración 24

Una vez ya creada la vlan ya podemos configurar desde el menú de interfaces o dando clic en el nombre de nuestra nueva interfaz.

System -	Interfaces +	Frewall +	Services + VPI	( + Status +	Diagnostics - G	sid + Help	•2	P
Interfaces / Interfac	(assign) LAN OPT1							
Interface has been added.	WAN							
Interface Assignments Inte	rface Groups	Wireless	LANs QinQs	PPPs GREs	OFs Bridger	LAGGs		
Interface		Network por	t					
WAN		reQ (	)			•		
LAN		em0 (00.1	c.cl):18:d0.be)			•	Delete	
OPT1		re1 (00:e0	4c:69:11.ac)				Column	
OPT2		VLAN 2 or	ı em0 - tan (Administ	ración)			Contra	
Available network ports:		ovpna1 (S	aporte teónico remot	0)			+ Add	
Save		ovpris i (s	apone techico remoi	9				

Ilustración 25

Ya estando dentro de la interfaz modificamos el Enable activando la interfaz, en description, se agrega el nombre de la LAN.

En la parte de lpv4 configuration type es para asignarle la lp fija y por último en la opción lpv4 addres se agrega la dirección lp. Le damos clic en save

Enable	Enable interface		
Description	Administración		
	Enter a description (mane) for the interface here.		
Pv4 Configuration Type	Static IPv4	(8)	
Pv6 Configuration Type	None		
MAC Address	ALARA AND A		
	This field can be used to modify ("spool") the MAC addre Enter a MAC address in the following format: scaccoccoc	co of this interface. color or leave blank.	
MTU			
	If this field is blank, the whapter's default MTU will be use	5. This is typically 1500 bytes but	can very in some circumstances.
MSS			
	If a value is entered in this field, then MSS clamping for T	CP connections to the value enter	red above minus 40 (TCP/IF header size) will be in effect
Speed and Duplex	Default (no preference, typically autoanlect)		
	Explicitly set aqueed and dupline mode for this interface, WARNING MUST be set to autoselect (outconstically neg	ctute speed) unless the port this	interface connects to has its speed and duples forced.
itatic IPv4 Configura	tion		
IPv4 Address	192.168.20.1		7 24 *
	Participation	121 66000000	Contract of Contractions of Co

Ilustración 26

### Configuramos el DHCP en una vlan

Ya configurada nuestra vlan el paso siguiente es activar DHCP en esta interfaz de red. Esto nos facilitara la administración. Damos clic en el menú services y después clic en la opción DHCP Server

Senie States	• Interferen • Passeil +	Services + VPN +	Biornal -	Dispression -	State -	theight -	
Services / DHCP	Server / LAN	Captive Portal Dec:P Partay Dec:P Server Dec:Pvh Ralay Dec:Pvh Server & RA					C@ M III 0
General Options		DNS Porwariler					1
Enable	R Enable OTCP server on LAN Inter	DNS Residuer					
BOOTP	Ignico BOOTP querine	KMP Provy					
Deny unknown charts	Only the ulterna defined below will	Load Balaricer	a subst				
Tyrnee denied clients	Deviaed objects will be ignored rate this option is not compatible with to	PPPsE Server	don a Pallove	Heat IP aildress is			
lgnore client identifiers	If a chief induities a unque ident This space may be useful eller a difference in error behavior induites the official (	Signal Provy Server Signal Review Provy Signal Control Provy Piller	RD will not be a still ultrary ideast	ringendied in die bewie Overe louit the warne b	narifmæn (b)Ad	C) without f	hatic theat. How researching
Subret	172.168.0.0	LIPHIP & NATION					
Balmet mask	285 255 334.0	Weller and AM					
Carolana and Concern	TWO LODGEST COMPANY AND AND ADDRESS						

llustración 27

En la página de DHCP Server damos clic a la pestaña de nuestra vlan y modificamos:

Enable activamos el DHCP, eso en dado caso si en algún momento no queremos seguir usándolo, es tan sencillo como desmarcar la opción)

Range From se agrega la ip donde comienza el DHCP a asignar, es muy recomendable dejar un rango para ip's fijas para servidores.

Y por último en Range To se agrega la Ip en la que finaliza el rango a repartir. Damos clic en save.

Sen C. System	<ul> <li>Interfaces •</li> </ul>	Firestall +	Services +	VPN -	fina-	Diagnostics +	Gold +	no-	•
Services / DHCP	Server / ADM	IN							C® ≅ Ш Щ 0
WAN LAN OP	ADMIN								
General Options									1
Enable	∉ Enable DHCP set	ver en ADMIN is	nterface						
Deny unknown clients	Only the clients of	iefned before wi	It get DHCP lease	es from this s	enet.				
Ignore denied clients	<ul> <li>Denied clients with the option is not as</li> </ul>	If be ignored rat republie with h	her than rejected slicver and canno	t be enabled	when a Fallow	r Peer IP address is	trenghnoo		
Submet	192,168.20.0								
Subnet mask	255.255.255.0								
Available range	192.168.20.1 - 192.1	68 20 254							
Range	192 168 20 100				1	82,168,20,200			

Creamos regla de firewall en pfSense para vlan

Ya tenemos creada y configurada la vlan en nuestro Pfsense, además de un rango de lp's asignadas por medio de DHCP. El siguiente paso es crear una regla de firewall que nos permita salida a internet. Damos clic en el menú Firewall y después a la opción de Rules.

Services / DHCF	Server / ADMI	NAT Roles						C@ ≅ ₩ @
The charges have been a walk ( AN ) OF	phied successfully	Schedules Traffic Shaper Vistual IPs						
General Options Evable	et Insite D-CP unv	oprose ADMIN Vete	rtica	-	-	-	-	
Deny unknown clients	© Grity the clients de	filled below will	pri DHCP made	es Toarn d'es ner	V81			
ignore denied clients	Denied clients will This update is not not	Decignored rathe	r Mart rejected	i it is stalled of	ter a fatime	r Pieer IP address: is		
Subort	192.168.20.0							
Subort Subort mask	192.168.20.0 255.255.255.8							
Subort mask Asulable range	192.168.29.0 255.255.255.8 192.168.20.1 - 292.5	0.101254						

Damos clic en la pestaña LAN y agregamos una regla dando clic al botón Add (si creamos más reglas podemos cambiar su orden de ejecución jugando con los botones Add arriba o Add debajo).

oating	WAN LAN	OPTS	ADMIN	OpenVPN						
iles (Dra	ag to Change O	rder)								
States	Protocol	Source	Port	Destination	Part	Gateway	Queue	Schedule	Description	Actions

Ya creando la regla modificamos lo siguiente:

En la parte de Action asignamos Pass, para dejar pasar el tráfico. En la parte de Interface se agrega el nombre de la vlan.

En Protocol seleccionamos any, para permitir todo tipo de tráfico aunque puede ser más específico y por ultimo damos clic al botón Save.

Syst	ien + i	iterfaces +	Firewall +	Services -	VPN +	Status +	Diagnostics +	Gold +	Help +	9
Firewall / Rule	s <mark>/</mark> Edit									≅ ⊯ ≡ 0
Edit Firewall Rule										
Actic	Pas	i.								
	Choos Hint: t where	e what to do w he difference b as with block t	vith packets tha etween block a he packet is dro	t match the crite nd reject is that opped silently. In	ria specified b with reject, a p either case, ti	ielow. packet (TCP R he original pa	ST or ICMP port unre sket in discarded.	achable for U	DP) is returned	to the sender,
Disable	nd 🛛 🖂 Die	able this rule								
	Set th	is option to dis	able this rule w	ithout removing	it from the list	t.				
Interfac	ADN ADN	IIN				•				
	Choos	e the interface	from which pa	ckets must come	e to match thi	s rule.				
Address Fami	by IPv4									
	Select	the Internet Pr	rotocol version	this rule applies	to					
Protoc	ol any									

Ya tenemos nuestra regla de firewall permitiendo la salida a internet en un freebsd PfSense. Damos clic al botón Apply Changes para activarla.

NMUNITY COP	G Sy	stem + In	iterfaces +	Feewall +	Services -	VP	N + Stab	n + Di	agnostics +	Gold +	Help +	Ģ
Firewa	ll / Rul	es / ADM	IN									≅⊯≣0
The firewa The chang	ill rule confi jes must be	guration has the applied for the	een changed. Im to take effic	ei.								🖌 Apply Changes
Floating	WAN	LAN		ADMIN 0	penVPN							
Rules (I	)rag to C	hange Orde	r)									
Rules (D	orag to C States	hange Orde Protocol	r) Source	Port De	stination	Port	Gateway	Queue	Schedule	Descripti	on	Actions
Rules (C	Orag to C States O/O B	hange Orde Protocol IPv4 *	r) Source +	Port De	stination	Port +	Gateway *	Queue none	Schedule	Descripti	on	Actions

Este fue una simple muestra de cómo crear, configurar y colocar protocolos como DHCP para trabajar con vlan's. Esto depende de nuestros requerimientos, porque puede ser más o menos complejo el esquema a realizar.

Por el momento en el Instituto Tecnológico de Cancún se realizó esas creaciones de vlan's para que obtenga un buen manejo en la funcionalidad de la red, mientras trabajan varios grupos de equipos en una sola red.

### RESULTADOS

Parte de los resultados obtenidos durante el desarrollo del proyecto son los siguientes:

- Durante la realización del proyecto se llevaron a cabo la investigación de como poder eliminar el pool de las direcciones del Pfsense, configurar el DHCP y la creación de las vlan's para un mejor rendimiento de la red.
- En la administración y el control del servidor Pfsense dio mejores resultados, ya que evitamos que los alumnos, docentes y administrativos del Instituto Tecnológico de Cancún no obtengan problemas en acceder en la red.
- 3. La red Instituto Tecnológico de Cancún ya tiene una mayor estabilidad en cuanto a la navegación del usuario, ya que la red está limitado a acceder páginas innecesarias y poder aprovechar la liberación del ancho de banda.

## **CONCLUSIONES Y RECOMENDACIONES**

En conclusión el uso del Pfsense es de mayor importancia para el manejo de todas las redes que obtiene el Instituto Tecnológico de Cancún, ya que este servidor nos brinda una mejor administración para que todos los alumnos, docentes y administrativos puedan obtener un mejor servicio de internet.

Actualmente se brinda un mejor servicio ya que se hizo modificaciones para poder extender más direcciones y se configuro para que no tenga sobre saturación.

Se recomienda realizar una bitácora donde se lleve el manejo del flujo de datos que se utilizan diarios para que se pueda evitar sobre cargas en la red y los usuarios tengan un mejor uso del internet sin interrupciones.

Aun con el servidor bien configurado es recomendable que este monitoreado en un lapso de tiempo para poder evitar ataques de virus o de los mismos usuarios de red.

## **COMPETENCIAS DESARROLLADAS Y/O APLICADAS**

Para poder realizar el servidor fue necesario desarrollar y aplicar las siguientes habilidades:

- Conocimiento del servidor PfSense, debido a que antes de realizar alguna configuración, es importante determinar cómo es su funcionalidad y de lo que es capaz de poder realizar en dicho servidor.
- Conocimiento del funcionamiento de las redes TCP/IP, ya que de esta forma se determinó de que rango están configuradas las lp's
- 3. Implementación de protocolos para lograr disminuir los huecos de seguridad en la red inalámbrica.
- Adaptación a cambios ya que se logró agregar una nueva red y ofrecer un mejor servicio de internet a los alumnos, administradores y docentes del Instituto Tecnológico de Cancún

# **REFERENCIAS BIBLIOGRÁFICAS Y VIRTUALES**

https://doc.pfsense.org/index.php/Traffic\_Shaping\_Guide#PFSense\_2.0\_Traffic\_S

haping\_Guide\_.28Work\_In\_progress.29

https://es.slideshare.net/Terrafx9/pfsense-11382123

https://www.bellera.cat/josep/pfsense/index\_cs.html

https://www.ecured.cu/Pfsense

http://www.firewallhardware.es/pfsense.html

https://es.wikipedia.org/wiki/Traducci%C3%B3n\_de\_direcciones\_de\_red

https://www.muycomputerpro.com/2014/01/07/que-es-un-servidor-proxy

http://drivemeca.blogspot.mx/2012/03/como-configurar-dhcp-server-en-

pfsense.html

http://drivemeca.blogspot.mx/2016/09/como-