ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE LA NUEVA ARQUITECTURA DE COMUNICACIONES INTERNA, ORIENTADA A LA SEGURIDAD DE LA INFORMACIÓN, EN BASE A LOS PROBLEMAS DE LA INFRAESTRUCTURA ACTUAL DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

WELLINGTON ROBYS BUCHELLI

GUAYAQUIL – ECUADOR

AÑO 2016

AGRADECIMIENTO

Agradezco en primer lugar a Dios, a mi Madre y a mi Abuela, mis apoyos en toda mi vida, mi motor en la lucha diaria para alcanzar mis metas y superarme día a día.

DEDICATORIA

Las personas luchan por alguna razón, mi razón de lucha es por mi familia, por tener una mejor calidad de vida, a ellos dedico el presente proyecto para conseguir un gran logro.

TRIBUNAL DE SUSTENTACIÓN

Mgs. Lenin Freire C.

PROFESOR DELEGADO POR LA

UNIDAD ACADÉMICA

Ing. Juan Carlos García

PROFESOR DELEGADO POR LA

UNIDAD ACADÉMICA

RESUMEN

El presente trabajo tiene como principal objetivo mejorar los sistemas de comunicaciones a nivel de infraestructura de redes, realizando los diferentes análisis orientados a la seguridad de la información, para que los usuarios tengan un nivel de comunicación optimo y seguro.

La implementación ha sido ejecutada y puesta en marcha con las seguridades informáticas que se explicarán en la presente documentación, entre las mejoras en la red se presentan: creación de nodos de distribución y de accesos en la red, implementación de Vlans, monitoreo y control, implementación de firewall´s, DMZ, IDS/IPS, aplicación de reglas de navegación, monitoreo de la red, implementación de Suricata, análisis y mitigación de problemas.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La realización del proyecto surge de las necesidades de mantener un servicio estable y confiable de los diferentes sistemas de comunicaciones a nivel de la infraestructura de red que actualmente tiene la Institución de Educación Superior, debido a la gran demanda de los diferentes usuarios como personal administrativo, docentes, estudiantes y usuarios externos.

La necesidad de contar con las diferentes herramientas de los sistemas de información, internet, y demás servicios que encierran las necesidades actuales; dio como resultado exigir a la institución a realizar la inversión para mejorar la infraestructura de comunicaciones, en base a los diferentes lineamientos orientando a la seguridad de la información y comunicaciones estables.

CAPÍTULO 1

GENERALIDADES

1.1. DESCRIPCIÓN DE PROBLEMA

La Institución de Educación Superior actualmente tiene una arquitectura de red plana con pocas seguridades lógicas internas y externas, corriendo el riesgo de ataques informáticos desde diferentes partes. Los usuarios actuales de la red, desconocen de los posibles ataques informáticos que se puedan presentar en una infraestructura de red.

La necesidad de acceder a los diferentes medios de investigación, exige a las Universidades conexiones informáticas de un alto grado de rendimiento, para que los diferentes usuarios no tengan problemas al momento de realizar sus labores diarias, toda institución de un alto grado

de aprendizaje exige a su personal docente y estudiantes a realizar investigaciones, accediendo a varios sitios de información como bibliotecas virtuales, centros de información, blogs, etc, haciendo del internet la herramienta diaria de trabajo como principal medio de acceso; es necesario implementar una infraestructura de comunicación estable, que llegue a los usuarios con niveles de conectividad excelentes, evitando problemas de pérdidas de conexión y demás.

La Institución de Educación Superior, tiene la necesidad de cambiar su infraestructura de comunicación a nivel de switch y seguridades lógicas en la red, que pueda soportar los diferentes servicios informáticos que actualmente brinda a la comunidad universitaria; la red de comunicación es en los actuales momentos en su parte lógica una red plana, controlada por equipos que no brindan las seguridades informáticas necesarias que actualmente exige una red de datos segura.

1.2. PROPUESTA DE SOLUCIÓN

Para la solución de la problemática planteada de la Institución de Educación Superior, se propone la implementación de una nueva arquitectura de red, con equipos de comunicaciones que soporten la creación de Vlan´s para la segmentación de la red, aplicando las diferentes políticas de seguridad para cada grupo de usuarios que serán definidos según las necesidades de la institución.

También Se implementará firewalll´s perimetrales para cada segmento de acceso, incluyendo un firewall de borde, para el control de la red LAN, DMZ y WAN. A continuación se detallan los diferentes puntos de beneficio de la implementación:

Arquitectura de red:

- Creación de nodos de distribución en la red
- Distribución de nodos de accesos
- Segmentación IP.
- Configuración de VTP server - Vlan´s
- Monitoreo y control de la red

Nivel Core:

- Implementación de firewall de borde Pfsense
- Control de la red DMZ
- Control de la red de acceso
- Limitar puertos abiertos hacia la DMZ y la red de acceso
- Implementación de IDS/IPS Suricata
- Implementación de Multiwan para servicios de internet

Nivel de acceso:

- Implementación de firewall de accesos Pfsense, por vlan, control de puertos.

- Aplicación de reglas de control de navegación Squid – SquidGuard
- Detección de problemas de seguridad con Suricata
- Monitoreo de la red inalámbrica.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. IMPLEMENTACIÓN DE LA NUEVA ARQUITECTURA DE RED

Para explicar la respectiva implementación de la nueva arquitectura de comunicaciones, es necesario realizar una pequeña introducción a la arquitectura anterior, para diferenciar las mejoras realizadas dentro del Campus Universitario.

Cabe indicar que la arquitectura de red plana, estuvo operativa desde 1995 hasta a mediados del 2014, donde se adquirieron los respectivos equipos que se detallarán más adelante en el presente documento.

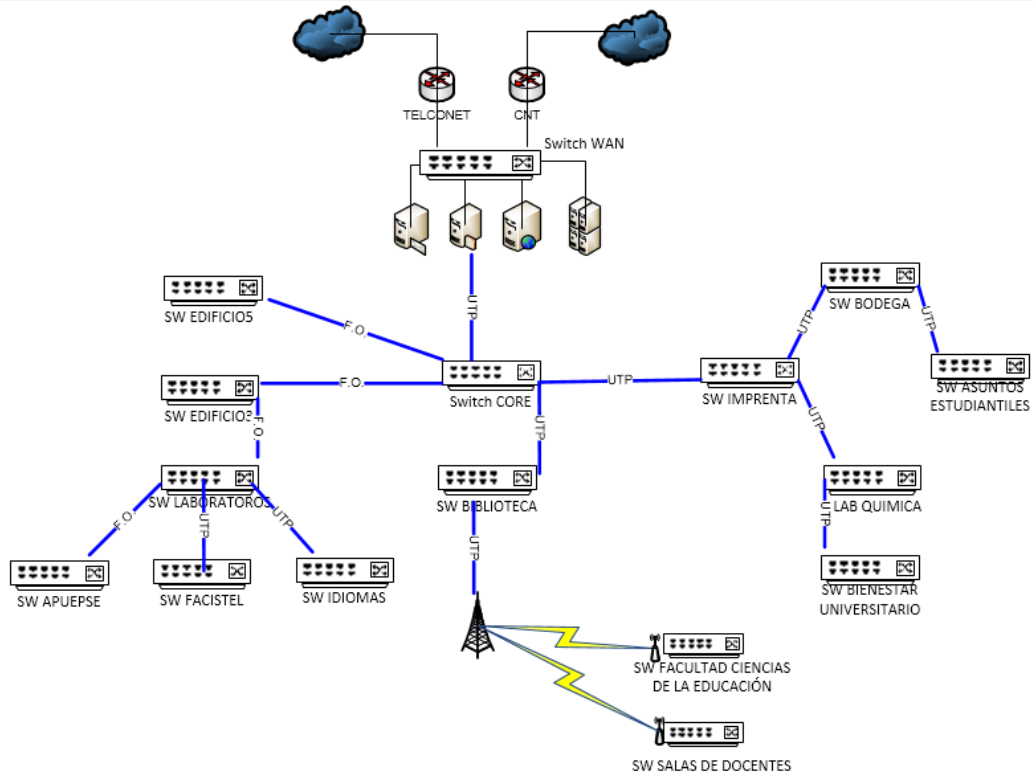


Figura 2.1 Esquema de arquitectura de red plana

Se muestra en la Figura 2.1. que se mantiene un nivel de seguridad mínimo para el control de red en la parte WAN y LAN, colocando un switch para manejar las interfaces WAN de los diferentes servidores, los cuales en sus interfaces LAN eran interconectados a otro switch CORE, donde se encontraban con todos los segmentos de red de los diferentes edificios; encontrando el gran problema de la red a nivel de seguridad informática, por lo que no se podían aplicar restricciones de accesos a los diferentes servicios informáticos y controlar mejor la red a nivel de Vlans.

En base a los problemas encontrados se procedió con el respectivo análisis para la implementación de la nueva arquitectura de red, creando nodos de distribución y de accesos para las diferentes áreas del Campus Universitario.

La creación de los nodos de distribución se consideró debido a las diferentes cargas de usuarios, respaldo de energía en cada sitio, y el acceso para el control de los equipos.

Los nodos de accesos serían los diferentes edificios y sus distribuciones internas, que solo atiendan máximo a un edificio contiguo, para mitigar los posibles problemas de derivación de comunicaciones por diferentes causas, y detectar los problemas rápidamente.

Los equipos adquiridos por la Institución fueron los Switch de marca CISCO, con los diferentes modelos de acuerdo a las necesidades reales de cada nodo de distribución y de acceso, contemplando el crecimiento a futuro del Campus Universitario, el cual ha sido coordinado con el departamento de Obras Civiles.

A continuación se detallan en la Figura 2.2 los equipos adquiridos y la ubicación de cada uno en los diferentes edificios del Campus Universitario.

EDIFICIOS	EQUIPOS
CENTRO DE COMPUTO	Cat4500 E-Series
EDIFICIO ADMINISTRATIVO 3	Cisco Catalyst 2960-X Switch 48 GigE
LABORATORIO1-2-3	
INCYT	
BIBLIOTECA	Cisco Catalyst 3650 Switch
EDIFICIO DE AULAS 10	Cisco Catalyst 2960C Switch 12 FE PoE
IMPRENTA	
POSTGRADO	
EDIFICIO DE AULAS 2	Cisco Catalyst 2960C Switch 8 FE
COLEGIO	
BIOLOGIA MARINA	
CENTRO COMPUTO	
EDIFICIO DE AULAS 7	
LAB QUIMICA	
EDIFICIO DE AULAS 1	
ASESORIA JURIDICA	
BIBLIOTECA 2	Cisco Catalyst 2960-X Switch 24 GigE 2
APUPSE	
ENFERMERIA	
BIENESTAR UNIVERSITARIO	
LABORATORIO1-2-3	
FAC SISTEMAS	
LABORATORIO7-8-9	
EDIFICIO ADMINISTRATIVO 1	
IDIOMAS	
EDIFICIO ADMINISTRATIVO 4	
CENTRO COMPUTO	
BODEGA	
EDIFICIO ADMINISTRATIVO 5	
CIVIL	
CENTRO COMPUTO	
MIPRO	

Figura 2.2 Equipos Switch Campus Universitario

En el Centro de Cómputo fue colocado el CISCO Catalyst 4500, el cual maneja toda la distribución y comunicación de la red LAN hacia los servidores que mantienen los diferentes servicios informáticos de la Institución de Educación Superior, implementando las diferentes Vlans que serán detallas en el capítulo correspondiente.

Los nodos de distribución son identificados por los detalles que se mencionó anteriormente (carga de usuarios, respaldos de energía, etc.), se detallan los edificios que realizaran la función de nodos de distribución:

- Centro de Cómputo.
- Edificio Administrativo 3.
- Laboratorio1-2-3.
- APUEPSE (Asociación de Profesores).
- Biblioteca Central.
- Imprenta.
- MIPRO

Los nodos de acceso, son los que mantienen la intercomunicación de las diferentes oficinas, cada nodo de acceso podría tener hasta un edificio dependiente de él; para evitar los posibles problemas que puedan presentarse si fallara algún equipo y que el corte de los servicios no se extienda a un alto porcentaje de usuarios.

A continuación se detallan los nodos de accesos, identificado por los edificios administrativos y edificios de aulas, cabe indicar que en los edificios de aulas se mantendrá la comunicación con los equipos inalámbricos, donde cada equipo inalámbrico soportara una carga de 40 usuarios cada uno.

- Edificio Administrativo 1.
- Edificio Administrativo 2.
- Edificio Administrativo 4.
- Edificio Administrativo 5.
- Edificio de Aulas 1.
- Edificio de Aulas 2.
- Facultad de Sistemas.
- Edificio de Idiomas
- Edificio de Aulas 7.
- Edificio de Aulas 10.
- Civil.
- Biología.
- Asesoría Jurídica.
- INCYT.
- Enfermería.
- Colegio.
- Laboratorio7-8-9.
- Postgrado.
- Laboratorio Química.
- Bienestar Universitario.
- Bodega.

Cada nodo de acceso alimentará a las diferentes oficinas dependiendo de las Vlans y los segmentos de red que se les asignen, eliminando los cuellos de botella que existían en la red plana.

En la Figura 2.3 se presenta la actual implementación de los equipos de comunicaciones en la arquitectura de red del Campus Universitario, la identificación de los nodos de distribución y de acceso se la realiza con los diferentes nombres de cada edificio, cabe indicar que se utilizó los mismos medios de comunicación ya implementados como la fibra óptica y el cableado utp de cada edificio.

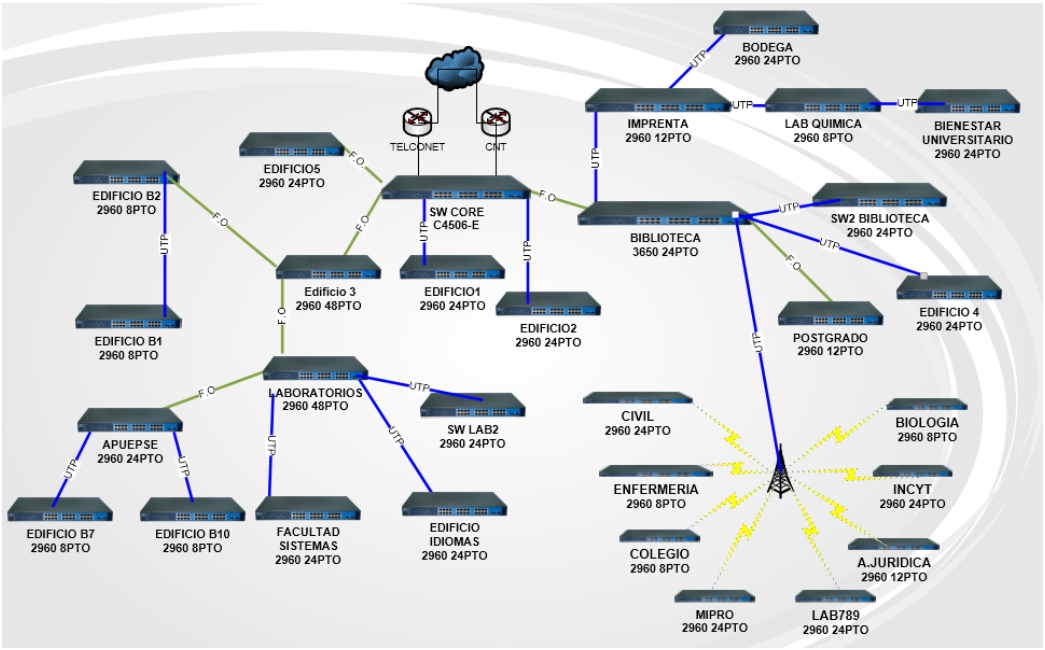


Figura 2.3 Implementación de la nueva arquitectura.

La distribución de los equipos se la ha realizado según las mediciones de cantidad de usuarios, consumo de servicios, y consumo de ancho de banda necesario por cada edificio, contemplando el respectivo crecimiento. Los equipos implementados han cumplido su función, el monitoreo respectivo de los equipos se mencionará más adelante, en donde se verificaran las diferentes cargas que tienen.

2.2. IMPLEMENTACIÓN DE SEGURIDADES LÓGICAS.

Después de realizar los respectivos laboratorios de prueba con los equipos de red, se procedió a la creación de las Vlans, según las necesidades reales de la Institución de Educación Superior; el control de las Vlans se la realiza desde el equipo Switch Cisco 4500, la distribución de las Vlans se las clasificó por los accesos de los diferentes usuarios.

Las Vlan son controladas desde el Cisco 4500, en modo VTP Transparent, debido a que no en todos los equipos es necesario el paso de las mismas Vlans, existe la necesidad de migraciones futuras de subredes, por lo cual se mantiene esta configuración. A continuación se detallan las respectivas Vlans operativas:

Vlans a nivel Core:

- Vlan Servidores DMZ.
- Vlan Proveedores.
- Vlan de Firewall por segmentos de red

Vlan Servidores DMZ.- mantendrá a todos los equipos servidores que distribuyen los diferentes servicios informáticos como por ejemplo: Quipux, Sitios Web, Base de Datos, DNS, Aplicaciones, Dspace, entre otros.

Vlan Proveedores.- contiene las conexiones hacia internet, por la salida de los proveedores Telconet y CNT, a cada servicio se le asignó una Vlan diferente para la creación posterior de una Multiwan.

Vlan de Firewall por segmentos de red.- vlan creada para mantener a los equipos que funcionan como firewall de cada segmento de red, realizando las funciones de proxys, firewall y control de IDS/IPS según las necesidades de la red.

Vlans a nivel de acceso:

- Vlan Oficinas Administrativas.
- Vlan Edificio Rectorado.
- Vlan Docentes.
- Vlan Servicio Wireless.
- Vlan Laboratorios.

Vlan Oficinas Administrativas.- la subred contendrá a las diferentes oficinas administrativas, tanto oficinas de Facultades y oficinas de las

Áreas Administrativas de la Institución, las cuales tendrían los mismos accesos a los servicios informáticos.

Vlan Edificio Rectorado.- la creación de la Vlan del edificio de Rectorado fue necesaria, debido a que en el edificio funcionan las dependencias principales de la Institución y siempre deberán tener acceso a los servicios importantes como el Internet y consultas a las Bases de Datos.

Vlan Docentes.- el personal docente de la Institución tiene designadas diferentes áreas de trabajo dentro del Campus Universitario, las cuales deben ser atendidas a diario con los diferentes servicios informáticos, por lo que se generó la creación de la respectiva subred, así mismo deben ser controlados en la utilización de los recursos informáticos asignados a cada Sala de Docentes.

Vlan Servicio Wireless.- mantendrá la conexión a través de los diferentes equipos wireless intercomunicando la navegación de los usuarios de la red inalámbrica como estudiantes, docentes, usuarios en general.

Las Vlans ayudarán a controlar el flujo de información de los segmentos de red, los cuales tendrán acceso a los diferentes servicios informáticos, controlados por sus respectivos firewalls de acceso a la DMZ; cabe indicar que también se realizó la creación de las respectivas subredes de

cada Vlan y los ruteos necesarios considerando los niveles de accesos de los usuarios.

Se mantienen las seguridades de accesos en cada Switch, a continuación se detallan las configuraciones:

- Diferente subred y Vlan de accesos para los switch.
- Seguridad en claves para accesos de las consolas.
- Bloqueo de ataques de login.
- Configuración de Vlan en puertos necesarios.

La distribución de las Vlans en la arquitectura de la red, se las coloca según las necesidades de los accesos por parte de los usuarios, como se muestra en la Figura 2.4, donde se detallan las diferentes Vlans en cada edificio.

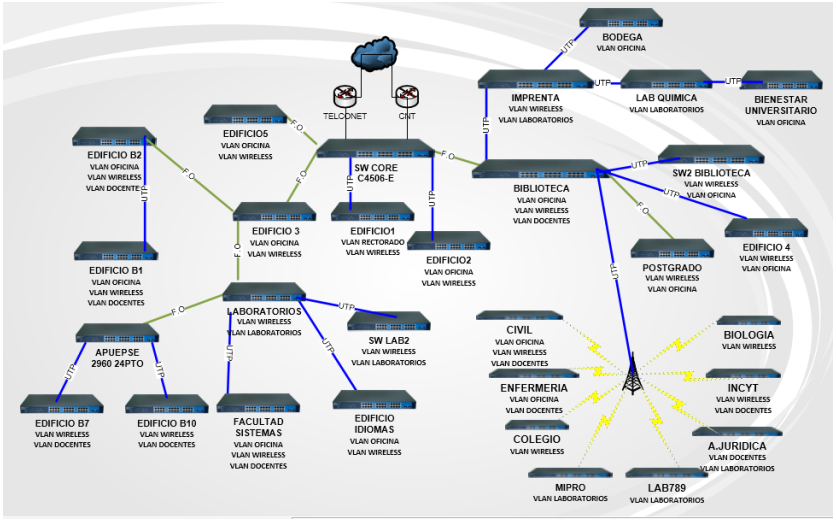


Figura 2.4 Implementación de Vlans.

2.3. IMPLEMENTACIÓN DE FIREWALL A NIVEL PERIMETRAL Y DE ACCESO.

Actualmente en el mercado existen varias soluciones de firewall, tanto comerciales y Open Source, los cuales se podrían aplicar según los recursos económicos que mantiene cada Institución. Debido a la limitante del recurso económico se buscó un firewall Open Source, realizando las respectivas investigaciones se procedió a aplicar Pfsense, el cual es una variante del proyecto MonoWall.

Pfsense es un proyecto Open Source, creado en el año 2004 por Chris Buechler y Scott Ullrich [1], distribución basada en FreeBSD, el objetivo de Pfsense es tener un firewall y router seguro, fácil de configurar y entendible donde se desee aplicar seguridades en la red; además permite añadir varios paquetes para el control de la red, según las necesidades del administrador.

La versión instalada para la implementación de Pfsense [2] es la 2.2.4 de 64 bits, la cual es la versión estable y será utilizada como firewall perimetral y firewall de accesos de las diferentes vlans en la red.

A continuación se detallan las funcionalidades de Pfsense:

- Instalación mediante LiveCd.
- Configuración vía consola o interface web.
- Firewall, filtrado por dirección origen/destino.

- Firewall, filtrado por protocolos.
- Stateful firewall.
- Logs de firewall y diferentes servicios.
- Ruteo.
- Alias IP, agrupamiento de direcciones.
- Normalización de paquetes.
- Nat, reenvío de puertos.
- Portal Cautivo.
- Redundancia con CARP, Pfsync.
- Balanceo de carga.
- Reportes, monitoreo, dashboard, reportes de consumo, etc.
- Implementación de VPN, con diferentes protocolos IPSec, PPTP, VPN sobre SS
- Backup de configuraciones.

La instalación de toda la infraestructura a nivel de firewall, esta implementada en VmWare con las respectivas máquinas virtuales, en un servidor HP Blade C3000, con alta disponibilidad para establecer una infraestructura operativa al cien por ciento, con las protecciones eléctricas seguras. El Blade C3000 cuenta con dos cuchillas a nivel de servidores, cada una con dos procesadores Xeon y 36 Gb de Ram; y dos sistema de almacenamiento externo de 20 Tb cada uno.

La instalación de la plataforma de Pfsense se la realiza mediante la ejecución del LiveCd, escogiendo la opción correspondiente para instalar el sistema operativo en el disco duro del equipo Figura 2.5.

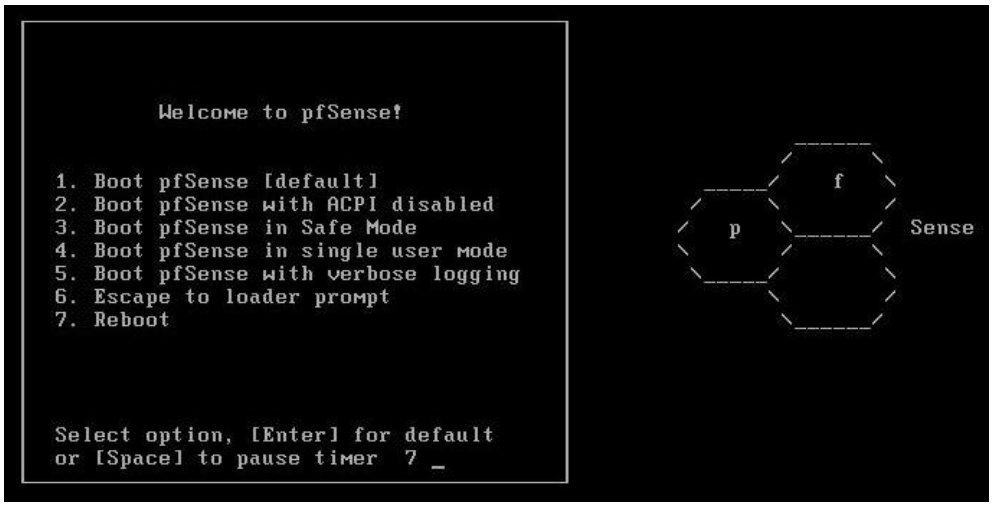


Figura 2.5. Inicio de la instalación de Pfsense

Si se permite correr la configuración desde el cd, solicitará las configuraciones necesarias de las interfaces de red, como es el caso de la Figura 2.6

Figura 2.6. Asignación de interfaces WAN, LAN.

Es necesario realizar el seguimiento de la configuración, debido a que en los mensajes sale la opción para realizar la instalación directa en el disco duro del equipo, como se muestra en la Figura 2.7; después de escoger la opción de instalación seguirá con el respectivo formateo del disco asignado, lo pasos se muestran en las figuras a continuación.

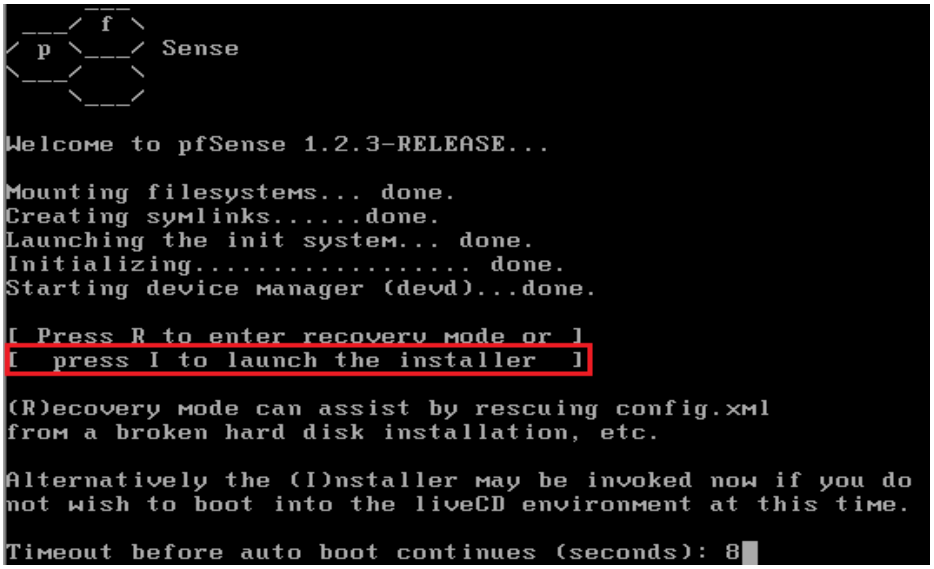


Figura 2.7. Opción de instalación en el disco duro del equipo.

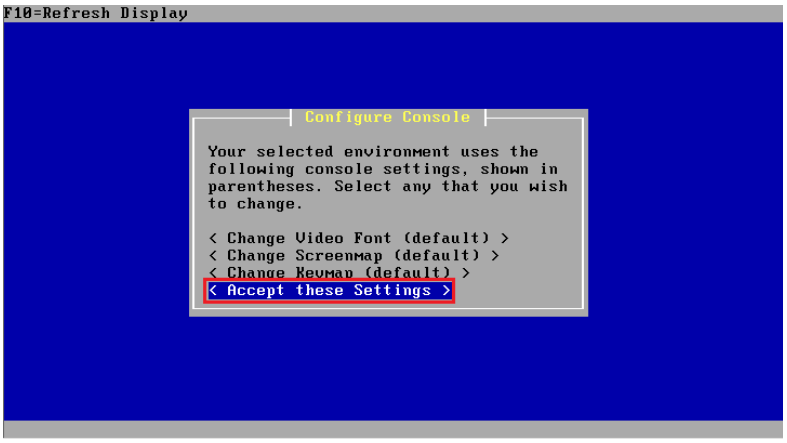


Figura 2.8. Inicio de instalación, configuración de video.

Figura 2.9. Instalación de Pfsense

Figura 2.10. Opción de formateo del disco local

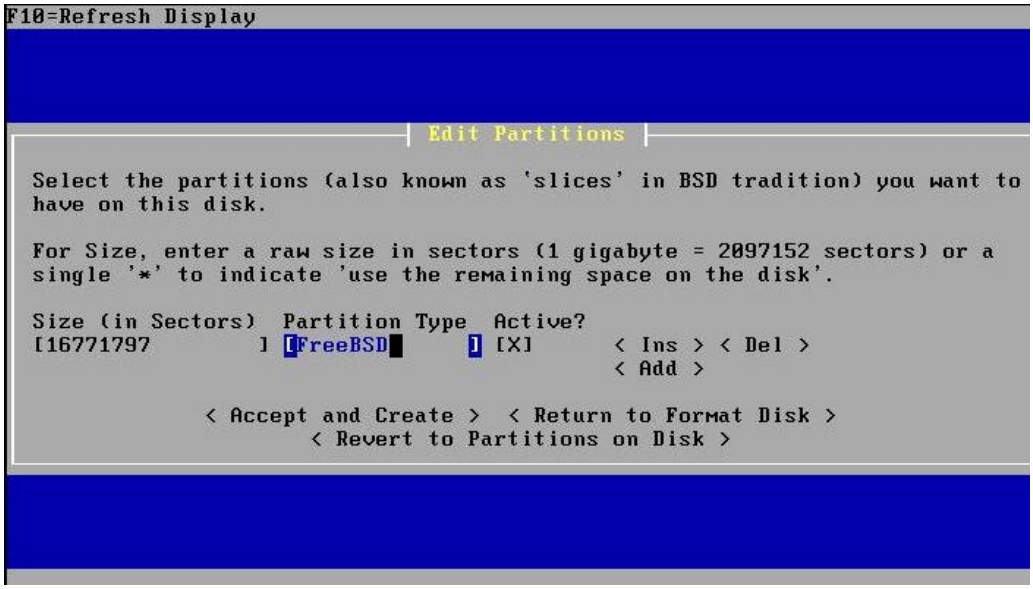


Figura 2.11. Selección del disco duro.

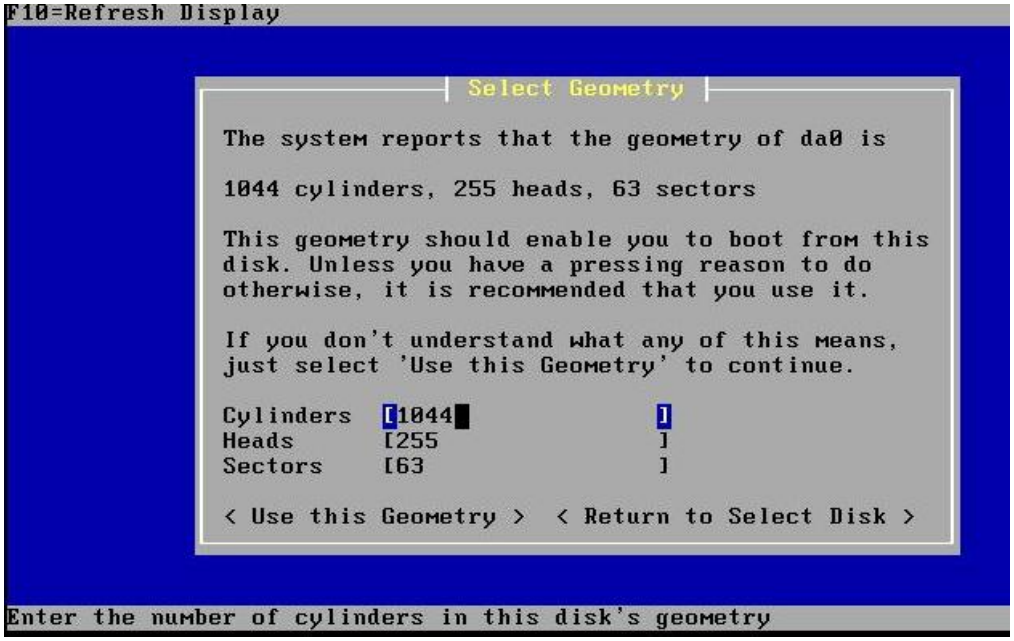


Figura 2.12. Instalación de la geometría del disco duro

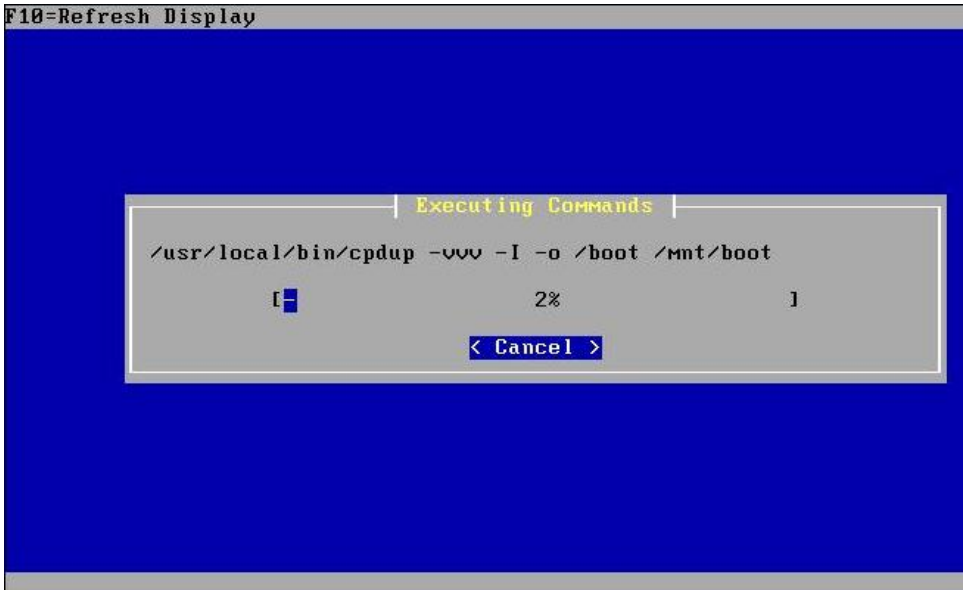


Figura 2.13. Instalación del sistema operativo de Pfsense.

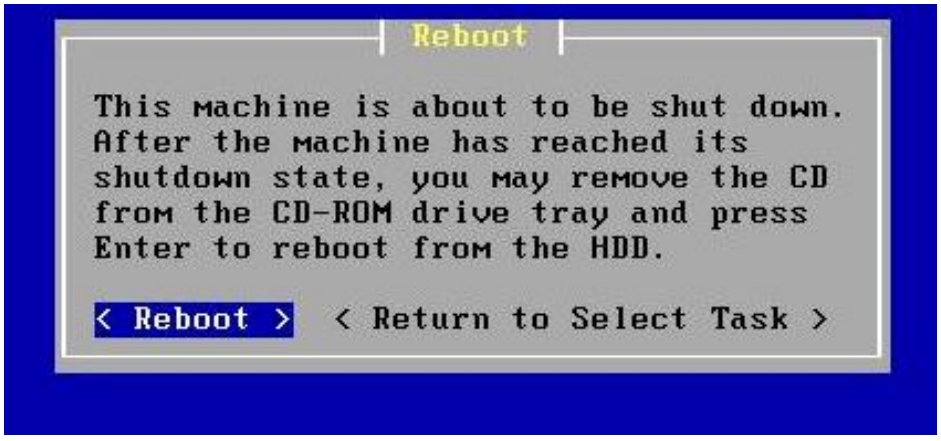


Figura 2.14. Finalización de la instalación de Pfsense.

Después de reiniciar el equipo, se presenta la pantalla de configuración de las interfaces instaladas, se procede con la respectiva configuración de las interfaces de red WAN, LAN y las demás, según las necesidades de la red, Figura 2.15 y 2.16; luego de eso es necesario iniciar la sesión

desde un equipo conectado a la red con el mismo direccionamiento IP para el acceso a la interface web de la configuración de la plataforma del PFsense, Figura 2.17.

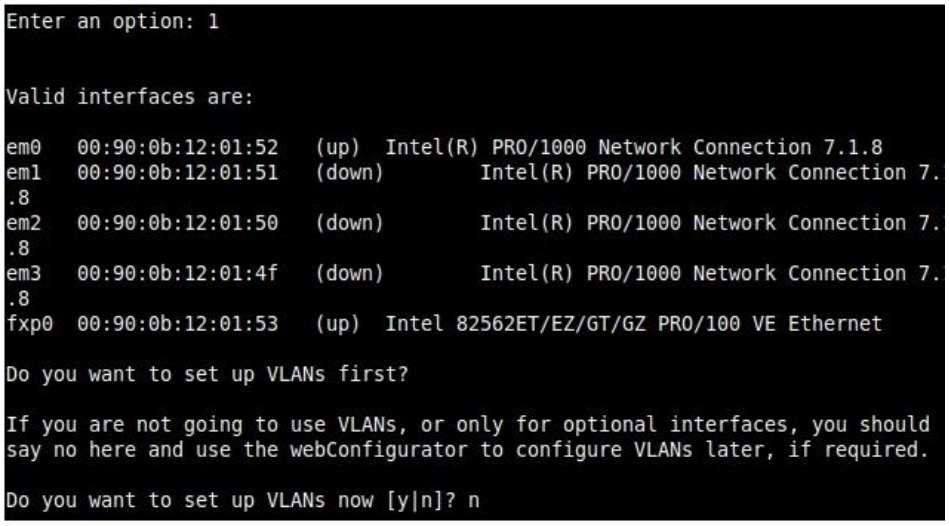


Figura 2.15. Asignación de las interfaces de red.

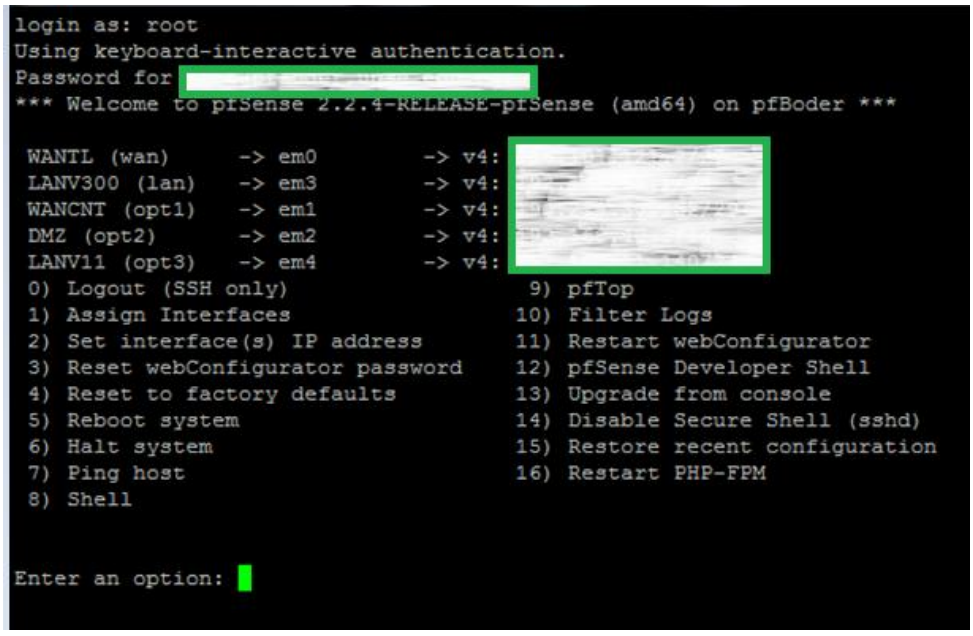


Figura 2.16. Configuración de las interfaces completadas.

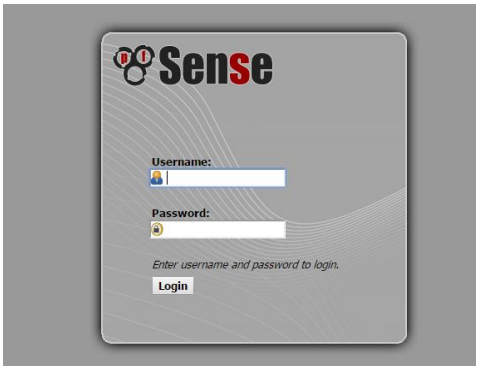


Figura 2.17. Inicio de sesión vía web del Pfsense

Realizado todo el proceso de instalación y configuración como se lo detalla en las figuras anteriores, la configuración de los servicios dependerá de las necesidades del administrador de la red.

Firewall de Borde.- realizará las funciones de control de las interfaces WAN, DMZ, LAN, Firewall, NAT, Multiwan, Routing; servicios habilitados de SSH, monitoreo de Gateways, servicio NTP (sincronización de tiempo). El Firewall de Borde se encargara de las siguientes funciones:

- Prevenir de ataques desde la WAN.
- Routing para servicios web desde la DMZ hacia la WAN.
- IP Alias, para manejo de grupos de IP y asignación de reglas en el firewall.
- Virtual IP, manejo de direcciones IP públicas para las interfaces WAN.
- Restricción de puertos desde la red WAN hacia la DMZ.
- Control de tráfico desde la LAN de Firewall de accesos hacia la DMZ y WAN.

- Manejo de Multiwan.
- IDS/IPS implementado con Suricat.

En la Figura 2.18, se presenta el dashboard del Firewall de Borde, con las configuraciones de las interfaces de red WAN de CNT y Telconet, LAN de firewall de accesos, red DMZ, y LAN de Vlan de control. Se puede observar la información en tiempo real de:

- Nombre del equipo.
- Versión del sistema operativo.
- Tipo de CPU utilizado, en este caso 2 Core.
- Tiempo de actividad.
- Fecha del día.
- DNS colocados en el equipo.
- Día de la última configuración realizada.
- Tamaño de la tabla de estado.
- Límite de conexiones y porcentaje de uso.
- CPU utilizado.
- Memoria RAM utilizada.
- Disco y swap utilizado.
- Monitoreo de los gateways para el control de la Multiwan.
- Interfaces activas.
- Servicios corriendo actualmente.
- Gráficos de consumo de las diferentes interfaces de red.

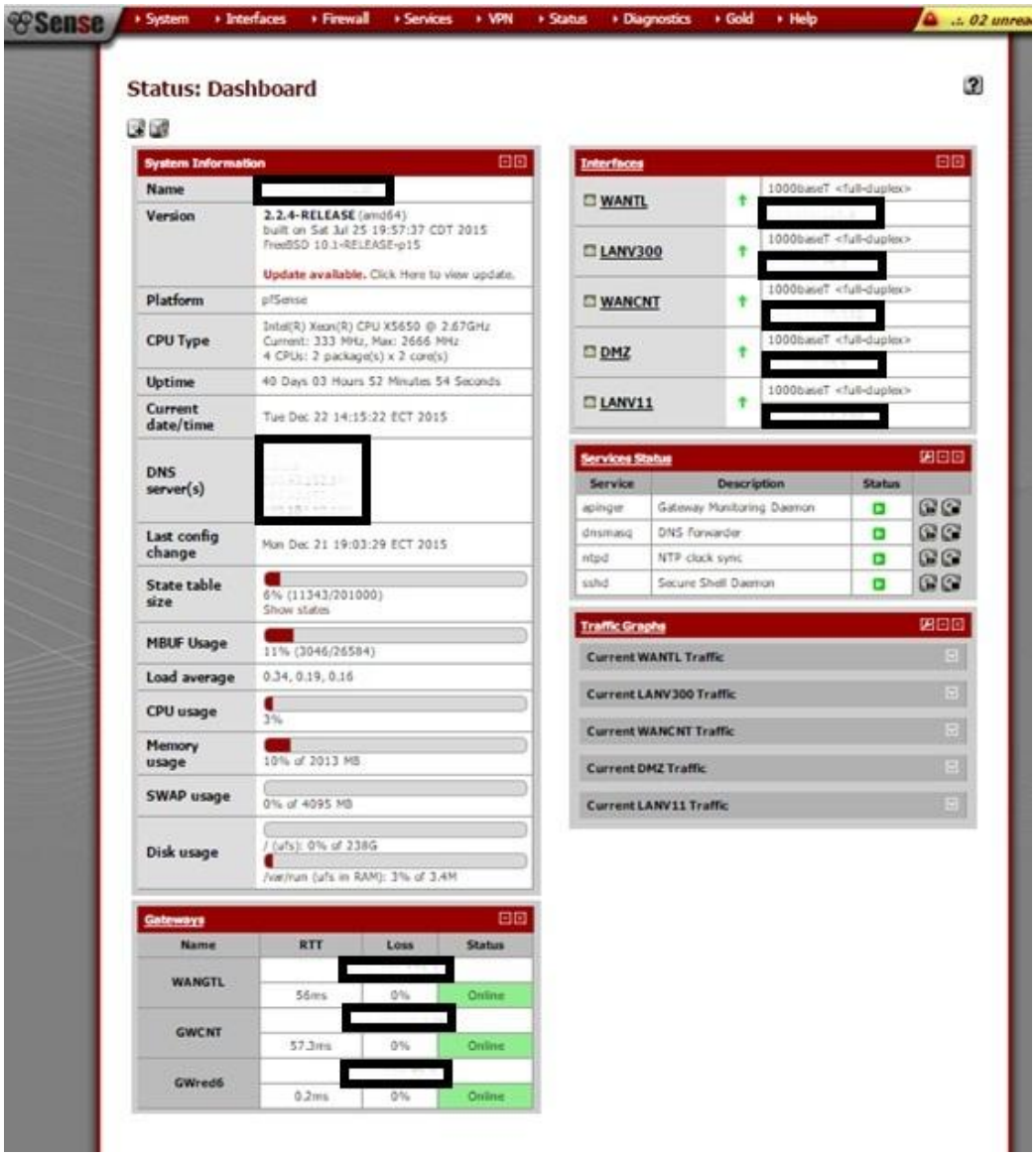


Figura 2.18. Dashboard que presenta el Firewall de Borde.

El dashboard de Pfsense, permite añadir diferentes widgets para el respectivo monitoreo del equipo, lo cual ayuda a resolver problemas de configuraciones según las funcionalidades del equipo. La Figura 2.19 muestra los diferentes widgets que se pueden presentar en el dashboard.

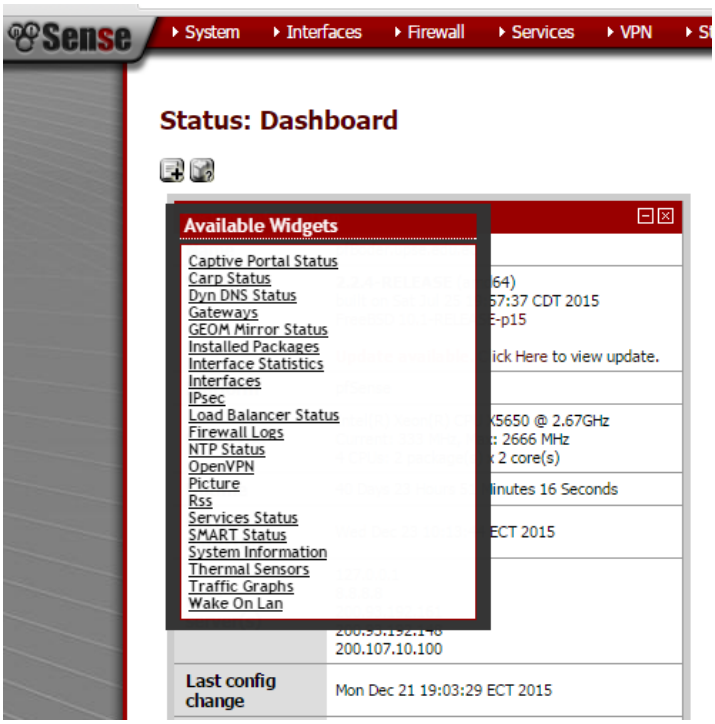


Figura 2.19. Widgets que se añaden al dashboard de pfsense

El manejo y configuración de las prestaciones de los diferentes menú, se los puede encontrar realizando las respectivas investigaciones en internet, por ahora solo se explicará las configuraciones realizadas en el Firewall de Borde, que ha sido implementada en la plataforma de Pfsense.

El Firewall de Borde tiene las dos interfaces WAN de los proveedores de internet Telconet y CNT, por lo que es necesario añadir los respectivos DNS con sus correspondientes gateways de salida, los cuales serían monitoreados por el Monitor IP del Pfsense, la IP asignada para el

monitoreo en cada gateway serán DNS externos para la verificación real del servicio de internet. En la figura 2.20 y 2.21 se presentan los DNS.

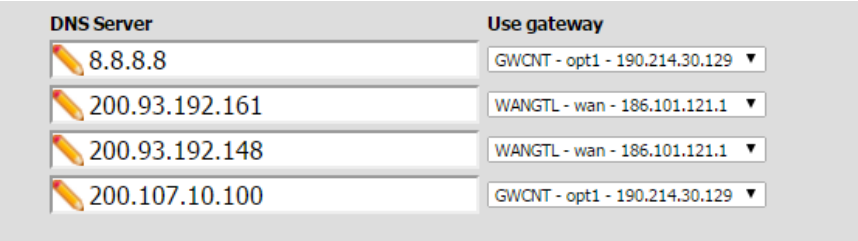


Figura 2.20. DNS de proveedores con sus respectivos gateways.

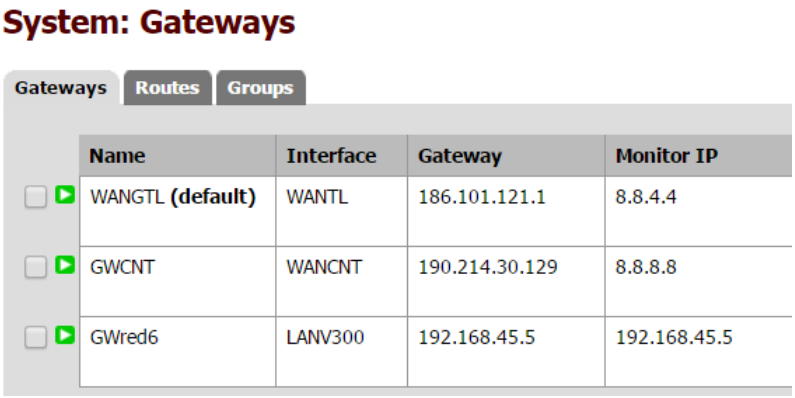


Figura 2.21. Gateways de proveedores con sus respectivos monitoreos.

En la sección de Routing, se maneja la parte de Grupos de Gateways, aquí se implementa la redundancia y balanceo de carga de los proveedores de internet, en el caso de la implementación se aplica solo redundancia, debido a que en la configuración se le asigna diferente Tier de prioridad a cada proveedor, esto haría que si un proveedor falla el otro entraría a funcionar, la alerta de la falla la daría el Monitor IP de cada Gateway.

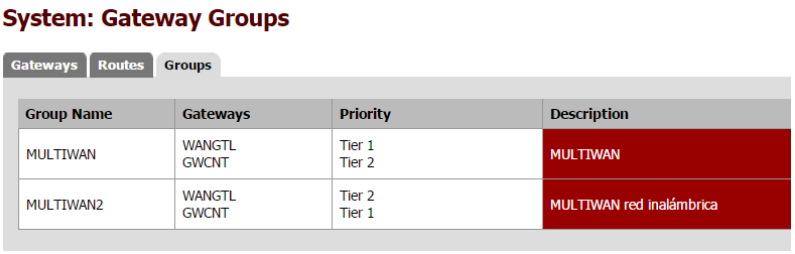


Figura 2.22. Creación de Multiwan de los proveedores de internet.

En la Figura 2.22 se presenta las respectivas configuraciones de las Multiwan para los servicios de las redes de oficinas con prioridad de salida por la red de Telconet y como alterna la salida con CNT. La red inalámbrica por la cantidad de usuarios en línea tiene un consumo de 60 Mbps, por lo que es asignada como prioridad la red de CNT y alterna al proveedor de Telconet.

Realizando las pruebas de conexión con las diferentes interfaces WAN, el tiempo de respuesta del cambio de proveedor es de 5 a 10 segundos, tiempo en que demora en dar la alerta el Monitor IP de la caída de la dirección IP colocada en el monitoreo de los gateways.

Para la explicación de las reglas del Firewall de Borde es necesario mostrar la arquitectura de la implementación de seguridad a nivel de firewall que se ha creado, en la Figura 2.23 se muestra la arquitectura funcional, donde se puede visualizar la red DMZ de servidores, los cuales manejan un direccionamiento de IP privada y los diferentes servicios son nateados a direcciones públicas por el firewall hacia el internet,

restringiendo los puertos necesarios para las salidas de los servicios informáticos.

La red de acceso de los Firewall de cada Vlan se puede visualizar, a este nivel los equipos Pfsense realizan también funciones de Proxy, control de navegación, control de accesos por puertos, IDS/IPS para detectar posibles ataques internos, el IDS/IPS es implementado con Suricata; dependiendo de los análisis y anomalías que se presenten el Suricata es ejecutado para encontrar el problema en la red.

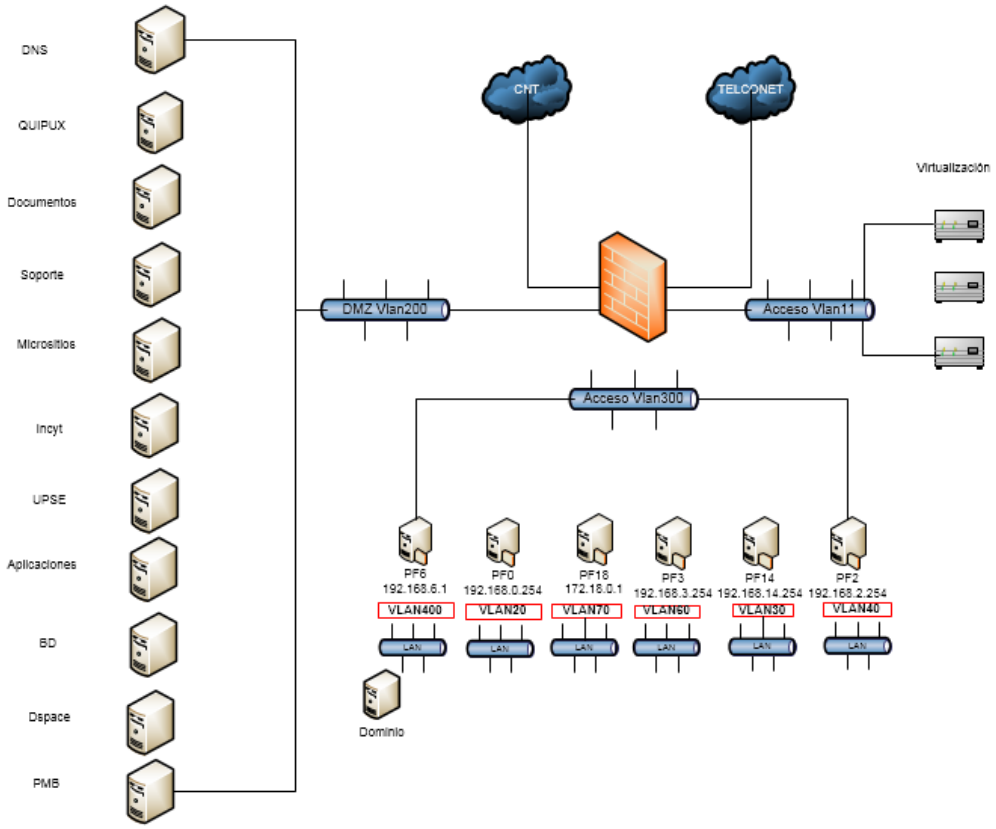


Figura 2.23. Arquitectura de Seguridad a nivel de Firewall

Toda la Arquitectura de Seguridad a nivel de Firewall y servidores, esta virtualizada, ahorrando los respectivos costos en la adquisición de equipos, tanto para servidores y firewalls.

El nateo de la DMZ hacia el internet y hacia la red LAN de las diferentes Vlans, se la realiza en la sección NAT 1:1 del Pfsense de Borde, como se presenta en la Figura 2.24, cada dirección IP privada de los servidores se apunta hacia las interfaces WAN o LAN, dependiendo de la salida de los servicios.

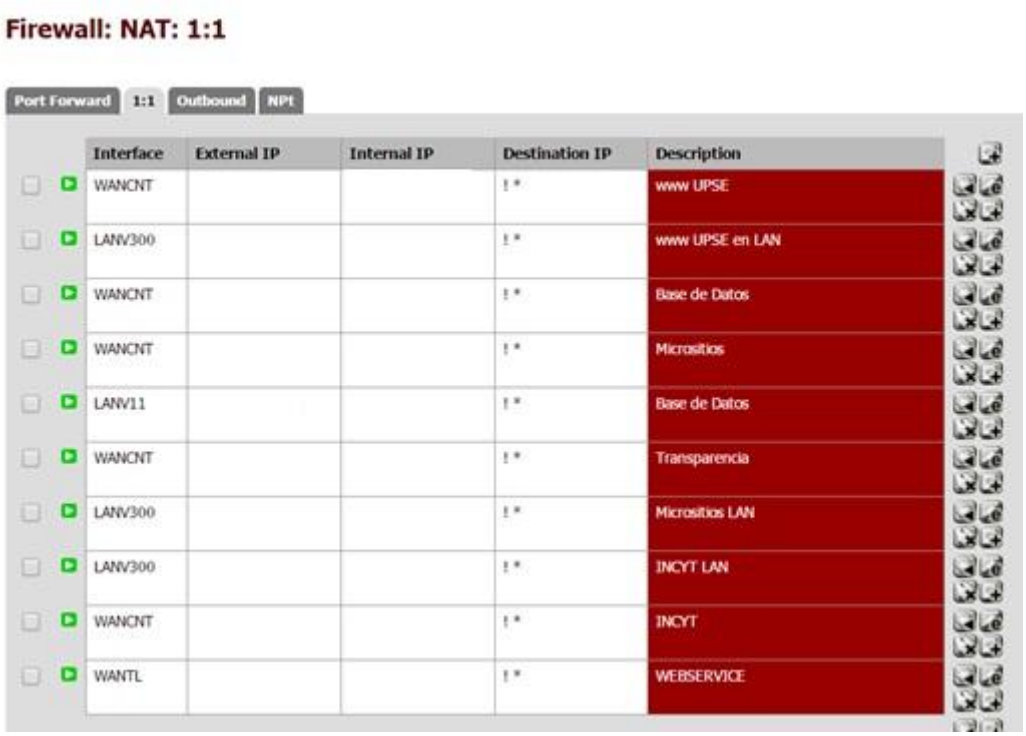


Figura 2.24. Configuración Nat de los servidores.

Por razones de seguridad y protección de datos se han eliminado las direcciones IP de los servicios. Las interfaces son asignadas según las necesidades de las salidas.

El nateo por puertos de los servidores de la DMZ hacia las diferentes redes se lo maneja en el Nat Port Forward, en este caso de la configuración se asignan puertos específicos para las salidas de varios servicios, como se lo demuestra en la Figura 2.25.

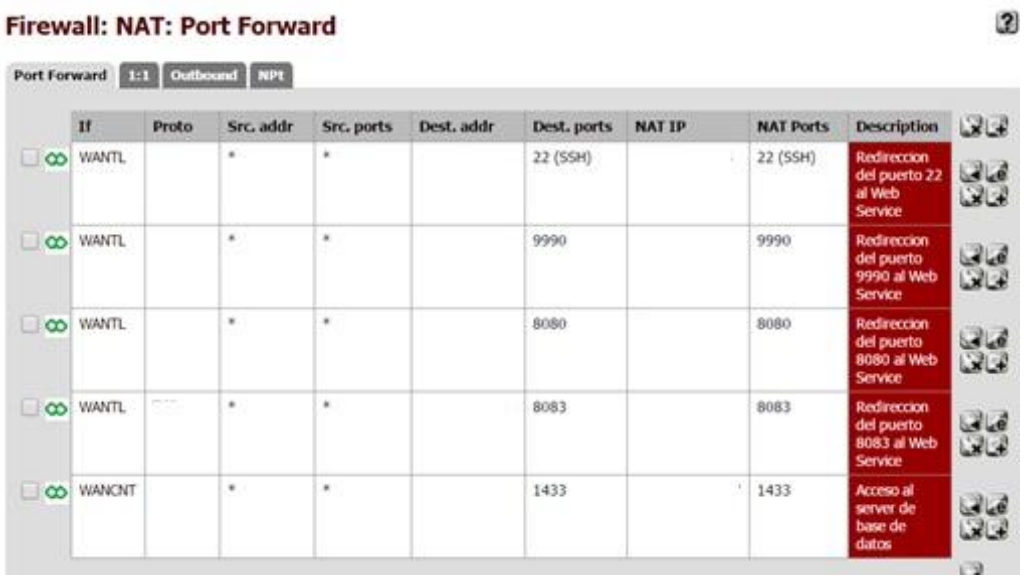


Figura 2.25. Configuración de salida de puertos.

En el presente Nat se pueden utilizar direcciones IP Virtuales, asignadas a las interface físicas del equipo, dependiendo de las salidas de los servicios por cada proveedor de internet, por ejemplo el servicio de

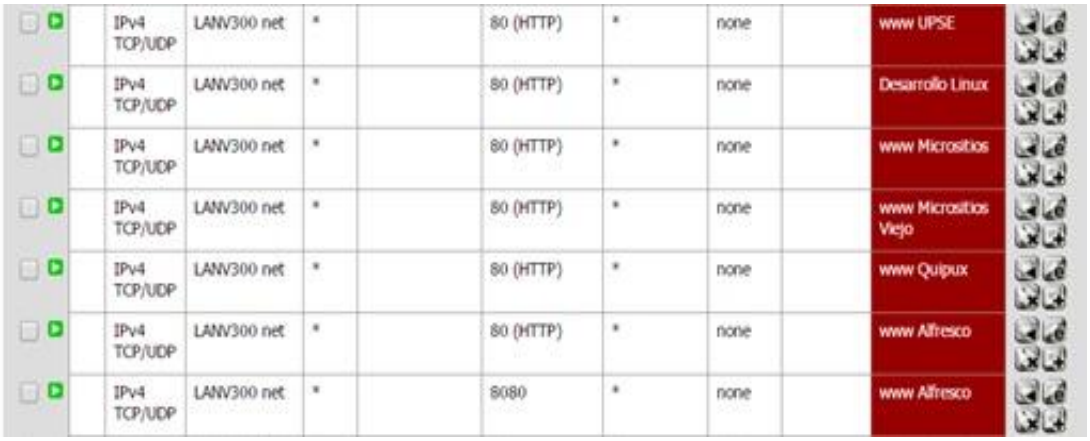
WebService, es una dirección virtual asignando un puerto específico para habilitar el servicio de SSH.

En la Figura 2.26 se muestran las IP Virtuales asignadas a las diferentes interfaces WAN, para salida por cada proveedor.

Figura 2.26. Asignación de IP Virtuales a las interfaces WAN.

Se ha destinado la salida de los servicios de correos electrónicos por la interface WAN de Telconet, para evitar los problemas de listas negras, y los servicios web que pueden salir por cualquier proveedor, dependiendo de las necesidades de la red.

Después de realizar las diferentes configuraciones anteriores, se puede proceder con las reglas de firewall de las diferentes interfaces, para ir restringiendo los puertos y accesos de cada equipo de las vlans en la red. A continuación se detalla las reglas de la interface LAN del Firewall de Borde, Figura 2.27.



	IPv4 TCP/UDP	LANV300 net	*		80 (HTTP)	*	none		www UPSE
	IPv4 TCP/UDP	LANV300 net	*		80 (HTTP)	*	none		Desarrollo Linux
	IPv4 TCP/UDP	LANV300 net	*		80 (HTTP)	*	none		www Micrositios
	IPv4 TCP/UDP	LANV300 net	*		80 (HTTP)	*	none		www Micrositios Viejo
	IPv4 TCP/UDP	LANV300 net	*		80 (HTTP)	*	none		www Quipux
	IPv4 TCP/UDP	LANV300 net	*		80 (HTTP)	*	none		www Alfresco
	IPv4 TCP/UDP	LANV300 net	*		8080	*	none		www Alfresco

Figura 2.27. Reglas de acceso desde la LAN – DMZ.

En la Figura 2.27 se muestra la interface LAN y el respectivo protocolo y puerto de origen, hacia la dirección IP de los servidores en la DMZ y el respectivo puerto de acceso, sin direccionar a algún Gateway especifico, debido a que no es necesario.

Como en toda configuración de firewall, las primeras reglas son las que toman la primera prioridad en la lectura y accesos de los servicios, por ello se ha colocado las reglas de acceso a la DMZ como primera opción de la red LAN, de ahí en adelante se priorizará las reglas según los accesos de la red.

Para las reglas de accesos de la red inalámbrica, se manejará ya las reglas con el Gateway Multiwan, con la salida del proveedor de internet CNT, haciendo referencia a la Figura 2.21, donde se detalla la Multiwan

2 con Tier1 a la interface WAN de CNT, en la Figura 2.28 se presentan las reglas de accesos.

	IPv4 TCP/UDP	192.168.45.7	*	*	80 (HTTP)	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	53 (DNS)	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	443 (HTTPS)	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	143 (IMAP)	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	993 (IMAP/S)	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	110 (POP3)	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	587 (SUBMISSION)	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	4443	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	5938	MULTIWAN2	none		Red Inalámbrica salida CNT
	IPv4 TCP/UDP	192.168.45.7	*	*	2096	MULTIWAN2	none		Red Inalámbrica salida CNT

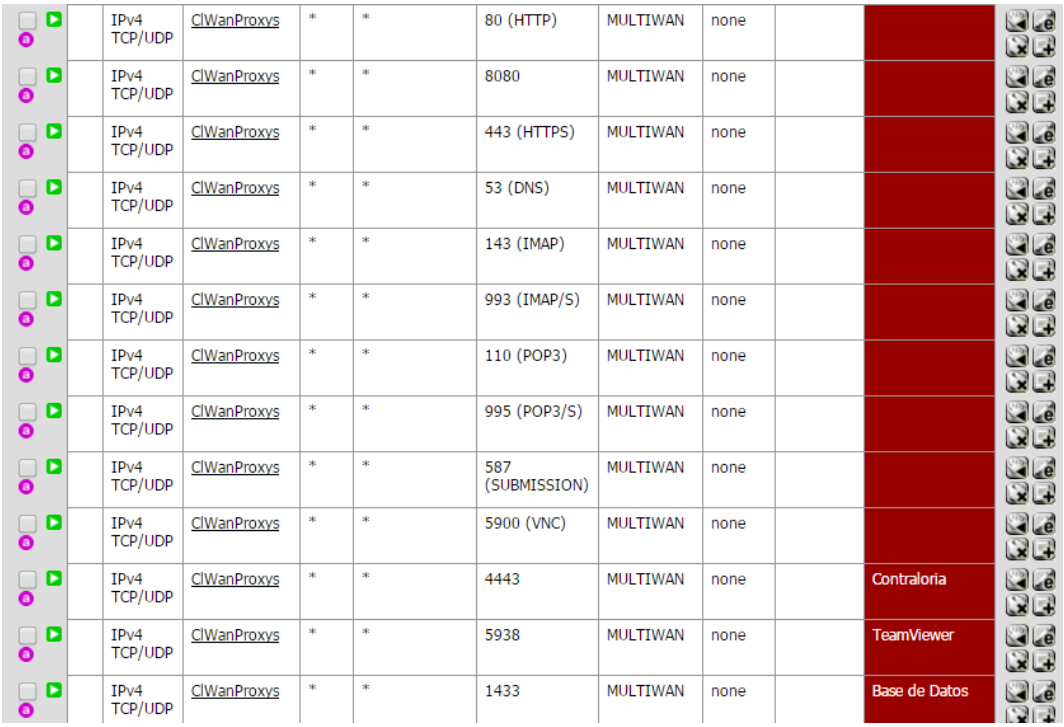
Figura 2.28. Reglas de accesos, salida por CNT.

Las reglas de la accesos para la red inalámbrica como se demuestra en la figura 2.28, solo se permiten los puertos necesarios para evitar ataques desde la red interna, cabe indicar que en la arquitectura de seguridad en un nivel abajo se encuentra otro equipo firewall que seguirá controlando el acceso de los puertos desde la red LAN de los usuarios, por lo que se reduce el riesgo de ataques internos.

Las reglas de firewall de las redes de oficinas, docentes y laboratorios, están configuradas mediante un grupo o alias de IP, asignando los diferentes puertos permitidos para el acceso de los servicios, en la Figura

2.29 se puede mostrar las reglas de accesos de los equipos Firewall-Proxys de las vlans a nivel LAN.

El alias ClWanProxys, contiene las diferentes direcciones IP de las interfaces WAN de cada Firewall-Proxy; haciendo más fácil el manejo de las reglas al asignar los respectivos puertos de accesos; la salida para el servicio de internet se la maneja con la Multiwan con Tier1 hacia el proveedor Telconet, dependiendo de las necesidades reales se puede asignar a una dirección IP la salida necesaria al internet por cualquiera de los dos proveedores.



IPv4 TCP/UDP	ClWanProxys	*	*	80 (HTTP)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	8080	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	443 (HTTPS)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	53 (DNS)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	143 (IMAP)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	993 (IMAP/S)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	110 (POP3)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	995 (POP3/S)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	587 (SUBMISSION)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	5900 (VNC)	MULTIWAN	none			
IPv4 TCP/UDP	ClWanProxys	*	*	4443	MULTIWAN	none		Contraloria	
IPv4 TCP/UDP	ClWanProxys	*	*	5938	MULTIWAN	none		TeamViewer	
IPv4 TCP/UDP	ClWanProxys	*	*	1433	MULTIWAN	none		Base de Datos	

Figura 2.29. Reglas de Firewall para las redes de Oficinas.

Después de realizar las diferentes configuraciones de las reglas del Firewall de Borde, se pueden consultar los respectivos logs, consumo de anchos de banda, tablas de estados, realizar respaldos de las configuraciones sea en general o por los servicios implementados, realizar diagnósticos de los servicios. En la Figura 2.30 se muestra el consumo de ancho de banda que mantienen las dos interfaces WAN de los proveedores Telconet y CNT.

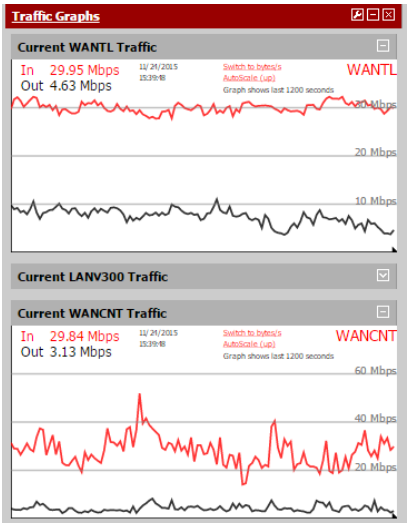


Figura 2.30. Consumo de ancho de banda.

Firewalls-Proxys de Acceso.- la arquitectura de seguridad implementada en la Figura 2.23 según las vlan de accesos están asignados los firewall en cada subred, realizan el control de:

- Control de accesos por puertos.
- Control de navegación a través de Squid.

- Control y denegación de sitios con SquidGuard.
- Monitoreo de la navegación de la LAN de usuarios.

Se realizara la explicación de la configuración general de cada servicio aplicado en los Firewall – Proxys de acceso, debido a que todos tienen la misma configuración de servicios, solo cambian las reglas de firewall por las solicitudes de accesos en las diferentes subredes.

Al igual que el Firewall de Borde, se realiza la instalación de la versión de Pfsense de 64 bits, debido a que es la versión actual y sin problemas de seguridades. Se mantiene la visualización del dashboard con los servicios y widgets añadidos, Figura 2.31.

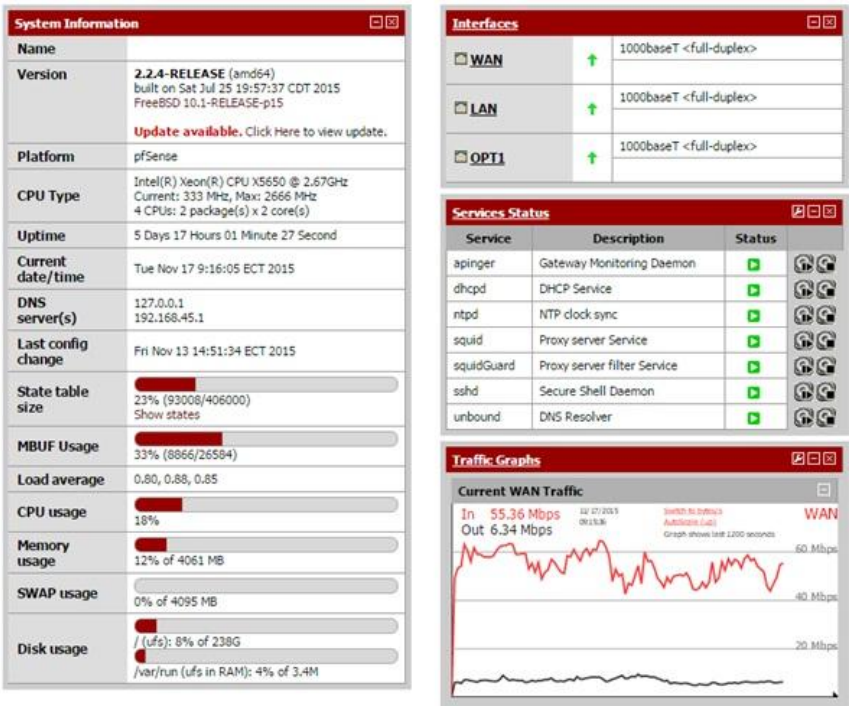


Figura 2.31. Dashboard de Firewall – Proxy.

La Figura 2.31 muestra el equipo que pertenece a la red inalámbrica, el cual fue instalado con doble procesador debido al consumo de recursos que se detectó, por las diferentes conexiones que mantiene, actualmente atiende a 2100 usuarios aproximadamente, y el consumo de ancho de banda varía entre 40 a 60 Mbps en la red de CNT.

Los servicios activos dependerán de las necesidades de cada subred, por ejemplo el servicio de DHCP estará activo en el equipo de la red inalámbrica, pero no en el equipo de oficinas y docentes, debido a que en esa subred será manejado por un controlador de dominio.

La instalación de cada paquete en el Pfsense se la realiza por la administración web, donde se puede seleccionar los paquetes necesarios según el tipo de servicio que se desee implementar; para el nivel de los Firewall – Proxys se han escogido los paquetes de Squid, SquidGuard y Suricata, en la Figura 2.32 se presentan los paquetes instalados.

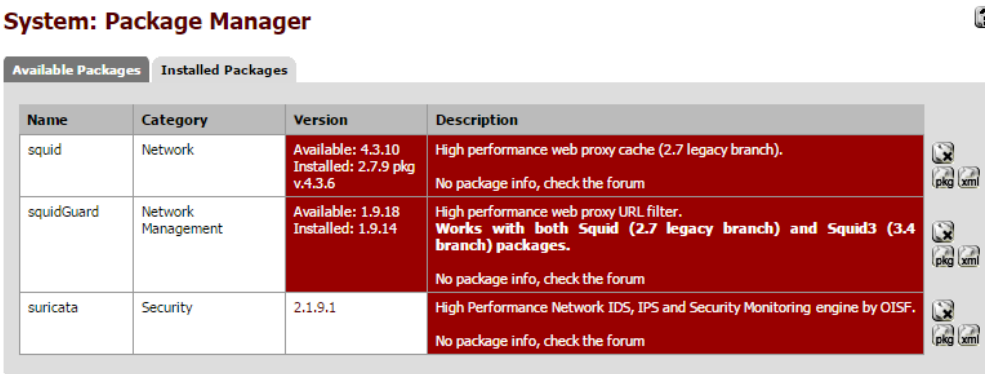


Figura 2.32 Paquetes de los servicios instalados.

La configuración de los servicios de Squid, se procede mediante el menú Services y seleccionando del menú la opción de Proxy Server; nuevamente según las necesidades de la red se realiza la configuración de un proxy transparente o no, para el control de la navegación, se pueden crear las respectivas reglas de accesos ACL, control de ancho de banda por Delay Pools, la Figura 2.33 muestra la interface de configuración con su respectivo menú dentro del servicio de Squid.

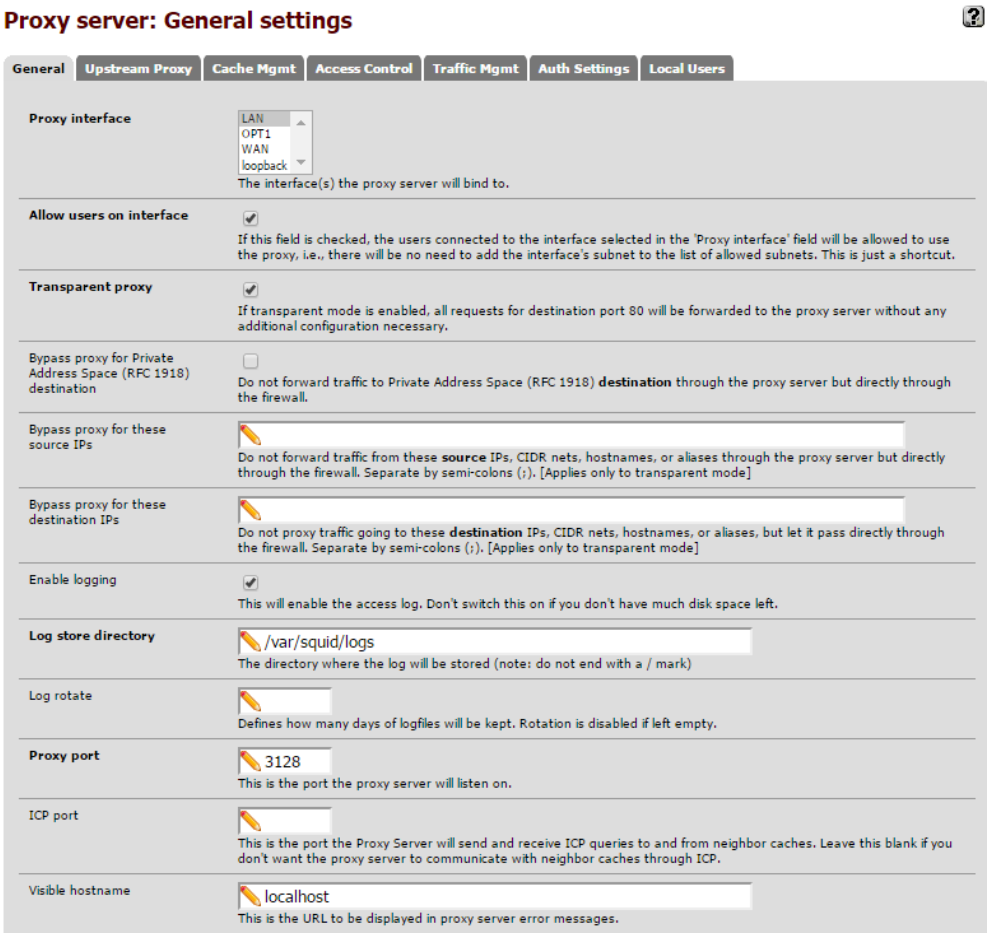


Figura 2.33.Interface de configuración del servicio de Squid

La implementación del control de la navegación se la realiza por medio del servicio de SquidGuard, donde se aplica la configuración de listas de accesos, frases permitidas o denegadas, direcciones IP sin restricciones, denegación de sitios por contenido, sitios permitidos por horarios. El servicio de SquidGuard ha ayudado a nivelar el consumo del ancho de banda, por las diferentes restricciones que se han implementado; a continuación en la Figura 2.34 se presenta la interface de configuración de Squidguard.

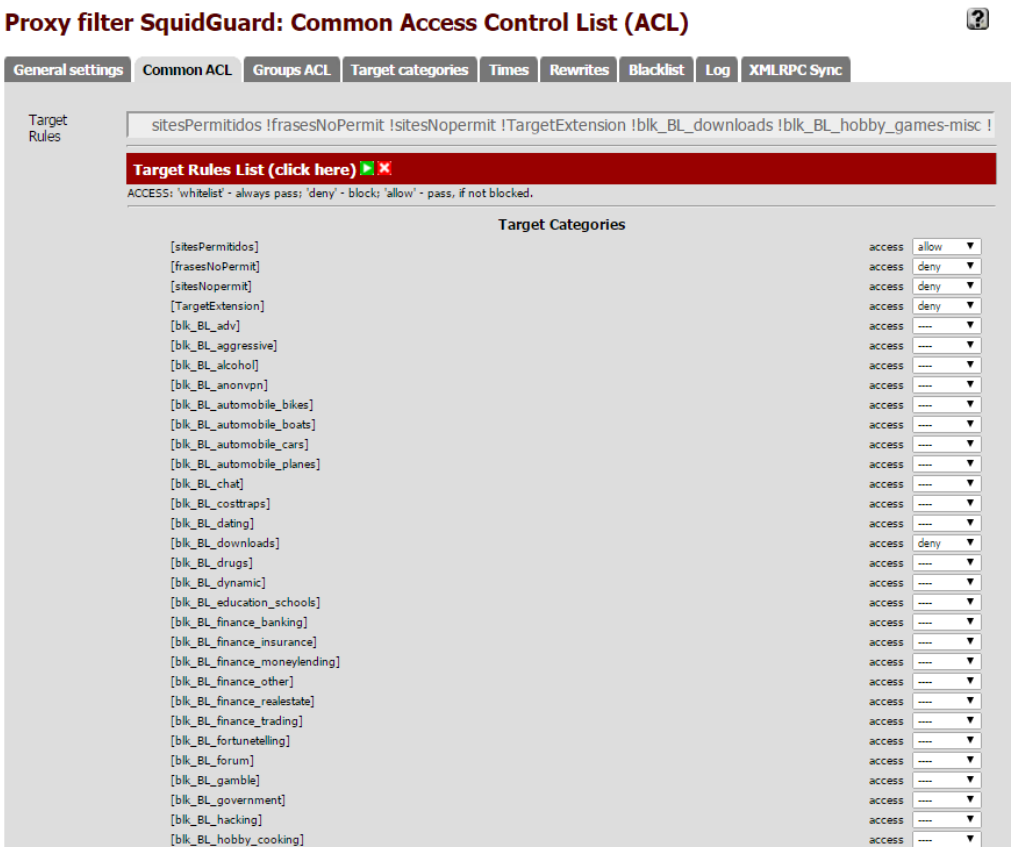


Figura 2.34. Interface de configuración de SquidGuard.

Las reglas de cada firewall dependerán de las necesidades de la red y de los diferentes usuarios, en la Figura 2.35 se muestra las reglas del firewall de la red de oficinas y de los accesos con privilegios a todos los puertos del equipo de ciertas direcciones IP asignadas a un Alias, para llegar a los servidores alojados en la DMZ; por las razones de las configuraciones de los servicios se ha permito estos accesos a la DMZ.

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule
		IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
		IPv4 *	IpTics	*	*	*	*	none		
		IPv4 *	ServidoresVm	*	*	*	*	none		
		IPv4 *	192.168.6.50	*	*	*	*	none		
		IPv4 TCP/UDP	LAN net	*	*	80 (HTTP)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	3128	*	none		
		IPv4 TCP/UDP	LAN net	*	*	8083	*	none		Puerto relaciones laborales
		IPv4 TCP/UDP	LAN net	*	*	443 (HTTPS)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	143 (IMAP)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	993 (IMAP/S)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	110 (POP3)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	995 (POP3/S)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	587 (SUBMISSION)	*	none		
		IPv4 TCP/UDP	LAN net	*	*	5900 (VNC)	*	none		

Figura 2.35. Reglas de Firewall de Vlan de Oficina.

2.4. IMPLEMENTACIÓN DE IDS/IPS SURICATA.

Suricata [3] como IDS/IPS ayuda a mejorar las seguridades de la red creando un nivel adicional para la prevención de vulnerabilidades que los firewall no puedan detectar; se escogió la opción de la implementación de Suricata por tener una arquitectura de multi-hilos en comparación con Snort. Suricata es creada por la comunidad Open Information Security Foundation (OISF), las principales características de Suricata son:

- Multi-hilo o multi-threading
- Captura de paquetes.
- Decodificador, inspección de la capa aplicación.
- Detección y comparación de firmas.
- Procesamiento de eventos y salida de alertas
- Detección de protocolos automáticos.
- Fast IP Matching.

La actual implementación de Suricata, ha ayudado a encontrar las diferentes vulnerabilidades en los segmentos de red a nivel de ataques internos o maquinas infectadas con botnets, trojanos, etc; que en muchos casos han hecho colapsar el segmento de red donde ha estado el problema.

Las configuraciones de Suricata [4] se las ha ido realizando desde los Firewalls – Proxys hasta el Firewall de Borde; en los equipos de accesos

se asignó el análisis a la interface LAN, con el fin de detectar los equipos que generen problemas para la red, la Figura 2.36 muestra la configuración de Suricata en una de las subredes de Oficinas y las respectivas anomalías detectadas.

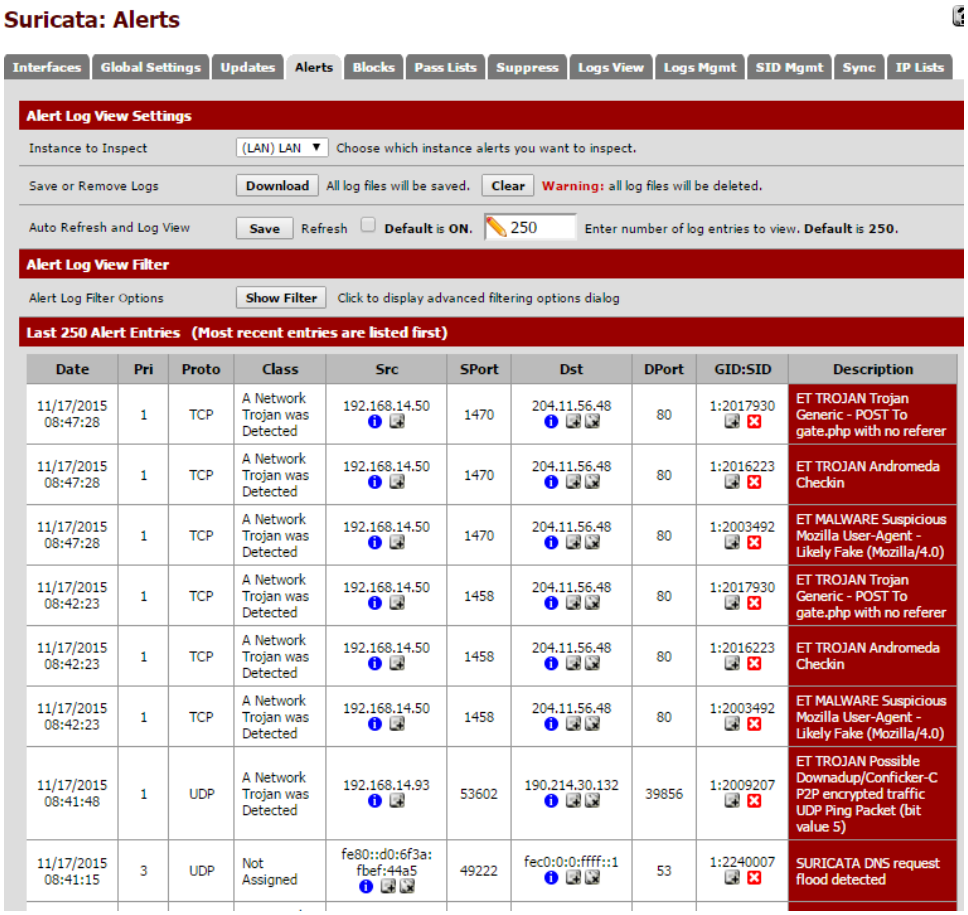


Figura 2.36. Detección de anomalías por Suricata en la subred de Oficinas.

Cabe indicar que en la ejecución de Suricata, se han detectado diferentes anomalías en los segmentos de red, considerando que a las subredes de Oficinas, Docentes y Laboratorio se tienen accesos a los

equipos para la eliminación de las vulnerabilidades; a diferencia de la red inalámbrica que depende de las maquinas o dispositivos de cada usuario. En la Figura 2.37 se muestra las detecciones de la red inalámbrica, las cuales permanecen en bloqueo hacia la IP destino.

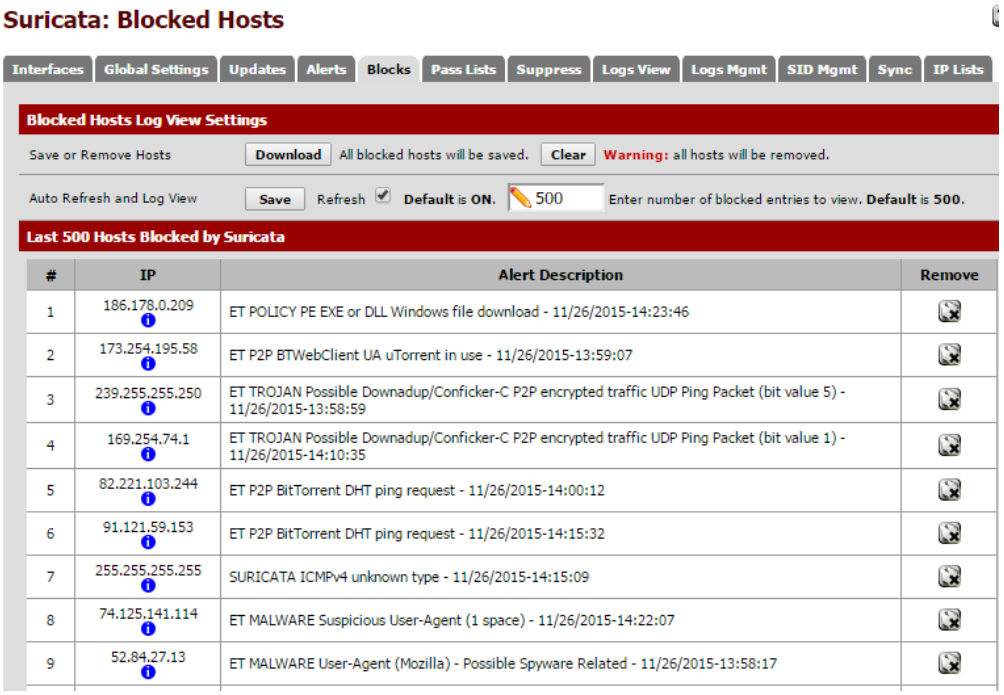


Figura 2.37 Detección y bloqueo de anomalías en la red inalámbrica.

2.5. IMPLEMENTACIÓN DEL MONITOREO DE LOS EQUIPOS DE RED.

El monitoreo de los equipos de red se ha implementado con el software PRTG Network Monitor [5] la versión libre, de la empresa Paessler; la instalación se la ha realizado con la opción límite de 100 sensores, los cuales han sido distribuidos en los diferentes equipos instalados en la arquitectura de red de la Figura 2.2.

Las funcionalidades que el software de monitoreo presenta son las siguientes:

- Soporte de protocolos SNMP y WMI.
- Visualización de consumo de ancho de banda por puertos.
- Mensajería en caso de ocurrir caídas de equipos.
- Mensajería cuando existen bajos consumos de ancho de banda.
- Mensajería cuando se presentan saturaciones.

El software de monitoreo ha ayudado a mejorar el control de la red, realizando las asistencias técnicas de forma inmediata, y dando pautas para mejorar el consumo de ancho de banda por sectores en los nodos de distribución y de acceso. La configuración de PRTG se la realiza mediante interface web, Figura 2.38 y muestra una consola en tiempo real del estado de la red, Figura 2.39.

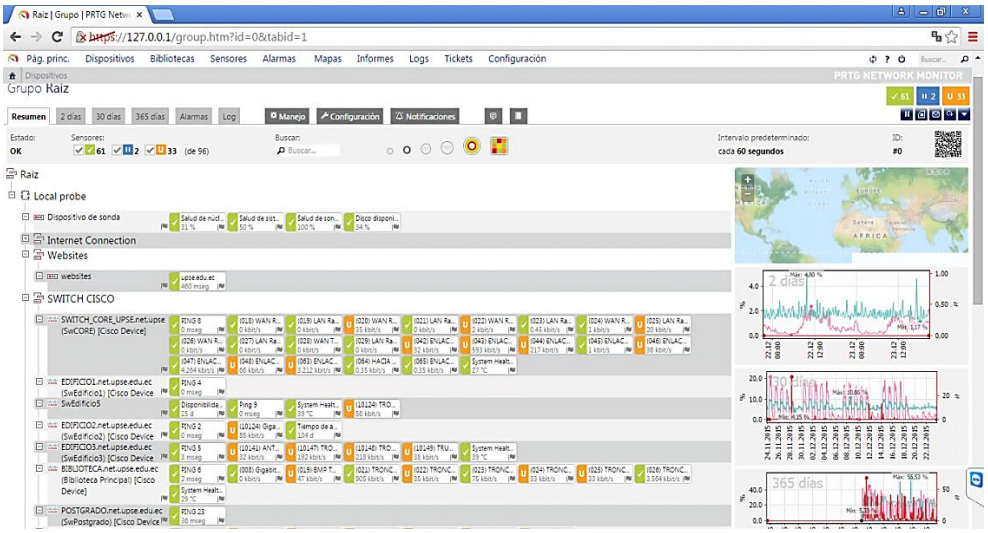


Figura 2.38 Interface de Configuración Web

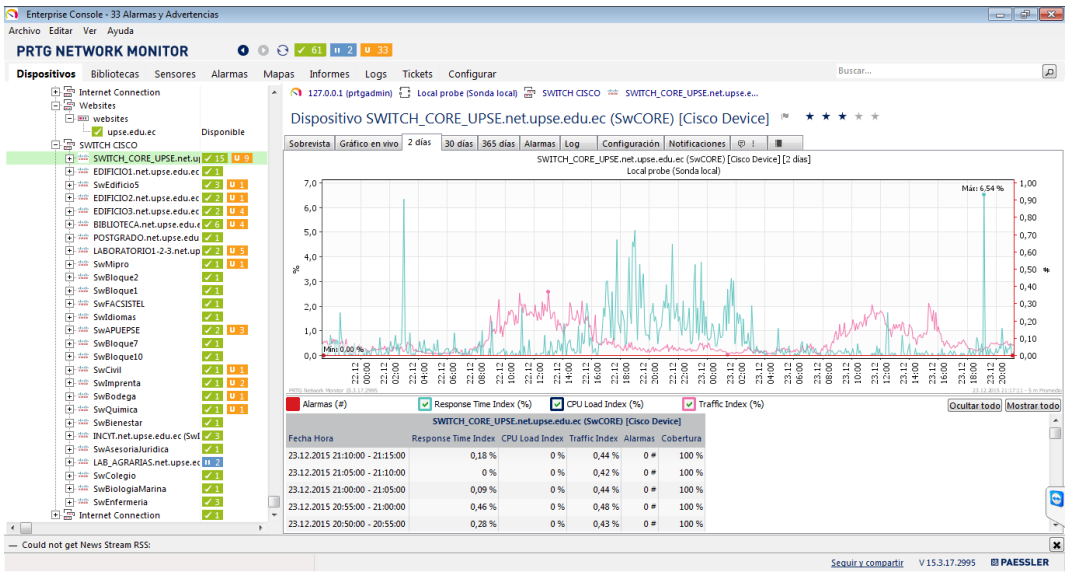


Figura 2.39 Consola en tiempo real del PRTG.

La configuración entre el PRTG y los equipos switch CISCO, se la ha realizado mediante SNMP con las respectivas seguridades; la mensajería del monitoreo se la realizó designando a un grupo de correos para la notificación de las novedades que se puedan presentar, para así asistir inmediatamente los sitios donde se encuentran ubicados los diferentes equipos de la red.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1. VERIFICACIÓN Y PRUEBAS DEL CONSUMO DEL ANCHO DE BANDA POR LOS DIFERENTES SEGMENTOS DE RED.

Realizada todas las implementaciones a nivel de la arquitectura de red Figura 2.2 y de las seguridades a nivel de firewall Figura 2.23, se puede realizar el monitoreo de los diferentes segmentos de red en sus respectivas Vlans, actualmente se tienen diferentes Firewall – Proxys por la segmentación de la red y por el acceso a los servicios informáticos.

La salida hacia el servicio de internet de las Vlans de rectorado, oficinas, docentes, se la realiza a través del proveedor Telconet, se realizó el

respectivo monitoreo, visualizando el consumo del ancho de banda de cada Firewall – Proxy, a continuación en la Figura 3.1 se muestra el consumo de la red de oficinas

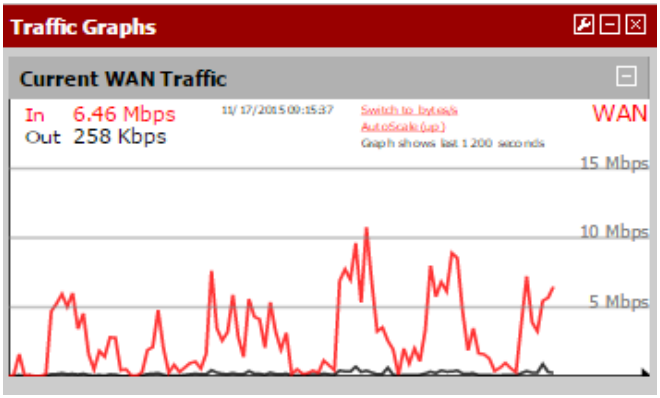


Figura 3.1 Gráfica de consumo de ancho de banda de la red de Oficinas

En el presente año se contrató el servicio de internet con la siguiente capacidad: Telconet 30 Mbps y CNT 70 Mbps; por lo que se designa para las subredes de Oficina y Docentes la salida por el servicio de Telconet; en cambio por el consumo y la cantidad de usuarios que actualmente se presentan en las subredes Wireless se designa la salida por el servicio de CNT.

Las redes de rectorado, oficinas y docentes mantienen una Mutiwan como proveedor principal a Telconet, es decir si se llegara a caer el servicio del proveedor 1, se cambiaría automáticamente al proveedor 2, en este caso CNT, en la Figura 3.2 se presenta el consumo del Firewall de Borde por cada interface de red de los proveedores.

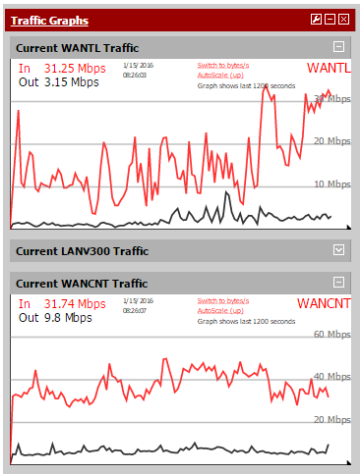


Figura 3.2 Consumo de ancho de banda por interfaces de proveedores

El monitoreo de cada Firewall – Proxy, también permite visualizar el consumo de ancho de banda por dirección IP, así se ha detectado los equipos que podrían presentar problemas de virus, o a usuarios que están utilizando sistemas de descargas que pueden burlar el control de los Proxys, lo cual es identificado y mitigado. En la Figura 3.3 se presenta la gráfica de consumo de ancho de banda por direcciones IP de la red inalámbrica.

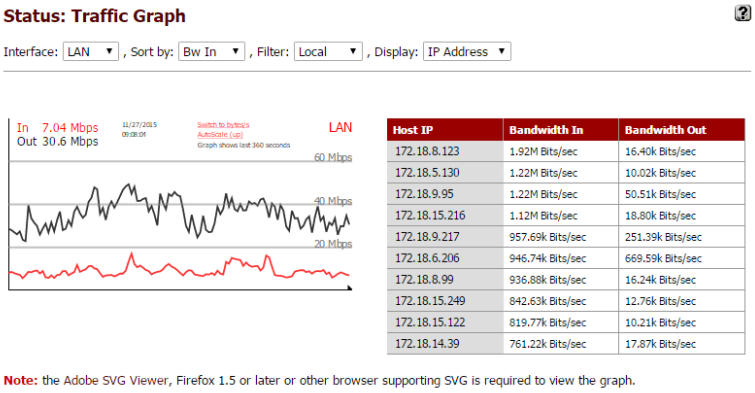
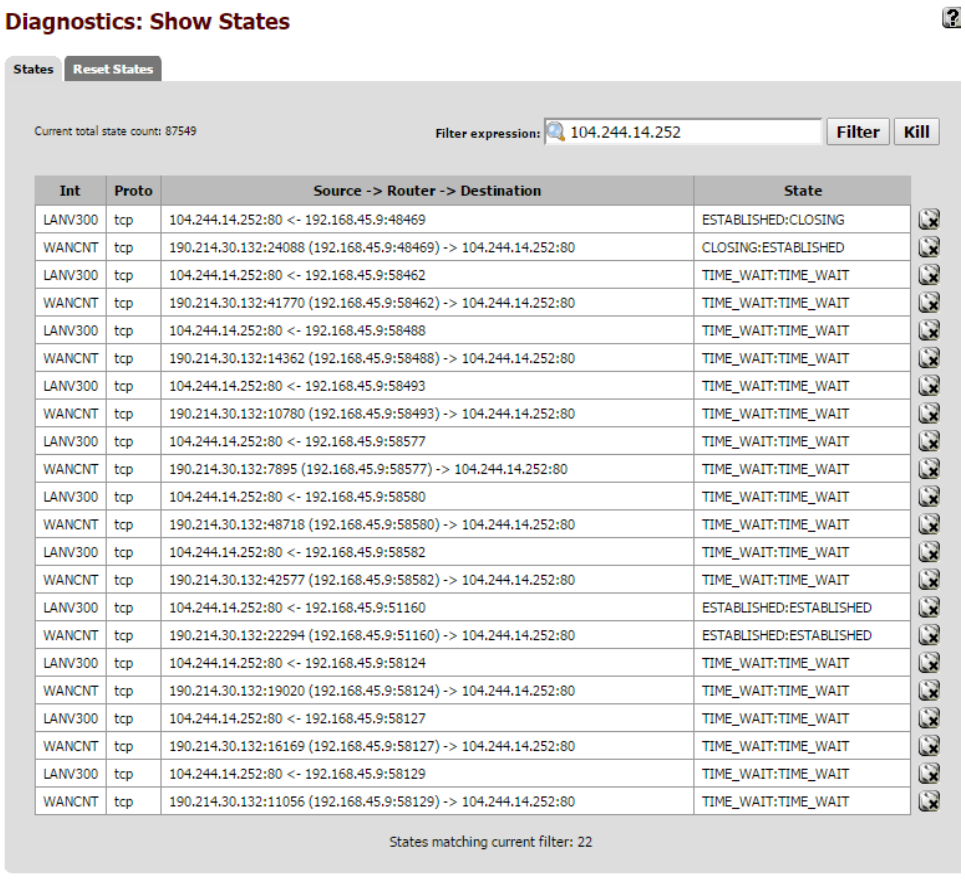


Figura 3.3 Consumo de ancho de banda por direcciones IP, red Wireless.

Cuando se verifica el consumo muy alto de una dirección IP, se visualizan los respectivos log del Squid, para monitorear el acceso a los diferentes sitios, también se visualiza la tabla de estado tanto del Firewall de Borde y de Acceso del segmento que se está monitoreando. Como por ejemplo en la Figura 3.4 se presenta la tabla de estado del Firewall de Borde, haciendo referencia a la IP de la interface WAN del Firewall – Proxy de la red Wireless.



Diagnostics: Show States

States | Reset States

Current total state count: 87549

Filter expression: 104.244.14.252 Filter Kill

Int	Proto	Source -> Router -> Destination	State
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:48469	ESTABLISHED:CLOSING
WANCNT	tcp	190.214.30.132:24088 (192.168.45.9:48469) -> 104.244.14.252:80	CLOSING:ESTABLISHED
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58462	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:41770 (192.168.45.9:58462) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58488	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:14362 (192.168.45.9:58488) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58493	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:10780 (192.168.45.9:58493) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58577	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:7895 (192.168.45.9:58577) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58580	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:48718 (192.168.45.9:58580) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58582	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:42577 (192.168.45.9:58582) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:51160	ESTABLISHED:ESTABLISHED
WANCNT	tcp	190.214.30.132:22294 (192.168.45.9:51160) -> 104.244.14.252:80	ESTABLISHED:ESTABLISHED
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58124	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:19020 (192.168.45.9:58124) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58127	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:16169 (192.168.45.9:58127) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT
LANV300	tcp	104.244.14.252:80 <- 192.168.45.9:58129	TIME_WAIT:TIME_WAIT
WANCNT	tcp	190.214.30.132:11056 (192.168.45.9:58129) -> 104.244.14.252:80	TIME_WAIT:TIME_WAIT

States matching current filter: 22

Figura 3.4 Tabla de Estado del Firewall de Borde.

Una vez identificado a que sitios estaría accediendo el usuario, se procede a la mitigación si fuera algún problema de virus o saltos de protección por parte de los usuarios; por lo general son problemas de virus en la red inalámbrica, y se procede con el bloqueo de la dirección IP por medio de la dirección MAC del usuario, dependiendo del riesgo del ataque.

3.2. ANÁLISIS DE LOS RESULTADOS DEL IDS/IPS SURICATA.

Suricata se ha implementado según las necesidades de las diferentes subredes, para identificar los problemas de seguridades, tanto en el Firewall de Borde y en los Firewall – Proxys de cada segmento de red; se empezó con la implementación en el segmento de la red Wireless, debido a que se identificó demasiado consumo del servicio de internet a nivel general y luego por cada dirección IP de los diferentes usuarios.

Se procedió con la implementación de Suricata en la red Wireless, detectando varias anomalías, entre ellas se encontraron botnets, diferentes tipos de virus, intentos de descargar por torrents, DNS poison, entre otros.

En la Figura 3.5, se presentan los resultados de las detecciones de las anomalías que fueron bloqueadas por el IDS/IPS Suricata, en donde se encuentra las botnets de los virus Conficker, Zeus, intentos de ping ICMP, malware alojados en navegadores.

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help | pfwin

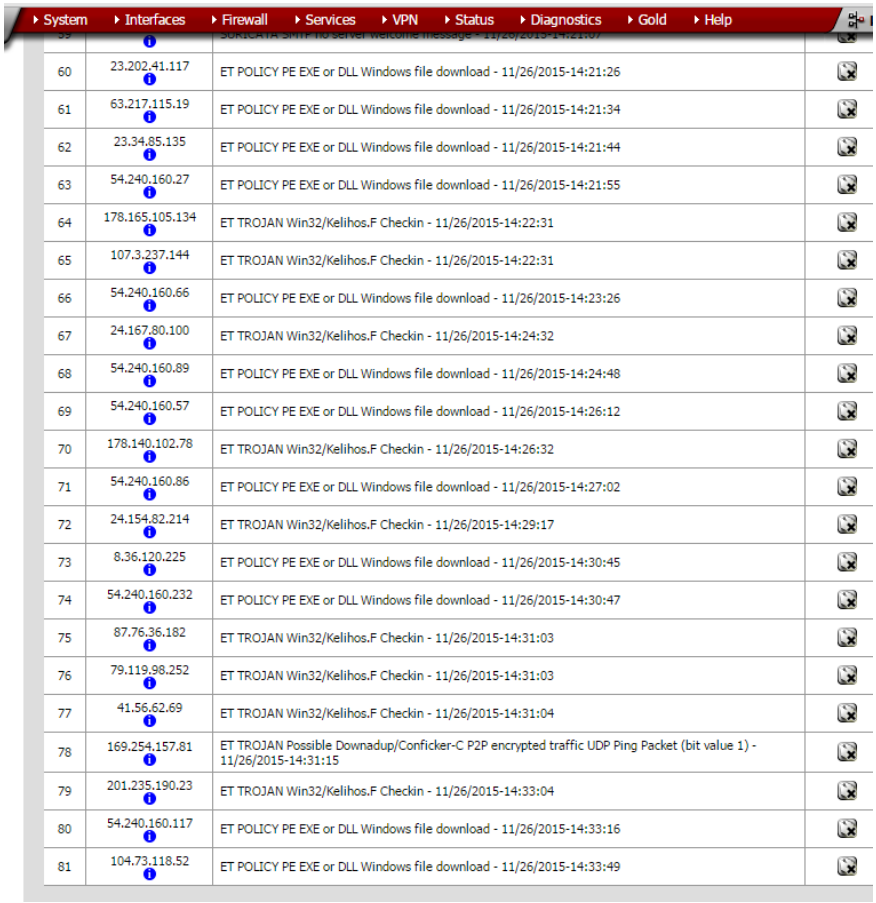
11/27/2015 09:06:27	3	ICMP	Not Assigned	172.18.9.142	3	172.18.0.1	3	1:2200027	SURICATA ICMPv4 unknown version
11/27/2015 09:06:27	3	ICMP	Not Assigned	172.18.9.142	3	172.18.0.1	3	1:2200027	SURICATA ICMPv4 unknown version
11/27/2015 09:06:27	3	ICMP	Not Assigned	172.18.9.142	3	172.18.0.1	3	1:2200027	SURICATA ICMPv4 unknown version
11/27/2015 09:06:26	3	IPV6-ICMP	Not Assigned	fe80::2c05:317e:d47a:564	135	ff02::1:ffc9:684f	0	1:2200079	SURICATA ICMPv6 invalid checksum
11/27/2015 09:06:25	3	IPV6-ICMP	Not Assigned	fe80::2c05:317e:d47a:564	135	ff02::1:ffc9:684f	0	1:2200079	SURICATA ICMPv6 invalid checksum
11/27/2015 09:06:24	1	TCP	A Network Trojan was detected	172.18.0.111	1590	176.9.82.215	80	1:35030	MALWARE-CNC Win.Trojan.Zeus variant outbound connection
11/27/2015 09:06:24	3	IPV6-ICMP	Not Assigned	fe80::2c05:317e:d47a:564	135	ff02::1:ffc9:684f	0	1:2200079	SURICATA ICMPv6 invalid checksum
11/27/2015 09:06:23	3	IPV6-ICMP	Not Assigned	fe80::2c05:317e:d47a:564	135	ff02::1:ffc9:684f	0	1:2200079	SURICATA ICMPv6 invalid checksum
11/27/2015 09:06:22	3	IPV6-ICMP	Not Assigned	fe80::2c05:317e:d47a:564	135	ff02::1:ffc9:684f	0	1:2200079	SURICATA ICMPv6 invalid checksum
11/27/2015 09:06:21	1	TCP	A Network Trojan was detected	172.18.12.71	49392	95.213.186.51	80	1:35549	MALWARE-CNC Win.Trojan.Zeus variant outbound connection
11/27/2015 09:06:10	1	TCP	A Network Trojan was detected	172.18.13.9	49426	95.213.186.51	80	1:2003492	ET MALWARE Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)
11/27/2015 09:06:07	1	UDP	A Network Trojan was detected	172.18.9.27	43378	157.56.52.48	40009	1:2009207	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)
11/27/2015 09:05:55	1	TCP	A Network Trojan was detected	172.18.0.111	1590	176.9.82.215	80	1:2003492	ET MALWARE Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)
11/27/2015 09:05:51	3	ICMP	Not Assigned	172.18.5.100	10	255.255.255.255	0	1:2200024	SURICATA ICMPv4 unknown type
11/27/2015 09:05:51	1	TCP	A Network Trojan was detected	172.18.12.71	49392	95.213.186.51	80	1:2003492	ET MALWARE Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)
11/27/2015 09:05:46	1	TCP	A Network Trojan was detected	172.18.10.137	50078	8.34.112.19	80	1:30261	PUA-ADWARE Lucky Leap Adware outbound connection

Figura 3.5 Muestra de bloqueo del IDS/IPS Suricata en la red Wireless.

Las anomalías en la red inalámbrica son críticas, debido a que por los problemas encontrados la dirección IP principal del servicio de internet alojada en la interface WAN del Firewall de Borde, muchas veces caía en las listas negras de los servicios de internet; por lo que se procedió a dejar permanentemente el servicio de Suricata activo en la red Wireless. Después de analizar los diferentes bloqueos del IDS/IPS y haciendo las pruebas de accesos a las direcciones IP públicas que eran bloqueadas,

se observó que algunas IP pertenecían a servicios validos como Facebook, sitios de páginas del Estado, servicios de Google, entre otros; por lo que se procedió a colocar las direcciones ya confirmadas en las listas de exclusiones y procediendo a bloquear la dirección de origen en la red LAN.

En la Figura 3.6 se puede observar los bloqueos finales del IDS/IPS Suricata, donde se presentan las direcciones IP públicas las cuales intentan realizar peticiones hacia la red LAN.



60	23.202.41.117	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:21:26
61	63.217.115.19	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:21:34
62	23.34.85.135	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:21:44
63	54.240.160.27	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:21:55
64	178.165.105.134	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:22:31
65	107.3.237.144	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:22:31
66	54.240.160.66	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:23:26
67	24.167.80.100	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:24:32
68	54.240.160.89	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:24:48
69	54.240.160.57	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:26:12
70	178.140.102.78	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:26:32
71	54.240.160.86	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:27:02
72	24.154.82.214	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:29:17
73	8.36.120.225	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:30:45
74	54.240.160.232	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:30:47
75	87.76.36.182	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:31:03
76	79.119.98.252	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:31:03
77	41.56.62.69	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:31:04
78	169.254.157.81	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1) - 11/26/2015-14:31:15
79	201.235.190.23	ET TROJAN Win32/Kelihos.F Checkin - 11/26/2015-14:33:04
80	54.240.160.117	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:33:16
81	104.73.118.52	ET POLICY PE EXE or DLL Windows file download - 11/26/2015-14:33:49

Figura 3.6 Bloqueos de direcciones Ip públicas por IDS/IPS Suricata.

Se verifica en la Figura 3.6 las diferentes anomalías que tratan de ingresar a la red LAN, las cuales son solicitadas por los equipos infectados en la red, se presentan las botnets de los virus Kelihos, Conficker, y otras detecciones.

Para la red de oficinas, docentes y laboratorios, las detecciones de Suricata han ayudado a identificar los diferentes equipos con problemas de seguridad, y procediéndolos a asistir para la respectiva eliminación de los problemas encontrados, a diferencia de la red Wireless. A continuación en la Figura 3.7 se presentan las detecciones en la red de oficinas por parte de Suricata.

Last 250 Alert Entries (Most recent entries are listed first)

Date	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
11/17/2015 08:59:24	1	TCP	A Network Trojan was Detected	192.168.14.50	1712	46.105.103.219	80	1:2018340	ET TROJAN Win32.Sality-GR Checkin
11/17/2015 08:59:14	1	UDP	A Network Trojan was Detected	192.168.14.93	63095	224.0.0.252	5355	1:2009207	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)
11/17/2015 08:58:54	3	UDP	Not Assigned	192.168.14.155	52951	192.168.14.254	53	1:2240007	SURICATA DNS request flood detected
11/17/2015 08:57:39	1	TCP	A Network Trojan was Detected	192.168.14.50	1692	204.11.56.48	80	1:2017930	ET TROJAN Trojan Generic - POST To gate.php with no referer
11/17/2015 08:57:39	1	TCP	A Network Trojan was Detected	192.168.14.50	1692	204.11.56.48	80	1:2016223	ET TROJAN Andromeda Checkin
11/17/2015 08:57:39	1	TCP	A Network Trojan was Detected	192.168.14.50	1692	204.11.56.48	80	1:2003492	ET MALWARE Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)
11/17/2015 08:53:09	1	UDP	A Network Trojan was Detected	192.168.14.93	53602	200.93.232.54	27046	1:2009207	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)
11/17/2015 08:52:37	1	UDP	A Network Trojan was Detected	192.168.14.93	53602	200.93.232.54	26879	1:2009208	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 16)
11/17/2015 08:52:37	1	UDP	A Network Trojan was Detected	192.168.14.93	53602	200.93.232.54	26876	1:2009205	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)
11/17/2015 08:52:36	1	UDP	A Network Trojan was Detected	192.168.14.93	53602	200.93.232.54	26888	1:2009206	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)

Figura 3.7 Detecciones de anomalías de la red de oficinas.

Las detecciones de Suricata muestran las direcciones IP de la red de oficinas que se encuentran infectadas, las cuales son identificadas y luego el servicio técnico del departamento de Sistemas realizará el respectivo trabajo para la eliminación de los problemas encontrados en cada equipo.

La implementación del IDS/IPS Suricata es compleja, debido a que el administrador de la red debe de estar en constante monitoreo de la detección de anomalías, para analizar los resultados y proceder a identificarlos como amenazas internas o externas, así mismo realizar las diferentes exclusiones que se pueden dar para la red.

3.3. MITIGACIÓN DE LOS PROBLEMAS ENCONTRADOS POR SURICATA.

La detección de las diferentes anomalías ha ayudado a mejorar el rendimiento de la red en las diferentes subredes que actualmente están implementadas; realizando los diferentes controles de ancho de banda y buscando las soluciones puntuales de los equipos infectados.

A continuación se detallan los procedimientos para la mitigación de las anomalías encontradas en las subredes de Oficinas, Docentes y Laboratorios:

- Identificación de las direcciones Ip en la red LAN.

- Identificación de la MAC del equipo.
- Bloqueo temporal del equipo según las anomalías encontradas.
- Asistencia en el sitio, identificación del problema aplicando análisis forense.
- Una vez detectada la amenaza se procederá con la eliminación o formateo del equipo si es necesario.

En los análisis forenses aplicados se ha detectado que para los casos de las botnets, aunque se mantienen abiertos solo los puertos necesarios en los Firewall – Proxys que alimentan a cada red LAN, la salida de las anomalías hacia el internet se ejecutan sin problemas; se identificó que utilizan las búsquedas de puertos abiertos y en muchos casos obtienen la salida por el puerto 80, designado para el servicio de internet.

Los intentos de descargas de bitorrens y servicios ICMP, el Firewall de cada subred si lo bloquea con efectividad, por las respectivas reglas de accesos, las cuales se pueden verificar en el respectivo log, Figura 3.8.

Last 50 firewall log entries.Max(50)

Act	Time	If	Source	Destination	Proto
✖	Dec 28 13:28:46	LAN	192.168.14.56:137	192.168.14.255:137	UDP
✖	Dec 28 13:28:46	OPT1	192.168.6.23:137	192.168.7.255:137	UDP
✖	Dec 28 13:28:47	OPT1	192.168.6.23:137	192.168.7.255:137	UDP
✖	Dec 28 13:28:47	LAN	192.168.14.56:137	192.168.14.255:137	UDP
✖	Dec 28 13:28:47	OPT1	192.168.6.23:137	192.168.7.255:137	UDP
✖	Dec 28 13:28:48	OPT1	192.168.6.23:137	192.168.7.255:137	UDP
✖	Dec 28 13:28:49	LAN	192.168.14.56:137	192.168.14.255:137	UDP
✖	Dec 28 13:28:49	LAN	192.168.14.56:137	192.168.14.255:137	UDP
✖	Dec 28 13:28:50	LAN	192.168.14.56:137	192.168.14.255:137	UDP
✖	Dec 28 13:28:50	OPT1	192.168.6.23	192.168.6.8	ICMP
✖	Dec 28 13:28:52	LAN	192.168.14.56:137	192.168.14.255:137	UDP
✖	Dec 28 13:28:52	LAN	192.168.14.56:137	192.168.14.255:137	UDP

Figura 3.8 Log de Firewall de Oficinas, bloqueo de puertos.

Para la mitigación de las anomalías de la red Wireless, los procedimientos son diferentes, debido a que es casi imposible tener accesos a los equipos de los usuarios, y la ejecución de las soluciones se las realiza directamente en los Firewall – Proxys, las cuales consisten en los siguientes pasos:

- Identificación de la dirección IP y MAC del equipo.
- Identificación del puerto de salida.
- Identificación de la IP Pública que solicita el servicio y verificación del servicio.
- Dependiendo del servicio, se bloquea permanentemente la IP Pública.
- Verificación del consumo de ancho de banda por IP del usuario.
- Bloqueo de la IP y MAC del usuario si el problema persiste.

Para controlar el consumo del ancho de banda por usuarios, se ha implementado los Delays Pool en el servicio de Squid, asignando 1 Mbps como máximo para la navegación de los usuarios, en caso que exista disponibilidad de ancho de banda. Así mismo se ha implementado el control de ancho de banda por usuario en los equipos de la red inalámbrica.

En la Figura 3.9, se muestran los bloqueos de los puertos que no están abiertos para la red, mitigando las amenazas que busquen alguna salida hacia el internet.

Last 50 firewall log entries.Max(50)

Act	Time	If	Source	Destination	Proto
	Dec 28 13:24:21	LAN	172.16.0.21:36377	255.255.255.255:10001	UDP
	Dec 28 13:24:21	LAN	172.16.0.58:35897	255.255.255.255:10001	UDP
	Dec 28 13:24:21	LAN	172.16.0.62:43924	255.255.255.255:10001	UDP
	Dec 28 13:24:21	LAN	172.16.0.30:52732	255.255.255.255:10001	UDP
	Dec 28 13:24:21	LAN	172.16.0.74:38180	255.255.255.255:10001	UDP
	Dec 28 13:24:20	LAN	172.16.0.86:49628	255.255.255.255:10001	UDP
	Dec 28 13:24:20	LAN	172.16.0.12:54728	255.255.255.255:10001	UDP
	Dec 28 13:24:20	LAN	172.18.2.210:34758	74.125.141.188:443	TCP:FPA
	Dec 28 13:24:20	LAN	172.18.8.22:58931	52.17.126.99:5223	TCP:S
	Dec 28 13:24:20	LAN	172.16.0.85:45521	255.255.255.255:10001	UDP
	Dec 28 13:24:20	LAN	172.16.0.84:47615	255.255.255.255:10001	UDP
	Dec 28 13:24:20	LAN	172.16.0.65:34482	255.255.255.255:10001	UDP
	Dec 28 13:24:20	LAN	172.16.0.5:54119	255.255.255.255:10001	UDP
	Dec 28 13:24:20	◀ LAN	127.0.0.1:3128	172.18.14.110:51764	TCP:FPA
	Dec 28 13:24:20	LAN	172.18.9.85:52990	192.168.14.135:445	TCP:S
	Dec 28 13:24:20	LAN	172.18.9.85:52992	192.168.14.135:139	TCP:S
	Dec 28 13:24:20	LAN	172.16.0.81:59634	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.16.0.107:59149	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.16.0.77:47165	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.16.0.56:42879	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.16.0.46:34535	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.16.0.19:51713	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.18.9.85:137	172.18.15.255:137	UDP
	Dec 28 13:24:19	LAN	172.16.0.43:54919	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.18.8.236:58230	174.37.199.206:443	TCP:FPA
	Dec 28 13:24:19	LAN	172.18.2.12:36461	74.125.141.95:443	TCP:FA
	Dec 28 13:24:19	OPT1	192.168.6.24:138	192.168.7.255:138	UDP
	Dec 28 13:24:19	LAN	172.16.0.20:59047	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.16.0.36:50850	255.255.255.255:10001	UDP
	Dec 28 13:24:19	LAN	172.16.0.70:49897	255.255.255.255:10001	UDP

Figura 3.9 Bloque de puertos del Firewall – Proxy de la red Wireless.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La implementación ha tenido barreras en el ámbito de inversión, se ha ido escalando la inversión a través de las máximas autoridades de la Institución de Educación Superior.

2. La actual arquitectura de comunicaciones mejoró todos los servicios informáticos brindados por el Departamento de Sistemas, desde el acceso a las aplicaciones locales y hacia el internet.

3. El monitoreo de los equipos de red, ha ayudado a resolver los problemas de forma oportuna, y a identificar las causas más propensas a errores de energía eléctrica, sean en nodos de distribución y de acceso; también se han corregido problemas locales de energía eléctrica.

4. La separación de las subredes por Vlans, mejora el control y manejo del direccionamiento IP en cada subred, y a identificar a los posibles usuarios que quieran acceder a los servicios que no estén permitidos en la subred.

5. La arquitectura de seguridad a nivel de Firewall de Borde y de Accesos, ha ayudado a mantener un mejor control de los diferentes esquemas de accesos a los servicios informáticos, control de ancho de banda, control de puertos y mitigación de amenazas internas y externas.

6. La implementación de IDS/IPS Suricata exige un nivel de hardware de alto rendimiento, por lo que se procedió a colocar dos procesadores en los equipos de Firewall de Borde y Firewall-Proxy de la red Wireless, por la cantidad de througput generado en los dos equipos.

7. Suricata a nivel del Firewall de Borde es activado cuando se necesita realizar los respectivos monitoreos en la red DMZ y en las redes de accesos, debido al tiempo que lleva depurar los falsos positivos.

8. Suricata ayudó a controlar los problemas de saturación, por los diferentes problemas encontrados.

9. Se han implementado políticas de seguridad a nivel institucional, y aceptadas por las máximas autoridades; ayudando a un mejor control en puntos específicos.

10. Los usuarios de las redes de Oficinas, Docentes y Laboratorios, tienen conocimiento de las posibles amenazas informáticas internas y externas a nivel de seguridad.

RECOMENDACIONES

1. Es necesario realizar la revisión periódica de los logs de cada switch de la arquitectura de red, para verificar los posibles problemas que se puedan presentar a nivel de redes.

2. Realizar el respectivo Plan de Mantenimiento Anual de los equipos, a nivel de la arquitectura de red y de la arquitectura de seguridad de firewalls.

3. Es necesario crear el Plan de Contingencias de cada arquitectura, para mantener la continuidad de los servicios informáticos de la Institución de Educación Superior.

4. La capacitación del personal es un punto vital, para el control, monitoreo y solución de los problemas en las diferentes arquitecturas.

5. EL Firewall de Borde, actualmente funciona en el rendimiento adecuado para la red, por miras de crecimientos es necesaria la adquisición de un Firewall dedicado que contenga las soluciones de IDS/IPS.

BIBLIOGRAFÍA

[1] Williamson, Matt , pfSense 2 Cookbook, Biblioteca virtual Ebook Lilbrary http://reader.eblib.com/(S(md25p2iwe2xjssfflq1u1ulu))/Reader.aspx?p=950585&o=2458&u=605417&t=1450800936&h=D11AB0278B86E518164EC965C04C5A6303C155E4&s=40854007&ut=8337&pg=1&r=img&c=-1&pat=n&cms=-1&sd=2# , fecha de consulta diciembre 2015.

[2] Electric Sheep Fencing LLC, Pfsense, https://www.pfsense.org

[3] The Open Information Security Foundation, Suricata IDS/IPS, http://suricata-ids.org/ fecha de consulta diciembre 2015.

[4] David Zientara, Configuraciones de Pfsense, http://pfsensesetup.com/ , fecha de consulta diciembre 2015

[5] Paessler AG, PRTG Network Monitor, https://www.es.paessler.com/prtg/product-information.