ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN UNIFICADA DE AMENAZAS (UTM) PARA LA EMPRESA DE CRÉDITOS PALACIO DEL HOGAR"

TRABAJO DE TITULACIÓN

Previo a la obtención del título de**:**

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Ing. Guido Fabian Miguez Gómez

GUAYAQUIL – ECUADOR

AÑO

2017

AGRADECIMIENTO

A Dios Todopoderoso por haberme bendecido con esta carrera, y haberme permitido culminar con éxito en su infinita Misericordia.

A mi madre y abuela que gracias a Dios han formado parte de mi camino a cada meta de mi vida.

A mi esposa e hijos que Dios me ha regalado y que son la fuerza de apoyo que está a mi lado en todo momento demostrando su amor hacia mí.

A la MGS. Laura Ureta Arreaga Tutor de Tesis, por su colaboración y ayuda para la realización de este trabajo de Titulación.

DEDICATORIA

A Dios el Altísimo y Todopoderoso, a mi madre Gardenia Gómez, a mi esposa Marta Guastay, a mis hijos Sebastián, Nehemías y Natalia; y a todos los que estuvieron conmigo en todo momento.

TRIBUNAL DE SUSTENTACIÓN

_____

DIRECTOR MSIG/MSIA

ING. LENÍN FREIRE

_____

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MSIG. LAURA URETA ARREAGA

_____

MIEMBRO DEL TRIBUNAL

MSIG. RAFAEL BONILLA

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

_____

Ing. Guido Fabian Miguez Gómez

RESUMEN

El presente proyecto es desarrollado con el fin de dar una solución óptima a los problemas de Control de Seguridad de la Información existente dentro de la Infraestructura de Red de la empresa, propios de las actividades de la empresa de Créditos **"Palacio del Hogar"**, esto por la falta de un Sistema de Gestión Unificada de Amenazas, permitiendo tener un mejor control y monitoreo del tráfico de red tanto entrante como saliente, permitiendo al profesional encargado del DATACENTER tener una completa administración de los recursos.

La empresa de Créditos **"Palacio del Hogar"** posee cuatro sucursales que cuentan con enlaces de datos contratado a la empresa TELCONET, a excepción de las Sucursales Ubicadas en el cantón de Santa Elena y Libertad, junto con los dispositivos móviles asignados en el área de cobranzas y ventas, y quienes necesiten acceden por medio de internet, a estos el UTM a Implementar permite accesos más seguros por medio de enlaces VPN.

El software UTM que se utiliza es el **"Endian Firewall Community",** considerado un Software OpenSource que permite como base de configuración clasificar en 5 zonas bien marcadas a toda la red de la empresa, siendo estas:

- **Roja:** Internet y Sucursales con Enlace de Datos
- **Naranja:** Zona DMZ

- **Azul:** Zona Wifi y Otros (podría considerarse como otra zona DMZ)
- **Verde:** LAN – Intranet de la Empresa
- **VPN:** Red Privada Virtual para Sucursales Externas y Móviles.

Además, el software posee muchas características adicionales como las siguientes: Configuración de Host, Enrutamientos Avanzados, Servidor DHCP por Zonas, Motor de Antivirus, IPS, Monitoreo de Tráfico en Directo, Proxy, VPN entre otros.

La solución a implementar tiene su respectiva complejidad, pero los beneficios a obtener por parte de la empresa son considerables, en el control de tráfico de la red entrante como saliente, accesos VPN seguros, control de navegación por Proxy, conexiones más seguras, monitoreo de recursos, entre otros.

ÍNDICE GENERAL

ABREVIATURAS Y SÍMBOLOS

ACL	Access Control List
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
CNT	Corporación Nacional de Telecomunicaciones
CPU	Central Processor Unit
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DTE	Data Terminal Equipment
DVR	Digital Video Recorder
FTP	File Transfer Protocol
FXO	Foreign. eXchange Office
GB	Gigabyte
GE	GigaEthernet
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System

IPSec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Media Access Control
MB	Megabyte
NAT	Network Address Translator
NIC	Network Interface Card
NMAP	Network Mapper
NTOP	Network Top
NTP	Network Time Protocol
NVR	Network Video Recorder
PAC	Programa Asistente Contable
PC	Personal Computer
POP3	Post Office Protocol
PSK	Pre-shared Key
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAM	Random Access Memory
SATA	Serial ATA
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAM	Stupid Pointless Annoying Messages
SQL	Structured Query Language
SQLi	Structure Qwery Languaje Injection

SSl	Secure Sockets Layer
TCP	Transmission Control Protocol
TUN	Namely Network Tunnel
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTM	Unified Threat Management
VLAN	Virtual LAN
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WWW	World Wide Web
XSS	Cross Site Scripting

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad el manejo de información en las empresas cada vez es más importante, y paralelamente como lo menciona Bontupalli que en la última década las amenazas a la seguridad de las redes informáticas han aumentado dramáticamente [1], provocando esto grandes problemas con la continuidad del negocio, que se traduce en la afectación de la disponibilidad de los servicios; para afrontar estos problemas existen muchas medidas que se podrían tomar como por ejemplo: firewall, antivirus, accesos VPN, IPS, IDS, Certificados SSL, entre otros.

La Empresa de Créditos “Palacio del Hogar” es una Empresa de tipo Pyme en el Mercado Guayaquileño, que ha crecido paulatinamente logrando poseer 4 sucursales, 3 dentro de la ciudad y 1 en la provincia de Santa Elena. Su DATACENTER se encuentra ubicado en el edificio administrativo dentro de las bodegas de Parque California II. Su proveedor de Internet y de Enlace de Datos dentro de Guayaquil es la empresa TELCONET y en Santa Elena BRIGTELECON. Dentro de su infraestructura posee un Servidor de Virtualización ESXI, un Sistema Financiero, un Servidor DNS, un Servidor de Telefonía IP (Elastix), un Servidor VPN, un Servidor de Dominio, Cámaras de Seguridad y a futuro pretende implementar un Servidor de Correo Electrónico Institucional.

Debido al flujo de información y el tipo de actividad empresarial se realiza la Implementación de un sistema de Gestión Unificada de Amenazas (UTM), por medio del Software OpenSource “Endian Community” donde se realiza la configuración con 5 zonas en diferentes Redes y con tarjetas de Red GE independientes que son las siguientes:

- Roja (WAN)
- Naranja (DMZ)
- Azul (DMZ2- Video y Wifi)
- Verde (LAN)
- VPN

Se establece las reglas de entrada y salida tanto de Internet como entre zonas, con el fin de implantar un esquema de mayor seguridad a los servicios de la empresa. Se configura NAT Destino para su Sistema Financiero, Telefonía IP y Video, se establece los accesos VPN respectivos para las sucursales que requieran conectarse a la Oficina Principal, se direcciona todo el tráfico de Internet al Proxy que tiene el UTM, se activa el IPS y Otros Servicios de Seguridad que Ofrece “Endian Community” entre sus funcionalidades.

En esta solución existe escalabilidad que permite a la empresa seguir creciendo y no estar obligada a tener que cambiar la implementación a corto ni a mediano plazo, ya que el UTM permite realizar configuraciones que ayuden a nuevas actividades

como un control QoS, controles SMTP para Servidores de Correo, Proxy DNS, Proxy FTP entre otros.

Esta Implementación otorgará a la empresa mayor seguridad en los accesos a sus servicios, logrando controlar y monitorear el flujo de información todo dentro de su tráfico de red. Además, la solución permitirá la obtención de reportes de forma diaria, mensual o semanal acorde con las necesidades de la empresa.

CAPÍTULO 1

GENERALIDADES

1.1. ANTECEDENTES

La Empresa de Créditos “Palacio del Hogar” se dedica a la venta al por mayor y menor de líneas de productos para Hogar y Tecnología, está conformada por 4 sucursales y una matriz principal, ubicadas 3 dentro de la ciudad de Guayaquil junto con la matriz y 2 en la provincia de Santa Elena en la ciudad de Santa Elena y Libertad, la misma posee en su DATACENTER los siguiente Servicios:

- Servidor de Virtualización ESXI
- Elastix (Sistema de Telefonía IP)
- Sistema Financiero PAC
- Servidor de Dominio
- Servidor DNS
- Servidor VPN
- Cámaras de Seguridad.

Las sucursales que se encuentran dentro de la ciudad de Guayaquil, se conectan por medio de enlace de datos con el proveedor de servicios TELCONET incluyendo el Servicio de Internet con un ancho de banda de 1MB 1:1 por medio de fibra óptica, para la Sucursal de Santa Elena el ISP es BRIGTELECON con un ancho de banda de 5MB 1:1 por medio de radio enlace, y para la Sucursal de Libertad el ISP es Netlife con un ancho de banda de 10MB con partición 2:1 por medio de fibra óptica; estas últimas sucursales acceden a los servicios del Sistema Financiero y de Telefonía IP por medio de direcciones IP públicas entregadas por el ISP de Guayaquil. Las sucursales acceden a los Servicios de la Empresa sin esquemas de seguridad, no se mantiene hardware o software que impida el paso o al menos lo filtre, provocando así la existencia de un gran riesgo de seguridad de la información dentro de la empresa.

1.2. DESCRIPCIÓN DEL PROBLEMA

La Empresa Almacenes “Créditos Palacio del Hogar” se dedica a la venta al por mayor y menor de líneas de productos para hogar y tecnología, su Data Center no cuenta con un esquema de seguridad perimetral, que controle el tráfico de entrada y salida de datos de los servidores de la empresa. La empresa ha ido creciendo y los servicios que tiene que otorgar son mayores. Inclusive tiene proyectos de ventas con dispositivos móviles en diferentes sectores de la ciudad y la instalación de un servidor de correo electrónico propio. A continuación se detalla por categorías los problemas de la empresa.

1.2.1. SEGMENTACIÓN Y RESTRUCTURACIÓN DE RED

- Servidores en la misma Red que los Equipos Clientes.
- Equipos WIFI en Matriz donde se encuentran los servidores utilizan el mismo segmento de red, donde no tiene ningún control de tráfico más allá de las contraseñas que permite administrar dichos equipo.

1.2.2. CONTROL DE TRÁFICO

- Vulnerabilidad en puerto 80 que permitió el cambio de la contraseña administrador del Servidor Elastix.
- Denegación de Servicio en el sistema financiero WEB.
- Denegación de Servicio con servidor DNS.
- E-mail Spoofing utilizando el servidor Financiero hasta saturar Disco Duro.
- Falta de Control del Tráfico entrante y saliente de la Matriz entre sus diferentes sucursales incluyendo los dispositivos móviles.

1.2.3. CONTROL ACCESOS REMOTOS CON SUCURSALES

- Vulnerabilidad en las conexiones hacia el Servidor Financiero para las ventas Móviles.
- Vulnerabilidad de Acceso a Recursos de Red de la Empresa (Archivos Compartidos, Telefonía IP, Servidor Financiero, Directorio Activo, correo electrónico) por parte de sucursales.

1.2.4. MONITOREO

- Falta de Monitoreo del Tráfico de Red tanto entrante como saliente de la empresa.

1.2.5. SERVICIOS ADICIONALES DE CONTROL

- Falta de Control en las asignaciones DHCP dentro de la Matriz.
- Falta de Control de Antivirus en el tráfico de Red.
- Vulnerabilidad en los archivos compartidos entre las diferentes Sucursales.
- Mala administración del ancho de banda que posee la empresa.
- Trasmisión de Video entre Sucursales saturando el ancho de Banda.

1.3. SOLUCIÓN PROPUESTA

En el DATACENTER que se encuentra en la Matriz ubicada en la Bodega California se realizará la implementación de un sistema de Gestión Unificada de Amenazas (UTM), por medio del Software OpenSource “Endian Community” donde se realizará las siguientes configuraciones con el fin de solucionar los problemas detectados clasificándolas por categorías.

1.3.1. SEGMENTACIÓN Y RESTRUCTURACIÓN DE RED

Se crearán 5 zonas con diferentes Segmentos de red y con tarjetas de Red GE independientes que son las siguientes:

- Roja (WAN)
- Naranja (DMZ)

- Azul (DMZ2 – Video y WIFI)
- Verde (LAN)
- VPN

1.3.2. CONTROL DE TRÁFICO

- Redirección de Puertos/NAT Destino: traducción de IP pública a Privada con redirección de puertos específicos, para servicios internos de la empresa puedan ser accesibles desde internet con las seguridades necesarias, habilitando el acceso por un puerto específico a determinada dirección IP externa.
- NAT Fuente: para equipos específicos que necesiten ser traducidos desde una dirección ip interna hacia una ip pública.
- Tráfico Enrutado de Entrada: configuración de reglas para tráfico de entrada a las diferentes zonas de la red.
- Tráfico de Salida: configuración de reglas para tráfico saliente de las diferentes zonas de la red.
- Tráfico entre zonas: configuración de reglas de tráfico entre las diferentes zonas de la red.
- Tráfico VPN: configuración de reglas de tráfico para accesos VPN.
- Acceso al Sistema: configuración de reglas de acceso para la administración del sistema basado en Lista de Control de Accesos - ACL.

- Proxy HTTP:configuración del servicio, creación de Políticas de Acceso, autenticación de usuarios en caso de ser necesario y el filtrado de los sitios web.

1.3.3. CONTROL ACCESOS REMOTOS CON SUCURSALES

- Configuración de Accesos VPN para sucursales externas que no posean enlace de datos, con OPENVPN e IPSEC dependiendo la necesidad de la conexión.

1.3.4. MONITOREO

- Acceso SSH: para la administración remota bajo consola utilizando el puerto 22, previo el aseguramiento del acceso.
- Notificación de Eventos: con el fin de mantener al administrador de red siempre informado de actividades relevantes del UTM.
- Backups y Restore: con opción a realizar de forma cifrada con claves públicas.
- Prevención de Intrusos: Configuración de reglas de SNORT de forma diaria con opción a personalización.
- Monitoreo de Tráfico: opción para monitorear y analizar el tráfico por las diferentes zonas de la red de la empresa.
- Servidor SNMP: Protocolo Simple de Administración de Red para la interacción con los diferentes dispositivos de red que soporten dicho protocolo de la capa de aplicación.

- Registros, Informes y Otros: se pretende visualizar reportes e informes del sistema, firewall, servicios, proxy tanto en tiempo real como en archivos y registros históricos de Logs.

1.3.5. SERVICIOS ADICIONALES DE CONTROL

- Servicio DHCP: habilitación y asignación fija para la DMZ por MAC Address y LAN de forma automática.
- DNS Dinámico: en caso de existir equipos con esta necesidad.
- Motor Antivirus: configuración de antivirus CLAMAV.
- Capacitación SPAM: monitoreo y control de spam.
- Calidad de Servicio QoS: configuración de dispositivos, clases y reglas para la calidad de servicio de la red en caso de ser necesario.

Con esta implementación se logrará establecer la seguridad perimetral en la matriz de la empresa, y para las sucursales se establecerá accesos VPN, así como se controlará todo el tráfico entrante y saliente de la red. Adicionalmente, se elaborará la documentación de toda la implementación.

Para esta implementación se necesita un equipo computador con las siguientes características mínimas:

- CPU: Intel x86 compatible (1GHz minimum, Dual-core 2 GHz recomendado), including VIA, AMD Athlon, Athlon 64, Opteron, Intel Core 2 Duo, Xeon, Pentium and Celeron processors.

- RAM: 1 GB recomendado.
- Disco: 20 GB Mínimo.
- Tarjetas de Red: 4 GE

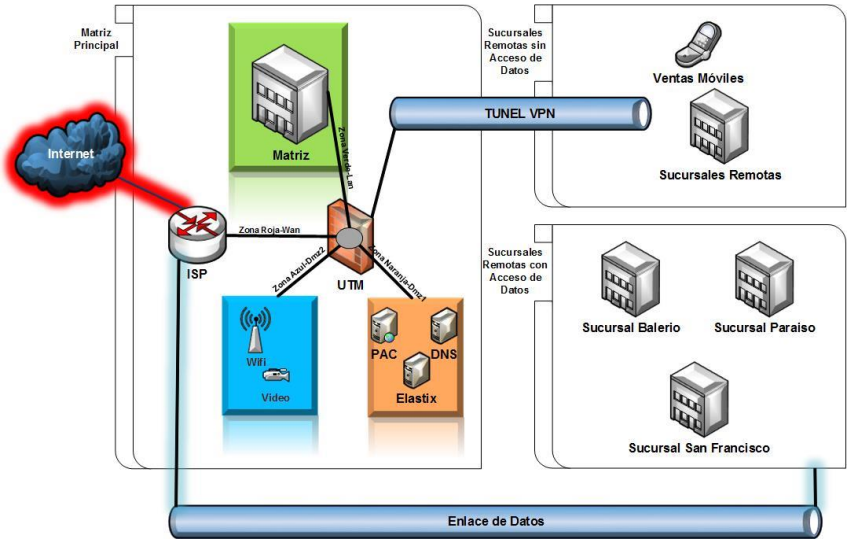


Figura 1.1 Diagrama de Implementación

1.4. OBJETIVO GENERAL

Implementar una solución integral de seguridad para la empresa de Créditos “Palacio del Hogar” a través de un Gestor Unificado de Amenazas (UTM).

1.5. OBJETIVOS ESPECÍFICOS

- Identificar los activos de información más relevantes y la topología de la red de datos con la que cuenta la empresa.
- Analizar y diseñar el plan de solución integral de seguridad (UTM) aplicable a la empresa seleccionada.
- Implementar la solución integral de seguridad (UTM) habilitando los siguientes componentes tales como: antivirus, anti-spam, firewall, filtros

web, IPS, VPN, Email-Security, Registro de Logs e informes según la necesidad requerida.

- Análisis de los resultados obtenidos y elaborar la documentación de la implementación.

1.6. METODOLOGÍA

La metodología a utilizar se detalla en la siguiente figura:

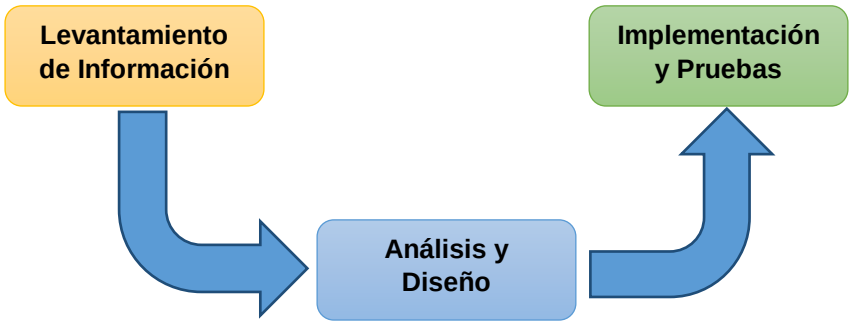


Figura 1.2 Metodología a Utilizar

1.6.1. LEVANTAMIENTO DE INFORMACIÓN

Comprende en realizar las siguientes tareas, observar la empresa y entrevistar al personal que interactúan con los diferentes Sistemas, el objetivo de esta fase es conocer con que equipos y servicios cuenta la empresa y cómo interactúan dentro de su red de datos, al final de esta fase se realizará la respectiva entrevista para la socialización con Gerencia General, para conocer sus puntos de vista y proceder de una forma más objetiva al análisis y diseño.

1.6.2. ANÁLISIS Y DISEÑO

En base al levantamiento de información obtenido se realiza un análisis minucioso, con el fin de minimizar y evitar inconvenientes técnicos futuros, una vez que se tiene dicha información, se procede al diseño de toda la configuración a realizar dentro de Palacio del Hogar, desde la topología de Red hasta los accesos de Usuarios VPN.

1.6.3. IMPLEMENTACIÓN Y PRUEBA

En base al diseño se realiza la implementación en el UTM Endian Community, plasmando la topología de red, las políticas, permisos de accesos, etc.; se configura los equipos tanto servidores como cliente en la nueva topología de red, y se proceden a ejecutar las pruebas de Acceso al UTM, entre Zonas, entre sucursales, por conexión VPN, Asignaciones de IP, Servicios Nateados, Reglas Aplicadas tanto en Firewall con en Proxy, entre otros.

CAPÍTULO 2

MARCO TEÓRICO

2.1. UTM

Según Kasperky Lab. la gestión unificada de amenazas, que comúnmente se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad, y por lo general un único producto de seguridad, que ofrece varias funciones de seguridad en un solo punto en la red. Un producto UTM generalmente incluye funciones como antivirus, anti-spyware, anti-spam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, network address translation) y compatibilidad para redes privadas virtuales (VPN, virtual private network). La solución se basa en la simplicidad, por lo que las organizaciones que puedan haber tenido proveedores o productos para cada tarea de seguridad por separado, los pueden tener todos centralizados en una sola solución, con el apoyo de un único equipo o segmento de TI, y que se administra, ejecuta y monitorea en una sola consola.

Los productos de gestión unificada de amenazas han ganado presencia en el sector debido a la aparición de amenazas combinadas, que son el resultado de la combinación de diferentes tipos de malware y ataques que apuntan a partes separadas de la red de forma simultánea. Puede ser difícil evitar estos tipos de ataques cuando se utilizan distintos productos y proveedores para cada tarea de seguridad específica, ya que cada aspecto tiene que administrarse y actualizarse de forma individual a fin de permanecer actualizado de cara a las últimas formas de malware y cibercrimen. A través de la creación de un único punto de defensa y el uso de una sola consola, las soluciones UTM facilitan en gran medida la tarea de tratar con amenazas variadas. [2]

2.2. SEGURIDADES CON UTM

Las seguridades de un Gestor Unificado de Amenazas va mucho más allá que un firewall en la red, ya que abarca muchos servicios adicionales que permite a las empresas concentrar su contingente y presupuesto en un solo punto, con esto permitiendo una mejor administración e inversión de recursos. Entre las funciones de seguridad tenemos las siguientes:

- **Monitoreo del Tráfico de Red en Tiempo Real:** mostrar la actividad de todos los host dentro de la red, permitiendo observar el consumo de ancho de banda, la interacción entre equipos, las conexiones entrantes como salientes, etc.

- **Balanceo y alta disponibilidad de enlaces de internet:** Distribuye la navegación para evitar saturaciones dentro de la red.
- **Calidad de Servicio (QoS):** la ITU expresa que es la totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio. [3]

- **Enrutamiento:** es un proceso que realiza un router para enviar paquetes a los diferentes destinos de la red por medio de sus direcciones IP.

- **Agregación de Enlaces:** Agregación de Enlaces según lo indica en su publicación la IEEE Computer Society, permite que uno o más enlaces a ser agrupadas juntas para formar un grupo de agregación, de tal manera que un cliente MAC puede tratar el Grupo de agregación de enlace como si se tratara de un único enlace . Con este fin, se especifica el establecimiento de DTE a DTE enlaces lógicos, que consiste en N instancias paralelas de dúplex completo de enlaces punto a punto que funcionan a la misma velocidad de datos. [4]

- **IPS:** equipo o software que contiene una base de datos con las amenazas informáticas y se actualiza de forma manual o automática.

- **DNS:** Servicio que permite relacionar los nombres de los host con sus respectivas direcciones ip dentro de un grupo de trabajo o dominio, generalmente usa el puerto TCP y UDP 53.

- **DHCP:** servicio que permite asignar direcciones ip de forma automática dependiendo el rango de la red que sea asignado.
- **NTP:** es un protocolo que usa el puerto UDP 123 y permite sincronizar los relojes de los sistemas informáticos.

- **Filtrado de Navegación Web:** este servicio permite crear políticas de acceso a diferentes sitios web.

- **NAT:** RFC 2663 – Network Address Translator, la traducción de direcciones de red es un método por el que las direcciones IP son mapeadas de un dominio de direcciones a otro, proporcionando enrutamiento transparente según P. Srisuresh y M. Holdrege. [5]

- **Protección antivirus y antispyware perimetral:** servicio que por internet se actualiza automáticamente con el fin de evitar que virus y spyware ingresen a la red de la empresa.

- **Cifrado de Correo Electrónico:** es un procedimiento por medio de algoritmos que permite cifrar los correos electrónicos.

- **Control de Aplicaciones:** de acuerdo al sitio de PandaSecurity el control de aplicaciones es una protección que te permite configurar qué programas de los instalados en tu equipo pueden ejecutarse o no. [6]

- **Antivirus de correo y protección Antispam:** servicio que permite filtrar spam y evitar que virus se propaguen por la red por medio de los correos electrónicos.

- **VPN:** corresponde a redes privadas virtuales, estas pueden ser por medio de protocolos como IPSec, OpenVPN, PPTP, L2TP.

- **Firewall:** como su traducción en español lo indica muro de fuego, que controla todo el tráfico entrante y saliente de una red.

2.3. TIPOS DE UTM

Según los servicios que disponen estos dispositivos podrían clasificarse en dos tipos específicos que son Hardware Appliances y, Software.

Existen diferentes compañías que los comercializan en el mercado tanto con licenciamiento como sin él (OpenSource), para tener una mejor idea de que UTMs son los mejores en el mercado nos basamos en el Cuadrante Mágico de Gartner [7], que nos muestra que los mejor ubicados son Fortinet, Check Point y Sophos.

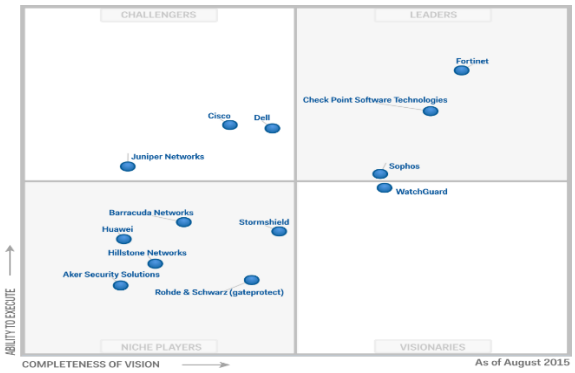


Figura 2.1 Cuadrante Mágico de Gartner de UTM

2.3.1. UTM POR HARDWARE APPLIANCES:

Son dispositivo rackeables y no rackeables que vienen con su respectivo Sistema Operativo dependiendo de la marca que se adquiera, y una infraestructura lista para su respectiva conexión y configuración dentro de la red de la empresa, no dependen de otro dispositivo para funcionar. Entre sus características principales están: Firewall Throughput, VPN Throughput y Cantidad Máxima de Usuarios.

Estos permiten medir su performance al momento de tener que tomar una decisión, dependiendo de la necesidad y presupuesto de la empresa; para esto TechTarget [8] nos muestra tablas comparativas con un detalle más específico de características y costos como se muestra en el Anexo “A” y “B”.

2.3.2. UTM POR SOFTWARE

Son sistemas operativos listos para ser instalados, existen con licencia y OpenSource, este software depende necesariamente de un hardware para poder funcionar, al referirnos a hardware se quiere decir que puede ir desde un potente servidor hasta una sencilla PC, siempre y cuando cumplan con las características mínimas que requiere el Software UTM, de este último depende el performance del mismo.

A continuación se ha tomado 3 UTM software de los múltiples existentes en el mercado para detallar sus respectivas características:

Sophos: ofrece el software UTM small Installer y UTM Manager. En la página de Sophos [9] se describe que para el uso comercial del software se debe necesariamente contratar una licencia, a excepción de la versión HOME que su licencia es free (libre), pero que permite usarlo solamente hasta 50 conexiones de forma personal más no comercial. Este UTM posee las siguientes características:

- Protección de Redes
- Protección de Redes Inalámbricas
- Protección Web
- Espacios seguros de Sandstorm
- Protección de Correo Electrónico
- Protección de Servidores Web

Zentyal: es un software licenciado que en base a su sitio web [10] su versión más reciente es la 4.2 y posee las siguientes características:

- Mail
- Basic Network & Firewall
- Dominio & Directorio
- Infraestructura

Endian: tomando como referencia su sitio web [11], este UTM posee una versión con licencia y una OpenSource conocida como Endian Firewall Community, con las siguientes características:

- Control de Aplicación

- Mail y Seguridad Web
- Acceso remoto Seguro
- Reporte y monitoreo de Red en Vivo
- Wifi y BYOD (Versión licenciada)
- Centralización de Administración y actualizaciones
- Firewall
- IPS
- Hotspot (Versión Licenciada)
- VPN
- Antivirus

2.4. HERRAMIENTA UTM A UTILIZAR EN LA IMPLEMENTACIÓN

La empresa de Créditos “Palacio del Hogar” no posee el presupuesto para licenciamiento de UTM, y la infraestructura es de una Pyme de menos de 40 trabajadores, el software a utilizar es el Endian Firewall Community, que es un UTM OpenSource que brinda varias utilidades que pueden ser implantadas y están acorde a las necesidades de la empresa. Este software ha sido implementado y probado en empresas como Dental Medical Corp., Plastiguayas, Casino de Tripulación de la Armada del Ecuador, y la Corporación SA ofreciendo excelentes resultados.

Hay dos factores principales que definen el haber seleccionado la solución Endian para la implementación como son el costo de licenciamiento y la operatividad; en cuanto a costos de licenciamiento encontramos que por

ejemplo Sophos es uno de los proveedores que comercializa su producto a precios accesibles, pero también tiene licenciamiento free que solo permite hasta 50 conexiones y para uso no comercial según indica en sus términos y condiciones [9], siendo una limitante al momento de implementar, otros en cambio otorgan licencias de prueba por 30 días, como por ejemplo Zentyal [10] también es un gran limitante a nivel empresarial; en relación a la operatividad de la herramienta Endian es completa y funcional, ya que su licencia free solo tiene limitado Hotspot y BYOD, los cuales, no son necesarios actualmente en la Empresa a implementar.

Endian posee diferentes soluciones tanto de hardware como de software, entre ellos Endian maneja software que incluye Sistema Operativo para equipos servidores o cualquier computador, protección de sistemas Virtualizados y servicio de seguridad en la nube [12].

2.4.1. ENDIAN UTM SOFTWARE PARA PC

Su SO permite convertir cualquier PC en un UTM, esta versión es ideal para aprovechar el hardware existente ya que la funcionalidad es idéntica al hardware Appliance de modo que no hay diferencias significativas.

Endian UTM Software posee la misma tecnología que se encuentra en sus dispositivos de hardware, tales como:

- Tecnología de Seguridad de Red.

- Calidad de Servicio y Gestión de Ancho de Banda
- Sistema de Prevención de Intrusos
- Hotspot
- VPN
- Seguridad de Correo
- Seguridad Web
- Notificaciones

2.4.2. UTM VIRTUAL: SOFTWARE DE SEGURIDAD Y PROTECCIÓN DE LA INFRAESTRUCTURA VIRTUAL

Con respecto a la protección y seguridad de infraestructuras virtualizadas, Endian asegura que la infraestructura virtual tanto interna como externa, permite integrarse con las diferentes plataformas virtuales, asegura toda la conectividad de red, entre otras cualidades adicionales.

Ventajas

- Soporte para cuatro plataformas virtuales: VMware, Xen, Hyper-V y KVM.
- Interfaz de usuario Intuitiva.
- Requisitos eficientes
- Escalabilidad
- Conjunto de herramientas para plataformas virtuales.

2.4.3. CASOS DE USO PARA UTM VIRTUAL

Protección de la Red Virtual: en su mayoría las redes virtuales no son muy diferentes a las redes físicas, por lo tanto los mismos principios de redes y seguridad pueden ser aplicados.

Seguridad de Conexión Externa: endian para ofrecer esta seguridad de conexión con el mundo exterior posee tecnologías como IPSec o SSL VPN (OpenVPN) y varias opciones adicionales de conectividad incluyendo red a red y acceso remoto individual.

Hosted/Servicios de Nube

Esta solución virtual puede mejorar cualquier servicio alojado desde simples servicios web y de correo electrónico, así como configuraciones complejas como Voip y VPN. El dispositivo virtual hace que la seguridad de su plataforma virtual sea sencilla, escalable y de mejor rentabilidad**.**

Todas las características del UTM Endian se muestran de forma detallada y específica en el Anexo “C”.

2.4.4. ENDIAN FIREWALL COMMUNITY

Listadas las características de Endian en lo que es Seguridad, a continuación se detalla todo lo concerniente a Endian Firewall Community, el UTM a implementar en la empresa Palacio del Hogar.

Esta herramienta OpenSource posee Seguridad Web y de Correo, Seguridad de acceso remoto, Monitoreo en vivo de red, administrador de eventos, Firewall, IPS, QoS, Antivirus, Multi-Wan (con Failover) y Reportes. A continuación se especifican a más detalle cada una de sus funcionalidades:

Sistema: Control Principal, Configuración de Red, Notificación de Eventos, Contraseñas, Consola Web, Acceso SSH, Configuración del Interfaz, Backups (Manuales y Programados), Apagar (Reiniciar y Apagar).

Estado: Estado del Sistema (Servicios, Memoria, uso de Disco, Tiempo de Servicio y Usuario, Módulos Cargados, Versión del Kernel), Estado de la Red (Interfaces, asignaciones dinámicas actuales, Estado de NIC, entradas de la tabla de enrutamiento, entradas de la tabla ARP), Gráficos del Sistema (CPU, Memoria, Swap, Disco Duro), Gráficos del Tráfico (Verde, Azul, Naranja y Rojo), Gráficos del Proxy, Conexiones, Conexiones VPN, Estadísticas de Correo SMTP, Lista de Correo.

Red: Editar Host, Enrutamiento (Estático y Política de enrutamiento), Interfaces (Editor de enlaces y VLANs).

Servicios: Servidor DHCP (Verde, Naranja y Azul), DNS Dinámico, Motor Antivirus ClamAV, Servidor de Fecha y Hora, Capacitación de Spam, Prevención de Intrusos (IPS, Reglas y Editor), Monitorización de Tráfico, Servidor SNMP, Calidad de Servicio (Dispositivos, clases y reglas).

Firewall: Redirección de Puertos (NAT destino, NAT fuente, Tráfico Enrutado de Entrada), Tráfico de Salida, Tráfico entre Zonas, Tráfico VPN, Acceso al Sistema, Diagramas de Firewall.

Proxy: HTTP (Configuración, Política de Acceso, Autenticación, Filtrado Web, Replicar Active Directory, Proxy HTTPS), POP3 (Configuración y filtro de correo no deseado), FTP (Proxys), SMTP (Configuración, Listas Negras y Blancas, Dominios de Entrada, Enrutamiento de Dominio, Enrutamiento de Correo, Avanzado), DNS (Proxy DNS, Enrutamiento de DNS, Anti-spyware)

VPN: Servidor OpenVPN, Cliente OpenVPN, IPsec, Autenticación, Certificados (Certificados, autoridad de Certificado, Certificados revocados, Lista de revocación de Certificados).

Registros e Informes: Registros en Tiempo Real, Resumen, Sistema, Servicio (IPS, OpenVPN, ClamAV), firewall, Proxy (HTTP, Informe HTTP y SMTP), Configuración, Marcas de Tiempo de Confianza.

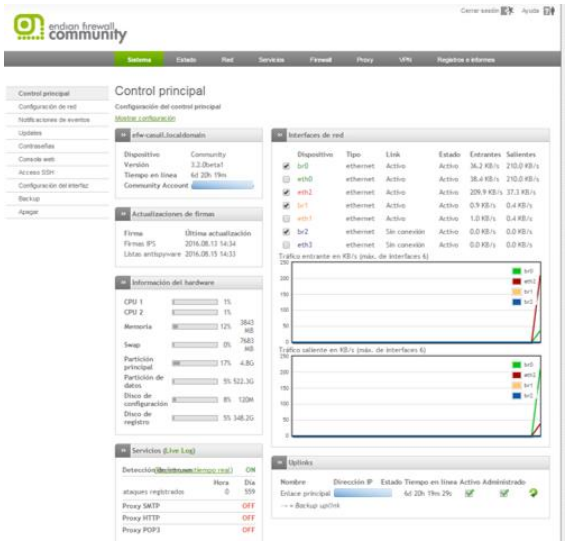


Figura 2.2 Endian Firewall Community

2.5. RIESGOS DE NO POSEER SEGURIDAD EN EMPRESAS

Una empresa que no tiene ningún tipo de seguridad implementada se encuentra más expuesta y vulnerable a cualquier tipo de ataque informático, existen muchos en la actualidad, pero se enlistan los más comunes a continuación:

Ataque por Inyección: más conocido como SQLi (Structure Qwery Languaje Injection) según el sitio web de Hostdime [13], es una técnica que permite modificar una cadena de consulta SQL, con el fin de obtener acceso a información de una Base de Datos a través de sus tablas, este es uno de los ataques más sencillos de ejecutar ya que solo necesita una pc y conocimiento básico de SQL.

DDoS: la denegación de Servicios (DoS) o denegación de Servicios Distribuidos (DDoS) según el sitio web de Hostdime [13] son las técnicas más

comúnmente usadas para atacar el funcionamiento de un servidor web. Consiste en inundar de paquetes con requerimientos externos un servicio logrando que no esté disponible para los verdaderos usuarios, para esto utilizan equipos externos de forma distribuida que envían peticiones a un determinado servidor hasta sobrecargarlo, y evitar que desempeñe su trabajo normal. Los ataques DDoS tienen 3 principales variedades como lo menciona HostDime en su blog: Los ataques de volumen, donde el ataque intenta desbordar el ancho de banda de un sitio específico.

- Los ataques de protocolo, donde los paquetes intentan consumir servicios o recursos de la red.
- Ataques a Aplicaciones, donde las peticiones se hacen con la intención de explotar el servidor web, mediante la capa de aplicación.

Fuerza Bruta: como indica el sitio web de Hostdime [13] está técnica básicamente intenta romper el acceso a un servidor aplicando combinaciones de posibles usuario y claves, por lo general estos ataques buscan contraseñas débiles para hacerse de la información, siendo recomendable usar contraseñas mucho más complejas, como por ejemplo: utilizar mínimo 8 caracteres entre mayúsculas, minúsculas, números y caracteres especiales.

Cross Site Scripting (XSS): Ignacio Pérez en el sitio web welivesecurity [14] publica que esta vulnerabilidad en si explota la confianza que un usuario tiene en un sitio en particular. Este tipo de vulnerabilidad puede ser de forma reflejada o de forma almacenada.

Forma Reflejada: Consiste en modificar valores que la aplicación web usa para pasar variables entre dos páginas. Un clásico ejemplo de esto es hacer que a través de un buscador se ejecute un mensaje de alerta en JavaScript. Con XSS reflejado, el atacante podría robar las cookies para luego robar la identidad, pero para esto, debe lograr que su víctima ejecute un determinado comando dentro de su dirección web.

Para esto, los cibercriminales suelen enviar correos engañosos para que sus víctimas hagan clic en un enlace disfrazado y así se produzca el robo.

Forma Almacenada: Consiste en insertar código HTML (programación web) peligroso en sitios que lo permitan; de esta forma quedará visible a los usuarios que ingresen en el sitio modificado.

DNS Spoofing: es un método para alterar las direcciones de los servidores DNS, con el fin de obtener información que sea ingresada por parte de la víctima.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1. DIAGRAMA DE RED DE LA MATRIZ Y SUCURSALES

Una vez dada las facilidades por parte de La Empresa de Créditos “Palacio del Hogar”, considerando que el Implementador del UTM, brinda servicios profesionales dentro de la empresa, se obtuvo información detallada técnicamente. Créditos “Palacio del Hogar” posee 1 Matriz, 3 sucursales dentro de la ciudad de Guayaquil, 1 en la ciudad de Santa Elena, 1 en la ciudad de Libertad y Dispositivos móviles que se conectan por medio de un plan de datos de MOVISTAR desde cualquier punto donde haya cobertura, la forma que se conectan entre sí dentro de Guayaquil para operar es por medio de un enlace de datos contratado a la empresa TELCONET, y para la Sucursal de Provincia se enlaza por medio de las IP Públicas que existen en la matriz. El servicio de Internet para Guayaquil es de 1MB Dedicado, de 5MB para Santa Elena 4:1, y de 10MB 2:1 para Libertad.

En las sucursales locales existen subredes [1] configuradas para distribuir el tráfico de video, telefonía y usuarios. A continuación se presenta el Diagrama de Red de Cada Sucursal.

Matriz Principal:

Ubicado en el Km. 12 de la vía a Daule, las redes que utiliza esta sucursal son: 192.168.0.0/24 que es el rango privado y un pool de 4 direcciones IP que en este trabajo se representa como **"A"**, **"B"**, **"C"** y **"D"** [2] que corresponde al rango público. La topología de red que usa es estrella, en esta sucursal se encuentra el DATACENTER con sus diferentes servicios.

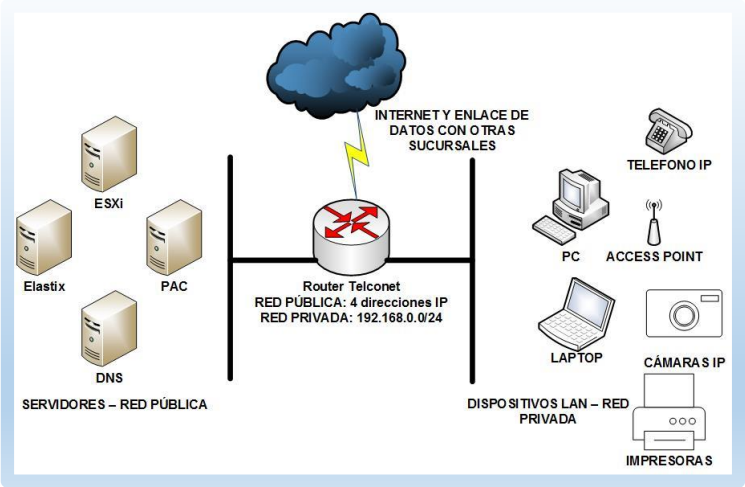


Figura 3.1 Diagrama de Red Matriz Principal

Sucursal Balerio:

Ubicado en Coop. Nueva Prosperina Solar 3, las redes que utiliza esta sucursal son: 192.168.1.0/24, 192.168.6.0/28, 192.168.7.0/28 y 192.168.8.0/28. La topología de red que usa es tipo estrella, y para acceder a

[1] Las direcciones IP privadas utilizadas en este trabajo son diferentes a las implementadas en la empresa por seguridad y buena práctica profesional.

[2] Por motivos de seguridad y buena práctica profesional las direcciones ip públicas reales de la empresa se representan con las letras A, B, C, D para la Matriz, con las letras "X", "Y" para la sucursal de Santa Elena y Libertad respectivamente; y con las letra "Z" para el NVR externo a la empresa.

la matriz y demás sucursales usa un enlace de datos contratado a TELCONET. Solamente existen equipos asignados a la red 192.168.1.0/24.

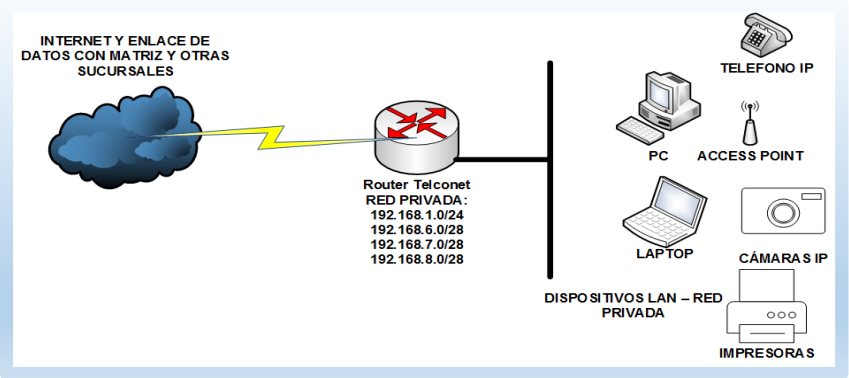


Figura 3.2 Diagrama de Red Sucursal Balerio

Sucursal Paraíso:

Ubicado en Flor de Bastión Calle 24 diagonal a Supermercado TIA, las redes que utiliza esta sucursal son: 192.168.11.0/24, 192.168.13.0/28, 192.168.14.0/28 y 192.168.15.0/28. La topología de red que usa es tipo estrella, y para acceder a la matriz y demás sucursales usa un enlace de datos contratado a TELCONET. La red 192.168.11.0/24 es usado para los computadores de trabajo y otros dispositivos adicionales. El sistema inalámbrico y de video se encuentra en la red 192.168.13.0/28 que solamente están utilizando 4 IP entre el dispositivo inalámbrico, el NVR y las cámaras IP. En esta sucursal hay que considerar que se encuentra el Gateway de voz que se enlaza con la central IP, la dirección IP asignada a este equipo es la 192.168.14.2., y los dos teléfonos IP asignados a esta sucursal que solo utilizan dos IP del rango de la red 192.168.14.0/28. La red 192.168.15.0/28 no está en uso.

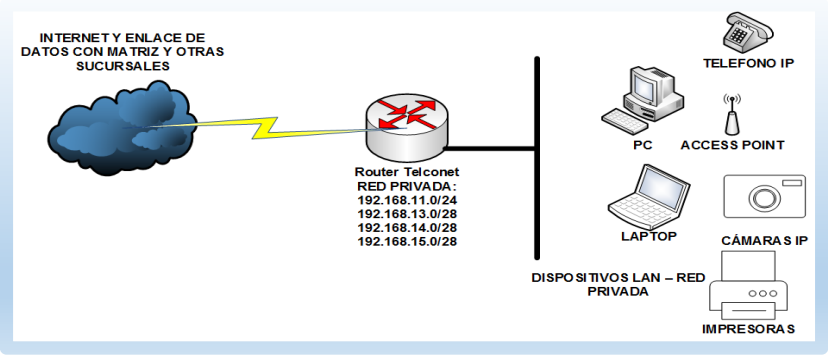


Figura 3.3 Diagrama de Red Sucursal Paraíso

Sucursal San Francisco:

Ubicado en San Francisco Av. 57 Diagonal a UPC, las redes que utiliza esta sucursal son: 192.168.12.0/24, 192.168.16.0/28, 192.168.17.0/28 y 192.168.18.0/28. La topología de red que usa es tipo estrella, y para acceder a la matriz y demás sucursales usa un enlace de datos contratado a TELCONET. La red 192.168.12.0/24 es usada para los computadores y otros dispositivos adicionales. La red 192.168.16.0/28 está asignada al sistema inalámbrico Wifi y de video utilizando solamente 5 IP. La red 192.168.17.0/28 es usado para la telefonía IP que se encuentra habilitado para dos teléfonos IP.

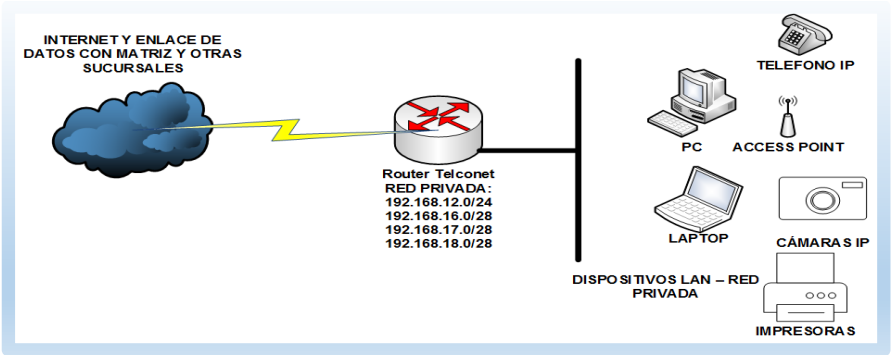


Figura 3.4 Diagrama de Red Sucursal San Francisco

Sucursal Santa Elena:

Esta sucursal se encuentra fuera de la Provincia del Guayas, ubicada en Colonche y Sucre Esquina – Provincia de Santa Elena, la Ip Pública fija que en este documento se la identificará como **"X"**, y las redes privadas que utiliza esta sucursal son: 192.168.88.0/24, 192.168.89.0/28 y 192.168.90.0/28. La topología de red que usa es tipo estrella, y para acceder a la matriz y demás sucursales usa las ip publicas asignadas a los diferentes servicios que se encuentran en el DATACENTER de la empresa. La red 192.168.88.0/24 es usado para los equipos de computación y otros. La red 192.168.89.0/28 es usado solamente por el DVR. La red 192.168.90.0/28 es usado para la conexión Inalámbrica de la sucursal.

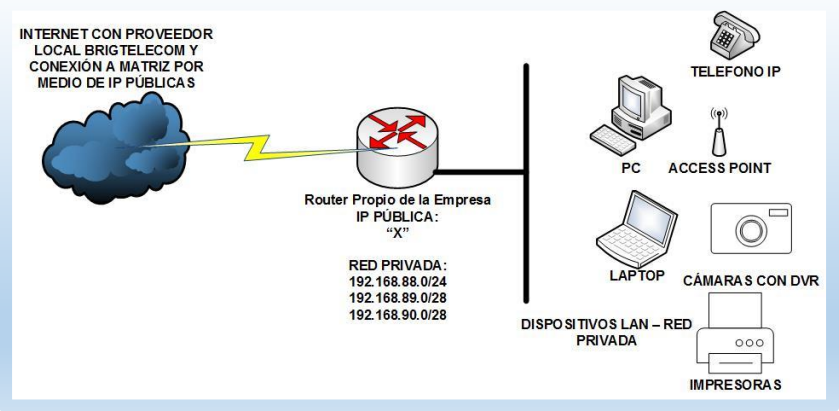


Figura 3.5 Diagrama de Red de Sucursal Santa Elena

Sucursal Libertad:

Esta sucursal se encuentra fuera de la Provincia del Guayas, ubicada en diagonal a Mercado Municipal de la ciudad – Provincia de Santa Elena, la ip pública fija dada por el proveedor que este documento se identificará como **"Y"**, la red privada que utiliza esta sucursal es la 172.16.30.0/24. La topología

de red que usa es tipo estrella, y para acceder a la matriz y demás sucursales usa las ip publicas asignadas a los diferentes servicios que se encuentran en el DATACENTER de la empresa. La red 172.16.30.1/24 es usado por todos los equipos de la red sin segmentación.

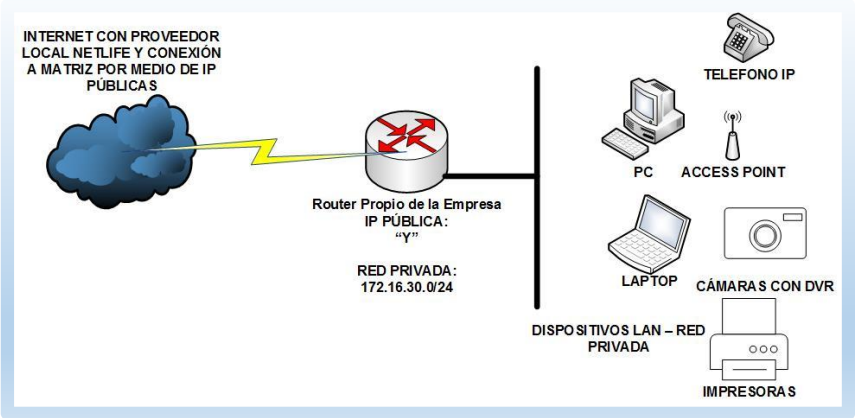


Figura 3.6 Diagrama de Red de Sucursal Libertad

3.2. SISTEMAS DE LA EMPRESA, SUS APLICACIONES Y SITIOS WEB PERMITIDOS EN LA EMPRESA.

Por su actividad comercial la empresa posee Sistemas de Información que soportan sus operaciones diarias. A continuación se detalla cada uno de ellos:

Sistema Financiero (PAC): este sistema tiene asignado para su acceso tanto desde la Intranet como del Internet la IP pública A. Este sistema maneja su propio lineamiento de perfiles por medio de credenciales con su respectivo usuario y clave. Las impresoras se encuentran ligadas a este sistema por medio del servicio cups, y la única forma que impriman tanto los recibos como las facturas, es compartiendo cada impresora en la red de cada sucursal y luego registrándola por medio de servicios samba en el Servidor Principal que

tiene instalado la versión de Linux Centos 5.11, dentro de la ciudad de Guayaquil no existe problemas al momento de realizar esta configuración por medio de ip privada ya que posee el enlace de datos por parte del ISP, en cambio en Santa Elena tienen que acceder por medio de una ip publica que se contrató con el ISP BRIDGETELCOM. El equipo servidor donde se ejecuta corre esta aplicación es un servidor HP Proliant ML310 G7 con un procesador Intel Xeon E3-1220 3.10GHz, memoria 12GB DDR3 y un RAID 1 de dos discos de 1TB SATA.

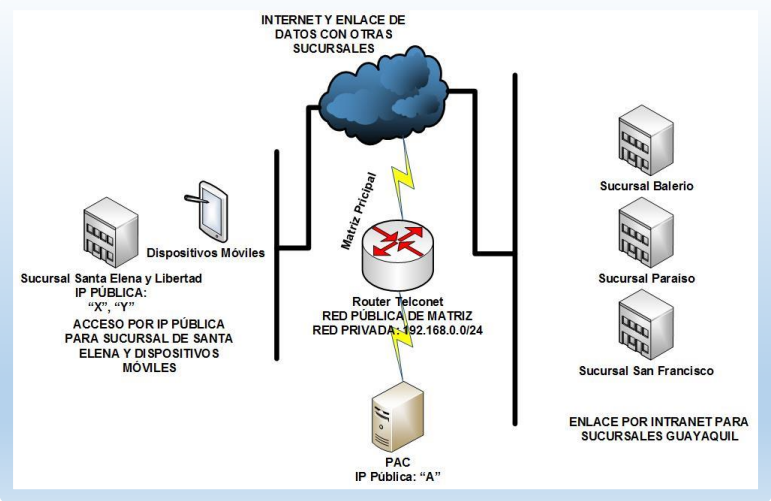


Figura 3.7 Diagrama de Conexión a Sistema Financiero - PAC

Sistema VMware ESXi 5.1: este sistema está instalado sobre un Servidor HP Proliant ML310 G7 con un procesador Intel Xeon E3-1220 3.10GHz, memoria 8GB DDR3 y un RAID 1 de dos discos de 1TB SATA, este software permite instalar sistemas operativos Virtualizados, al momento se encuentra instalado para Telefonía IP Elastix 2.5 y Servidor DNS, Dominio y Directorio Activo en Windows Server 2008 R2. La Ip asignada a este servidor es la IP Privada

192.168.0.2 y se encuentra en el DATACENTER ubicado en la matriz principal.

Elastix 2.5: este sistema operativo es utilizado para servicios de telefonía IP, se encuentra virtualizado sobre ESXi5.1, los recursos asignados son 2GB de Memoria RAM y 200GB de Disco Duro, la IP Pública Asignada es la B, Elastix interactúa con tres Gateway marca Grandstream para las líneas PSTN, y teléfonos IP de la misma Marca. Los Gateway se encuentran distribuidos de la siguiente manera:

- Grandstream GXW - 4108 con la IP 192.168.14.2 en la sucursal de Paraíso, a este equipo se conectan en los puertos FXO líneas de CNT y movistar en el caso de bases celulares.
- Grandstream HT-502 con la ip 192.168.0.11 en la matriz, a este equipo se conecta la PSTN que viene de Garita Principal de Seguridad.
- Grandstream HT- 502 con la ip 192.168.0.12 en la matriz, a este equipo se conectan una línea de CNT.

Servidor DNS, Dominio y Directorio Activo: estos sistemas se encuentran en servidores virtualizados en ESXi 5.1, la ip privada asignada es la 192.168.0.5, los recursos asignados a estos servicios son 2GB de Memoria RAM y 500GB de Disco Duro. En este servidor también comparten archivos que las diferentes sucursales acceden, en este equipo se encuentra creado el dominio Palacio.com, donde se registran solamente los clientes con enlace de

datos dado por el ISP Utilizando el Directorio Activo para el registro de Computadores y usuarios.

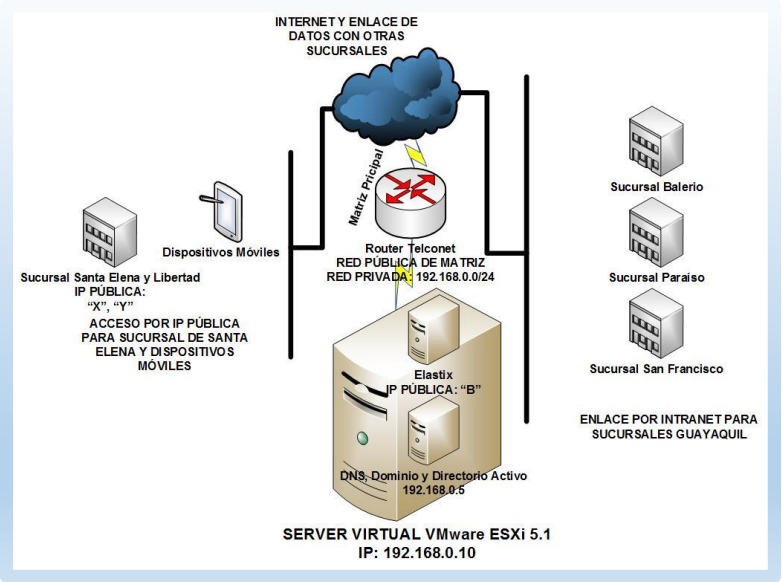


Figura 3.8 Diagrama de Conexión a Sistemas Virtualizados

Aplicación para Registro de Asistencia: este sistema está instalado en el computador del Jefe de Recursos Humanos con la ip 192.168.0.27, en las diferentes sucursales se encuentra instalado un dispositivo de registro de Huellas Digitales, configurado dentro de cada red respectivamente, por medio del enlace de datos del ISP las sucursales locales acceden de forma privada a estos dispositivos, a diferencia de la sucursal de Santa Elena que accede por medio de una IP pública asignada al router de dicha sucursal.

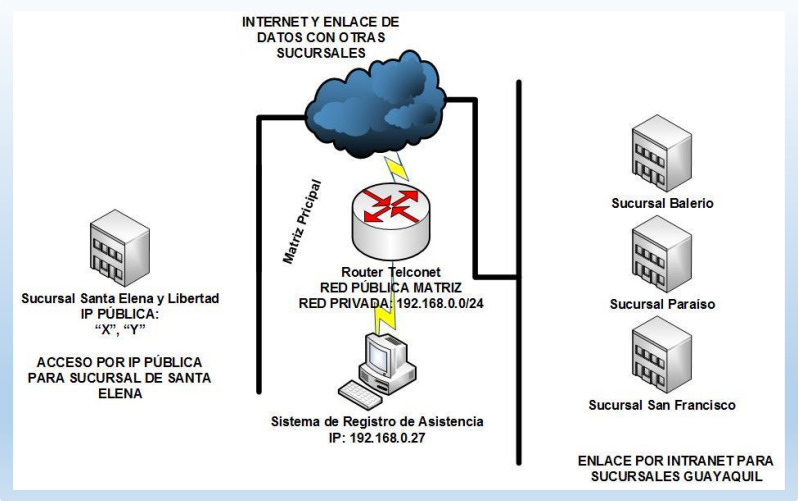


Figura 3.9 Diagrama de Conexión para Registro de Asistencia

Sistemas de Cámaras de Seguridad: este sistema está instalado en un computador ubicado en el DATACENTER con el objetivo de visualizar las Cámaras IP de las Sucursales en una pantalla de 32 Pulgadas y solo grabar el video de la matriz, ya que en cada de una de ellas tienen sus respectivos dispositivos NVR y DVR, la ip asignada a este equipo es la 192.168.0.15., para la visualización se utiliza el software Security Monitor Pro para las cámaras Dlink y Hikvision 4200 para el DVR ubicado en Santa Elena, a este último se accede por medio de la IP Publica representada con la letra **"X"**.

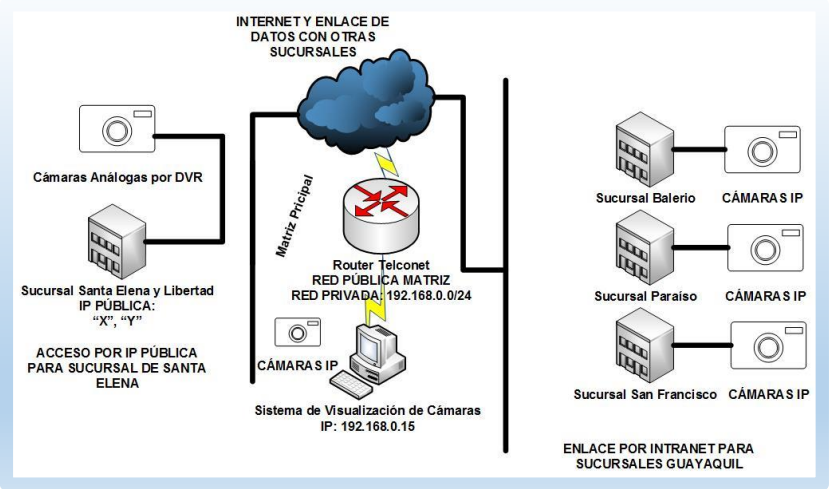


Figura 3.10 Diagrama de Conexión para Cámaras de Seguridad

Servidor VPN: cuentan con un servidor VPN bajo Untangle pero al momento no está en uso ya que los accesos por parte de los equipos de Santa Elena, Libertad y los Dispositivos Móviles los hacen directamente por las IP públicas asignados a cada Servicio. Pero en este equipo se conectaban diferentes usuarios entre ellos el Gerente y sus colaboradores el Ing. Cristian Apunte, la Srta. Ana Lucia Juela, el Ing. Efraín Barrera de la Empresa PROVEDATOS Proveedora del Software Financiero, y el Eco. Humberto Mendoza.

Servidor de Correo Electrónico: al momento solamente está en proyecto su implementación bajo el Sistema Operativo de Zimbra.

Servicio Web implementado por EQUIFAX: este sistema está instalado en el Servidor del Sistema Financiero como servicio adicional, ya que depende directamente de los datos existentes en el PAC para realizar el análisis crediticio automático de los clientes de la Empresa.

Sitios WEB Permitidos en la Empresa: los sitios WEB que son de importancia para la empresa Créditos Palacio del Hogar según la entrevista a usuarios de la empresa como se muestra en el Anexo “D” son los siguientes:

- Sitios Estatales como SRI, Ministerio de Trabajo, Registro Civil, Seguro Social entre otros.
- Proveedores de la Empresa incluido sitios de facturación electrónica como CARTIMEX, MAVESA, TECNOMEGA, COMPUMICRO, CHAIDE&CHAIDE entre otros.
- Sitios Administración y Manejo de Correo Institucional, Hosting, etc.
- Sitios de Consulta e Interés General como Noticieros, mercados en línea, etc.
- Redes Sociales (Facebook, Twitter, YouTube, Instagram) solamente a gerencia y el área de Diseño Gráfico y Publicidad Web.
- Servicios de Nube de Hotmail, Google, Dropbox, MyCloud, iCloud, etc.

3.3. ACCESOS ESPECIALES PARA USUARIOS DE LA EMPRESA.

Por medio de una entrevista realizada al gerente General como se muestra en el Anexo “E”, se detalla los permisos especiales solicitados para la empresa:

Matriz.

- Las sucursales y matriz pueden acceder exclusivamente a los siguientes servicios: PAC, Servidor de Telefonía IP y Servidor de Archivos Compartidos y DNS.

- El administrador de la red tendrá acceso a toda la red sin excepción por temas de soporte, esta regla deberá ser habilitada solamente si es necesaria, mientras tanto debe estar deshabilitada.
- Todos los Usuarios de la empresa deben ser controlados en la navegación en Internet.
- El jefe de recursos humanos debe tener acceso a los equipos biométricos de todas las sucursales para obtener los reportes.
- Salida a Internet sin restricción para el Gerente General, al contador, a la encargada de Marketing y Ventas, al administrador de la Red, y sus respectivos dispositivos.
- Las cámaras IP deben ser monitoreadas por la chica encargada de Ventas, debe tener un acceso en su PC.
- Nadie puede tener acceso a los equipos de sucursales a excepción de la persona encargada de la administración de la red
- La empresa EQUIFAX y Provedatos debe acceder para pruebas del Sistema que ellos están instalando en el servidor PAC.
- Debe existir en la matriz un dispositivo inalámbrico que permita la salida a internet para reuniones de gerencia con proveedores y personal externo.
- El Gerente debe poder ver las cámaras IP desde su IPhone.
- El Gerente debe poder Visualizar Reportes de telefonía desde su IPhone.

Sucursales por Enlace de Datos

- Navegación controlada de internet para todos los usuarios.

- Salida libre de Internet a Celular que hace cobros con tarjeta de Crédito con el sistema Data móvil.
- Permiso de Navegación de WhatsApp.

Accesos Remotos

- Acceso solo al sistema financiero PAC con los respectivos permisos para imprimir.
- La persona encargada de soporte del sistema financiero PAC solo debe tener acceso a este servicio.
- La sucursal de Santa Elena debe poder acceder al PAC también por IP Pública.
- Reglas que no hayan sido contempladas deben estar bloqueadas.

3.4. POLÍTICAS DE SEGURIDAD EN LA EMPRESA.

La empresa cuenta con las siguientes políticas de seguridad:

Seguridad Informática:

- Cada trabajador tiene asignado un equipo de cómputo con su respectivo usuario y contraseña.
- Existe un encargado en el matriz de receptar las novedades técnicas suscitados en cada sucursal, y luego notificar al área de sistemas.
- Está prohibido instalar programas en las computadoras de la empresa.
- Todo el personal administrativo cuenta con un correo electrónico institucional y puede usarlo dentro y fuera de la empresa.

- Todo usuario nuevo que ingresa debe registrar su huella digital en los dispositivos biométricos.
- A todo usuario que deja de laborar en la empresa, se le retira los permisos de acceso a correo y a todos los sistemas.

Seguridad de la Información:

- Diariamente se realizan Backups automáticos del sistema financiero.
- Semanalmente se realiza un respaldo manual del Sistema Financiero.
- Todos los accesos a los programas principales están restringidos por medio de usuario y contraseña.
- Los usuarios tiene prohibido divulgar sus credenciales de acceso con los demás usuarios.
- El cambio de contraseñas de los usuarios se los realiza después de determinado tiempo, esto lo administra el Servidor de Dominio de Windows.
- A todos los equipos se realiza una revisión de virus por lo menos cada mes.
- Los antivirus se actualizan de forma automática al conectarse a internet.

Mantenimiento y Correcto Uso de la Infraestructura:

- Todos los Sistemas Operativos de Windows deberán estar actualizados con los últimos Update y parches de seguridad.
- Todos los equipos deberán estar conectados a un regulador de voltaje o UPS.
- Cuando exista cortes de poder el encargado del DATACENTER debe apagarlos en menos de 10 minutos que dura la batería del UPS.

- Cada seis meses se revisará el funcionamiento de la red con el fin de detectar algún desperfecto o prevenir los mismos.
- Cada Seis meses se realizará limpieza de los equipos de todas las sucursales y matriz.

3.5. LEVANTAMIENTO DE ACTIVOS DE LA EMPRESA

En esta sección se procede a enlistar los activos informáticos que existen dentro de la empresa, que permiten tomar decisiones al momento de la implementación.

Matriz Principal:

Tabla 1 Equipos dentro del DATACENTER

Cant.	Tipo de Equipo	Observaciones Importantes	Estado
2	Servidor	HP Proliant ML310e G7	Activo
1	Desktop	Intel Pentium Dual Core E5500, memoria 2GB, Disco Duro de 500GB SATA	Inactivo
1	Switch	Dlink con 24 puertos no administrable	Activo
1	Switch	Cisco Administrable con 8 puertos	Activo
1	Access Point	Dlink	Activo
1	Desktop	Intel Pentium Dual Core E5500, memoria 2GB, Disco Duro de 1TB SATA funciona de NVR local	Activo

Son 31 los equipos que usan los usuarios dentro de esta sucursal y que influencian en el tráfico de red, como se detalla a continuación:

Tabla 2 Equipos de Matriz

Cantidad	Tipo de Equipo	Observaciones
3	Laptop	Usadas por Gerencia.
8	Pc de Escritorio	Usadas por los usuarios Administrativos, contables y otros.
9	Teléfonos IP	Usadas por los usuarios Administrativos, contables y otros.
4	Cámaras IP	Ubicadas en toda el área
3	Impresoras	Ubicadas en diferentes áreas de las cuales dos son de red
2	Dispositivos Inalámbricos	Utilizados para enlazar las cámaras IP.
1	Equipo Biométrico	Para el Registro de Asistencia
1	Gateway de Voz	Para enlazar Garita Principal con Teléfonos IP.

Sucursal Balerio:

Son 13 los equipos que usan los usuarios dentro de esta sucursal y que influencian en el tráfico de red, como se detalla a continuación:

Tabla 3 Equipos de Sucursal Balerio

Cantidad	Tipo de Equipo	Observaciones
3	Pc de Escritorio	Distribuidas entre caja, administración y ventas.
2	Teléfonos IP	Dos fijos
4	Cámaras IP	Ubicadas en toda el área
1	Impresora	Para toda el área
2	Dispositivos Inalámbricos	Utilizados para enlazar las cámaras IP.
1	Equipo Biométrico	Para el Registro de Asistencia
1	NVR	Utilizado para la grabación de Video
1	Switch	De 8 puertos Poe y Administrable.

Sucursal Paraíso:

Son 13 los equipos que usan los usuarios dentro de esta sucursal y que influencian en el tráfico de red, como se detalla a continuación:

Tabla 4 Equipos de Sucursal Paraíso

Cantidad	Tipo de Equipo	Observaciones
3	Pc de Escritorio	Distribuidas entre caja, administración y ventas.
2	Teléfonos IP	Uno fijo y otro inalámbrico
2	Cámaras IP	Ubicadas en toda el área
1	Impresora	Para toda el área
1	Dispositivo Inalámbrico	Utilizados para enlazar las cámaras IP.
1	Equipo Biométrico	Para el Registro de Asistencia
1	Gateway de Voz	En este dispositivo enlazado con la central IP de Elastix se conectan las líneas de CNT y Bases Celulares para la distribución en toda la empresa
1	NVR	Utilizado para la Grabación de video
1	Switch	8 puertos Administrable

Sucursal San Francisco:

Son 13 los equipos que usan los usuarios dentro de esta sucursal y que influencian en el tráfico de red, como se detalla a continuación:

Tabla 5 Equipos de Sucursal San Francisco

Cantidad	Tipo de Equipo	Observaciones
3	Pc de Escritorio	Distribuidas entre caja, administración y ventas.
2	Teléfonos IP	Los dos fijos
3	Cámaras IP	Ubicadas en toda el área
1	Impresora	Para toda el área
1	Dispositivo Inalámbrico	Utilizados para enlazar las cámaras IP.
1	Equipo Biométrico	Para el Registro de Asistencia
1	NVR	Utilizado para la Grabación de video
1	Switch	8 puertos Administrable

Sucursal Santa Elena:

Son 9 los equipos que usan los usuarios dentro de esta sucursal y que influencian en el tráfico de red, como se detalla a continuación:

Tabla 6 Equipos de Sucursal Santa Elena

Cantidad	Tipo de Equipo	Observaciones
1	Laptop	Para Ventas
2	Pc de Escritorio	Distribuidas entre caja y ventas.
1	Teléfonos IP	Fijo
1	DVR	Conectado con 3 cámaras
1	Impresora	Para toda el área
1	Dispositivo Inalámbrico	Para uso interno
1	Equipo Biométrico	Para el Registro de Asistencia
1	Router	Este equipo tiene registrada un ip pública para la comunicación con la matriz

Sucursal Libertad:

Son 8 los equipos que usan los usuarios dentro de esta sucursal y que influencian en el tráfico de red, como se detalla a continuación:

Tabla 7 Equipos de Sucursal Libertad

Cantidad	Tipo de Equipo	Observaciones
2	Pc de Escritorio	Distribuidas entre caja y ventas.
1	Teléfonos IP	Fijo
1	DVR	Conectado con 4 cámaras
1	Impresora	Para toda el área
1	Dispositivo Inalámbrico	Para uso interno
1	Equipo Biométrico	Para el Registro de Asistencia
1	Router	Este equipo tiene registrada un ip pública para la comunicación con la matriz

Sucursales Móviles y Otros Accesos Remotos:

Son 9 los equipos que usan los usuarios remotamente y que influencian en el tráfico de red, como se detalla a continuación:

Tabla 8 Equipos de Sucursales Móviles

Cantidad	Tipo de Equipo	Observaciones
1	Laptop	Para Ventas en Ferias
2	Tablet	Para Ventas y Cobranzas.
1	Laptop	Técnico de PROVEDATOS
1	Smartphone	Gerente General

Cantidad	Tipo de Equipo	Observaciones
1	Laptop	Gerente general
1	Laptop	Ing. Cristian Apunte
1	Laptop	Eco. Humberto Mendoza
1	Smartphone	Srta. Ana Lucía Juela

En total los equipos a acceder a la red son 103 entre matriz y sucursales incluyendo equipos Servidores.

3.6. LEVANTAMIENTOS DE RIESGOS INHERENTES DE LA EMPRESA

Los riegos inherentes encontrados que puedan afectar la operatividad de la empresa después de todo el levantamiento de información anterior, son los siguientes:

- Penetración desde Internet por puertos abiertos.
- Ataque de Fuerza Bruta, Denegación de Servicios, SQLi, entre otros desde el internet.
- Uso de Servidor desde el internet para Propagación de Spam.
- Robo de Información y modificación de datos desde el Internet.
- Interceptación y Robo de Información al momento de la comunicación entre la sucursal y matriz.
- Acceso de usuarios de la LAN no autorizados a los diferentes servicios.
- Saturación de navegación en la Red provocando que los servidores no den el suficiente y óptimo servicio.
- Acceso no autorizado a los servidores VOIP, ESXi, DNS y Directorio Activo y modificación de configuraciones por parte de usuarios de la LAN.
- Caída de los Servidores por el uso interno de direcciones IP asignadas a estos equipos.

- Acceso no autorizado de usuarios de la Red interna y modificación de datos de configuración en Gateway de Voz IP.
- Uso de Direcciones IP sin autorización.
- Accesos no autorizados a la Red interna.
- Caída del Servicio de Navegación de Internet en la matriz y sucursales de Guayaquil.
- Descarga de Virus y cualquier tipo de Malware.
- Retrasos y mala elaboración de trabajos internos y externos de la empresa.
- Problemas en el cumplimiento de obligaciones con empresas externas gubernamentales, como SRI, IESS, etc.
- Problemas en Grabación de Video en los Dispositivos NVR dentro de la empresa.
- Cambio de contraseña al usuario administrador de la Central IP Elastix.
- Ingreso de Virus por medio de Internet.
- No poder identificar responsabilidades de los usuarios de la red al momento de una violación de seguridad a los diferentes sistemas internos de la empresa.

CAPÍTULO 4

ANÁLISIS Y DISEÑO

4.1. ANÁLISIS DE INFORMACIÓN OBTENIDA POR PARTE DE LA EMPRESA

El análisis se lo hace primeramente de forma general y luego por cada sucursal.

4.1.1. ANÁLISIS GENERAL

- La empresa tiene como proveedor de Internet en Guayaquil a la Empresa TELCONET, en Santa Elena a BRIGTELECOM y en Libertad a NETLIFE.
- La empresa posee un pool de 4 direcciones IP pública que en todo el documento se especificarán como A, B, C y D; por motivos de seguridad.
- La empresa posee Internet de 1MB Dedicado en Guayaquil y 5MB 4:1 en Santa Elena.

- Dos de las direcciones IP públicas se encuentran asignadas directamente a los servidores, que no es correcto para la seguridad de mencionados equipos, y 2 se encuentran disponibles. La asignación es de la siguiente manera:

Tabla 9 Uso de Direcciones IP Públicas

Servicio	Ip Pública Asignada
Sistema Financiero (PAC)	A
Sistema Elastix	B
Disponible	C
Disponible	D

- El dispositivo Gateway de voz se encuentra en una red y ubicación diferente a la del Servidor Elastix.

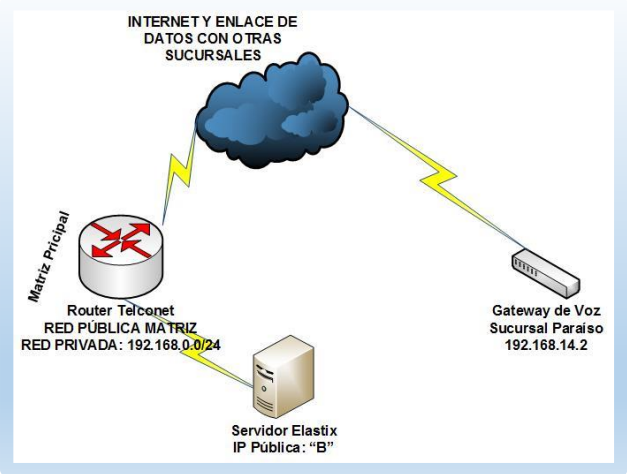


Figura 4.1 Ubicación de Equipos principales para Telefonía IP

- Existe más del 70% de la red de las diferentes sucursales donde se puede apreciar un desperdicio de direcciones ip, como se muestra en la siguiente tabla:

Tabla 10 Desperdicio de Direcciones IP

Red	Disponibles	Usados incluye IP Gateway	No utilizadas	% Desperdiciado
192.168.0.0/24	254	39	215	85%
192.168.1.0/24	254	14	240	94%
192.168.6.0/28	14	1	13	93%
192.168.7.0/28	14	1	13	93%
192.168.8.0/28	14	1	13	93%
192.168.11.0/24	254	4	250	98%
192.168.13.0/28	14	4	10	71%
192.168.14.0/28	14	4	10	71%
192.168.15.0/28	14	1	13	93%
192.168.12.0/24	254	4	250	98%
192.168.16.0/28	14	5	9	64%
192.168.17.0/28	14	3	11	79%
192.168.18.0/28	14	1	13	93%
192.168.88.0/24	254	5	249	98%
192.168.89.0/28	14	2	12	86%
192.168.90.0/28	14	2	12	86%
172.16.31.0/24	254	5	249	98%
TOTALES	1410	90	1320	

- No existe ningún tipo de Seguridad Perimetral ni interna para los diferentes servicios que otorga la empresa.
- Los Servidores se encuentran el mismo segmento de red de la LAN de la matriz y no en un segmento DMZ.
- Todas las sucursales acceden a internet por medio de cada Router del ISP de forma independiente respetando el 1MB del enlace.
- Los dispositivos móviles no utilizan redes VPN para conectarse a los servidores.
- El Servidor VPN de la empresa no está operativo.
- Las direcciones IP utilizadas por los Servidores que pertenecen a la Red LAN de la Matriz son los siguientes:

Tabla 11 Servidores con IP de la LAN

Servicio	Ip Pública Asignada
Server VMware ESXi 5.1	192.168.0.10
DNS, Dominio y Active Directory	192.168.0.5
Registro de Asistencia	192.168.0.27
Sistema de Visualización de Cámaras	192.168.0.15

- La empresa posee menos de 20 políticas de seguridad, no posibles de evidenciar para la administración de la red y los servicios hacia el Internet.
- La empresa no posee ningún tipo de control de tráfico y navegación.

4.1.2. MATRIZ

- Los servidores no se encuentran en una DMZ.
- Existe un 85% de direcciones IP desperdiciadas dentro de la red 192.168.0.0/24
- Existen 2 Ip públicas sin asignación, C y D.
- Existen accesos inalámbricos sin ningún firewall que controle su tráfico de red.
- Las cámaras ip están dentro del mismo segmento de red consumiendo el ancho de banda de la red LAN.

4.1.3. SUCURSAL BALERIO

- Existen redes que no están siendo usadas como la 192.168.6.0/28, 192.168.7.0/28, 192.168.8.0/28.
- Todos los dispositivos de red están dentro del mismo rango, es decir, no hay segmentación de tráfico de datos, video y telefonía.

- Dispositivos Inalámbricos sin control de firewall.
- El 94% de las direcciones Ip de la red 192.168.1.0/24 están desperdiciadas.

4.1.4. SUCURSAL PARAÍSO

- La red 192.168.15.0/28 no se encuentra usada por ningún dispositivo de red dentro de esta sucursal.
- Dispositivos Inalámbricos sin control de firewall.
- En esta sucursal se encuentra el Gateway de voz de 8 puertos con las diferentes líneas telefónicas tanto convencionales como celulares.
- La red 192.168.13.0/28 está siendo usada para la trasmisión de video y equipos WIFI.
- La red 192.168.14.0/28 está siendo usada para Telefonía Ip de la sucursal.
- Tanto la red 192.168.13.0/28 y 192.168.14.0/28 sus direcciones IP no están siendo usadas en un 71% en base a la necesidad de esta sucursal.
- El 98% de las direcciones Ip de la red 192.168.11.0/24 están desperdiciadas.

4.1.5. SUCURSAL SAN FRANCISCO

- La red 192.168.18.0/28 no se encuentra usada por ningún dispositivo de red dentro de esta sucursal.

- Dispositivos Inalámbricos sin control de firewall.
- La red 192.168.16.0/28 está siendo usada para la trasmisión de video y equipos WIFI y existe un 64% de Disponibilidad de direcciones IP.
- La red 192.168.17.0/28 está siendo usada para Telefonía Ip de la sucursal, y posee un 79% de direcciones Ip disponibles.

  El 98% de las direcciones Ip de la red 192.168.12.0/24 están desperdiciadas.

4.1.6. SUCURSAL SANTA ELENA

- Esta sucursal se encuentra fuera de la Provincia del Guayas y su proveedor de internet es BRIGTELECOM y su servicio es de 5MB con compartición 4:1.
- Esta sucursal tiene asignado por parte del ISP la Ip pública X, que se encuentra configurada en el router de última milla.
- Esta sucursal accede a los servicios de telefonía IP y sistema financiero por medio de las Ip públicas de matriz.
- Existen NAT destino en el router de esta sucursal, para la conexión hacia su dispositivo biométrico y para la publicación de cámaras de video vigilancia.
- Su único control perimetral es el router tanto para red cableada como para la red inalámbrica WIFI.
- En esta sucursal existe un DVR que realiza las grabaciones de video.

- Existen 3 redes, 2 tienen direcciones IP desperdiciadas.

4.1.7. SUCURSAL LIBERTAD

- Esta sucursal se encuentra fuera de la Provincia del Guayas y su proveedor de internet es NETLIFE y su servicio es de 10MB con compartición 2:1.
- Esta sucursal tiene asignado por parte del ISP la ip pública Y, que se encuentra configurada en el router de última milla.
- Esta sucursal accede a los servicios de telefonía IP y sistema financiero por medio de las Ip públicas de matriz.
- Existen NAT destino en el router de esta sucursal, para la conexión hacia su dispositivo biométrico y para la publicación de cámaras de video vigilancia.
- Su único control perimetral es el router tanto para red cableada como para la red inalámbrica WIFI.
- En esta sucursal existe un DVR que realiza las grabaciones de video.
- Existe un desperdicio de direcciones IP ya que su red es la 172.16.30.0/24.

4.2. ANÁLISIS DE RIESGO INHERENTE

Para el análisis de Riesgo Inherente de la Empresa de créditos Palacio del Hogar, se utiliza un método cuantitativo que busca identificar cuáles son los riesgos existentes en relación con la Seguridad de los servidores y de la red

de la empresa; se procede a desarrollar una matriz considerando los siguientes parámetros:

Identificación del Riesgo:

	A	B	C
1	IDENTIFICACIÓN DE RIESGO		
2	Descripción de la Falla	Efectos de la Falla	Descripción del Riesgo Inherente
3			

Figura 4.2 Matriz Identificación de Riesgo

- **Descripción de la Falla: (Columna A)** este campo permite identificar cuáles son las fallas de seguridad existentes dentro de la empresa.

- **Efectos de la Falla: (Columna B)** este campo permite describir los efectos que podría ocasionar una determinada falla de seguridad dentro de la Organización.

- **Descripción del Riesgo Inherente: (Columna C)** el riesgo inherente es el resultado de una falla esta haya sido observada o no y el efecto que puede causar, en este campo se describe los riesgos que provocan las diferentes fallas de seguridad.

Análisis de Riesgo:

D	E	F	G	H	I	J	K
ANÁLISIS DEL RIESGO							
Probabilidad			Impacto			RESULTADO (PXI)/9	Categoría del Riesgo
A(3)	M(2)	B(1)	S(3)	M(2)	L(1)		

Figura 4.3 Matriz de Análisis del Riesgo

- **Probabilidad: (Columna D, E y F)** descripción o medida de la posibilidad de ocurrencia de un riesgo identificado en cada columna de la matriz. para poder medirla se utiliza la siguiente escala cualitativa:
  - **A:** Probabilidad Alta
  - **M:** Probabilidad Media
  - **B:** Probabilidad Baja

Cada una con una valoración numérica de 3 a 1 respectivamente. Para poder decidir qué valor otorgar al riesgo es necesario hacerse la pregunta ¿Qué tan probable es que el riesgo se materialice?

- **Impacto: (Columna G, H y I)** consiste en valorar qué tan significativo es el impacto dentro de la organización y de sus procesos si el riesgo se llegara a materializar, para medir este impacto se ha designado los siguientes niveles:
  - **S:** Significativo
  - **I:** Impacto Moderado
  - **I:** Impacto Leve

Cada una con una valoración numérica de 3 a 1 respectivamente. Para poder otorgar uno de los niveles planteados es necesario responder la siguiente pregunta ¿Cuánto afecta la materialización del riesgo al objetivo del proceso?

- **Resultado: (Columna J)** consiste en obtener el producto entre la probabilidad e impacto y a este dividir para el número máximo de calificación, con esto se puede obtener el porcentaje que necesitamos como resultado. Es decir (P x I)/9.

- **Categoría de Riesgo: (Columna K)** consiste en ubicar el riesgo en una escala según su prioridad para su respectiva administración, con el objetivo de minimizarlo. Como parte de esta administración al momento de tomar decisiones se ha asociado ciertas nomenclaturas con los colores Verde, Amarillo y Rojo, como se muestra en la siguiente figura:

		PROBABILIDAD		
		B (1)	M (2)	A (3)
IMPACTO	L (1)	BL 11%	ML 22%	AL 33%
	M (2)	BM 22%	MM 44%	AM 66%
	S (3)	BS 33%	MS 66%	AS 100%

Figura 4.4 Tabla de Categorización del Riesgo Inherente

Como podemos observar en la figura 4.13 se categoriza el Riesgo en base a colores y nomenclaturas, que a continuación se procede a describir de forma más explícita sus 9 categorías:

BL: Riesgo con probabilidad de ocurrencia baja e impacto leve. Su valor corresponde al 11% del valor máximo otorgado. Se lo identifica de color verde como un riesgo de prioridad baja de atención.

ML: Riesgo con probabilidad de ocurrencia media e impacto leve. Su valor corresponde al 22% del valor máximo otorgado. Se lo identifica de color verde como un riesgo de prioridad baja de atención.

AL: Riesgo con probabilidad de ocurrencia alta e impacto leve. Su valor corresponde al 33% del valor máximo otorgado. Se lo identifica de color amarillo como un riesgo de prioridad media de atención.

BM: Riesgo con probabilidad de ocurrencia baja e impacto moderado. Su valor corresponde al 22% del valor máximo otorgado. Se lo identifica de color verde como un riesgo de prioridad baja de atención.

MM: Riesgo con probabilidad de ocurrencia media e impacto moderado. Su valor corresponde al 44% del valor máximo otorgado. Se lo identifica de color amarillo como un riesgo de prioridad media de atención.

AM: Riesgo con probabilidad de ocurrencia alto e impacto moderado. Su valor corresponde al 66% del valor máximo otorgado. Se lo identifica de color rojo como un riesgo de prioridad inmediata de atención.

BS: Riesgo con probabilidad de ocurrencia baja e impacto significativo. Su valor corresponde al 33% del valor máximo otorgado. Se lo identifica de color amarillo como un riesgo de prioridad media de atención.

MS: Riesgo con probabilidad de ocurrencia media e impacto significativo. Su valor corresponde al 66% del valor máximo otorgado. Se lo identifica de color rojo como un riesgo de prioridad inmediata de atención.

AS: Riesgo con probabilidad de ocurrencia alta e impacto significativo. Su valor corresponde al 100% valor máximo otorgable. Se lo identifica de color verde como un riesgo de prioridad inmediata de atención.

Una vez analizado los parámetros a utilizar en el análisis de riesgo inherente, se procede a aplicar dicha matriz para los riesgos inherentes detallados en el numeral 3.6 “Levantamiento de Riesgos Inherentes de la Empresa”:

Tabla 12 Matriz de Análisis de Riesgo Inherente Ejecutado

IDENTIFICACIÓN DE RIESGO			ANÁLISIS DE RIESGO							
Descripción de la Falla	Efectos de la Falla	Descripción del Riesgo Inherente	Probabilidad			Impacto			RESULTADO (PXI)/9	Categoría del Riesgo
			A(3)	M(2)	B(1)	S(3)	M(2)	L(1)		

IDENTIFICACIÓN DE RIESGO			ANÁLISIS DE RIESGO							
Descripción de la Falla	Efectos de la Falla	Descripción del Riesgo Inherente	Probabilidad			Impacto			RESULTADO (PXI)/9	Categoría del Riesgo
			A(3)	M(2)	B(1)	S(3)	M(2)	L(1)		
El Servidor del Sistema Financiero (PAC) y la Central IP Elastix tienen asignado directamente una IP pública	Puertos Abiertos	Penetración desde Internet por puertos abiertos	3			3			100%	AS
	Servidor Atractivo a ataques	Ataque de Fuerza Bruta, Denegación de Servicios, SQLi, entre otros desde el internet	3			3			100%	AS
	Servicios sin Protección	Uso de Servidor desde el internet para Propagación de Spam	3			3			100%	AS
	Vulnerabilidad de Accesos por la ventana de Login del Sistema	Robo de Información y modificación de datos desde el Internet		2		3			67%	MS
Conexión de Sucursales Móviles, de Santa Elena y Libertad sin ningún túnel de Seguridad	Viaje de información por el Internet sin ningún tipo de Protección	Interceptación y Robo de Información al momento de la comunicación entre la sucursal y matriz		2		3			67%	MS
Servidores Internos de la Empresa comparten direcciones IP de la Red LAN	Fácil acceso a la información por parte de toda la LAN	Acceso de usuarios de la LAN no autorizados a los diferentes servicios		2		3			67%	MS
	Mala Administración de Ancho de Banda	Saturación de navegación en la Red provocando que los servidores no den el suficiente y óptimo servicio		2			2		44%	MM
	Visualización de equipo desde cualquier red	Acceso no autorizado a los servidores VOIP, ESXi, DNS y Directorio Activo y modificación de configuraciones por parte de usuarios de la LAN			1	3			33%	BS
	Duplicidad de direcciones IP	Caída de los Servidores por el uso interno de direcciones			1	3			33%	BS

IDENTIFICACIÓN DE RIESGO			ANÁLISIS DE RIESGO							
Descripción de la Falla	Efectos de la Falla	Descripción del Riesgo Inherente	Probabilidad			Impacto			RESULTADO (PXI)/9	Categoría del Riesgo
			A(3)	M(2)	B(1)	S(3)	M(2)	L(1)		
		IP asignadas a estos equipos								
Acceso a Gateway de Voz desde cualquier red dentro de la empresa	Visualización de equipo desde cualquier red	Acceso no autorizado de usuarios de la Red interna y modificación de datos de configuración en Gateway de Voz IP			1	3			33%	BS
Red mal segmentada	Demasiadas IP sin asignación	Uso de Direcciones IP sin autorización		2		3			67%	MS
Falta de IPS	Vulnerabilidad de Acceso de Intrusos a la Red Interna	Accesos no autorizados a la Red interna	3			3			100%	AS
Acceso a Internet libre desde cualquier computador de la Red	Consumo de Ancho de Banda por parte de los usuarios	Caída del Servicio de Navegación de Internet en la matriz y sucursales de Guayaquil	3			3			100%	AS
	Navegación en Páginas Peligrosas	Descarga de Virus y cualquier tipo de Malware		2		3			67%	MS
Falta de Administración de Tráfico de Red	Navegación Lenta	Retrasos y mala elaboración de trabajos internos y externos de la empresa	3			3			100%	AS
	No acceso inmediato a páginas importantes	Problemas en el cumplimiento de obligaciones con empresas externas gubernamentales, como SRI, IESS, etc.	3			3			100%	AS
Cámaras IP dentro del mismo segmento de red que la LAN	Consumo de ancho de banda por exceso de trasmisión de video	Problemas en Grabación de Video en los Dispositivos NVR dentro de la empresa		2				1	22%	ML
Puerto 80 de Server Elastix Visible para el Internet	Vulnerable a exploit para cambio de contraseña de Admin	Cambio de contraseña al usuario administrador de la Central IP Elastix		2		3			67%	MS

IDENTIFICACIÓN DE RIESGO			ANÁLISIS DE RIESGO							
Descripción de la Falla	Efectos de la Falla	Descripción del Riesgo Inherente	Probabilidad			Impacto			RESULTADO (PXI)/9	Categoría del Riesgo
			A(3)	M(2)	B(1)	S(3)	M(2)	L(1)		
No tener Antivirus Perimetral en la Red	Infección de equipos dentro de la red de la Empresa	Ingreso de Virus por medio de Internet	3			3			100%	AS
No tener Registro Documentación de Control de Accesos y Permisos	Pérdida de control en permisos asignados a los diferentes usuarios	No poder identificar responsabilidades de los usuarios de la red al momento de una violación de seguridad a los diferentes sistemas internos de la empresa.		2		3			67%	MS

Como podemos evidenciar en la Tabla 4.4 casi todos los riesgos ameritan de una inmediata atención, ya que en la empresa no existe al momento ningún tratamiento (Mitigar, Transferir, Aceptar y Evitar) para ellos. Solamente el riesgo de “Problemas en Grabación de Video en los Dispositivos NVR dentro de la empresa”, no es necesario priorizarlo para tratarlo ya que es un riesgo con probabilidad de ocurrencia media e impacto leve.

4.3. DISEÑO DE LA NUEVA ESTRUCTURA DE RED PARA IMPLEMENTACIÓN DE UTM

En base al análisis realizado se considera el siguiente diseño para la implementación del UTM con el OpenSource Endian Community Firewall:

- Segmentación y Restructuración de la Red
- Control de tráfico
- Control de Accesos Remotos con Sucursales

- Monitoreo

4.3.1. SEGMENTACIÓN Y RESTRUCTURACIÓN DE LA RED

La red de toda la empresa cuenta con un enlace de datos contratado a TELCONET de 1MB Dedicado, igual que el servicio de internet. Se crean 5 zonas para esta segmentación, ROJA, NARANJA, VERDE, AZUL y VPN, con sus direcciones ip respectivas como se muestra en la siguiente tabla:

Tabla 13 Red por Zonas

Zona	Red	Aplicación
ROJA	Direcciones IP Públicas Matriz 192.168.0.0/30	Internet
NARANJA	172.16.100.0/27	Servidores
AZUL	172.16.200.0/27	Video y Wifi
VERDE	192.168.2.0/26	Red LAN Matriz
VPN	10.20.30.0/26	Red Privada Sucursales Ext.

Redes para Sucursales con Enlace de Datos

Las redes para las Sucursales se cambiarán en coordinación con la empresa TELCONET que es la proveedora del enlace de datos entre sucursales dentro de Guayaquil, todas estas redes serán direccionadas por parte del ISP a la ip 192.168.0.2 que pertenece al UTM, es decir, formarán parte de la zona roja configurada en el equipo, a continuación, se detalla por sucursales la asignación a realizar:

Tabla 14 Redes para Sucursales Enlazadas por TELCONET

Sucursal	Red	Aplicación
BALERIO	192.168.1.0/28	Computadoras, Impresoras y Equipo Biométrico
	192.168.6.0/28	Teléfonos IP
	192.168.7.0/28	Sistema de Video IP y Acceso a Datos Wifi
PARAISO	192.168.11.0/28	Computadoras, e Impresoras
	192.168.13.0/28	Acceso Wifi para Datos y Cámaras IP
	192.168.14.0/28	Telefonía IP
SAN FRANCISCO	192.168.12.0/28	Computadoras, e Impresoras
	192.168.16.0/28	Acceso Wifi para Datos y Cámaras IP
	192.168.17.0/28	Teléfonos IP

Asignación de IP a Zona Naranja o Red DMZ

En esta zona se ubican los equipos servidores de la empresa que se asignará las siguientes direcciones IP de la red 172.16.100.0/27:

Tabla 15 Direcciones IP Zona DMZ

Server	IP	Servicio
PAC – Sistema Financiero de la Empresa	172.16.100.2	Sistema Financiero
VMware ESXi 5	172.16.100.3	Servidor de Virtualización
Elastix	172.16.100.4	Central IP bajo Plataforma OpenSource de Elastix
DNS, Dominio y Archivos Compartidos	172.16.100.5	Servicio Interno de DNS, Dominio y Archivos Compartidos

Asignación de IP a Zona Verde o Red LAN

En esta zona se ubican los equipos de la LAN de Matriz que se asignará los siguientes rangos de direcciones IP de la red 192.168.2.0/26:

Tabla 16 Rangos IP Zona Verde

Asignación	Rango IP
Computadores y Equipos de usuario Final	192.168.2.1-192.168.2.20
Teléfonos IP	192.168.2.31-192.168.2.50

Asignación	Rango IP
Disponibles Rango Computadores	192.168.2.21-192.168.2.30
Disponibles para DHCP	192.168.2.51-192.168.2.61

Asignación de IP a Zona Roja o WAN

En esta zona se asignarán las siguientes IP Públicas relacionadas con los respectivos Servicios de la empresa, esta configuración será ejecutada por medio de NAT como se detalla a continuación:

Tabla 17 Asignación de Pool de IP Públicas

Ip Pública	Servicio
A	PAC- para ocasiones excepcionales ya que este servicio será accedido externamente por medio de VPN
B	Server VPN
C	Telefonía IP con central Elastix
D	Cámaras ip y Otros servicios, Se asignarán con diferentes puertos.

4.3.2. CONTROL DEL TRÁFICO

Para controlar el Tráfico se establecerán una serie de políticas para cada Red de la Empresa Créditos Palacio del Hogar; las listas de control de acceso que en esta sección se detallan controlará todo el tráfico, y lo que en estas políticas no esté permitido será automáticamente denegado su acceso. Para este control se clasifica el control de Tráfico en 7 escenarios:

1. Redirección de Puertos/NAT Destino/NAT Fuente
2. Tráfico Enrutado de Entrada
3. Tráfico de Salida
4. Tráfico entre Zonas

5. Tráfico VPN
6. Acceso al Sistema
7. Proxy

1. **Tráfico de Redirección de Puertos/NAT Destino:** la asignación queda de la siguiente Manera:

Tabla 18 Políticas de NAT Destino

Ip Entrada	Servicio	Política	Ip Destino	Observación
A **Origen IP Pública EQUIFAX**	TCP:80,443	Permitir con IPS	172.16.100.2	Acceso EQUIFAX a Sistema PAC
A **Origen X, Y**	TCP:80	Permitir con IPS	172.16.100.2	Acceso Santa Elena a Sistema PAC
C **Origen X, Y**	TCP y UDP:5060-5500, 10000-20000, 8000, 3478	Permitir con IPS	172.16.100.4	Acceso a Servidor IP Elastix desde WAN
D **Origen Z**	TCP:9012	Permitir con IPS	172.16.200.4:80	Cámara Bodega 1
D **Origen Z**	TCP:9013	Permitir con IPS	172.16.200.5:80	Cámara Bodega 2
D **Origen Z**	TCP:9014	Permitir con IPS	172.16.200.6:80	Cámara Bodega 3
D **Origen Z**	TCP:9022	Permitir con IPS	192.168.1.6:80	Cámara Balerio 1
D **Origen Z**	TCP:9023	Permitir con IPS	192.168.1.7:80	Cámara Balerio 2
D **Origen Z**	TCP:9024	Permitir con IPS	192.168.1.8:80	Cámara Balerio 3
D **Origen Z**	TCP:9025	Permitir con IPS	192.168.1.9:80	Cámara Balerio 4
D **Origen Z**	TCP:9032	Permitir con IPS	192.168.13.3:80	Cámara Paraíso 1
D **Origen Z**	TCP:9033	Permitir con IPS	192.168.13.4:80	Cámara Paraíso 2
D **Origen Z**	TCP:9034	Permitir con IPS	192.168.13.6:80	Cámara Paraíso 3
D **Origen Z**	TCP:9035	Permitir con IPS	192.168.13.7:80	Cámara Paraíso 4
D **Origen Z**	TCP:9042	Permitir con IPS	192.168.16.2:80	Cámara San Fran 1

Ip Entrada	Servicio	Política	Ip Destino	Observación
D **Origen Z**	TCP:9043	Permitir con IPS	192.168.16.3:80	Cámara San Fran 2
D **Origen Z**	TCP:9044	Permitir con IPS	192.168.16.4:80	Cámara San Fran 3

2. **Tráfico Enrutado de Entrada:** la configuración queda de la siguiente Manera:

Tabla 19 Políticas de Tráfico Entrante

Origen	Destino	Servicio	Política	Observación
Ip Privada de Sucursal Externa por Enlace de Datos	172.16.100.4	TCP y UDP:5000-5500, 10000-20000, 8000, 3478	Permitir con IPS	Acceso a Servidor IP Elastix desde Sucursales
Ip Privada de Sucursal Externa por Enlace de Datos	172.16.100.2	TCP:80, 139, 445	Permitir con IPS	Acceso a PAC Servicio de Impresión
Ip Privada de Sucursal Externa por Enlace de Datos	172.16.100.5	TCP y UDP:135, 1025, 1026, 53, 137, 138, 139, 88, 1801, 2101, 2103, 2105, 3527, 389, 119, 80, 443, 25, 445, 464, 500, 563, 593, 636, 3268, 3269, 5722, 123, 9389, 67, 2535, 49152:65535	Permitir con IPS	Acceso a Server DNS - AD y Archivos Compartidos

3. **Tráfico de Salida:** la configuración se efectuará filtrando por IP, por MAC y Por Sucursal como se muestra en la siguiente tabla:

Tabla 20 Políticas de Tráfico Saliente

Origen	Destino	Servicio	Política	Observación
MAC del Administrador del UTM y de la Red	192.168.1.0/28 192.168.11.0/28 192.168.12.0/28 192.168.13.0/28 192.168.14.0/28 192.168.16.0/28 192.168.17.0/28	Cualquier Servicio	Permitir con IPS	Acceso Administrador de la Red a Sucursales esta regla por default deshabilitada
Direcciones MAC de LAN Matriz	WAN	TCP: 80, 443	Permitir con IPS	Salida Internet sin Proxy Matriz por MAC
Ip Privada de Sucursal Paraíso	WAN	TCP: 80, 443	Permitir con IPS	Salida Internet sin Proxy Paraíso
Ip Privada de Sucursal Balerio	WAN	TCP: 80, 443	Permitir con IPS	Salida Internet sin Proxy Balerio
Ip Privada de Sucursal San Francisco	WAN	TCP: 80, 443	Permitir con IPS	Salida Internet sin Proxy San Francisco
Ip Privada de Zona Azul	WAN	TCP: 80, 443	Permitir con IPS	Salida Internet sin Proxy Zona Azul
Ip Privada Equipos de Cualquier Red de la Empresa	WAN	TCP y UDP: 5222, 5223, 5228, 5242, 3478	Permitir con IPS	Salida solo WhatsApp incluido llamada (3478)
Ip Privada de Matriz	192.168.1.0/28 192.168.11.0/28 192.168.17.0/28 X, Y	TCP: 5005	Permitir con IPS	Acceso a Biométricos de Sucursales desde Matriz
Ip Privada Equipos de Cualquier Red de la Empresa	X, Y	TCP:8090	Permitir con IPS	Salida a Cámaras Sucursal Santa Elena y Libertad
Ip se Server Financiero PAC	192.168.1.0/28 192.168.11.0/28 192.168.12.0/28	TCP y UDP: 139, 445	Permitir con IPS	Acceso desde PAC a Sucursales Servidor de Impresión
Ip Privada Equipos de Cualquier Red de la Empresa	WAN	TCP: 25, 26, 110, 143, 995, 993, 587, 465, 995	Permitir con IPS	Salida a Correo
Servidor DNS interno de la Empresa	WAN	TCP y UDP: 53	Permitir con IPS	Salida a DNS

Origen	Destino	Servicio	Política	Observación
Cualquier Equipo de la Red de la Empresa	WAN	TCP y UDP:53	Denegar	Bloqueo de Salida a DNS Toda la Red
Cualquier Equipo de la Red de la Empresa	WAN	ICMP: 8, 30	Denegar	Bloqueo de PING

Para el caso de Filtrado por MAC el Formato de Control se Puede Observar en el Anexo “F”.

4. **Tráfico entre Zonas:** para este control de tráfico se implementará las siguientes políticas:

Tabla 21 Políticas de Tráfico Inter-Zona

Origen	Destino	Servicio	Política	Observación
Mac de PC Administrador de la Red	VERDE AZUL NARANJA	Cualquiera	Permitir con IPS	Administrador de la Red a Zonas de Firewall
Mac de PC que tiene que visualizar Cámaras por VNC	Ip de Servidor de Cámaras	TCP: 5900, 5800	Permitir con IPS	Acceso a Cámaras de Vigilancia por VNC solo visualización
Ip Privada de Servidor PAC	192.168.2.13 192.168.2.15	TCP y UDP: 139, 445	Permitir sin IPS	Acceso desde Servidor Financiero PAC a Servicios de Impresión
Ip Privada de Equipos de Matriz que Impriman desde Server PAC	172.16.100.2	TCP y UDP: 139, 445	Permitir sin IPS	Acceso a Servicio de Impresión hacia PAC
Ip Privada que tengan que ingresar al PAC vía WEB	172.16.100.2	TCP: 80	Permitir sin IPS	Acceso a PAC vía WEB
Ip Privada o Zonas con Acceso al Servidor DNS interno	172.16.100.5	TCP y UDP: 53	Permitir sin IPS	Acceso a Servicios DNS
Red LAN de	172.16.100.4	TCP y	Permitir	Acceso de LAN

Origen	Destino	Servicio	Política	Observación
Teléfonos IP		UDP: 5060:5500, 10000:20000, 8000, 3478	sin IPS	a Server IP Matriz
Ip Privada o Zona que necesite acceso a Active Directory y Carpetas Compartidos	172.16.100.5	TCP y UDP: 135, 1025, 1026, 53, 137, 138, 139, 88, 1801, 2101, 2103, 2105, 3527, 389, 119, 80, 443, 25, 445, 464, 500, 563, 593, 636, 3268, 3269, 5722, 123, 9389, 67, 2535, 49152:65535	Permitir con IPS	Acceso solo a Directorio Activo y Carpetas Compartidas

5. **Tráfico VPN:** para controlar este tráfico se levantará el Servicio OpenVPN que nos permite usar certificados y usuarios para las diferentes conexiones que sean necesarias dentro de la empresa. Esta opción será configurada en las sucursales externas sin enlace de datos y dispositivos móviles. Hay que considerar que este servicio al ser OpenSource no cuenta con todas las seguridades recomendadas por expertos en este tipo de conexiones, como puede ser zonas de análisis y cuarentena de una conexión previa a su interacción con los servicios de la empresa; por tema costos la opción de OpenVPN de endian soluciona los problemas actuales existentes en la empresa con un nivel de seguridad aceptable.

Se realiza la creación de los siguientes usuarios con su respectiva IP fija para un mejor control de este tráfico según el levantamiento realizado, considerando que se utiliza un tipo de autenticación PSK (usuario/contraseña):

Tabla 22 Usuarios VPN con dirección IP

Usuario	Cargo	Dirección Ip
Alberto Fuela	Gerente General	10.20.30.2
Ing. Guido Miguez	Implementador	10.20.30.3
Ing. Efraín Barrera	Soporte Provedatos	10.20.30.4
PC de Sucursal Santa Elena	Caja	10.20.30.5
Ing. Cristhian Apunte	Contador	10.20.30.6
PC de Sucursal Libertad	Caja	10.20.30.7
Ana Lucía Juela	Marketing y Ventas	10.20.30.8
Eco. Humberto Mendoza	Administración	10.20.30.9
Laptop de Ferias Móviles	Ventas Móviles	10.20.30.10
PC de Sucursal Libertad	Ventas	10.20.30.11
Tablet Ventas y Cobranzas Móviles Libertad	Ventas Móviles	10.20.30.12
Tablet Ventas y Cobranzas Móviles Santa Elena	Ventas Móviles	10.20.30.13
Tablet Ventas y Cobranza Matriz	Ventas Móviles	10.20.30.14
Tablet Ventas y Cobranza Sucursal Balerio	Ventas Móviles	10.20.30.15
Tablet Ventas y Cobranza Sucursal Paraíso	Ventas Móviles	10.20.30.16
Tablet Ventas y Cobranza Sucursal San Francisco	Ventas Móviles	10.20.30.17

A continuación se detalla las listas de control de Acceso VPN:

Tabla 23 Políticas de Tráfico VPN

Origen	Destino	Servicio	Política	Observación
Usuarios VPN que utilicen Impresoras de Impresión de Recibos Y Facturas	172.16.100.2	TCP y UDP: 139, 445	Permitir con IPS	Acceso a PAC para Servicios de Impresión
Usuarios VPN que acceden a PAC vía Web	172.16.100.2	TCP: 80	Permitir con IPS	Acceso a PAC vía Web
Usuario VPN	172.16.200.4	TCP: 80	Permitir	Acceso a

Origen	Destino	Servicio	Política	Observación
Gerente General	172.16.200.5 172.16.200.6 192.168.1.6 192.168.1.7 192.168.1.8 192.168.1.9 192.168.13.3 192.168.13.4 192.168.13.6 192.168.13.7 192.168.16.2 192.168.16.3 192.168.16.5		con IPS	Cámaras IP
Usuario VPN Administrador de UTM y Administrador de Redes y Seguridades	192.168.2.0/26 172.16.100.0/27 172.16.200.0/27 192.168.1.0/24 192.168.6.0/28 192.168.7.0/28 192.168.11.0/28 192.168.12.0/28 192.168.13.0/28 192.168.14.0/28 192.168.16.0/28 192.168.17.0/28 10.20.30.0/26 0.0.0.0/0	Cualquier Servicio	Permitir con IPS	Acceso a Administrador de Red y UTM
Servidor PAC	Servidor OpenVPN	TCP y UDP: 139, 445	Permitir con IPS	Acceso PAC a Usuarios VPN para Servicios de Impresión
Usuario VPN Gerente General	Servidor de Telefonía IP	TCP: 80, 443	Permitir con IPS	Acceso a Reportes y Grabaciones de Elastix
Usuarios VPN que tengan usuarios de Telefonía	Servidor de Telefonía IP	TC y UDP: 5060:5500, 10000:20000, 8000, 3478	Permitir con IPS	Permiso de usuarios VPN para llamadas IP

6. **Acceso al Sistema:** se configurará solo los servicios que sean necesarios para la administración y operatividad del UTM los cuales se muestran en la siguiente tabla:

Tabla 24 Políticas de Acceso al Sistema

Dirección de Origen	Interfaz de Origen	Servicio	Política	Observación
Cualquier	B	UDP: 1194	Permitir con IPS	Acceso a Servicio OpenVPN configurado en el UTM
Mac de Administrador de la Red	VERDE	TCP: 10443, 443	Permitir con IPS	Permisos de Administrador de Red
Ip VPN de Usuario Administrador UTM	VPN SERVER: default	TCP: 10443, 443	Permitir con IPS	Acceso a Puertos que utiliza endian desde Usuario VPN
192.168.1.0/24 192.168.11.0/28 192.168.12.0/28 192.168.13.0/28	ROJO	TCP: 3128	Permitir con IPS	Acceso a Puerto de Proxy habilitado en el UTM
Cualquier	ROJO	Cualquier	Denegar	Bloque de Acceso desde Internet a Cualquier Otro Servicio del UTM

7. **Proxy:** se configurará el Servicio de Proxy HTTP, con sus respectivas políticas de acceso y filtrado WEB.

Tipo de Proxy: el tipo de proxy a usar en las Zona Verde, Naranja y Azul será **"No Trasparente",** ya que la cantidad de equipos y su Directorio Activo permite la respectiva configuración manual.

Puerto a Utilizar por el Proxy: 3128

Tamaño Máximo de Carga y Descarga: sin límite

Puertos Permitidos: revisando los sitios web permitidos en la empresa se llega a la conclusión que se usará puertos de navegación HTTP y HTTPS, para correo electrónico POP3, SMTP

sin certificados y con certificados, y ciertos sitios web de proveedores como en el caso de Cartimex que usa para navegación en ciertos servicios el puerto 88, junto con MAVESA que para su facturación Electrónica el puerto 8084.

Administración de Cache: para el tamaño del cache del proxy se asignará 4GB de espacio en disco duro.

Reglas de Filtrado Web: se considera crear 3 tipos de filtros en el Proxy: “Navegación Libre”, “No Pornografía, Redes Sociales, Audio y Video” y, “No Pornografía, video, si Facebook”.

Políticas de Acceso: a continuación las políticas a implementar en el proxy:

Tabla 25 Políticas de Proxy HTTP

Política	Origen	Destino y Autenticación	Cuando	Agente de Usuario
Acceso sin Filtro WEB	Ip de Contador	Cualquiera Ninguna	Siempre	Cualquiera
Acceso Denegado a tipos MIME	Ip de Sucursales Matriz, Balerio, Paraíso y San Francisco que usan Proxy	Cualquiera Ninguna	Siempre	Cualquiera
Filtro de No Pornografía, Redes Sociales, Audio y Video	Ip de Sucursales Matriz, Balerio, Paraíso y San Francisco que usan Proxy	Cualquiera Ninguna	Siempre	Cualquiera

4.3.3. CONTROL DE ACCESO REMOTO CON SUCURSALES

Para el control de Accesos Remotos se realizará bajo los siguientes parámetros:

- Usar conexión privada virtual por medio del servidor OpenVPN.
- Usar el puerto UDP 1194 y la red 10.20.30.0/26
- Configurar conexiones para solo dispositivos tipo TUN.
- Este servidor no debe permitir la conexión de varios equipos con la misma cuenta.
- Debe bloquear cualquier respuesta DCHP procedente del túnel.
- Las ACL de conexión deben ser administradas por el Firewall del UTM.
- Los usuarios al momento de conectarse tienen que ingresar su usuario y clave.
- Los permisos serán otorgados por usuarios no por IP en el Firewall VPN.
- A cada usuario se le asignara una dirección IP fija de la red 10.20.30.0/26.
- Los usuarios a crear son los siguientes:

Tabla 26 Usuarios VPN

Nombre	Usuario	Puesto
Sr. Alberto Fuela	Usuarios no	Gerente General
Ing. Guido Miguez		Implementador y Soporte a UTM
Ing. Efraín Barrera		Soporte Sistema PAC Empresa Provedatos
Pc de Caja en Sucursal Santa Elena		Caja Sucursal Santa Elena
Ing. Cristian Apunte		Contador

Nombre	Usuario	Puesto
PC de Caja Sucursal Libertad	se enlistan por seguridad de la información, ya que podría ser blanco de cualquier tipo de ataque informático.	Caja Sucursal Libertad
Srta. Ana Lucía Juela		Marketing y Ventas
Eco. Humberto Mendoza		Administrador
Laptop Ferias		Laptop para Ferias de Mercadería
PC de Ventas Sucursal Libertad		Ventas Libertad
Tablet Ventas y Cobranzas Móviles Sucursal Libertad		Ventas y Cobranzas Móviles Sucursal Libertad
Tablet Ventas y Cobranzas Móviles Sucursal Santa Elena		Ventas y Cobranzas Móviles Sucursal Santa Elena
Tablet Ventas y Cobranzas Móviles Matriz		Ventas y Cobranzas Móviles Matriz
Tablet Ventas y Cobranzas Móviles Sucursal Balerio		Ventas y Cobranzas Móviles Sucursal Balerio
Tablet Ventas y Cobranzas Móviles Sucursal Paraíso		Ventas y Cobranzas Móviles Sucursal Paraíso
Tablet Ventas y Cobranzas Móviles Sucursal San Francisco		Ventas y Cobranzas Móviles Sucursal San Francisco

- El único servidor al momento que está permitido a ser accedido por este tipo de conexión, para todos los usuarios VPN es el 172.16.100.2 en los puertos 80, 139 y 445, que forma parte de la empresa como el Sistema Financiero llamado PAC, el mismo que puede acceder hacia el servicio VPN en los puertos 139, y 445 que son puertos de impresión.
- El único usuario con permisos a todas las redes y servicios por medio de VPN es el Usuario Administrador del UTM y de toda la red.

- El dominio a propagar será el de la empresa Créditos Palacio del Hogar.
- Estos permisos y cualquier adicional tendrá que ser registrado en el formato que se adjunta en el Anexo “G” de este documento, con la respectiva firma de validación del usuario, el Encargado del Dpto. de Sistemas y el Gerente General.

4.3.4. MONITOREO

Para monitoreo se utilizará las siguientes alternativas existentes en el UTM:

- **Accesos SSH:** para los accesos SSH a la consola del UTM, se utilizará el puerto 22 para los accesos internos por parte del Administrador de la Red desde su PC registrada, y desde el internet solamente se ingresará por medio de VPN, pero solo será habilitado cuando sea necesario por medio del administrador de la red. Adicional, el acceso SSH debe ser por medio de autenticación basada en contraseña y en calve pública.
- **Notificación de Eventos:** la notificación se enviará desde un correo que se solicitará crear con el nombre de infoendian@palaciodelhogar.com.ec, al correo del administrador de la Red de la Empresa Geovanny Santana, giovanny.santana@palaciodelhogar.com.ec, las notificaciones a enviar serán las siguientes:
  - El Enlace es Conectado

- Se desconectó el enlace
- Se inició el sistema
- Se está apagando el Sistema
- Reinicio del Sistema
- Todos los enlaces están desconectados
- Los enlaces están conectados
- El enlace está activo
- Reactivación de enlace
- Inicio de sesión con éxito de SSH
- El inicio de sesión de SSH ha fallado
- El disco está casi lleno

- **Backups y Restore:** los respaldos se realizarán de forma automática de forma semanal, y de forma manual cuando se realice algún cambio significativo del UTM.
- **Prevención de Intrusos:** este servicio será configurado para todo el tráfico de la red, la actualización de su base de datos se realizará diariamente.
- **Monitorización de Tráfico:** el monitoreo de tráfico en tiempo real será habilitado para todas las redes, con esta herramienta que ya incluye el UTM se podrá realizar estadísticas y un mejor análisis de lo que se navega dentro de la red de la empresa. Se debe mantener el historial de los Host para cualquier tipo de auditoría a futuro.

- **Estados:** en el UTM existirá reportes en tiempo real sus diferentes Estados y datos estadísticos de los siguientes servicios:
  - Sistema
  - De la red
  - Gráficos del Sistema
  - Gráficos del tráfico
  - Gráficos del Proxy
  - Conexiones
  - Conexiones VPN
  - Estadísticas de correo SMTP y Cola de Correo en caso de tener un servidor de correo.

- **Registros, Informes y Otros:** para poder obtener esta información el UTM se configurará de una forma que almacene todos los registros que se ejecutan dentro del tráfico de red de la empresa, en tiempo real y en tiempo no real, con esto el usuario podrá tener un control más eficiente de la actividad reportada en tiempo real por el UTM en el antivirus CLAMAV, firewall, servicio Web, OpenVPN, proxy HTTP, Prevención de Intrusos y el sistema que se ejecuta en el dispositivo de seguridad de Créditos Palacio del Hogar.

4.3.5. SERVICIOS ADICIONALES DE CONTROL

Los servicios adicionales de control que serán configurados en el UTM endian son los siguientes:

- **Servidor DHCP:** el servicio DHCP del UTM será habilitado solo para la zona verde, es decir la LAN de la empresa en el rango IP desde 192.168.2.51 hasta 192.168.2.61; este servicio nos permite realizar asignaciones fijas por MAC para el segmento de red 192.168.2.0/26, los dispositivos a fijarlos en la red son:
  - Impresora Epson L355 Wifi con la IP 192.168.2.8
  - El IPhone del Gerente General con la IP 192.168.2.51
  - La Laptop del Gerente General con la ip 192.168.2.11

El tiempo de asignación por defecto es de 60 minutos, y el tiempo máximo de asignación es de 120 minutos, la puerta de enlace será la 192.168.2.62, el DNS primario el 172.16.100.5 y el DNS secundario el 192.168.2.62.

- **DNS Dinámico:** este servicio no se configurará ya que no tienen ninguno instalado.
- **Motor de Antivirus:** el antivirus a utilizar en el UTM es el ClamAV que viene pre configurado en el UTM, las actualizaciones de su base de datos será automática con una frecuencia de 1 hora cada proceso.
- **Capacitación SPAM:** este servicio aún no se habilitará ya que a la fecha no tienen instalado un servidor de correo.

CAPÍTULO 5

IMPLEMENTACIÓN Y PRUEBAS

5.1. INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN FIREWALL

Primeramente debemos descargar el ISO del sitio WEB www.endian.com, una vez descargado a continuación se detalla los pasos de instalación y configuración de Endian Firewall Community:

1. Ubicación de Tarjetas de Red en Computador a Implementar la Herramienta.
2. Cargar el Instalador de Endian desde el medio a utilizar (CD o USB)
3. Seleccionar el idioma a instalar
4. Presionar OK en la ventana de Bienvenida de Endian
5. Después aparecerá una ventana de advertencia especificando que el proceso de instalación borrará todos los datos del disco duro, si deseamos continuar seleccionamos YES.
6. No seleccionar la opción de consola ya que no es necesaria para esta instalación.

7. Asignar la dirección IP 192.168.2.62/26 en la ventana de configuración considerando que es la dirección ip que trabajará como puerta de enlace a la red LAN.
8. Una vez instalado aparecerá la ventana principal de endian, donde se puede apreciar las configuraciones efectuadas para la red LAN (Zona Verde) y opciones de forma general para trabajar desde el Shell de Endian. En este paso aún no podemos acceder desde el navegador vía web ya que falta la configuración inicial.
9. Desde cualquier computador de la red LAN ingresar a la dirección https://192.168.2.62:10443 para realizar la configuración inicial, en la primera pantalla agregar el certificado SSL al navegador WEB.
10. En la ventana de interfaz gráfica de bienvenida presionar >>>> que significa siguiente
11. Seleccionar Idioma de la Interfaz Gráfica y Aceptar Términos y Condiciones.
12. No restaurar desde Backups a menos que sea una instalación que posea dicho archivo.
13. Establecer credenciales tanto para el súper usuario root como para el usuario admin.

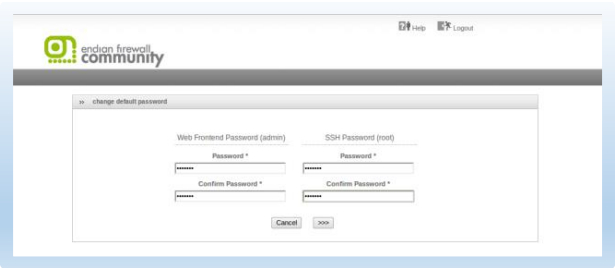


Figura 5.1 Ventana de Credenciales

14. Definimos como Modo de Red “Enrutamiento” y Tipo de Enlace “Ethernet Estático”

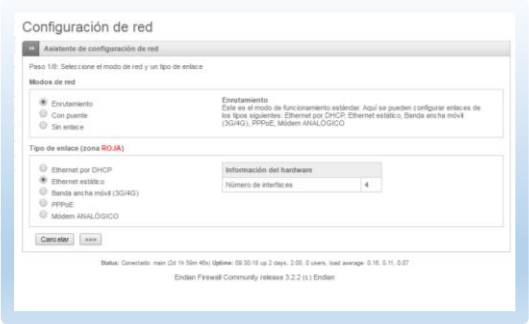


Figura 5.2 Modo de Red y Tipo de Enlace

15. Definir las Ip de Puerta de enlace correspondiente a cada zona de la siguiente manera:

    Verde: Ya definida previamente en la instalación – 192.168.2.62

    Naranja: 172.16.100.30

    Azul: 172.16.200.30

    Roja: 192.168.0.2

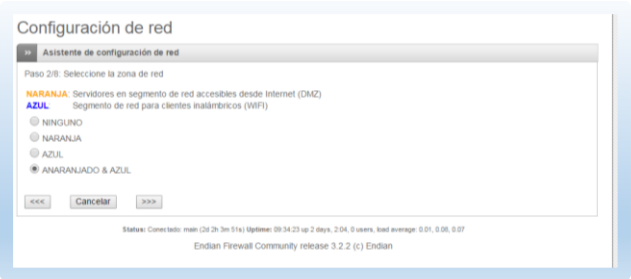


Figura 5.3 Zonas Endian

16. Configurar los siguientes DNS: 210.193.100.138 y 210.193.100.151 y dar clic en siguiente hasta finalizar la configuración, esperar aproximadamente

60 segundos y se presentará la Interfaz Gráfica de Administración Principal de Endian Firewall, como se muestra en el Anexo “H”.

5.2. SEGMENTACIÓN Y RESTRUCTURACIÓN DE RED

Para la Segmentación de la Red considerando el levantamiento de información ejecutado anteriormente, se coordina con la empresa TELCONET el cambio de las redes en todos sus Routers, después de esto se procede a definir las cuatro zonas que permite configurar la herramienta Endian:

Zona Verde: La red a utilizar en esta zona es 192.168.2.0/26 y se asigna a la interfaz física eth0.

Figura 5.4 Zona Verde

La Distribución de direcciones IP en la LAN queda de la siguiente manera:

Tabla 27 Asignación de Direcciones IP Zona Verde

Rango de Direcciones	Asignación
192.168.2.1-192.168.2.20	Equipos de Administración Interna y Computadores de Usuarios
192.168.2.21-192.168.2.30	Disponibles para PC
192.168.2.31-192.168.2.50	Teléfonos IP
192.168.2.52-192.168.2.61	Disponibles Rango para Servicio DHCP

Zona Naranja: para esta zona se crea una VLAN con ID 100 con la red 172.16.100.0/27 en la interfaz física eth01.

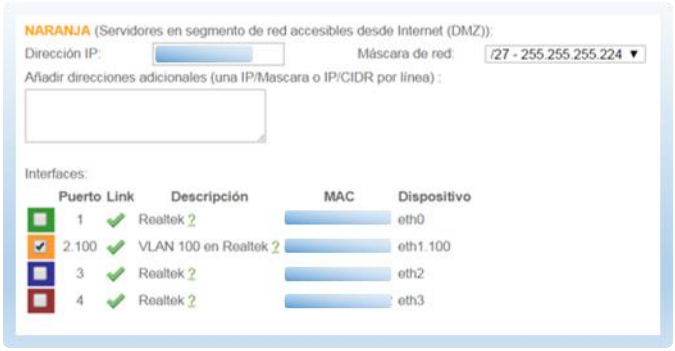


Figura 5.5 Zona Naranja

Zona Azul: para esta zona se asigna la red 172.16.200.0/27 en la interfaz física eth2.

Figura 5.6 Zona Azul

Zona Roja: en esta zona se considera la ip 192.168.0.2/30 que enlaza con el router del ISP, en la interfaz física eth3, donde se dispone de acceso al pool de direcciones IP públicas A, B, C, D. Por esta interfaz también estará configurada la red VPN 10.20.30.0/26 y el acceso de todas las Sucursales que tienen enlace de datos.

Figura 5.7 Zona Roja WAN

5.3. CONTROL DE TRÁFICO

Una vez configurado endian con su funcionalidad básica se procede a ubicarlo en la red, para realizar cambios paulatinamente en las reglas de control de tráfico respectivas. Para que no haya interrupción en la labor diaria de la empresa este trabajo se realiza en la noche, empezando con la ubicación de los servidores en su respectiva zona con accesos abiertos aun sin ningún control de tráfico, en especial usando la opción NAT del firewall, con el objetivo que para el usuario sea trasparente el uso de los servicios de PAC y telefonía IP a sus respectivas IP Públicas.

Una vez ubicado el UTM y funcionando sin problemas se procede a realizar la configuración de listas de control de acceso en endian, utilizando la opción de Firewall que trae el UTM, por medio de este servicio se configura los permisos del tráfico dentro de la red de la empresa, los módulos disponibles son:

- El reenvió de puertos/NAT
- Tráfico Enrutado de entrada
- Tráfico entre zonas
- Tráfico VPN

- Tráfico de Acceso al Sistema

Para a configuración de los diferentes módulos se debe tener las siguientes consideraciones globales:

- Las reglas que se definan aquí se convertirán en comandos IPTABLES del Sistema de forma organizada, para la interoperabilidad de las redes registradas en el UTM.
- Conocer cuál es la fuente y el destino del tráfico (Cualquiera, IP, RED, Rango de IP, MAC, ZONA, Interfaz, Usuario VPN, Enlace Activo)
- Conocer el servicio, puerto o protocolo a usar en las diferentes reglas.
- Conocer que política se utilizará, siendo estas permitir, permitir con IPS, rechazar o denegar.
- Habilitar o deshabilitar la regla.
- El registro de todos los paquetes esta deshabilitado por default, ya que solo registra solo los paquetes filtrados dependiendo la regla, no es recomendable habilitar esta opción ya que el tamaño de archivos de registro aumentará rápidamente.
- Todas las reglas tienen un campo de observación donde se puede especificar en resumen que hace dicha implementación.
- La posición de las reglas es importante ya que las iptables se procesan en el orden que aparece en las listas, es decir la regla 1 se aplicará primero que la regla 2, e inclusive anulará a la regla 2 si existe una denegación por parte de la regla precedente, y así sucesivamente con las demás regla.

- Las acciones que Endian UTM nos permite son: Mover, Activar/Desactivar, Modificar y eliminar Reglas.
- Ningún tráfico permitido, será bloqueado automáticamente por el firewall sin necesidad de especificar la regla, a menos que sea necesario especificar para permisos especiales del firewall.
- Una vez hecho los cambios el firewall debe ser reiniciado, pero para esto está el botón aplicar que lo hace automáticamente, caso contrario la regla no se aplicará.

5.3.1. REDIRECCIÓN DE PUERTOS/ NAT DESTINO

Tomando en cuenta la recomendación general y el levantamiento de información del numeral 4.3.2 del Diseño del Control de tráfico, se configura la siguientes Reglas con el respectivo orden de prioridad:

Posición de Regla: Primera

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a la empresa EQUIFAX para la manipulación del WebService cuando fuere necesario.

Parámetros Generales:

En esta regla se define como IP entrante las de la Empresa EQUIFAX para la utilización del WebService instalado en Server PAC.

Dirección IP Pública Local de entrada: A

Dirección IP Privada: 172.16.100.2

Puertos a usar: TCP: 80 y 443.

Política de Filtrado: Permitir con IPS

Habilitación de Log: SI

Activada: SI

Observación: Acceso Equifax a Sistema PAC

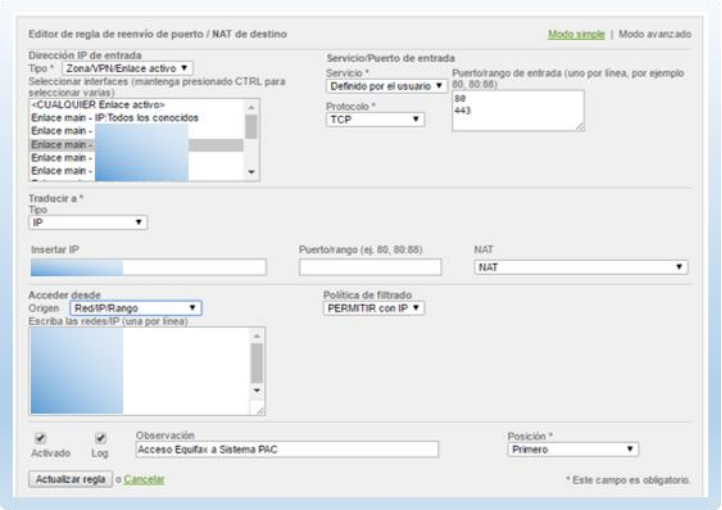


Figura 5.8 Primera Regla NAT Destino

Posición de Regla: Segunda

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a la IP Pública de la Sucursal Santa Elena, para cualquier computador que quiera acceder al PAC desde la misma.

Parámetros Generales:

En esta regla se define como direcciones IP entrantes la X y la Y de las sucursales de Santa Elena.

Dirección IP Pública Local de entrada: A

Dirección IP Privada: 172.16.100.2

Puertos a usar: Externo e Interno TCP: 80

Política de Filtrado: Permitir con IPS

Habilitación de Log: SI

Activada: SI

Observación: Acceso Santa Elena a Sistema PAC

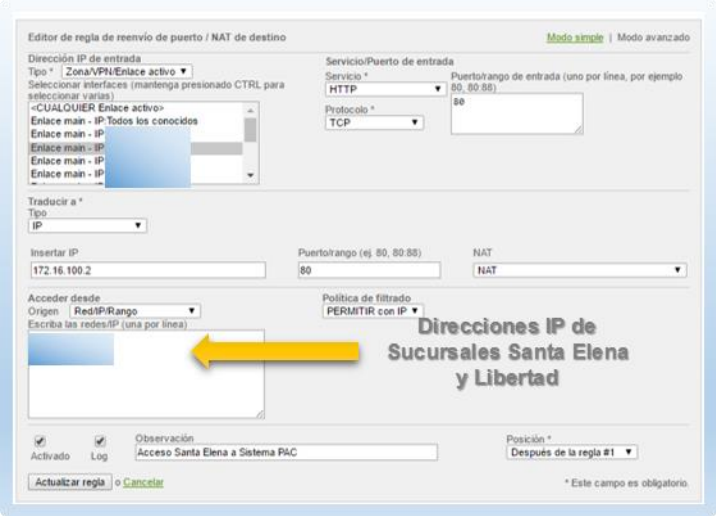


Figura 5.9 Segunda Regla NAT Destino

Posición de Regla: Tercera

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a los servicios de telefonía IP de la Empresa.

Parámetros Generales:

En esta regla se define como direcciones IP entrantes la X y la Y de las sucursales de Santa Elena.

Dirección IP Pública Local de entrada: C

Dirección IP Privada: 172.16.100.4

Puertos a usar: TCP y UDP: 5000-5500, 10000-20000, 8000, 3478.

Política de Filtrado: Permitir con IPS

Habilitación de Log: SI

Activada: SI

Observación: Acceso a Servidor IP Elastix desde WAN

Figura 5.10 Tercera Regla NAT Destino

Posición de Regla: Cuarta a Diecisiete

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso para visualizar cámaras IP de forma independiente, desde un equipo remoto. Ubicado fuera del Internet de la Empresa.

Parámetros Generales:

En esta regla se define como IP entrante: Z.

Dirección IP Pública Local de entrada: D

Dirección IP Privada: 172.16.200.4, 172.16.200.5, 172.16.200.6, 192.168.1.6, 192.168.1.7, 192.168.1.8, 192.168.1.9, 192.168.13.3, 192.168.13.5, 192.168.13.6, 192.168.13.7, 192.168.16.2, 192.168.16.3, y 192.168.16.5.

Puertos a usar: Externo TCP: 9012- 9044, Interno TCP: 80.

Política de Filtrado: Permitir con IPS

Habilitación de Log: NO necesario

Activada: SI

Observación: Cámara + Sucursal + Número de Identificación.

Figura 5.11 Reglas 4 a 17 NAT Destino

5.3.2. TRÁFICO DE ENRUTADO DE ENTRADA

Tomando en cuenta la recomendación general y el levantamiento de información del numeral 4.3.2 del Diseño del Control de tráfico, una vez coordinado con TELCONET el cambio de las redes de las sucursales, se configura la siguientes Reglas con el respectivo orden de prioridad:

Posición de Regla: Primera

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso desde las Sucursales al Servicio de Telefonía IP por Intranet.

Parámetros Generales:

En esta regla se define como Redes entrantes a: 192.168.1.0/28, 192.168.13.0/28, 192.168.14.0/28 y 192.168.17.0/28.

Dirección IP Destino: 172.16.100.4

Puertos a usar: TCP y UDP: 5000-5500, 10000-20000, 8000, 3478.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a Servidor IP Elastix desde Sucursales.

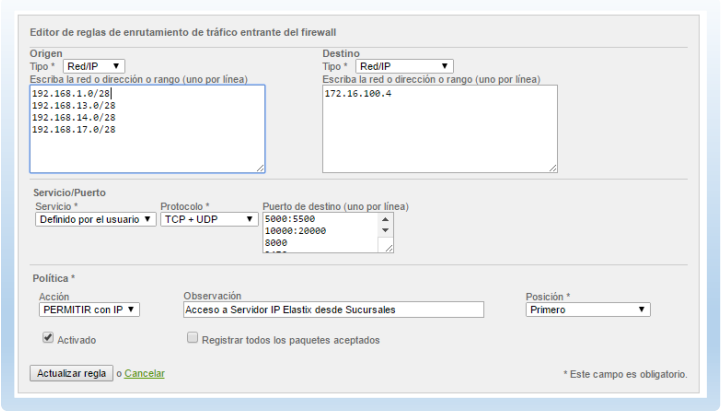


Figura 5.12 Primera Regla Tráfico Entrante

Posición de Regla: Segunda

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso desde las Sucursales al Sistema PAC y a su servicio de impresión.

Parámetros Generales:

En esta regla se define como Redes entrantes a: 192.168.1.0/28, 192.168.11.0/28, 192.168.12.0/28 y 192.168.13.0/28.

Dirección IP Destino: 172.16.100.2

Puertos a usar: TCP: 80, 139 y 445

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a PAC y Servicio de Impresión

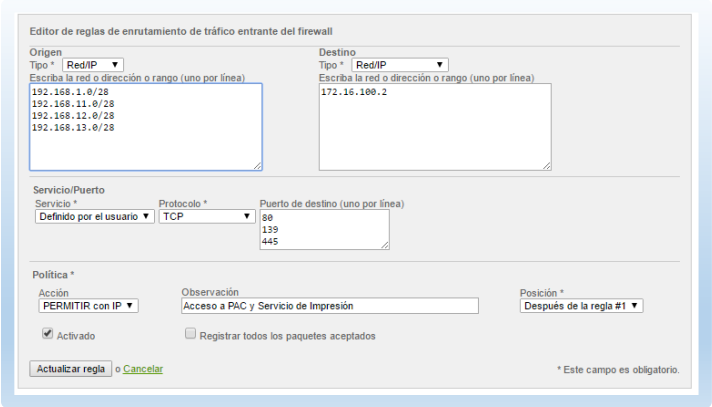


Figura 5.13 Segunda Regla Tráfico Entrante

Posición de Regla: Tercera

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso desde las Sucursales al Servidor Active Directory, DNS y Archivos Compartidos.

Parámetros Generales:

En esta regla se define como Redes entrantes a: 192.168.1.0/28, 192.168.11.0/28, 192.168.12.0/28 y 192.168.13.0/28.

Dirección IP Destino: 172.16.100.5

Puertos a usar: TCP y UDP: 135, 1025, 1026, 53, 137, 138, 139, 88, 1801, 2101, 2103, 2105, 3527, 389, 119, 80, 443, 25, 224, 464, 500, 563, 593, 636, 3268, 3269, 5722, 123, 9389, 67, 2535 y 49152-65535.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a Server DNS-AD y Archivos Compartidos.

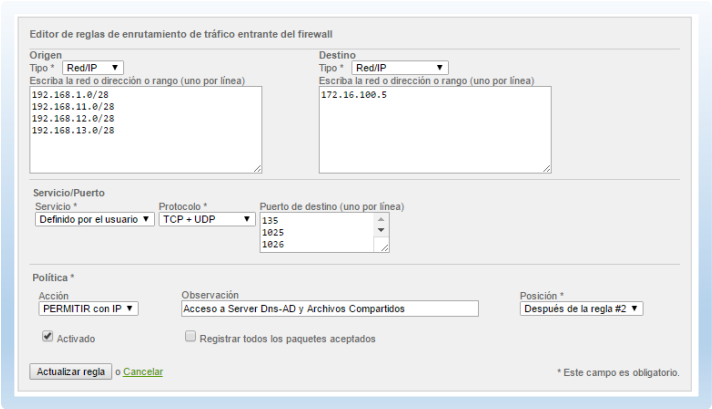


Figura 5.14 Tercera Regla Tráfico Entrante

5.3.3. TRÁFICO DE SALIDA

Tomando en cuenta la recomendación general y el levantamiento de información del numeral 4.3.2 del Diseño del Control de tráfico, se configura la siguientes Reglas con el respectivo orden de prioridad:

Posición de Regla: Primera

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso al computador que usa el administrador de la red de la empresa, hacia las sucursales con enlace de datos (Intranet), esta regla tiene la particularidad que solo debe ser habilitada de forma manual cuando el

administrador necesita hacer algún trabajo en sucursales, caso contrario estará por defecto inhabilitada.

Parámetros Generales:

En esta regla se define MAC Origen: MAC Administrador.

Direcciones IP Destino: 192.168.1.0/28, 192.168.11.0/28, 192.168.12.0/28, 192.168.12.0/28, 192.168.13.0/28, 192.168.14.0/28, 192.168.16.0/28, 192.168.17.0/28

Puertos a usar: Cualquiera.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: NO

Observación: Acceso Administrador de la Red a Sucursales.

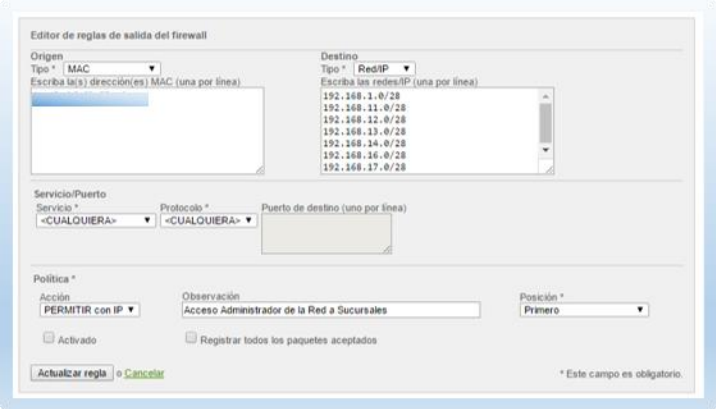


Figura 5.15 Primera Regla Tráfico de Salida

Posición de Regla: Segunda

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a Internet a equipos de matriz registrando sus direcciones MAC.

Parámetros Generales:

En esta regla se define MAC Origen: direcciones MAC autorizadas de matriz para salida de internet, esta MAC están registradas en el respectivo formato que se adjunta en el Anexo “F”.

Direcciones IP Destino: Salida a Internet Zona Roja

Puertos a usar: TCP: 80 y 443.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida Internet sin Proxy Matriz por MAC.

Figura 5.16 Segunda Regla Tráfico de Salida

Posición de Regla: Tercera

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a Internet a equipos de la sucursal Paraíso registrando sus direcciones ip.

Parámetros Generales:

En esta regla se define dirección IP origen: 192.168.13.9 y 192.168.13.10

Direcciones IP Destino: Salida a Internet Zona Roja

Puertos a usar: TCP: 80 y 443.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida Internet sin Proxy Paraíso.

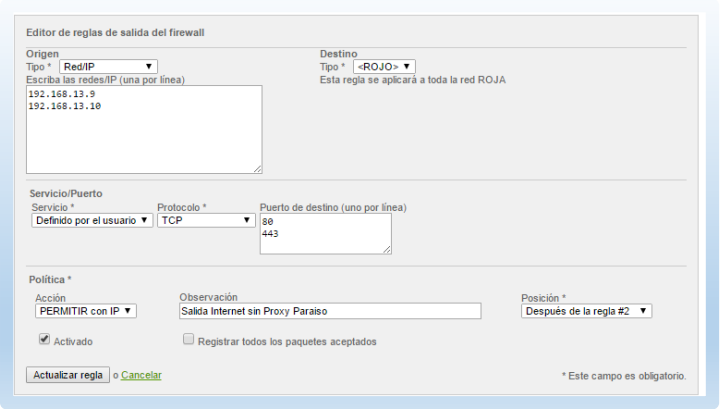


Figura 5.17 Tercera Regla Tráfico de Salida

Posición de Regla: Cuarta

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a Internet a equipos de la sucursal Balerio registrando sus direcciones IP.

Parámetros Generales:

En esta regla se define dirección IP origen: 192.168.1.10 y 192.168.1.11.

Direcciones IP Destino: Salida a Internet Zona Roja

Puertos a usar: TCP: 80 y 443.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida Internet sin Proxy Balerio.

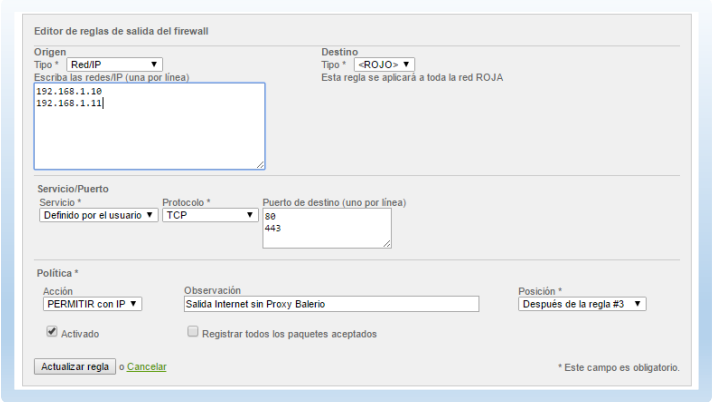


Figura 5.18 Cuarta Regla de Tráfico de Salida

Posición de Regla: Cinco

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a Internet a equipos de la sucursal San Francisco registrando sus direcciones IP.

Parámetros Generales:

En esta regla se define dirección IP origen: 192.168.12.10.

Direcciones IP Destino: Salida a Internet Zona Roja

Puertos a usar: TCP: 80 y 443.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida Internet sin Proxy San Francisco.

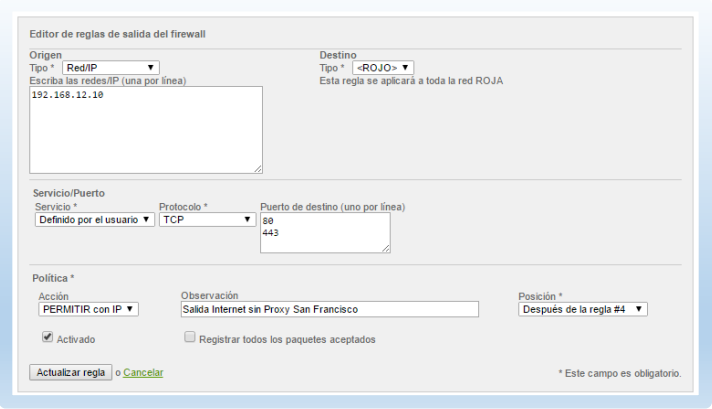


Figura 5.19 Quinta Regla de Tráfico de Salida

Posición de Regla: Sexta

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a Internet a un dispositivo router WIFI que permita navegar a personal que forma parte de reuniones e invitaciones de Gerencia. Para esta regla el dispositivo se lo ubica dentro de la red azul.

Parámetros Generales:

En esta regla se define dirección IP origen: 172.16.200.1

Direcciones IP Destino: Salida a Internet Zona Roja

Puertos a usar: TCP: 80 y 443.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida Internet sin Proxy Zona Azul.

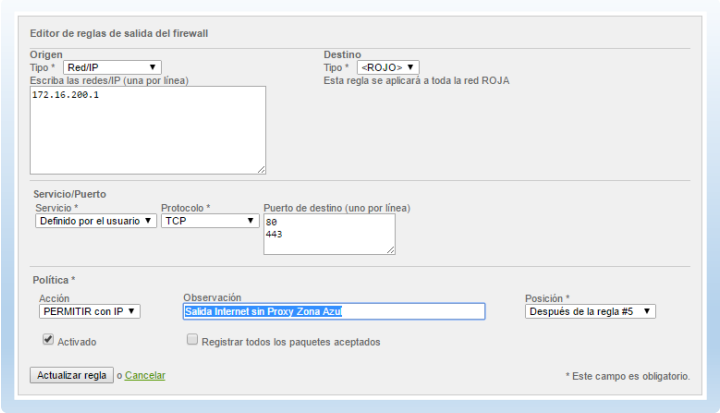


Figura 5.20 Sexta Regla de Tráfico de Salida

Posición de Regla: Séptima

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a WhatsApp a ciertos dispositivos de la red tanto en matriz como en sucursales.

Parámetros Generales:

En esta regla se define las siguientes direcciones IP origen: 192.168.1.10 y 192.168.1.11 (Sucursal Balerio), 192.168.12.10 (Sucursal San Francisco), 192.168.13.9 y 192.168.13.10 (Sucursal Paraíso)

Direcciones IP Destino: Salida a Internet Zona Roja

Puertos a usar: TCP y UDP: 5222, 5223, 5228, 5242 y 3478 para llamadas.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida solo WhatsApp incluido llamada (3478).

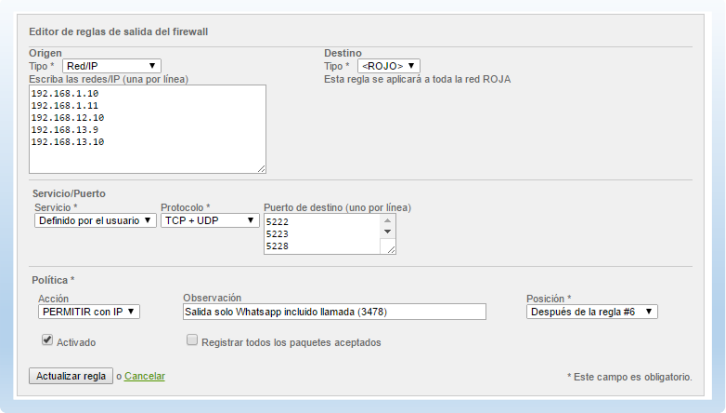


Figura 5.21 Séptima Regla de Tráfico de Salida

Posición de Regla: Octava

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso del Jefe de Recursos Humanos a todos equipos biométricos de las sucursales.

Parámetros Generales:

En esta regla se define las siguientes direcciones IP origen: 192.168.2.17

Direcciones IP Destino: 192.168.1.0/28, 192.168.11.0/28, 192.168.17.0/28 y X.

Puertos a usar: TCP: 5005.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a Biométricos de Sucursales desde Matriz.

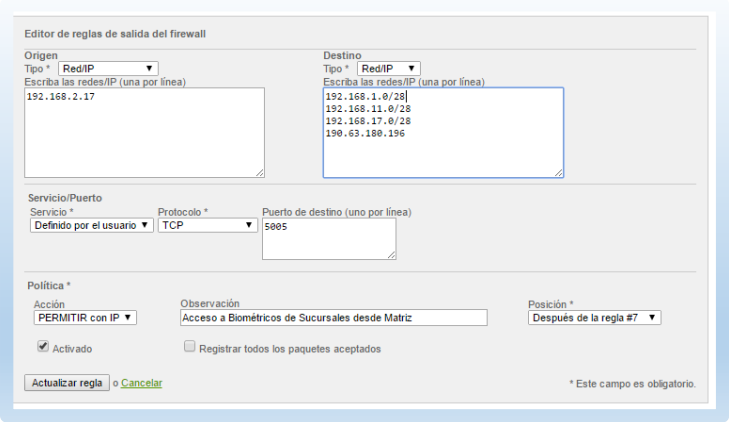


Figura 5.22 Octava Regla de Tráfico de Salida

Posición de Regla: Novena

Objetivo de Regla: El objetivo de esta regla es dar permiso de salida a cámaras de sucursal Santa Elena.

Parámetros Generales:

En esta regla se define la siguiente dirección IP origen: 192.168.2.51

Direcciones IP Destino: X.

Puertos a usar: TCP: 8090.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida a Cámaras Sucursal Santa Elena.

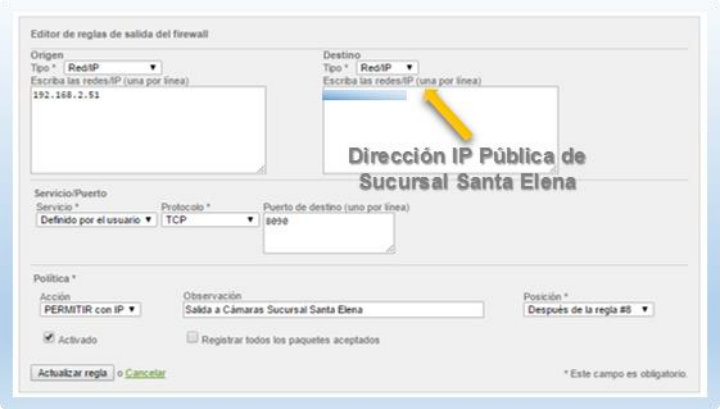


Figura 5.23 Novena Regla de Tráfico de Salida

Posición de Regla: Décima

Objetivo de Regla: El objetivo de esta regla es dar permiso de acceso a puertos de impresión usadas por el Servidor PAC, esta regla es necesaria para que haya respuesta de impresión en las diferentes sucursales, caso contrario no podrían imprimir.

Parámetros Generales:

En esta regla se define la siguiente dirección IP origen: 172.16.100.2

Direcciones IP Destino: 192.168.1.0/24, 192.168.11.0/28 y 192.168.12.0/28.

Puertos a usar: TCP y UDP: 139, 445.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso desde PAC a Sucursales Servidor de Impresión.

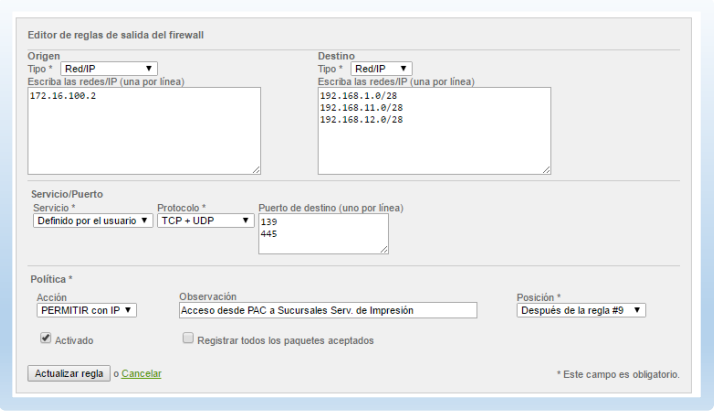


Figura 5.24 Décima Regla de Tráfico de Salida

Posición de Regla: Undécima

Objetivo de Regla: El objetivo de esta regla es dar permiso de salida a matriz y sucursales para salida a puertos de correo electrónico.

Parámetros Generales:

En esta regla se define la siguientes direcciones IP origen: 172.16.200.1, 192.168.2.0/26, 192.168.1.0/28, 192.168.11.0/28 y 192.168.12.0/28

Direcciones IP Destino: Internet Zona Roja.

Puertos a usar: TCP: 25, 26, 110, 143, 995, 993, 587, 465

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida a Correo Electrónico.

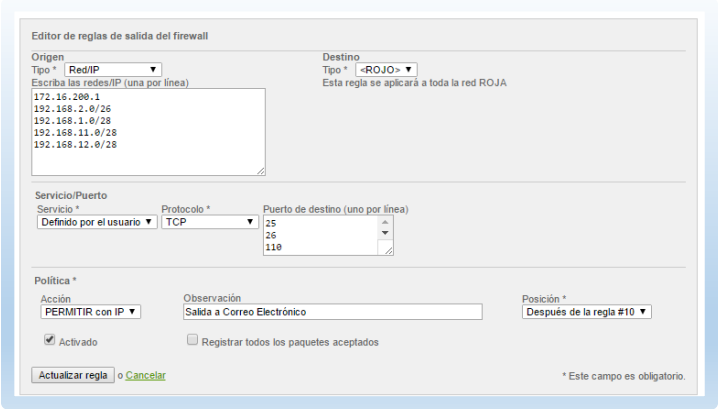


Figura 5.25 Undécima Regla de Tráfico de Salida

Posición de Regla: Duodécima

Objetivo de Regla: El objetivo de esta regla es dar permiso de salida a Servidor DNS solo a este servicio.

Parámetros Generales:

En esta regla se define la siguiente dirección IP origen: 172.16.100.5.

Direcciones IP Destino: Internet Zona Roja.

Puertos a usar: TCP y UDP: 53

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Salida a DNS.

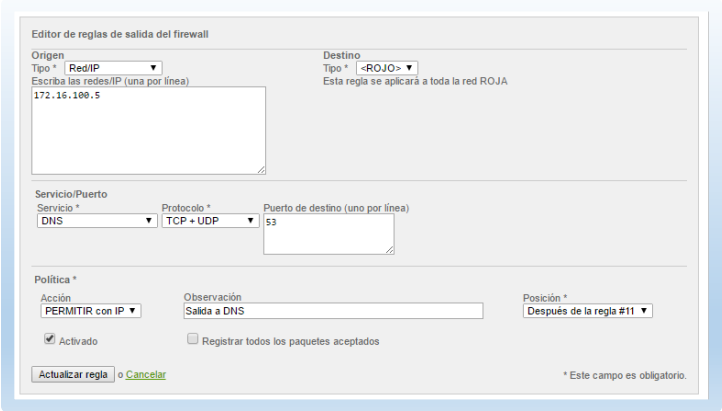


Figura 5.26 Duodécima Regla de Tráfico de Salida

Posición de Regla: Treceava

Objetivo de Regla: El objetivo de esta regla es bloquear el tráfico DNS para cualquier equipo de la red interna, con el fin de evitar que este puerto sea usado para DNS Spoofing o cualquier otro ataque.

Parámetros Generales:

En esta regla se define para cualquiera de la red como origen.

Direcciones IP Destino: Internet Zona Roja.

Puertos a usar: TCP y UDP: 53

Política de Filtrado: Denegar

Registrar Paquetes Aceptados: SI

Activada: SI

Observación: Bloqueo de Salida a DNS Toda la Red.

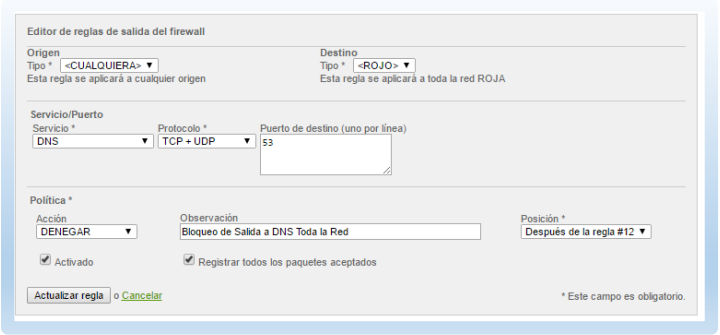


Figura 5.27 Treceava Regla de Tráfico de Salida

Posición de Regla: Catorceava

Objetivo de Regla: El objetivo de esta regla es bloquear el tráfico ICMP para cualquier equipo de la red interna, con el fin de evitar que este puerto sea usado para DOS o cualquier otro ataque que involucre a este protocolo.

Parámetros Generales:

En esta regla se define para cualquiera de la red como origen.

Direcciones IP Destino: Internet Zona Roja.

Puertos a usar: ICMP: 8 y 30

Política de Filtrado: Denegar

Registrar Paquetes Aceptados: SI

Activada: SI

Observación: Bloqueo de PING.

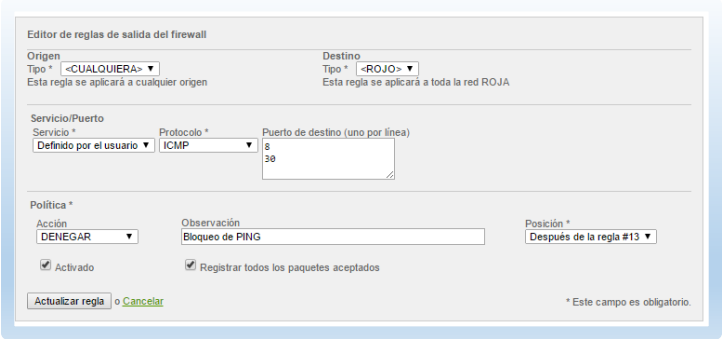


Figura 5.28 Catorceava Regla de Tráfico de Salida

Cabe indicar que endian bloquea automáticamente todo el tráfico que no se permita, pero existe una regla de excepción creada por el sistema que especifica el bloqueo ICMP, ya que endian lo tiene desbloqueado por default como se muestra en la siguiente figura.

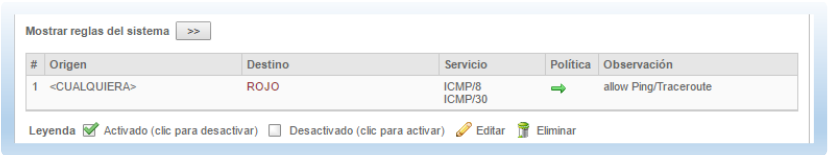


Figura 5.29 Regla por Default del Sistema para Tráfico de Salida

5.3.4. TRÁFICO ENTRE ZONAS (INTER-ZONA)

Tomando en cuenta la recomendación general y el levantamiento de información se procede a crear las siguientes reglas inter-zona:

Posición de Regla: Primera

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al administrador de la red a todas las zonas registrando la MAC de su equipo, esta regla se habilitará solo cuando fuere necesaria, ya que por defecto estará inhabilitada.

Parámetros Generales:

En esta regla se define la dirección MAC origen: MAC Administrador

Direcciones IP Destino: Zona Verde, Azul y Naranja

Puertos a usar: Cualquiera

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: NO

Observación: Administrador de la Red a Todas las Zonas.

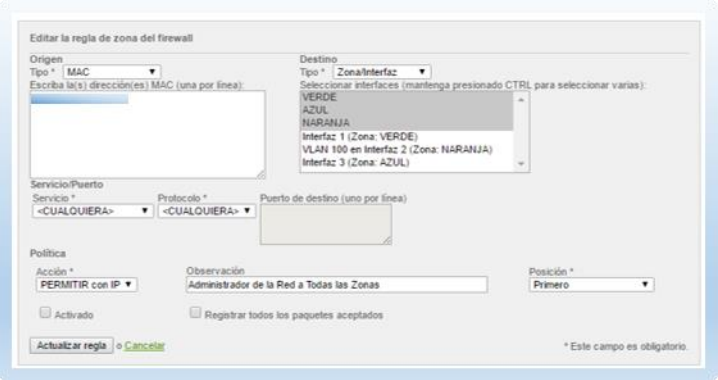


Figura 5.30 Primera Regla Inter-Zona

Posición de Regla: Segunda

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al encargado de visualizar las cámaras IP por medio de la MAC del respectivo equipo, utilizando el servicio de VNC.

Parámetros Generales:

En esta regla se define la dirección MAC origen: MAC administrador de cámaras

Dirección IP Destino: 172.16.200.11

Puertos a usar: TCP: 5800 y 5900

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a Cámaras de Vigilancia por VNC.

Figura 5.31 Segunda Regla de Tráfico Inter-zona

Posición de Regla: Tercera

Objetivo de Regla: El objetivo de esta regla es permitir el acceso a los servicios de impresión desde el Sistema PAC hacia las IP de los equipos que imprimen por medio de este servicio, ya que si no existe esta regla no podrían imprimir.

Parámetros Generales:

En esta regla se define la dirección IP origen: 172.16.100.2

Direcciones IP Destino: 192.168.2.13 y 192.168.2.15

Puertos a usar: TCP y UDP: 139 y 445

Política de Filtrado: Permitir

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso PAC a Equipos con Servicio de Impresión.

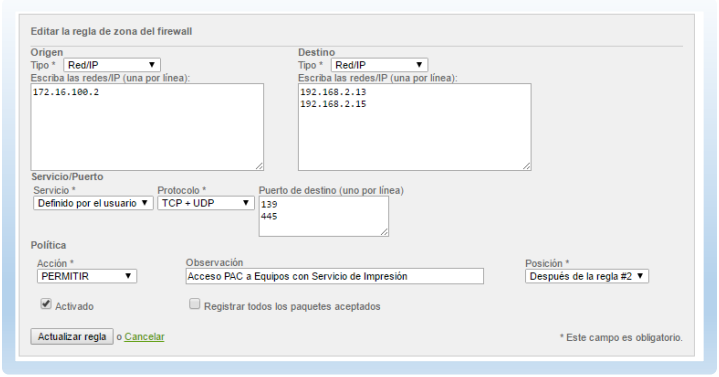


Figura 5.32 Tercera Regla de Tráfico Inter-zona

Posición de Regla: Cuarta

Objetivo de Regla: El objetivo de esta regla es permitir el acceso a los servicios de impresión desde las pc que requieren este servicio de impresión hacia el Sistema PAC, ya que si no existe esta regla no podrían imprimir.

Parámetros Generales:

En esta regla se define las direcciones IP origen: 192.168.2.13 y 192.168.2.15

Direcciones IP Destino: 172.16.100.2

Puertos a usar: TCP y UDP: 139 y 445

Política de Filtrado: Permitir

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso desde Equipos a PAC-Servicio de Impresión.

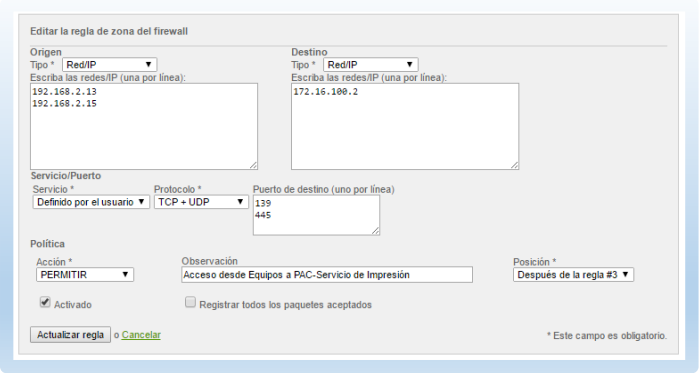


Figura 5.33 Cuarta Regla de Tráfico Inter-zona

Posición de Regla: Quinta

Objetivo de Regla: El objetivo de esta regla es permitir el acceso vía Web al sistema Financiero PAC desde la zona verde y del dispositivo WIFI de reuniones.

Parámetros Generales:

En esta regla se define las direcciones IP origen: 192.168.2.0/26 y 172.16.200.1.

Direcciones IP Destino: 172.16.100.2

Puertos a usar: TCP: 80

Política de Filtrado: Permitir

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a PAC vía Web.

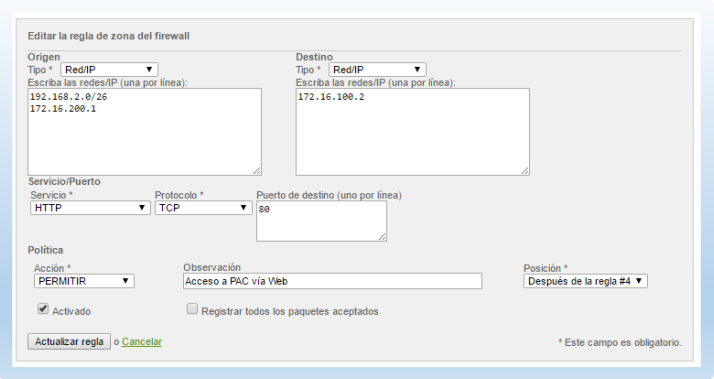


Figura 5.34 Quinta Regla de Tráfico Inter-zona

Posición de Regla: Sexta

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al servidor DNS, desde las zonas VERDE, AZUL y NARANJA.

Parámetros Generales:

En esta regla se define las zonas de origen: VERDE, AZUL y NARANJA.

Direcciones IP Destino: 172.16.100.5

Puertos a usar: TCP y UDP: 53

Política de Filtrado: Permitir

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Todas las Zonas de Red a Servidor DNS Interno.

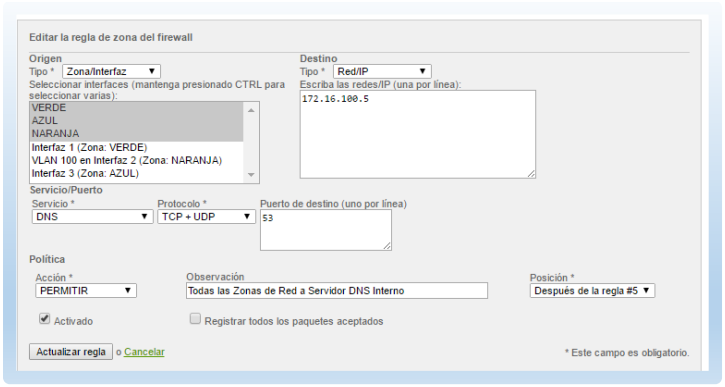


Figura 5.35 Sexta Regla de Tráfico Inter-zona

Posición de Regla: Séptima

Objetivo de Regla: Permitir el acceso a los teléfonos ip de la red LAN.

Parámetros Generales:

En esta regla se define la red de origen: 192.168.2.0/26

Dirección IP Destino: 172.16.100.4

Puertos a usar: TCP y UDP: 5060:5500, 10000:20000, 8000, 3478.

Política de Filtrado: Permitir

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a Server IP Matriz.

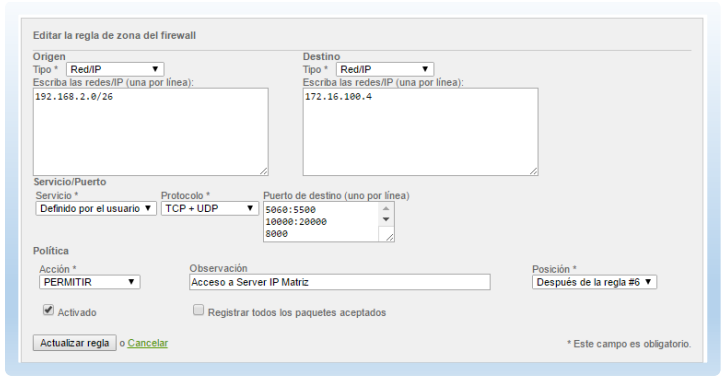


Figura 5.36 Séptima Regla de Tráfico Inter-zona

Posición de Regla: Octava

Objetivo de Regla: El objetivo de esta regla es permitir el acceso desde las zonas naranja y verde hacia los servicios de Active Directory, DNS y archivos compartidos.

Parámetros Generales:

En esta regla se define las zonas de origen: VERDE, AZUL y NARANJA.

Dirección IP Destino: 172.16.100.5

Puertos a usar: TCP y UDP: 135, 1025, 1026, 53, 137, 138, 139, 88, 1801, 2101, 2103, 2105, 3527, 389, 119, 80, 443, 25, 224, 464, 500, 563, 593, 636, 3268, 3269, 5722, 123, 9389, 67, 2535 y 49152-65535.

Política de Filtrado: Permitir

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso Verde y Naranja a AD y Archivos Compartidos.

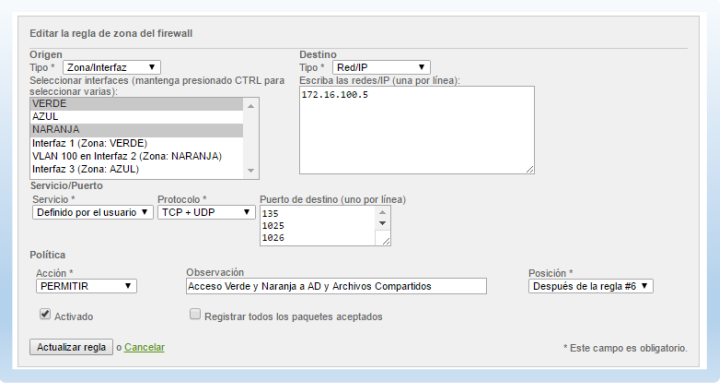


Figura 5.37 Octava Regla de Tráfico Inter-zona

5.3.5. TRÁFICO VPN

Tomando en cuenta la recomendación general y el levantamiento de información se procede a crear las siguientes reglas VPN donde intervienen los usuarios que necesitan acceder remotamente a los servicios de la empresa de una forma mucho más segura, para esto se configura el servicio OpenVPN del UTM Endian con las siguientes reglas:

Posición de Regla: Primera

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al servicio de impresión desde los usuarios VPN de Santa Elena y Libertad hacia el servidor PAC.

Parámetros Generales:

En esta regla se define como origen los usuarios VPN de las sucursales Santa Elena y Libertad.

Dirección IP Destino: 172.16.100.2

Puertos a usar: TCP y UDP: 139 y 445

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a PAC Servicio de Impresión.

Figura 5.38 Primera Regla de Tráfico VPN

Posición de Regla: Segunda

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al sistema PAC vía web desde los usuarios VPN.

Parámetros Generales:

En esta regla se define como origen los usuarios VPN necesarios con permisos de acceso al Sistema Financiero PAC.

Dirección IP Destino: 172.16.100.2

Puertos a usar: TCP: 80

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a PAC vía Web.

Figura 5.39 Segunda Regla de Tráfico VPN

Posición de Regla: Tercera

Objetivo de Regla: El objetivo de esta regla es permitir el acceso a las Cámaras IP de forma individual para el Gerente General.

Parámetros Generales:

En esta regla se define como origen el usuario VPN del Gerente General

Direcciones IP Destino: 172.16.200.4, 172.16.200.5, 172.16.200.6, 192.168.1.6, 192.168.1.7, 192.168.1.8, 192.168.1.9, 192.168.13.3, 192.168.13.4, 192.168.13.6, 192.168.13.7, 192.168.16.2, 192.168.16.3, 192.168.16.5.

Puertos a usar: TCP: 80.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso Cámaras IP.

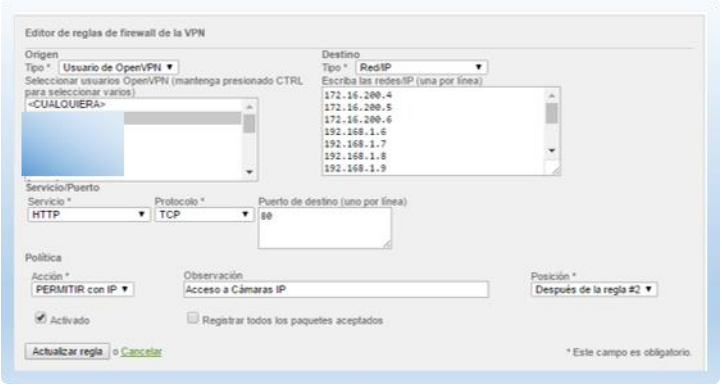


Figura 5.40 Tercera Regla de Tráfico VPN

Posición de Regla: Cuarta

Objetivo de Regla: El objetivo de esta regla es permitir el acceso a todo el tráfico de la red al Ing. Guido Miguez para Soporte de UTM y Redes por medio de un usuario VPN. Esta regla por defecto esta deshabilitada hasta que sea necesaria su activación por parte del administrador de la red de la empresa.

Parámetros Generales:

En esta regla se define como origen al usuario VPN del Ing. Guido Miguez.

Direcciones IP Destino: 192.168.2.0/26, 172.16.100.0/27, 172.16.200.0/27, 192.168.1.0/24, 192.168.6.0/28, 192.168.7.0/28, 192.168.11.0/28, 192.168.12.0/28, 192.168.13.0/28, 192.168.14.0/28, 192.168.16.0/28, 192.168.17.0/28, 10.20.30.0/26, 0.0.0.0/0

Puertos a usar: Cualquiera

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: NO

Observación: Acceso Ing. Guido Miguez.

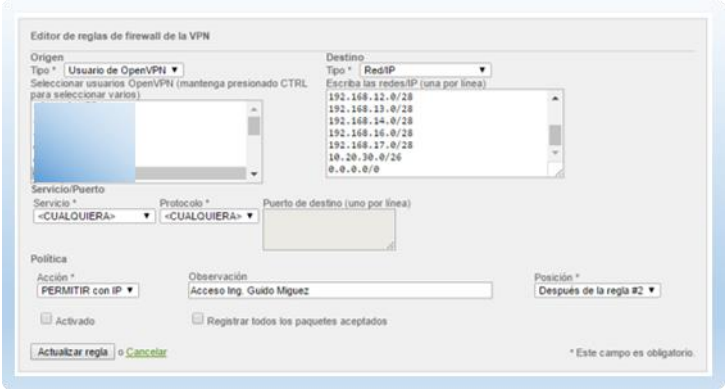


Figura 5.41 Cuarta Regla de Tráfico VPN

Posición de Regla: Quinta

Objetivo de Regla: El objetivo de esta regla es permitir que el servidor VPN pueda responder a la petición de impresión del sistema PAC con los usuarios VPN, sin esta regla no se puede imprimir.

Parámetros Generales:

En esta regla se define como origen la IP: 172.16.100.2.

Destino: Servidor OpenVPN Default

Puertos a usar: TCP y UDP: 139 y 445.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: PAC a OpenVPN (Impresoras).

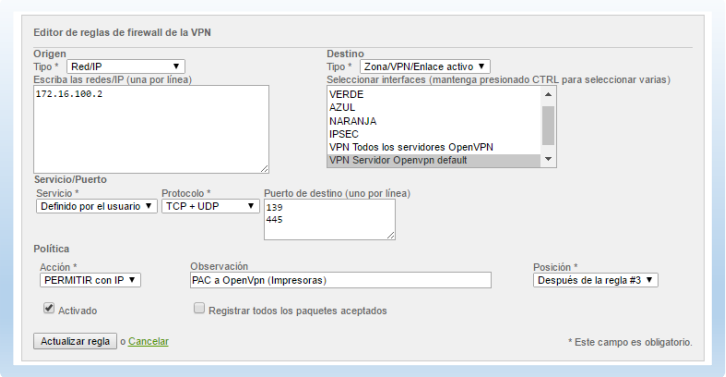


Figura 5.42 Quinta Regla de Tráfico VPN

Posición de Regla: Sexta

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al Gerente General para visualizar los reportes y grabaciones del servidor de telefonía IP.

Parámetros Generales:

En esta regla se define como origen al usuario VPN del Gerente General.

Destino: 172.16.100.4

Puertos a usar: TCP: 80 y 443.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a reportes y grabaciones en Elastix.

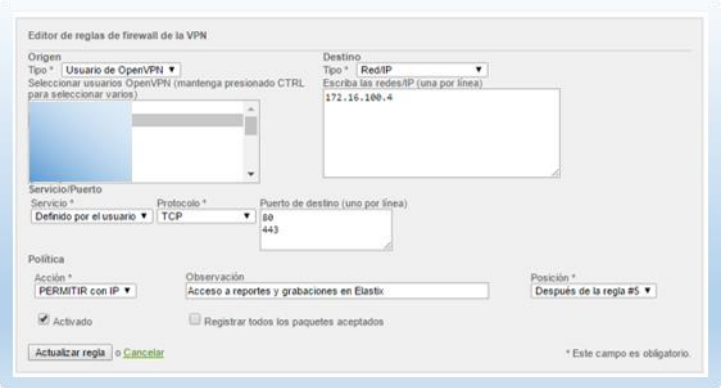


Figura 5.43 Sexta Regla de Tráfico VPN

Posición de Regla: Séptima

Objetivo de Regla: El objetivo de esta regla es permitir el acceso a los usuarios VPN para realizar llamadas IP fuera de la empresa.

Parámetros Generales:

En esta regla se define como origen al usuario VPN del Gerente General.

Destino: 172.16.100.4

Puertos a usar: TCP y UDP: 5060:5500, 10000:20000, 8000 y 3478.

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Permiso de usuarios VPN para llamadas IP.

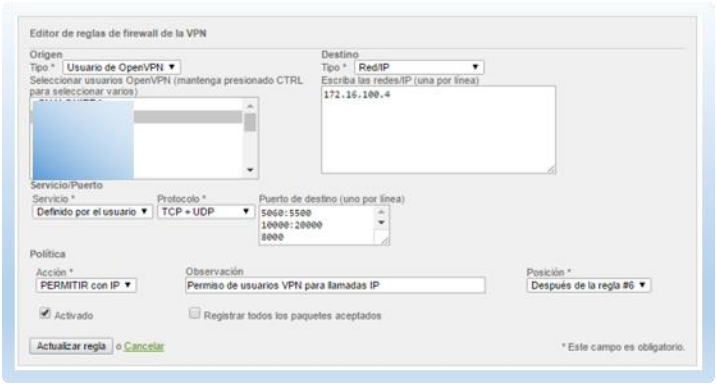


Figura 5.44 Séptima Regla de Tráfico VPN

En el tráfico VPN existe una regla que forma parte del sistema que bloquea el tráfico DHCP como se muestra en la siguiente figura:

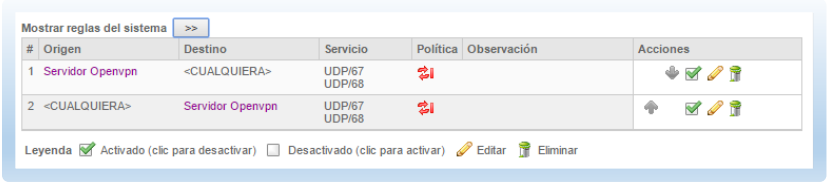


Figura 5.45 Reglas del Sistema para Tráfico VPN

5.3.6. TRÁFICO DE ACCESO AL SISTEMA

En esta sección se configura todos los puertos, zonas y direcciones IP que tengan que interactuar con el Endian UTM, tomando en cuenta que este dispositivo es el primer filtro de seguridad después del Router del ISP, considerando las interfaces de entrada del tráfico:

Posición de Regla: Primera

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al servidor OpenVPN de cualquier lugar del mundo por medio de Internet hacia la IP B, habilitando solamente el respectivo puerto.

Parámetros Generales:

En esta regla se define como origen: Cualquier red de Internet.

Interfaz de Origen: B

Puertos a usar: UDP: 1194

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: SI

Activada: SI

Observación: Acceso a Servidor OpenVPN de Endian.

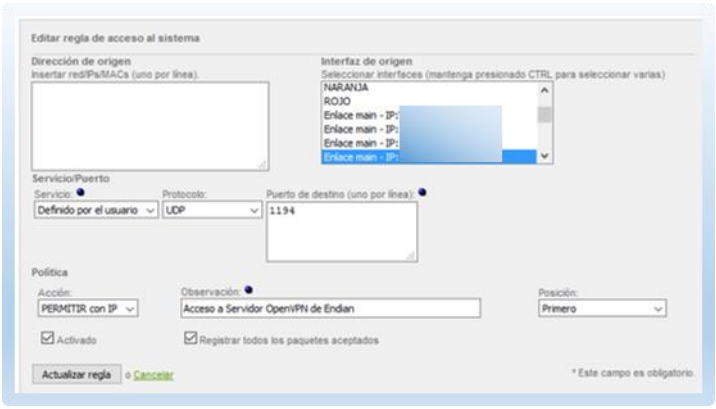


Figura 5.46 Primera Regla de Acceso al Sistema

Posición de Regla: Segunda

Objetivo de Regla: El objetivo de esta regla es permitir el acceso a la administración del UTM por parte del Administrador de la Red de la Empresa por medio de la Intranet.

Parámetros Generales:

En esta regla se define como origen la MAC: MAC administrador.

Interfaz de Origen: Interfaz de zona verde

Puertos a usar: TCP: 10443 y 443

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: SI

Activada: SI

Observación: Permisos de Administración desde Intranet.

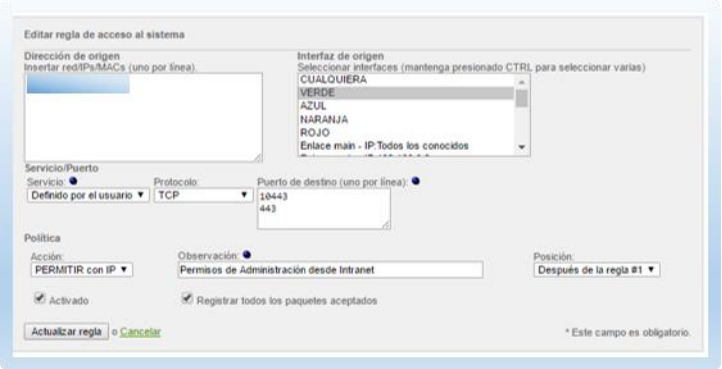


Figura 5.47 Segunda Regla de Tráfico de Acceso al Sistema

Posición de Regla: Tercera

Objetivo de Regla: El objetivo de esta regla es permitir el acceso a la administración del UTM desde Internet, por medio de la IP asignada al usuario VPN.

Parámetros Generales:

En esta regla se define como origen: 10.20.30.3

Interfaz de Origen: VPN Server Default

Puertos a usar: TCP: 10443 y 443

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: SI

Activada: SI

Observación: Acceso solo a Endian desde Internet.

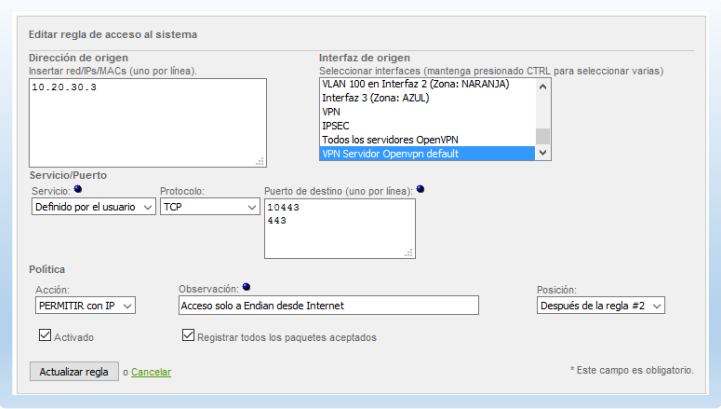


Figura 5.48 Tercera Regla de Tráfico de Acceso al Sistema

Posición de Regla: Cuarta

Objetivo de Regla: El objetivo de esta regla es permitir el acceso al Proxy del UTM Endian por parte de las sucursales, utilizando el puerto definido en su respectiva configuración.

Parámetros Generales:

En esta regla se define como origen las siguientes direcciones IP: 192.168.1.0/24, 192.168.11.0/28, 192.168.12.0/28 y 192.168.13.0/28.

Interfaz de Origen: Interfaz de zona roja

Puertos a usar: TCP: 3128

Política de Filtrado: Permitir con IPS

Registrar Paquetes Aceptados: NO

Activada: SI

Observación: Acceso a Puerto Proxy desde Sucursales.

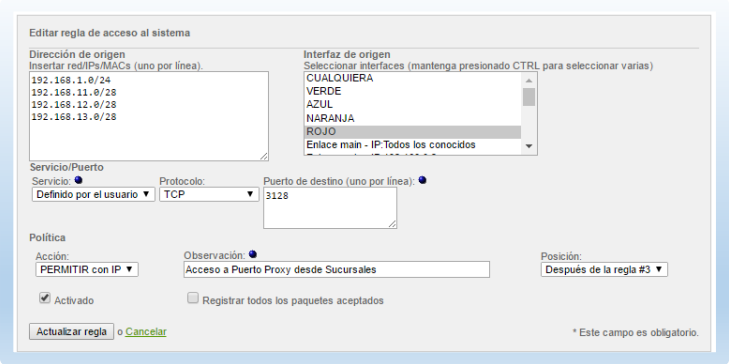


Figura 5.49 Cuarta Regla de Tráfico de Acceso al Sistema

Posición de Regla: Quinta

Objetivo de Regla: El objetivo de esta regla es bloquear el acceso a cualquier otro puerto no permitido en el UTM endian, ya que en el sistema por defecto vienen ciertos puertos habilitados como se muestra en la siguiente imagen:

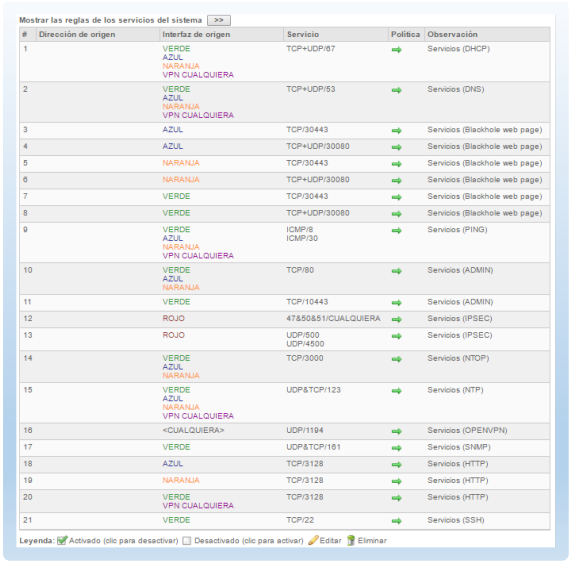


Figura 5.50 Reglas por defecto de Tráfico Acceso al Sistema

Parámetros Generales:

En esta regla se define como origen: Cualquier Red.

Interfaz de Origen: Interfaz de zona roja

Puertos a usar: Cualquiera

Política de Filtrado: Denegar

Registrar Paquetes Aceptados: SI

Activada: SI

Observación: Bloqueo Total.

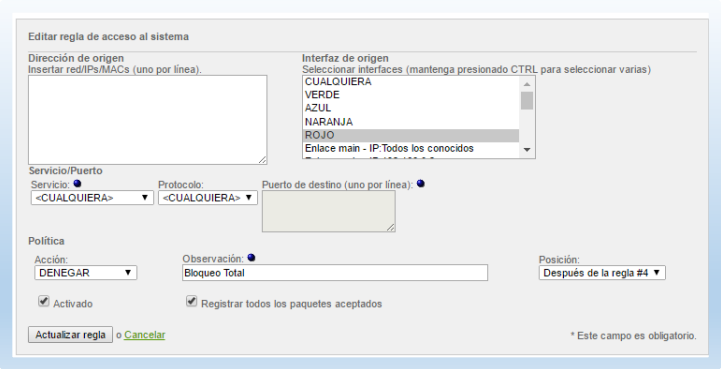


Figura 5.51 Quinta Regla de Tráfico de Acceso al Sistema

5.3.7. TRÁFICO DE PROXY HTTP

En esta sección se configura las reglas que se aplicarán a los equipos que naveguen a través del proxy, este servicio es parte del UTM. La configuración es la siguiente:

Proxy tipo No Trasparente para todas las zonas

Acceso por medio del puerto 3128.

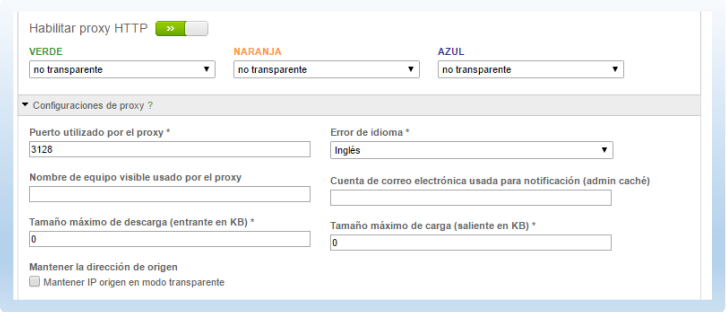


Figura 5.52 Configuración de Acceso a Proxy HTTP

Puertos Permitidos (desde cliente), por defecto: 80 # http, 21 # ftp, 70 # gopher, 210 # wais, 1025-65535. 280 # http-mgmt, 488 # gss-http, 591 # filemaker, 777 # multiling http, 800 # Squid (for icons)

Asignados por el Usuario según levantamiento de Información: 88 # Cartimex, 2096 # Webmail, 25 # correo, 26 # correo, 110 # correo, 995 # correo, 993 # correo, 143 # correo, 587 # correo, 8080 # factel1, 8087 # factel, 8084 # facmavesa

Puertos SSL Permitidos (desde el cliente), por defecto: 443 # https, 563 # snews, 3001 # ntop. Definidos por el usuario: 5938 # Teamviewer, 2096 # Webmail, 2083 # Cpanel, 8084 # facmavesa, 25 # correo, 26 # correo, 995 # correo, 993 # correo, 143 # correo, 587 # correo.

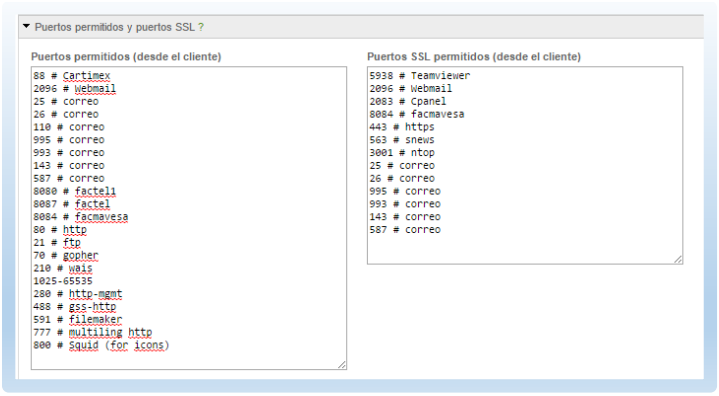


Figura 5.53 Puertos Permitidos por el Proxy

Habilitar Registro del Proxy HTTP, y administrar la cache con 4096MB del tamaño en cache del disco duro, 512MB Tamaño del cache en la memoria, 204800KB tamaño máximo de objeto, 0KB tamaño mínimo de Objeto, y activar modo sin conexión.

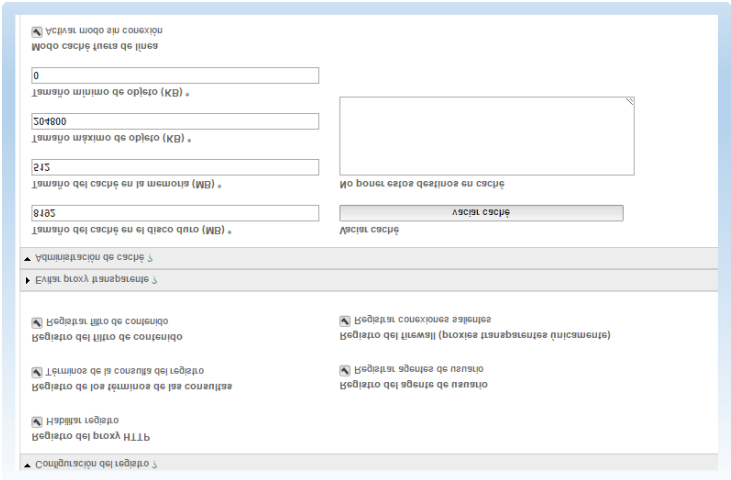


Figura 5.54 Registro y Cache de Proxy

Para el Filtrado Web se crearan los siguientes:

- No_XXX_Video_Si_Facebook

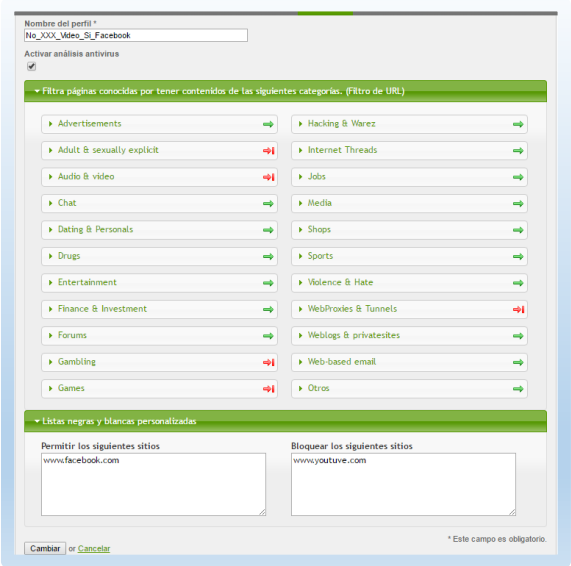


Figura 5.55 Filtro No_XXX_Video_Si_Facebook

- Navegación libre

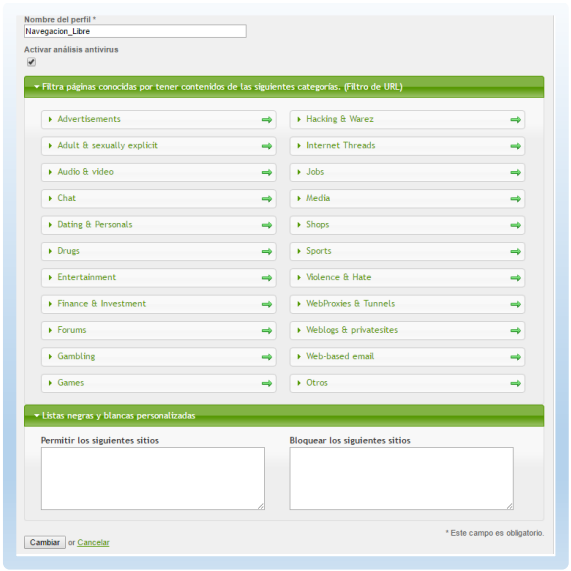


Figura 5.56 Filtro Navegación Libre

- No_Redes_Sociales_XXX_Audio_Video

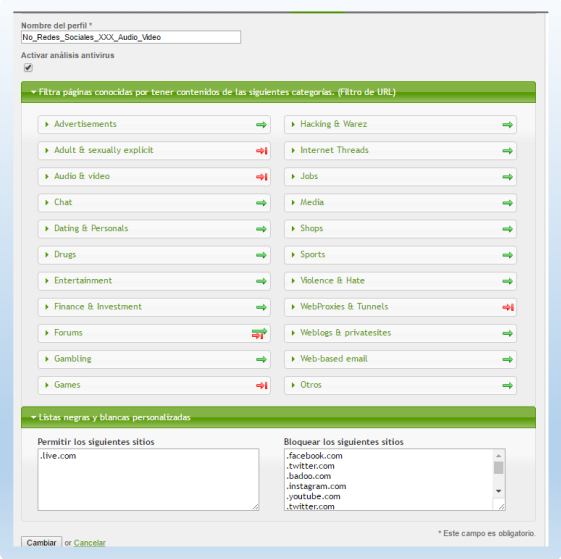


Figura 5.57 Filtro No_Redes_Sociales_XXX_Audio_Video

Las políticas de Acceso para los equipos que navegan por medio del proxy se representan en las siguientes reglas:

Posición de Regla: Primera

Objetivo de Regla: El objetivo de esta regla es permitir el acceso libre a Internet sin ningún filtro WEB al Jefe de Recursos Humanos.

Parámetros Generales:

En esta regla se define como origen la dirección IP: 192.168.2.18.

Destino: Cualquiera

Filtro: Ninguno

Activada: SI

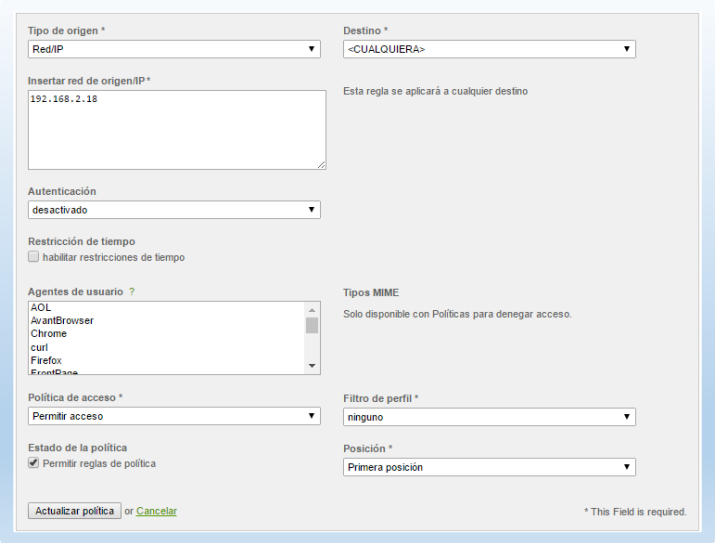


Figura 5.58 Primera Regla Proxy HTTP

Posición de Regla: Segundo

Objetivo de Regla: El objetivo de esta regla es bloquear a todas las redes los diferentes Tipos MIME de audio, video, etc.

Parámetros Generales:

En esta regla se define como origen las direcciones IP: 192.168.2.0/26, 192.168.1.0/28, 192.168.11.0/28, 192.168.12.0/28, 192.168.13.0/28

Destino: Cualquiera

Filtro: Ninguno

Tipo MIME: audio/mid, audio/midi, audio/mp3, audio/mpeg, audio/wav, audio/x-mp3, audio/x-mpegurl, audio/x-ms-wma, audio/x-pn-realaudio, audio/x-wav, audio/mid, audio/midi, audio/mp3, audio/mpeg, audio/wav, audio/x-mp3, audio/x-mpegurl, audio/x-ms-wma, audio/x-pn-realaudio, audio/x-wav, binary/octet-stream, video/flv, video/mpeg, video/x-flv, video/x-ms-asf, video/x-ms-asx, video/x-msvideo, y video/x-ms-wmv.

Activada: SI

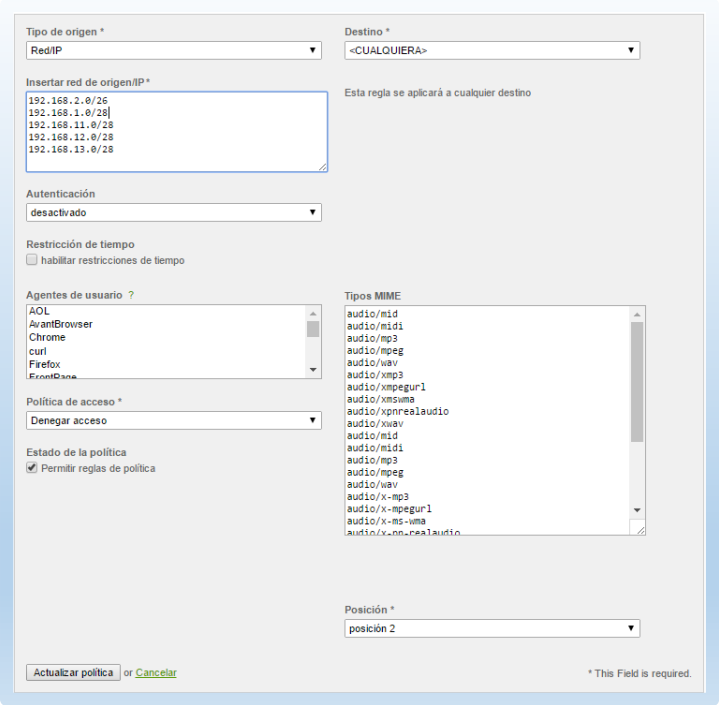


Figura 5.59 Segunda Regla Proxy HTTP

Posición de Regla: Tercera

Objetivo de Regla: El objetivo de esta regla es permitir la navegación de internet a toda la red por medio de un filtro general para todas las sucursales.

Parámetros Generales:

En esta regla se define como origen las direcciones IP: 192.168.2.0/26, 192.168.1.0/28, 192.168.11.0/28, 192.168.12.0/28, 192.168.13.0/28

Destino: Cualquiera

Filtro: No_Redes_Sociales_XXX_Audio_Video

Activada: SI

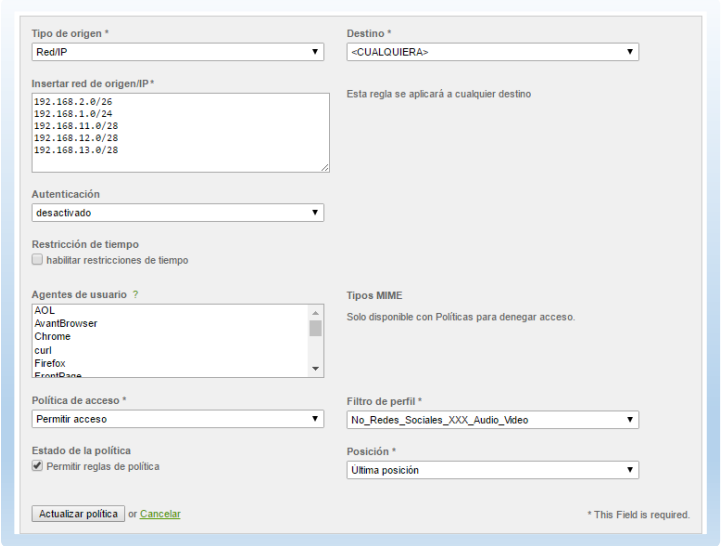


Figura 5.60 Tercera Regla Proxy HTTP

5.4. CONTROL DE ACCESOS REMOTOS CON SUCURSALES

Para el acceso remoto con las sucursales se utiliza el Servidor OpenVPN que viene incluido en el UTM, con los siguientes parámetros:

- Tipo de Autenticación: PSK
- Certificado con base a una IP que no pertenece a la red es decir 192.168.0.3.
- Retraso de desencadenadores habilitado para aumentar el rendimiento con varias conexiones simultáneas.
- Nivel de contenido de registro normal.
- Puerto UDP: 1194
- Dispositivos tipo TUN ya que es compatible con varios dispositivos.
- Subred VPN: 10.20.30.0/26
- Deshabilitado “Permitir varias conexiones para una cuenta”.
- Habilitado “Bloquear respuestas DHCP procedentes del túnel”

- Renegociación en 3600 segundos
- Conexiones de cliente a cliente administradas por el firewall UTM.
- Habilitar Forzar este dominio de Palacio.com.
- Tipo de autenticación hereda la opción global.

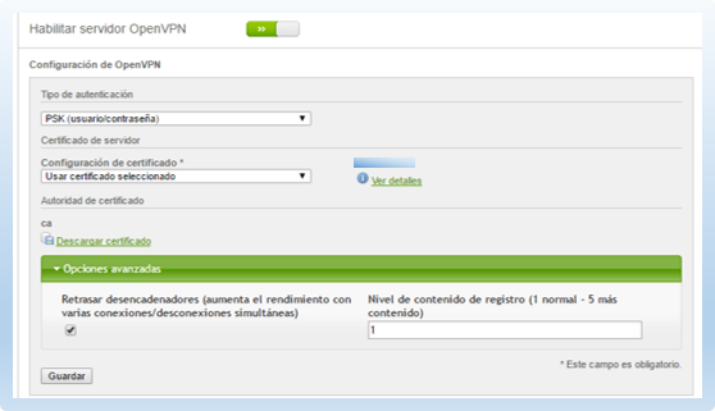


Figura 5.61 Configuración de Certificado VPN

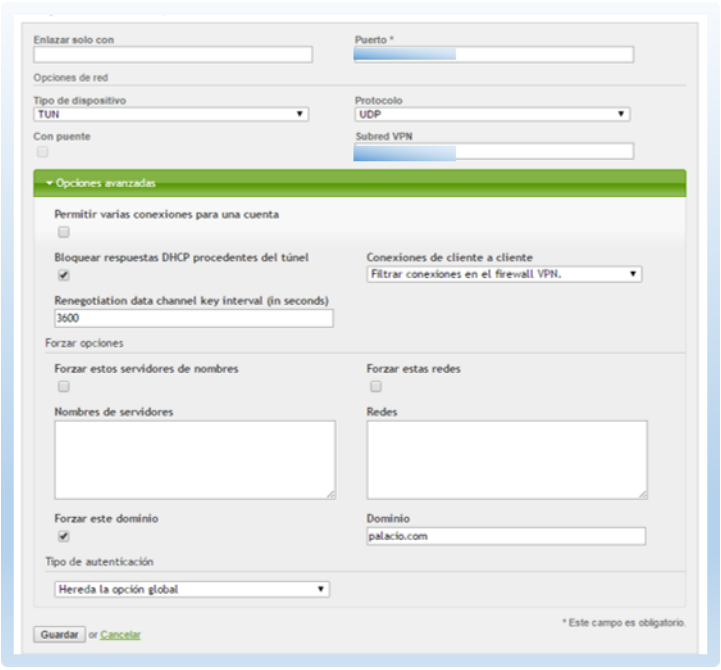


Figura 5.62 Configuración de Servidor OpenVPN

Para la configuración de los usuarios se consideran los siguientes parámetros:

- Se asigna IP fija para cada usuario
- Nombre de Usuario
- Observación que describimos el nombre completo del usuario y la respectiva dirección IP fija asignada.
- Contraseña del Usuario
- Usar el mismo certificado global
- Sin información adicional del usuario
- Habilitar “Invalidar opciones de OpenVPN” con el fin de realizar configuraciones propias.
- En el caso de no especificar ninguna red o zona en especial se habitará todo el tráfico del cliente hacia el servidor VPN.
- Forzar la conexión a la Red de servidores 172.16.100.0/27
- Asignar dirección IP estática de la red 10.20.30.0/26
- Definimos si está activo o no.

Las reglas aplicadas para cada usuario se encuentran en la sección 5.3.5 Tráfico VPN, controladas por el firewall UTM.

5.5. MONITOREO

Acceso SSH: Para la configuración del acceso SSH se consideran los siguientes parámetros:

- Permitir autenticación Basada en contraseña
- Permitir autenticación basada en clave pública

- No habilitar el reenvío de tráfico TCP.
- Clave pública de 256, 2048 y 1024 bits

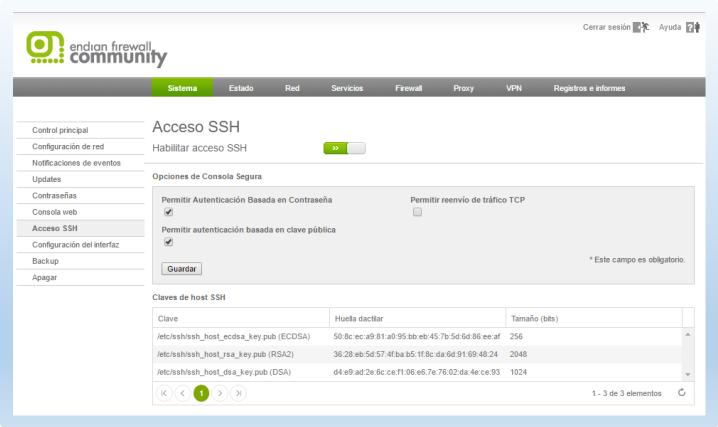
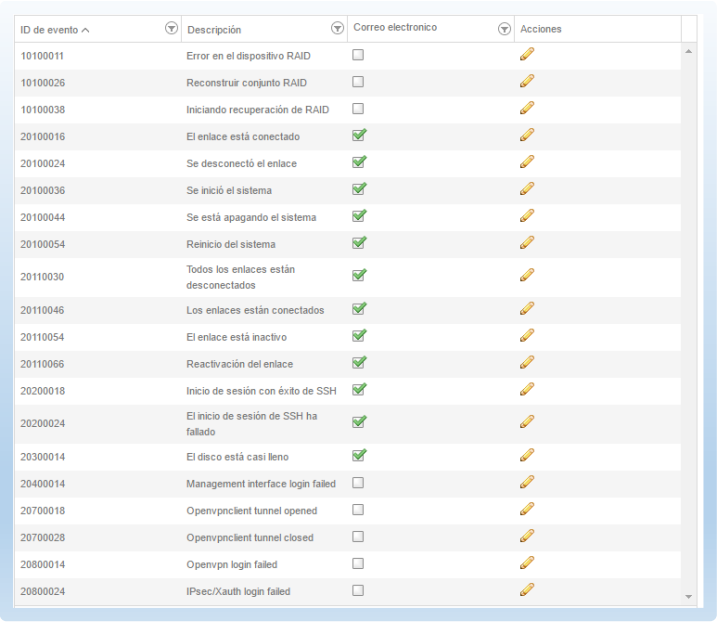


Figura 5.63 Configuración Acceso SSH

Notificación de Eventos: la notificación se enviará desde el correo infoendian@palaciodelhogar.com.ec, al correo giovanny.santana@palaciodelhogar.com.ec, de los siguientes eventos:

- El Enlace es Conectado
- Se desconectó el enlace
- Se inició el sistema
- Se está apagando el Sistema
- Reinicio del Sistema
- Todos los enlaces están desconectados
- Los enlaces están conectados
- El enlace está activo
- Reactivación de enlace
- Inicio de sesión con éxito de SSH, OpenVPN e IPsec
- El inicio de sesión de SSH, OpenVPN e IPSec ha fallado

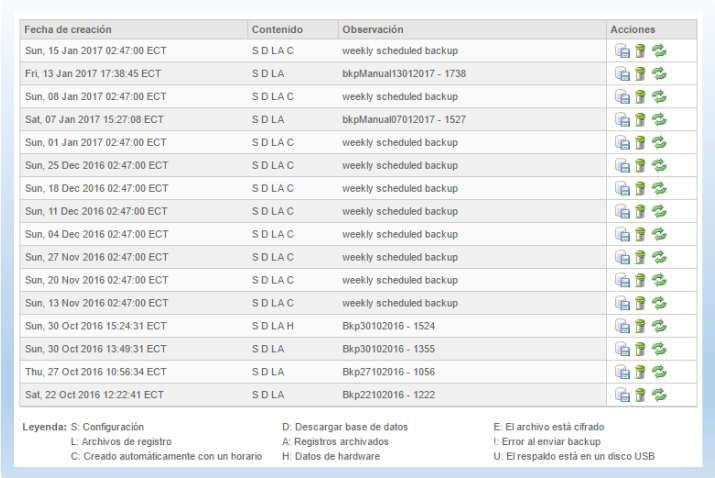
- El disco está casi lleno



ID de evento	Descripción	Correo electronico	Acciones
10100011	Error en el dispositivo RAID	☐	
10100026	Reconstruir conjunto RAID	☐	
10100038	Iniciando recuperación de RAID	☐	
20100016	El enlace está conectado	☑	
20100024	Se desconectó el enlace	☑	
20100036	Se inició el sistema	☑	
20100044	Se está apagando el sistema	☑	
20100054	Reinicio del sistema	☑	
20110030	Todos los enlaces están desconectados	☑	
20110046	Los enlaces están conectados	☑	
20110054	El enlace está inactivo	☑	
20110066	Reactivación del enlace	☑	
20200018	Inicio de sesión con éxito de SSH	☑	
20200024	El inicio de sesión de SSH ha fallado	☑	
20300014	El disco está casi lleno	☑	
20400014	Management interface login failed	☐	
20700018	Openvpnclient tunnel opened	☐	
20700028	Openvpnclient tunnel closed	☐	
20800014	Openvpn login failed	☐	
20800024	IPsec/Xauth login failed	☐	

Figura 5.64 Eventos a Notificar

Backups y Restore: el respaldo se programa para que se ejecuta una vez por semana, el UTM nos permite descargar los respaldos para en caso de cualquier problema de funcionamiento restaurarlos. El UTM permite cifrar los respaldos y enviarlos por correo pero esta opción no se usará en este caso, ya que los archivos son demasiado grandes. El sistema mantendrá los últimos 10 respaldos automáticos, y manuales indefinidamente.



Fecha de creación	Contenido	Observación	Acciones
Sun, 15 Jan 2017 02:47:00 ECT	S D LA C	weekly scheduled backup	
Fri, 13 Jan 2017 17:38:45 ECT	S D LA	bkpManual13012017 - 1738	
Sun, 08 Jan 2017 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sat, 07 Jan 2017 15:27:08 ECT	S D LA	bkpManual07012017 - 1527	
Sun, 01 Jan 2017 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 25 Dec 2016 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 18 Dec 2016 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 11 Dec 2016 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 04 Dec 2016 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 27 Nov 2016 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 20 Nov 2016 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 13 Nov 2016 02:47:00 ECT	S D LA C	weekly scheduled backup	
Sun, 30 Oct 2016 15:24:31 ECT	S D LA H	Bkp30102016 - 1524	
Sun, 30 Oct 2016 13:49:31 ECT	S D LA	Bkp30102016 - 1355	
Thu, 27 Oct 2016 10:56:34 ECT	S D LA	Bkp27102016 - 1056	
Sat, 22 Oct 2016 12:22:41 ECT	S D LA	Bkp22102016 - 1222	

Leyenda: S: Configuración
L: Archivos de registro
C: Creado automáticamente con un horario
D: Descargar base de datos
A: Registros archivados
H: Datos de hardware
E: El archivo está cifrado
!: Error al enviar backup
U: El respaldo está en un disco USB

Figura 5.65 Conjunto de Backups a la fecha

Para los respaldos manuales como automáticos se puede elegir entre los siguientes parámetros:

- Configuración
- Base de datos
- Fichero de registros actuales
- Fichero de registros antiguos
- Datos de hardware

Prevención de Intrusos: el IPS se configura de la siguiente manera:

- Obtener Snort diariamente de forma automática.
- El UTM también permite actualizar de forma manual los Snort, inclusive personalizados.
- Las reglas habilitadas serán las que trae por defecto el UTM no se editará ninguna.

Monitorización de Tráfico: para el monitoreo de tráfico el Endian UTM trae incorporado la Herramienta Ntop que permite obtener los siguiente:

- Traductor de Flujo
- El Top de los Host en Envío y Recepción
- El Top de aplicaciones
- El Top ASNs
- El Top del Flujo de envío
- Flujos Activos
- El historial de navegación de los host de la red
- Estadísticas de consumo de ancho de banda, del tráfico de la red, de paquetes, protocolos, etc.
- Permite monitorear el tráfico por interfaces, entre otras cosas.

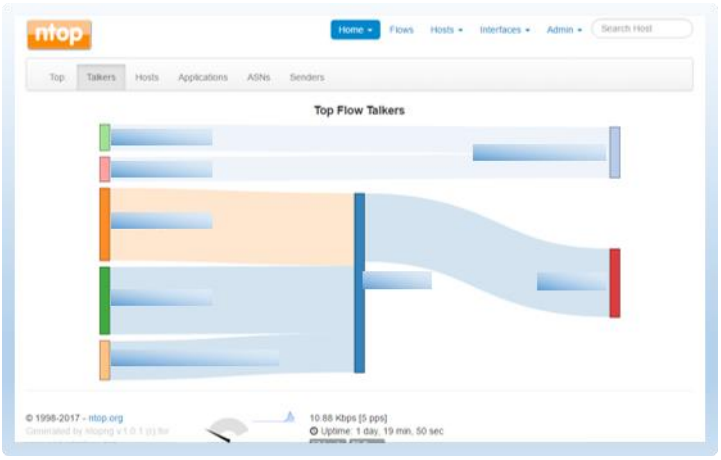


Figura 5.66 Interfaz Ntop

Estados: el UTM tiene por defecto diferentes estados que permite monitorearlo como los que se muestran a continuación:

Estado del Sistema: comprende servicios, memoria, uso de disco, tiempo de servicios y usuarios, módulos cargados, versión del Kernel.

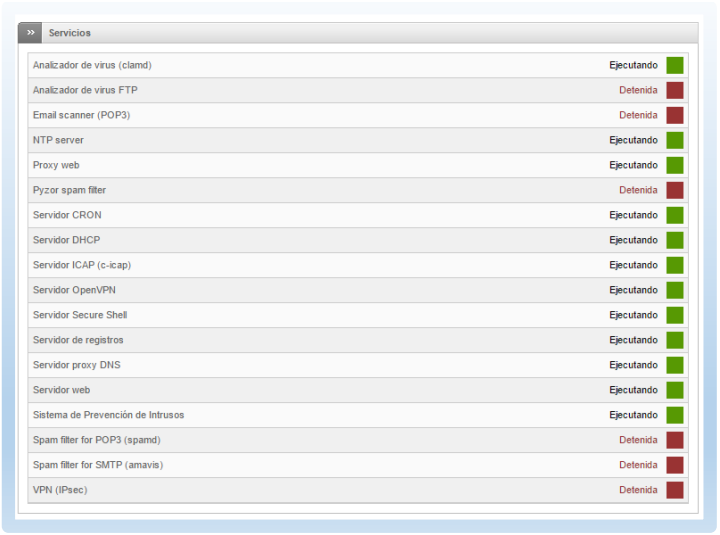


Figura 5.67 Estado de Servicios

Estado de la Red: comprende interfaces, asignaciones dinámicas actuales, estados de NIC, entradas de la tabla de enrutamiento, entradas de la tabla ARP.

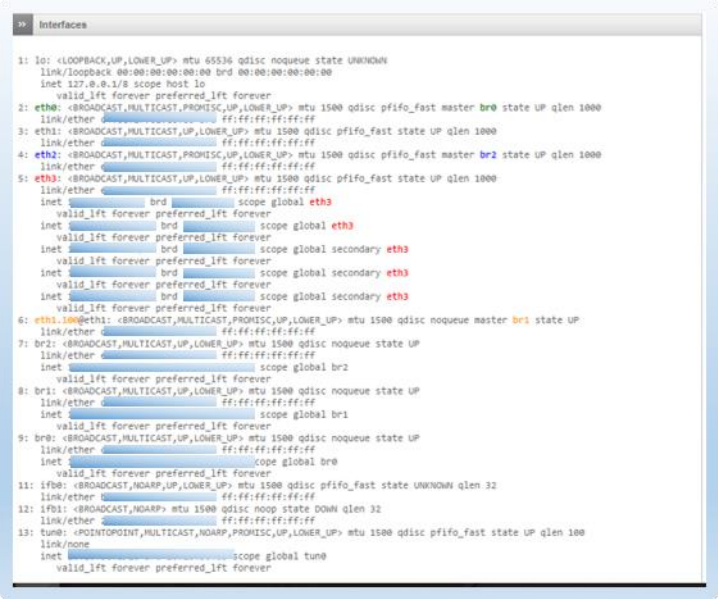


Figura 5.68 Estado de Interfaces

Gráficos del Sistema: comprende gráficos del CPU, gráfico de memoria y gráfico de Swap.

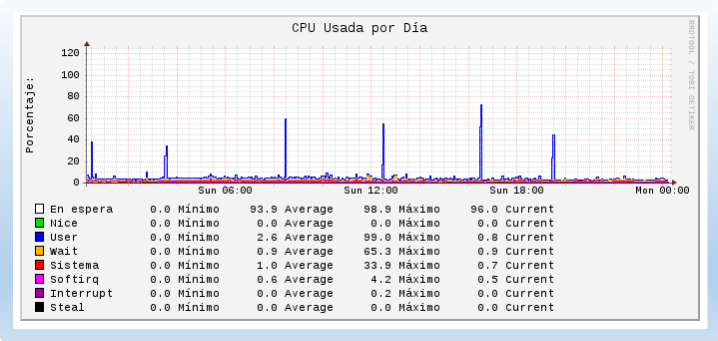


Figura 5.69 Gráfico de CPU

Gráficos del Tráfico: comprende gráficos Verde, gráfico Azul, gráfico Naranja y gráfico Rojo o enlace principal.

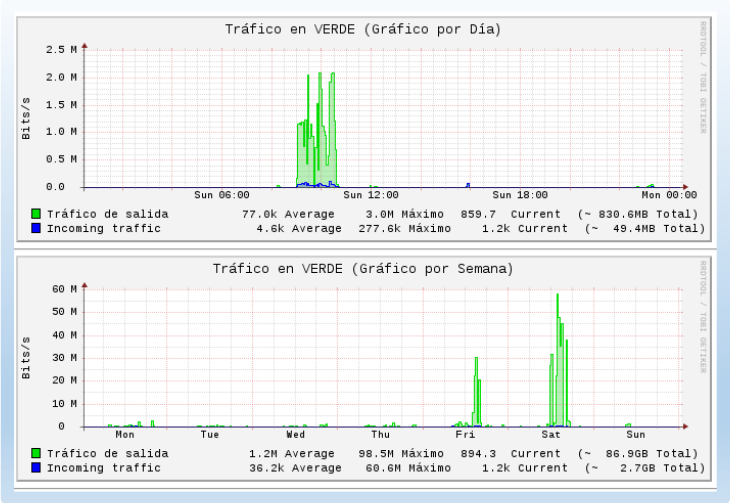


Figura 5.70 Gráfico Zona Verde

Gráficos del Proxy: comprende Gráfico Total por Día, acceso total por día, cache hits por día y cache hits ratio sobre los 5 minutos por día.

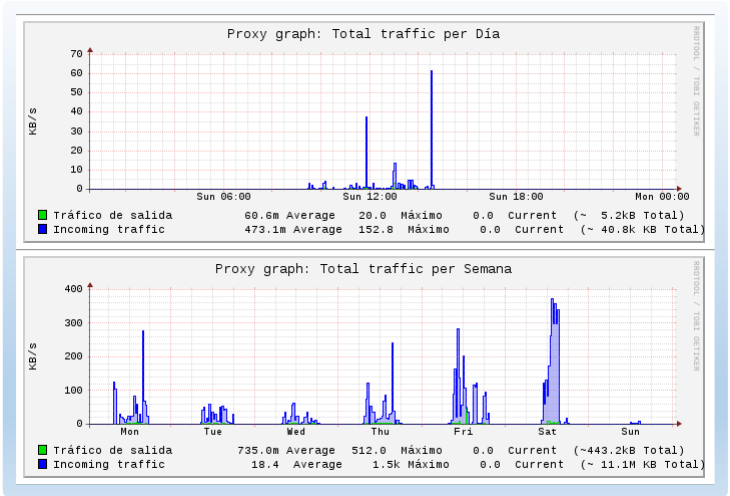


Figura 5.71 Gráficos del Proxy

Estado de Conexiones: realiza seguimiento de las conexiones IPTABLES.

Figura 5.72 Seguimiento de IPtable

Conexiones VPN: permite monitorear que usuarios están conectados, que servicio está usando, dirección IP Remota, dirección IP VPN, y fecha y hora de conexión, en esta sección se puede desconectar manualmente a cualquier usuario conectado.

Estadística de correo SMTP y cola de correo no implementado ya que no disponen aún de servidor de correo interno, subcontratan servicio de hosting.

Registros, Informes y Otros: el UTM posee un visor en Tiempo Real como se muestra en la siguiente Imagen:

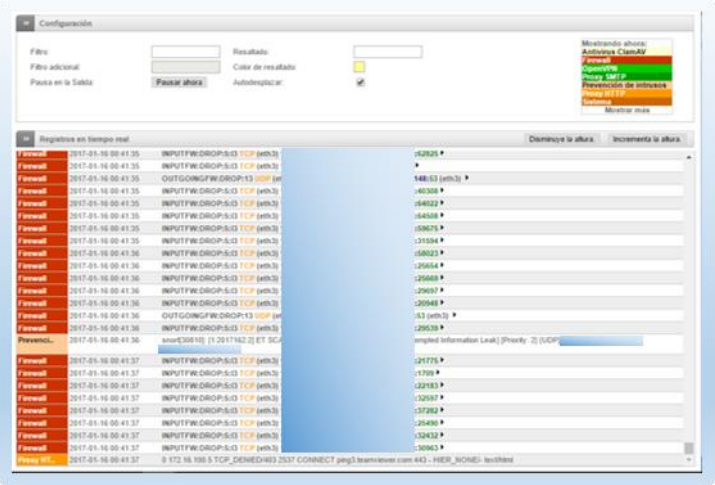


Figura 5.73 Visor en Tiempo Real

En la sección de registros e informes también podemos encontrar reportes almacenados, cuya configuración se modifica de 56 días a 365 días de almacenamiento y de nivel de detalle baja a alta:

- Registro del Sistema
- Servicios: IDS, OpenVPN, ClamAV.
- Firewall
- Proxy: HTTP, Informe HTTP, SMTP

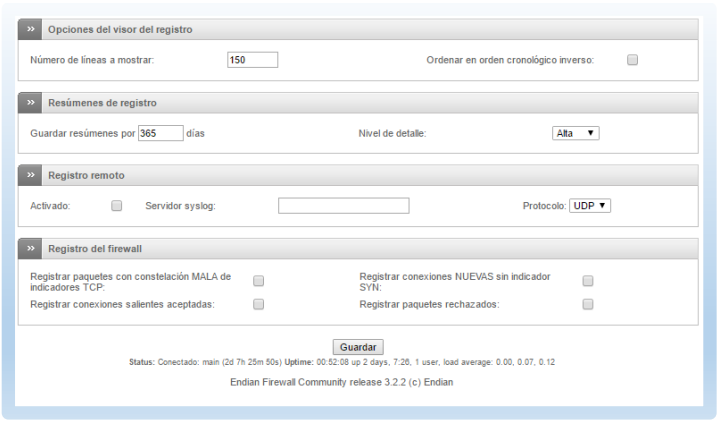


Figura 5.74 Configuración de Registro de Endian

Todo reporte puede ser obtenido en rangos de fecha que el usuario desee consultar, para poder realizar cualquier tipo de auditoría durante los últimos 365 días con un nivel de detalle alto.

5.6. SERVICIOS ADICIONALES DE CONTROL

Servidor DHCP: el servicio DHCP del UTM es habilitado solo para la zona verde, es decir la LAN de la empresa en el rango IP desde 192.168.2.51 hasta 192.168.2.61; este servicio nos permite realizar asignaciones fijas por MAC para el segmento de red 192.168.2.0/26, los dispositivos a fijarlos en la red son:

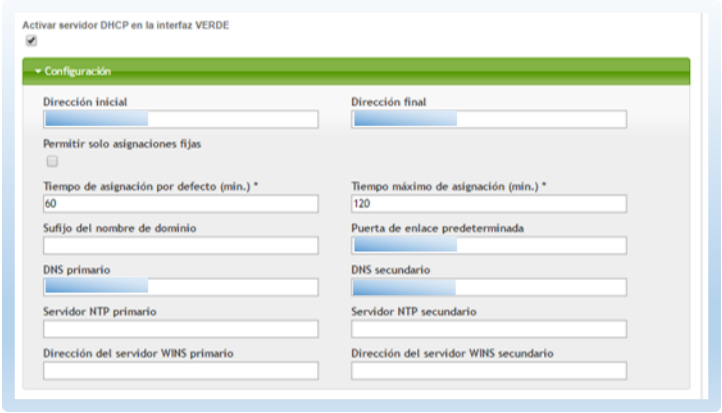


Figura 5.75 Configuración de Servicio DHCP

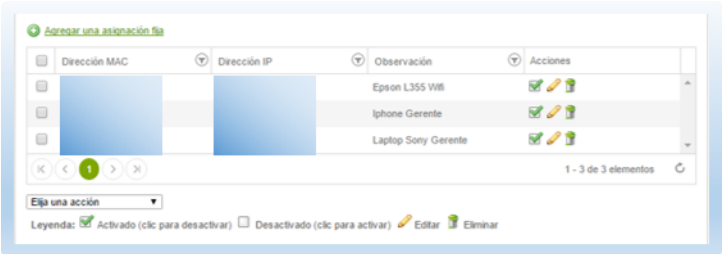


Figura 5.76 Asignación de IP Fija

DNS Dinámico: este servicio no se configura ya que no tienen ninguno instalado.

Motor de Antivirus: el antivirus a utilizar en el UTM es el ClamAV que viene pre configurado en el UTM.

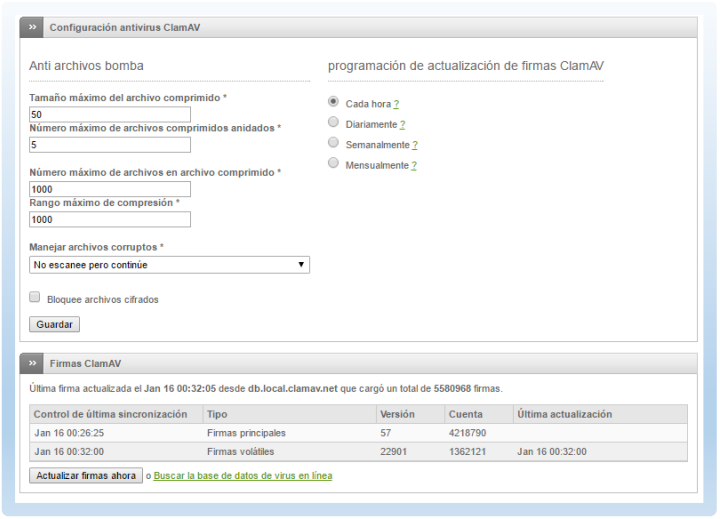


Figura 5.77 Configuración de ClamAV

Capacitación SPAM: no se configura ya que no existe correo electrónico dentro de la empresa.

5.7. PRUEBAS DE IMPLEMENTACIÓN

Para las pruebas de Implementación se realiza en el siguiente orden:

- Pruebas de reglas NAT
- Pruebas de Reglas en Red Interna y VPN de la Empresa
- Pruebas de Acceso al Sistema UTM
- Pruebas de Notificación de Eventos.

5.7.1. PRUEBAS DE REGLAS NAT

Para las pruebas de Reglas de NAT se procede a dar los mismos permisos a una dirección IP Externa a la Empresa, y para identificarla se usa la dirección web https://www.whatismyip.com/es/, dando como resultado la IP 186.46.129.92 que procederemos a realizar las pruebas de permisos de las Reglas 1 y 2.

Paso 1: asignar la dirección IP pública obtenida en las reglas uno y dos como se muestra en la siguiente imagen:

Figura 5.78 Asignación de IP Externa par Prueba de Regla 1 y 2

Paso 2: una vez asignado se procede a abrir en cualquier navegador web la IP A para probar los accesos permitidos en la regla, a continuación se muestra una imagen donde se puede apreciar que si se puede acceder al sistema PAC de la empresa:

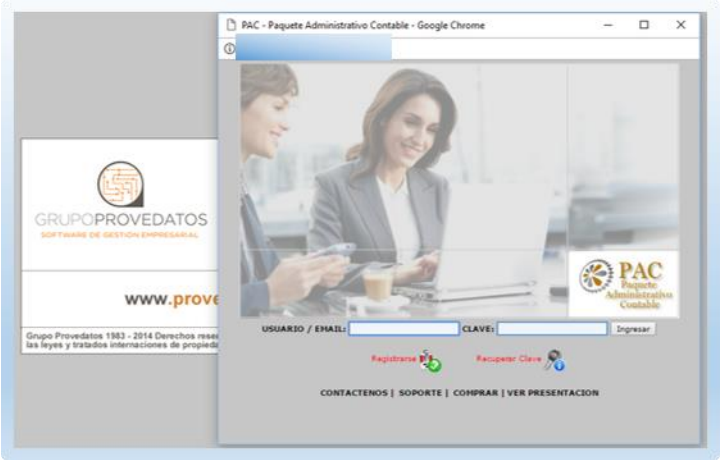


Figura 5.79 Prueba de Acceso Regla 1 y 2

Paso 3: una vez comprobado el permiso habilitado, procedemos a deshabilitarlo; en la siguiente imagen se puede observar que el acceso ahora está bloqueado.

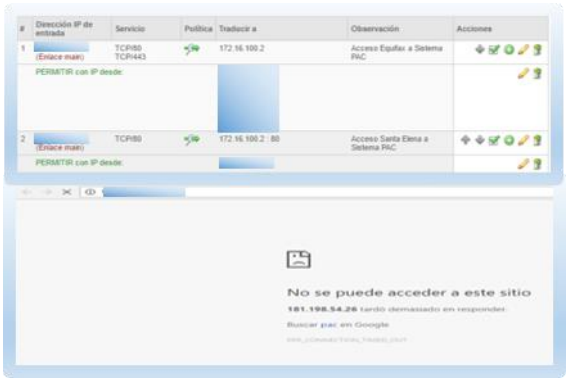


Figura 5.80 Acceso bloqueado a Sistema PAC

Para la prueba de la regla 3 utilizamos la aplicación Zoiper diseñada para la configuración de cuentas de telefonía IP, esta configuración se la realiza en un IPhone con la extensión 31 facilitada por la empresa

desde una IP Pública autorizada por el Firewall, el resultado es exitoso como se muestra en la siguiente imagen:

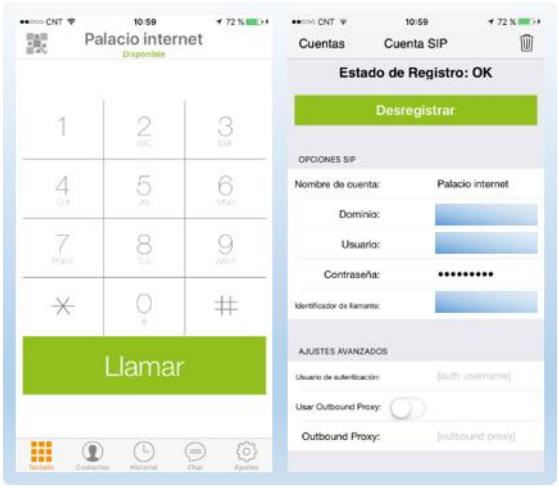


Figura 5.81 Prueba de Regla 3 Acceso con Zoiper

Para la Prueba de la regla 4 a la 17 se toma accede al equipo que esta fuera de la red de la empresa y probamos las direcciones IP asignadas a las cámaras IP con sus respectivos puertos, en este caso se toma la D: 9013, y la regla permite acceder como se muestra a continuación:

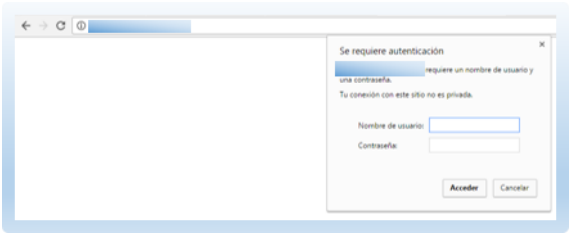


Figura 5.82 Prueba de Reglas 4 a 17 de Acceso a Cámaras IP

5.7.2. PRUEBAS DE REGLAS EN RED INTERNA Y VPN DE LA EMPRESA.

Para la Prueba de las reglas configuradas en las sucursales con enlace de datos y matriz se toma acciones en común como: los permisos de acceso al PAC, la denegación de PING a los servidores y entre redes, acceso a internet sin y con Proxy HTTP, denegación de acceso a Servicios adicionales de cualquier servidor. Para esta prueba se toma cualquier computador de la red interna de la empresa, en este caso se toma la PC del Administrador de la Red para probar sus respectivos permisos, y luego una PC de la matriz para realizar las pruebas de acceso respectivas. En las siguientes imágenes se muestra las diferentes pruebas realizadas:

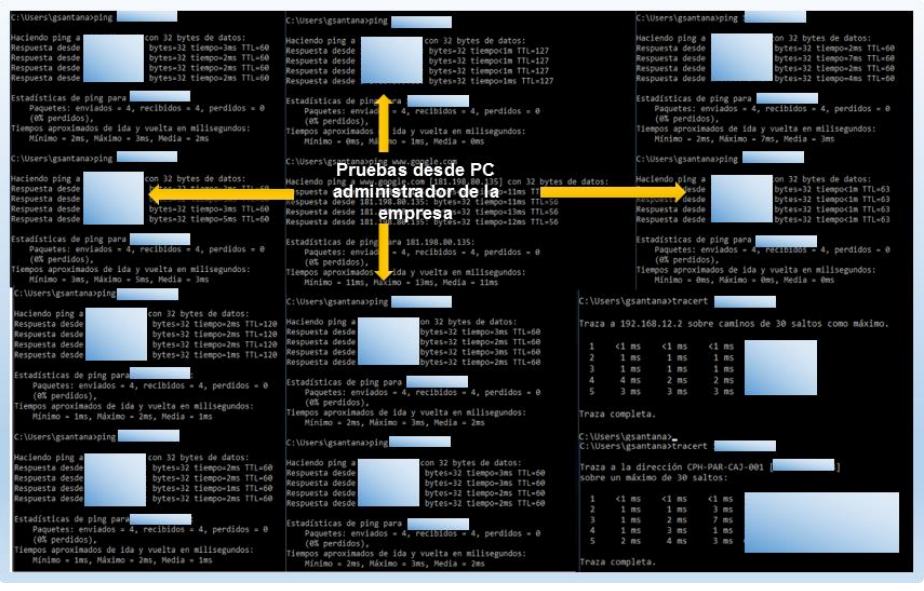


Figura 5.83 Pruebas de Acceso Administrador de Red

Para continuar con las pruebas se toma la PC del Ec. Humberto Mendoza quien posee restricciones aplicadas por el firewall, entre ellas el PING a las mismas direcciones IP que el Administrador de Red si tiene permisos de acceso, a continuación las pruebas respectivas:

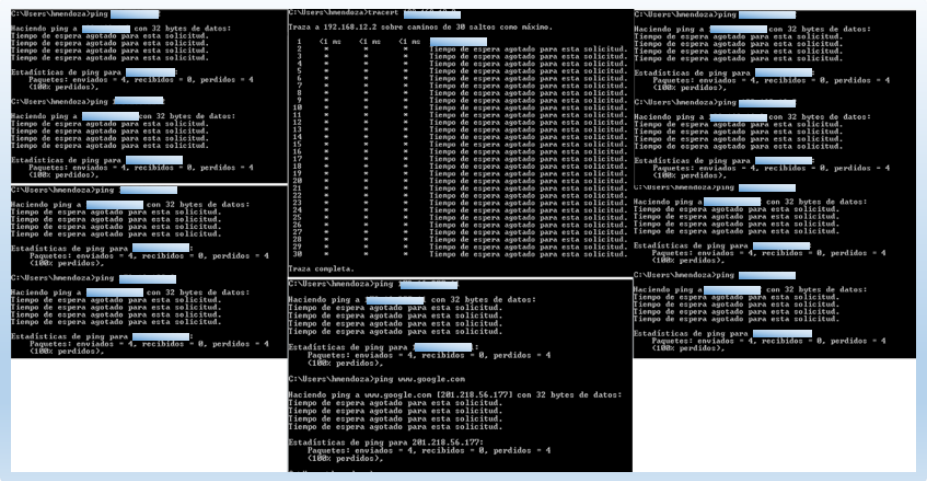


Figura 5.84 Prueba desde Pc de Usuario de Matriz

En una de las pruebas de PING anteriores podemos observar que no tiene permisos ICMP a la dirección IP 172.16.100.2, que es el Sistema PAC de la empresa, sin embargo, accede al puerto 80 de ese mismo equipo demostrando la aplicación de las reglas en el Firewall del UTM como se muestra en la siguiente imagen:

Figura 5.85 Permisos a PAC desde Usuario Restringido

Para probar le Proxy HTTP que está configurado en este usuario se realiza el ingreso a www.facebook.com, www.twitter.com, www.instagram.com, e ingresamos una dirección web que no existe como se muestra en la siguiente imagen:

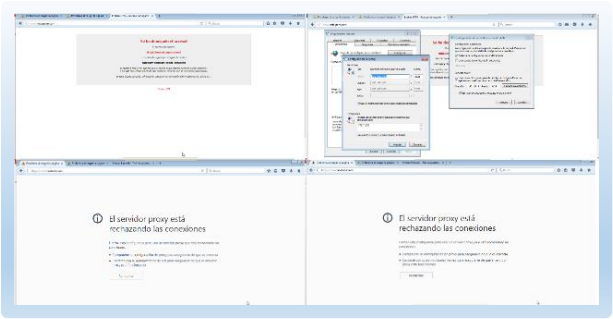


Figura 5.86 Prueba de Proxy HTTP

La siguiente prueba se realiza desde un equipo de la red 172.16.100.0/27 y 172.16.200.0/27, para la primera se toma el Servidor PAC con la dirección IP 172.16.100.2 y de la segunda red se toma la dirección IP 172.16.200.11 del Server de Cámaras respectivamente, donde se evidencia que el acceso se encuentra bloqueado.

Para la prueba de Accesos VPN se realiza desde uno de los usuarios de la ciudad de Libertad, que tiene asignado la dirección IP 10.20.30.11.

Primeramente verificamos en el firewall los usuarios que se encuentran conectados al momento como se muestra en la siguiente imagen:

Figura 5.87 Usuarios VPN Conectados

Una vez verificado procedo a realizar la prueba de conexión desde el usuario mencionado, donde la conexión es satisfactoria como se muestra a continuación:

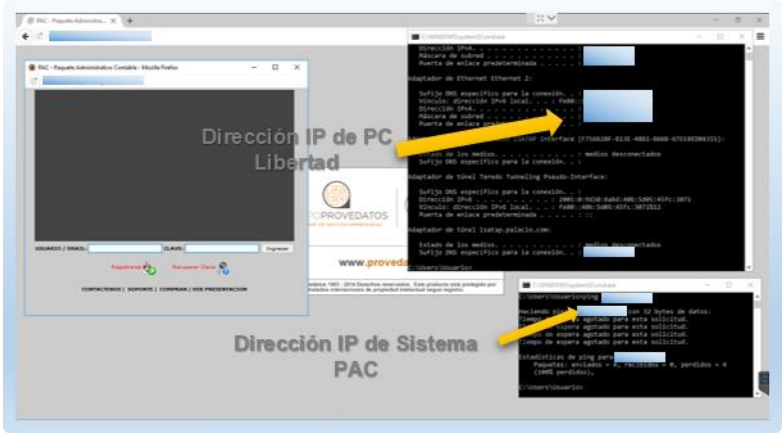


Figura 5.88 Prueba de Acceso desde Usuario VPN

Se realiza un escaneo de puertos con Nmap y el resultado es el esperado según las políticas aplicadas en el UTM, a continuación la respectiva captura:

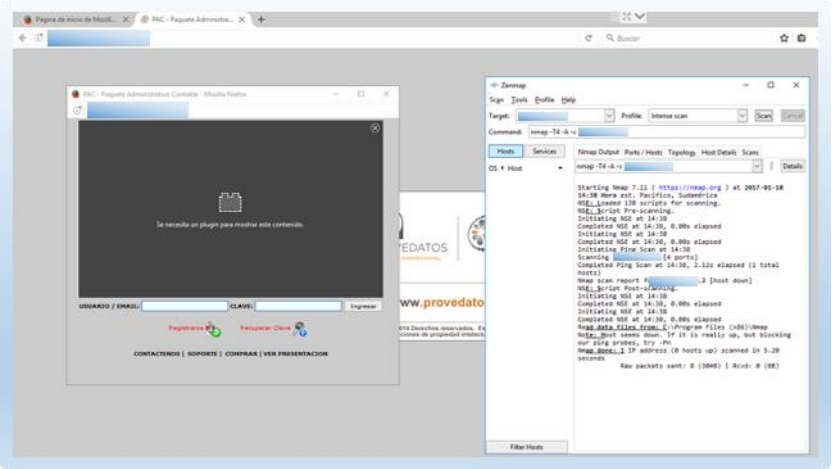


Figura 5.89 Prueba de Acceso VPN con Nmap

5.7.3. PRUEBAS DE ACCESOS Y VULNERABILIDADES AL SISTEMA UTM

Para realizar las pruebas de Acceso al Sistema primeramente se considera las existentes, donde se encuentra denegado todo acceso a excepción de los puertos propios de endian en sus servicios de Acceso WEB, VPN y Proxy, a continuación una prueba de PING a su dirección IP Pública desde una oficina externa a la Empresa.

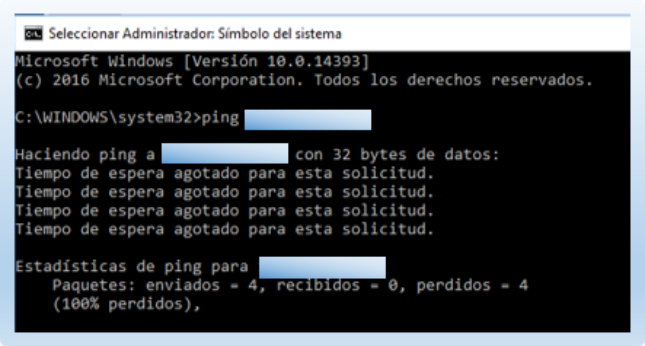


Figura 5.90 Prueba de PING a UTM

Como se visualiza en la imagen el Protocolo ICMP bloqueado, esta configuración aplica a toda la red pública asignada a la Empresa.

Después, se realiza un escaneo con la aplicación Zenmap con el siguiente comando Nmap –p 1-65535 –T4 –A –v –Pn #IP, que permite escanear sin necesidad de hacer ping todos los puertos existentes incluyendo investigación de versión. Los resultados obtenidos son muy favorables al observar que todos los puertos de las direcciones IP públicas de la empresa se encuentran filtrados, como se muestra en el Anexo “I” de este documento.

Para verificar si existe alguna vulnerabilidad se utiliza la herramienta Nessus en su versión 6.9.3, donde se obtiene los siguientes resultados por cada IP Pública de la Red Asignada:

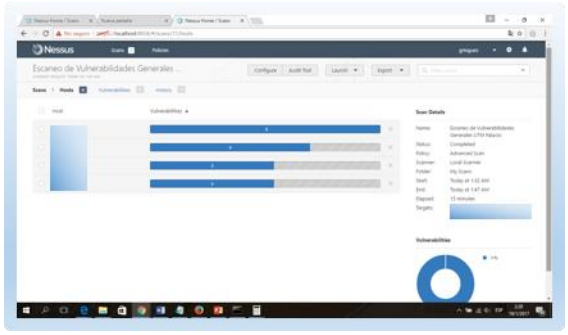


Figura 5.91 Análisis de Vulnerabilidades con Nessus

Como se observa en la imagen no existen vulnerabilidades de Riesgo en ninguna de las direcciones IP asignadas a la empresa, solamente información general como se muestra a continuación:

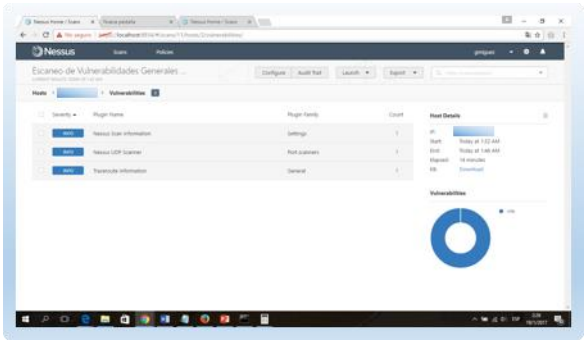


Figura 5.92 Detalle Análisis A

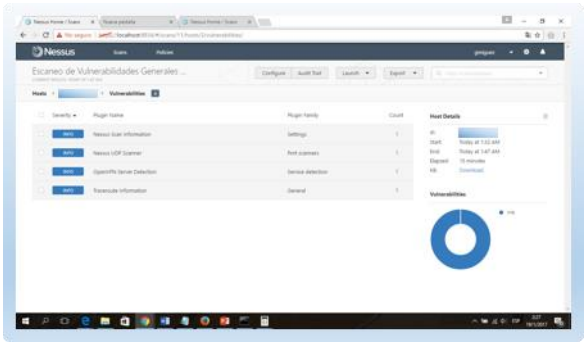


Figura 5.93 Detalle Análisis IP B

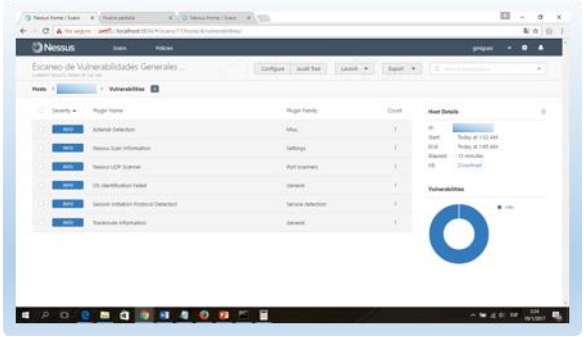


Figura 5.94 Detalle Análisis IP C

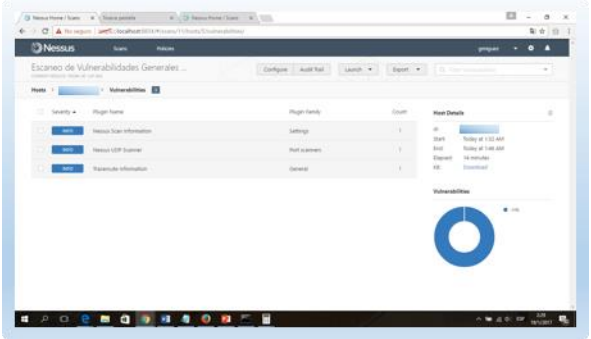


Figura 5.95 Detalle Análisis IP D

5.7.4. PRUEBAS DE NOTIFICACIÓN DE EVENTOS (ESCENARIO REAL)

En esta sección se muestra un escenario real de un ataque de fuerza bruta realizado al UTM de la empresa, tratando de ingresar con diferentes tipos de credenciales. Este ataque consiste en probar las diferentes combinaciones posibles para recuperar una contraseña y poder acceder con permisos elevados, y tomar el control de cualquier herramienta informática. El ataque fue sobre el puerto SSH que estuvo abierto en ese lapso de tiempo. El notificador de eventos de endian reportó el ataque que empezó a las 00:00 del domingo 15 de Enero del 2017, las notificaciones se encuentran en la bandeja de entrada del

correo geovanny.santana@palaciodelhogar.com.ec como se muestra a continuación:

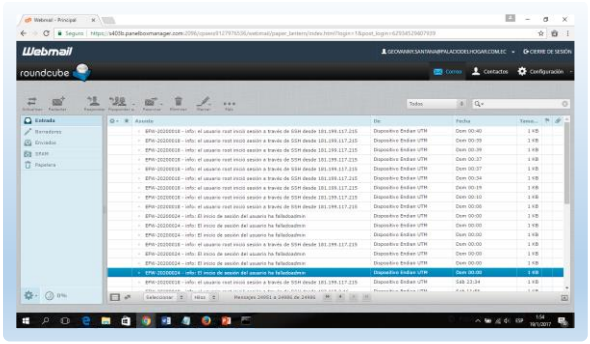


Figura 5.96 Correos de Ataque de Fuerza Bruta

El ataque fue realizado entre las 00:00 del 15 de Enero del 2017 hasta las 11:53 del mismo día como se muestra en los siguientes correos:

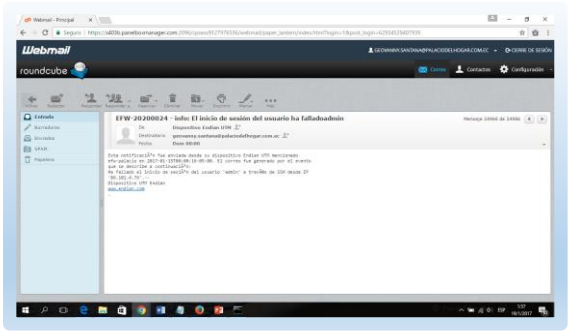


Figura 5.97 Reporte de Inicio de Ataque

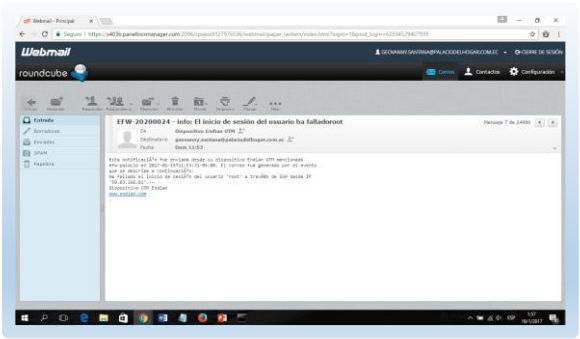


Figura 5.98 Reporte de Fin de Ataque

El ataque duró 713 minutos y fue ejecutado aproximadamente 35,007012 ataques por minuto que da como resultado un envío masivo de 24960 correos por parte de endian, entre los usuarios detectados se encontraron los siguientes: root, admin, 500, john, user, lms, test, ncuser, tomcat, etc. Las direcciones IP aleatorias utilizadas para ataque son: 59.63.166.81 que pertenece a Pekin-China, 201.178.52.37 no localizable, 188.34.144.240 Iran, Hewan-China, y otras. En Conclusión el UTM resistió al ataque y no se vulneró la seguridad perimetral de la empresa, como acción se deshabilitó el puerto 22 y solamente se permite el acceso por VPN o desde la pc del Administrador de la red siempre y cuando se lo habilite, ya que por defecto esta deshabilitado.

Una vez finalizadas todas las pruebas se puede constatar los siguientes puntos importantes:

- El UTM solo puede ser accedido para administración desde el pc del administrador dentro de la empresa.
- El UTM puede ser accedido para administración desde Internet por conexión VPN y por el momento solo está autorizado al usuario Implementador gmiguez.
- El UTM resistió a un ataque de fuerza bruta de aproximadamente 12 horas el domingo 15 de enero del 2017.
- El UTM reportó por medio de correo los intentos de violación de seguridad.

- Los accesos desde internet a los servicios dentro de la empresa se encuentran filtrados por el firewall.
- Las redes internas de la empresa se encuentran correctamente filtradas con os permisos que corresponden.
- Los usuarios VPN solo pueden acceder a la red que el firewall se lo permita.
- Los permisos VPN de las sucursales remotas están bien aplicadas.
- En el análisis de vulnerabilidades con Nessus el Resultado solo arrojó resultados informativos que no se ubican en ningún nivel de vulnerabilidad en la escala de bajo, medio o alto, dado por el software.
- El administrador de la red tienen acceso a todas las redes para su respectiva administración y control.

CAPÍTULO 6

PLAN DE IMPLEMENTACIÓN

6.1. FASES DE IMPLEMENTACIÓN

6.1.1. LEVANTAMIENTO DE INFORMACIÓN EN MATRIZ Y SUCURSALES GUAYAQUIL

En esta fase se visita la oficina matriz de la empresa ubicada en Parque California II Bodegas F37 y F38, con el objetivo de entrevistar al Gerente General y solicitar autorización para obtener información necesaria para la implementación del UTM. Para este levantamiento de información se sigue el siguiente proceso:

Entrevista al Gerente General: en esta entrevista se consulta a nivel gerencial las políticas de seguridad existentes y qué expectativas se tiene en relación a la implementación de seguridad a realizar, las respuestas obtenidas se adjuntas en los Anexo “D” de este trabajo.

Entrevista a Usuarios de la Empresa: en esta entrevista se puede obtener requerimientos propios de los usuarios de la empresa como:

Acceso a internet en páginas de trabajo y sistemas que son primordiales para ellos.

Visita DATACENTER de la Empresa: gracias a que el Ing. Guido Miguez (Implementador) brinda servicios externos en la empresa se tiene las facilidades para obtener información como: Servicio Instalados en la empresa, Proveedor de Internet y de Enlace de Datos de oficina matriz y sucursales en Guayaquil, proveedor de internet y tipo de enlace con sucursales remotas, redes existentes en matriz y sucursales, equipos de administración de red existentes, equipos de computación, dispositivos adicionales y de control existentes.

Visita a Sucursales: la visita a sucursales se realiza en el siguiente orden:

- Sucursal Balerio.
- Sucursal Paraíso
- Sucursal San Francisco
- Sucursal Santa Elena y,
- Sucursal Libertad.

En estas visitas se puede palpar que dispositivos de red, tipo de computadores y dispositivos se utilizan para el trabajo diario.

Identificación de Riesgos Inherentes Existentes: por cada paso anterior se toma apuntes de los posibles riegos existentes que puedan afectar a la operatividad de la empresa.

6.1.2. ANÁLISIS

Con toda la información obtenida se realiza las siguientes actividades:

Análisis General: en este proceso se puede obtener las falencias existentes en las redes y servicios de la oficina matriz y sucursales. La asignación de direcciones IP en los equipos servidores de la empresa, computadores y dispositivos que sean utilizados para la actividad diaria dentro de la empresa.

Análisis de Oficina Matriz Y Sucursales: se analiza problemas independientes por cada sucursal de la empresa, desarrollando gráficos estadísticos explicativos para ayudar a la toma de decisiones.

Análisis de Riesgo Inherente: para este análisis se utiliza un método cuantitativo que nos permite medir los riesgos inherentes existentes dentro de la empresa, pudiendo medir en tres niveles su probabilidad entre Alta, Media y Baja, e impacto entre Significativo, Moderado y Leve.

6.1.3. DISEÑO

El diseño comprende en la segmentación y restructuración de red, control de tráfico, control de accesos remotos, monitoreo y servicios adicionales.

Segmentación y Restructuración de Red: consiste en modificar las redes actuales que existen en la empresa por un diseño más óptimo, para una correcta implementación de las ACL en el UTM.

Control de Tráfico: consiste en crear las ACL de la empresa en base a reglas de tráfico entrante, tráfico saliente, Tráfico Inter-zonas, tráfico VPN, Tráfico entrante al sistema UTM y proxy HTTP.

Control de Accesos Remotos: consiste en crear todo lo necesario para el funcionamiento del servidor VPN, como por ejemplo usuarios, certificados y su respectiva configuración.

Monitoreo: establecer las políticas de control para los respaldos, notificación de eventos, estadísticas y reportaría en general del sistema UTM. Entre los reportes se considera firewall, VPN, Proxy HTTP y cualquier tráfico que pase por el equipo.

Servicios Adicionales de Control: entre los servicios adicionales a implementar esta DCHP solo para la LAN de la empresa en las oficinas

de Matriz, Antivirus a toda la red por parte del UTM y Prevención de Intrusos para todo el Tráfico de la red.

6.1.4. IMPLEMENTACIÓN

Para la implementación se sigue el orden planteado en la etapa de diseño, pero ahora en el quipo UTM que va a ser ubicado en la empresa. Para las respectivas configuraciones se considera primeramente la segmentación de la red y después todo el control de tráfico, monitoreo y servicios adicionales disponibles en Endian Firewall Community.

6.1.5. PRUEBAS

Para las pruebas se realizará sobre los siguientes procesos de control más relevantes en las configuraciones de seguridad implementadas:

Pruebas de todas las Reglas NAT Destino: para esta prueba se asigna los permisos del diseño a una IP pública externa a la empresa, para probar si las reglas realmente están funcionando.

Pruebas de Reglas en red Interna y VPN de la Empresa: para esta prueba primeramente se toma el computador del administrador de la red, ya que este equipo posee permisos especiales en el firewall, después se toma un equipo de cualquier usuario para probar las denegaciones respectivas. Dentro de estas pruebas se encuentra el acceso al Sistema PAC y otros servicios de la empresa como el Proxy HTTP, DNS, VPN. Para prueba de VPN se accede a un usuario remoto

de una de las sucursales de la provincia de Santa Elena, adicional, se prueba los permisos existentes entre las diferentes zonas internas como la VERDE, NARANJA Y AZUL y su interacción entre ellas.

Pruebas de Acceso y Vulnerabilidades al Sistema UTM: se realiza una prueba de ICMP hacia las direcciones ip públicas configuradas en el UTM, se realiza un escaneo de puertos exhaustivo con no ping con Nmap y un análisis de vulnerabilidad con el aplicativo Nessus, con el fin de verificar el nivel de seguridad existente en el endian firewall Community.

Prueba de Notificaciones: en esta prueba se verifica que el sistema envíe los correos con las alertas configuradas al administrador de la red, con el fin de monitorear constantemente el UTM.

6.2. CRONOGRAMA DE IMPLEMENTACIÓN

El tiempo de implementación del UTM en la empresa Palacio del Hogar es de 163 días hábiles como se muestra en el Anexo “J”.

6.3. RECURSOS

Los recursos a utilizar son el Gerente General, el Administrador de Red, todos los Usuarios de la empresa y el Implementador.

6.4. ANÁLISIS DE RIESGO RESIDUAL

Para el análisis de Riesgo Residual se realiza en base a los riesgos inherentes identificados en la empresa Créditos “Palacio del Hogar”, considerando los siguientes parámetros de mediación mediante un análisis cuantitativo:

Probabilidad de Ocurrencia:

- Alta: considerando que la probabilidad de ocurrencia sea de al menos 1 al mes.
- Media: considerando que la probabilidad de ocurrencia sea de al menos 1 vez al año.
- Baja: considerando que la probabilidad de ocurrencia sea una en 5 años o no haya sucedido.

Impacto:

- Alto: que la ocurrencia del escenario sea de gran impacto en el proceso.
- Medio: que la ocurrencia del escenario sea de mediano impacto en el proceso.
- Bajo: que la ocurrencia del escenario sea de bajo impacto en el proceso.

Calificación de Efectividad Individual de Controles:

- Inefectivo: el control no trabaja adecuadamente o no existe.
- Efectivo con Oportunidad de Mejora: el control existe y puede ser mejorado.
- Efectivo: el control existe y trabaja adecuadamente.

Calificación Conjunta de Controles:

- No confiable: los controles no se encuentra implementado en el proceso de la empresa.
- Insuficiente: los controles no proporcionan un nivel de mitigación suficiente en el proceso de la empresa.
- Confiable: los controles tiene un nivel de mitigación adecuado pero aún no es suficiente.
- Adecuado: los controles tienen un nivel adecuado de mitigación de riesgos.

La severidad del riesgo se calcula en base a la probabilidad de ocurrencia y el impacto que este genere. En base a estos parámetros se realiza el análisis de riesgo residual como se muestra en el Anexo “K”, los resultados obtenidos son aceptables porque el UTM Endian permite mitigar los riesgos inherentes encontrados al momento del levantamiento de información.

6.5. ENTRENAMIENTO

En el entrenamiento se lo realiza orientado a otorgar la capacidad de manejo y operación del UTM a la persona encargada designada por el Gerente, que en este caso es el Administrador de la Red de la empresa. El tiempo de duración es de 10 días laborables, con dos horas diarias de capacitación. Para esta capacitación se aborda la siguiente estructura:

Respaldos

- Tipos de Respaldos.
- Configuración de Respaldo Automáticos.

- Configuración de Respaldos Manuales.
- Exportación de Respaldo.
- Restauración de Respaldo

Firewall

- Manejo de Reglas de Redirección de Puertos/NAT de destino.
- Manejo de Reglas de NAT Fuente.
- Manejo de Reglas de Tráfico Enrutado de Entrada.
- Manejo de Tráfico de Salida.
- Manejo de Tráfico entre zonas.
- Manejo de Tráfico VPN.
- Manejo de Tráfico de Acceso al Sistema.

Proxy HTTP

- Configuración Inicial del Proxy HTTP
- Configuración de Clientes del Proxy
- Tipos de Proxy HTTP
- Manejo de Políticas de Acceso.
- Tipos de Autenticación.
- Manejo de Filtrado WEB.

VPN

- Configuración de OpenVPN
- Manejo de Usuarios VPN.

- Instalación y Configuración de OpenVPN en equipos clientes.

Monitoreo

- Monitoreo de todo el Sistema.
- Manejo de estadísticas de UTM.
- Manejo de Ntop para monitoreo de tráfico.
- Registro e Informes de Antivirus ClamAV, Firewall, Servicio Web, OpenVPN, Proxy HTTP, IPS y Sistema.

Servicios Adicionales

- Configuración de Servicios DHCP.
- Administración de IPS.
- Administración de Antivirus ClamAV.

En el Anexo “L” se muestra el documento de capacitación dada a Geovanni Santana quien es al Administrador de la Red y del Centro de Cómputo de la Empresa.

6.6. COMPARATIVA DE SITUACIÓN ACTUAL CON SITUACIÓN ANTERIOR

Con la Implementación del UTM Endian en la empresa de Créditos “Palacio del Hogar” se han creado y mejorado procesos de seguridad que anteriormente no existían o no estaban funcionando de una forma óptima en la

institución, a continuación se detalla una tabla comparativa de la situación Actual y la situación anterior de la empresa:

Tabla 28 Comparativa de Situación Actual vs Anterior de la Empresa

Situación Actual	Situación Anterior
Existe una herramienta de Seguridad UTM	No Existía UTM
Existe Reglas de NAT donde se puede Filtrar los accesos a los servidores	El Acceso a los Servicios eran de forma directa por IP Pública asignada para cada Servidor
Existe un Proxy HTTP que controla la navegación de los Usuarios	No existía Proxy HTTP
La red esta segmentada en Zona Roja, Naranja, Verde, Azul y VPN	No existía segmentación de Red
Todo el Tráfico de las sucursales con enlace de datos es redirigido al UTM	El tráfico era independiente en cada sucursal
Los accesos remotos para los sucursales remotas fuera del enlace de datos se realizan por medio de VPN	La conexión era directa a las IP públicas
Existe registro de todo el tráfico de la red	No existía registro de tráfico
La empresa cuenta con Ntop que es una herramienta de monitoreo en línea del tráfico de la red	No existía ninguna herramienta de monitoreo en línea del tráfico de la red
El UTM cuenta con un IPS incluido	La empresa no contaba con ningún IPS
La empresa cuenta con un Notificador de eventos que envía los correos que sean necesarios al correo del administrador para mantenerlo al tanto de cualquier actividad del UTM	No existía ningún notificador de eventos
Existe un manejo de Backups del UTM automático y manual	No existía ningún tipo de UTM por lo tanto no existía esta opción
La empresa cuenta con herramientas de monitoreo y estadísticas del sistema y de todo el tráfico de red	No existía este servicio
Monitorización de conexión VPN	No existía este tipo de servicio
Existen opciones de escalabilidad si fuere necesario DNS dinámico, control de tráfico SMTP, QoS	No existía estos beneficios de escalabilidad dentro de la empresa
El UTM cuenta con un firewall que filtra el tráfico de entrada, salida, entre zonas, VPN y de acceso al sistema.	No existía ningún firewall perimetral
El acceso al servicio de telefonía IP esta filtrado por los puertos necesarios	El acceso era directo a la IP pública con todos los puertos sin ningún tipo de filtro.
Existen muchas más opciones que la empresa podría usar como es el Proxy FTP, HTTPS, DNS, SMTP,	No se contaba con estas opciones

Situación Actual	Situación Anterior
POP3	
El acceso a la administración del UTM lo tiene el computador del Administrador y el encargado de Soporte.	No existía UTM
Solución a Riesgos para la empresa que tienen relación con la seguridad de la información, por medio de un análisis de riegos tanto inherente como residual, apoyado por los controles que permite la herramienta UTM Endian	Existían Riesgos sin ningún tipo de control.
Las redes quedan subneteadas con la cantidad necesaria para trabajar.	Existían Redes en la empresa que desperdiciaban gran cantidad de direcciones IP
Clasificación de dispositivos por los permisos de navegación y acceso que estos necesiten	Ningún tipo de clasificación
Administración de ACL por medio de reglas individuales o en grupo, por dirección MAC, por dirección IP, por red, por usuario VPN o por Interfaz	No existía administración alguna
Los clientes VPN solo tiene acceso a la dirección IP y puerto necesario para su trabajo todo lo demás está bloqueado	Acceso directo a Ip pública sin filtro de puertos
El proxy http permite condicionar los permisos por horas, por usuarios, por direcciones ip, por navegadores o por MAC.	No existía proxy http
Todos los puertos que no se usan están bloqueados.	Todos los puertos sin filtro
El acceso a las direcciones IP públicas de la empresa solamente es por medio del Puerto del Server OpenVPN	Las direcciones IP Públicas de la empresa estaban visibles para todo el Internet
El acceso desde internet a la zona DMZ-Naranja de la empresa es por medio de VPN o especificando una dirección IP para ser Nateada solamente en los puertos necesarios	No existía Zona DMZ
Las cámaras IP de la empresa pueden ser accedidas solamente por medio de VPN	Eran visibles para todo Internet
Las ventas móviles acceden por medio de VPN al sistema financiero PAC	Accedían a la Ip pública del Servidor financiero PAC

El beneficio adquirido por la empresa es muy importante en el área de la Seguridad de la Información con la implementación del UTM, porque anteriormente no existía ningún tipo de seguridad perimetral, dando como

resultado esto una completa inseguridad a los servidores de la empresa, inclusive, recibiendo ataques como en la descripción del problema se detalla; en la actualidad ya existe en la institución un mayor control para cualquier ataque informático considerando que nada es 100% seguro pero si se ha logrado implementar un tipo de mejora para evitar violaciones de seguridad que perjudiquen la empresa.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El Endian UTM es una herramienta OpenSource que permitió solucionar los problemas de Seguridad existentes en la Empresa de Créditos Palacio del Hogar, otorgando una forma efectiva y amigable para la Administración del Tráfico de Red, siendo esta una herramienta que permite a la empresa tener escalabilidad en sus operaciones de crecimiento a largo plazo.

2. El UTM Endian Firewall Community queda implementado aproximadamente en un 75% de sus funcionalidades, porque algunas aun no son necesarias implementarlas como Proxy SMTP, Proxy FTP, Servidor de Tiempo, Proxy DNS, Servicio SNMP, etc.

3. Quedan establecidos formatos de documentos y normativas para el registro de nuevas reglas en el UTM con el fin de tener mayor control y registro de las actividades del equipo.

4. La aplicación de los controles por medio del UTM permitieron mitigar todos los riesgos encontrados en la Empresa en la etapa de Levantamiento de Información, porque todos tenían que ver con la falta de control de tráfico de la red y de sus servicios, inclusive, algunos controles tienen oportunidad de mejora.

5. En endian UTM permite monitorear en tiempo real todo el tráfico que circula a través de sus interfaces por medio de la aplicación NTOP, pudiendo realizar filtros y análisis estadísticos de la actividad en el Equipo.

6. El endian UTM guarda registros de Logs del Sistema y de todos sus servicios, siendo estos el Firewall con todas sus reglas, el Proxy HTTP, las conexiones VPN, los resultados del IPS, los resultados del Antivirus ClamAV, y todo lo concerniente al tráfico de toda la red.

7. El UTM se actualiza automáticamente de forma diaria, quedando instalada la última versión que es la 3.2.2, con sus últimas bases de datos de todos sus servicios.

8. Todas las reglas quedan aplicadas en base al levantamiento de información realizado, pudiendo estas ser desactivadas o modificadas si fuere necesario, así como también crear nuevas reglas, realizando el respectivo registro en la documentación de los Anexos.

9. Las conexiones VPN utilizan el Servidor OpenVPN del UTM para el control de tráfico de conexiones externas, por medio de usuarios que pueden tener acceso a determinados y filtrados servicios de la empresa.

10. Todas las direcciones de IP Públicas de la empresa de Créditos “Palacio del Hogar” se encuentran filtradas en sus 65535 puertos, y solo habilitado por VPN cualquier tipo de conexión desde el Internet.

11. Las redes con enlace de datos de las sucursales forman parte de la Zona Roja de la Empresa determinada por el UTM, y en las políticas son tratadas como tales para acceder a cualquier tipo de servicio, pudiendo ser controladas desde el equipo Endian porque todo el tráfico de red es redirigido hacia su dirección IP.

12. El UTM endian permite realizar análisis estadísticos de todos sus módulos incluyendo gráficas, siendo estos: estado del Sistema, estado del Hardware del equipos, estado de la Red, estado del Antivirus, estado del Servidor VPN, estado del Firewall, estado del Proxy HTTP.

13. El 15 de enero del año 2017 el UTM endian resistió un ataque de fuerza bruta que quiso vulnerar la seguridad del login de la aplicación, este proceso duro aproximadamente 12 horas, y fue notificado al correo del administrador de la red con aproximadamente 30000 correos.

RECOMEDACIONES

1. Realizar monitoreo diario del tráfico de Endian UTM con el fin de controlar cualquier anomalía que pueda suscitarse en el dispositivo, pudiendo ser esta algún tipo de ataque constante con el fin de vulnerar la seguridad de la empresa.

2. Usar los formatos de documentos elaborados, y si fuere necesario crear nuevos formatos para tener un control más óptimo de las seguridades de la empresa.

3. Considerar a futuro obtener una herramienta para independizar el acceso VPN de la empresa, pero siempre detrás del UTM, tomando en cuenta que al ser un Software OpenSource no contiene todas las implementaciones de seguridad adicionales, que en la actualidad es sugerida por empresas que comercializan este tipo de dispositivos.

4. Verificar constantemente si existe alguna nueva versión del UTM para inmediatamente instalarla para evitar cualquier tipo de Exploit que pudiere generarse con el paso de versiones.

5. Realizar mantenimiento del hardware del equipo mínimo dos veces al año, es decir cada 6 meses con el fin de mantener sus partes en buen estado de operación y evitar la caída del servicio.

6. Registrar en los formatos la creación, modificación, eliminación o desactivación de alguna de las reglas del UTM, con la debida autorización y firma de las personal involucradas en el proceso.

7. Realizar en lo posible un análisis de Riesgo Inherente al año, con el fin de aplicar controles que permitan mantener un buen nivel de seguridad de la información en la empresa de Créditos “Palacio del Hogar”.

8. Considerar la posibilidad de configurar un equipo adicional con las mismas configuraciones, con el fin de mantener la continuidad del Servicio en beneficio de la empresa y de sus colaboradores, tanto internos como externos.

9. Realizar capacitaciones y talleres de seguridad para los empleados de la empresa, para obtener un nivel mucho más alto de seguridad, contando con personal interno idóneo en el manejo de la información, porque toda la seguridad no solo depende el equipo UTM.

BIBLIOGRAFÍA

[1] Bontupalli, V., & Taha, T. M. (2015). Comprehensive survey on intrusion detection on various hardware and software. En 2015 National Aerospace and Electronics Conference (NAECON) (pp. 267-272). https://doi.org/10.1109/NAECON.2015.7443081

[2] Kaspersky Lab Mexico. (s. f.-b) ¿Qué es la gestión unificada de amenazas (UTM)?, http://latam.kaspersky.com/mx/internet-security-center/definitions/utm, fecha de consulta 10 de mayo de 2016

[3] E.800: Definiciones de los términos relativos a la calidad de servicio, https://www.itu.int/rec/T-REC-E.800-200809-I/es, fecha de consulta 15 de mayo del 2016

[4] Amendment to Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications-Aggregation of Multiple Link Segments. (2000). IEEE Std 802.3ad-2000, i-173. https://doi.org/10.1109/IEEESTD.2000.91610

[5] Srisuresh, P., & Holdrege, M. (s. f.). IP Network Address Translator (NAT) Terminology and Considerations, https://tools.ietf.org/html/rfc2663, consultado el 17 de mayo del 2016

[6] Control de aplicaciones. Panda Security, http://www.pandasecurity.com/homeusers/downloads/docs/product/help/gl/2016/sp/04.htm, consultado el 18 de Mayo del 2016

[7] Gartner Reprint. (s. f.-b), https://www.gartner.com/doc/reprints?id=1-3GF2LZD&ct=160830&st=sb&elqTrackId=6A6D2182D022250B184DFD10C5D49112&elq=c52c5c0298794f4e9a9a959bb9e4fc78&elqaid=3226&elqat=1&elqCampaignId=, consultado el 20 de mayo del 2016

[8] Comparing the best UTM products in the industry. (s. f.-b), http://searchsecurity.techtarget.com/feature/Comparing-the-best-UTM-products-in-the-industry, consultado el 20 de mayo del 2016

[9] SG UTM: Gestión unificada de amenazas de última generación con espacio seguro de firewall | Sophos UTM 9. (s. f.), https://www.sophos.com/es-es/products/unified-threat-management.aspx, consultado el 21 de mayo del 2016

[10] Zentyal Server | Zentyal. (s. f.-b), http://www.zentyal.com/zentyal-server/, consultado el 21 de mayo del 2016

[11] Endian UTM 3.2 Reference Manual — Endian UTM 3.2 Reference Manual. (s. f.), http://docs.endian.com/3.2/utm/index.html, consultado el 25 de mayo del 2016

[12] Endian - Secure everyThing: Firewall UTM, Hotspot, VPN, IoT. (s. f.), http://www.endian.com/, consultado el 23 de mayo del 2016

[13] HDCO. Tipos De Ataques Más Comunes A Sitios Web Y Servidores.(2014, septiembre 9), http://blog.hostdime.com.co/tipos-de-ataques-mas-comunes-a-sitios-web-y-servidores/, consultado el 25 de mayo del 2016

[14] Ignacio Pérez. Comprendiendo la vulnerabilidad XSS (Cross-site Scripting) en sitios web (2015, abril 29), http://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/, consultado el 28 de mayo del 2016

ANEXOS

Anexo “A”. Comparativa de Performance de UTMs

Product	Firewall Throughput (Rated)	VPN Throughput (Rated)	Maximum Users
Entry-level/Small Office UTM Appliances			
Barracuda X Series	1 to 1.9 Gbps	100 to 200 Mbps	100 to 200
Check Point NG Threat Protection Appliances	750 Mbps to 3 Gbps	140 to 400 Mbps	Up to 100
Cisco Meraki	200 Mbps	70 Mbps	50
Dell SonicWall NSA Series	600 Mbps to 1.9 Gbps	150 Mbps to **1.1 Gbps**	25 to 250
Fortinet FortiGate	800 Mbps to 2.5 Gbps	350 Mbps to 1 Gbps	10 to 600
Juniper SRX Series	700 Mbps to 5.5 Gbps	75 to 800 Mbps	N/A
Sophos SG Series	1.5 to **6 Gbps**	325 Mbps to 1 Gbps	**Unrestricted**
WatchGuard	200 Mbps to 1.4 Gbps	30 to 240 Mbps	200 to 500
Midrange UTM Appliances			
Barracuda X Series	2.1 to 6 Gbps	300 to 800 Mbps	300 to 1,000
Check Point NG Threat Protection Appliances	3 to 30 Gbps	1.2 to 2.5 Gbps	Up to 1,500
Cisco Meraki	250 to 750 Mbps	70 to 200 Mbps	500
Dell SonicWall NSA Series	3.4 to 9 Gbps	1.5 to 4.5 Gbps	1,000 to 4,000
Fortinet FortiGate	8 to 16 Gbps	200 Mbps to 14 Gbps	600 to 2,000
Juniper SRX Series	7 to **55 Gbps**	1.5 to **15 Gbps**	N/A
Sophos SG Series	11 to 27 Gbps	1 to 5 Gbps	**Unrestricted**
WatchGuard	2 to 14 Gbps	250 Mbps to 10 Gbps	**Unrestricted**
High-end UTM Appliances			
Check Point NG Threat Protection Appliances	77 to 110 Gbps	17 Gbps to 50 Gbps	1,500+
Cisco Meraki	1 Gbps	500 Mbps to 1 Gbps	10,000
Dell SonicWall NSA Series	12 Gbps	5 Gbps	6,000
Fortinet FortiGate	10 to 45 Gbps	17 to 25 Gbps	20,000
Juniper SRX Series	65 Gbps to **2 Tbps**	22 to **100 Gbps**	N/A
Sophos SG Series	40 to 60 Gbps	8 to 10 Gbps	**Unrestricted**
WatchGuard	10 to 35 Gbps	2 to 10 Gbps	**Unrestricted**

TechTarget

Anexo “B”. Comparativa de Precios de UTMs

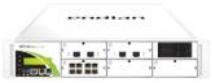
Product	Lowest Cost	Highest Cost
Barracuda X Series*	$1,430	$12,620**
Check Point Next Generation Threat Prevention Appliances	$11,300	$200,000+
Cisco Meraki	$895	$47,995
Dell SonicWall NSA Series	$1,700	$29,995
Fortinet FortiGate	$640	$130,000+
Juniper Networks SRX Series	$1,700	$60,350
Sophos SG Series	$640	$61,600
WatchGuard XTM and Firebox	$420	$84,990

*Barracuda does not require customers to purchase per-user, per-module or VPN licenses. However, customers must purchase an Energize Updates and Instant Replacement Subscription for each Barracuda product.

**Price for the highest cost Barracuda appliance, which is considered a mid-range product.

TechTarget

Anexo “C”. Endian Hardware

Small Networks	Endian UTM Mini 25	Endian UTM Mini 25 WiFi	Endian UTM Mercury 50
			
Firewall Throughput	1.2 Gbit/s	1.2 Gbit/s	1.55 Gbit/s
VPN Throughput (IPsec & SSL)	120 Mbit/s	120 Mbit/s	155 Mbit/s
IPS Throughput	100 Mbit/s	100 Mbit/s	120 Mbit/s
Antivirus Throughput (Proxy)	120 Mbit/s	120 Mbit/s	150 Mbit/s
Web Security Throughput	180 Mbit/s	180 Mbit/s	250 Mbit/s
Concurrent Sessions	300,000	300,000	300,000
Medium Networks	**Endian UTM Mercury 100**	**Endian UTM Macro 250**	**Endian UTM Macro 500**
			
Firewall Throughput	2.5 Gbit/s	5.1 Gbit/s	10 Gbit/s
VPN Throughput (IPsec & SSL)	220 Mbit/s	880 Mbit/s	1.4 Gbit/s
IPS Throughput	160 Mbit/s	590 Mbit/s	900 Mbit/s
Antivirus Throughput (Proxy)	250 Mbit/s	1.4 Gbit/s	2.5 Gbit/s
Web Security Throughput	400 Mbit/s	2.7 Gbit/s	4.8 Gbit/s
Concurrent Sessions	500,000	1,500,000	2,500,000
Large Networks	**Endian UTM Macro 1000**		**Endian UTM Macro 2500**
			
Firewall Throughput	20 Gbit/s		30 Gbit/s
VPN Throughput (IPsec & SSL)	2.5 Gbit/s		4 Gbit/s
IPS Throughput	1.8 Gbit/s		2.5 Gbit/s
Antivirus Throughput (Proxy)	3.5 Gbit/s		5 Gbit/s
Web Security Throughput	10 Gbit/s		15 Gbit/s
Concurrent Sessions	2,500,000		5,000,000

Anexo “D”. Entrevista a usuarios de la Empresa

Créditos Palacio del Hogar
El Rey de los Créditos

Guayaquil, 02 de Junio del 2016

1. **¿Qué accesos necesitan para su trabajo?**
   - Acceso al Sistema PAC
   - Extensiones de teléfonos
   - Páginas de trabajo como el SRI, Ministerio de Trabajo, Registro Civil, Seguro Social, entre otros.
   - Páginas de facturación electrónica y para consultar productos como CARTIMEX, MAVESA, TECNOMEGA, COMPUMICRO, CHAIDE/CHAIDE y otros.
   - Correo Institucional.
   - Sitios de consulta en general, mercados en línea.
   - Servicios de Nube Hotmail, google, Dropbox, MyCloud, ICloud, etc.

Ing. Cristhian Apunte
Jefe de Recursos Humanos

Ing. Guido Miguez
Implementador

Créditos "Palacio del Hogar"
Cristian Apunte Medina
APODERADO GENERAL / GERENTE RRHH
FECHA:

Anexo “E”. Entrevista a Gerente General

Créditos Palacio del Hogar
El Rey de los Créditos

Guayaquil, 01 de Junio del 2016

1. **¿A qué páginas web deben acceder los usuarios?**
   Deben acceder solo a páginas de trabajo, no a redes sociales ni videos.
2. **¿Necesita permisos de Internet para redes sociales y otras páginas para algún usuario de la empresa?**
   Si, para el contador, para la Srta. Ana Lucía, el administrador de la red y para mí.
3. **¿Quién puede acceder a los equipos biométricos?**
   Solo el Ing. Cristhian Apunte que es el Encargado de Recursos Humanos.
4. **¿El administrador de toda la red y del área informática de la empresa debe tener acceso a todo para soporte?**
   Sí, porque tiene que dar soporte a toda la empresa, de ahí nadie más debe tener.
5. **¿Quiénes deben acceder al Sistema Financiero PAC?**
   Todos los Usuarios
6. **¿Quiénes deben acceder al Servidor de Telefonía IP?**
   Todas las sucursales que tienen teléfonos y Yo desde cualquier parte que me encuentre.
7. **¿Quiénes pueden ver las Cámaras de la Empresa?**
   La Srta. Ana Lucía Juela solo dentro de la empresa y Yo de cualquier parte.
8. **¿Para las sucursales de la provincia de Santa Elena que necesita?**
   Acceso al Sistema PAC, una extensión de teléfono y poder ver las cámaras.
9. **¿Algún tema adicional?**
   Si, La empresa Equifax y Provedatos debe tener acceso al Sistema Financiero porque están realizando una implementación, quiero un acceso inalámbrico con permisos de internet solo cuando haya reuniones con gente externa, WhatsApp para los celulares en las sucursales, y quiero tener acceso desde mi iPhone a reportes y grabaciones de telefonía.

CRÉDITOS PALACIO DEL HOGAR
GERENTE GENERAL
Firma Autorizada

Alberto Flueta Valdez
Gerente General

Ing. Guido Miguez
Implementador

Anexo “F”. Registro de Direcciones MAC que son ingresadas al Firewall

Créditos Palacio del Hogar
El Rey de los Créditos

Registro de Direcciones MAC que son Ingresadas al Firewall

Ord.	Dirección MAC	Dirección IP	Nombre del Equipo	Usuario Encargado	Número de Regla	Fecha	Observaciones

Geovanni Santana

Administrador de Centro de Cómputo

Anexo “G”. Registro de Reglas en el UTM

Créditos Palacio del Hogar
El Rey de los Créditos

Registro de Reglas en UTM

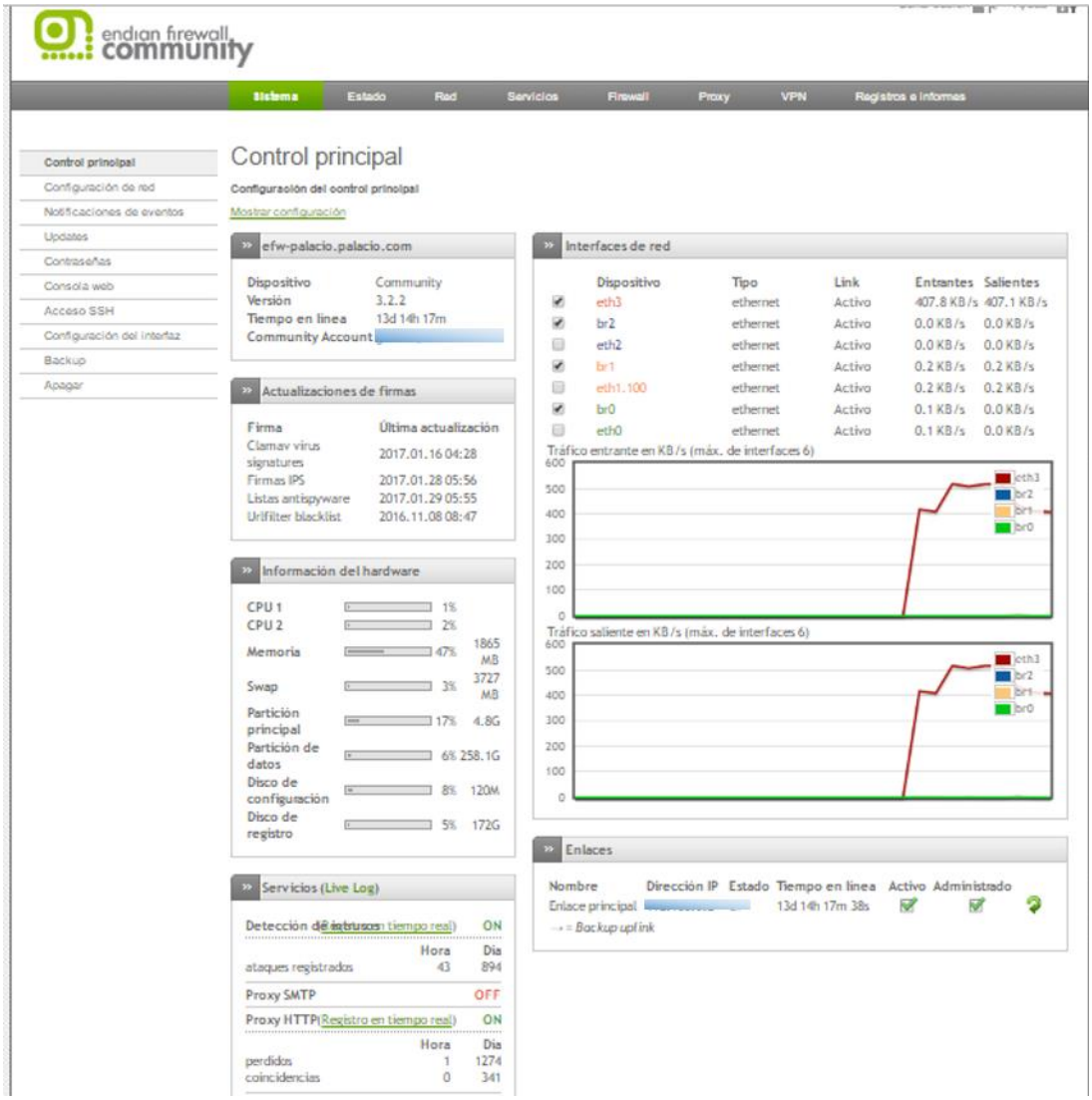
Fecha:

Nombre de usuario:

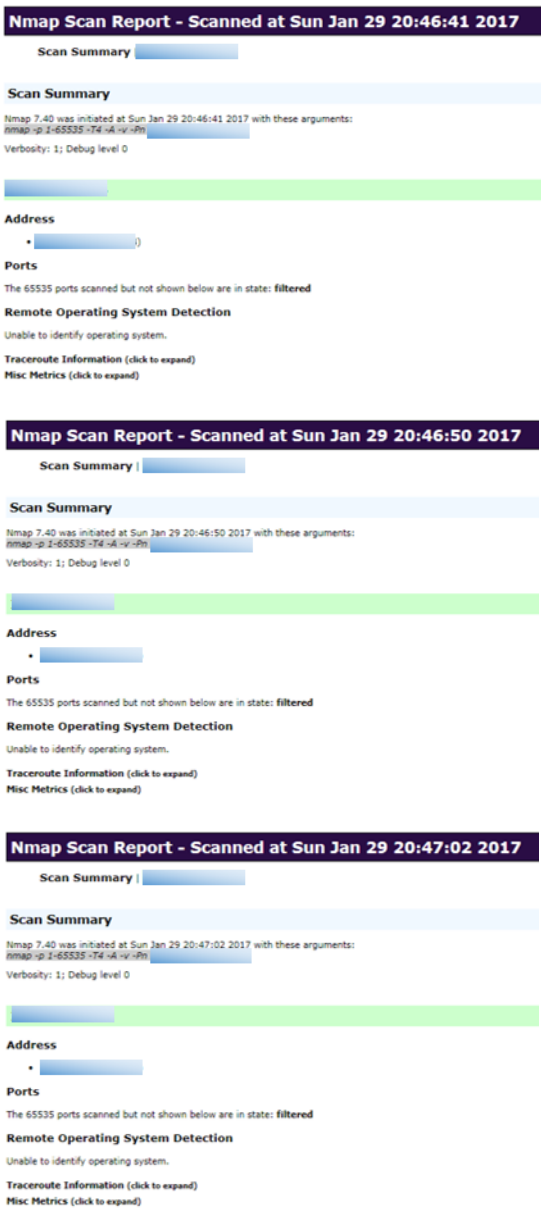
Ord.	Origen	Destino	Servicio	Política	Tipo de Regla	Filtrado Web	Observación

Geovanny Santana Administrador de Centro de Cómputo	Firma de Usuario al que se le otorga el Permiso	Alberto Fuela Gerente General

Anexo “H”. Interfaz Gráfica de Administración Principal de Endian Firewall



Anexo “I”. Resultados de Escaneo Nmap



Nmap Scan Report - Scanned at Sun Jan 29 20:46:41 2017

Scan Summary

Scan Summary

Nmap 7.40 was initiated at Sun Jan 29 20:46:41 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v -Pn

Verbosity: 1; Debug level 0

Address

-)

Ports

The 65535 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)
Misc Metrics (click to expand)

Nmap Scan Report - Scanned at Sun Jan 29 20:46:50 2017

Scan Summary |

Scan Summary

Nmap 7.40 was initiated at Sun Jan 29 20:46:50 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v -Pn

Verbosity: 1; Debug level 0

Address

-

Ports

The 65535 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)
Misc Metrics (click to expand)

Nmap Scan Report - Scanned at Sun Jan 29 20:47:02 2017

Scan Summary |

Scan Summary

Nmap 7.40 was initiated at Sun Jan 29 20:47:02 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v -Pn

Verbosity: 1; Debug level 0

Address

-

Ports

The 65535 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)
Misc Metrics (click to expand)

Nmap Scan Report - Scanned at Sun Jan 29 20:47:09 2017

Scan Summary |

Scan Summary

Nmap 7.40 was initiated at Sun Jan 29 20:47:09 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v -Pn

Verbosity: 1; Debug level 0

Address

-

Ports

The 65535 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)
Misc Metrics (click to expand)

Anexo “J”. Cronograma de Implementación

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predeces	Nombres de los recursos
1		**Implementación de UTM En Créditos Palacio del Hogar**	**163 días**	**mié 1/6/16**	**vie 13/1/17**		
2		**Levantamiento de Información**	**21 días**	**mié 1/6/16**	**mié 29/6/16**		ING GUIDO MIGUEZ
3		Entrevista con Gerente General	1 día	mié 1/6/16	mié 1/6/16		GERENTE GENERAL;ING GUIDO MIGUEZ
4		Entrevista a Usuarios de la Empresa	1 día	jue 2/6/16	jue 2/6/16	3	ING GUIDO MIGUEZ;TRABAJADORES DE LA EMPRESA
5		**Visita DATACENTER de la Empresa**	**6 días**	**lun 6/6/16**	**lun 13/6/16**	**4**	ADMINTRADOR DE RED;ING GUIDO MIGUEZ
6		Revisión de Equipos de Red Existentes	1 día	lun 6/6/16	lun 6/6/16		
7		Revisión de Servicios de la Empresa	3 días	mar 7/6/16	jue 9/6/16	6	
8		Revisión de configuraciones de Red	2 días	vie 10/6/16	lun 13/6/16	7	
9		**Visita a Sucursales**	**12 días**	**mar 14/6/16**	**mié 29/6/16**	**8**	ING GUIDO MIGUEZ
10		Levantamiento en Matriz	2 días	mar 14/6/16	mié 15/6/16		
11		Levantamiento en Sucursal Balerio	2 días	jue 16/6/16	vie 17/6/16	10	
12		Levantamiento en Sucursal Paraiso	2 días	lun 20/6/16	mar 21/6/16	11	
13		Levantamiento en Sucursal San Francisco	2 días	mié 22/6/16	jue 23/6/16	12	
14		Levantamiento en Sucursal Santa Elena	2 días	vie 24/6/16	lun 27/6/16	13	
15		Levantamiento en Sucursal Libertad	2 días	mar 28/6/16	mié 29/6/16	14	
16		Identificación de Riesgo Inherente	21 días	mié 1/6/16	mié 29/6/16		ING GUIDO MIGUEZ
17		**Análisis y Diseño**	**29 días**	**jue 30/6/16**	**mar 9/8/16**	**15**	ING GUIDO MIGUEZ

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predeces	Nombres de los recursos
18		Análisis General	3 días	jue 30/6/16	lun 4/7/16		
19		Análisis de Oficina Matriz y Sucursales	3 días	mar 5/7/16	jue 7/7/16	18	
20		Análisis de Riesgo Inherente	4 días	vie 8/7/16	mié 13/7/16	19	
21		Diseño de Segmentación y restructuración de Red	3 días	jue 14/7/16	lun 18/7/16	20	
22		Diseño de Control de Tráfico	7 días	mar 19/7/16	mié 27/7/16	21	
23		Diseño del Control de Accesos Remotos	3 días	jue 28/7/16	lun 1/8/16	22	
24		Diseño de Formas de Monitoreo	3 días	mar 2/8/16	jue 4/8/16	23	
25		Diseño de Servicios Adicionales de UTM	3 días	vie 5/8/16	mar 9/8/16	24	
26		**Implementación y Pruebas**	**85 días**	**mié 10/8/16**	**mar 6/12/16**	**25**	ING GUIDO MIGUEZ
27		Cambio de Redes en las Sucursales	7 días	mié 10/8/16	jue 18/8/16		
28		Instalación y Configración Inicial del UTM	1 día	vie 19/8/16	vie 19/8/16	27	
29		Creación de Zonas ROJA, VERDE, NARANJA Y AZUL en UTM	1 día	lun 22/8/16	lun 22/8/16	28	
30		Conexión de UTM a la red con configuraciónes Básicas para su funcionamiento	2 días	mar 23/8/16	mié 24/8/16	29	
31		Configuración de Reglas NAT destino	2 días	jue 25/8/16	vie 26/8/16	30	
32		Configuración de Tráfico Entrante	5 días	lun 29/8/16	vie 2/9/16	31	
33		Configuración de Tráfico Saliente	5 días	lun 5/9/16	vie 9/9/16	32	
34		Configuración de Tráfico Inter-Zona	5 días	lun 12/9/16	vie 16/9/16	33	

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predeces	Nombres de los recursos
35		Configuración de Tráfico VPN	5 días	lun 19/9/16	vie 23/9/16	34	
36		Configuración de Acceso al Sistema	7 días	lun 26/9/16	mar 4/10/16	35	
37		Configuración de Proxy HTTP	3 días	mié 5/10/16	vie 7/10/16	36	
38		Configuración de Accesos Remotos	3 días	lun 10/10/16	mié 12/10/16	37	
39		Configuración de Monitoreo	3 días	jue 13/10/16	lun 17/10/16	38	
40		Configuración de Servicios Adicionales	3 días	mar 18/10/16	jue 20/10/16	39	
41		Pruebas y Corecciones de Reglas NAT	5 días	vie 21/10/16	jue 27/10/16	40	
42		Pruebas y Corrección de Reglas en Red Interna y VPN de la Empresa	15 días	vie 28/10/16	jue 17/11/16	41	
43		Pruebas de Vulnerabilidades y Corrección de Acceso al UTM	10 días	vie 18/11/16	jue 1/12/16	42	
44		Pruebas de Notificación de Eventos	3 días	vie 2/12/16	mar 6/12/16	43	
45		**Análisis de Riesgo Residual**	**3 días**	**mié 7/12/16**	**vie 9/12/16**	**44**	ING GUIDO MIGUEZ
46		**Correcciones y Modificaciones de Implementación**	**15 días**	**lun 12/12/16**	**vie 30/12/16**	**45**	ING GUIDO MIGUEZ
47		**Entrenamiento**	**10 días**	**lun 2/1/17**	**vie 13/1/17**	**46**	ADMINTRADOR DE RED;ING GUIDO MIGUEZ

Anexo “K”. Análisis de Riesgo Residual

Información del proceso	Escenarios de riesgo	Análisis de controles					Calificación del riesgo residual		
Proceso	**Escenario**	**Controles**	**Descripción de la implementación del control**	**Tipo de control**	**Efectividad del control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**
Acceso al Servidor del Sistema Financiero (PAC) y la Central IP Elastix tienen asignado directamente una IP pública	Penetración desde Internet por puertos abiertos, Ataque de Fuerza Bruta, Denegación de Servicios, SQLi, entre otros desde el internet, Uso de Servidor desde el internet para Propagación de Spam y Robo de Información y modificación de datos desde el Internet	Creación de Reglas NAT con IPS en el UTM filtrando el tráfico de acceso al Servidor PAC	Permitir el Acceso a los Servicios del PAC solamente al puerto TCP: 80 desde las dirección ip de confianza X	Correctivo	Efectivo	Adecuado	Baja	Bajo	Baja
		Creación de Reglas NAT con IPS en el UTM filtrando el tráfico de acceso al Servidor PAC	Permitir el Acceso a los Servicios de Telefonía IP solamente a los puertos TCP y UDP: 5060-5500, 10000-20000, 8000 y 3478 desde las direcciones ip de confianza X, Y	Correctivo	Efectivo con oportunidad de mejora				

Información del proceso	Escenarios de riesgo	Análisis de controles					Calificación del riesgo residual		
Proceso	**Escenario**	**Controles**	**Descripción de la implementación del control**	**Tipo de control**	**Efectividad del control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**
		Creación de Usuarios VPN para el Acceso a estos servicios	Se realiza la creación de usuarios VPN en el UTM, filtrando en el firewall los permisos únicamente a los servicios de PAC y Telefonía IP	Correctivo	Efectivo				
		Configuración de Notificaciones en el UTM	Configuración de Notificaciones en el UTM de intentos de acceso, inicialización del sistema, caída de enlaces, entre otros eventos adicionales que permitan controlar la operatividad del UTM	Preventivo	Efectivo				

Información del proceso	Escenarios de riesgo	Análisis de controles					Calificación del riesgo residual		
Proceso	**Escenario**	**Controles**	**Descripción de la implementación del control**	**Tipo de control**	**Efectividad del control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**
		Registro Impreso de Nuevos Permisos otorgados	Esto llevará acabo del Administrador de la Red con la respectiva autorización firmada del Gerente General, y responsabilidad del usuario a quien se asigne el permiso	Preventivo	Efectivo con oportunidad de mejora				
Conexión de Sucursales Móviles y de Santa Elena sin ningún túnel de Seguridad	Viaje de información por el Internet sin ningún tipo de Protección	Levantar el Servicio VPN del UTM.	Habilitar el Servicio OpenVPN del UTM Endian, configurando el Certificado, el Puerto y la red VPN	Correctivo	Efectivo	Adecuado	Baja	Bajo	Baja

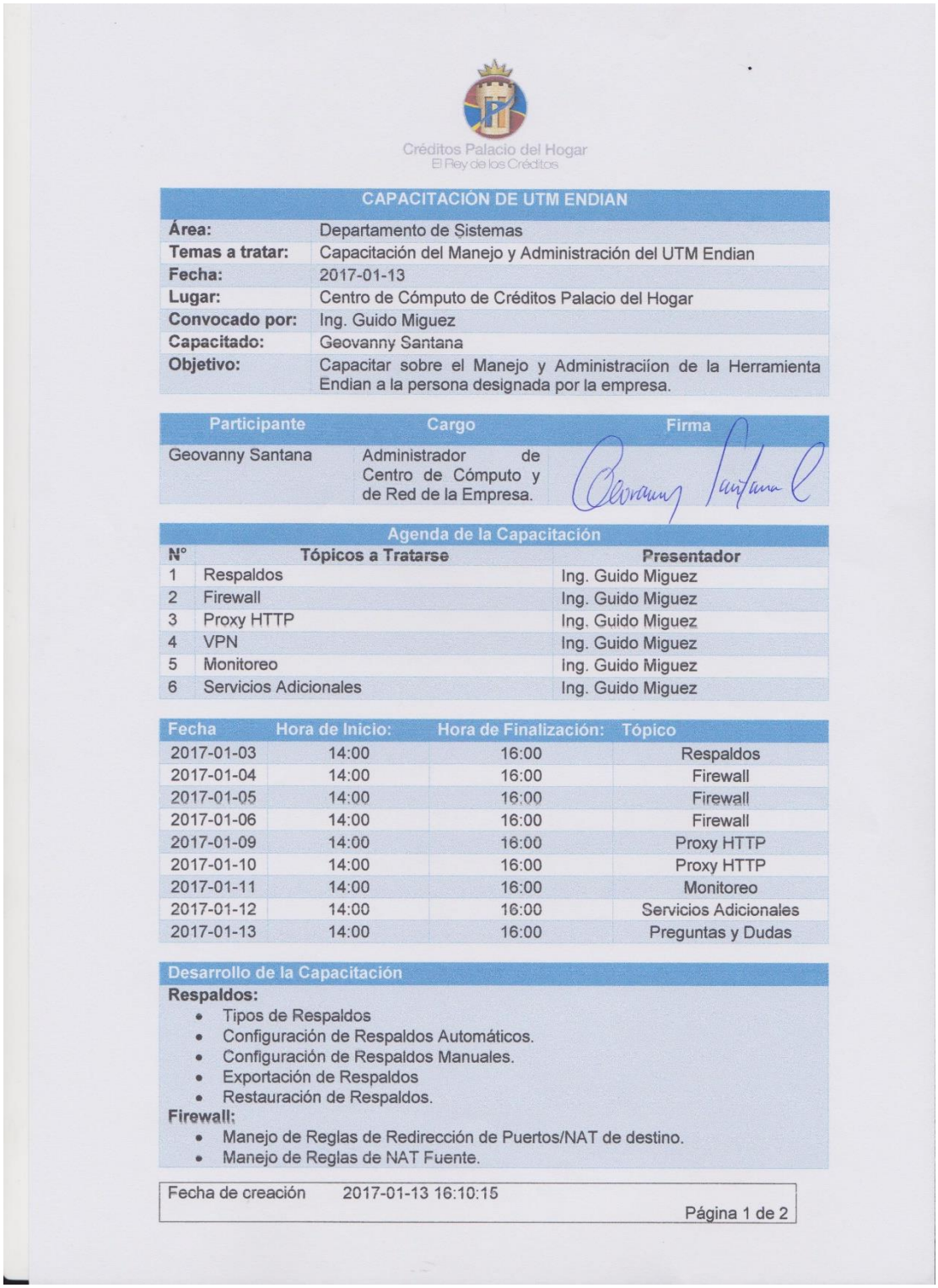
Información del proceso	Escenarios de riesgo	Análisis de controles					Calificación del riesgo residual		
Proceso	**Escenario**	**Controles**	**Descripción de la implementación del control**	**Tipo de control**	**Efectividad del control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**
		Crear Usuarios VPN y filtrar permisos por el firewall del UTM según los accesos que necesiten	Crear usuario para los accesos remotos que sean necesarios por parte dela empresa	Correctivo	Efectivo				
Comparten direcciones IP de la Red LAN con Servidores Internos de la Empresa	Fácil acceso a la información por parte de toda la LAN	Segmentar la Red y Filtrar permisos entre redes	Definir en el UTM Zona Roja, Verde, Naranja, Azul y VPN, y filtrar los permisos necesarios entre ellas	Preventivo	Efectivo	Confiable	Baja	Bajo	Baja
	Mala Administración de Ancho de Banda	Segmentar la Red y Configurar un Proxy HTTP	Definir en el UTM Zona Roja, Verde, Naranja, Azul y VPN, y configurar un proxy HTTP para los usuarios de palacio del hogar	Correctivo	Efectivo				

Información del proceso	Escenarios de riesgo	Análisis de controles					Calificación del riesgo residual		
Proceso	**Escenario**	**Controles**	**Descripción de la implementación del control**	**Tipo de control**	**Efectividad del control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**
	Visualización de equipo desde cualquier red	Bloquear accesos que no sean necesarios en el firewall	Bloquear todo tipo de acceso entre redes incluyendo el Protocolo ICMP, exceptuando equipos que en realidad necesite permisos	Correctivo	Efectivo				
	Duplicidad de direcciones IP	Crear Redes diferentes en la Empresa	Ubicar Servidores en un red independiente de la red de los usuarios	Correctivo	Efectivo				
Acceso a Gateway de Voz desde cualquier red dentro de la empresa	Visualización de equipo desde cualquier red	Filtrar Permisos en Firewall	Configurar en el Firewall del UTM permisos de acceso a la dirección IP del Gateway de Voz solo al Servidor IP y al Administrador de la red	Preventivo	Efectivo	Adecuado	Baja	Bajo	Baja
Mala Segmentación de la Red	Desperdicio del Direcciones IP	Subnetear las Redes de la Empresa	Coordinar con ISP para reconfiguración de redes y Crear redes con tamaño necesario en UTM	Correctivo	Efectivo	Confiable	Baja	Bajo	Baja

Información del proceso	Escenarios de riesgo	Análisis de controles					Calificación del riesgo residual		
Proceso	**Escenario**	**Controles**	**Descripción de la implementación del control**	**Tipo de control**	**Efectividad del control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**
Falta de IPS	Acceso Vulnerable de Intrusos a la Red Interna	Habilitar IPS en el UTM	Habilitar y configurar IPS incluyendo actualizaciones diarias de base de datos de snort	Correctivo	Efectivo	Confiable	Baja	Medio	Baja
Acceso a Internet libre desde cualquier computador de la Red y Falta de Administración de Tráfico de Red	Consumo de Ancho de banda y Navegación en Páginas Peligrosas	Configurar Proxy HTTP	Habilitar Proxy de UTM, crear reglas de filtrado de navegación en e l puerto 3128 y permitir almacenamiento de suficiente cache para una navegación mucho más rápida y controlada.	Correctivo	Efectivo	Adecuado	Baja	Bajo	Baja
Cámaras IP ubicadas del mismo segmento de red que la LAN	Consumo de ancho de banda por exceso de trasmisión de video	Crear Red solo para Cámaras IP	Configurar una red independiente considerada azul para solo cámaras IP y filtrar por Firewall solo direcciones IP específicas	Correctivo	Efectivo	Confiable	Baja	Bajo	Baja

Información del proceso	Escenarios de riesgo	Análisis de controles					Calificación del riesgo residual		
Proceso	**Escenario**	**Controles**	**Descripción de la implementación del control**	**Tipo de control**	**Efectividad del control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**
Puerto 80 de Server Elastix Visible para el Internet	Vulnerable a exploit para cambio de contraseña de Admin	Filtrar Acceso con UTM	Filtrar por dirección IP y acceso VPN el Acceso externo al Servidor	Correctivo	Efectivo	Adecuado	Baja	Medio	Baja
No tener Antivirus Perimetral en la Red	Infección de equipos dentro de la red de la Empresa	Habilitar Antivirus en el UTM	Activar el Servicio de Antivirus ClamAV configurado con actualizaciones diarias y chequeo de todo el tráfico	Preventivo	Efectivo	Adecuado	Baja	Bajo	Baja
No tener Registro Documentación de Control de Accesos y Permisos	Pérdida de control en permisos asignados a los diferentes usuarios	Crear Formato de Documento de Registro de Permisos	Crear un documento donde firme el usuario, el administrador de la red y el gerente general	Correctivo	Efectivo con oportunidad de mejora	Adecuado	Baja	Bajo	Baja
		Habilitar Registro de Logs en UTM	Habilitar el Registro de Logs para todo el tráfico de la red	Correctivo	Efectivo				

Anexo “L”. Entrevistas a Encargado del Centro de Cómputo.



Créditos Palacio del Hogar
El Rey de los Créditos

CAPACITACIÓN DE UTM ENDIAN	
Área:	Departamento de Sistemas
Temas a tratar:	Capacitación del Manejo y Administración del UTM Endian
Fecha:	2017-01-13
Lugar:	Centro de Cómputo de Créditos Palacio del Hogar
Convocado por:	Ing. Guido Miguez
Capacitado:	Geovanny Santana
Objetivo:	Capacitar sobre el Manejo y Administraciíon de la Herramienta Endian a la persona designada por la empresa.

Participante	Cargo	Firma
Geovanny Santana	Administrador de Centro de Cómputo y de Red de la Empresa.	

Agenda de la Capacitación		
N°	**Tópicos a Tratarse**	**Presentador**
1	Respaldos	Ing. Guido Miguez
2	Firewall	Ing. Guido Miguez
3	Proxy HTTP	Ing. Guido Miguez
4	VPN	Ing. Guido Miguez
5	Monitoreo	Ing. Guido Miguez
6	Servicios Adicionales	Ing. Guido Miguez

Fecha	Hora de Inicio:	Hora de Finalización:	Tópico
2017-01-03	14:00	16:00	Respaldos
2017-01-04	14:00	16:00	Firewall
2017-01-05	14:00	16:00	Firewall
2017-01-06	14:00	16:00	Firewall
2017-01-09	14:00	16:00	Proxy HTTP
2017-01-10	14:00	16:00	Proxy HTTP
2017-01-11	14:00	16:00	Monitoreo
2017-01-12	14:00	16:00	Servicios Adicionales
2017-01-13	14:00	16:00	Preguntas y Dudas

Desarrollo de la Capacitación

Respaldos:

- Tipos de Respaldos
- Configuración de Respaldos Automáticos.
- Configuración de Respaldos Manuales.
- Exportación de Respaldos
- Restauración de Respaldos.

Firewall:

- Manejo de Reglas de Redirección de Puertos/NAT de destino.
- Manejo de Reglas de NAT Fuente.

Fecha de creación 2017-01-13 16:10:15

Página 1 de 2

Desarrollo de la Capacitación

- Manejo de Reglas de Tráfico Enrutado de Entrada.
- Manejo de Tráfico de Salida.
- Manejo de Tráfico entre zonas.
- Manejo de Tráfico VPN.
- Manejo de Tráfico de Acceso al Sistema.

Proxy HTTP

- Configuración Inicial del Proxy HTTP
- Configuración de Clientes del Proxy
- Tipos de Proxy HTTP
- Manejo de Políticas de Acceso.
- Tipos de Autenticación.
- Manejo de Filtrado WEB.

VPN

- Configuración de OpenVPN
- Manejo de Usuarios VPN.
- Instalación y Configuración de OpenVPN en equipos clientes.

Monitoreo

- Monitoreo de todo el Sistema.
- Manejo de estadísticas de UTM.
- Manejo de Ntop para monitoreo de tráfico.
- Registro e Informes de Antivirus Clamav, Firewall, Servicio Web, OpenVPN, Proxy HTTP, IPS y Sistema.

Servicios Adicionales

- Configuración de Servicios DHCP.
- Administración de IPS.
- Administración de Antivirus ClamAV.

N°	Compromiso Adquirido	Fecha Asignada (aaaa / mm / dd)	Responsable	Estado
1	Administrar el UTM	2017-01-13	Geovanny Santana	N.A.