# Implementación de una Red Segura para los Laboratorios del DEEE Utilizando un Dispositivo UTM

**ESCUELA POLITÉCNICA DEL EJÉRCITO**
**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA**

Departamento de Ingeniería Electrónica

Cristian Guerra

email: cristhian173@hotmail.com

## 1. RESUMEN

Este proyecto de grado proporciona a la red del Departamento de Eléctrica y Electrónica seguridades a nivel de capa de aplicación en el stack de modelo TCP/IP, filtrado web, reconocimiento de usuarios, funcionalidades de red en capa 2, informes de eventos diarios gestionados por el Administrador de la red y recuperación ante falla unificados en un solo software UTM (Unified Threat Management) con interfaz web al cual se puede acceder por cualquiera de las direcciones públicas asignadas a las interfaces del servidor y por el puerto 443/TCP, usado para la transferencia segura de páginas web HTTPS/SSL.

.

Se incluyen estudios de vulnerabilidades actuales y clásicos que atacan las redes principalmente de las universidades, considerando el hecho de que la mayoría de intrusiones a cualquier red provienen de los mismos usuarios; también se desarrolla un estudio de la mayoría de protocolos usados internamente y así determinar cuáles son los destinos que generan mayor consumo de red, de esta manera se pueden establecer medidas de restricción a páginas consideradas como fraudulentas o a su vez no necesarias dentro de un recinto universitario y estudio

Para el desarrollo del proyecto se cuenta con un estudio de la red del DEEE tanto físico como lógico, en el que se verifican desempeños antes y después de la implementación del mismo, con el propósito de que el servidor sea adaptado a la topología actual de la red, añadiendo servicios y manteniendo los que actualmente se tienen levantados, gestionados por el administrador sobre una interfaz amigable y de fácil configuración, de tal manera que la actualización de los

servicios y funciones puedan ser en cualquier momento actualizados.

## 2. INTRODUCCIÓN

Hoy en día, tal y como se presentan los avances tecnológicos, así mismo se presentan los ataques a redes tanto públicas como privadas, al punto de que no existen redes seguras sino simplemente redes fiables. Entendiéndose como red fiable a toda aquella red que se supone responderá tal y como el planeador de la misma espera que lo haga; es decir, al menos cumplirá con una política de seguridad actualizada y que no sea fácilmente vulnerada.

A breves rasgos, se tiene entendido que una red fiable debe poseer 3 aspectos: confidencialidad, disponibilidad e integridad. Confidencialidad porque a la red sólo deberán acceder aquellas personas autorizadas a hacerlo y que se entiende, no compartirán dichos privilegios con entidades externas al sistema. Disponibilidad porque cada una de los elementos pertenecientes a una red deberán estar accesibles y la gran parte del año. Por último, integridad porque estos elementos de la red sólo podrán ser modificados por quienes son autorizados a hacerlo. Como se ve claramente, cada uno de estos tres elementos depende el uno del otro, y son los que hacen de una red robusta ante ataques.

Se integra en un solo dispositivo de red a la mayoría de los elementos de protección con los que hoy en día se puede contar para una red, como son: Antispam - Antiphishing - Filtro de contenidos - Antivirus - Detección/Prevención de Intrusos (IDS/IPS); mismos que serán implementados en una red ya estructurada y que se encuentra operando. De tal manera que ésta red (red del Departamento de Electrónica de la ESPE) quede operando al finalizar dicho propósito con las tres características ya expuestas anteriormente (Disponibilidad, Confidencialidad e Integridad).

## 3. UTM (Unified Thread Management)

Un UTM (Unified Thread Management) es un dispositivo de red que presta los servicios convencionales de un firewall, también integra otras funciones tales como anti-spam, antivirus, detección de intrusos (IDS/IPS), malware y gestión de tráfico, todo eso a nivel de capa de aplicación. Este administrador de tráfico realiza los procesos a modo de proxy, analizando y permitiendo tráfico en función de las instrucciones implementadas en el dispositivo.

La finalidad de los equipos UTM es el de cada vez ir incrementando mas las capacidades de protección para una red en un solo equipo, sea esta el de una gran empresa o una red local pequeña. Sin embargo, este servicio puede ser de gran utilidad u obsoleto dependiendo de si hubo un estudio de planificación para el correcto uso del mismo.

En la actualidad, el mercado UTM se encuentra en gran apogeo, y según datos publicados hace poco más de un año, éste copará más del 33,6% del negocio de seguridad de redes hasta antes del 2012. Según datos de Europa, solo durante el segundo trimestre del 2009, el mercado de dispositivos de seguridad cayeron aproximadamente un 9,6%, mientras que los dispositivos UTM cayeron hasta el segundo trimestre del año anterior tan sólo un 0,6%, dejando ganancias por sobre los 113 millones de euros. Tan buenas son las cifras estadísticas, que la mayoría de las empresas están cada vez más interesadas en la integración de cada vez más servicios en un solo dispositivo. Empresas como: Juniper, Check Point, Watchguard, Netgear, Stonesoft, Crossbeam Systems y Astaro, Fortinet, Trend Micro, Secure Computing, Cisco, SonicWall, lideran el mercado y compiten para ofrecer mejores servicios.

## 4. TOPOLOGÍA DE RED DEL DEEE

De manera resumida la red de los laboratorios se encuentra conformada de la siguiente manera:

- 3 tarjetas de red, donde cada una de ellas cumplirá con funciones distintas.
- La primera tarjeta de red cumplirá con la función de troncal por dónde pasarán las VLANs y por la que se levantarán los servicios DHCP, DNS.
- La segunda tarjeta de red será GATEWAY para la conexión con el internet que provee la Universidad.
- La tercera tarjeta también será GATEWAY para la otra conexión del Departamento para la salida al internet y por donde solo ciertos usuarios de cada VLAN podrán acceder.
- Un switch de puerto GIGA, mismo que tendrá un puerto nativo y tres puertos designados para cada VLAN ya mencionadas anteriormente.
- Tres switches, cada uno de los cuales direccionará cada VLAN.

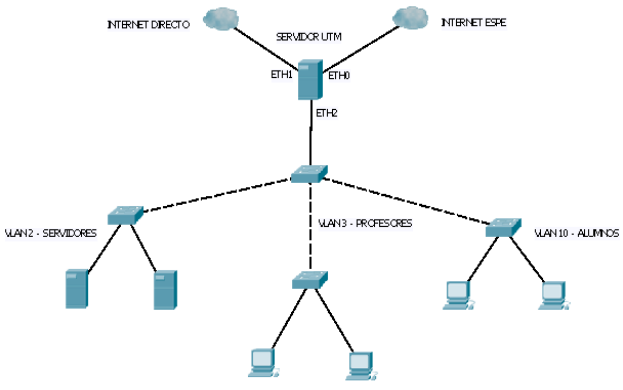


**Figura 1** Topología de la red de pruebas

El servidor actúa como GATEWAY ante las dos salidas que se tiene al internet (FastEthernet 0, FastEthernet 1), que en modo de operación normal, por cada una los usuarios de las VLANs están saliendo dependiendo de cómo se lo determine, pero en caso de falla la una interfaz actúa como back up de la otra, FAILOVER. La interfaz FastEthernet 2 es por donde se levantarán los servidores DHCP y DNS por VLAN, como ya se lo mencionó anteriormente y se lo detalla en la siguiente tabla:

**Tabla 1** Configuración de VLANs

| Interfaz | Red | Name | VLAN |
|---|---|---|---|
| **Eth0** | 201.234.84.173/30 | Red WAN | N/A |
| **Eth2:2** | 10.1.30.1/24 | Red de Profesores | 2 |
| **Eth2:3** | 10.1.29.1/24 | Red de Alumnos | 3 |
| **Eth2:10** | 10.10.0.1/24 | Red de Servidores | 10 |

## 5. IMPLEMENTACIÓN ZENTYAL UTM

Zentyal UTM es conocido en el mercado por su interfaz gráfica muy amigable con el usuario y versatilidad en cualquier topología. Presenta gráficamente al usuario el procesamiento de datos en tiempo real y utiliza herramientas de sistema de GNU y combinación del núcleo o Kernel libre similar a Linux, es decir, que todo el código usado puede ser modificado y redistribuido libremente bajo los términos de la Licencia Pública General de GNU. El proyecto GNU en sí fue creado para mantener un espíritu de cooperación entre los usuarios. Es así que se establece una interacción entre el núcleo del sistema operativo y el usuario o los programas de aplicación.

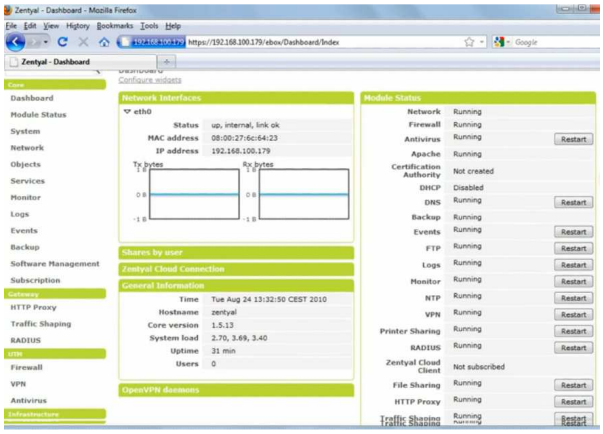


**Figura 2** Interfaz de Zentyal

El círculo verde en la figura 3, es la configuración de GATEWAYS y FAILOVER. Al término FAILOVER se le relaciona con el concepto de tener dos interfaces redundantes y una de ellas en modo standby. En el círculo rojo, describe a la red interna dividida en dos partes, la primera que maneja DHCP por tres VLANs y la segunda en la que un switch capa 2 opera como VLAN nativa. El círculo amarillo es aquella red de servidores con una política de enrutamiento similar a la de ciertos hosts que no tienen restricciones de acceso web o ancho de banda.

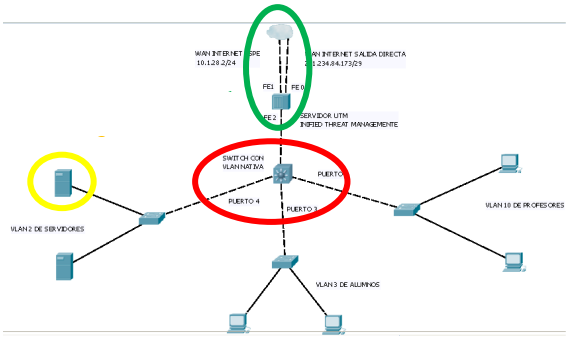

**Figura 3** Topología de la Red del DEEE

En la figura 4, se observa físicamente cómo se encuentran asignadas las interfaces tanto LAN como WAN.

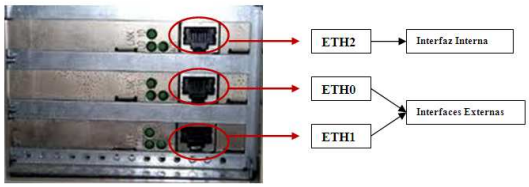


**Figura 4** Posición de las interfaces de red

Para añadir una dirección de DNS, se da click en el botón Añadir del módulo correspondiente y se ingresa la dirección del servidor que resuelve los nombres de dominio, en el primer caso es el 200.31.6.34, servidor gratuito y lo provee el IMPSAT, se lo configura en nuestra red como back up por si el de la ESPE tiene algún problema. Luego, las direcciones de los servidores del DEEE son: **10.1.0.101** y **10.1.0.104.** A la derecha de cada servidor se encuentran unas flechas de color azul apuntando para arriba o abajo, esto es porque se pueden ordenar los servidores por prioridad, siendo el mayor el que se encuentra primero. El nombre del dominio es **espe.edu.ec.**

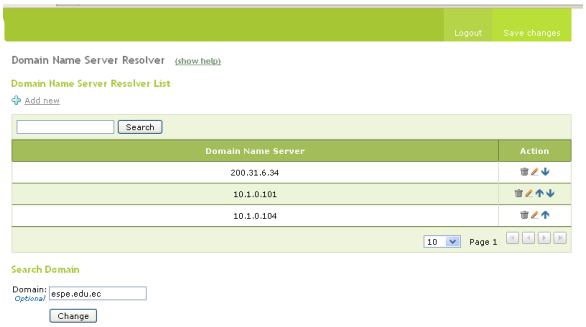


**Figura 5** Direcciones DNS

Para la configuración de las dos interfaces WAN como back up la una de la otra, se debe establecer las dos direcciones IP como GATEWAY. Primero se da click en el botón añadir nuevo y se ingresa los datos de cada interfaz. Para la interfaz ETH0 se da el nombre de la conexión al que está conectado, **INTERNET ESPE,** la dirección de red, **10.1.28.1** y en weight se le da peso, prioridad o importancia en la red, se le configura en 10, por consecuencia es la salida **Default**. Para la interfaz ETH1, el nombre será **INTERNET DIRECTO,** la dirección de red con la que fue configurada, **201.234.84.169** y tendrá un peso de 5. A las dos interfaces se les habilita el visto en la casilla de **ENABLED,** pues las dos estarán en operación.

Para establecer políticas de balanceo de tráfico, se tiene la configuración de acuerdo a la siguiente figura:

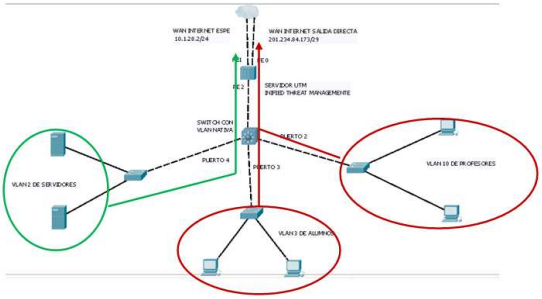


**Figura 6** Política de Balanceo para VLAN2

Como se puede observar en la gráfica anterior, mediante las reglas que se muestran en la siguiente figura 7, se ingresa establece el balanceo de tráfico, así: las interfaces **VLAN2, 3 y 10** tienen como source **ANY,** destination **ANY,** y service **ANY,** es decir, sin importar el destino de los paquetes o de que tipo son, ni a dónde se dirigen van a salir: la VLAN2 por el INTERNET ESPE y las VLANs 3 y 10 por el INTERNET DIRECTO, según la gráfica que se muestra a continuación:


**Figura 7** Políticas de balanceo de tráfico

## 6. CONCLUSIONES

- Se logró implementar en el Departamento de Eléctrica y Electrónica un servidor UTM (Unified Threat Management) que dote de seguridad y protección contra amenazas.
- De acuerdo a la fundamentación teórica analizada se logró determinar que el mecanismo más óptimo y robusto para proteger a la red del Departamento es el software Zentyal UTM, mismo que cuenta con políticas de administración de usuarios, ancho de banda, balanceo de carga, DHCP y DNS.
- Los laboratorios de Electrónica y Redes se encuentra segmentado en redes definidas por 3 VLANs: Profesores, Estudiantes y Masters y se ha precisado el nivel de protección a las tres redes por igual, diferenciándose únicamente por el bloqueo de ciertos tipos de usuarios a páginas que puedan vulnerar la red del DEEE.
- Se adaptó el servidor ZENTYAL UTM a la red del DEEE, comprobando que el direccionamiento en cada interfaz sea el correcto, de tal manera que dos interfaces sean GATEWAY para la salida a internet por dos proveedores distintos y que tengan configurado FAILOVER (recuperación ante fallos), y la tercera interfaz que administre las redes LAN del Departamento y en donde se analiza balanceo de carga, accesibilidad, políticas de direccionamiento en el FIREWALL y filtrado WEB.

- Los hosts del a VLAN de ESTUDIANTES son enrutados exitosamente por la salida a internet que pasa por el departamento de Tecnologías de Información y Comunicaciones de la ESPE, mientras que los miembros de la VLAN de PROFESORES sale directamente a internet.
- Una vez creadas las restricciones de acceso a ciertas páginas de internet para los estudiantes, las pruebas de ping muestran que ya no llegan al destino, es decir, se quedan en el primer salto, que es el servidor UTM.
- Debido a que en el servidor se tiene levantado puertos GIGA tanto hacia las salidas a internet como a la parte LAN, no existen colas de paquetes o paquetes descartados en ninguno de los puertos

## 7. REFERENCIAS BIBLIOGRÁFICAS


- **Cristian Palacios, Andrea Albán**, "DISEÑO E IMPLEMENTACIÓN DE UNA HONEYNET PARA LA RED DEL DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA (DEEE) UTILIZANDO VIRTUALIZACIÓN", Capítulo II, Escuela Politécnica del Ejército, 2011.
- **Joel Snyder, Opus One**, "EVALUATING UNIFIED THREAT MANAGEMENT PRODUCTS FOR ENTERPRISE NETWORKS", QuarkXPress™, Agosto 2006.
- **WatchGuard Technologies; Inc.**, "ZERO DAY PROTECTION", Septiembre 2006.
- **Villalón Huerta, Antonio**, "SEGURIDAD EN UNIX Y REDES", Versión 2.1, Julio 2002.
- **eBox TECHNOLOGIES S.L.**, "ZENTYAL 2.2 OFFICIAL DOCUMENTATION", http://doc.zentyal.org/en/, 2004 – 2011.
- **Marc Catalaa, Jean**, "GUIA DE DIMENSIONAMIENTO FIREWALL/UTM", SONICWALL, Manager, Southern Cone, jmcatalaa@sonicwall.com, Abril 2010.