TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSTGRADO

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA INTEGRADO DE GESTIÓN DE EQUIPOS DE SEGURIDAD

Tesis para optar el Título de Magister en Ingeniería de las Telecomunicaciones, que presenta el Ingeniero:

Ronald Enrique Saavedra Mejía

ASESOR: Mg. Antonio Ocampo Zúñiga

Lima – Septiembre 2015

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

DEDICATORIA

A mi padre, con gratitud y cariño por su incansable apoyo, consejo y ejemplo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

AGRADECIMIENTOS

Principalmente a mis padres por su apoyo y motivación a lo largo de mi formación profesional.

A mi Asesor de Tesis Mg. Antonio Ocampo Zúñiga por compartir su experiencia y orientarme en la realización del presente trabajo.

Al Director de la Maestría en Ingeniería de las Telecomunicaciones, Dr. Carlos Silva Cárdenas y por apoyar en todo momento la realización del presente trabajo de tesis pese a todos los inconvenientes presentados.

A mis jefes de trabajo Mg. Sandro Sánchez Cuzcano, Mg. Francisco Tejada Kubuota por la confianza y apoyo brindado en hacer posible la realización del presente trabajo.

Finalmente agradecer a todas las personas que me acompañaron a lo largo de esta empresa agradecerles por su amistad, consejo y palabras de ánimo.

Muchas gracias a todos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ÍNDICE

RESUMEN 1
INTRODUCCIÓN 2
CAPÍTULO I: ANÁLISIS DE LA PROBLEMÁTICA 3
1.1. ANÁLISIS DE LA PROBLEMÁTICA 3
CAPÍTULO II: MARCO TEÓRICO 4
2.1. ADMINISTRACIÓN DE RED 4
2.2. COMPONENTES BÁSICOS 5
2.3. MODELOS DE GESTIÓN 8
CAPÍTULO III: ESCENARIO DE ESTUDIO 12
3.1. ARQUITECTURA DE RED 12
3.2. SISTEMA DE PREVENCIÓN DE INTRUSOS 14
3.3. CORTAFUEGOS 16
3.4. WEB PROXY 17
3.5. RETOS DE GESTIÓN 18
CAPÍTULO IV: IMPLEMENTACIÓN Y RESULTADOS 21
4.1. DETALLE DEL SISTEMA 21
4.2. FUNCIONAMIENTO DEL SISTEMA 24
4.3. IMPLEMENTACIÓN DEL SISTEMA 26
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 49
5.1. CONCLUSIONES 49
5.2. RECOMENDACIONES 50
REFERENCIAS 51

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ÍNDICE DE FIGURAS

Figura 1 – Administración de Red [1].....4
Figura 2 – Costos Totales de Adquisición [1].....5
Figura 3 – Partes Básicas de la Administración de Redes [1].....6
Figura 4 – Partes del Agente de Administración [1].....7
Figura 5 – Formato MIB SNMP [2].....7
Figura 6 – Modelo de Referencia TMN Jerarquía de Administración [1].....8
Figura 7 – Modelo de Referencia TMN Asociado al Modelo FCAPS [1].....9
Figura 8 – Funcionamiento de Gestión de Servicios de TI [3].....11
Figura 9 – Topología Conexiones de Red.....12
Figura 10 – Disposición de Equipos de Seguridad de Red.....13
Figura 11 – Topología de Alta Disponibilidad de Red.....14
Figura 12 – Topología IPSs.....15
Figura 13 – Topología de Firewalls.....16
Figura 14 – Topología Proxy Web.....18
Figura 15 – Arquitectura del Sistema.....21
Figura 16 – Topología del Sistema.....23
Figura 17 – Entorno de Simulación.....27
Figura 18 – Proceso de Construcción de Gráficas.....29
Figura 19 – Construcción de Gráficas RRDTool.....30
Figura 20 – Tráfico en el Sensor IPS.....32
Figura 21 – Ataques Sensores IPS.....33
Figura 22 – Bytes Procesados en el Sensor IPS.....33
Figura 23 – Conexiones Firewall Check Point.....35
Figura 24 – Consumo CPU Firewall Check Point.....35
Figura 25 – Consumo de Memoria Firewall Check Point.....35
Figura 26 – Paquetes Acceptados Firewall Check Point.....36
Figura 27 – Paquetes Bloqueados Firewall Check Point.....36
Figura 28 – Consumo CPU Nodos Firewall Juniper.....38
Figura 29 – Consumo Promedio Nodos Firewall Juniper.....38
Figura 30 – Consumo Memoria Nodos Firewall Juniper.....39
Figura 31 – Temperatura Nodos Firewall Juniper.....39
Figura 32 – Tráfico Interfaz Firewall CheckPoint.....40
Figura 33 – Tráfico Interfaz Firewall Juniper.....40
Figura 34 – Conexiones Proxy Bluecoat.....42
Figura 35 – Conexiones HTTP Cliente vs Servidor Proxy Bluecoat.....42
Figura 36 – Peticiones Servidor HTTP Proxy Bluecoat.....42

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Figura 37 – Archivos Escaneados ProxyAV Bluecoat. 43
Figura 38 – Virus Detectados ProxyAV Bluecoat. 43
Figura 39 – Ventana de Configuración de Umbrales. 44
Figura 40 – Notificación de Alertas. 45
Figura 41 – Log Notificación de Alertas. 45
Figura 42 – Estado de Equipos Monitoreados. 46
Figura 43 – Panel General Syslog. 46
Figura 44 – Estado de Alertas Syslog. 47
Figura 45 – Reporte Generado con Nectar. 48

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

ÍNDICE DE TABLAS

Tabla 1 – Especificaciones Técnicas de Cacti [8].....22
Tabla 2 – Equipos Virtualizados.....27
Tabla 3 – Tipos de Datos [8].....28
Tabla 4 – IPS Parámetros de Funcionamiento.....30
Tabla 5 – OIDs por Sensor.....31
Tabla 6 – OIDs Indicadores de Tráfico.....32
Tabla 7 – OIDs Performance Firewall Check Point.....34
Tabla 8 – OIDs Performance Nodos Juniper.....37
Tabla 9 – OIDs Proxy Web Bluecoat.....41

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ACRÓNIMOS

IP	Internet Protocol
IPv4	Internet Protocol version 4
LAN	Local Area Network
MIB	Management Information Base
NMS	Network Management System
QoS	Quality of Service
SNMP	Simple Network Management Protocol
RRA	Round Robin Archive
RRD	Round Robin Database
SLA	Service Level Agreement
NOC	Network Operations Center
TMN	Telecommunications Management Network
FCAPS	Fault, Configuration, Accounting, Performance, Security,
TCO	Total Cost Ownership
MIB	Management Information Base
SMI	Structure of Management Information
OID	Object Identifier
ASN.1	Abstract Syntax Notation One
IDS	Intrusion Detection System

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

IPS	Intrusion Prevention System
HA	High Availability
DMZ	Demilitarized Zone
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
RHEL	Red Hat Enterprise Linux
CLI	Command Line Interface
EPEL	Extra Packages for Enterprise Linux
PHP	Personal Home Page
SMTP	Simple Mail Transfer Protocol
MTA	Mail Transport Agent

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

RESUMEN

El presente trabajo de tesis tiene por fin implementar el piloto de una herramienta basada en software libre, a partir de un diseño funcional que nos permita lograr la gestión integrada de distintos dispositivos de seguridad de la información dispuestos en una red en producción. Para ello el desarrollo de este documento se concentra en el uso de Cacti como una herramienta de libre acceso desarrollada en lenguaje de programación PHP, que permite la generación y presentación de gráficas haciendo uso del estándar RRDTool, que mediante el uso de una interfaz web, logra la interacción con la información obtenida de equipos de seguridad heterogéneos a través del protocolo SNMP.

En el primer capítulo se detalla la problemática a tratar en el presente trabajo de tesis, desarrollando en el capítulo segundo los conceptos básicos del proceso de gestión de redes en el contexto de las buenas prácticas de la administración de los servicios de TI, continuando con el detalle del escenario en estudio y el requerimiento de gestión por parte de los equipos a monitorear. Para lograr esto se desarrolló una plataforma de monitoreo haciendo uso de una distribución comercial de Linux, teniendo inicialmente que simular el escenario de estudio incluyendo la mayoría de los equipos involucrados en este trabajo, proceso que se detalla conjuntamente con el proceso de implementación y obtención de resultados en el capítulo cuarto. Para finalmente mostrar la utilidad de la herramienta y como esta puede facilitar el trabajo de administración de equipos de seguridad a partir de la puesta en operación de la herramienta de gestión.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

INTRODUCCIÓN

Los requerimientos actuales de eficiencia y disponibilidad en las redes de datos va en aumento día con día, debido a su constante uso y cada vez más importante papel cuando de lograr una mayor productividad y competitividad se trata. Para lograr ello la administración de redes y las herramientas de gestión se vuelven un factor crítico muy poco tomado en cuenta.

En el mercado actual existe una gran oferta de herramientas orientadas a la integración, monitoreo y administración de redes adecuadas para todo requerimiento y sobre todo en función de los costos de adquisición o licenciamiento. Por ello, la tarea de administrar una variedad de dispositivos de red independientemente de su función, capacidad y particular método de administración, propios de cada fabricante; son razones por las cuales el integrar el monitoreo de diferentes dispositivos a lo largo de una red, se vuelve una tarea extensa y difícil al momento de integrar redes heterogéneas, siendo el uso de soluciones basadas en software libre una propuesta económicamente atractiva en costos de implementación y sobre todo con un gran potencial para su desarrollo.

El alcance del presente trabajo de tesis abarca el desarrollo de un gestor integrado de red en busca de atender necesidades reales de monitoreo y administración de equipos de seguridad informática, a fin de lograr una gestión proactiva que permita optimizar el uso de los recursos y garantizar la disponibilidad de los servicios soportados.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

CAPÍTULO I: ANÁLISIS DE LA PROBLEMÁTICA

1.1. ANÁLISIS DE LA PROBLEMÁTICA

Uno de los objetivos de la gestión de redes es reducir al mínimo la frecuencia y el impacto en el negocio de las condiciones que reducen la disponibilidad o el rendimiento de la infraestructura de red. La gestión eficaz requiere tener información relevante para identificar las causas de origen de problemas que puedan afectar el funcionamiento de la red y tener una base para el análisis de tendencias en el uso de la red, la cual al no ser abordada, podría poner en peligro la disponibilidad o su rendimiento a futuro. La correcta selección de herramientas para proporcionar esta información se vuelve una tarea difícil cuando las herramientas en uso se limitan a brindarnos información genérica, como el uso de ancho de banda, CPU, o paquetes perdidos. Obtener la información de los dispositivos de red en función de información específica y relevante de su funcionamiento es una tarea que muy pocas herramientas pueden lograr, esta es una de las razones por la que cada fabricante ofrece diferentes herramientas de gestión de acuerdo a la tarea o función que desempeña cada equipo. Ante esta heterogeneidad se hace necesario tener una visión integrada de los diferentes dispositivos de red sin importar cuál sea su función para lograr una gestión eficiente de los mismos, razón por la cual el presente trabajo abarca el diseño e implementación de una herramienta integral de gestión de equipos de seguridad informática.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO II: MARCO TEÓRICO

2.1. ADMINISTRACIÓN DE RED

La administración de redes se refiere a las actividades, métodos, procedimientos y herramientas que se refieren a la operación, administración, mantenimiento y aprovisionamiento de sistemas en red [1].

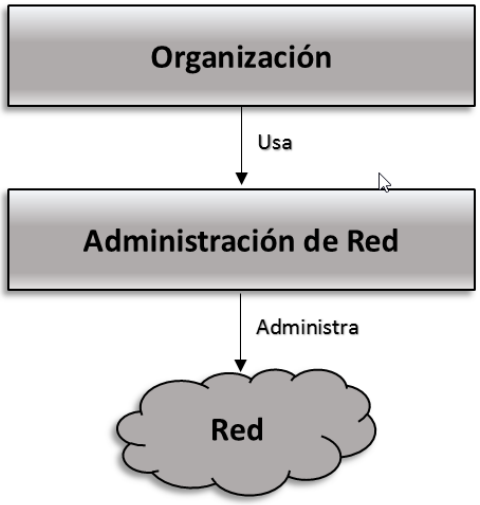

Figura 1 – Administración de Red [1].

- **Operación:** Se ocupa de mantener la red y los servicios que proporciona la red funcionando sin problemas. Incluye el seguimiento de la red para detectar problemas tan pronto como sea posible.
- **Administración**: Se ocupa de hacer el seguimiento de los recursos de la red y la forma en que se asignan para obtener el mejor desempeño de los recursos empleados.
- **Mantenimiento:** se ocupa de realizar reparaciones, implementación de medidas correctoras y preventivas con el fin de asegurar el mejor desempeño de la infraestructura de red durante un tiempo definido.
- **Aprovisionamiento:** se ocupa de la configuración de los recursos de la red para apoyar a un determinado servicio en función de los cambios requeridos y el crecimiento de la red.

La administración de redes eficientes divide la eficiencia en tres aspectos. El aspecto número uno a tener en cuenta son los costos totales de adquisición o TCO detallado en la figura 2. Para

Tesis publicada con autorización del autor
No olvide citar esta tesis

lograr un menor TCO se enfoca la administración de la red en el uso de herramientas que permitan maximizar la productividad del personal de operaciones a un menor costo [1].

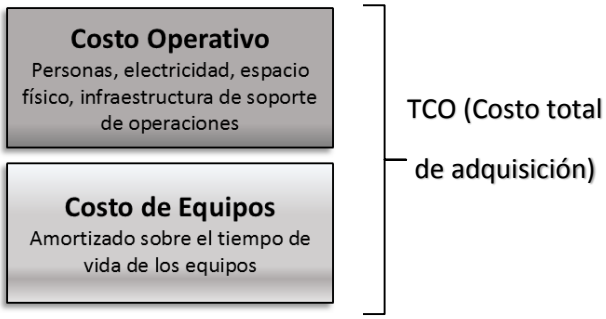

Figura 2 – Costos Totales de Adquisición [1].

El segundo aspecto y no menos importante radica en la calidad de los servicios, definidos por la confiabilidad y disponibilidad de los equipos que los soportan. Para ello lograr asegurar la disponibilidad de cada servicio es una tarea que equivocadamente se concentra solo en lograr redundancia de equipos; teniendo como principal reto anticipar las posibles causas de incidencias y responder en el menor tiempo ante ellas [1].

Finalmente, una red eficiente es aquella que brinda una mayor ganancia en base a la inversión realizada. Habiendo definido los dos aspectos anteriores para la administración eficiente de redes, estos se complementan en busca de obtener una mayor calidad de los servicios a un menor costo teniendo como resultado mayores ganancias.

2.2. COMPONENTES BÁSICOS

Dentro de los componentes de la administración de redes, definidos en a la figura 3, el componente principal reside en el sistema de administración, que consiste en el uso de una aplicación o su conjunto para brindar las herramientas responsables de facilitar las tareas de administración de los dispositivos de red.

Tesis publicada con autorización del autor
No olvide citar esta tesis

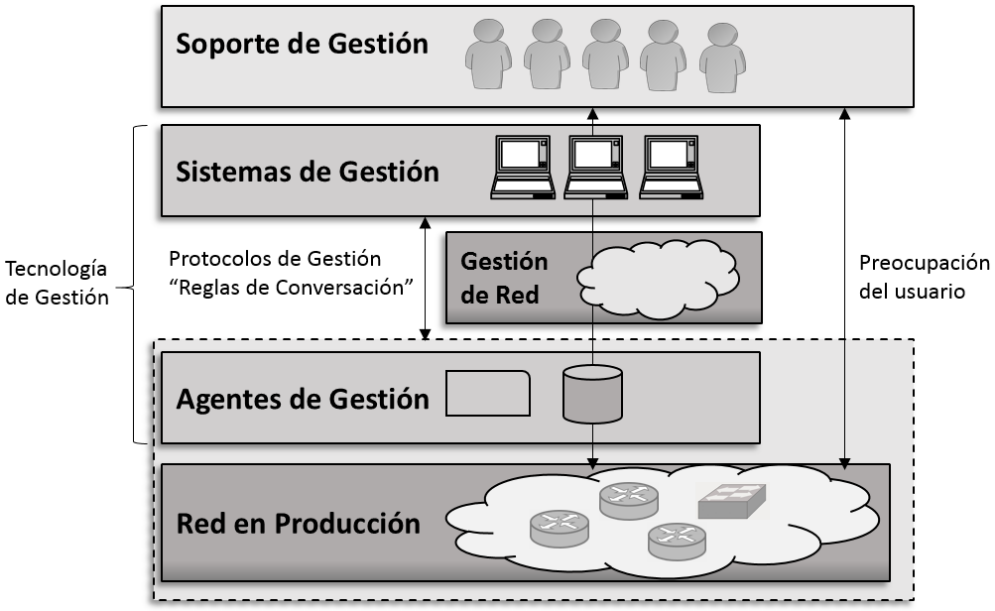

Figura 3 – Partes Básicas de la Administración de Redes [1].

El principio de un sistema de administración de red es el uso de tecnologías que en base al uso de protocolos de comunicación se logre obtener información detallada de los dispositivos de red que facilite la tarea de gestión integrada de los mismos. Para ello se puede disponer de una red dedicada para la administración, cuya principal ventaja es que separa el tráfico de administración del tráfico de la red en producción, obteniendo a partir de ello una menor latencia del tráfico en curso y una mejor disposición de los dispositivos de red frente a vulnerabilidades de seguridad. Pero se debe tener en cuenta que el uso de una red dedicada implica una mayor inversión, razón por la cual en muchos casos resulta ser una opción muy poco atractiva o inviable [1].

Las tecnologías en uso por el sistema son las que proporcionan las herramientas de gestión que haciendo uso de los protocolos de gestión y la información almacenada proveniente de las MIBs, deben lograr la integración de los diferentes dispositivos de red independientemente de su función, fabricante o particularidad de gestión. Para ellos la elección de la aplicación o aplicaciones a utilizar son de gran importancia.

Finalmente los agentes o sistema administrado que corresponde a los dispositivos de red y los componentes que definen el tipo de interacción con el sistema de administración se observa en la figura 4.

Tesis publicada con autorización del autor
No olvide citar esta tesis

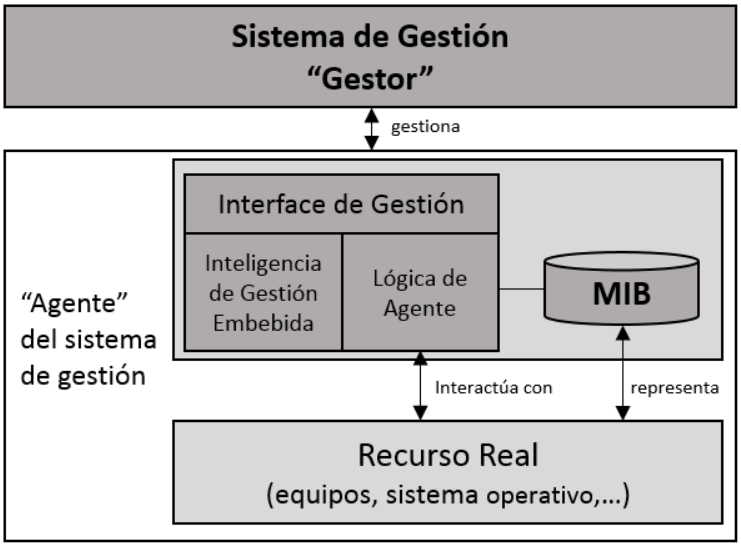

Figura 4 – Partes del Agente de Administración [1].

- **MIB:** Es la base de información de los recursos a administrar que nos permite obtener información representativa y detallada de los mismos. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Se presentan como una estructura jerárquica a modo de árbol definida por una SMI, donde se distribuyen variables de información que son identificadas por octetos definidos por la ASN.1 conocidos como OIDs [2].

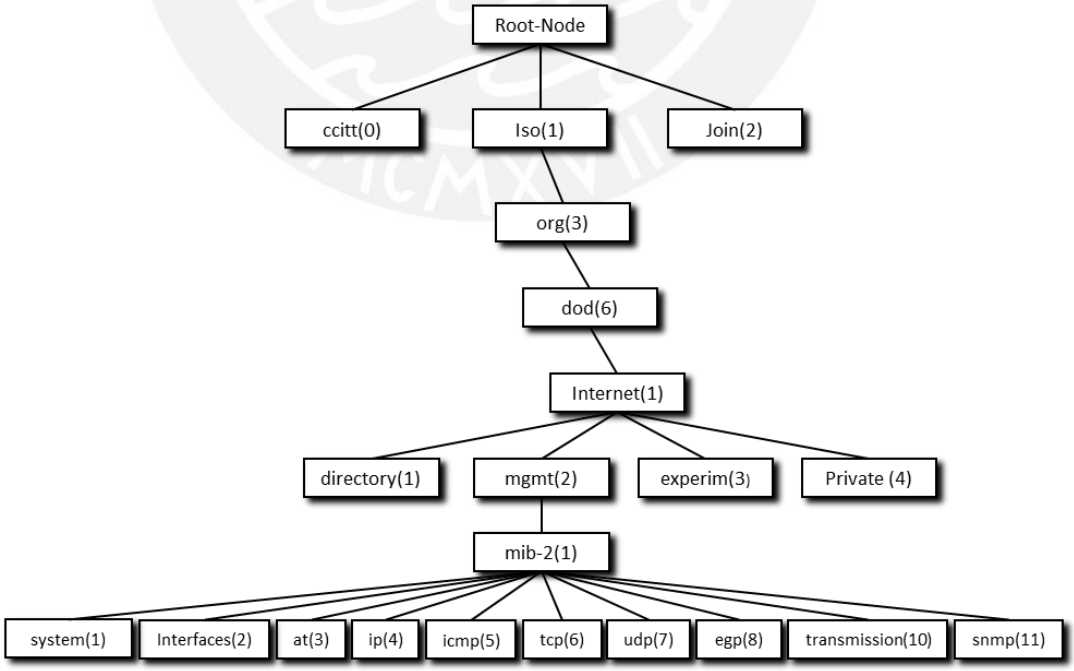

Figura 5 – Formato MIB SNMP [2].

Tesis publicada con autorización del autor
No olvide citar esta tesis

- **Management Interface:** Responsable de soportar el protocolo de gestión que define las reglas de comunicación con el sistema de administración. Para la gestión de los agentes se pueden definir uno o más protocolos de acuerdo al tipo de comunicación que se desea obtener, tanto para la gestión de estado o cambio de los agentes. Entre los protocolos soportados más conocidos tenemos: SNMP, ICMP, telnet, SSH, Netconf, entre otros [1].

- **Core Agent Logic:** Es la responsable de lograr la interacción entre la interface de gestión, la MIB y los recursos o también conocidos como dispositivos de red [1].

2.3. MODELOS DE GESTIÓN

Para la administración de redes, los modelos de referencia de gestión se utilizan como marcos conceptuales para la organización de las diferentes tareas y funciones que forman parte de la gestión de red. Uno de los estándares definido por la Unión Internacional de Telecomunicaciones (UIT-T) para la gestión de una red de telecomunicaciones de donde proviene su nombre TMN. Este estándar cubre una amplia gama de temas relacionados con los principios de utilización de las redes y como estas deben ser administradas en base a la definición de normas a cumplir.

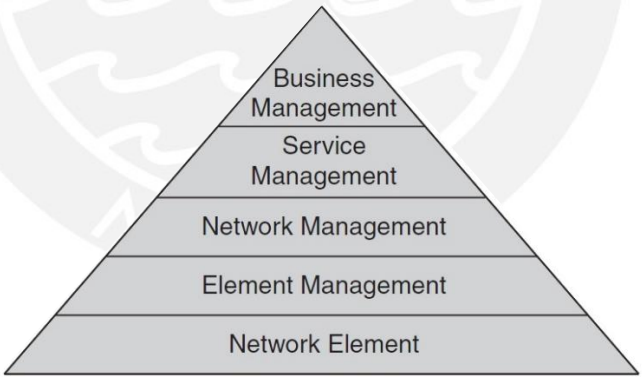

Figura 6 – Modelo de Referencia TMN Jerarquía de Administración [1].

Otro modelo de gestión más comúnmente utilizado divide las funciones de gestión en cinco categorías FCAPS (fault-management, configuration, accounting, performance, and security) modelo que se define en base de los objetivos de trabajo de gestión de red, que en realidad vendría a ser parte de un modelo de referencia de gestión más amplio al modelo de referencia de TMN [1]. El modelo de referencia TMN abarca mucho más que las capas de gestión; la

Tesis publicada con autorización del autor
No olvide citar esta tesis

categorización de funciones de gestión que establece el modelo FCAPS es uno de los conceptos que el modelo TMN establece.

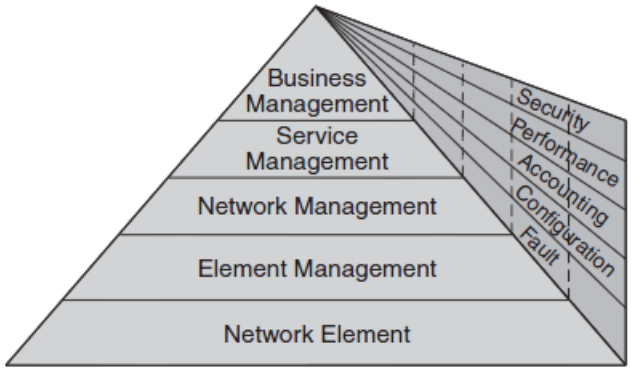

Figura 7 – Modelo de Referencia TMN Asociado al Modelo FCAPS [1].

- **Fault-management:** En este nivel los problemas de red son encontrados y corregidos. Se identifican, y se toman medidas para evitar que se produzcan o se repitan, de este modo, la red se mantiene operativa, reduciendo al mínimo el tiempo de incidencias [1].

- **Configuration:** Esta función contempla la gestión de configuraciones, buscando recopilar la información específica de cada dispositivo en la red (características, capacidades, configuración actual). El objetivo de la función es lograr el control de los cambios que ocurran en los dispositivos de la red. Plantea el registro actualizado de los equipos y programas en uso [1].

- **Accounting:** Conocido también como nivel de asignación, se dedica a la distribución de recursos de manera óptima y equitativa entre los segmentos de la red. Esto hace posible el uso eficaz de los recursos disponibles minimizando el costo de operación [1].

- **Performance:** Nivel involucrado con el manejo del funcionamiento global de la red. Se prioriza maximizar el rendimiento evitando cuellos de botella e identificando los problemas potenciales. Una parte importante del esfuerzo es identificar las mejoras, que lograran mejorar el desempeño general de la infraestructura de red [1].

Tesis publicada con autorización del autor
No olvide citar esta tesis

- **Security:** Este nivel es responsable de asegurar la infraestructura de red, frente a posibles ataques de seguridad. Se asegura la confidencialidad de la información limitando las autorizaciones de acceso en cada segmento de la red [1].

Si bien el marco FCAPS es un gran modelo para la definición de los objetivos de gestión de la red, dentro del enfoque de mejores prácticas para la prestación de servicios de TI que amplía el modelo FCAPS es el Information Technology Infrastructure Library o ITIL, diseñado para proporcionar un mejor marco para ofrecer garantías de calidad hacia la prestación de mejores prácticas de gestión de red. Este modelo define los siguientes equipos de gestión de red [3].

- **Soporte del Servicio:** Esto es típicamente un centro de operaciones de red (NOC) en la mayoría de las organizaciones. El servicio se centra en garantizar la disponibilidad de los servicios de red a los usuarios finales. Esta área se centra en los aspectos de la resolución de problemas, mesa de ayuda y el apoyo a nuevas aplicaciones a través de la red. Funciones que subyacen tras el servicio de apoyo incluyen la gestión de problemas, gestión de configuración y la gestión de cambios [3].

- **Entrega del Servicio:** Factor clave de la gestión del servicio que consiste en asegurar que las aplicaciones soportadas través de la red, vienen siendo ofrecidos de manera consistente. Esta disciplina incluye la gestión de la capacidad y modelado de aplicaciones. Los SLA o acuerdos de niveles de servicio son los parámetros clave utilizados para definir la calidad de servicio entregado a los usuarios finales [3].

- **Gestión de Seguridad:** La seguridad ha sido un enfoque de gestión de red prevalente durante varios años con características claves para asegurar que las amenazas externas se mitiguen median te el uso de cortafuegos y equipos que aseguren los medios de acceso externos a la red. Gestión de la seguridad también incluye gestión de la configuración de los derechos y permisos a través de la red para asegurarse de que no se tenga acceso no autorizado a información confidencial dentro de la red [3].

- **Gestión de Infraestructura:** Es el responsable de la instalación y la configuración física de todos los dispositivos de red de la organización. Cuando los cambios son aprobados por el comité de cambios, la gestión de la infraestructura es la responsable de

Tesis publicada con autorización del autor
No olvide citar esta tesis

hacer cumplir los cambios en base al plan de ejecución realizado por los especialistas involucrados en los cambios [3].

- **Gestión de Aplicaciones:** Se ha diseñado con el único propósito de asegurar que una aplicación tiene la configuración y el diseño apropiados para ser implementado. Esta disciplina debe lograr asegurar que cualquier aplicación implementada esté totalmente habilitada para prestar el servicio al usuario final [3].

- **Gestión de Activos de Software:** Es diseñado para ser la gestión parcial de configuración, ya que proporciona información esencial sobre del software instalado en cada dispositivo. Es responsable licenciamiento y mantenimiento de software [3].

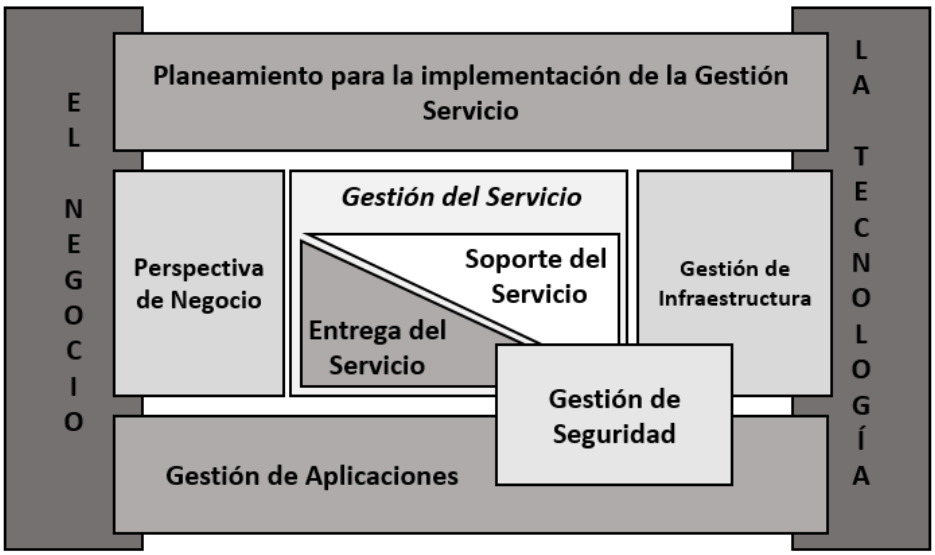

Figura 8 – Funcionamiento de Gestión de Servicios de TI [3].

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO III: ESCENARIO DE ESTUDIO

3.1. ARQUITECTURA DE RED

El escenario sobre el cual se implementará la herramienta de gestión propuesta corresponde a la infraestructura de red de un operador de servicios de telecomunicaciones, responsable de soportar información sensible y confidencial de usuarios, motivo por el cual se mantendrá en reserva el detalle técnico de la información utilizada para la elaboración del presente trabajo.

Para comprender el requerimiento de gestión de red, debemos entender los servicios soportados por los dispositivos de red a gestionar. En la figura 9 se observa de manera global el tipo de conexiones externas, dentro de las cuales tenemos la red MPLS de la empresa, responsable de brindar la interconexión entre las agencias de la empresa a nivel nacional, empresas colaboradoras y segmentos de la red LAN de la empresa. Por otro lado se tiene enlaces externos hacia Internet que hacen posible la salida de tráfico y diferentes tipos de conexiones remotas al interno de la red. Por lo detallado cada una de las conexiones externas de la red soporta servicios de vital importancia para el negocio de la empresa por lo que asegurar la disponibilidad de dichos enlaces y mantener los niveles de seguridad frente a posibles intentos de intrusión en los mismos, es uno de los retos de gestión de la red en estudio.

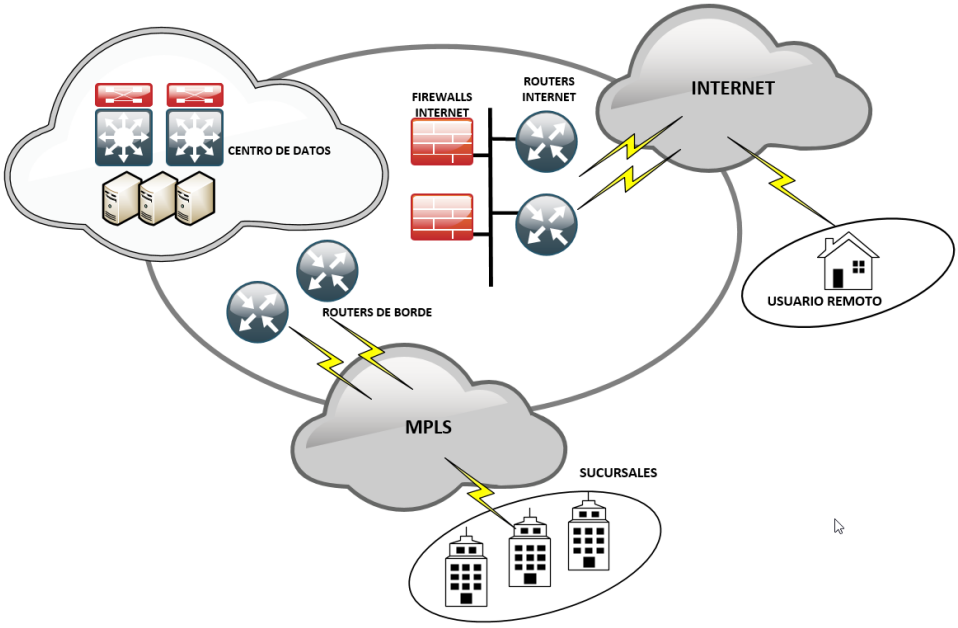

Figura 9 – Topología Conexiones de Red.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Frente a este tipo de conexiones existentes, es de especial atención entender los requerimientos de seguridad tanto entre segmentos de red, frente al requerimiento de acceso de empleados, agencias, empresas colaboradores y requerimientos específicos de comunicación entre segmentos de red de la empresa. Para lo cual la disposición de equipos de seguridad a lo largo de la de la arquitectura de red mostrada en la figura 10, son de vital importancia frente al objetivo de asegurar la integridad de la información, por lo cual tanto la operación como la gestión de los mismos definen un gran reto de gestión por su cantidad, función y heterogeneidad.

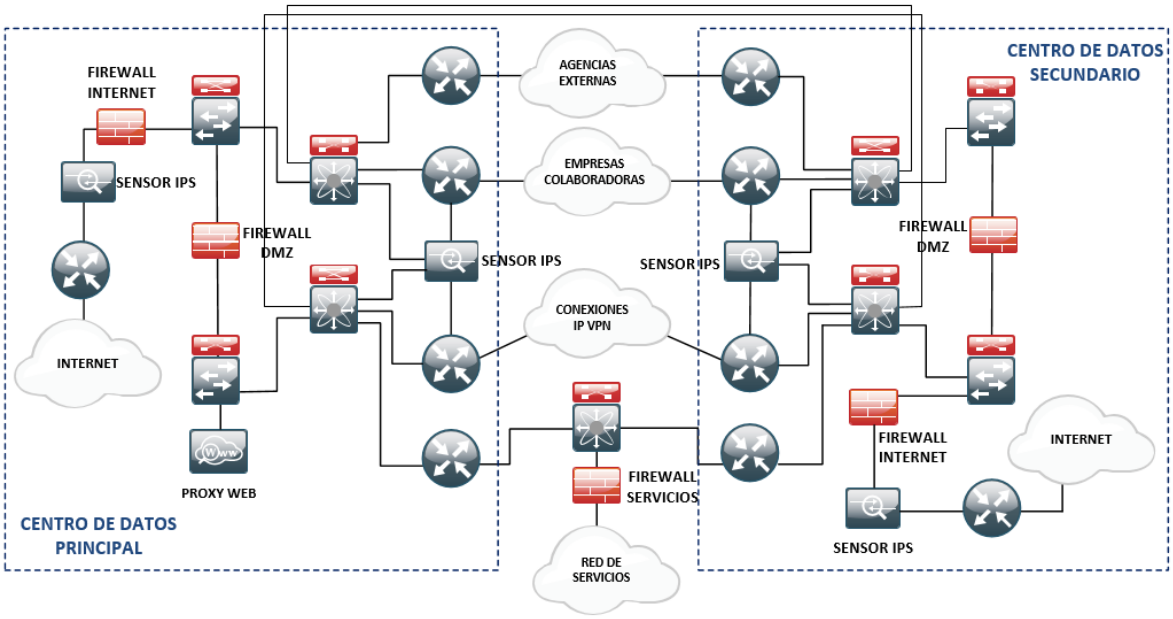

Figura 10 – Disposición de Equipos de Seguridad de Red.

La arquitectura de red atiende al requerimiento de alta disponibilidad de los servicios soportados haciendo uso de una topología de redundancia física frente a desastres concentra su infraestructura de TI en dos centros de datos o nodos interconectados, razón por la cual la mayoría de los dispositivos de función critica como los elementos de seguridad cuentan con redundancia física, es decir cada dispositivo critico cuenta con dos equipos interconectados dispuestos en modo activo – pasivo o activo – activo ubicados físicamente en dos centros de datos diferentes. Teniendo en cuenta que uno de los pocos equipos que no cuenta con ningún tipo redundancia es el proxy web de la red, tal como se observa en la figura 11.

Tesis publicada con autorización del autor
No olvide citar esta tesis

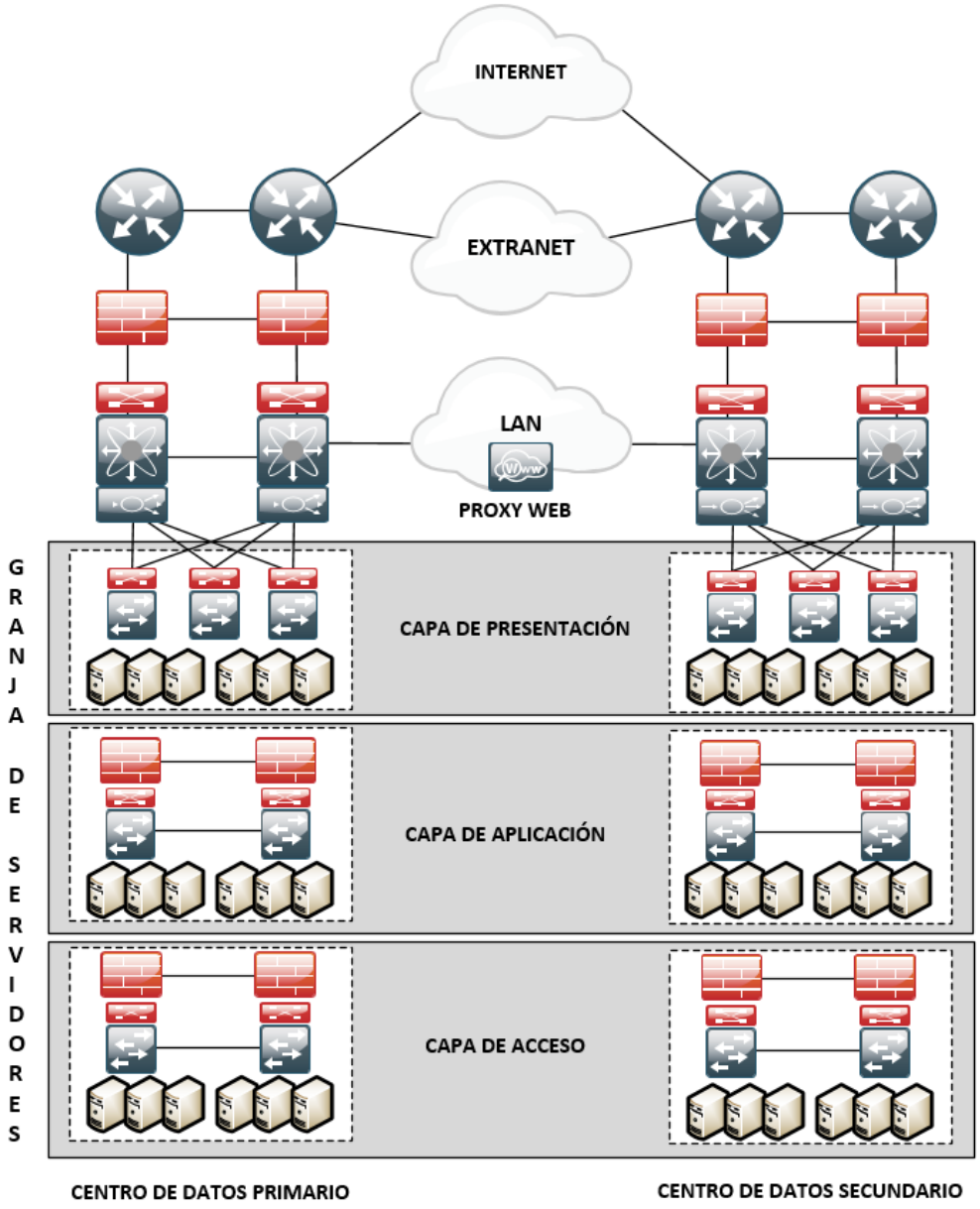

Figura 11 – Topología de Alta Disponibilidad de Red.

Habiendo detallado la infraestructura de red en estudio nos concentraremos en el detalle de los dispositivos de seguridad a ser gestionados por la herramienta propuesta, dentro de los cuales podemos listar a los sensores IPS/IDS, Firewalls y Proxy Web como los principales responsables de garantizar la seguridad al interior de la red en estudio.

3.2. SISTEMA DE PREVENCIÓN DE INTRUSOS

La disposición de los IPS/IDS dentro de la topología de red en uso, los coloca como el primer frente de control de seguridad respecto de ataques tanto de conexiones externas como al interno

Tesis publicada con autorización del autor
No olvide citar esta tesis

de la red, por lo que la disposición de los sensores a lo largo de la red responde a los requerimientos de seguridad de los segmentos más sensibles frente a posibles ataques. La función primaria de un sensor es analizar el tráfico en la red seleccionada para responder cuando se detecte un ataque. El sensor examina cada paquete de red, en busca de patrones y comportamientos en el tráfico de red que indiquen actividad maliciosa. El sensor examina los paquetes según una serie de políticas configuradas que determinan qué tipo de ataques o comportamiento debe ser vigilado y de acuerdo a eso el tipo de respuesta que tendrá el equipo para cada tipo de alerta de acuerdo a su criticidad.

La topología en uso tal como se muestra en la figura 12 contempla la distribución de los sensores de cara a los segmentos más propensos a ser atacados, como por ejemplo la conexión a internet o entre las mismas DMZs. Para ello el tráfico monitoreado por los sensores es centralizado en un equipo de administración o consola de manera de poder tener un detalle de las alertas, amenazas y respuestas del sistema frente a posibles ataques.

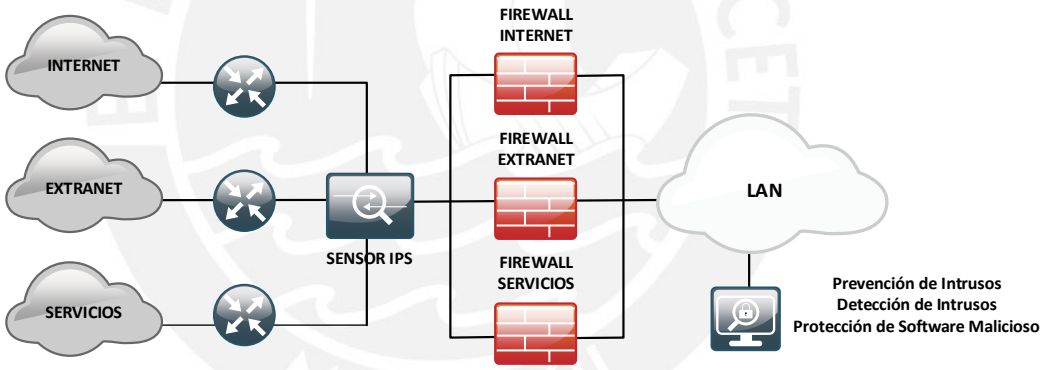

Figura 12 – Topología IPSs.

Las limitaciones de este tipo de dispositivos y su principal vulnerabilidad radica en que por el tipo de detección y atenuación de las amenazas de seguridad responden a los ataques identificados y reportados en las base de datos de los fabricantes, que para su accionar inmediato debe estar plenamente identificado en las firmas de seguridad instaladas en los equipos. Además el modo de trabajo de estos dispositivos, denominado “modo promiscuo” pretende recibir todo el tráfico posible en curso, siendo limitado por el requerimiento de hardware dedicado ya que al ser el objetivo el monitoreo de enlaces principales del orden de 1 a 10 Gigabytes por segundo la capacidad de reflejar dicho tráfico para su monitoreo en algunos casos se descarta como opción limitando su trabajo en número y eficiencia.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Los principales parámetros de funcionamiento de estos equipos responden principalmente al tipo de respuestas generadas respecto del análisis de malware en el tráfico de paso por cada uno de los sensores configurados en el equipo, que en nuestro caso particular dicha información se concentran en la consola de administración, por lo que es de especial atención la información complementaria que podamos obtener a partir de las MIBs de los equipos.

3.3. CORTAFUEGOS

El segundo frente de seguridad responde al uso de firewalls, que se concentran en limitar el tráfico de entrada y salida por cada una de sus interfaces estableciendo el paso o no de los paquetes de datos mediante el filtrado de los mismos en respuesta a la configuración de políticas de seguridad, que son las establecen el tratamiento de los paquetes recibidos en base a su IP de origen, IP de destino, protocolo o puerto en uso. Para ello la disposición de los mismos, al igual que los IPS responde al requerimiento de garantizar el control de acceso no autorizado a la red, tal como se muestra en la figura 13.

El uso de firewalls a lo largo de la infraestructura de red implica un reto mayor ya que no cuenta con una homogeneidad de equipos, es decir no son de similar fabricante por ende son equipos que responden a un entorno de gestión y lógica de funcionamiento totalmente diferentes, que por su número, capacidad y ubicación, convierten su gestión en una tarea compleja.

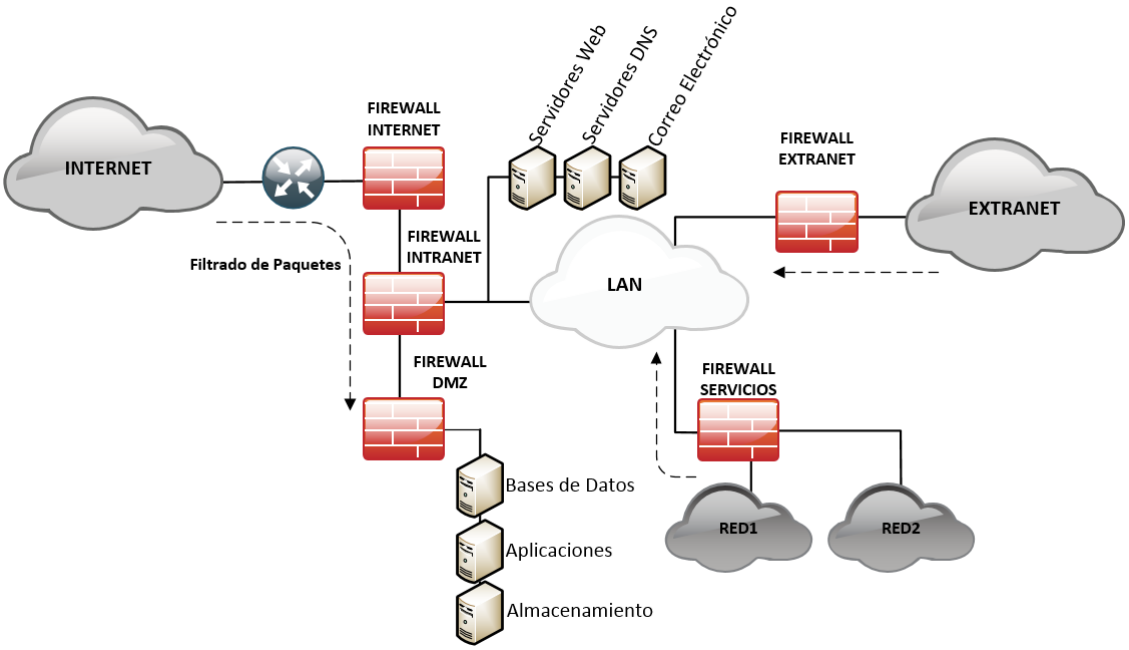

Figura 13 – Topología de Firewalls.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Dentro de los parámetros de operación, dada la función de filtrado de tráfico que desempeñan y por la misma carga de trafico soportado existen parámetros básicos de funcionamiento a tomar en cuenta al momento de monitorear el estado de estos equipos. Para ello agruparemos por un lado las estadísticas de las interfaces de red en uso del equipo buscando reflejar información como el tráfico de entrada y salida, el ancho de banda en uso, errores de recepción, tiempos de respuesta, entre otros.

En segundo lugar la información del funcionamiento del equipo nos permite observar el estado de los recursos de hardware del equipo como por ejemplo, el porcentaje en uso de los procesadores, uso de memoria RAM, uso de la capacidad de almacenamiento, la temperatura en el chasis del equipo, entre otros. A partir de cada fabricante se definen los rangos de trabajo óptimos para cada uno de los recursos del equipo fuera de los cuales se debe tener un plan de acción para su corrección.

Cabe mencionar que al tener equipos dispuestos en alta disponibilidad, el monitoreo de ambos debe ser tomado en cuenta dado que por el tipo de disposición podrían estar trabajando en configuración activo – activo o activo – pasivo es decir, se podría tener la distribución de la carga de tráfico en ambos recursos sin saberlo por lo que tener esto claro nos anticipa el poder interpretar de mejor manera los datos arrojados producto de la herramienta de gestión.

Como ya mencionamos anteriormente en base a la MIBs de cada equipo acompañada de su particularidad se pueden obtener parámetros mucho más específicos del funcionamiento de cada equipo, en el caso de los firewalls el flujo de tráfico en curso aceptado, rechazado o descartado definido por las políticas de filtrado configuradas en el equipo.

3.4. WEB PROXY

Componente de red responsable del control del tráfico hacia internet, el proxy web dispuesto como se indica en la figura 14, que tiene como principales funciones el filtrado de tráfico web, detención spyware y malware, almacenar en memoria cache contenidos web, autenticación de usuarios principalmente. Todo esto es realizado de manera que en su interacción con el directorio activo de la empresa permita la definición de grupos de trabajo que tengan configuradas políticas de acceso; logrando de esta manera definir perfiles de navegación hacia internet de manera segura en función del requerimiento de acceso de los usuarios registrados en

Tesis publicada con autorización del autor
No olvide citar esta tesis

el dominio de la empresa. De esta manera se tiene un control eficiente del uso que hace cada empleado de la conexión a internet, además gracias a la integración con otros dispositivos del mismo fabricante se puede tener un control activo de malware producto del acceso a internet y la obtención de reportes detallados de las conexiones a través del proxy.

Este equipo por el tipo de funciones que cumple y al no contar con redundancia física, es de especial atención, ya que de su disponibilidad depende el acceso a internet de los usuarios al interno de la red, que al ser de gran número podrían lograr exceder el consumo de recursos en el equipo dada su capacidad de funcionamiento. Esto en el día a día se refleja en latencia y pérdida de conexiones a internet, y una serie de incidencias producto de esto. Es por ello que el monitoreo de parámetros específicos del equipo como CPU, consumo de memoria, consumo que memoria cache, cantidad de usuarios concurrentes deben ser tomados en cuenta para resguardar la salud del equipo.

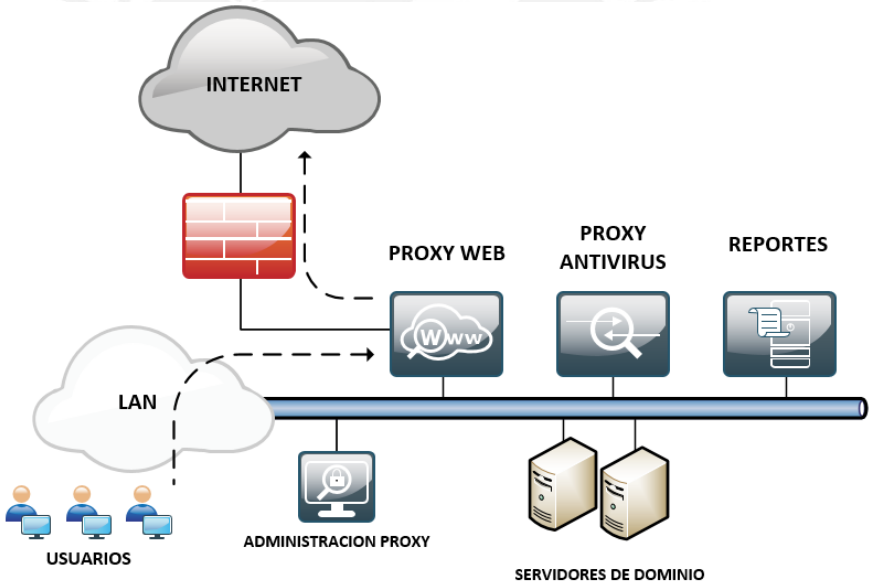

Figura 14 – Topología Proxy Web.

3.5. RETOS DE GESTIÓN

La implementación de un gestor para la red comprende un conjunto de retos de naturaleza técnica, que en su mayoría responden a la particularidad de función de cada aplicación que involucra el sistema de gestión de red. Dentro de los restos que involucra la implementación del sistema de gestión de la red en estudio tenemos los siguientes:

Tesis publicada con autorización del autor
No olvide citar esta tesis

- **Alarmas:** Con los servicios de comunicaciones, cada segundo de interrupción del servicio de un solo equipo puede conllevar a la pérdida ingresos importantes para una empresa. Es por esto que una de las preocupaciones dentro de la gestión de red es automatizar el seguimiento de la información proporcionada por los mismos elementos de red, que en su mayoría son capaces brindar información de manera específica de su funcionamiento, anomalías o errores. En nuestro caso el escenario de estudio cuenta con un sistema de gestión muy limitado ya que carece de compatibilidad con equipos de seguridad y no se tienen claros los parámetros de monitoreo y la relevancia de cada uno de ellos, es por esta razón que su interacción se ve muy limitada y no se llega a brindar información precisa y mucho menos la interacción necesaria para poder anticipar problemas o responder frente a incidencias; ante esta necesidad es que se requiere primeramente poder definir parámetros críticos de operación en los equipos a monitorear para que en base a estos se puedan definir eventos que permitan una mejor gestión de los mismos.

- **Concurrencia:** Un factor a definir por las aplicaciones de monitoreo, es definir si el monitoreo se realizara en tiempo real o cada cierto periodo de tiempo, teniendo que tener en cuenta que el tráfico de administración de los dispositivos de red que no solo corresponde a la herramienta a implementar, sino por el contrario existen aplicaciones y servicios en funcionamiento que actualmente frente al ingreso de tráfico adicional en la red y al no poder segmentar el tráfico de gestión de los equipos, estos pueden llegar a saturar enlaces críticos en la red.

- **Capacidad:** La capacidad de las aplicaciones de monitoreo va de la mano con la frecuencia de actualización de datos, definido por el tipo de monitoreo a realizar, razón por la que los recursos asignados al sistema de gestión deben ser capaces de procesar la información de la totalidad de equipos sincronizados y los procesos a generar en cada tarea definida por las aplicaciones del sistema.

- **Tecnología:** El uso de las diferentes tecnologías define tres aspectos a tener en cuenta. Primeramente el uso de protocolos de comunicación que definen las reglas de comunicación a utilizar por las aplicaciones de gestión de los cuales depende la obtención de la información de los dispositivos a ser gestionados. En Segundo lugar los sistemas de gestión requieren de un almacenamiento a largo plazo por esta razón se debe

Tesis publicada con autorización del autor
No olvide citar esta tesis

definir el uso de una base de datos para el almacenamiento de la información obtenida y su uso por parte de las aplicaciones de gestión. Esto a su vez en función de su capacidad debe permitir tener un histórico de toda la información recopilada. Y finalmente para la presentación de la información obtenida se requiere el uso de un modelador de datos, que permita mostrar la información obtenida de manera clara y simple al operador mediante el uso una interface de usuario que haga posible tener visión global del estado de la red. Todos estos aspectos se detallan a mayor detalle en el siguiente capítulo.

- **Integración**: Es uno de los aspectos técnicos a tener en cuenta al momento de gestionar equipos que cumplen diferentes funciones y son de diferentes fabricantes, en general la red en estudio es un claro ejemplo de red heterogénea por lo que el integrar este tipo de dispositivos resulta de una tarea compleja por no contar con una lógica única y un modo similar de ser configurados.

Tesis publicada con autorización del autor
No olvide citar esta tesis

CAPÍTULO IV: IMPLEMENTACIÓN Y RESULTADOS

4.1. DETALLE DEL SISTEMA

La base del sistema de monitoreo a implementar está basado en Cacti, una herramienta gráfica de monitoreo de red basada en lenguaje de programación PHP que hace uso principalmente del protocolo SNMP para recoger datos de los dispositivos de red monitoreados y ser presentados de manera gráfica haciendo uso del motor de generación de gráficos RRDtool, que por su capacidad limitada de almacenamiento, interactúa con la información almacenada en una base de datos MySQL que es presentada al usuario mediante una interfaz web haciendo uso de un servidor APACHE[7].

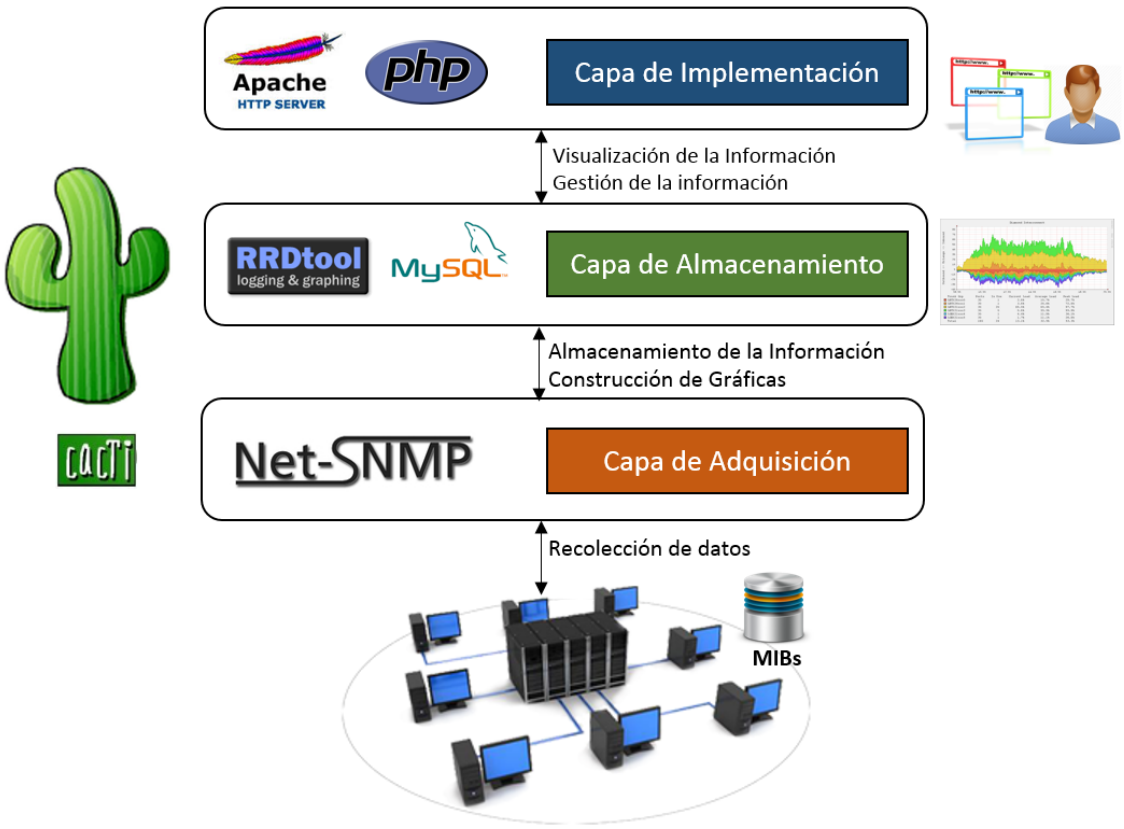

Figura 15 – Arquitectura del Sistema.

Dentro de las principales especificaciones técnicas de Cacti detalladas en la tabla 1, se puede observar comparativamente con la gran gama de plataformas existentes [8], que técnicamente es una propuesta bastante versátil, ya que cumple con todas las funciones tomadas en cuenta al momento de comparar. Esta versatilidad es lograda principalmente por su arquitectura basada en

Tesis publicada con autorización del autor
No olvide citar esta tesis

plugins, que permite integrar de manera independiente herramientas adicionales en código abierto que dan la posibilidad de personalizar las aplicaciones de gestión de acuerdo a los requerimientos particulares de cada red a la plataforma, que adicionalmente son desarrolladas y puestas a prueba por un foro de trabajo en constante actividad.

Tabla 1 – Especificaciones Técnicas de Cacti [8].

FUNCIONES	CACTI
Genera reportes	Si
Agrupamiento lógico	Si
Muestra tendencia de datos	Si
Predicción de tendencias	Vía plugin
Auto descubrimiento	Vía plugin
Requiere software cliente	No
Soporta SNMP	Todas las versiones
Soporta Syslog	Si
Soporta Plugins	Si
Proporciona alertas	Si
Desarrollo de aplicaciones Web	Full Control
Monitoreo distribuido	Si
Manejo de inventarios	Si
Tipo de plataforma	PHP
Método de almacenamiento	RRDtool, MySQL
Tipo de licencia	GPL
Soporta mapas	Vía Plugin
Permite control de acceso	Si
Soporta IPv6	Si
Última actualización	Julio 2015
Última versión	0.8.8f

Una de las principales desventajas de Cacti es que basa su soporte en un foro público muy activo para conseguir el apoyo y actualizaciones referente a todos los ámbitos de la operación, razón por la cual el soporte del servicio se torna en uno de los principales inconvenientes tomados en cuenta al momento de optar por una herramienta basada en software libre.

Si bien Cacti puede hacer uso de Linux o Windows como sistema operativo, en nuestro caso optamos por hacer uso de una distribución comercial de Linux Red Hat en su versión 6.5 como el sistema operativo utilizado en el servidor, principalmente dadas las características de estabilidad y soporte como requisitos básicos para ser alojado dentro de la infraestructura de red en estudio. En la figura 16 se observa la disposición del servidor con respecto de los equipos a

Tesis publicada con autorización del autor
No olvide citar esta tesis

gestionar teniendo en cuenta que la comunicación entre los mismos se realizara dentro de una DMZ de gestión configurada específicamente para este propósito.

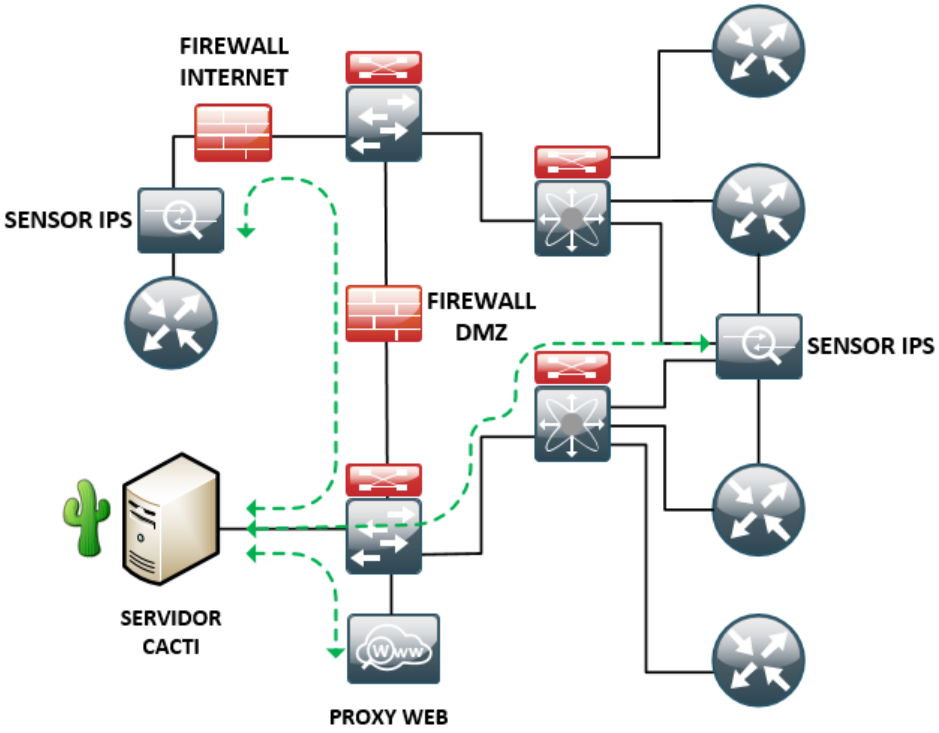

Figura 16 – Topología del Sistema.

Para el servidor que alojara a Cacti se solicitó la asignación de hardware con la perspectiva de poder soportar un mayor número de equipos a gestionar y que frente a una mayor carga de trabajo no se presenten limitantes de capacidad de hardware para lo cual y por recomendaciones obtenidas del foro oficial de Cacti se utilizaron las siguientes especificaciones de hardware [9]:

- Procesador: Xeon 2 - 3GHz
- Memoria RAM: 4096MB
- Disco Duro: 350GB
- Interface de red: Giga Ethernet

Los requerimientos de software utilizado para el funcionamiento de Cacti tomados en cuenta en base a la recomendación encontrada en la página oficial son los siguientes [7]:

- Red Hat Enterprise Linux 6 - 64 bits.
- RRDTool 1.3.x o superior.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- MySQL 5.1.x o superior.
- PHP 5.x para funciones avanzadas.
- A Web Server (Apache) 2.2.x o superior.
- Net-snmp 5.5 o superior.

4.2. FUNCIONAMIENTO DEL SISTEMA

El sistema de monitoreo utiliza para la recolección de información del estado de los elementos de red el protocolo SNMP en su versión 2c en la mayoría de los dispositivos a gestionar, existiendo excepciones donde se utilizara SNMP en su versión 3 por un requerimiento técnico del equipo, teniendo que definir los paramentos de seguridad requeridos para ello.

El poller de recolección de datos a utilizar es llamado Spine, un poller desarrollado en lenguaje C que se esfuerza principalmente en ser lo más rápido posible, llegando a trabajar en ciclos de 1 minuto agrupando la información a ser mostrada en periodos de 5 minutos. El uso del protocolo SNMP directamente responsable de sondeos periódicos en los equipos hace uso de información adjunta en la traps proporcionados por cada equipo para ser exportado al sistema central de almacenamiento en este caso una base de datos MySQL.

Cacti utiliza el formato RRD para almacenar los datos recopilados en series de tiempo. El formato RRD por sus características es una solución de almacenamiento limitado porque es de un tamaño fijo y no crece, pero por cada periodo de tiempo en su extensión llega requerir un alto consumo de recursos de almacenamiento. Para ello se almacena un RRA o archivo RRD alojado en una base de datos MySQL de manera secuencial, obteniendo de manera sencilla un histórico de la información recopilada en un periodo de tiempo. Algo importante para el sistema de monitoreo es que de la relación de los datos almacenados y la capacidad de almacenamiento se define la extensión de tiempo del histórico de la información recibida de cada equipo.

Las principales funciones de la plataforma se han desarrollado para poder ser adicionadas a manera de plugins, si bien la versión oficial solo incluye un menú principal, parámetros configuración básicos y el plugin “Graphs” para la generación de gráficas existe una gran variedad de plugins escritos que están disponibles en el sitio web oficial de Cacti. Esto nos permite incorporarlas al sistema, manteniendo la independencia de cada módulo, de manera que todos los archivos de este se encuentren separados y la parte central del sistema no tenga que ser

Tesis publicada con autorización del autor
No olvide citar esta tesis

modificada, además los módulos pueden ser activados y desactivados sin afectar al resto del sistema. Dentro de los plugins utilizados por la plataforma implementada tenemos:

- **Architecture:** Este plugin permite separar las funciones complementarias sin necesidad de modificar los archivos base de instalación de Cacti, que en la versión 0.8.8c ya viene incluido en la versión base de Cacti [7].

- **Settings:** Proporciona la plataforma de gestión que soportara la arquitectura de funciones a manera de plugins de Cacti. Es decir en la pestaña de dicho plugin se tendrá el menú de configuración base para la mayoría de los plugins en uso [7].

- **Thold:** Plugin gracias al cual se podrá interactuar con las gráficas obtenidas de manera tal que a partir de la definición de umbrales de trabajo se puedan generar acciones de notificación a manera de alertas [7].

- **Monitor:** Plugin que permite mostrar el estado de los dispositivos monitoreados. Además permite observar el estado de los servicios dentro de cada uno de estos dispositivos [7].

- **Syslog:** Permite centralizar los mensajes de estado de los equipos monitoreados permitiendo a partir de los mismos definir eventos a partir de su clasificación. Es una herramienta muy útil para recibir principalmente mensajes de alarmas generados por los propios equipos monitoreados [7].

- **Cycle:** Permite mostrar al usuario una vista cíclica y personalizada de las gráficas obtenidas de un equipo en particular y las presenta de manera cíclica de tal manera de poder tener una visión total de todas las gráficas en un periodo de tiempo [7].

- **Nectar:** Permite generar de manera programada reportes personalizados de los datos obtenidos en un periodo de tiempo por la herramienta. Estos reportes son enviados mediante correo electrónico de acuerdo a las especificaciones de la información requerida [7].

- **Remote:** Permite tener la opción de acceder de manera remota a los equipos monitoreados vía protocolos Telnet o SSH para acceder al CLI de los equipos y de esta manera poder centralizar otra herramienta adicional de gestión [7].

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.3. IMPLEMENTACIÓN DEL SISTEMA

Como tarea inicial dentro del proceso de implementación se tuvo que instalar el sistema operativo que alojara la plataforma de monitoreo, como ya indicamos anteriormente se utilizó la distribución Red Hat en su versión 6.5, en este caso uno de los principales inconvenientes del uso de esta distribución fue el uso de repositorios para la instalación del software requerido previamente para la instalación del Cacti. Ante esta problemática se tuvo que hacer uso en un primer momento de un repositorio local que si bien lo generamos a partir del disco de instalación del sistema, no cuenta con todos los paquetes requeridos necesarios para la instalación de Cacti, razón por la cual se hizo uso de repositorios públicos compatibles con Red Hat, entre ellos el principal EPEL.

Durante el proceso de instalación de Cacti la configuración de la base de datos y la asignación de privilegios sobre carpetas especificas fue una de las tareas que complico por semanas lograr configurar de manera correcta la herramienta a fin configurar el poller de monitoreo deseado, ya que si bien obteníamos el cuadro de la gráfica deseado no se observaban datos sobre la misma.

Para lograr la implementación de la plataforma de monitoreo dentro de la red en producción primeramente se tuvo que demostrar que su uso en términos de compatibilidad y configuraciones requeridas por parte de los equipos a gestionar era factible dado que la implementación del mismo dependía de poder sincronizar más de una comunidad SNMP, dado el uso una plataforma de monitoreo en producción según se indicó previamente. Además se logró evidenciar que la obtención de las gráficas de los parámetros deseados de los equipos era posible.

Para esto se hizo uso de una PC con procesador Intel Core i7 de 3.70 GHz, con 16 GB de memoria RAM y con sistema operativo Windows 8 de 64 bits, haciendo uso de VMware Workstation en su versión 10 como entorno de virtualización, principalmente por la compatibilidad con la extensión de las imágenes de los equipos obtenidos y el conocimiento de dicha plataforma.

Tesis publicada con autorización del autor
No olvide citar esta tesis

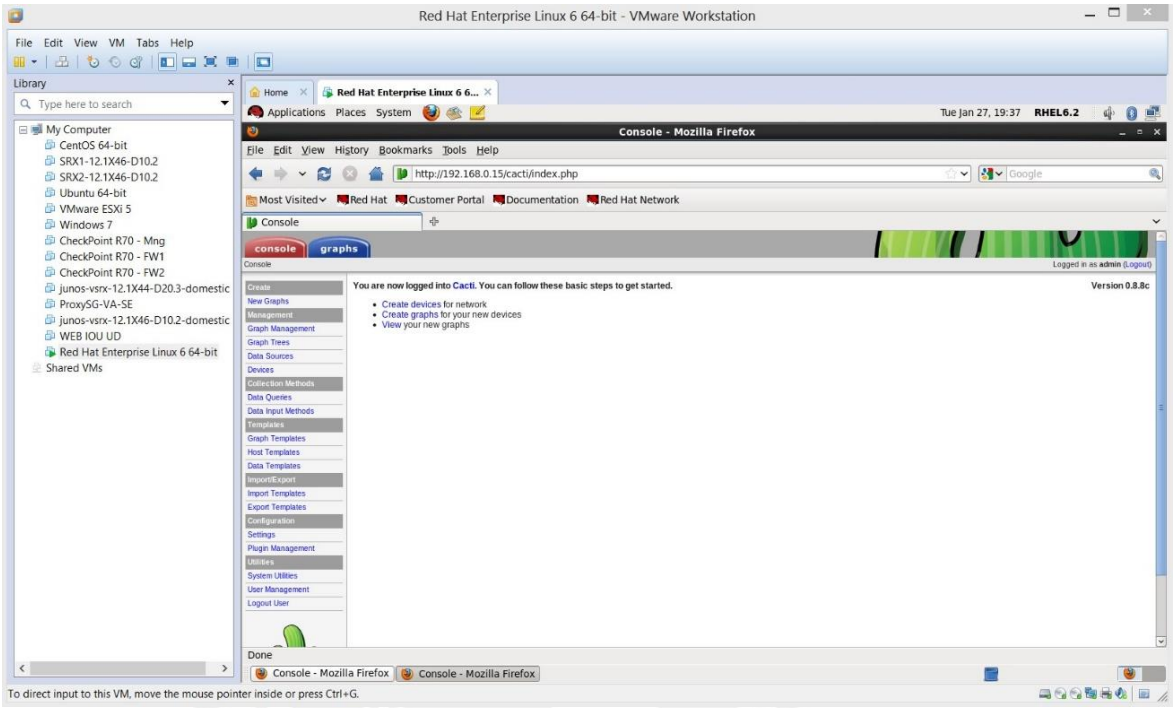

Figura 17 – Entorno de Simulación.

Uno de los principales retos dentro de la implementación del escenario virtualizado fue la adquisición de la versión virtual de los equipos a monitorear y que a su vez estos en su versión pudieran replicar las configuraciones de alta disponibilidad de manera similar a equipos físicos. Para esto se hizo uso de documentación de los fabricantes logrando replicar en su mayoría las configuraciones de los equipos en producción con lo cual atendimos el principal requerimiento previo a la implementación del sistema. El detalle de las imágenes utilizadas en el entorno virtualizado se detalla en la tabla 2.

Tabla 2 – Equipos Virtualizados.

PLATAFORMA	IMAGEN	VERSIÓN
Virtualización	vmware-wsx-server-1.0.1-894247	WMware-WSX 10.0.1
Check Point Firewall	Check_Point_Install_and_Upgrade_R77.Gaia	Gaia R77.10
Juniper Firewall	junos-vsrx-12.1X46-D10.2-domestic	Junos 12.1X46-D10.2
Bluecoat Web Proxy	proxySG-VA-SE	SGOS 6.4.2.1
Servidor Linux	rhel-server-6.5-x86_64-dvd	RHEL 6.5

Para la implementación del servidor se facilitó un servidor virtualizado acorde con las características solicitadas. Una vez completado el proceso de instalación del software se

Tesis publicada con autorización del autor
No olvide citar esta tesis

procedió a configurar el tipo de poller a usar, que como ya mencionamos anteriormente se configuro el poller Spine definiendo ciclos de 1 minuto. Adicional a esto tenemos que los periodos de tiempo definidos por el temporizador de procesos del sistema operativo conocido como Cron se definió en 5 min, esto quiere decir que a pesar que los ciclos de trabajo del poller sean de un minuto la información se mostrara en periodos de 5 minutos.

Paso seguido se realizó la sincronización de los equipos teniendo en cuenta la IP de administración de los equipos y la configuración de parámetros de comunicación requeridos para el uso del protocolo SNMP. Para lo cual se definió la versión del protocolo a utilizar en cada equipo y el nombre de la comunidad SNMP a configurar en los equipos a sincronizar. Para la configuración de los parámetros SNMP soportados en cada uno de los equipos se recurrió a documentación técnica de cada equipo proporcionada en los sitios web de cada fabricante.

Para la construcción de los gráficos se configuró inicialmente Data Templates, que como su nombre lo indica es una plantilla para la recopilación de los datos que deseamos graficar a partir de los OIDs obtenidos. Por ejemplo para obtener el porcentaje en uso del CPU de un firewall Juniper, tal como se observa en la figura 18 corresponde a un valor encontrado en la MIB "jnxJsSPUMonitoringMIB", debemos tener en cuenta que puede haber más de un archivo MIB en el equipo. Una vez identificado el valor .1.3.6.1.4.1.2636.3.39.1.12.1.1.1.4.9.1.0.0 se definirá la naturaleza o tipo de dato. En este caso existen 4 tipos de datos que se detallan en la tabla 3 a continuación.

Tabla 3 – Tipos de Datos [8].

NOMBRE	TIPO	DESCRIPCIÓN
ABSOLUTE	Valor absoluto	Contador que se resetea tras su lectura, registra el valor asumiendo un valor inicial 0
DERIVE	Contador, puede decrecer	Registra el incremento o decremento haciendo uso de valores negativos
GAUGE	Indicador, distintos valores en el tiempo	Registra el valor "tal como lo medimos"
COUNTER	Contador, siempre se incrementa	Registra el incremento/intervalo tiempo

Una vez definida la plantilla del dato, construiremos la plantilla del grafico denominada Graph Template; aquí definimos los datos que queremos mostrar en la gráfica, para lo cual relacionamos los Data Templates previamente creados, así como la manera en que los datos obtenidos deben ser mostrados, como por ejemplo el tamaño de la gráfica, el nombre, el color a utilizar, la leyenda de la gráfica y los valores que deseamos mostrar.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Finalmente dentro de los Host Templates se agrupan los Graph Templates correspondientes a un equipo en particular de tal manera que se una vez se sincronice un equipo de similares características se pueda relacionar la plantilla correspondiente a las gráficas que deseamos obtener de ese equipo con las finalidad de no tener que repetir todo el proceso.

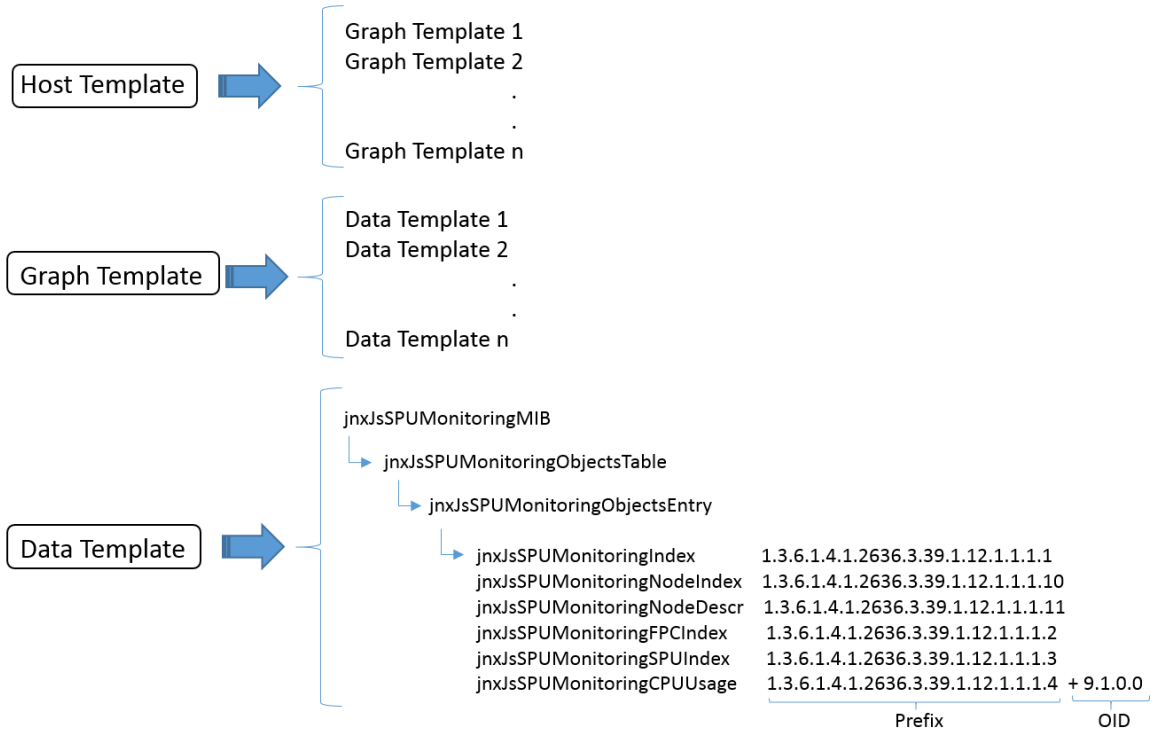

Figura 18 – Proceso de Construcción de Gráficas.

Se debe tener en cuenta que para que la construcción de cada gráfica cada Data Template debe tener asignado un RRA o archivo con extensión rrd para ello en la pestaña Data Sources relacionamos el Data Template creado específicamente a uno de los equipos sincronizados de tal manera que se cree un archivo que hará referencia a la información recopilada de un solo equipo. En la figura 19 podemos observar que los comandos generados por la RRDTool asigna al archivo “fw1-checkpoint_acc_119.rrd” la información para construcción de la gráfica deseada.

Tesis publicada con autorización del autor
No olvide citar esta tesis

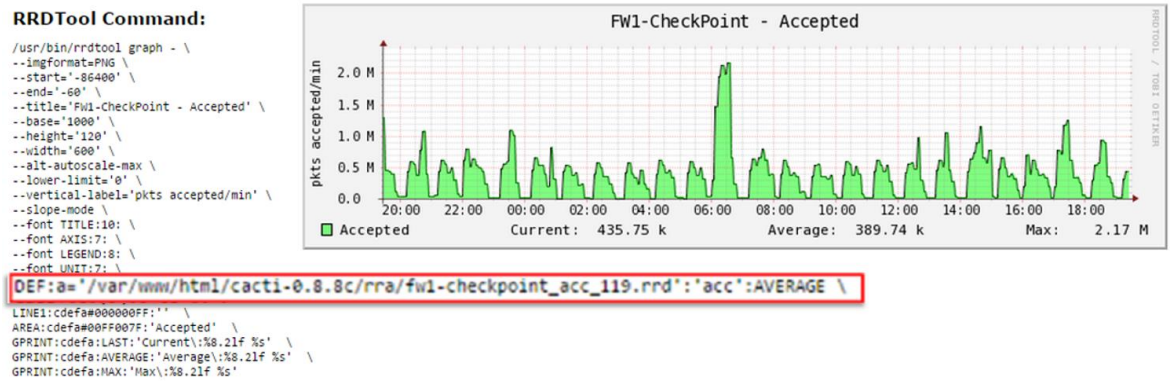

Figura 19 – Construcción de Gráficas RRDTool.

Para la construcción de las gráficas no existe un documentación detallada por los fabricantes en la mayoría de los casos, razón por la cual se tuvo que validar e identificar cada uno de los valores de los OIDs asignados a los parámetros a monitorear, de esta manera se evaluó si la información proporcionada correspondía a la información de monitoreo deseada comparándola con los datos obtenidos en el mismo equipo, para tal propósito se elaboró una serie de tablas que indican la relación de cada OID y el parámetro a monitorear en cada equipo, empezando por el sensor IPS modelo M6050 de marca McAfee, en el cual identificamos parámetros de funcionamiento e información del tráfico a través del equipo, cuyo detalle se observa en la tabla 4.

Tabla 4 – IPS Parámetros de Funcionamiento.

COMPONENT	OID	DESCRIPTION
INTEGER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.1.2	Total TCBs
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.2.2	Total active TCP flows
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.3.2	Total active UDP flows
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.4.2	Total TCP flows created
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.5.2	Total timed out flows
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.6.2	Total TCP flows in timewait
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.7.2	Total flows in SYN state
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.1.8.2	Total inactive TCP flows
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.5.1.2	Sensor Average Load
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.5.1.2.2	Sensor Highest Load
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.5.1.3.2	Pending IP Frag Reassembly Count
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.5.1.5.2	Total Alerts Sent Count
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.5.1.6.2	SensorLoad IndicatorConfig
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.5.1.7.2	Sensor Max Traffic Capacity
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.5.1.8.2	Sensor Total Bytes Processed

Tesis publicada con autorización del autor
No olvide citar esta tesis

En la tabla 5 detallamos la correlación a tener en cuenta para la construcción del valor de los OIDs para el monitoreo de cada sensor del equipo, es decir cada OID detallado almacena información de indicadores de tráfico en cada uno de los sensores que variaran en los 2 últimos dígitos del OID en referencia a la información proporcionada de cada sensor, que de acuerdo al modelo del sensor varia en número y nombre.

En el caso del modelo M6050 los sensores van del 5A – 5B al 8A – 8B que de acuerdo a la tabla 5 corresponde a los OIDs finalizados en 2.10 al 2.16 para cada uno de los prefijos a usar para la construcción de las gráficas.

Tabla 5 – OIDs por Sensor.

OID	SENSOR
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.1	1A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.2	1B
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.3	2A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.4	2B
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.5	3A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.6	3B
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.7	4A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.8	4B
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.9	5A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.10	5B
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.11	6A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.12	6B
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.13	7A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.14	7B
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.15	8A
SNMPv2-SMI::enterprises.8962.X.X.X.X.X.X.X.X.2.16	8B

En la tabla 6 agrupamos los indicadores de tráfico a través de los sensores. Que en este caso que por el modo de funcionamiento del equipo en modo bridge, deriva en que sus interfaces no tienen asignadas una dirección MAC o IP desde la cual poder obtener información de las mismas de manera tradicional, haciendo uso de la información brindada por los OIDs se logró uno de los aportes a la gestión de dichos equipos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 6 – OIDs Indicadores de Tráfico.

COMPONENTE	OID	DESCRIPCIÓN
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.1	Total Packets Received
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.3	Total Multicast Packets Received
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.4	Total Broadcast Packets Received
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.5	Total Bytes Received
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.6	Total CRC Errors Received
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.7	Totla Packets Sent
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.8	Total Unicast Packets Sent
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.9	Total Multicast Packets Sent
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.10	Total Broadcast Packets Sent
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.11	Total Bytes Sent
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.3.1.12	Total CRC Errors Sent
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.4.1.2	Get In Spoof Count
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.1.4.1.3	Get Out Spoof Count
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.2.2.1.9	Port Attack Packet Drop
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.2.2.1.10	Port Reassem Timeout Drop
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.2.2.1.13	Tcp Error Drop
COUNTER	.1.3.6.1.4.1.8962.2.1.3.1.2.2.1.14	Udp Error Drop

A partir de los OIDs identificados dentro de las gráficas construidas se pudo evidenciar la cantidad de tráfico en curso por cada sensor, así como el detalle de los ataques bloqueados de paso por cada uno los sensores, así como la cantidad de información procesada en los equipos. De esta manera se obtiene una visión más amplia de la tarea de los sensores y los ataques presentes en cada segmento de red monitoreado. La totalidad de gráficas obtenidas para este equipo se adjuntan en los anexos.

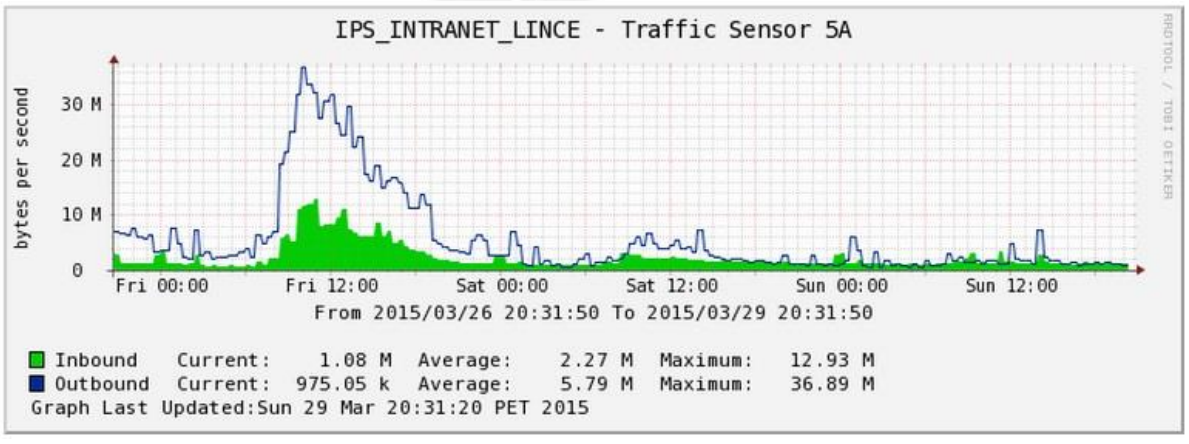

Figura 20 – Tráfico en el Sensor IPS.

Tesis publicada con autorización del autor
No olvide citar esta tesis

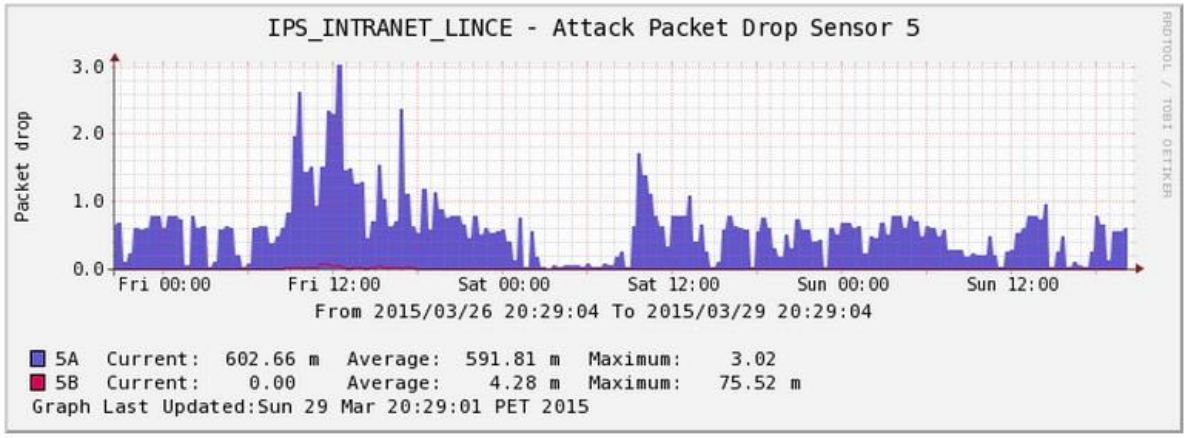

Figura 21 – Ataques Sensores IPS.

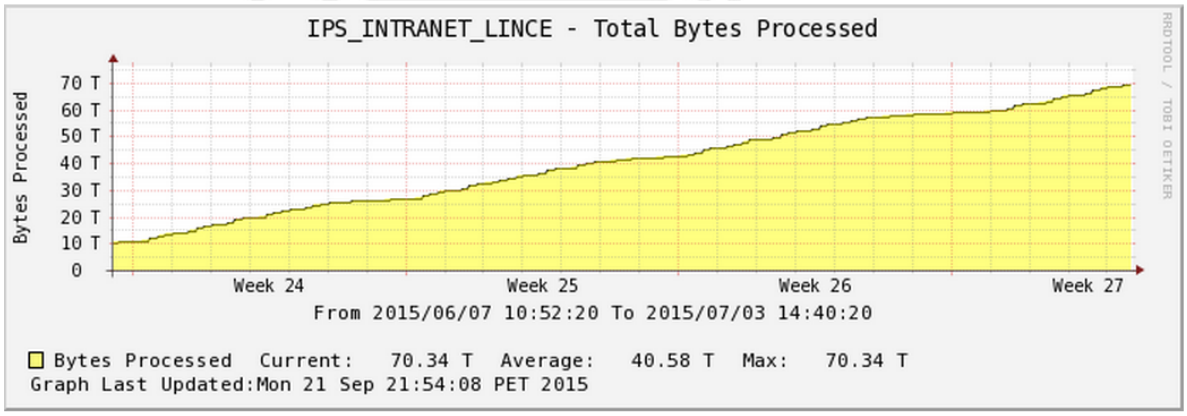

Figura 22 – Bytes Procesados en el Sensor IPS.

Para el caso los firewalls en producción tenemos equipos de dos fabricantes distintos cada uno con una arquitectura de trabajo muy diferente así como las MIBs utilizadas en cada uno. Para lograr los objetivos de monitoreo en dichos equipos se identificaron OIDs correspondientes principalmente a parámetros de funcionamiento y salud del equipo.

Para el caso de los firewalls modelo 4800 de la marca Check Point, por el tipo de configuración de alta disponibilidad la sincronización con Cacti se realiza de manera independiente para cada equipo, es decir se sincronizo de manera individual cada equipo con su IP de administración, obteniendo así los OIDs detallados en la tabla 7.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 7 – OIDs Performance Firewall Check Point.

COMPONENTE	OID	DESCRIPCIÓN
GAUGE	.1.3.6.1.4.1.2620.1.1.25.3.0	Firewall connections
COUNTER	.1.3.6.1.4.1.2620.1.1.25.8.0	Packets Accepted Throughput
COUNTER	.1.3.6.1.4.1.2620.1.1.25.9.0	Packets Dropped Throughput
COUNTER	.1.3.6.1.4.1.2620.1.1.4.0	Packets Accepted
COUNTER	.1.3.6.1.4.1.2620.1.1.5.0	Packets Rejected
COUNTER	.1.3.6.1.4.1.2620.1.1.6.0	Packets Dropped
COUNTER	.1.3.6.1.4.1.2620.1.1.7.0	Packets Logged
GAUGE	.1.3.6.1.4.1.2620.1.6.7.2.1.0	CPU usage User
GAUGE	.1.3.6.1.4.1.2620.1.6.7.2.2.0	CPU usage System
GAUGE	.1.3.6.1.4.1.2620.1.6.7.2.3.0	CPU usage Idle
GAUGE	.1.3.6.1.4.1.2620.1.6.7.2.4.0	CPU usage
GAUGE	.1.3.6.1.4.1.2620.1.6.7.4.1.0	Memory Total Virtual
GAUGE	.1.3.6.1.4.1.2620.1.6.7.4.2.0	Memory Active Virtual
GAUGE	.1.3.6.1.4.1.2620.1.6.7.4.3.0	Memory Total Real
GAUGE	.1.3.6.1.4.1.2620.1.6.7.4.4.0	Memory Active Real
GAUGE	.1.3.6.1.4.1.2620.1.6.7.4.5.0	Memory Free Real
GAUGE	.1.3.6.1.4.1.2620.1.6.7.6.1.6.1.0	Disk Usage Partition sda1
GAUGE	.1.3.6.1.4.1.2620.1.6.7.6.1.6.2.0	Disk Usage Partition sda2
GAUGE	.1.3.6.1.4.1.2620.1.6.7.6.1.6.3.0	Disk Usage Partition sda3
GAUGE	.1.3.6.1.4.1.2620.1.6.7.8.1.1.3.1.0	Temperature

Dentro de las gráficas construidas tenemos las estadísticas de tratamiento de tráfico por parte del equipo, es decir las estadísticas de tráfico por interfaces, numero conexiones, consumo de recursos del equipo, entre otras. El principal aporte a la gestión de estos equipos es la implementación de mecanismos de respuesta en base a umbrales de trabajo que evidencian el estado anómalo del funcionamiento del equipo mediante alertas generadas a partir de la información obtenida en las gráficas, algunas de las cuales como el número de conexiones, el consumos de CPU y memoria se muestran a continuación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

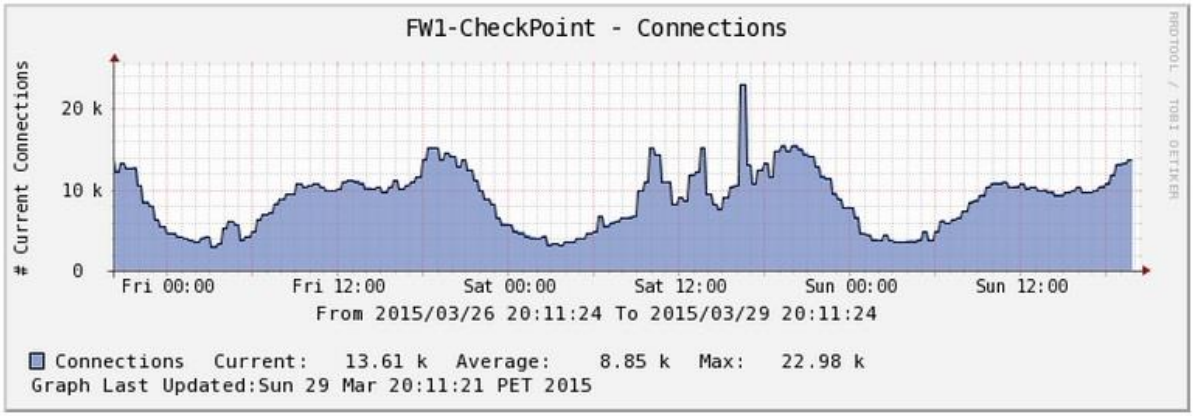

Figura 23 – Conexiones Firewall Check Point.

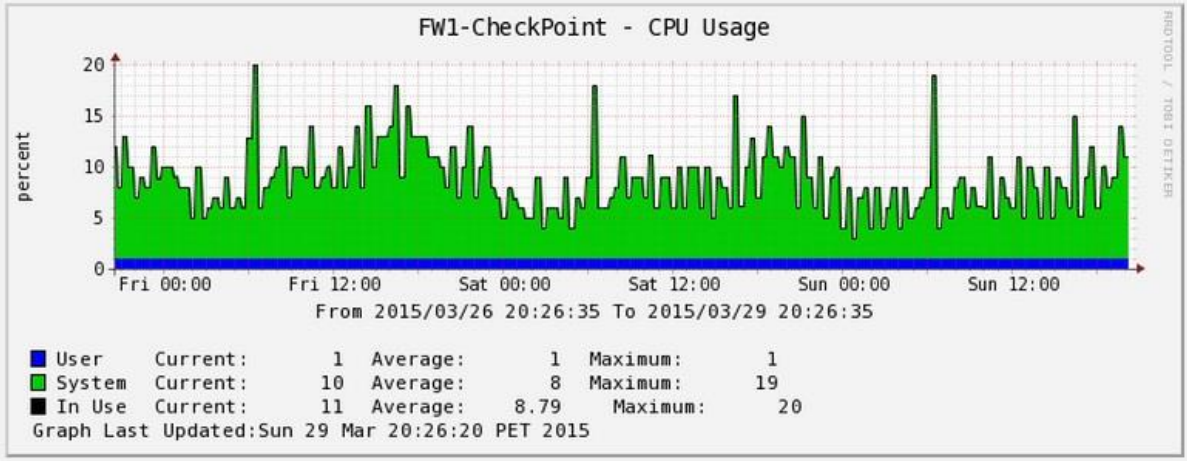

Figura 24 – Consumo CPU Firewall Check Point.

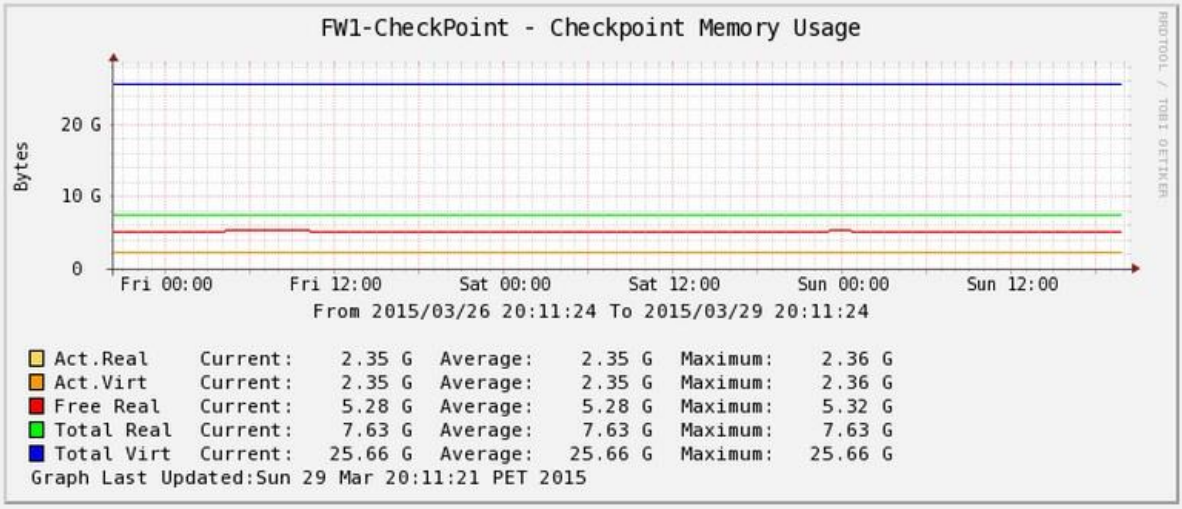

Figura 25 – Consumo de Memoria Firewall Check Point.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Así mismo se logró obtener las gráficas de la cantidad de trafico aceptado y rechazado por el firewall a partir de las políticas de seguridad configuradas en el equipo, valores que nos permiten evidenciar el tratamiento del tráfico a través de los equipos.

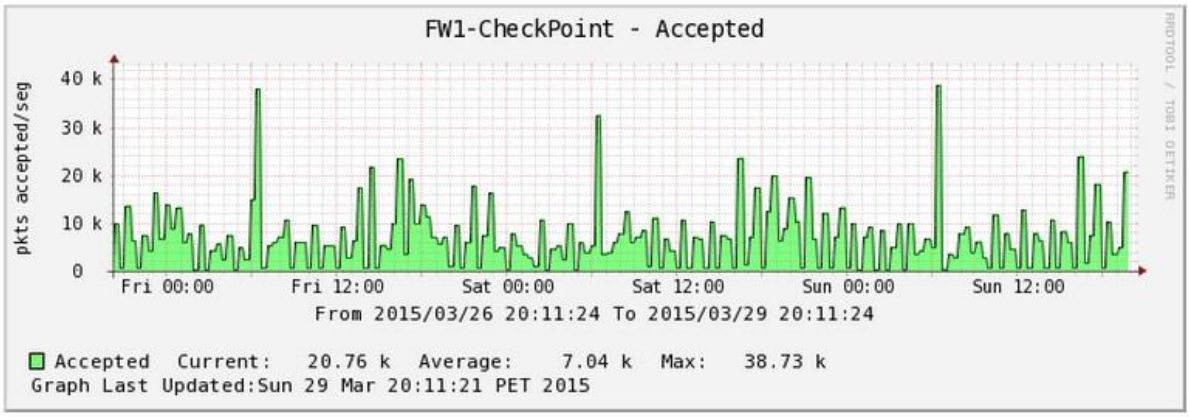

Figura 26 – Paquetes Acceptados Firewall Check Point.

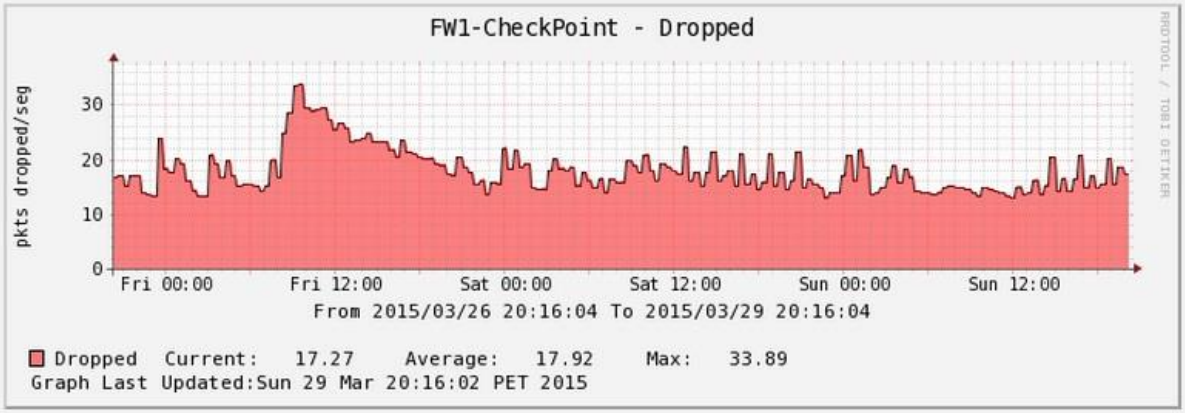

Figura 27 – Paquetes Bloqueados Firewall Check Point.

Para el caso de los firewalls de modelo SRX3400 de la marca Juniper, fue más complejo descifrar la información contenida en los OIDs por el tipo de configuración utilizada para lograr la redundancia de ambos equipos, ya que en este caso cada equipo se identifica a manera de nodos que responden a una sola IP en cada interface lógica configurada, por lo que la sincronización con la plataforma de monitoreo responde a la sincronización con la IP de un solo equipo, es por esta razón que la correlación de OIDs en sus últimos dígitos responden a la información de un nodo en particular del cluster.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 8 – OIDs Performance Nodos Juniper.

COMPONENTE	OID	DESCRIPCIÓN
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0	Used memory % for Routing Engine Node 0
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.11.9.3.0.0	Used memory % for Routing Engine Node 1
INTEGER	.1.3.6.1.4.1.2636.3.1.13.1.13.9.1.0.0	System Uptime Node 0
INTEGER	.1.3.6.1.4.1.2636.3.1.13.1.13.9.3.0.0	System Uptime Node 1
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.20.9.1.0.0	Load Average 1 Min Node 0
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.20.9.3.0.0	Load Average 1 Min Node 1
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.21.9.1.0.0	Load Average 5 Min Node 0
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.21.9.3.0.0	Load Average 5 Min Node 1
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.22.9.1.0.0	Load Average 15 Min Node 0
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.22.9.3.0.0	Load Average 15 Min Node 1
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.7.12.1.0.0	Sytem Temperature Node 0
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.7.12.3.0.0	Sytem Temperature Node 1
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0	CPU usage of Routing Engine Node 0
GAUGE	.1.3.6.1.4.1.2636.3.1.13.1.8.9.3.0.0	CPU usage of Routing Engine Node 1
GAUGE	.1.3.6.1.4.1.2636.3.31.1.1.1.1.1	Storage Percent Used /config/
GAUGE	.1.3.6.1.4.1.2636.3.31.1.1.1.1.2	Storage Percent Used /root/
GAUGE	.1.3.6.1.4.1.2636.3.31.1.1.1.1.3	Storage Percent Used /var/
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.4.21	CPU Usage of Packet Forwarding Engine Node 1
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.4.5	CPU Usage of Packet Forwarding Engine Node 0
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.5.21	Packet Forwarding Memory Usage Node 1
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.5.5	Packet Forwarding Memory Usage Node 0
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.6.21	Current PFE Session Count Node 1
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.6.5	Current PFE Session Count Node 0
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.7.21	Maximum session availability per PFE Node 1
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.7.5	Maximum session availability per PFE Node 0
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.8.21	Current CP Session Count Node 1
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.8.5	Current CP Session Count Node 0
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.9.21	Maximum CP Session availability Node 1
GAUGE	.1.3.6.1.4.1.2636.3.39.1.12.1.1.1.9.5	Maximum CP Session availability Node 0
GAUGE	1.3.6.1.4.1.2636.3.39.1.12.1.4.1.3.0	Current Total Sessions Node 0
GAUGE	1.3.6.1.4.1.2636.3.39.1.12.1.4.1.3.1	Current Total Sessions Node 1
GAUGE	1.3.6.1.4.1.2636.3.39.1.12.1.4.1.4.0	Max Sessions Node 0
GAUGE	1.3.6.1.4.1.2636.3.39.1.12.1.4.1.4.1	Max Sessions Node 1
COUNTER	1.3.6.1.4.1.2636.3.39.1.12.1.4.1.5.0	Sessions Created per Second Node 0
COUNTER	1.3.6.1.4.1.2636.3.39.1.12.1.4.1.5.1	Sessions Created per Second Node 1

Por la configuración de alta disponibilidad dispuesta para estos equipos la construcción de las gráficas fue una tarea más compleja ya que en una sola gráfica se agruparon OIDs

Tesis publicada con autorización del autor
No olvide citar esta tesis

correspondientes al estado de ambos nodos, lo que implica el uso de más de un Data Source y la manera en que estos deben ser mostrados.

Tal como se observa en las gráficas obtenidas a pesar de tener una configuración de redundancia activo – pasivo se identifica un consumo activo de recursos en ambos nodos, esto debido a que el nodo activo constantemente replica la información al nodo secundario con la finalidad de reducir el tiempo de respuesta en caso las conexiones en curso llegarán a conmutar al equipo secundario y viceversa.

Tal es así que en las figuras 28 y 29 se observan las gráficas obtenidas con valores similares de CPU y consumo en ambos nodos, comportamiento que no se presenta en las gráficas en la figuras 30 y 31 donde los valores de consumo de memoria y temperatura de los equipos son completamente distintos.

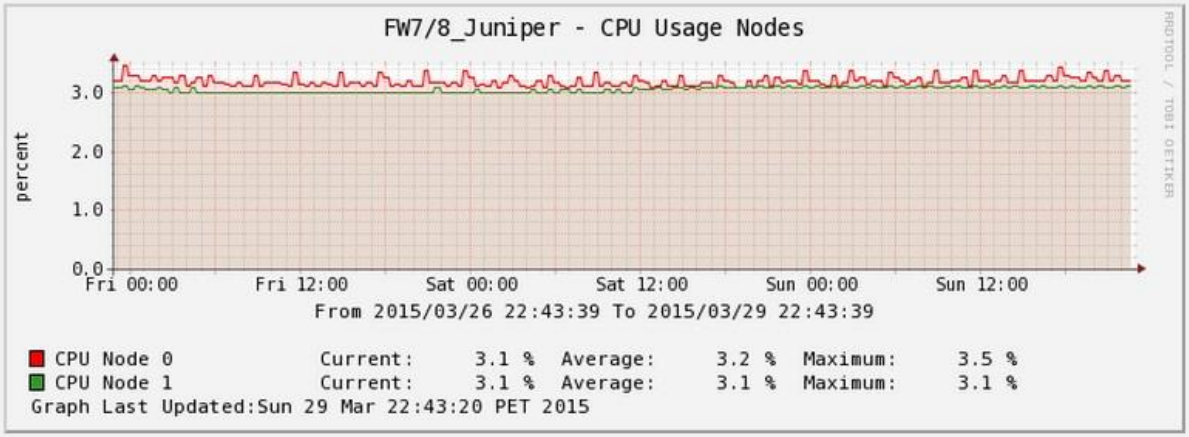

Figura 28 – Consumo CPU Nodos Firewall Juniper.

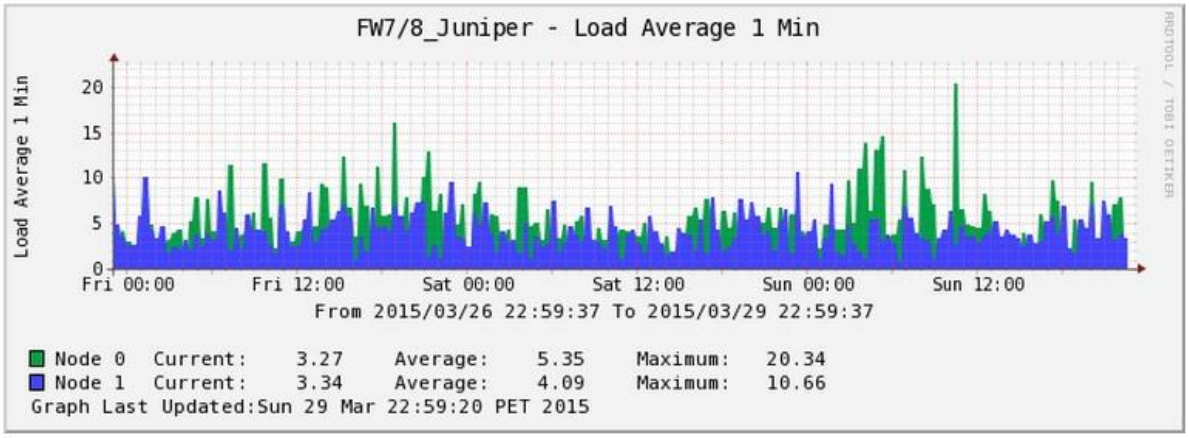

Figura 29 – Consumo Promedio Nodos Firewall Juniper.

Tesis publicada con autorización del autor
No olvide citar esta tesis

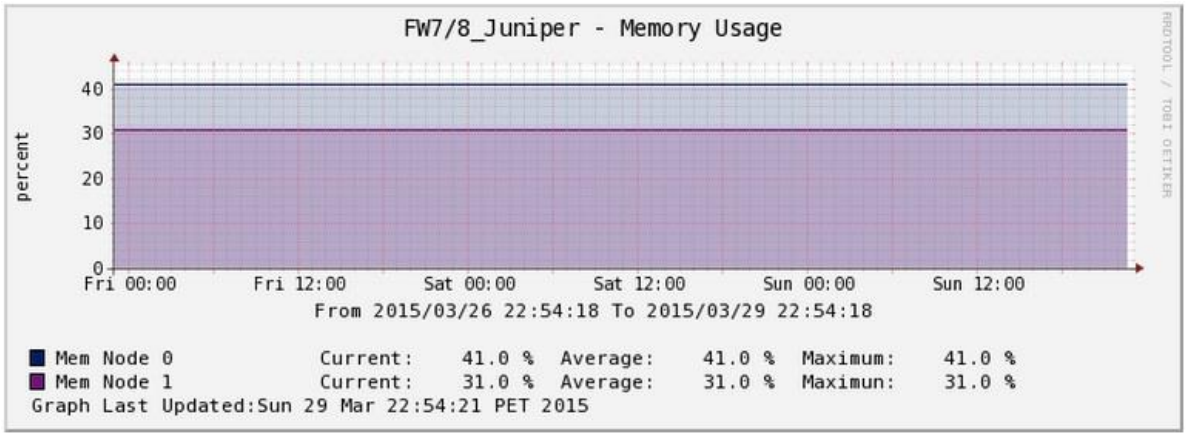

Figura 30 – Consumo Memoria Nodos Firewall Juniper.

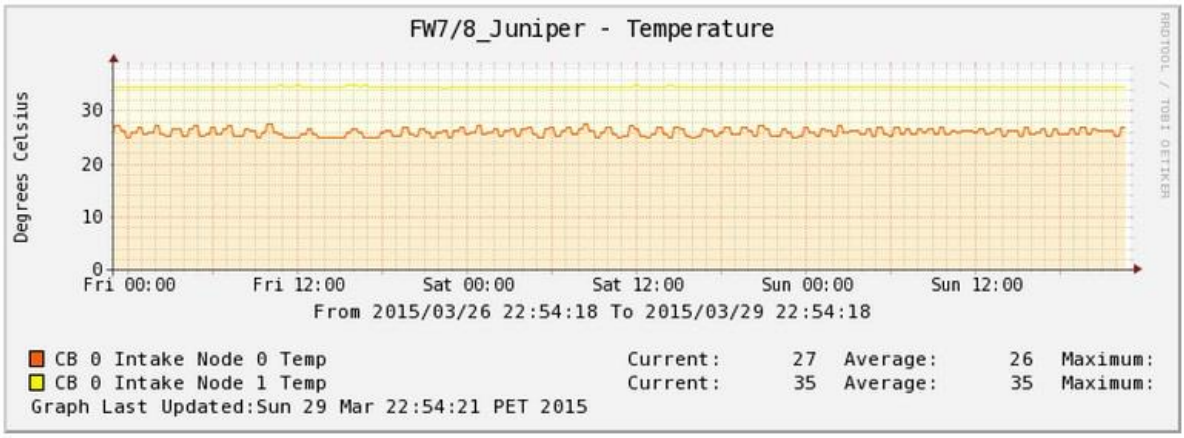

Figura 31 – Temperatura Nodos Firewall Juniper.

Para la construcción de las gráficas del tráfico a través de las interfaces de los firewalls, así como los errores y ancho de banda se pudo utilizar OIDs estándar para la obtención de dichos valores, razón por la cual no se detalla un cuadro específico respecto de los OIDs utilizados para la construcción de dichas gráficas. A continuación en las figuras 32 y 33 se observa un ejemplo de las gráficas obtenidas de las interfaces en los firewalls Check Point y Juniper.

Tesis publicada con autorización del autor
No olvide citar esta tesis

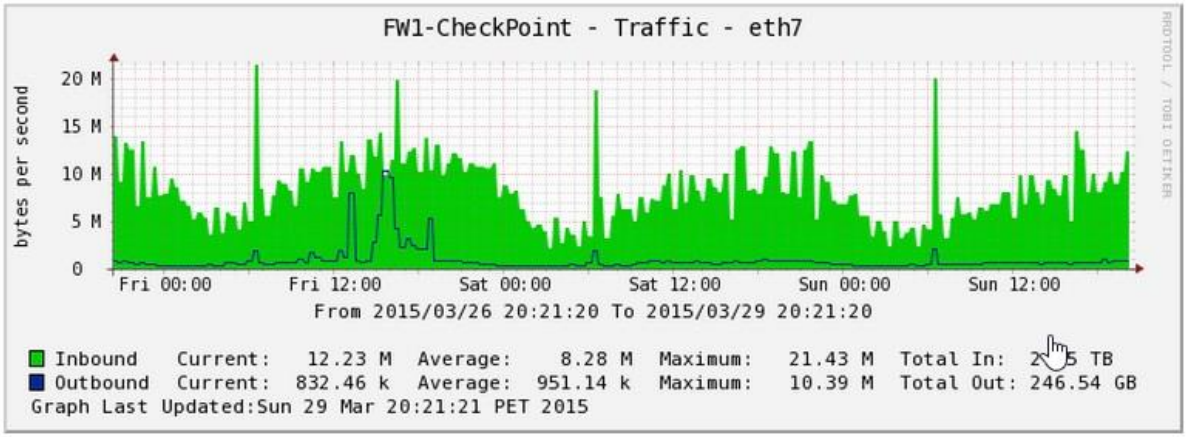

Figura 32 – Tráfico Interfaz Firewall CheckPoint.

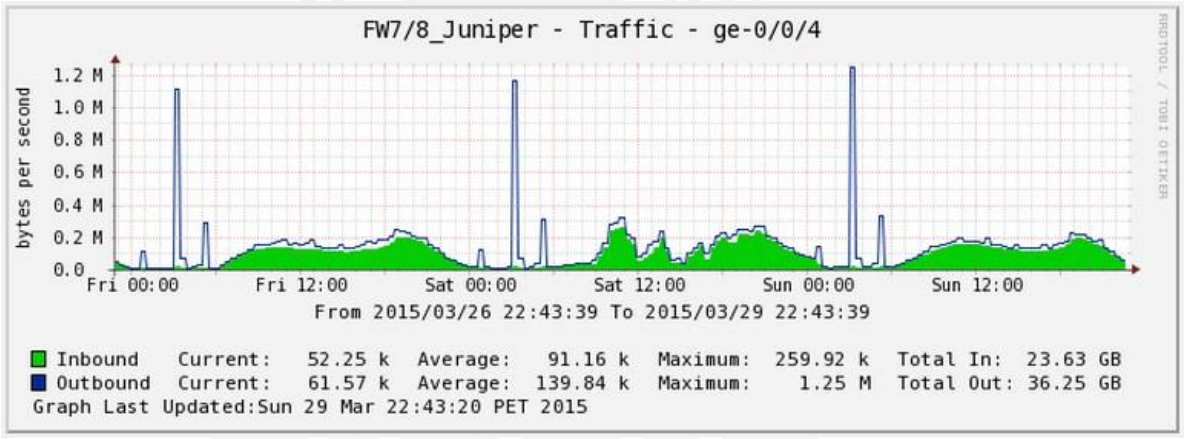

Figura 33 – Tráfico Interfaz Firewall Juniper.

Finalmente en el caso del proxy web modelo SG900-30 y el equipo antivirus AV1400, ambos parte de la solución del proxy web de marca Bluecoat, se logró a obtener una mayor documentación de los OIDs para cada uno de los equipos, razón por la cual se pudo lograr construir gráficas más detalladas de la performance de los equipos. Como se indicó inicialmente por el requerimiento de disponibilidad del equipo y por no contar con ningún tipo de redundancia, es de gran aporte para su gestión el tener el mayor detalle posible del estado de estos equipos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 9 – OIDs Proxy Web Bluecoat.

COMPONENTE	OID	DESCRIPCIÓN
GAUGE	.1.3.6.1.2.1.1.3.0	Uptime
GAUGE	.1.3.6.1.2.1.1.3.0	Uptime
COUNTER	.1.3.6.1.2.1.6.5.0	TCP Counters
COUNTER	.1.3.6.1.2.1.6.6.0	TCP Counters
COUNTER	.1.3.6.1.2.1.6.7.0	TCP Counters
COUNTER	.1.3.6.1.2.1.6.8.0	TCP Counters
GAUGE	.1.3.6.1.2.1.6.9.0	TCP Current Established
COUNTER	.1.3.6.1.3.25.17.3.2.1.1.0	HTTP Client Requests
COUNTER	.1.3.6.1.3.25.17.3.2.1.2.0	HTTP Client Hits
COUNTER	.1.3.6.1.3.25.17.3.2.2.1.0	HTTP Server Requests
INTEGER	.1.3.6.1.4.1.3417.2.1.1.1.1.1.5.1	Temperature Motherboard
INTEGER	.1.3.6.1.4.1.3417.2.1.1.1.1.1.5.2	Temperature CPU
COUNTER	.1.3.6.1.4.1.3417.2.10.1.1.0	Files Scanned
GAUGE	.1.3.6.1.4.1.3417.2.10.1.10.0	Slow ICAP Connections
COUNTER	.1.3.6.1.4.1.3417.2.10.1.2.0	Viruses Detected
GAUGE	.1.3.6.1.4.1.3417.2.10.1.7.0	AV License Days Remaining
GAUGE	.1.3.6.1.4.1.3417.2.11.2.2.2.0	Objects in Cache
GAUGE	.1.3.6.1.4.1.3417.2.11.2.3.4.0	Memory Pressure
GAUGE	.1.3.6.1.4.1.3417.2.11.3.1.3.1.0	HTTP Client Connections
GAUGE	.1.3.6.1.4.1.3417.2.11.3.1.3.4.0	HTTP Server Connections
GAUGE	.1.3.6.1.4.1.3417.2.4.1.1.1.4.1	CPU Usage
GAUGE	.1.3.6.1.4.1.3417.2.4.1.1.1.4.1	CPU Usage
GAUGE	.1.3.6.1.4.1.3417.2.4.1.1.1.4.2	Disk Usage
GAUGE	.1.3.6.1.4.1.3417.2.4.1.1.1.4.2	Memory Usage
GAUGE	.1.3.6.1.4.1.3417.2.4.1.1.1.4.3	Network Usage Int 0
GAUGE	.1.3.6.1.4.1.3417.2.4.1.1.1.4.4	Network Usage Int 1

Al contar con una documentación más completa por parte del fabricante se pudo elaborar una serie de gráficas más específicas a diferencia de los equipos anteriores, pudiendo identificar información específica del desempeño del equipo en su función de Proxy. Entre las gráficas obtenidas tenemos el total de conexiones de usuarios mostrada en la figura 34, el número de conexiones generadas por el equipo mostradas en la figura 35 y el detalle de las conexiones HTTP generadas por el equipo en la figura 36. La totalidad de gráficas obtenidas se pueden observar en los anexos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

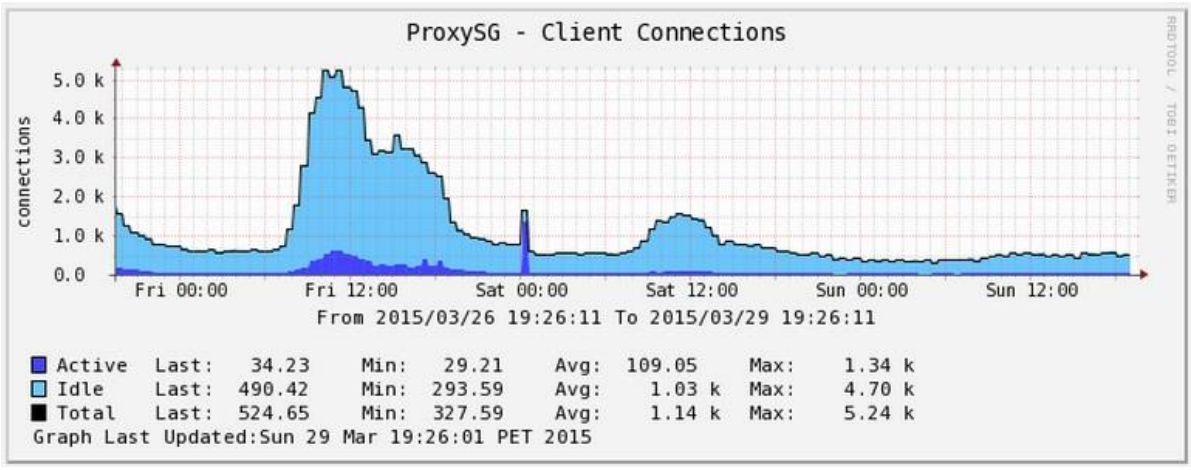

Figura 34 – Conexiones Proxy Bluecoat.

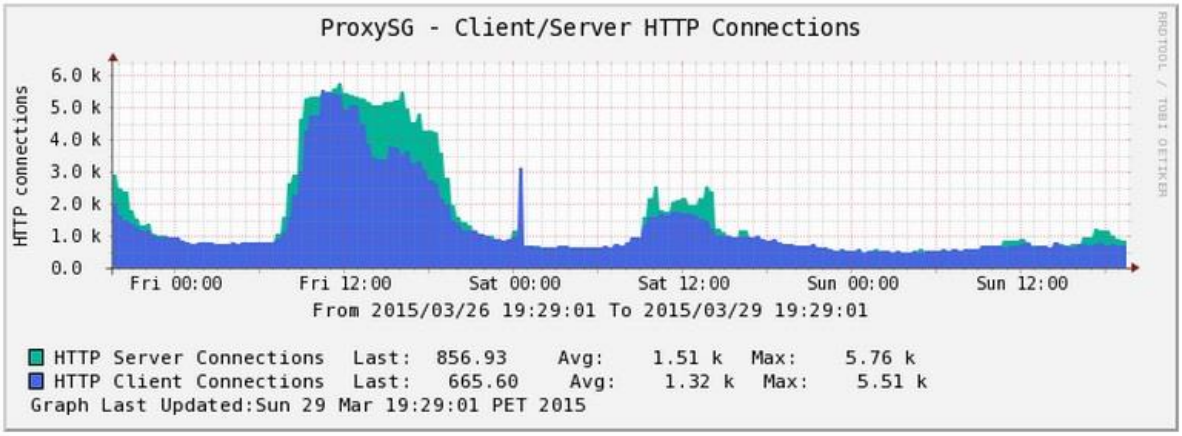

Figura 35 – Conexiones HTTP Cliente vs Servidor Proxy Bluecoat.

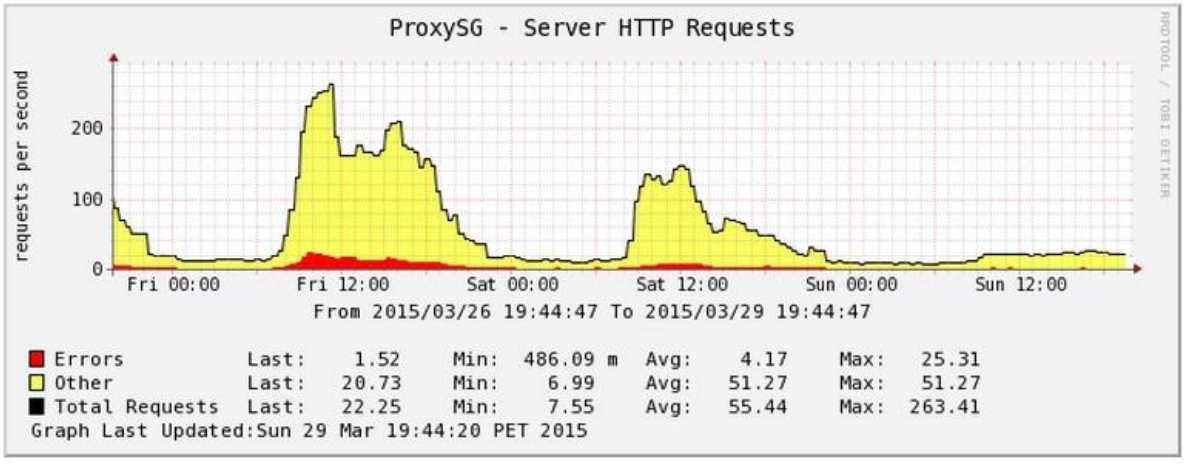

Figura 36 – Peticiones Servidor HTTP Proxy Bluecoat.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Para el caso del Proxy AV se logró construir las gráficas con el detalle de la cantidad de archivos escaneados en busca de virus y la cantidad de virus encontrados, tal como se muestra en las figuras 37 y 38.

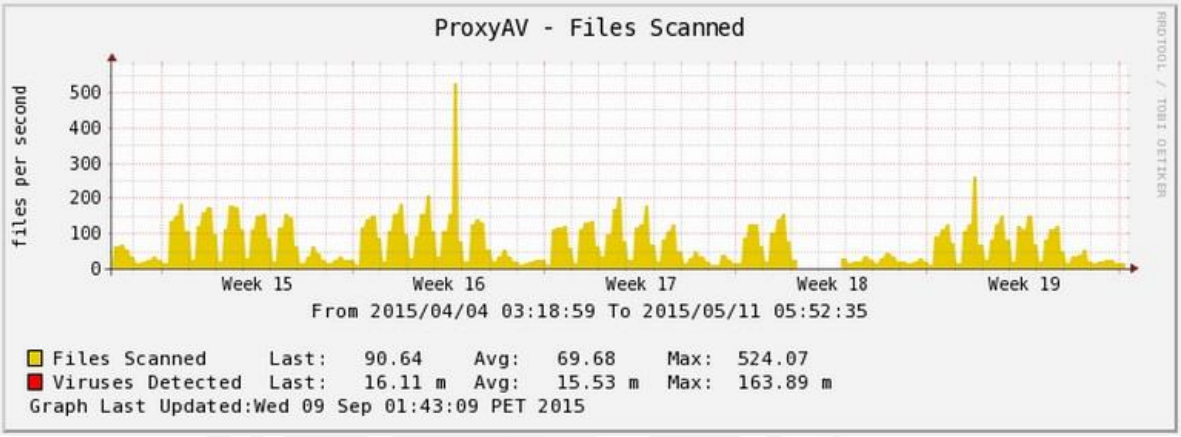

Figura 37 – Archivos Escaneados ProxyAV Bluecoat.

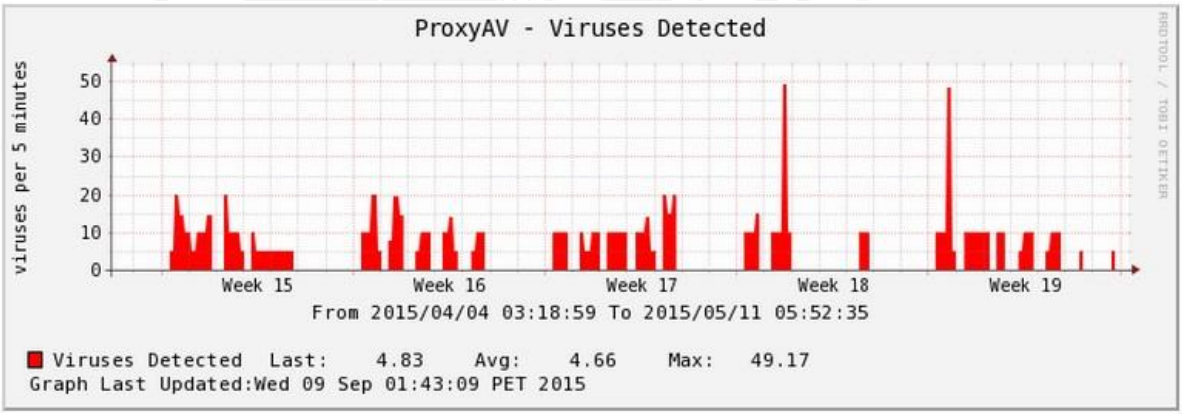

Figura 38 – Virus Detectados ProxyAV Bluecoat.

Una vez completada la construcción de las gráficas para cada uno de los equipos, se definieron rangos de funcionamiento que reflejen el buen estado o correcto funcionamiento de los equipos. A partir de los valores obtenidos por los Data Source en uso en cada gráfica se definieron valores máximos y mínimos fuera de los cuales se generará una advertencia o alerta que será notificada mediante correo electrónico, tarea para la cual se hizo uso del plugin Thold, tal como se observa en la figura 39.

Tesis publicada con autorización del autor
No olvide citar esta tesis

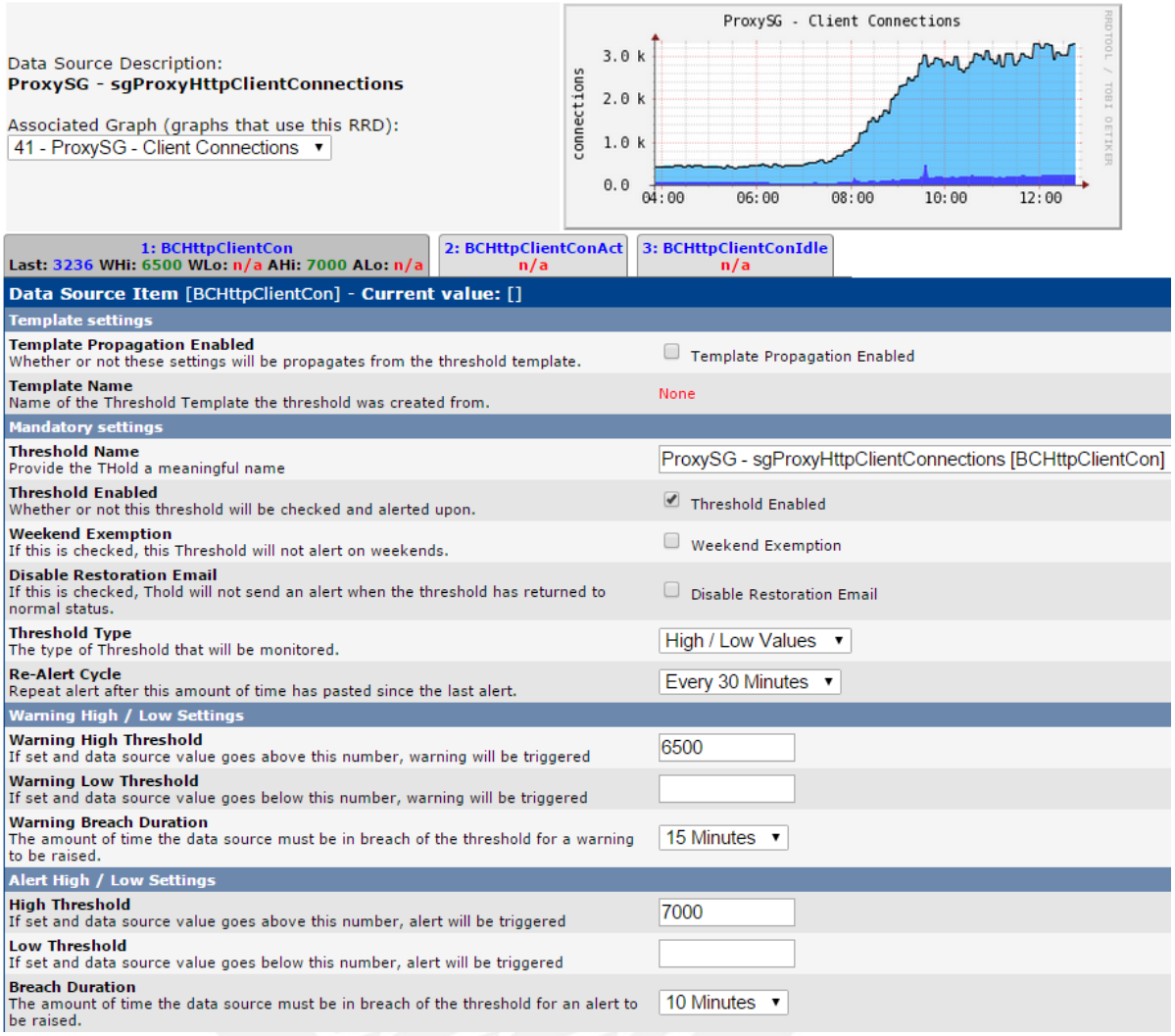

Figura 39 – Ventana de Configuración de Umbrales.

Una vez se presenten valores dentro de los umbrales y duración configurados, la herramienta debe ser capaz de notificar de este evento, para lo cual se instaló y configuro un agente MTA en este caso “Sendmail” para la generación de correos mediante el uso de un servidor SMTP propio de la empresa que nos da la posibilidad de poder enviar notificaciones vía correo tal como se muestra en la figura 40.

Tesis publicada con autorización del autor
No olvide citar esta tesis

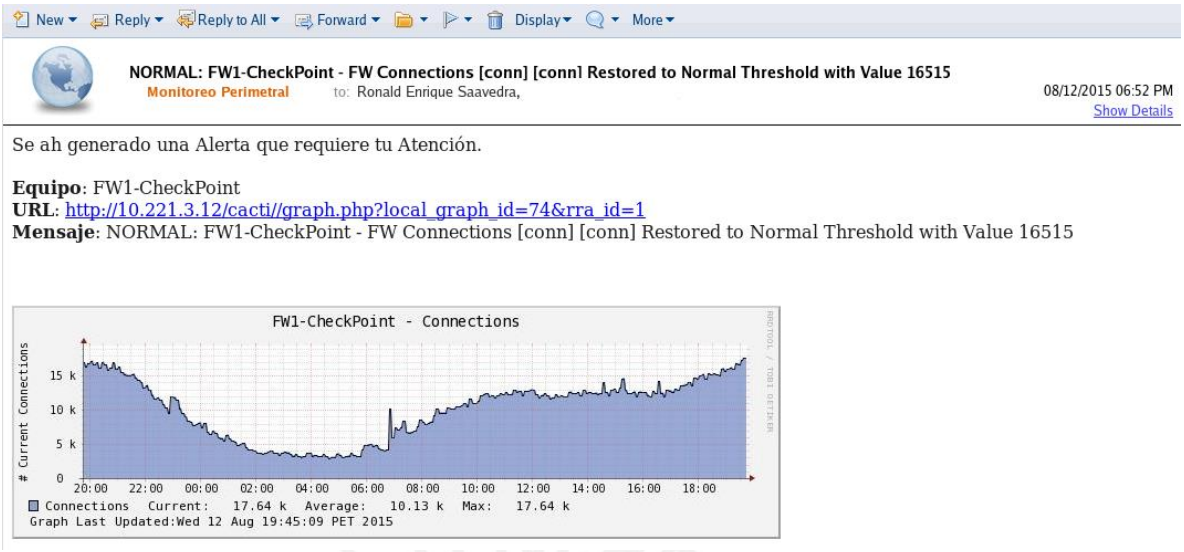

Figura 40 – Notificación de Alertas.

Además dentro de la herramienta se puede tener una visualización histórica de los eventos notificados, de manera que se tiene el detalle de la fecha, hora y valores de las alertas notificadas por cada parámetro monitoreado en cada equipo.

Host	Threshold	Time**	Alarm Value	Current Value	Status	Type	Event Description
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 21:47:08	N/A	16187	Restoral	High/Low	NORMAL: FW1-CheckPoint
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 21:42:09	17000	18979	Warning	High/Low	WARNING: FW1-CheckPoin
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 21:32:08	N/A	16966	Restoral	High/Low	NORMAL: FW1-CheckPoint
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 21:22:18	17000	19000	Warning	High/Low	WARNING: FW1-CheckPoin
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 21:05:09	17000	17957	Warning	High/Low	WARNING: FW1-CheckPoin
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 20:45:15	20000	20093	Alarm	High/Low	ALERT: FW1-CheckPoint -
FW2-Checkpoint	FW2-Checkpoint - FW Connections [conn]	2015-09-07 20:18:09	N/A	11922	Restoral	High/Low	NORMAL: FW2-Checkpoint
FW2-Checkpoint	FW2-Checkpoint - FW Connections [conn]	2015-09-07 20:12:09	12000	12281	Warning	High/Low	WARNING: FW2-Checkpoin
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 20:10:17	20000	24064	Alarm	High/Low	ALERT: FW1-CheckPoint -
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-07 18:52:14	17000	19725	Warning	High/Low	WARNING: FW1-CheckPoin
FW2-Checkpoint	FW2-Checkpoint - FW Connections [conn]	2015-09-02 14:44:09	N/A	7515	Restoral	High/Low	NORMAL: FW2-Checkpoint
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-02 14:44:09	N/A	11621	Restoral	High/Low	NORMAL: FW1-CheckPoint
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-02 14:41:10	20000	27628	Alarm	High/Low	ALERT: FW1-CheckPoint -
FW2-Checkpoint	FW2-Checkpoint - FW Connections [conn]	2015-09-02 14:41:10	15000	23312	Alarm	High/Low	ALERT: FW2-Checkpoint -
FW2-Checkpoint	FW2-Checkpoint - FW Connections [conn]	2015-09-01 18:51:48	N/A	10547	Restoral	High/Low	NORMAL: FW2-Checkpoint
FW1-CheckPoint	FW1-CheckPoint - FW Connections [conn]	2015-09-01 18:51:48	N/A	16873	Restoral	High/Low	NORMAL: FW1-CheckPoint

Figura 41 – Log Notificación de Alertas.

Así mismo dentro de la pestaña Host Status se puede observar interacción con el Plugin Monitor que es el que notifica el estado de los equipos sincronizados con la herramienta, además nos presenta algunos datos del estado de monitoreo por cada equipo, a partir de los cuales se notifica cuando por algún motivo el estado de la sincronización se ve afectada. Como se muestra en la figura 42 también se puede observar el número de gráficas obtenidas por cada equipo así como los Data Sources en uso.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Figura 42 – Estado de Equipos Monitoreados.

Para obtener un mayor detalle de los equipos monitoreados se configuró en cada uno de los equipos la IP del servidor Cacti como servidor Syslog, con el propósito de poder incluir dentro de Cacti un servidor Syslog se instaló el aplicativo "Rsyslog" que junto al uso de una base de datos mysql independiente a la utilizada por Cacti y el plugin Syslog se pudo obtener el detalle de los logs en cada equipo sincronizado. Tal como se muestra en la figura 43, se logró obtener un historio de eventos reportados de acuerdo a su nivel de prioridad en cada equipo.

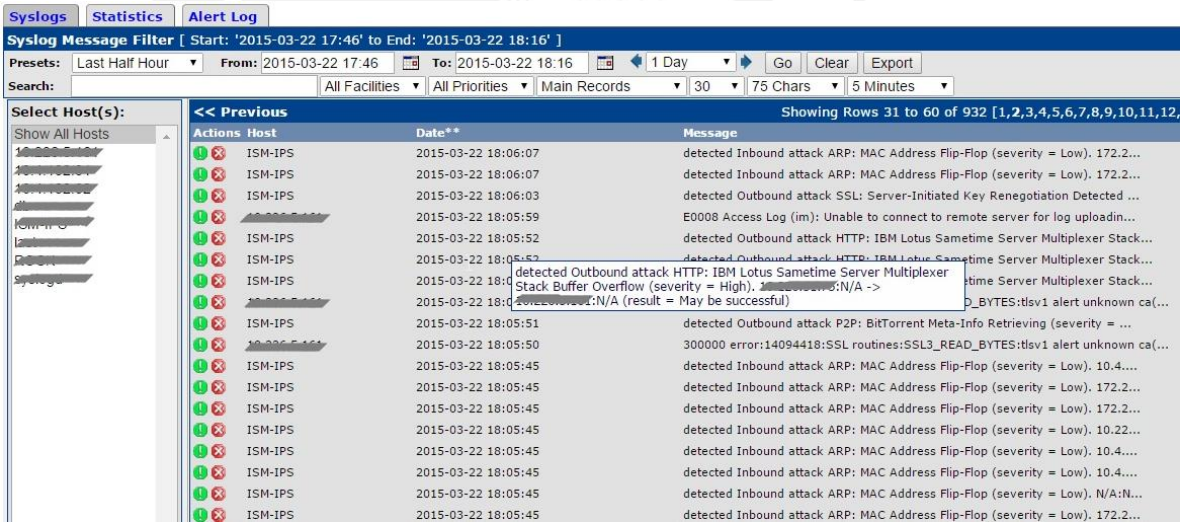

Figura 43 – Panel General Syslog.

De acuerdo a la prioridad con que los eventos son reportados se definieron reglas de alerta, según las cuales de acuerdo al tipo de evento o a las veces que un evento es notificado se ejecutarán tareas de notificación de alertas sobre las cuales se puede observar un histórico con datos de las mismas, tal como se muestra en la figura 44. Adicional a esto las alertas son

Tesis publicada con autorización del autor
No olvide citar esta tesis

enviadas mediante correo en un reporte diario de acuerdo a su nivel de criticidad, de tal manera de poder hacer un seguimiento continuo de los eventos más relevantes mostrados por la herramienta.

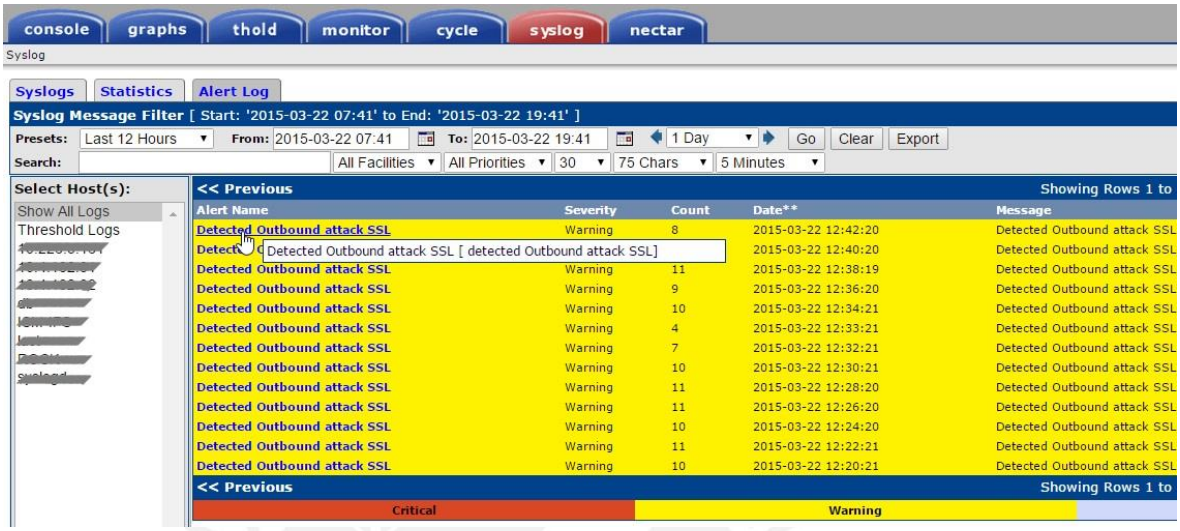

Figura 44 – Estado de Alertas Syslog.

Finalmente para poder contar con un reporte gráfico de los equipos sincronizados utilizamos el plugin Nectar a partir del cual podemos generar reportes de manera periódica a partir de las gráficas obtenidas por la herramienta. De esta manera automatizamos la tarea de elaboración de reportes de manera personalizada por equipo, gráfica, data source, generados a una hora específica del día, de información deseada y recopilada en un lapso de tiempo específico que es enviada vía correo tal como se observa en la figura 45.

Tesis publicada con autorización del autor
No olvide citar esta tesis

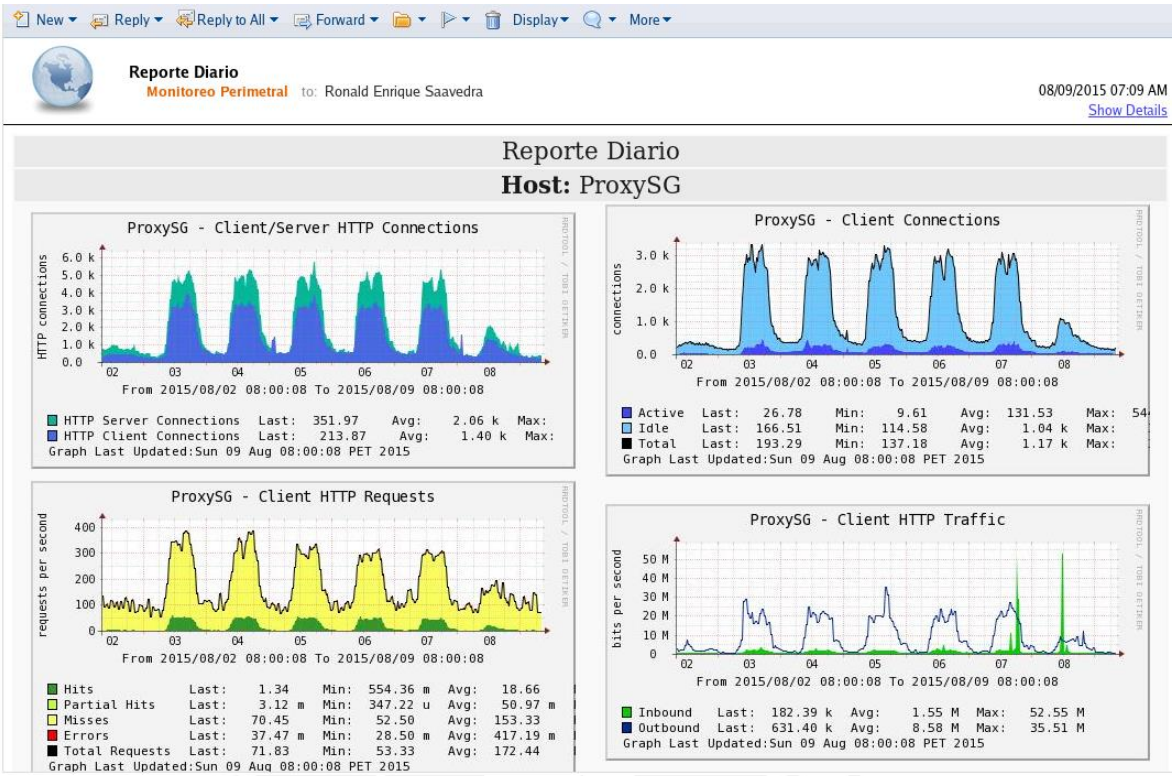

Figura 45 – Reporte Generado con Nectar.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

1. El presente trabajo de tesis ha logrado demostrar algunas de las ventajas del uso de una plataforma de gestión de equipos de seguridad en una red en producción entre las cuales podemos detallar:
   - Se integró el monitoreo de equipos de seguridad heterogéneos en la red. Se logró implementar el monitoreo de 1 cluster compuesto por 2 firewalls Check Point, 1 cluster de 2 firewalls Juniper, 1 sensor IPS McAfee, 1 proxy web Bluecoat, 1 proxy antivirus Bluecoat.
   - Se logró el monitoreo de parámetros de funcionamiento y rangos de operación acorde con los requerimiento de gestión propios de cada equipo, detallados en el capítulo 4. Entre los cuales podemos mencionar, el monitoreo de conexiones en cada equipo, así como el detalle de consumo de recursos en cada uno de los equipos sincronizados.
   - Se automatizó el proceso de notificación vía correo electrónico de advertencias y alertas en cada uno de los equipo sincronizados, logrando obtener un monitoreo activo a partir de la generación de notificaciones y reportes.

2. Se demostró que se puede atender los principales requerimientos de gestión de equipos de seguridad heterogéneos en una red mediante el uso de tecnologías disponibles y de libre acceso, sin implicar mayores costos de licenciamiento o adquisición.

3. Finalmente en base a la implementación del sistema de gestión, se logró obtener una herramienta de monitoreo que en base a su diseño funcional nos permite anticipar posibles fallas de funcionamiento y mejorar los tiempos de respuesta frente a incidencias.

Tesis publicada con autorización del autor
No olvide citar esta tesis

5.2. RECOMENDACIONES

1. Se recomienda continuar el desarrollo del sistema de gestión con el objetivo de lograr automatizar tareas de gestión que no fueron cubiertas en el alcance del presente trabajo de tesis. Dentro de las cuales podemos mencionar, monitoreo de servicios a partir de scripts, generación de backups, construcción de gráficas de estado de la red a partir del plugin wheathermaps, entre otras que pudieran brindar un mayor aporte a las tareas de gestión.

2. Se recomienda también continuar con el desarrollo de las funciones de interacción con el sistema de monitoreo a fin de lograr incluir otros medios de notificación adicionales al correo electrónico, como por ejemplo mensajes SMS o llamadas.

3. Además se recomienda continuar el estudio de las MIBs de los equipos gestionados, con la finalidad de poder identificar OIDs correspondientes a parámetros de críticos de operación que pudieron ser dejados de lado en el presente trabajo.

4. Finalmente se recomienda incluir en el sistema de gestión a equipos de comunicaciones como switches y routers que no pudieron ser incluidos en el presente estudio por no contar con la gestión de los mismos, a fin de obtener una visión más completa del estado de la red.

Tesis publicada con autorización del autor
No olvide citar esta tesis

REFERENCIAS

[1] Network Management Fundamentals. Alexander Clemm. Cisco Press, First Printing, USA, November 2006.

[2] Essential SNMP. Douglas R. Mauro and Kevin J. Schmidt. O'Reilly Media, Second Edition, September 2005.

[3] ITIL - Information Technology Infrastructure Library, Junio 2014. URL http://www.trizsigma.com/itil.html

[4] CCDA 640-864 Official Cert Guide. Anthony Bruno, Steve Jordan. First Printing, USA, May 2011.

[5] Design Zone for Data Centers, Data Center - Site Selection for Business Continuance; Julio 2014. URL http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/dcstslt.html

[6] CISSP Training Kit. David R. Miller. O'Reilly Media, USA, 2013.

[7] Official Site Cacti, Junio 2014. URL http://www.cacti.net/

[8] Comparison of network monitoring systems, Septiembre 2015. URL https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

[9] Cacti Forums, Junio 2014. URL http://forums.cacti.net/

Tesis publicada con autorización del autor
No olvide citar esta tesis