CRITERIOS Y PROCEDIMIENTOS PARA LA CREACIÓN DE POLÍTICAS DE GESTIÓN EN EL CONTEXTO DE LAS REDES DE TELECOMUNICACIONES

ANEXOS

ADRIANA MARÍA GUSTIN REBOLLEDO
CARLOS ALBERTO ASTUDILLO TRUJILLO

Director: Ing. OSCAR J. CALDERÓN CORTÉS

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
GRUPO DE NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES - GNTT
POPAYÁN, DICIEMBRE DE 2008

TABLA DE CONTENIDO

TABLA DE FIGURAS

ANEXO A

LENGUAJES PARA LA ESPECIFICACIÓN DE POLÍTICAS

En este anexo, se presenta algunos de los lenguajes utilizados para la especificación de políticas.

A.1 Ponder

Ponder es uno de los lenguajes de libre distribución para la especificación de políticas más antiguo, fruto de investigaciones del Colegio Imperial de Inglaterra. Este lenguaje es orientado a objetos, y permite la definición de políticas de gestión y seguridad para sistemas distribuidos. Además del lenguaje, Ponder define un marco de trabajo para el desarrollo y la aplicación de las políticas.

Ponder realiza una distinción entre los siguientes tipos de políticas:

- **Políticas Básicas**: Reglas que definen el comportamiento para un conjunto de sujetos. Éstas políticas son capaces de expresar autorizaciones (políticas de seguridad relacionadas con control de acceso), obligaciones, prohibiciones y delegaciones.

- **Meta políticas**: Especifican restricciones sobre el conjunto de políticas, determinando el tipo de políticas permitidas o los elementos utilizados en ellas.

- **Políticas Compuestas**: Agrupan a las políticas básicas, en este sentido pueden definir grupos de políticas, roles, relaciones, y estructura de gestión.

La Figura 1 muestra los tipos de políticas existentes en Ponder previamente descritas.

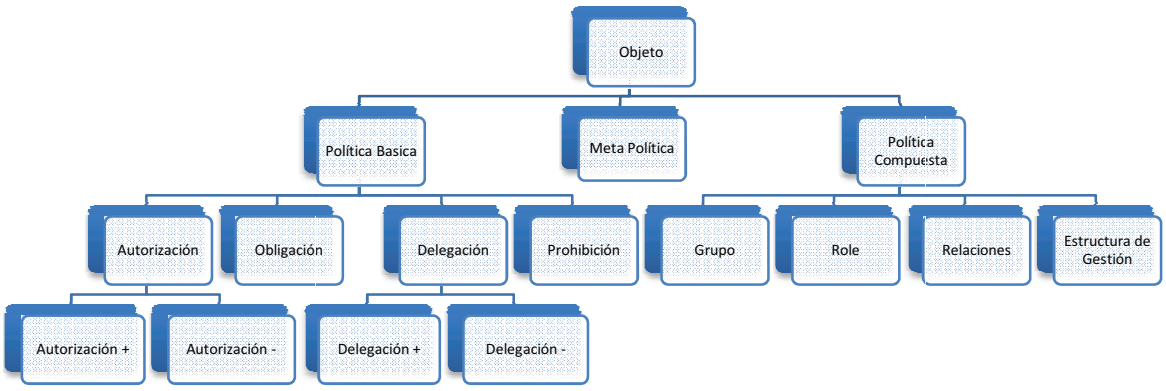

Figura 1. Políticas en Ponder

A.2 Policy Description Language – PDL

El lenguaje de Descripción de políticas (PDL - Policy Description Language) [1], también conocido como Lenguaje de Definición de Políticas (PDL - Policy Definition Language) es un lenguaje de definición de políticas desarrollado en los laboratorios Bell que no solo se utiliza en el campo de la gestión de red, sino que también se utiliza en inteligencia artificial.

PDL define las políticas como una colección de principios generales que permite especificar el comportamiento deseado de un sistema. Las políticas en este lenguaje se formulan utilizando el paradima de reglas de políticas ECA (Evento-Condición-Acción). Una ventaja notable de PDL es su excelente representación de eventos, mostrando que las reglas ECA son una propuesta flexible para especificar políticas de Gestión.

Este lenguaje ha sido implementado y usado en algunos productos Alcatel-Lucent [2].

A.3 Security Policy Language – SPL

SPL [3] es un lenguaje de libre distribución para expresar políticas de seguridad, que ayuda a decidir la aceptación de determinados eventos (soporta control de acceso). Esta aceptación depende de múltiples factores inherentes al contexto específico en el que cada evento ocurra (por ejemplo: Autor, destinatario, evento, etc.).

SPL se implementa por un monitor de eventos que decide si permite, prohíbe o ignora un evento determinado.

A.4 Trust Policy Language – TPL

TPL [4] es un lenguaje basado en XML, desarrollado en los laboratorios de IBM.

El principal propósito de TPL es mapear entidades a roles, basado en la emisión de certificados de terceros. Un rol en TPL es un conjunto de entidades que puede representar una unidad organizacional específica (por ejemplo: empleados, administradores, interventores, etc.). Los certificados son declaraciones generales acerca del sujeto (por ejemplo: Un usuario puede tener un certificado de algún instituto con su título y su promedio) y las condiciones de sus campos pueden ser dados por las políticas de una compañía (por ejemplo: un empleado debería presentar un certificado de un instituto reconocido y el promedio de calificaciones deberá estar por encima de 4.0).

TPL hace una separación entre los emisores de los certificados y el propietario del recurso; sólo el propietario define las políticas de control de acceso y confidencialidad.

A.5 eXtensible Access Control Markup Language - XACML

XACML [5] es una especificación XML de OASIS para expresar políticas de control de acceso a información en Internet. XACML describe un lenguaje de políticas y un lenguaje de Solicitud / Respuesta. El lenguaje de Políticas es utilizado para describir requerimientos generales de control de acceso y tiene extensiones para poder definir nuevas funcionalidades, nuevos tipos de datos, etc. El lenguaje Solicitud / Respuesta proporciona una forma de expresar consultas para determinar si una acción específica debería permitirse, interpretando el resultado.

XACML define 3 componentes principales para su modelo de políticas. Éstos son:

- **Reglas**: Es la unidad elemental de una política y está compuesta por un Sujeto que hace referencia a los recursos y acciones para los cuales la regla se debe aplicar; un Efecto que indica la consecuencia de la evaluación positiva de la regla; y una Condición que refina la aplicabilidad de la política.

- **Políticas**: Es un conjunto de reglas con otros tres componentes:
  - Un Objetivo y un Identificador que indican cómo se evalúan las reglas.
  - y las Obligaciones que indican operaciones específicas que deben realizarse en conjunto con la aplicación de las decisiones de autorización.

- **Conjunto de Políticas**: Reúne varias políticas.

XACML define también un marco de trabajo de gestión de políticas mostrado en la Figura 2, el cual es una extensión del modelo IETF/DMTF para un servicio particular que es control de acceso.

Figura 2. Marco de Trabajo de gestión de Políticas XACML

A.6 Policy Framework Definition Language - PFDL

Debido a que PCIM no es un lenguaje de especificación de políticas, fue utilizado como base para el desarrollo de lenguajes de especificación de políticas basados en objetos.

Uno de esos lenguajes es PFDL [6], cuyo propósito es transformar una especificación de negocio a una forma común independiente del proveedor y de los dispositivos. De esta manera, se proporciona un camino para que múltiples proveedores interpreten la política de la misma forma.

Las políticas describen por completo las funciones de negocio que deben lograrse, mientras que el conjunto de reglas de políticas define como esas funciones de negocio se obtienen.

A.7 Policy Management for Autonomic Computing – PMAC, Autonomic Computing Policy Language – ACPL y SPL

PMAC [7] es un marco de trabajo dirigido por políticas que tiene como objetivo materializar la visión de Computación Autónoma (AC – Autonomic Computing). PMAC proporciona un conjunto de herramientas muy completo que incluye un editor, análisis del sistema y de las capacidades de despliegue, y lenguajes de políticas.

PMAC está implementado en java, y propone 2 lenguajes de políticas diferentes:

- **Autonomic Computing Policy language – ACPL [8]**: Basado en XML; se utiliza para definir las partes de una expresión de política (representación escrita de una política).

La base de ACPL es ACEL (Autonomic Computing Expresion language) y facilita la escritura de las reglas de políticas.

- **Simple Policy Language – SPL [9]**: Es un lenguaje más amigable que ACPL y puede ser escrito fácilmente en un editor de texto. En PMAC todas las políticas escritas en SPL instantáneamente son transformadas en ACPL.

EL SPL de PMAC proporciona sólo un sub conjunto de la funcionalidad que ofrece ACPL e implica costos adicionales; sin embargo, trae como ventaja su simplicidad.

ANEXO B

DESCRIPCIÓN DE LA INFRAESTRUCTURA FÍSICA Y LÓGICA DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA

B.1 Infraestructura Física

La estructura física de la red de datos de la Universidad del Cauca está dividida en los sectores de**:** **Ingenierías** (con IPET, Física, Tulcán y Laboratorios de Química), **Medicina** (comprende salud y el Hospital), **Educación** (con servicios generales), **Santo Domingo**, **Las Guacas**, **Vicerrectoría de Investigaciones**, **Consultorio Jurídico**, **El Carmen** (con Casa Caldas, Casa Mosquera, Casa Rosada y Casa Albán), **Unidad de Salud** y **Santander de Quilichao**. Los sectores constituidos por uno o más edificios quedan conectados entre sí a través de un backbone de fibra óptica multimodo y monomodo.

Físicamente la red de la Universidad posee una topología de doble estrella, teniendo como centro los edificios del IPET y El Carmen, como se muestra en la Figura 1. Existen sectores en los cuales la cantidad de equipos es demasiado baja, como es el caso del Consultorio Jurídico y del hospital Alfonso López, por tanto no es necesario llegar ahí directamente. El enlace al Consultorio Jurídico se realiza por medio de modem HDSL (High bit-rate Digital Subscriber Line) contratado con Emtel, y el enlace al hospital Alfonso López se realiza a través de un servicio de ADSL con una velocidad de 256 kbps. La conexión con el sector de Santander de Quilichao se realiza a través de un enlace inalámbrico desde Cali a través de ETB con una velocidad de 1Mbps.

Actualmente el acceso WAN o acceso a Internet se realiza a través de los ISP´s (proveedores de servicio de internet) EMTEL y ETB. La conexión con EMTEL se realiza a través de fibra óptica con un ancho de banda contratado de 8 E1s (16 Mbps Dedicados) y la Conexión con ETB se realiza a través de un radioenlace con las tres cruces con una capacidad de 6 E1s (12 Mbps Dedicados), para un total de 28 Mbps de acceso a internet.

El acceso remoto o acceso telefónico se realiza por medio de un enlace primario (PRI- Primary Rate Interface) de la red digital de servicios integrados (RDSI) para 30 canales (los cuales permiten una velocidad máxima de 56 Kbps si el usuario se conecta a través de una línea telefónica analógica; 64 Kbps cuando el usuario tiene el servicio RDSI; y 128 Kbps cuando utiliza los 2 canales B); este enlace es suministrado por EMTEL.

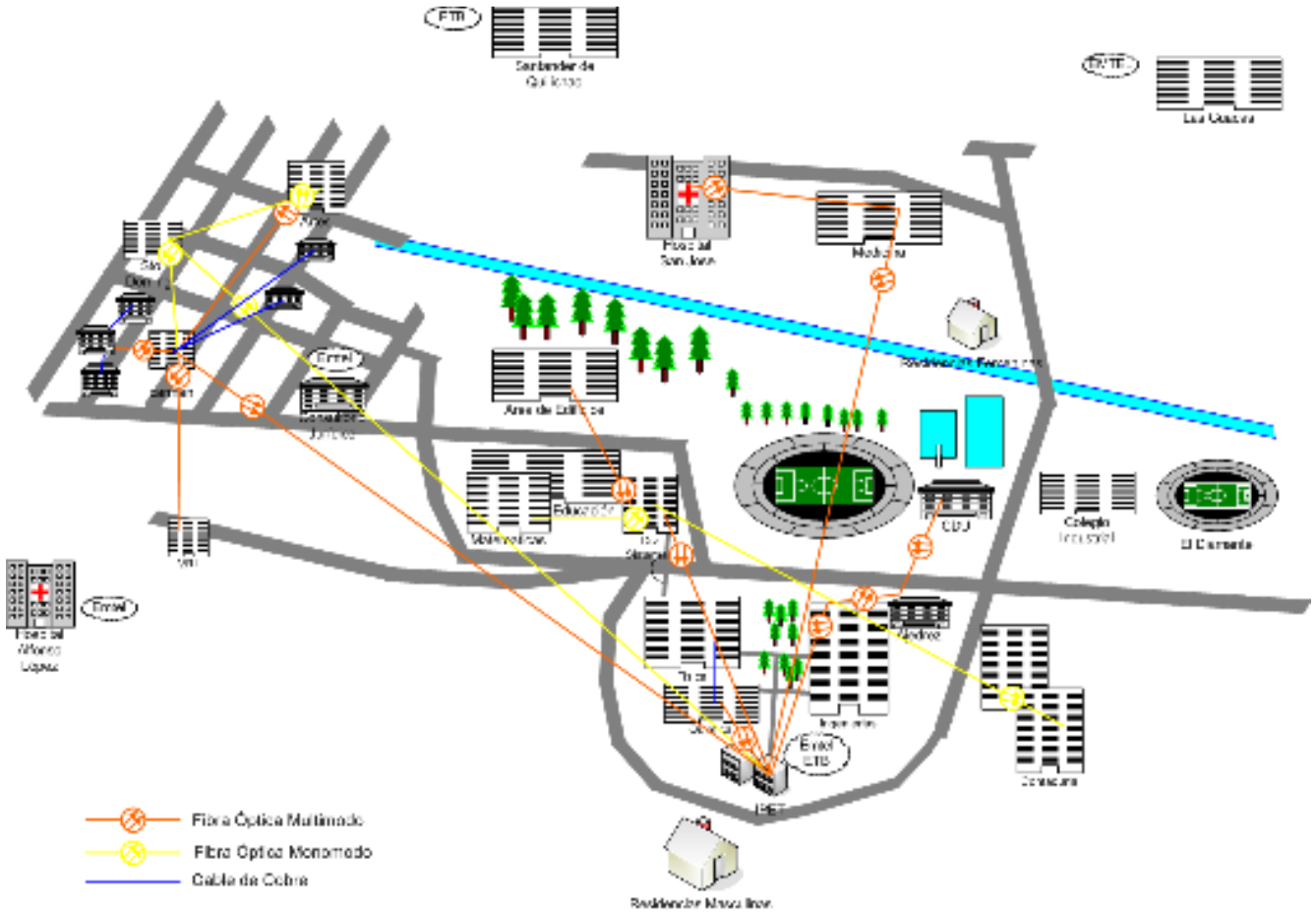

Figura 3. Infraestructura Física de la Red de Datos de la Universidad del Cauca

La infraestructura física de la red de cada edificio ha sido desarrollado bajo las directrices de sistemas de cableado estructurado, utilizando par trenzado no-apantallado (Unshielded Twisted Pair - UTP) Categoría 5 y Categoría 6; teniendo por lo menos un centro de cableado en cada edificio y sus respectivos puntos de red que se extienden hasta los puestos de trabajo dentro del edificio. En edificios grandes donde las limitaciones de distancia del Cableado no permiten que un solo centro de cableado recoja todos los puntos de red, tienen centros de cableado secundarios que recogen los puntos de red distantes; y que a su vez están conectados al centro de cableado principal (conocido como centro de cableado 1 o CC1) a través de un número de cables UTP, determinado por el tamaño en puntos de red de los centros de cableado secundarios.

La Universidad tiene conectados aproximadamente 3000 equipos de cómputo a su red, los cuales interactúan con cerca de 40 servidores. Actualmente y dependiendo de las necesidades de cada facultad o sede, la red es utilizada para transmitir datos, voz, video y compartir recursos (impresoras, módems, discos, etc.). En su mayor parte la Universidad posee como sistema operativo de sus equipos de cómputo Windows pero ha empezado a adoptar Linux y otras tecnologías libres.

B.2 Infraestructura Lógica

La Red de la Universidad del Cauca está conformada por una LAN (red de área local) que utiliza una tecnología descrita en el estándar 802.3 del IEEE (Institute of Electrical and Electronic Engineers), el cual habla de un método de acceso al medio denominado Acceso Múltiple por Detección de Portadora con Detección de Colisión (Carrier Sense Multiple Access/Collision Detection - CSMA/CD).

IEEE 802.3 permite un funcionamiento a 10 Mbps sobre diferentes medios físicos (coaxial, par trenzado, fibra óptica); sin embargo el estándar a evolucionado permitiendo alcanzar velocidades de 100, 1000 y 10000 Mbps, oficialmente conocidos como IEEE 802.3u, 802.3z, 802.3a y comúnmente llamados Fast-Ethernet, Gigabit-Ethernet, y 10 Gigabit-Ethernet, respectivamente.

Como se mencionó previamente la red de datos cuenta con un backbone en fibra óptica el cual a pesar de poseer una topología de doble estrella físicamente, tiene una topología de una solo estrella, con centro en el IPET. Aunque físicamente Santo Domingo se conecta al Carmen, lógicamente tiene una conexión directa al IPET ya que la fibra óptica esta puenteada en el Carmen evitando la conmutación de datos en ese punto.

La infraestructura de equipos de red se divide en Core, Distribución y Acceso. La Universidad cuenta con un equipo de Core Cisco Catalyst 4507R que provee conexiones Gigabit Ethernet en sus puertos de cobre y fibra óptica, éste se encuentra ubicado en el IPET. En cada sector existe por lo menos un switch Ethernet conectado a través de su puerto de alta velocidad al backbone, estos equipos de distribución son Cisco Catalyst 3750G que suministran conexiones Gigabit Ethernet a los equipos de acceso. Los Equipos de Acceso o Borde son Cisco 2950 y 2960G que suministran conexiones a 10Mbps, 100 Mbps y 1Gbps, además de algunos Hubs Ethernet, que suministran

conexiones a 10Mbps a los usuarios finales. Estos equipos se encuentran repartidos entre los centros de cableado principal y secundarios, conectados utilizando el cableado estructurado existente basado en UTP Categoría 5 y 6.

La Figura 4 ilustra la arquitectura de interconexión real entre Internet y la intranet de la Universidad del Cauca. Como se aprecia, todo el tráfico hacia y desde Internet pasa a través del gestor de ancho de banda NetEnforcer AC-404 y también a través del Firewall FortiGate 310B.

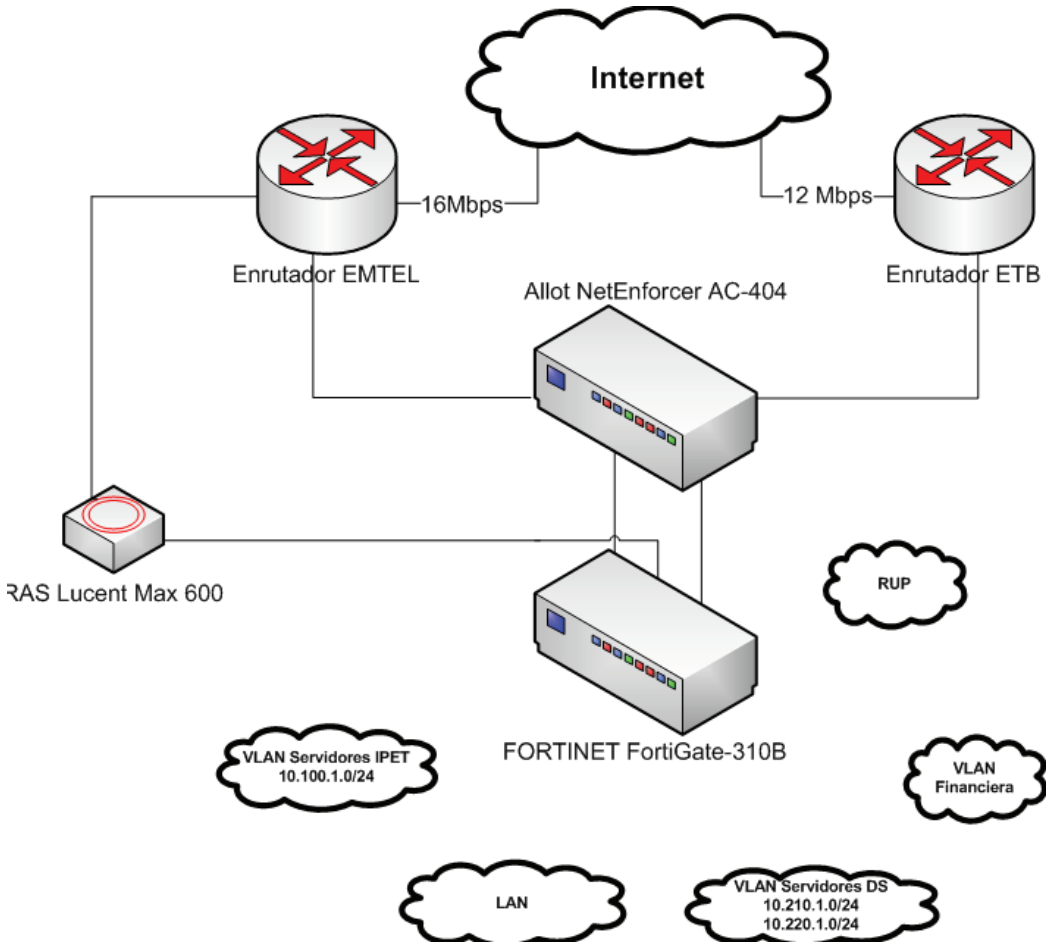

Figura 4. Interconexión entre Internet y la Intranet de la Unversidad.

A continuación se presentan cada una de las subredes que se encuentran en la actualidad. Sin embargo, al momento de escribir este documento se tenía planeado la expansión de éstas, ya que se estaba segmentando la red por sectores o edificios. Están en proyectos crear la subred del sector de ingenierías, y de otras facultades:

- 172.16.0.0/16: Esta subred privada aloja la mayor parte de los equipos de la red que no tienen conexión directa a redes externas. Los equipos pertenecientes tienen acceso a recursos HTTP y FTP por medio de servidores proxy y algunos cuentan con servicio de NAT (Traducción de direcciones de red) para acceso a otro tipo de recursos que no pueden ser accedidos por el servicio de proxy.
- 172.19.0.0/16: Subred asignada al sector de las guacas. Cuenta con acceso a los mismos servicios que la red anterior.
- 172.20.0.0/16: Esta es la subred asignada a Santander de Quilichao y también cuenta con los mismos servicios de la sub-red 172.16.0.0/16.
- 172.21.0.0/16: Esta es la Subred asignada al Consultorio Jurídico. Cuenta con las mismas prestaciones de las subredes anteriores. Se enlaza por medio del enlace de EMTEL.
- 10.200.2.0/24: Esta es una sub-red que tiene acceso a recursos externos, pueden salir directamente a internet. Se utiliza para asignárselas a ciertos funcionarios, y docentes de la universidad que requieren de un servicio "especial".
- 10.200.1.0/24: Esta es la red asignada a los servidores de la red de datos. Éstos por el momento se encuentran alojados en el IPET.
- 10.210.1.0/24: Esta es la sub-red de todas las estaciones de trabajo del área de servidores, estas tienen privilegios para acceder a los servidores y herramientas de la red. Se encuentran protegidos por una VLAN.
- 10.220.1.0/24: Esta es la sub-red de los servidores de la División de Sistemas que manejan los Sistemas de Información y las Bases de Datos). Próximamente la mayoría de los servidores van a ser trasladados a este lugar. Se encuentran protegida por una VLAN.
- 10.230.1.0/24: Esta es la sub-red de financiera, se encuentra protegida por una VLAN debido a que ésta requiere de una alta seguridad ya que se realizan pagos y transferencias bancarias.
- 190.5.195.0/24: Esta subred es suministrada por el proveedor de servicio EMTEL.
- 190.24.10.128/25: Esta subred es suministrada por el proveedor de servicio ETB.

La red universitaria se encuentra dividida en subredes IP lógicas gracias a las capacidades de enrutamiento que brinda el switch de núcleo multinivel que interconecta cada subred, así como del nuevo equipo Firewall FortiGate. La Figura 5 ilustra de manera lógica la distribución de estas subredes.

La red universitaria pertenece a la red universitaria de Popayán (RUP). Ésta es una red regional, conformada por varias universidades de Popayán que tiene como objeto promover y coordinar el desarrollo de aplicaciones avanzadas de redes de telecomunicaciones y cómputo en la región, enfocada al desarrollo científico y educativo de la sociedad.

La RUP se conecta a la red académica de tecnología avanzada RENATA, que es la red de redes regionales académicas en Colombia a través de EMTEL. Renata a su vez se conecta a la red de Cooperación Latinoamericana de Redes Avanzadas (CLARA) para tener acceso de alta velocidad a más de 700 instituciones de educación superior y centros de investigación de América y Europa.

CLARA se conecta a la red norteamericana Internet 2 y conecta a la Red Avanzada Europea GEANT, gracias al proyecto América Latina Interconectada con Europa (ALICE).

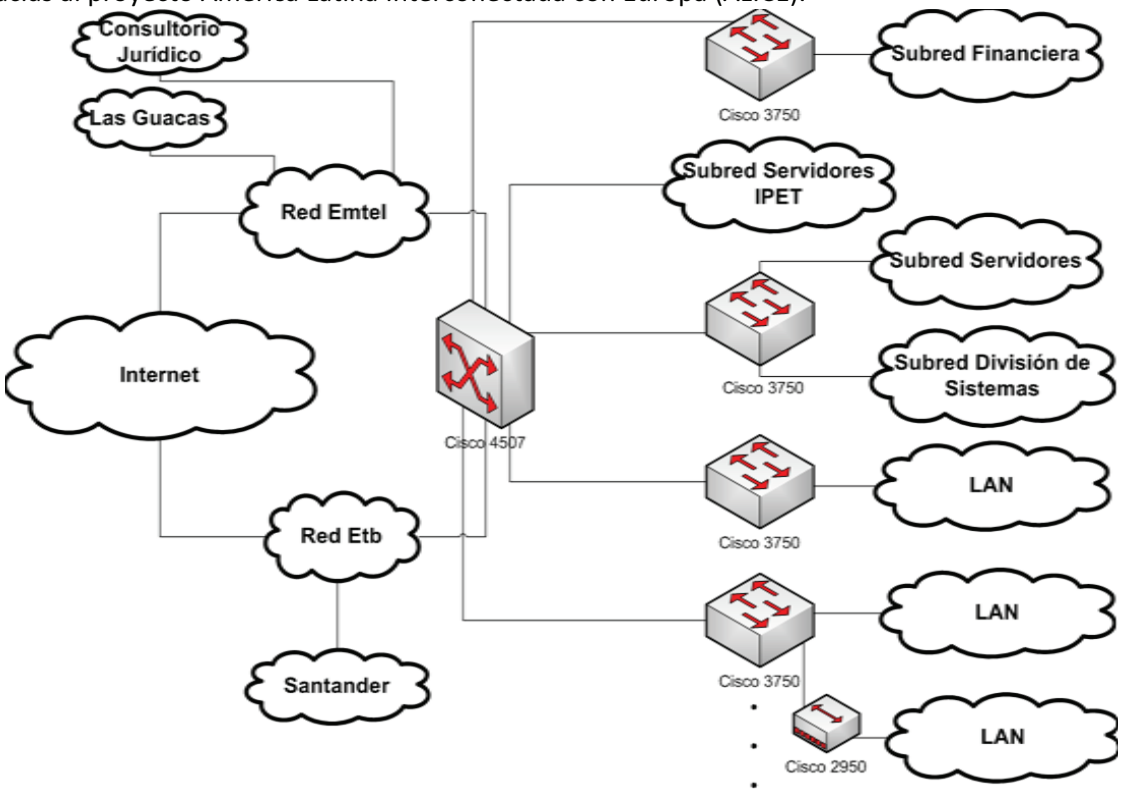

Figura 5. Distribución Lógica de las Subredes de la Red de Datos.

ANEXO C

PRODUCTOS COMERCIALES PARA LA GESTIÓN BASADA EN POLÍTICAS

La mayor parte de las herramientas asociadas a la gestión basada en políticas son prototipos de investigación y hay muy pocos ejemplos que están siendo aplicados en un entorno comercial. La mayoría de estas herramientas comerciales son específicas para la gestión de calidad de servicio, aunque algunos incluyen también la configuración del control de acceso.

A continuación se presenta una descripción de los productos comerciales más importantes utilizados por proveedores de red, proveedores de servicio y redes corporativas, específicas para la gestión de QoS.

C.1 Cisco QoS Policy Manager – QPM

Por medio de una interfaz basada en web QPM define las políticas de QoS y las traduce en comandos específicos para los dispositivos a través de una interfaz de línea de comandos (CLI - Command Line Interface) [10]. Dado que las políticas no especifican los elementos a los cuales están dirigidas, el administrador asigna manualmente a través de una consola de gestión los dispositivos a los cuales se aplican cada política.

QPM sigue la representación de IETF para una regla de política de QoS, la cual consta de un conjunto de condiciones y de una serie de acciones. Las acciones (clasificar, limitar, configurar y poner en cola el tráfico) se aplican sobre un flujo de tráfico si este flujo coincide con los filtros (condiciones) definidos en las políticas.

C.2 Cisco CiscoAssure

CiscoAssure es una herramienta que da soporte a las operaciones de gestión de QoS y además permite al administrador definir políticas de control de acceso para los dispositivos que se están gestionando.

Aunque las políticas se especifican utilizando el paradigma condición/acción definido por el estándar-CIM de la IETF, la herramienta almacena sus propias políticas en una base de datos. La interfaz de usuario permite a los administradores especificar fácilmente múltiples condiciones para activar políticas.

Las condiciones pueden especificarse de acuerdo a combinaciones de direcciones IP (origen y/o destino), puertos de aplicación, o protocolos que se estén utilizando (IP, TCP o UDP). Las acciones se aplican a los enrutadores utilizando el lenguaje de la interfaz de línea de comandos (CLI) Cisco. La interoperabilidad entre múltiples proveedores se proporciona con una implementación de COPS.

C.3 HP PolicyXpert

HP PolicyXpert define una política como una combinación de una o más reglas. Una regla de política consta de una única acción y de una o más condiciones. Estas reglas se construyen a partir de una o más condiciones, las cuales se basan en información de paquetes, hora del día o información de un protocolo de nivel superior como HTTP URL o VLAN ID. La herramienta soporta muchos estándares, incluyendo COPS, DiffServ y RSVP.
HP PolicyXpert brinda soporte a la gestión de dispositivos de varios proveedores. También ofrece un Kit de Desarrollo de Software Agente (SDK - Agent Software Development Kit) que permite a los proveedores a desarrollar soporte para los mecanismos de calidad del servicio específicos para sus dispositivos.

C.4 Allot Communications NetPolicy

Este producto también sigue los lineamientos de la IETF. Una regla de política se compone de condiciones y acciones. Las condiciones se utilizan para comparar direcciones IP, protocolos, datos de aplicación, configuración de tipo de servicio (ToS) y la hora del día. El administrador puede agrupar dispositivos en dominios y aplicar manualmente un conjunto de reglas de políticas en uno de los dominios existentes. El repositorio de políticas se implementa utilizando LDAP y la información de la política se pasa a los dispositivos de destino utilizando COPS o CLI.

Esta Solución está compuesta por el NetEnforcer y el NetXplorer, Su arquitectura distribuida consta de tres niveles:

- Múltiples NetEnforcers,
- Un servidor NetXplorer, y
- Clientes GUI (Graphic user interface – interfaz gráfica de usuario).

La Figura 6 presenta un resumen de la arquitectura del sistema, y su relación con la arquitectura de gestión de IETF.

- ***NetEnforcer***

  Los dispositivos para gestión de ancho de banda Allot NetEnforcer [11] proporcionan el control dinámico que los operadores de red necesitan para optimizar la entrega, el rendimiento y la rentabilidad de servicios de banda ancha y WAN. Los dispositivos NetEnforcer ayudan a los operadores a identificar, clasificar, y priorizar el tráfico de red por aplicaciones y por usuarios [12].

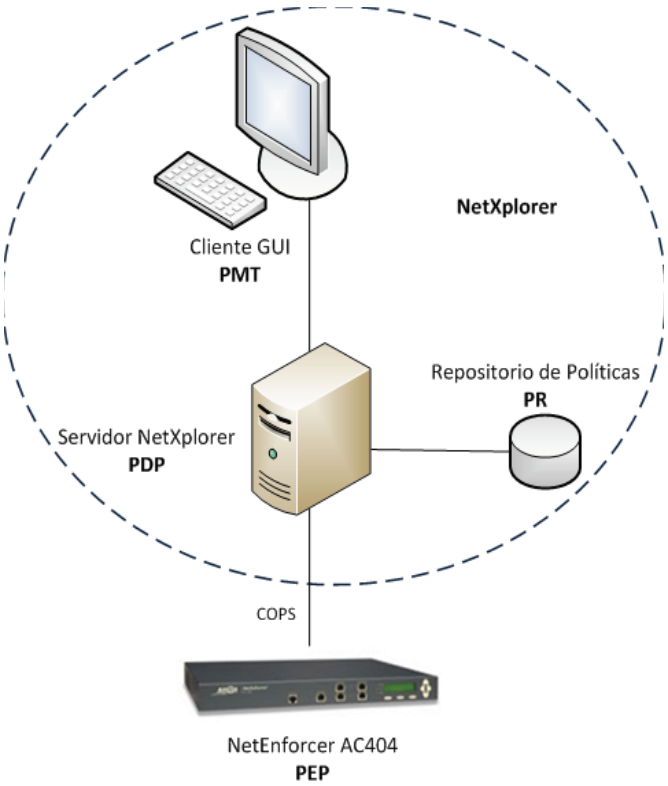

Figura 6. Arquitectura de Políticas de Allot Communications

- ***Gama de Modelos***

  Los dispositivos Allot NetEnforcer están disponibles en una variedad de modelos diseñados para adaptarse a los requerimientos de cualquier red de banda ancha o WAN.

  - La serie NetEnforcer AC-400 (ver Figura 7) está especialmente diseñada para gestionar tráfico de Internet en enlaces Ethernet de hasta 200 Mbps.

Figura 7. NetEnforcer AC-400

  - La serie NetEnforcer AC-800 (ver Figura 8) está especialmente diseñada para gestionar tráfico de Internet en enlaces Ethernet de hasta 620 Mbps.

Figura 8. NetEnforcer AC-800

- La serie NetEnforcer AC-1000 (ver Figura 9) está especialmente diseñada para gestionar tráfico de Internet en enlaces Ethernet de hasta 2 Gbps.

Figura 9. NetEnforcer AC-1000

- La serie NetEnforcer AC-2500 (ver Figura 10) está especialmente diseñada para gestionar tráfico de Internet en enlaces Ethernet de alta velocidad de hasta 5 Gbps.

Figura 10. NetEnforcer AC-2500

- ***Productos de la Serie NetEnforcer AC – 400[13]***

Esta serie está disponible en 2 modelos muy útiles para monitoreo y la gestión de todo tipo de tráfico en enlaces de hasta 200 Mbps: NetEnforcer AC-402 y AC-404. La Red de Datos de la Universidad del Cauca cuenta actualmente con el equipo NetEnforcer AC-404.
Principales Características:

- 2 o 4 puertos (para AC-402 y AC-404 respectivamente).
- Rango de velocidades de operación: 2, 10, 45 y 100 Mbps.
- Gestión centralizada.
- Identifica cientos de aplicaciones y protocolos.
- Priorización de tráfico basada en la definición de políticas de QoS.
- Alarmas pro-activas.
- Control de conexión basado en políticas.
- Rendimiento a prueba de fallos.

- ***NetXplorer***

  Allot NetXplorer [14] es un software de gestión centralizado que trabaja en conjunto con los dispositivos NetEnforcer para ofrecer a las redes de gestión la inteligencia necesitan para optimizar los servicios IP. NetXplorer le permite ver y entender a los operadores de red cómo su ancho de banda se consume por las aplicaciones y los usuarios de la red [15]. Su interfaz intuitiva y la amplia variedad de funcionalidades que proporciona ayuda a los operadores de red para:

  - Regular el ancho de banda por aplicación y por usuario.
  - Analizar los patrones de tráfico y las tendencias de uso.
  - Identificar el tráfico malicioso y neutralizar los ataques.
  - Traducir las decisiones de negocios en servicios y políticas de control de tráfico.

  Los Proveedores de Servicios utilizan el NetXplorer para:
  - Implementar diferentes servicios de valor agregado.
  - Tomar medidas de tráfico para facturación.
  - Ofrecer auto-monitoreo y auto-aprovisionamiento de servicios a los clientes de las empresas.

  Las Empresas utilizan el NetXplorer para:
  - Gestionar proactivamente el tráfico de la red.
  - Asegurar el desempeño de aplicaciones críticas.

C.5 Análisis de las Herramientas Comerciales de GBP

Además de las herramientas consideradas aquí, hay otros productos de varias empresas que proporcionan características similares; Lucent RealNet Rules, Nortel's Optivity, Extreme Networks's ExtremeWare, Gold Wire Technology's Formulator y Dorado Software's Redcell Suite son algunos de estos. Basados en nuestra investigación de las diferentes herramientas disponibles, podemos resumir sus características así:

Ninguna de las herramientas presentadas previamente soporta un lenguaje de especificación de políticas, ni considera la automatización del ciclo de vida de las políticas. Es de aclarar que estas herramientas son de primera generación, esto quiere decir que su funcionalidad es tan solo un conjunto de las funcionalidades proyectadas o prometidas de la GBP. Además, ninguna adapta automáticamente la configuración de los elementos de la red cuando cambian las condiciones dentro de la red gestionada; sino que por el contrario dichas configuraciones deben agregarse manualmente por el administrador a través de la consola de gestión. También algunas se construyeron con soluciones propietarias lo que impide la interoperabilidad entre los distintos elementos de la red y entre soluciones de distintos proveedores.

ANEXO D

ARTÍCULOS PUBLICADOS

D.1 Propuesta de un modelo de ciclo de vida de las políticas para la gestión de redes de Telecomunicaciones

Tipo de Publicación: Articulo en Revista.

Información de la Publicación: Ingenium, Revista de la Facultad de Ingeniería de la Universidad de San Buenaventura de Bogotá, pp. 24 - 32. ISSN: 0124-7492.

Fecha de Publicación: Junio de 2008.

Información Adicional: Revista Indexada en Latindex y en el Publindex de COLCIENCIAS (Categoría C).