FACTIBILIDAD DE IPSEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO

Jorge Enrique López Logacho[1] Juan Carlos Oleas Castelo[2] Darwin Leonidas Aguilar Salazar[3]

[1] *Maestrante en Redes y Conectividad, Departamento de Ingeniería Eléctrica y Electrónica, Escuela Politécnica del Ejército, Sangolquí, Ecuador, Quito,* georgelopez05@hotmail.com

[2] *Director de tesis, Telefónica, Ecuador, Quito,* juan.oleas@telefonica.com

[3] *Docente oponente, Departamento de Ingeniería Eléctrica y Electrónica, Escuela Politécnica del Ejército, Sangolquí, Ecuador, Quito,* dlaguilar@espe.edu.ec

Resumen: El presente trabajo tiene como objetivo realizar un breve análisis de factibilidad para la implementación de túneles IPSec sobre el protocolo IPv6 para la red LAN de la Universidad Politécnica Salesiana Sede Quito, Campus Girón, se ha realizado el levantamiento del estado inicial de la red y se han determinado claramente los lineamientos de diseño, tanto modular como jerárquico, finalmente se ha propuesto las configuraciones a seguir para la implementación del protocolo de seguridad en la red, con las pruebas respectivas de su funcionamiento, obteniéndose como conclusión que es totalmente factible la propuesta de implementación en la red de la mencionada institución.

Palabras clave: IPv6, IPSec, Seguridades, Universidad Politécnica Salesiana, SA, ESP, Encriptación.

Abstract : This paper aims to make a brief analysis on the feasibility of implementing IPSec tunnels on the IPv6 protocol for LAN network in the Universidad Politécnica Salesiana Sede Quito, Campus Giron has made the lifting of the initial state of the network and have clearly established design guidelines, both modular and hierarchical, finally proposed configurations to continue to implement the security protocol in the network, the respective tests of its operation, obtaining the conclusion that it is entirely feasible proposal network implementation that institution

Keywords: IPv6, IPSec, Securities, Salesian Polytechnic University, SA, ESP, encryption.

I Introducción

IPv6 aparece como una propuesta de solución a las limitaciones que aparecieron en IPv4, debe proporcionar autenticación y encriptación, para aumentar la seguridad, la existencia de cabeceras de extensión de autenticación facilita el encriptamiento de seguridad, lo que permite garantizar la integridad e identidad del paquete. El protocolo IPv6 introduce rutinas específicas para la encriptación y autenticación de los diferentes tipos de paquetes, la aplicación de ellos solamente depende de que estas funciones estén disponibles, esta es una de las muchas razones para que la Universidad Politécnica Salesiana Sede Quito, Campus Girón ofrezca un escenario apropiado para la realización de la propuesta de implementación del protocolo IPSec en su infraestructura. La red de este campus posee las características y necesidades que justifican esta investigación puesto que maneja información crítica que define el correcto funcionamiento de la institución como tal.

II. Análisis de Factibilidad de la implementación de IPSec en la UPS

A. Levantamiento de situación inicial de la red.

Dentro del diseño de red de la universidad, se deberá analizar los siguientes aspectos: modularidad

y jerarquía.

Diseño modular.-La modularidad es el principio fundamental del diseño de la red empresarial puesto que define cómo está ensamblada en sus múltiples bloques, que han sido diseñados por separado, esto permite una mejor aplicación de la jerarquía y la redundancia. Este diseño se compone de los siguientes módulos:

Núcleo de la empresa.- Interconecta el resto de módulos, mantiene la redundancia total y ofrece servicio continuado, en la UPS este módulo está compuesto por el switch Cisco Catalyst 507R, el equipo cuenta con sistemas redundantes.

Campus de la empresa.- En este modulo se encuentran todos los elementos de red que operan independientemente, su finalidad es ofrecer conectividad entre el core y los usuarios finales, en el Campus Girón esto se lleva a cabo mediante los switch Cisco Catalyst 3750, los que físicamente se conectan al core por medio de fibra óptica multimodo.

Data center de la empresa.- Aquí se debe identificar tres submódulos: Servidores, redes y almacenamiento. El submódulo de servidores está divido en dos áreas: la de servidores internos y la zona desmilitarizada, en el submódulo de los servidores internos, están conectados directamente al switch core, por medio de tecnología Gigabit Ethernet, el segmento SAN esta constituido por un servidor HP DL380G7. La red mantiene conectividad por fibra canal con el switch core. El submódulo de la zona desmilitarizada contiene los servidores de acceso público como el de mail, el servidor web, el de tarifación y antivirus, el DHCP y DNS entre otros, estos equipos van conectados al Cisco ASA 5520, se cuenta con soluciones Blade donde reposan las aplicaciones más críticas como el servicio de educación virtual, servidor de archivos, de directorio activo, de aplicaciones, proxy y e-mail, en otros equipos se han implementado el pool de servidores proxy, la aplicación de gestión de red y el servidor de backup, adicionalmente se dispone de servidores HP Proliant DL-380G4 para el segmento SAN, video conferencia, tarifación y el antivirus. El resto de servidores están sobre plataformas de diferentes tecnologías, que ofrecen servicios de red como DHCP, DNS, SQUID, VoIP, IVR, AVAC.

Frontera de la empresa.- Contempla la conectividad a Internet, el acceso WAN y el acceso remoto a los servicios internos de la organización se lo realiza por medio de dos proveedores de datos, estos son Telconet a través de un router Cisco 3825 y CNT por medio de un router Cisco 2801, de esta manera los campus Sur, Kennedy, Cayambe y Latacunga acceden a Internet a través de la infraestructura del campus. La seguridad de borde se lo controla por un ASA 5520, que maneja el sistema de prevención de intrusiones y el firewall, el acceso remoto a aplicaciones internas de la organización se lo realiza por medio de un Servidor de Acceso Remoto o RAS, que está conectado a la PTSN de CNT, al igual que el Gateway VoIP. La seguridad se fortalece con un pool de servidores proxy, el control de tráfico y calidad de servicio se lo hace con el Cisco Packet Shaper 1700, tal como se muestra en la figura 1. Adicionalmente las VLAN´s de acceso se gestionan en el switch de capa 3 CISCO 4507R ubicado en el datacenter y el acceso a la WAN se lo hace por un router CISCO 2801 para el proveedor CNT y un router Cisco 3825 para el proveedor Telconet.

Servicios de red.- Básicamente manejan servicios de seguridad y administración tales como

Jorge E López. georgelopez05@hotmail.com

Activa directory, proxy, squid y antivirus, servicios de aplicaciones orientadas a usuarios como mail, web, AVAC, SIEVAC, biométrico, fileserver, servicios de infraestructura y de comunicaciones tales como DNS, DHCP, VoIP, videoconferencia y almacenamiento.

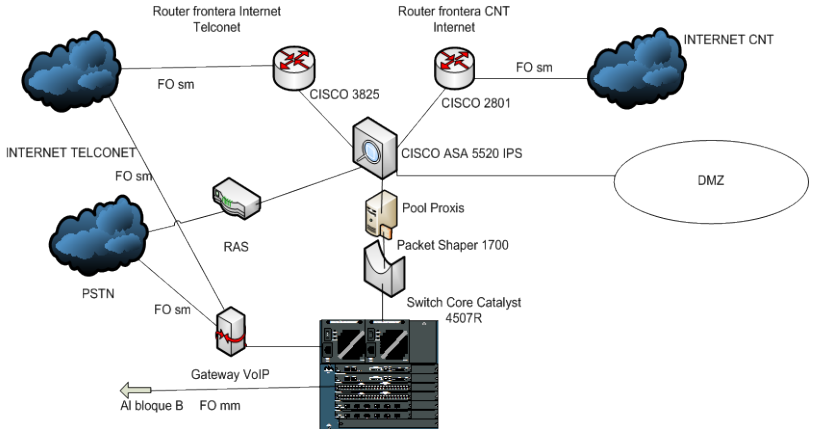

Figura 1. Infraestructura de acceso y seguridad.

El diseño jerárquico.- Permite poner en un orden cada módulo descrito anteriormente, de esta manera se definen funciones puntuales dentro de cada capa, permitiendo una mayor flexibilidad frente a las actualizaciones, detección de fallas y la escalabilidad. Se obtiene una mayor eficiencia en el diseño implementación, mantenimiento, administración y proyección de la red, la infraestructura se torna más confiable, ofreciendo una mejor relación costo/beneficio. Cada capa tiene funciones específicas asignadas.

La capa de núcleo.- En la red actual se dispone de un switch core marca Cisco, de la serie Catalyst 4507R ubicado en el MDF[1] del centro de cómputo, este equipo permite la conectividad del backbone de fibra óptica, que interconecta los switch de piso Cisco Catalyst 3750, los cuales están ubicados en los SDF[2]s del campus y se interconectan por fibra óptica a 1 Gbps.

La capa de distribución.- Provee el medio de comunicación entre la capa de acceso y el core. Las funciones de esta capa son proveer ruteo, filtrado, acceso a la red WAN, access-list, filtrado de paquetes, cola de espera, se implementa la seguridad y políticas de red.

La capa de acceso.- En esta capa se lleva a cabo la conmutación y ruteo estático exclusivamente, esta tarea se la hace mediante los switch Cisco 3750 distribuidos en los SDF tanto del bloque A, como del bloque B, participan 29 switches de piso, se ubican también los switch que conforman la capa de borde dado que también cumplen funciones de acceso. Los SDF's con sus respectivos switch proveen servicios a aproximadamente 500 usuarios.

B. Propuesta de implementación.-

Una vez que se ha realizado el levantamiento de estado inicial de la red del Campus Girón, se realizará la consiguiente propuesta de implementación del protocolo IPSec sobre la plataforma

[1] Estructura de distribución de señales (Main Distribution Frame)
[2] Cuartos de Distribución Secundarios de cableado

Jorge E López. georgelopez05@hotmail.com

IPv6.

Propuesta de direccionamiento.- En el Ecuador, quien está encargado de administrar las direcciones ipv6 es el consorcio CEDIA que identifica a la red de la Universidad Politécnica Salesiana, con el segmento 2800:68:0016::/483, para los proveedores se tiene la dirección 2800:2a0::/32 asignada a Telconet y la dirección 2800:370::/32, asignada a CNT[4].[5]

Requerimientos de infraestructura con IPv6.- Las plataformas operativas de los servidores tienen las funcionalidades IPv6 ya instaladas como estándar, por lo tanto incorpora IPSec.

Planificación de la implementación de IPv6.- Realizar una migración de IPv4 a IPv6 conlleva mucho trabajo y planificación cuidadosa, que incluyen un nuevo diseño de red y capacitación al personal que la administra, de esta manera se han identificado los siguientes lineamientos a tener en cuenta para la correcta implementación.[1]

Análisis de situación inicial.- La Universidad debe determinar con claridad las razones para adoptar el nuevo protocolo, incluidos los requerimientos del negocio, la implementación de IPv6 crea ventajas competitivas al incrementar la flexibilidad de los nuevos servicios.

Análisis de beneficios.- La UPS deberá hacer un análisis de los beneficios de la implementación de IPv6, uno de los factores clave es mantener la continuidad del negocio mientras se realiza el proceso de migración, esto está garantizado puesto que las implementaciones se las realizarán de acuerdo a un cronograma y por segmentos, la seguridad, operatividad y el rendimiento quedan garantizados, a nivel técnico el principal beneficio de este proyecto recae obviamente en el incremento sustancial de la seguridad.

Análisis de costos.- Todo cambio en la configuración de una red conlleva los costos asociados, en estos escenarios de migración se debe tener en cuenta las actualizaciones de hardware, software, aplicaciones y los costos operativos, en el caso de la Universidad, el impacto económico es relativamente muy bajo puesto que la inversión necesaria en lo referente a las actualizaciones de las aplicaciones para que sean compatibles con IPv6, las actualizaciones de los IOS en los router y en el switch core ya ha sido hechas, de acuerdo a un plan progresivo de migración de IPv4 a IPv6.

Análisis de riesgos.- Todo cambio en una red incluye un riesgo, el retorno de inversión no es inmediato, sin embargo se garantiza una ganancia. El riesgo más representativo es a nivel técnico, si bien es cierto la infraestructura actual de la red es totalmente compatible con IPv6, el proceso de implementación no estará exento de problemas de configuración al inicio, los que se deberán ir solucionando por parte de los administradores de la red.

Equipos de transición.- La organización deberá crear un equipo de personas dedicadas a la tarea de la migración, a este grupo deberán pertenecer los administradores de red, desarrolladores y técnicos, quienes estarán encabezados y bajo la autoridad del director del departamento de TI. Cada grupo de trabajo tendrá sus respectivas tareas de trabajo claramente definidas.

Planificación del piloto.- Cuando se introduce una nueva tecnología o un nuevo protocolo a una red en operación, es necesario primero hacer las pruebas preliminares en laboratorio, donde se puede controlar las variables y corregir los errores, para realizar este proceso se deberá realizar tareas como la identificación del plan de direccionamiento, el que permitirá identificar el rango de direcciones que se van a usar. El direccionamiento se ha planificado de acuerdo al bloque de direcciones asignado por LACNIC y CEDIA para la universidad. En cuanto a los mecanismos de transición, de acuerdo a la capacidad de coexistir IPv4 e IPv6,

[3] Fuente: http://ipv6.cedia.org.ec/index.php/asignaciones
[4] Fuente: http://ipv6.cedia.org.ec/index.php/la-realidad

durante el diseño se debe tomar en cuenta cuales serán los mecanismos a usar para migrar de protocolo, en el caso de la UPS, el escenario es IPv6 nativo, todos los host, servidores, equipos activos, servicios y aplicaciones trabajarán exclusivamente con este protocolo.

Seguridad.- Una organización debe destinar una gran cantidad de recursos para garantizar la seguridad de los datos, en este caso la investigación se centra exclusivamente en el protocolo IPSec.

C. Implementación de los túneles IPSec.

Se determinó con claridad cuáles serán las VLAN donde se implementará IPSec, tomando en cuenta la criticidad de la información que se tramita por las mencionadas VLAN, tomado la decisión de proteger las siguientes VLAN detalladas en la tabla 1:

VLAN	Nombre	Estado
1	Default	Activa
3	ADMINISTRATIVA	Activa
6	VoIP	Activa
11	INTERNET	Activa
12	IUS	Activa
13	SOL	Activa
14	INSPECTORIA-ADMINISTRATIVA	Activa
16	Abya-Yala	Activa
18	LNS	Activa
99	VLAN0099	Activa
112	Administrativosv2	Activa
114	VLAN-WLC	Activa
115	VLAN-WLC2	Activa
118	IDIOMAS	Activa
810	SERVIDORES-INTERNOS	Activa
820	SERVIDORES-PUBLICOS	Activa
830	SERVIDORES-PROXY	Activa

Tabla 1. VLAN a proteger con IPSec

En la figura 2, se muestra la topología lógica del Campus Girón, en rojo se ha indicado las VLAN a proteger. Adicionalmente se puede observar que también está protegido todo el segmento donde están situados los dispositivos encargados de la seguridad de la red.

Jorge E López. georgelopez05@hotmail.com

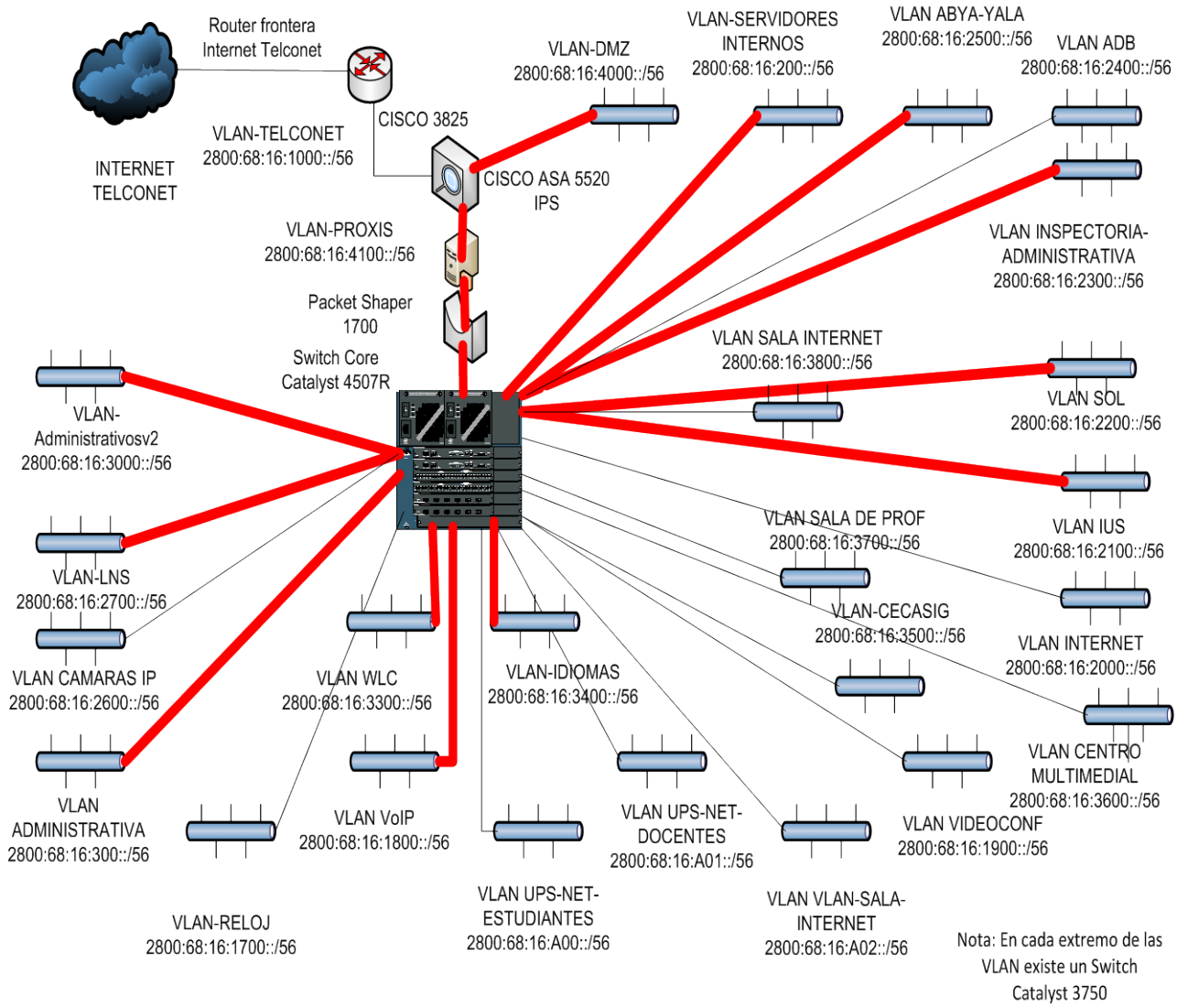

Figura 2. Diagrama de las VLAN a proteger con IPSec

Como se puede apreciar en la figura, se ha propuesto la implementación de los túneles IPSec entre el switch core y las respectivas VLAN seleccionadas de acuerdo a los criterios expuestos anteriormente, las mismas que están resaltadas en rojo, cabe destacar que no se han tomado en cuenta todas las VLAN del campus puesto que al implementar en todas ellas los túneles IPSec, daría como resultado una carga extra en el equipo del core.

D. Simulación de la implementación con IPSec.

Este proceso se lo realizará en una plataforma de simulación conocida como GNS3, se escogió esta aplicación puesto que permite obtener los datos muy cercanos a los reales, adicionalmente trabaja con los IOS de CISCO, por lo que las configuraciones, y los resultados serán los mismos que se los tendrían en el caso de trabajar con equipos reales. El IOS usado en la simulación es el c2691-advipservicesk9-mz.124-15.T6 implementado en el emulador del router Cisco 2691. [6]

En la figura 3 se muestra el diseño lógico a implementarse en la simulación.

Jorge E López. georgelopez05@hotmail.com

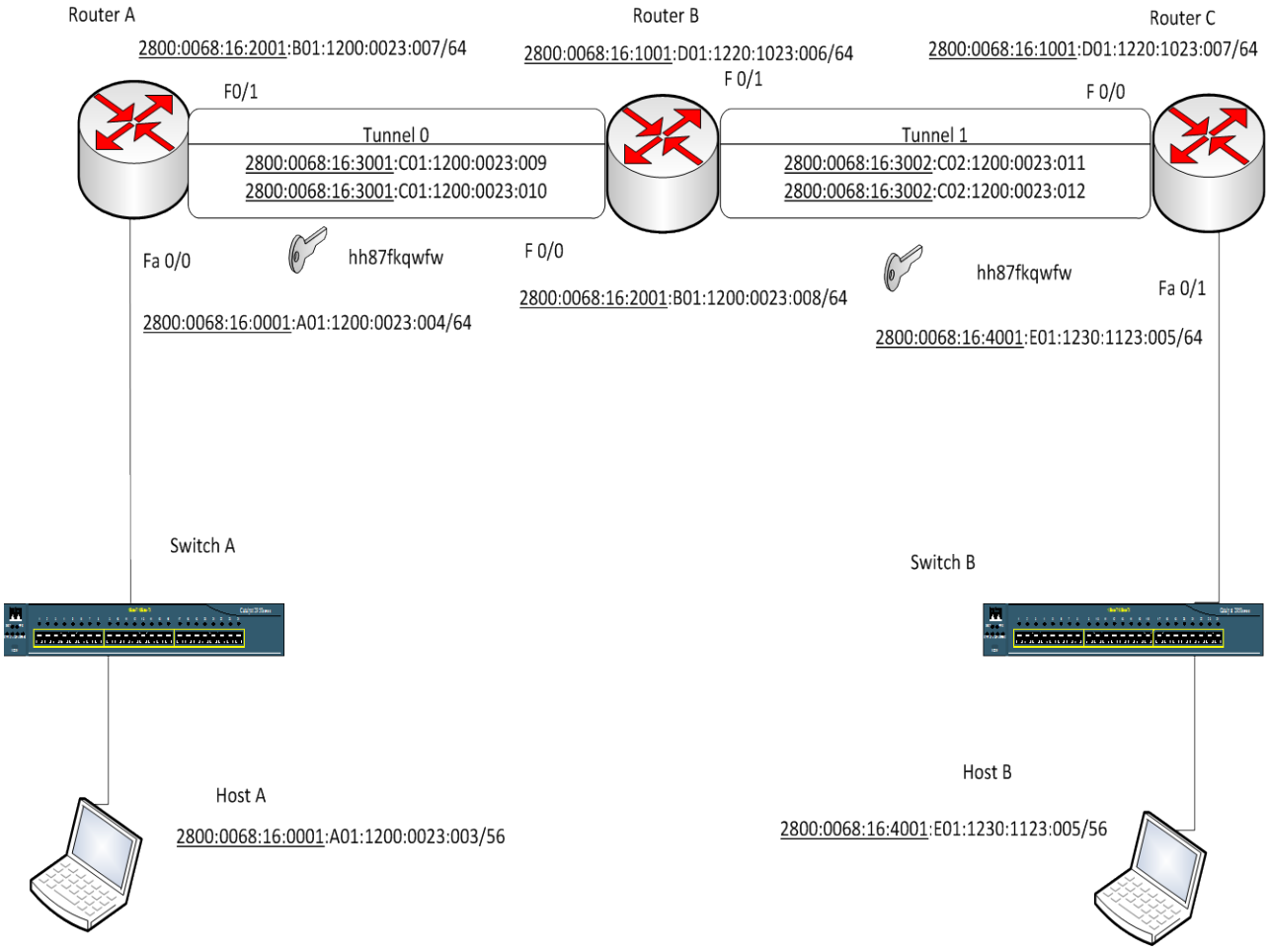

Figura 3. Diseño lógico implementado

Configuración. Para implementar IPSec, inicialmente se debe implementar los parámetros IKE, utilizados para validar las políticas entre pares, este protocolo define el método de intercambio de claves sobre ip en una la fase de negociación segura, los pares intercambian las políticas IPSec para la autenticación y la encriptación del tráfico de datos. IKE controla la autenticación, el algoritmo de encriptación y el método de intercambio de claves usado por las políticas para encriptar tráfico de datos enviado a través de un túnel VPN, este control se lo realiza en ambos extremos. Para permitir la negociación, en primer lugar hay que crear una política ISAKMP y configurar la asociación entre los pares que participan en esta política, en este punto se define la autenticación, los algoritmos de encriptación y la función hash utilizada para enviar tráfico de control entre los dos nodos de la VPN. La elección de un algoritmo de encriptación controlará la confidencialidad del canal de control entre los dos nodos, adicionalmente, el algoritmo hash controla la integridad de los datos. Para la autenticación de claves pre-compartidas, se usará encriptación 3DES y MD5 como algoritmo hash, además de diffie-hellman grupo 1 se usa para crear una clave secreta compartida por los pares para la política IKE. La SA tendrá un tiempo de vida de 86400 segundos, que es tiempo máximo en el que una política de seguridad se utiliza sin necesidad de negociarla de nuevo, esta configuración se debe aplicarla a los dos nodos.

El *IPSec transform-set* es un parámetro de configuración cifrada que negocian los routers para

formar las SA. IKE está formado por una cabecera de autenticación, se usara el modo túnel, razón por la cual se usará la cabecera ESP, se procederá a configurar el túnel IPSec, inicialmente se implementará una política IKE y una clave pre-compartida. La política será la misma en los dos extremos:

Catalyst_4507R

Catalyst_4507R (config)# crypto isakmp policy 1 //configuración de la política IKE con prioridad 1

Catalyst_4507R(config-isakmp-policy)# authentication pre-share //establece el modo de autenticación con clave precompartida

Catalyst_4507R(config-isakmp-policy)# hash MD5 //establece MD5 como algoritmo de hash para garantizar la integridad

Catalyst_4507R(config-isakmp-policy)# group 1 //especifica el identificador de grupo deDiffie-Hellman en la política IKE

Catalyst_4507R(config-isakmp-policy)# encryption 3DES //especifica 3DES como algoritmo de cifrado

Catalyst_4507R(config-isakmp-policy)# lifetime 86400 //especifica el tiempo de vida en segundos para la SA

Catalyst_4507R(config-isakmp-policy)# exit

Catalyst_4507R(config)# crypto isakmp key 0 cisco address ipv6 2800:0068:16:2001:B01:1200:0023:008/128 //define la clave precompartida, "hh87fkqwfw",en texto plano, "0", y la IP del que será el otro extremo del túnel 0

Catalyst_4507R(config)# crypto keyring ANILLO //define el nombre del keyring que se usará durante la autenticación

Catalyst_4507R(config-keyring)# pre-shared-key address ipv6 2800:0068:16:2001:B01:1200:0023:008/128 key chh87fkqwfw //define la clave precompartida a usar durante la autenticación IKE

Catalyst_4507R(config-keyring)# exit

Catalyst_4507R(config)# crypto ipsec transform-set TRANSFORMADA esp-3DES //define un transform-set, es decir, una combinación de protocolos y algoritmos que sea aceptable por routers IPSec

Catalyst_4507R(cfg-crypto-trans)# crypto ipsec profile PERFIL //define los parámetros que se van a usar para el cifrado IPSec entre los dos routers

Catalyst_4507R(ipsec-profile)# set transform-set TRANSFORMADA //especifica el transform-set que se puede usar

Catalyst_4507R(ipsec-profile)# exit

Catalyst_4507R(config)# interface tunnel 0 //configuración de la interfaz virtual tunnel 0

Catalyst_4507R(config-if)# ipv6 address 2800:0068:16:3001:C01:1200:0023:10/64

Catalyst_4507R(config-if)# ipv6 enable

Catalyst_4507R(config-if)# tunnel source 2800:0068:16:2001:B01:1200:0023:008 //define el origen del túnel

Catalyst_4507R(config-if)# tunnel destination 2800:0068:16:2001:B1:1200:23:007 //define el destino del túnel

Catalyst_4507R(config-if)# tunnel mode ipsec ipv6 //establece el modo de encapsulamiento para la interfaz tunnel 0

Catalyst_4507R(config-if)# tunnel protection ipsec profile PERFIL

//asocia la interfaz tunnel 0 con el perfil

Catalyst_4507R(config-if)# exit

Catalyst_4507R(config)# ipv6 route 2800:0068:16:4001:E01:1230:1123:005/64 tunnel 0 //configura una ruta estática de forma que todo el tráfico que vaya a la red local de la derecha pase por el túnel

Todos los nodos deben ser configurados de forma igual para que la conexión en el túnel se establezca, adicionalmente el nombre del transform-set debe ser el mismo dentro del comando ipsec profile.

III. Evaluación de resultados y discusión

Verificación de conectividad entre los Host. La conectividad se puede verificar haciendo un ping desde el host a al host b y viceversa, se obtuvo la siguiente salida

```
HostA#ping  2800:68:16:4001:E01:1230:1123:6
Type escape sequence to abort.
Sending 2500, 1500-byte ICMP Echos to 2800:68:16:4001:E01:1230:1123:6, timeout is 5 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (2500/2500), round-trip min/avg/max = 88/306/2176 ms
```

Como se puede observar, la conectividad está establecida y el porcentaje de paquetes transportados es del 100%, con una demora promedio de 306 ms, lo que significa que ningún paquete se perdió de extremo a extremo, a pesar que los mencionados paquetes fueron sometidos al proceso de encriptación. Las pruebas se han realizado con un tamaño de paquete igual a 1500 bytes y con un tiempo de vida de 5 s, valores que normalmente son los que se encuentran en una red real.

Comprobación de la configuración IPSec. Este proceso se lo realiza mediante el comando *show crypto IPSec sa*, que como resultado indica las direcciones de las interfaces de entrada y salida de los paquetes encriptados, indica el numero de paquetes encriptados y desencriptados, el número de

Jorge E López. georgelopez05@hotmail.com

errores durante la encriptación, el túnel virtual que está usando esa ruta, el identificador de la cabecera esp y de la sa, el identificador del crypto-map, el algoritmo de cifrado así como el tiempo de vida de la clave de encriptación, entre los parámetros más importantes.

```
Catalyst_4507R#show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 2800:68:16:2001:B01:1200:23:8
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2800:68:16:2001:B01:1200:23:7 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 36023, #pkts decrypt: 36023, #pkts verify: 36023
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 2800:68:16:2001:B01:1200:23:8,
     remote crypto endpt.: 2800:68:16:2001:B01:1200:23:7
     path mtu 1514, ip mtu 1514, ip mtu idb Tunnel0
     current outbound spi: 0xA299BCF3(2727984371)
     inbound esp sas:
      spi: 0xE8A19F25(3902906149)
        transform: esp-3DES ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4576641/542)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVA
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xA299BCF3(2727984371)
        transform: esp-3DES ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4584845/534)
```

IV. Trabajos relacionados

Scott Hogg en su trabajo IPv6 Security [2], da los lineamientos para el diseño e implementación de las seguridades en una red empresarial, estos lineamientos se tomaron como referencia para la propuesta de implementación de la presente investigación, con la diferencia que se tuvo que acoplar a la realidad de la red bajo estudio.

Erick Luján, en su tesis titulada Seguridad en IP con el protocolo IPSec para IPv6 [3] determina la arquitectura del protocolo IPSec para ipv6 orientado a entornos de internet, en la presente investigación , se realiza el análisis de la arquitectura del protocolo para redes LAN.

McFarlan, Sambi y Nikihil en su trabajo denominado IPv6 for enterprise Networks [4] especifican claramente los lineamientos a seguir durante el diseño de red jerárquico y la planificación de la implementación de una red LAN en entornos IPv6, sin embargo el documento no contempla el diseño modular, tema que si es analizado en la propuesta de implementación para la UPS.

V. Conclusiones y trabajo futuro

La investigación demostró la factibilidad de la implementación del protocolo IPSec en un entorno nativo IPv6 dentro de un escenario LAN, como en el caso del Campus Girón de la Universidad Politécnica Salesiana, de acuerdo a la información levantada del estado inicial, se pudo determinar

que la infraestructura de red y servidores es totalmente compatible con IPv6 y por lo tanto con IPSec. En base a los resultados del análisis de la arquitectura IPSec, claramente se ha determinado que al trabajar a nivel de red, es transparente ante las aplicaciones, las que generalmente son el objeto de los ataques, esto conlleva a que la red aumentará su nivel de protección puesto que el protocolo de seguridad se propone ser implementado en los routers y switch de capa 3, esta seguridad se aplica a todo el tráfico que cruza por estos dispositivos, esto permite ofrecer seguridad individual de un extremo a otro al asegurar las subredes virtuales, adicionalmente en el caso de una futura implementación, las mencionadas aplicaciones no se verán alteradas de ninguna manera, puesto que IPSec soporta todos los tipos de servicios IP.

De acuerdo a lo obtenido en la simulación y en las pruebas respectivas, se valida la factibilidad de la implementación del protocolo en mención, puesto que los resultados mostraron que en el escenario propuesto se determina claramente que los paquetes cursados se encriptan y encapsulan correctamente sin desmedro apreciable del rendimiento, adicionalmente de evidencia que tienen menos porcentaje de paquetes perdidos cuando pasan por el túnel IPSec, dando como resultado que en una implementación en el escenario real significará que la información es transferida en forma íntegra y segura.

A futuro se propone la realización de propuestas de implementación de portales cautivos y servicios AAA, esto con el fin de solidificar el escenario de seguridad que deberá ser implementado. Es imperativo que se realice el respectivo proceso de capacitación orientado al equipo de técnicos quienes estarán a cargo de la implementación de esta propuesta, en especial al administrador de red de la Institución puesto que será la persona encargada de gestionar este proceso

Agradecimientos

A todos quienes colaboraron de una u otra manera con el desarrollo de esta investigación.

Referencias Bibliográficas

[1]Cisco Systems.(2007). Implementing IPSec in IPv6 Security. [en línea],US: CISCO Systems Inc. Disponible en:
http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-ipsec_xe.pdf [Marzo 25, 2011]

[2]Hogg Scott.(2009). IPv6 Security. Indianápolis: Cisco Systems, Inc. Published by Cisco Press. ISBN-13: 978-1-58705-594-2.

[3]Luján Montes Erick Fernando (2005). Seguridad en IP con el protocolo IPSec para ipv6. Tesis de Ingeniería en Ciencias y Sistemas. Universidad San Carlos de Guatemala. Guatemala.

[4]McFarlan Shannon., Sambi Muninder., Sharma Nikihil., Hooda Sanjay.(2011). IPv6 for enterprise Networks, US. Cisco Systems, Inc. Published by Cisco Press. ISBN-10: 1-58714-227-9.

[5]Moreno Constante Alex Alfonso, Valencia Falcón Cristian Alejandro.(2012). Implementación de un Plan Piloto para la interconexión de IPv6 sobre IPv4, utilizando el Protocolo Dual Stack en la Universidad Politécnica Salesiana Campus Sur dentro de la subred CIMA (Centro de Investigación en Modelación Ambiental) con la frontera del proveedor Telconet. Tesis de Ingeniería en sistemas. Universidad Politécnica Salesiana. Quito

[6]Teare Diane. Implementing Cisco IProute. (2010). Indianapolis, Cisco Systems, Inc. Cisco Press.

Jorge E López. georgelopez05@hotmail.com