Herramienta de Gestión de Red para la monitorización y control de seguridad de nodos de red con agentes SNMP en la detección de intrusiones de red

Dr. Abraham Jorge Jiménez Alfaro[1], Mtro. Edgar Corona Organiche[2],
Dra. Griselda Cortés Barrera[3], Dra. Mercedes Flores Flores[4]

Resumen

En este artículo se presenta la arquitectura de una herramienta de gestión de red para el control y monitorización necesarios para detectar de manera efectiva intrusiones de red. La intrusión, es cualquier conjunto de acciones

Acerca de los autores

[1, 2, 3 y 4] Docente del Posgrado de Ingeniería en Sistemas Computacionales del Tecnológico Nacional de México / Tecnológico de Estudios Superiores de Ecatepec.

que tratan de comprometer la integridad, confidencialidad o disponibilidad de un recurso de red. La detección de intrusos es la capacidad de detectar ataques en una red, incluyendo dispositivos y computadores. La herramienta permite ejecutar tareas distribuidas sobre diferentes nodos de la red, lo cual requiere repetidas acciones de recogida de datos, configuración y análisis cada vez que sucede un nuevo evento y mantener la funcionalidad de la misma; para ello, se emplean agentes del Protocolo de Administración Simple de Red (SNMP, por sus siglas en inglés) y el acceso a la base de datos jerárquica de variables de Información Gestionada del dispositivo (MIB, por sus siglas en inglés).

Palabras Clave: *Arquitectura de Gestión, Intrusiones de Red, Agentes SNMP, Base de Información Gestionada MIB.*

Abstract

This article presents the architecture of a network management tool for the control and monitoring necessary to effectively detect network intrusions. The intrusion is any set of actions that try to compromise the integrity, confidentiality or availability of a network resource. Intrusion detection is the ability to detect attacks on a network, including devices and computers. The tool allows distributed tasks to be executed on different nodes of the network, which requires repeated data collection, configuration and analysis actions each time a new event occurs and to maintain its functionality; to do this, Simple Network Management Protocol (SNMP) agents and access to the hierarchical database of Managed Device Information (MIB) variables are used.

Keywords: *Management Architecture, Network Intrusions, SNMP Agents, MIB Managed Information Base.*

Introducción

La información de configuración describe la naturaleza y estado de los recursos (tanto físicos como lógicos) que forman la red. Esta información incluye una especificación del recurso y de los atributos de ese recurso (por ejemplo: nombre, dirección, número de identificación, estados, características operacionales, versión del software, entre otros). Esta información (en realidad, toda la información de gestión) se puede estructurar de diversas formas desde los agentes SNMP y una base a objetos o variables de red (Stallings, 2015).

La tarea de aprendizaje de un detector de intrusiones, consiste en construir un modelo de predicción (un clasificador) capaz de distinguir entre la conexiones malignas, llamadas intrusiones o ataques, y conexiones normales.

El emplear agentes SNMP hace posible que la información sea accesible por agentes de administración y agentes clientes asociadas a los nodos o dispositivos a gestionar. Esta función permite al administrador especificar el rango y el tipo de valores que puede tomar un determinado atributo de un agente, el rango puede ser una lista de todos los valores posibles o los valores superior e inferior permitidos, así como modificar los objetos o variables del dispositivo de red. Para accesar a estos objetos o variables on-line, en línea, se deben crear los correspondientes agentes de administración y clientes, empleando el protocolo de administración simple de red (SNMP). Una vez modificadas las variables, es necesario inicializar el dispositivo o nodo para que se incorporen los nuevos parámetros de configuración, lo cual permite restablecer configuraciones de seguridad en casos de intrusiones de red.

Materiales y Métodos

I.- Arquitectura de Gestión de Red

La gestión de red (Stallings, 2017) es el conjunto de tareas de monitorización, configuración, información y control, necesarias para operar de manera efectiva una red. Dichas tareas pueden estar distribuidas sobre diferentes nodos de la red, lo cual puede requerir repetidas acciones de recogida de datos y su análisis, cada vez que sucede un nuevo evento en la red.

Una conexión es una secuencia de paquetes TCP, Protocolo de Control de Transmisión (Transmission Control Protocol, por su nombre en inglés) con un inicio y final bien definidos, como flujos de datos entre dos direcciones IP, Protocolo de Internet (Inernet Protocol, por su nombre en inglés). Todas las conexiones se etiquetan como normales o como un tipo específico de ataque. Cada conexión consta de unos 100 bytes.

Las redes son cada vez más importantes en empresas y organizaciones, tomando en consideración: la tendencia a redes más grandes, más complejas, más heterogéneas; la red y las aplicaciones distribuidas se hacen imprescindibles; los costos de gestión de la red aumentan; la gestión de la red no se puede hacer a mano, se requieren herramientas de gestión de red automatizadas. Para cumplir estas premisas, las funciones de la arquitectura funcional se agrupan en dos categorías:

Monitorización, Funciones de “lectura”:

- Observar y analizar el estado y comportamiento de la configuración de red y sus componentes.
- Abarca: prestaciones, fallos y costos.

Control, Funciones de “escritura”:

- Alterar parámetros de los componentes de la red.
- Abarca: configuración y seguridad.

Así también, cumple tres objetivos fundamentales:

- **Identificación de la información**: identificar la información a monitorizar.
- **Diseño de mecanismos de monitorización**: cómo obtener esa información.
- **Utilización de la información**: para qué utilizar la información obtenida dentro de las distintas áreas funcionales de gestión de red.

La información Estática es generada y almacenada por el propio elemento de red (por ejemplo, un ruteador almacena su propia configuración).

La información Dinámica puede almacenarla el propio elemento, u otro encargado de ello (por ejemplo, en una red de área local (LAN) cada elemento puede almacenar el número total de paquetes que envía, o un elemento de la LAN puede estar escuchando y recoger esa información.

La información Estadística se genera por cualquier elemento que tenga acceso a la información dinámica con base en dos opciones básicas:

1.- Puede enviarse toda la información dinámica al gestor de red para que realice las estadísticas.

2.- Si el gestor no necesita toda la información, ésta puede ser resumida por el propio elemento antes de enviarla al gestor, ahorrando procesamiento en el gestor y generando menos tráfico en la red.

La arquitectura considera los siguientes elementos en la seguridad de la información:

1.- **Ataques a la seguridad:** Qué acciones pueden comprometer la seguridad de la información que pertenece a una organización.

2.- **Mecanismos de seguridad:** Qué mecanismos hay que implementar para detectar, prevenir o recuperarse de un ataque a la seguridad de la información.

3.- **Servicios de seguridad:** Qué servicios ofrecer al usuario respecto a la transferencia de información en una red de datos. Los servicios de seguridad tratan de contrarrestar los ataques y para ello hacen uso de los mecanismos de seguridad para proporcionar ese servicio.

Los módulos de la arquitectura de gestión de red se estructuran en cuatro configuraciones:

1.- La estación que ejecuta la aplicación de monitorización y control, es también un elemento de la red, y debe gestionarse. Por ello se incluye el Agente y los Objetos de Administración, véase Figura 1.

Figura 1

Estación como elemento de red.

2.- Configuración normal de monitorización y control de otros elementos de red. El gestor y los agentes deben compartir el mismo protocolo de gestión y sintaxis y semántica de la MIB, véase Figura 2.

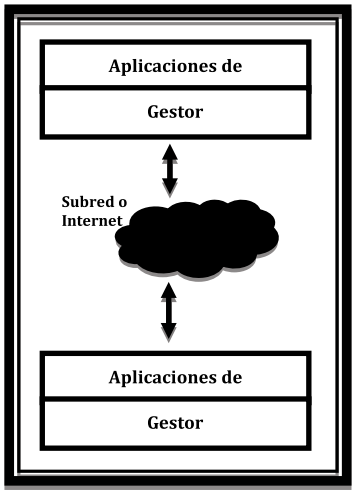

Figura 2

Configuración de otros elementos de la red.

3.- Configuración con agentes que monitorizan el tráfico de una red, monitores remotos o monitores externos, véase Figura 3.

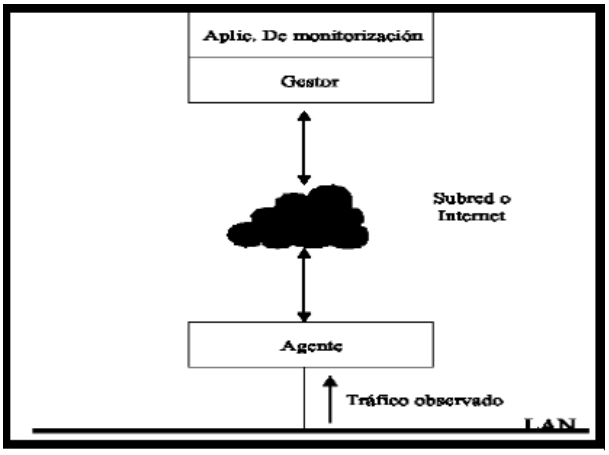

Figura 3

Monitores remotos.

4.- Cuando existen elementos que no usan el mismo protocolo de gestión que el gestor, se utilizan proxies, véase Figura 4.

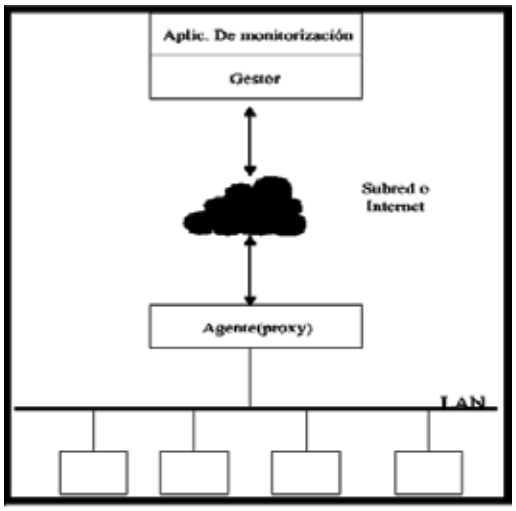

Figura 4

Proxies.

Estas configuraciones dan lugar a la comunicación y control, enviando comandos a los agentes SNMP y recibiendo respuestas; de esta forma, la arquitectura de gestión permite la monitorización y control de los nodos de la red.

La arquitectura de gestión utiliza el concepto de capas o layers, considerando:

1.- Servicio de Seguridad (N): Es la capacidad que el nivel *N* y de los niveles inferiores ofrecen a las entidades de nivel N+1 en el campo de la seguridad en el interfaz entre el nivel N y el nivel N+1 por medio de las primitivas de servicio.

2.- Función de seguridad (N): Es una función relativa a la seguridad de acuerdo al servicio proporcionado al nivel *N*, controlado por el control lógico de la entidad (N).

3.- Mecanismo de seguridad (N): Mecanismo de nivel *N* que realiza una parte de una función de seguridad de nivel *N*.

Los servicios de seguridad definidos son autenticación de entidad par, control de acceso, confidencialidad de datos, integridad de datos, no repudio (con prueba de origen, con prueba de entrega). Para proporcionar estos servicios de seguridad, es necesario incorporar en niveles apropiados SNMP y MIB (cifrado, firma digital, mecanismos de control de acceso, integridad de datos, intercambio de autenticación, entre otros).

En la arquitectura de gestión de Red una entidad de nivel *N* se compone de tres partes:

1.- **Control Lógico:** Realiza la lógica del protocolo usando funciones y variables.

2.- **Mecanismos:** Controlados por el elemento de control opera con la variables realizando funciones.

3.- **Variables:** La mayoría de las cuales son locales a cada entidad.

El control lógico puede ser modelado como una máquina de estado finita extendida por SNMP. Los mecanismos se pueden, a su vez, dividir en tres grupos cada uno, realizando su misión en un interfaz del nivel *N*:

1.- **Mecanismos de Interfaz de Nivel Superior:** Realizados en el interfaz entre el nivel N+1 y el nivel N.

2.- **Mecanismos de Interfaz de Nivel Inferior:** Realizados en el interfaz entre el nivel N y el nivel N-1.

3.- **Mecanismos de Protocolo**: Consiste en el diálogo entre entidades pares.

La arquitectura de la herramienta de gestión SNMP y MIB con la entidad par de un nivel (*N*) así como su interrelación con el entorno, se muestra en la Figura 5:

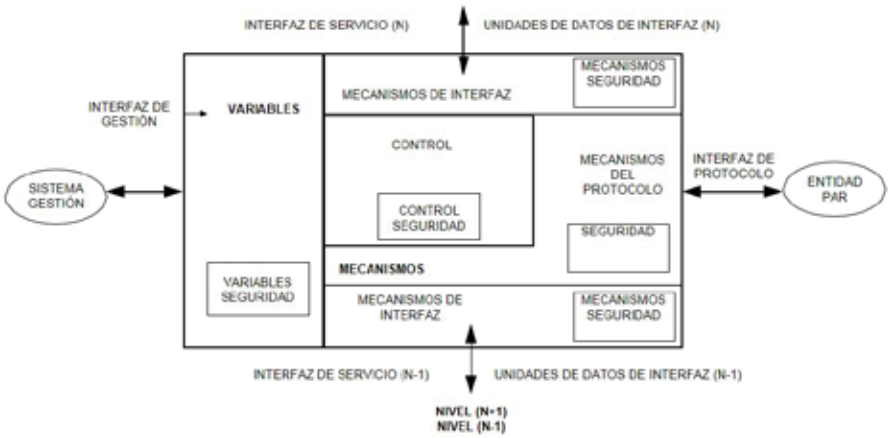

Figura 5

Arquitectura Gestión de Red para la monitorización y control de seguridad de nodos de red con agentes SNMP en la detección de intrusiones de red.

II.- Arquitectura y Agentes

Los entornos de red, sus configuraciones y funcionamiento, forman parte de la gestión de red; algunos de los elementos en los que se hace hincapié de forma determinante en la configuración y el monitoreo, son las variables que residen en la base de datos de los dispositivos que interviene en la red (Stallings, 2015). El protocolo de administración de red simple (SNMP), permite el acceso a las bases de datos del dispositivo y modificar parámetros asociados a las mismas, con lo que los cambios se reflejan de manera inmediata. SNMP es un protocolo que permite la gestión de los recursos que están disponibles en una red. Dentro de un entorno de red gestionado con SNMP habrá un conjunto de nodos de la red que se encarguen de la gestión y un conjunto de componentes de la misma (hosts, concentradores, ruteadores, modems, entre otros.) que podrán ser gestionados por estas estaciones, así como la base de datos donde se encuentra toda la información que se gestiona. Esta base de datos se denomina MIB (Management Information Base).

Para la arquitectura funcional de monitorización, se consideran los siguientes elementos para su implementación:

- Agente de gestión
- Gestor
- Objeto gestionado
- Protocolo de gestión

El agente de gestión se encarga de supervisar un elemento de la red. Se comunica con el gestor para atender sus peticiones y para informarle de eventos acaecidos en el objeto gestionado. El agente de gestión suele residir físicamente en el elemento gestionado.

El gestor es un software residente en una estación de gestión que se comunica con los agentes y que ofrece al usuario una interfaz a través de la cual comunicarse con los agentes de gestión.

Los objetos gestionados son las abstracciones de los elementos físicos de la red que se gestionan (tarjeta de red, concentrador, módem, ruteador, etcétera). Se pueden manejar los atributos y las operaciones que se pueden realizar sobre el objeto. De la misma forma, las notificaciones que dicho objeto puede generar así como las relaciones con otros objetos, también son susceptibles de ser controladas. La base de datos de gestión (MIB) previamente mencionada está formada por todos los objetos gestionados.

Protocolo de gestión es el que especifica cómo se realizará la comunicación entre los agentes de gestión y el gestor. En nuestro caso, este protocolo es el SNMP. La comunicación se realiza con base en requerimientos, respuestas y notificaciones, véase Figura. 6.

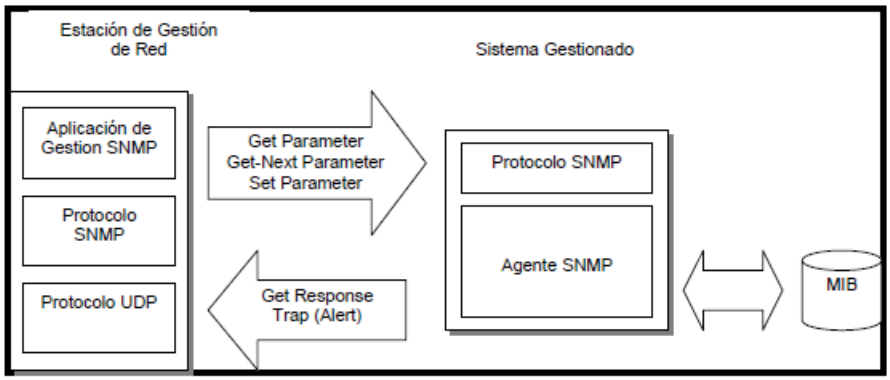

Figura 6

Elementos de gestión de la arquitectura de Gestión de Red.

Los mensajes SNMP implementados son:

1.- **Get Request**: Para leer el valor de una o varias variables del MIB.
2.- **Get Next Request**: Para realizar lecturas secuenciales a través del MIB.
3.- **Get Response**: Es el mensaje de respuesta a un Set Request, Get Request o Get Next Request.
4.- **Set Request**: Mensaje enviado para establecer el valor de una variable.
5.- **Trap**: A través de este mensaje se hacen notificaciones de eventos.

Estos cinco tipos de mensajes SNMP son encapsulados en datagramas UDP. Los mensajes de petición y respuesta son enviados al puerto 161, mientras que las notificaciones de eventos usan el puerto 162.

El MIB se organiza en forma de árbol. Cada nodo del árbol tiene asociado un número entero y una etiqueta de texto. Un nodo se identifica unívocamente con una secuencia de números enteros, que identifican los nodos a través de los cuales hay que pasar para llegar desde la raíz al nodo de interés. El siguiente gráfico muestra parte del árbol definido por ISO (International Standards Organization), véase Figura 7.

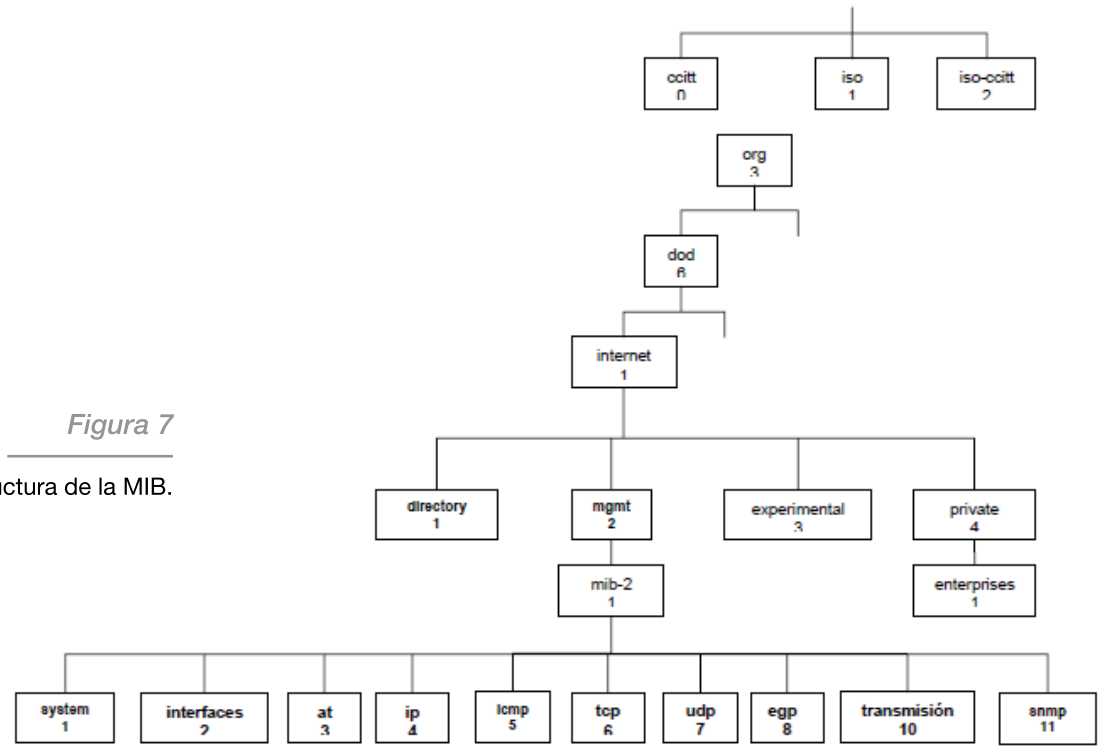

Figura 7

Estructura de la MIB.

Con estos elementos, se implementan los gestores y agentes de la arquitectura, que permitirán gestionar un nodo de red, véase Figura 8.

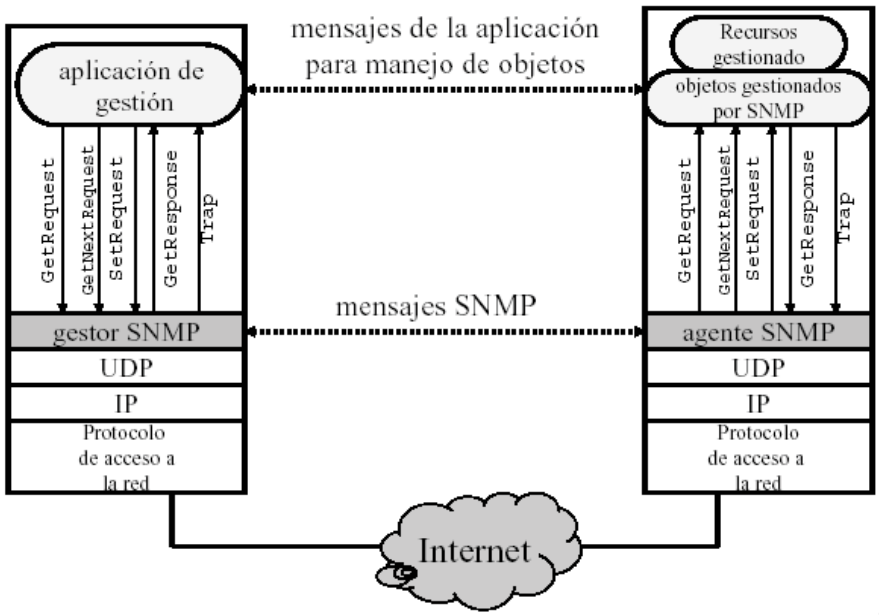

Figura 8

Elementos gestionados por la arquitectura con gestor y agente SNMP.

El **agente de gestión** se encarga de supervisar un elemento de la red. Se comunica con el sistema gestor para atender las peticiones e informarle de eventos sucedidos en el objeto gestionado; dicho agente de gestión es parte del dispositivo; el **gestor** es el software residente en una estación de gestión que se comunica con los agentes y que ofrece al usuario una interfaz a través de la cual comunicarse con los elementos de gestión para obtener información de los recursos gestionados. Además recibe las notificaciones enviadas por los agentes, éste componente se programa y forma parte de del programa de configuración; los **objetos gestionados** son las abstracciones de los elementos físicos de la red que se gestionan (tarjeta de red, concentrador, módem, ruteador, entre otros.). Se pueden manejar los atributos y las operaciones realizables sobre el objeto. De la misma forma, las notificaciones que dicho objeto puede generar así como las relaciones con otros de la red, también son susceptibles de ser controladas. La base de datos de gestión (**MIB**) previamente mencionada, está formada por todos los objetos gestionados, y es parte del dispositivo gestionado. Finalmente, el **protocolo de gestión, SNMP**, específica cómo se realiza la comunicación entre los agentes de gestión y el gestor.

Resultados

Para implementar la arquitectura de gestión, se realizó un software modular, que funciona en ambientes Windows y Linux, el cual permite accesar a las primitivas funciones de monitorización, control y configuración asociadas al protocolo SNMP, véase Figura 9.

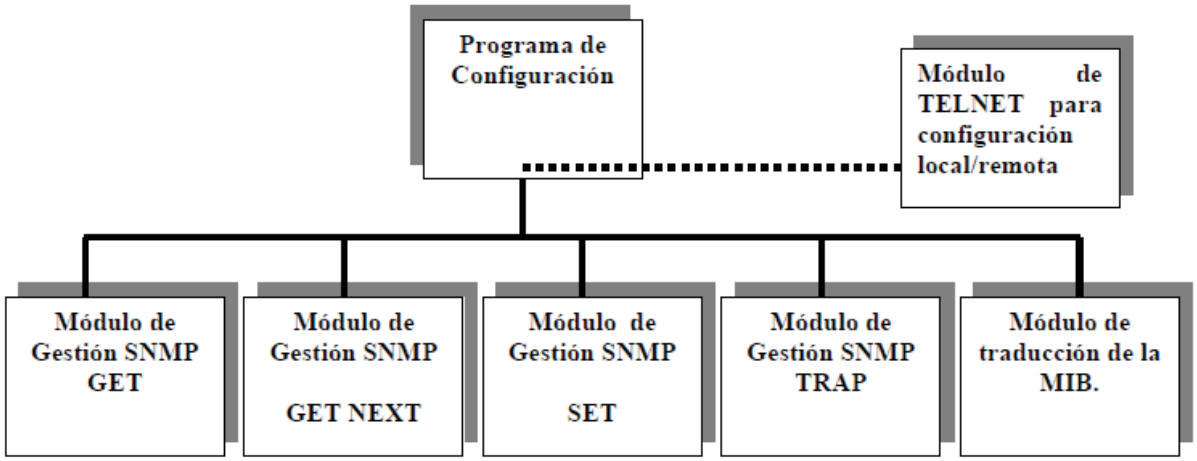

Figura 9

Estructura modular para implementar la arquitectura de gestión de red por SNMP.

Formalmente, una entidad de nivel ***N*** en un sistema ***A***, A_N, puede ser modelada como una tripleta: (C_A, V_A, M_A),donde $\mathbf{C}_A$ es el Control lógico, $\mathbf{M}_A$ es el Conjunto de Mecanismo y $\mathbf{V}_A$ el conjunto de Variables.

El conjunto de variables de la entidad A_N es la unión del conjunto de variables de protocolo de la entidad A_N y el conjunto de *variables de seguridad* de la entidad A_N

$$V_{A_N} = V_{A_N,P} \bigcup V_{A_N,S}$$

Similarmente, el conjunto de mecanismos de la entidad A_N es la unión del conjunto de mecanismos de protocolo, el conjunto de mecanismos de interfaz, el conjunto de mecanismos de seguridad y el conjunto de otros mecanismos:

$$M_{A_N} = M_{A_N,P} \cup M_{A_N,I}, M_{A_N,S} \cup M_{A_N,O}$$

Las variables de seguridad incluyen claves e información que controla la selección y uso de varios mecanismos de seguridad. Los valores de las variables de seguridad pueden ser establecidas por el gestor del sistema, o pueden ser resultado de la negociación con un nivel superior, o como parte de control de la entidad.

Un contexto de seguridad de nivel ***N*** entre instancias de dos Sistemas A y B, $A_{N,i}$ y $B_{N,j}$ se puede definir formalmente como:

$$SC_{A_{Ni},B_{Nj}} = (V_{A_{Ni},S}, V_{B_{Nj},S}) \cup (M_{A_{Ni},S}, M_{B_{Nj},S})$$

El uso de un contexto de seguridad en la red implica conocer los mecanismos criptográficos empleados, claves usadas, funciones de seguridad requeridas, entre otros. El contexto de seguridad puede ser establecido por medio de un acuerdo previo, gestión y negociación. Es posible negociar varios contextos de seguridad y manejarlos del mismo modo que son manejados los contextos de presentación en el nivel de presentación con las primitivas SNMP.

Las funciones de seguridad pueden ser autónomas (es decir, estar siempre activas o con posibilidad de ser activadas por los sistemas de gestión guiados por una política de seguridad), o bien pueden ser activadas en un momento dado, significando en este caso que su uso es negociado y controlado por el usuario final mediante la invocación de primitivas, ver Figura 10.

```
% snmptranslate system.sysUpTime.0
.1.3.6.1.2.1.1.3.0

% snmptranslate -Td -Ib 'sys.*ime'
.1.3.6.1.2.1.1.3
sysUpTime OBJECT-TYPE
  -- FROM SNMPv2-MIB, RFC1213-MIB
  SYNTAX TimeTicks
  MAX-ACCESS     read-only
  STATUS current
  DESCRIPTION    "The time (in hundredths of a second) since the
network
           management portion of the system was last re-
initialized."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(1)
3 }

% snmptranslate -Tp system
+--system(1)
   |
   +-- -R-- String    sysDescr(1)
   |        Textual Convention: DisplayString
   +-- -R-- ObjID     sysObjectID(2)
   +-- -R-- TimeTicks sysUpTime(3)
   +-- -RW- String    sysContact(4)
   |        Textual Convention: DisplayString
   +-- -RW- String    sysName(5)
   |        Textual Convention: DisplayString
   +-- -RW- String    sysLocation(6)
   |        Textual Convention: DisplayString
   +-- -R-- Integer   sysServices(7)
   +-- -R-- TimeTicks sysORLastChange(8)
   |        Textual Convention: TimeStamp
   |
   +--sysORTable(9)
      |
      +--sysOREntry(1)
         |
```

Figura 10

SNMP TRANSLATE.

Una de las claves de la flexibilidad de la arquitectura de gestión, es el empleo de SNMP y el uso de “variables” como forma de representación de los recursos, tanto físicos como lógicos, en los sistemas gestionados. En cada nodo gestionado, el agente SNMP proporciona una base de datos llamada MIB (Management Information Base), que contiene objetos de datos, más conocidos como variables MIB. La monitorización del nodo la lleva a cabo la estación gestora, la cual periódicamente lee los valores de estas variables. El control del nodo se realiza mediante el cambio de los valores de las variables. Adicionalmente, existe una operación *trap* para permitir al nodo gestionado informar a una estación gestora sobre determinadas condiciones o eventos inusuales, véase Figura 11.

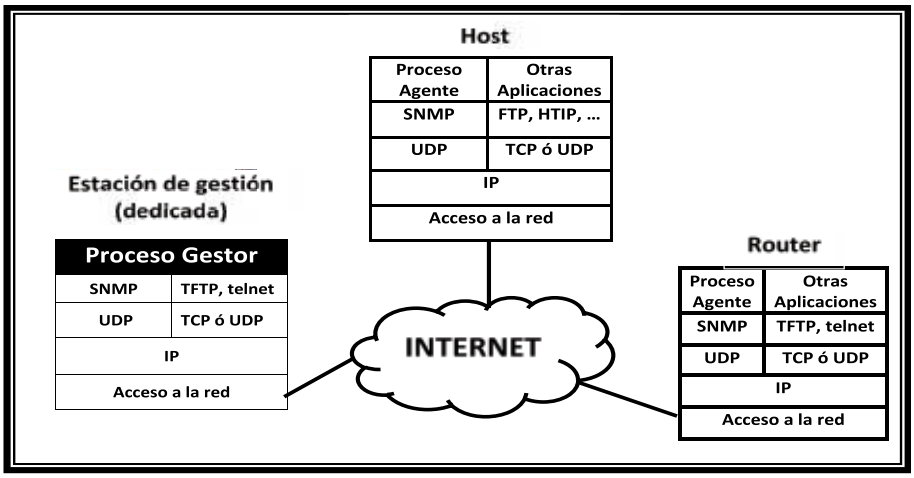

Figura 11

Modelo de configuración estación gestora y sistemas gestionados.

Conclusiones

La implantación de servicios de seguridad en el nivel de red, permite que a las entidades finales se las pueda ofrecer un servicio de seguridad, independientemente de la tecnología de las distintas redes que separan a las entidades pares. Los servicios de seguridad a través de SNMP son a este nivel: confidencialidad orientada y no orientada a conexión, confidencialidad aplicada al análisis de tráfico, integridad (orientada a conexión sin recuperación y no orientada a conexión), autenticación de entidades pares y de origen de datos y control de acceso.

Los servicios de seguridad proporcionados en el subnivel IP, puede ser empleados para brindar seguridad entre un sistema final y un sistema intermedio (por ejemplo un encaminador). El ofrecer servicios de seguridad en sistemas intermedios, puede tener algunas ventajas. En muchas topologías de red, un sistema intermedio a menudo actúa como elemento de interconexión entre una red de área local o una red de área amplia y una red de entre una entidad administrativa “local” y otras entidades administrativas. Proporcionar servicios de seguridad en el elemento intermedio, es especialmente atractivo desde la perspectiva de la gestión de red cuando se quiere que un grupo de sistemas se vean afectados en vez de todos los sistemas finales.

A partir del análisis realizado de la arquitectura de gestión, se determina que es producto de dos grandes vertientes de la gestión de redes: la monitorización y el control. Se incorpora la monitorización para las funciones de lectura con lo que permite observar, analizar el estado y el comportamiento de la configuración de red y sus componentes. En lo correspondiente al control, tiene como objeto las funciones de escritura, con lo que permite alterar parámetros de los componentes de la red.

Con estos tipos de información cubre los objetivos de: a) Identificación del nodo a configurar; b) mecanismos de monitorización y control para obtener la información y c) seguridad de la red obtenida dentro de las distintas áreas funcionales de gestión de red. Para probar la arquitectura, se desarrolló un software modular que permite implementar estas categorías, por lo que es posible monitorizar y controlar las intrusiones de red en:

1.- **Recursos de comunicación**: dispositivos de Redes de área local y amplia (LANs, WANs).

2.- **Hardware de computación**: Servidores, estaciones de trabajo, dispositivos de conectividad tales como ruteadores, conmutadores, concentradores, entre otros.

La información que se proporciona, es recogida y supeditada a las necesidades de la organización. Algunos ejemplos de la información que se maneja, son: **a) Identificación de usuario; b) Emisor-Receptor; c) Número de Paquetes, y d) Inicio y fin de un proceso de transmisión; protocolos asociados a la capa de transporte del modelo TCP/IP, y otros.**

Los resultados obtenidos muestran que es posible monitorear cualquier dispositivo de conectividad que esté en la red y acceder a la configuración correspondiente.

Los módulos del software modular se programaron en C/C++ para facilitar su portabilidad, ya que de manera indistinta se emplearon los ambientes Windows y LINUX. Los servicios de seguridad definidos en la arquitectura de gestión que se pueden ofrecer en el nivel de red, son:

1.- Autenticación de entidad par: Puede ser implementado con los mecanismos de intercambio de autenticación o de firma digital.

2.- Autenticación de datos de origen: Puede ser implementado con los mecanismos de encriptación o de firma digital.

3.- Servicio de control de acceso: Proporciona los mecanismos adecuados de control de acceso. El control de acceso permite a los sistemas finales, controlar el establecimiento de conexiones de red y rechazar llamadas no deseadas. También permite que una o más subredes controlen el uso del recurso de nivel de red.

4.- Confidencialidad orientada a conexión: Puede ser implementado con los mecanismos de encriptación y control de encaminamiento.

5.- Confidencialidad aplicada al control de tráfico: Puede ser implementado con un mecanismo de tráfico de relleno, en conjunción con un servicio de confidencialidad en capas inferiores al nivel de red y con mecanismos de control de encaminamiento.

6.- Integridad orientada a conexión sin recuperación: Puede ser implementado con un mecanismo de integridad de datos, algunas veces en conexión con un mecanismo de encriptado.

7.- Integridad no orientada a conexión: Puede ser implementado con un mecanismo de integridad de datos, algunas veces en conexión con un mecanismo de encriptado.

Referencias

Comer, D. (2000). *Internetworking With TCP/IP.* Prentice Hall: Englewood Cliffs, NJ.

Craig H. (2003). *Networking Personal Computers, whit TCP/IP.* O'Relly Associates, Inc. Sebastopol, CA.

Huitema, C. (2001). *Routing in the Internet*. Prentice Hall: Englewood Cliffs, NJ.

Kirch, O. (2001). *The Linux Network Administrators Guide*.

Liu, C. (2000). *Managing Internet Information Services*. O'Relly Associates, Inc. Sebastopol, CA.

Liu, Cricket, *et al*. (2000). *Managing Internet Information Services*. O'Relly Associates, Inc. Sebastopol, CA.

Stallings, W. (2015). *SNMP, SNMPv2, SNMPv3, RMON 1 y 2*.México, Prentice-Hall.

Stallings, W. (2017). *Comunicaciones y redes de computadoras*. México, Prentice-Hall.