Planificación e implantación de la seguridad en las redes de próxima generación

W. Baluja García[1], C. Anías Calderón[1]

[1] *Departamento de Telecomunicaciones, Instituto Superior Politécnico José Antonio Echeverría, CUJAE.*

RESUMEN

En el artículo se exponen algunos elementos sobre la seguridad en las Redes de Próxima Generación (NGN, por sus siglas en inglés). Se resumen varios aspectos importantes de la experiencia acumulada en las tareas de Planificación e Implantación de la seguridad en diferentes implementaciones NGN. En estas tareas se ha empleado una Arquitectura de Seguridad y un Sistema de Gestión, obtenidos para este tipo de redes en trabajos anteriores. Todo esto permite presentar varios resultados teórico-prácticos de importancia, con el objetivo de que puedan ser generalizados en entornos similares.

Palabras claves: Arquitectura de seguridad, gestión de seguridad, Redes de Próxima Generación, seguridad de redes

Planning and implanting security in Next Generation Networks

ABSTRACT

This article exposes some elements about security in Next Generation Networks (NGN). Several important experiences aspects in planning and implanting security in NGN are summarized. In these tasks are used the Security Architecture and Management System, obtained in previous works for this network's class. All it permits to show some theorist and practical important results, for its generalization in similar places.

Key words: Network security, Next Generation Networks, security Architecture, security management.

INTRODUCCIÓN

Operadores y proveedores de servicios afrontan los avances tecnológicos y, en particular, el advenimiento de las Redes de Próxima Generación como siguiente paso en el desarrollo de las telecomunicaciones.

La revolución que está ocurriendo en las redes y los servicios, hace que aparezcan nuevos retos en el trabajo de seguridad. Entre otras novedades, puede mencionarse que los servicios de telefonía y video se ven afectados por amenazas provenientes del mundo IP (*Internet Protocol*): programas malignos, *spam*, denegación de servicios y otros. Además, aparecen nuevas técnicas para realizar el fraude de manera exitosa.

La industria de las telecomunicaciones y de la información está trabajando en busca de nuevas soluciones de seguridad que puedan ser aplicadas a cualquier tipo de red, servicios y aplicaciones. Para lograr esto, en un mundo tan heterogéneo en cuanto a fabricantes, proveedores y clientes, se requiere del trabajo con soluciones estándares.

A continuación se comentan diversos aspectos tratados en las tareas de planificación e implantación de la seguridad en redes o soluciones NGN (basadas en el empleo de *softswitch*), como parte del ciclo continuo de la gestión de seguridad. Se exponen, brevemente, algunas conclusiones obtenidas en esta labor, con el objetivo de que puedan ser generalizadas en entornos similares.

Este trabajo de planificación e implantación se ha realizado empleando como bases la Arquitectura de Seguridad para redes de Telecomunicaciones (AS-T) y el Sistema de Gestión de Seguridad para redes de Telecomunicaciones (SGS-T) [1].

ARQUITECTURA DE SEGURIDAD PARA LAS REDES DE PRÓXIMA GENERACIÓN

De acuerdo a la propuesta de Arquitectura de Seguridad para redes de Telecomunicaciones[1], el único elemento que debe ser configurado especialmente para obtener la arquitectura correspondiente a las NGN, es el denominado Estructura Modular de la Red. El Modelo de Amenazas y la Pirámide de Seguridad permanecen inalterables, pues los análisis realizados en su definición son válidos para este tipo de redes.

Se propone el empleo de una Estructura Modular que parte del Modelo Básico de Referencia (MBR) de las NGN[2]. El uso del MBR garantiza dividir el problema de seguridad en dos partes fundamentales: la seguridad en el transporte y la seguridad en los servicios, enfoque ventajoso en entornos donde aparecen múltiples proveedores de servicios y que está acorde a las prácticas tradicionales de la gestión de redes. Igualmente, la definición de tres planos: usuario, control y gestión, permite trabajar la seguridad atendiendo a los tres grupos de actividades fundamentales que se llevan a cabo en las NGN.

Del cruce de estratos y planos del MBR se obtienen seis módulos (ver Figura 1) con los cuales se debe trabajar, ya sea de forma individual o grupal, en la aplicación de las plantillas que se utilicen (de Dimensiones, de arquitectura funcional o de Áreas de Trabajo[1]).

Los módulos obtenidos se enumeran a continuación:

1. Estrato de Transporte, Plano de Usuario.
2. Estrato de Transporte, Plano de Control.
3. Estrato de Transporte, Plano de Gestión.
4. Estrato de Servicios, Plano de Usuario.
5. Estrato de Servicios, Plano de Control.
6. Estrato de Servicios, Plano de Gestión.

Debe tomarse en consideración que el MBR plantea una visión funcional de las NGN. Las diferentes implementaciones de estas redes pueden conducir a la unión de los planos de control de los dos estratos (módulos 2 y 5), de acuerdo a la tecnología de control empleada. Lo mismo puede ocurrir con el plano de gestión (módulos 3 y 6)[2].

De esta forma, la Arquitectura de Seguridad para NGN (AS-NGN) queda como muestra la Figura 2, y hereda todas las características, facilidades de uso y valores que posee la AS-T[1].

Para los casos de implementaciones de redes NGN de mayor complejidad, y/o análisis muy pormenorizados de la seguridad, se propone utilizar plantillas que permitan ajustar la Estructura Modular de la Red a una arquitectura funcional diferente, con mayor cantidad de módulos, de acuerdo al interés de los especialistas.

En este sentido se introduce el empleo de la plantilla de cuatro capas (Figura 3), la cual representa una arquitectura funcional de red empleada por múltiples fabricantes y operadores en la descripción de algunas de sus soluciones NGN[3,4]. Esta plantilla divide el análisis de seguridad en más capas, manteniendo la compatibilidad con los estratos del MBR.

Cuando se aplica la plantilla de cuatro capas, no se modifica la influencia de los planos de actividades, pero el cruce de estratos y planos incrementa el número de módulos a doce, en lugar de seis. Vale resaltar que pudiera aplicarse esta plantilla sólo a uno de los planos, para realizar un análisis particular.

Adicionalmente, los diferentes operadores y fabricantes pueden acomodar el análisis de seguridad a su visión funcional de las NGN, a partir de crear y aplicar otras plantillas similares a esta.

Cualquier sistema u organización de gestión de seguridad que utilice la AS-NGN aquí propuesta debe centrar su trabajo en planificar, implementar, y mantener actualizados los componentes de la Pirámide de Seguridad en la red de telecomunicaciones en cuestión. Esto se logra a partir de la revisión constante de los cambios que se pueden producir en las amenazas y en las características de la red, y de la efectividad que se tenga en la implantación de los componentes de la Pirámide.

Es en las tareas de planificación e implantación de la seguridad que se pretende hacer mayor énfasis en el presente trabajo.

PLANIFICACIÓN E IMPLANTACIÓN DE LA SEGURIDAD EN LAS NGN

El empleo de la AS-NGN es válido para cualquiera de las tareas de gestión de seguridad que pueden realizarse en este tipo de redes. Adicionalmente, en el trabajo desarrollado hasta el momento por los autores, esas tareas de gestión se han ejecutado utilizando el Sistema de Gestión de Seguridad para redes de Telecomunicaciones [1].

A partir de este momento se expondrán las ideas empleadas y las experiencias generales obtenidas durante la realización de las tareas de Planificación e Implantación de la seguridad, en diferentes implementaciones NGN. Las etapas de dicho proceso se aprecian en la Figura 4.

En la etapa de Definición de Objetivos se debe utilizar la Estructura Modular de la Figura 1. Aquí son perfectamente vigentes, como punto de partida, los objetivos básicos de seguridad definidos para la conformación de la Pirámide del AS-T[1]. Si la red NGN es muy compleja, o el análisis a desarrollar más pormenorizado, se sugiere el empleo de la plantilla de cuatro capas de la Figura 3.

En la Evaluación de Riesgos se considera, especialmente, la influencia de dispositivos como los *Media Gateway* (MG) de cualquier tipo (de acceso, de señalización, troncales y universales), los controladores de *Media Gateway* (MGC), los servidores asociados al MGC, los servidores de aplicaciones y de gestión, y los equipos empleados para ofrecer conectividad en cada una de las capas (conmutadores gestionables y enrutadores). Por otra parte, durante el proceso de Identificación de Amenazas y de Vulnerabilidades, de la

Evaluación de riesgos, y en la etapa de Elaboración de Políticas, debe tomarse en consideración todo el análisis realizado al respecto en trabajos anteriores [5].

En la Tabla 1 se muestra una relación de medidas de seguridad para el Módulo 1 de la Estructura Modular de la red NGN. Esta relación ha sido obtenida a partir de los análisis realizados para la selección de Mecanismos de Seguridad en las etapas de Elaboración de políticas (ver Figura 4) ejecutadas hasta el momento. Las medidas resumidas en la tabla no constituyen una relación exhaustiva, pero sí contienen los mecanismos de seguridad más importantes empleados en las implementaciones y pruebas realizadas.

Por otra parte, cada mecanismo enunciado debe analizarse en el entorno particular donde se aplica. Por ejemplo, en infraestructuras de red dependientes de mallas de conmutadores de capa 2 (*switch*), la rapidez de recuperación de conexión ofrecida por el protocolo STP (*Spanning Tree Protocol*) no resulta suficiente en algunos casos, por lo que la calidad de los servicios (en particular de la voz) se ha visto afectada seriamente (lo que afecta la dimensión de Disponibilidad).

Así también, existen muchos otros aspectos a tomar en consideración en este proceso de Planificación e Implantación de la seguridad[1,5]. Este es el caso, entre otros, de las soluciones de cifrado, las cuales deben aplicarse sin impedir que funcionen adecuadamente los puntos de escucha legal, necesarios en soluciones de seguridad estatal.

ESQUEMA GENERAL DE SEGURIDAD PARA LAS NGN

A partir del análisis realizado acerca de las tendencias tecnológicas, problemas y soluciones de seguridad de las redes de telecomunicaciones; y tomando en cuenta los resultados de la aplicación del SGS-T y la AS-NGN en diferentes tareas, particularmente en procesos de Planificación e Implantación, se presenta un esquema general de seguridad para las redes NGN, el cual se muestra en la Figura 5.

Debe observarse que el esquema de la red se obtiene de la utilización de la plantilla de cuatro capas (Figura 3). En este caso se ha dividido la capa de Aplicaciones en "Gestión" y "Aplicaciones de contenido y/o de valor agregado", por ser los dos grupos más representativos que se encuentran en operadores y proveedores de servicios. Además, se añadió el enlace a otras redes (operadores, proveedores, Internet, entre otros).

En este esquema debe destacarse la presencia de los siguientes principios:

Separación del tráfico: Resulta de especial importancia, desde la etapa de diseño de la red, manejar la separación de los tres tipos de tráfico fundamentales de las NGN, correspondientes a los planos de gestión, control y usuario, mediante el empleo de túneles (cifrados o no). Esto se refleja en las líneas discontinuas de diferentes colores que aparecen en la Figura 5. De igual forma, debe estar protegido el tráfico que circula entre las redes de los usuarios y los equipos de Acceso. En todos los casos debe prestarse atención diferenciada a las redes o enlaces inalámbricos.

Defensa perimetral: La defensa perimetral de cada una de las zonas de la red NGN se realiza a través del empleo de cortafuegos. En los cortafuegos se propone utilizar los mecanismos de filtrado de paquetes y la detección de intrusiones de red. Estas soluciones pueden estar integradas en un equipo o distribuidas en varios de ellos.

El filtrado de paquetes debe controlar el tráfico de los diferentes planos de actividades de las NGN. En este caso, los colores en las líneas discontinuas de la Figura 5, permiten observar el tráfico que circula hacia o desde las diferentes zonas de la red. Dentro del tráfico de cada plano, debe también restringirse el uso de protocolos o servicios no permitidos en cada una de las zonas.

Otro grave problema que debe minimizarse por esta vía es el de los ataques que empleen *spoofing* IP[6].

En el caso de la detección de intrusiones de red, su tarea es mucho más compleja y requiere un nivel de procesamiento mucho mayor, por lo que demanda una configuración muy cuidadosa. Esto último se acentúa en el cortafuego que se encuentra entre el Núcleo de la red NGN y el enlace con Otras redes.

La configuración de estas soluciones de seguridad, en particular de los IDS (*Intrusion Detection System*), debe tomar en consideración las principales amenazas para las NGN[5].

Distribución de Servidores de Seguridad: Los servidores de seguridad tienen diferentes funciones. Incluyen un almacén de *logs*, que contiene los registros que generan o utilizan las soluciones de seguridad de su zona. Además, proveen los servicios PKI (*Public Key Infrastructure*) necesarios para establecer una Infraestructura de No Repudio y Registro de Eventos, para la Respuesta a Incidentes dentro del SGS-T[1].

En estos servidores también se ubican los respaldos de información (salvas) de cada zona de la red (configuración de dispositivos y servicios, perfiles de usuarios y otros), y los servicios AAA para la autenticación de usuarios y el registro de eventos de la zona.

Defensa en Profundidad: En los servidores de todas las zonas, ya sean de seguridad o no, deben implementarse, como mínimo, los mecanismos de seguridad siguientes: antivirus, filtrado de paquetes y *Host Intrusion Detection System* (HIDS).

En el caso de los enrutadores del Núcleo se propone ejecutar un filtrado de paquetes sencillo, que proteja las diferentes zonas de la red NGN de los ataques de *spoofing* IP y de la circulación indebida de los tres tipos de tráfico fundamentales, siguiendo lo establecido en la Figura 5. Esta medida permite establecer redundancia para el filtrado de paquetes que se realiza en los cortafuegos, cuidando no sobrecargar estos enrutadores.

Redundancia en los enlaces: Para preservar la claridad del esquema de la Figura 5 no se han representado la mayoría de las soluciones de redundancia que forman parte de la Infraestructura de Recuperación de Incidentes[1]. Sólo se han simbolizado los enlaces redundantes entre los enrutadores del

Núcleo. En este caso se tiende a establecer mallas entre todos los enrutadores y, en ocasiones, hasta varios planos de estas mallas. Además, deben considerarse los enlaces redundantes entre cada zona y el núcleo de la red, así como la redundancia de servidores y de bases de información.

Por último, debe añadirse que ha sido comprobada la influencia que pueden tener sobre la QoS (*Quality of Service*), los aspectos mencionados en este trabajo que suponen medidas activas sobre el comportamiento de la red (filtrado, IDS, VPN y otros). Los resultados de estas pruebas confirman la posibilidad de utilizar Soluciones de Seguridad (según definición de la AS-T [1]) típicas, sin afectar la QoS de los servicios VoIP (Voz sobre IP), plataforma fundamental de las actuales implementaciones de las NGN.

CONCLUSIONES

En las definiciones, planteamientos y propuestas realizadas en este trabajo se ha utilizado como base la AS-T, lo cual facilita la realización de cada grupo de tareas y garantiza la presencia de los elementos de análisis más importantes en la gestión de seguridad.

Un resultado relevante es la particularización, y comprobación del uso del SGS-T y de la Arquitectura de Seguridad para el caso de las NGN, en específico, en la Planificación e Implantación de la seguridad. Esto se realizó utilizando componentes de la Arquitectura de Seguridad, tales como la Estructura Modular de la Red y las plantillas.

Todo lo expuesto en este artículo, incluyendo la tabla de medidas de seguridad para el Módulo 1, y el esquema general de seguridad para las NGN, sirve como base para las tareas de gestión de seguridad en las implementaciones de estas redes que con frecuencia se están llevando a cabo en los operadores nacionales e internacionales.

En próximos trabajos se ofrecerán detalles sobre otras tareas de gestión definidas en el SGS-T que han sido ejecutadas con éxito en implementaciones NGN.

REFERENCIAS

1. **BALUJA, W.**: "Arquitectura y Sistema Para la Gestión de Seguridad de las Redes de Telecomunicaciones". Tesis de doctorado. Cuba, 2006.
2. Unión Internacional de Telecomunicaciones (UIT-T) "General principles and general reference model for Next Generation Networks". Recomendación Y.2011, 2004.
3. Alcatel Corp. "Alcatel IMS Solution", 2006. Disponible en: http://www.alcatel.com/global/convergence/alcatelimssolution.html.
4. Huawei Technologies. "U-SYS SoftX3000 SoftSwitch System Technical Manual". *Volume System Description*, 2004.
5. **BALUJA, W. & ANÍAS, C.**: "Amenazas y defensas de seguridad en las redes de Próxima Generación (NGN)". Artículo. *Revista Ingeniería y Competitividad*, vol. 8, no. 2, pp. 7-16, Colombia, 2006.
6. **BALUJA, W.:** "Los ataques *spoofing*. Estudio de sus manifestaciones más comunes". Artículo. *Revista Ingeniería Eléctrica, Automática y Comunicaciones*, vol. 22, no. 2, ISPJAE, Cuba, 2001.

AUTORES

Walter Baluja García. Ingeniero en Telecomunicaciones y Electrónica. Master en Telemática. Doctor en Ciencias Técnicas. Especialista en Seguridad de Redes y Sistemas. Jefe del departamento de Telecomunicaciones y Telemática del ISPJAE.

Correo electrónico: walter@tesla.cujae.edu.cu

Caridad Anías Calderón. Ingeniera en Telecomunicaciones. Master en Telemática. Doctora en Ciencias Técnicas. Especialista en Comunicaciones Ópticas. Especialista en Gestión de Redes y Servicios. Vicerrectora del ISPJAE.

Correo electrónico: cacha@tesla.cujae.edu.cu

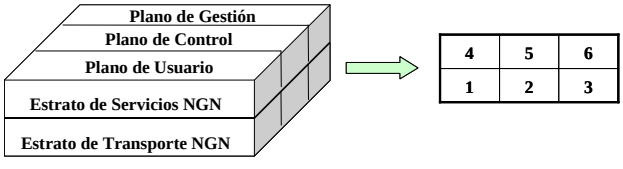

Figura 1. Estructura Modular de las NGN[1].

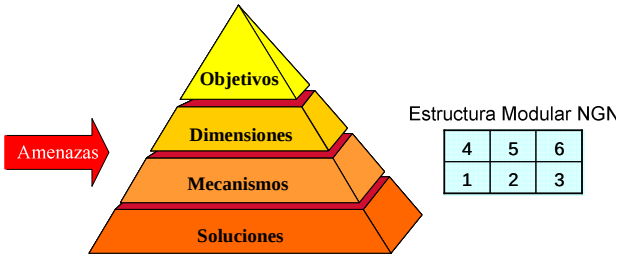

Figura 2. Arquitectura de Seguridad para NGN

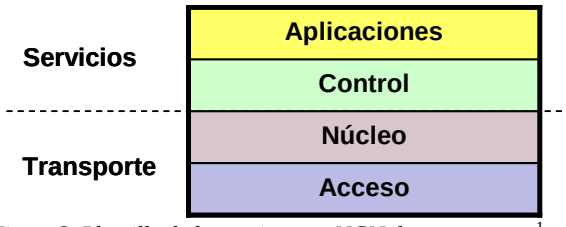

Figura 3. Plantilla de la arquitectura NGN de cuatro capas[1].

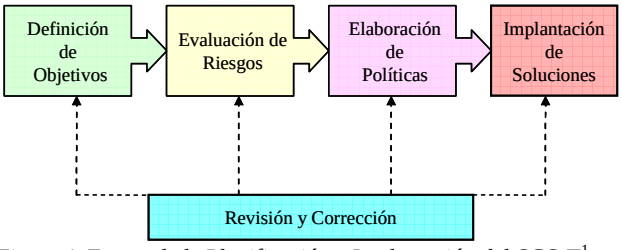

Figura 4. Etapas de la Planificación e Implantación del SGS-T[1].

Tabla 1. Medidas de seguridad para el Módulo 1 de la Estructura Modular de la red NGN.

Módulo 1: Estrato de Transporte, Plano de Usuario	
Dimensiones de Seguridad	**Medidas de Seguridad**
Autenticación	• Usar AAA (*Authentication, Authorization y Accounting*) para la autenticación en los dispositivos de conectividad, incluyendo los inalámbricos. Siempre que sea posible utilizar, como opción por defecto, soluciones externas del tipo de Radius. • Utilizar mecanismos de autenticación fuertes en los MG (*Media Gateways*) correspondientes. Si es posible emplear certificados digitales. • Proteger el tráfico de autenticación de usuarios a través de VPN (*Virtual Private Networks*) o alguna solución de cifrado (válido para enrutadores, MG y otros dispositivos). • Emplear IPSec (*IP Security*) para comprobar la autenticidad de los datos de usuario que se intercambian. • Minimizar la cantidad de usuarios con acceso a estos dispositivos.

	• Modificar los parámetros de las cuentas de usuarios por defecto.
Control de Acceso	• Separar en una red virtual (Capa2 o Capa 3) el tráfico de usuarios entre los MG y con otros elementos red. • Usar AAA (en particular la autorización) para el control de acceso a los dispositivos de conectividad. • Usar direcciones IP privadas. • Usar filtrado de paquetes en los enrutadores que regulan el acceso a las diferentes zonas de la red. • Emplear NIDS (*Nework Intrusion Detection Systems*) en la discriminación de tráfico que circula entre las diferentes zonas de la red. • Usar Puntos de Control de Acceso con filtrado de paquetes en los sistema inalámbricos. • Emplear cualquier otro mecanismo de control de acceso que permita garantizar que los elementos de red no proporcionen información sobre las actividades del usuario de extremo (posición geográfica, llamadas realizadas o sitios Web visitados, entre otros) a personas o dispositivos no autorizados.
No repudio	• Registrar todos los eventos de acceso a los equipos o canales involucrados en la red NGN. Pueden emplearse servidores Radius y/o servidores de *logs* centralizados. • Esta información de registro debe ser almacenada y/o duplicada en otros dispositivos de salva o almacenamiento de este módulo. • Proteger esta información contra accesos no autorizados y/o desastres.
Confidencialidad	• En los casos necesarios los datos serán cifrados desde el extremo de usuario o en determinados segmentos de la red. • Proteger con cifrado los datos que circulan por sistemas inalámbricos. • Diferenciar o aislar el tráfico de usuario (datos, voz y video) del resto, con el empleo de redes virtuales (VPN, VPLS (*Virtual Private LAN Service*) u otro según el caso). • Emplear cualquier otro mecanismo de confidencialidad que permita garantizar que los elementos de red no proporcionen información sobre las actividades del usuario de extremo a personas o dispositivos no autorizados.
Integridad	• Aislar el tráfico de usuario (datos, voz y video) del resto, con el empleo de redes virtuales.

	• Emplear IPSec para comprobar la integridad de los datos de usuario que se intercambian. • Emplear verificadores de integridad para los datos almacenados en los dispositivos de transporte y servidores asociados.

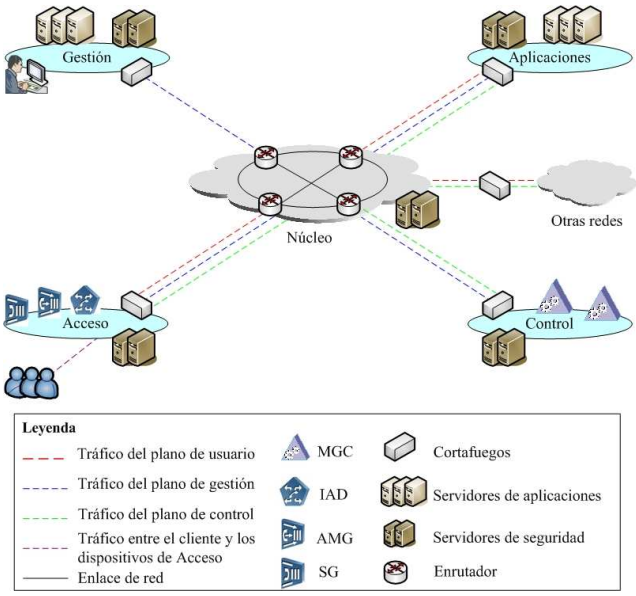

Figura 5. Esquema de seguridad de una red NGN típica.