Arquitectura de seguridad para la red de próxima generación

INTRODUCCIÓN

Las redes de telecomunicaciones de próxima generación —*Next Generation Network* (NGN)— que ofrecen servicios de multimedia —voz, datos y video— están soportadas por la familia de protocolos IP, en las que están presentes las vulnerabilidades, amenazas y riesgos propios de las redes de datos tradicionales y de las redes de telefonía IP [1]. Estos constituyen serios problemas de seguridad a enfrentar, recayendo principalmente sobre los operadores de telecomunicaciones y los proveedores de servicio la responsabilidad de ofrecer un servicio seguro y confiable a los clientes, proteger sus propias redes para cuidar su imagen y garantizar la continuidad en el servicio [2-3].

Estos servicios pueden ser objeto de ataques de denegación de servicios —*Denial of Service* (DoS) y *Distributed Denial-of-Service* (DDoS)—, robo o suplantación de identidad, manipulación y corrupción de datos, fraude telefónico, virus y SPIT —el equivalente del conocido SPAM en las redes de datos—, entre otros, con posibles afectaciones, por ejemplo, las caídas de servidores SIP y, por lo tanto, de todo el sistema, anulación de servicios, teléfonos saturados con llamadas y mensajes de texto no solicitados, redireccionamiento de llamadas, corrupción de datos y programas y acciones fraudulentas para usurpar tarjetas de crédito o hacer llamadas con cargo a terceros [4].

Sin embargo, es posible controlar la infraestructura de estas redes para prevenir las amenazas y mantener su seguridad. El uso de mecanismos de encriptación de extremo a extremo o de productos como los cortafuegos (*firewalls*), los controladores de sesión de borde —*Session Border Control* (SBC)— y los sistemas de detección de intrusiones —*Intrusion Detection System* (IDS)— pueden significar factores clave en la protección de este tipo de redes [5-7].

Variante de arquitectura de seguridad para la red NGN

Para enfrentar las amenazas y los riesgos de seguridad de la red NGN concebida como el soporte principal de todos los tipos de comunicaciones —servicios de datos de banda ancha, voz, multimedia, mensajería y otros—, se acometió la tarea de proponer una arquitectura de seguridad para la red NGN, en proceso de instalación en Cuba, adaptada a las características y condiciones del entorno cubano teniendo en cuenta las diferentes

Por MSc. Raymundo Pérez Sierra y MSc. Deborah Reyes Roig, Especialistas B en Telemática, Dirección Central de Desarrollo y Tecnología
raymundo.perez@etecsa.cu, deborah.reyes@etecsa.cu

etapas de desarrollo previstas [8].

Se procedió, entonces, al estudio y evaluación de diferentes enfoques y soluciones de seguridad para este tipo de red de nueva generación, aportados por reconocidas empresas productoras y suministradoras de estas tecnologías a nivel mundial, así como de diversos trabajos de prestigiosas instituciones, funcionarios y especialistas relacionados con el tema publicados en Internet [9-10].

La arquitectura de seguridad propuesta incluye lineamientos y medidas con un enfoque integral y personalizado, cuyo alcance abarca los sistemas y las redes de telecomunicaciones constituidos por elementos de la tecnología de redes de próxima generación, distribuidos en sus diferentes capas o niveles.

En su definición se tuvo en cuenta, además, la experiencia acumulada en la instalación, puesta a punto y pruebas de campo y aceptación de tecnologías NGN y de acceso de banda ancha —xDSL y WIMAX— de varios proveedores en nuestro país.

Lineamientos

La propuesta de arquitectura de seguridad para la red NGN está sustentada en lineamientos aplicables a nuestro entorno, aunque también extensibles a otros por su carácter general, cuyos contenidos incluyen aspectos de perfil estratégico y operativo sobre la organización, administración y el uso de los recursos tecnológicos y humanos involucrados.

Dichos lineamientos son:

1. La seguridad de la red NGN ha de abarcar todas las capas de la red. Es necesario adoptar un método por capas que, combinado con una sólida gestión y aplicación de la política, brinde soluciones modulares, flexibles y adaptables. La seguridad por capas permite ofrecer grados de seguridad variables. Cada nivel adicional se basa en las capacidades de la capa inferior y ofrece más seguridad con mayor granularidad. El diseño debe responder a la estrategia de resistencia, identificación y recuperación ante una intrusión o un ataque determinado.
2. La arquitectura tiene un carácter integral y engloba a los elementos de núcleo NGN —*softswich*, *media gateways* y otros—, la infraestructura de la red de transporte (*backbone*) IP/MPLS —también llamada red IP/MPLS—, los sistemas de acceso de los usuarios o clientes a la red, los sistemas de gestión y los componentes del centro de datos y del punto de acceso a la red Internet —*Network Access Point* (NAP)—.
3. En la proyección, diseño e implementación de esta arquitectura de seguridad deberán participar todas las áreas implicadas en el desarrollo, la implementación y explotación de la red NGN y, con carácter obligatorio, las especialidades de seguridad, tecnologías de la información, planeamiento, operación y gestión, con especial énfasis de esta última en el proceso de configuración de los dispositivos y sistemas de seguridad.
4. La arquitectura de seguridad se sustenta en las siguientes bases:

◆Definir las zonas de seguridad:

-Segura: los elementos de la red están bajo el control y la supervisión del operador de telecomunicaciones.

-No segura: los elementos de la red están fuera del control y la supervisión del operador de telecomunicaciones.

◆Segregar el tráfico por tipo —señalización, RTP, dato y gestión— desde el acceso y a través de la red IP/MPLS mediante redes privadas virtuales —*Virtual Private Network* (VPN)— de capa 2 o 3, identificadas según las zonas de seguridad en que se establezcan.

◆Emplear pasarelas (*gateways*) de acceso en el borde del núcleo IP: el servidor de acceso remoto de banda ancha para el acceso xDSL (BRAS), la pasarela de red de servicio de acceso para el acceso vía WiMax —ASN-GW— o el controlador de estaciones base para el acceso vía GSM / GPRS (BSC).

◆Proteger los elementos del núcleo NGN, incluidos los de la gestión, y los centros de aseguramiento

—centro de datos y NAP— con cortafuegos, controladores de sesión de borde, inspección profunda de paquetes DPI, sistemas detectores de intrusos y prevención contra intrusos (IDS/IPS), entre otros, según corresponda.

- Autenticación, autorización y contabilidad mediante servicios AAA y DHCP en interacción con las pasarelas de acceso.
- Disponibilidad mediante tecnologías de alta confiabilidad —*carrier grade* o *carrier class*— y redundancia de enlaces y de equipamiento en los nodos y elementos vitales de la red y el núcleo NGN.
- Gestión centralizada de las trazas (*logs*) de seguridad.

5. Controlar los tráficos de señalización y RTP provenientes de los elementos de la pasarela de medios (*media gateways*) de la zona insegura a través del SBC que actúa como *proxy* y elemento de protección del *softswich*. Como medida excepcional de refuerzo de la seguridad, se deberá enrutar también a través del SBC el tráfico de señalización proveniente de los elementos de la pasarela de medios de la zona segura.
6. A partir del despliegue de la red que se vaya alcanzando, priorizar en una primera etapa los dispositivos de control de la NGN —elementos del *softswitch*, *media gateways*, etc.— y los elementos de la red de transporte IP/MPLS, además asegurar, en la medida en que se incorporen, los accesos de los usuarios finales y la red Metro Ethernet (ME). De igual forma, prestar atención especial al centro de datos y al NAP, según sus etapas de desarrollo previstas.
7. El empleo de tecnologías NGN de diferentes proveedores para integrarse al soporte de telecomunicaciones exige garantizar la interoperabilidad entre las mismas.
8. Concebir la gestión de trazas de seguridad de la red NGN y el *backbone* IP/MPLS como una función centralizada de presencia obligatoria desde las primeras etapas de desarrollo de la red. La gestión consiste en recolectar las trazas, procesarlas, analizarlas, correlacionarlas en el tiempo y tomar decisiones. Esta función deberá realizarla el personal especializado de seguridad, con el empleo de sistemas y herramientas apropiados, en un centro de gestión o de operación de la seguridad de la red.
9. Aprovechar las facilidades de la tecnología en cuanto al empleo de certificados digitales en los diferentes modos de autenticación en interacción obligada con los servidores AAA, como una manera de garantizar la legitimidad de la identidad de los usuarios y terminales en el proceso de conexión a la red para recibir los servicios correspondientes.
10. Aplicar las opciones de empleo de protocolos seguros basados en técnicas criptográficas en el proceso de gestión de los elementos integrantes de la red —por ejemplo, SSH, HTTPS, FTPS y SNMPv3— que regularmente ofrecen las tecnologías NGN instaladas.
11. En los accesos por vía inalámbrica, garantizar la confiabilidad, la integridad y la disponibilidad de la información (datos) en el tramo de transmisión por radio —interfaz de aire— entre los terminales de usuarios y las estaciones base, con la implementación de las medidas de seguridad recomendadas en los estándares internacionales, según corresponda.
12. Negociar con los proveedores, mediante la consignación en los contratos, que asuman la responsabilidad de garantizar las acciones periódicas de mantenimiento de la seguridad de los sistemas y las aplicaciones propietarias de su tecnología, como las actualizaciones de sistemas antivirus y de versiones de software del equipamiento, "parcheo" de seguridad, corrección de vulnerabilidades de seguridad, entre otras. Estas acciones deberán ser ejecutadas mediante mecanismos implementados que posibiliten su aplicación, con la participación conjunta de los especialistas y los proveedores.

13. Dada la complejidad que presenta el proceso de asimilación, implementación y mantenimiento de los sistemas de seguridad de la red NGN en todas sus capas, donde interactúa un conjunto de dispositivos, servidores y aplicaciones de seguridad, es imprescindible contemplar y garantizar la capacitación del personal de seguridad informática que participa en su planeamiento, implementación, mantenimiento y operación, incluyendo a los especialistas de gestión de la seguridad, desde el inicio del proceso de contratación y durante su ejecución.
14. Contemplar y utilizar los recursos humanos necesarios para el planeamiento, la implementación, el mantenimiento y la operación de la arquitectura de seguridad de la red NGN, incluyendo el personal de la gestión de la seguridad, que define los deberes funcionales específicos por cada una de las áreas de trabajo implicadas.

Medidas específicas por capas de la red

La arquitectura de seguridad contiene un grupo importante de medidas específicas por cada uno de los niveles o capas de la red NGN.

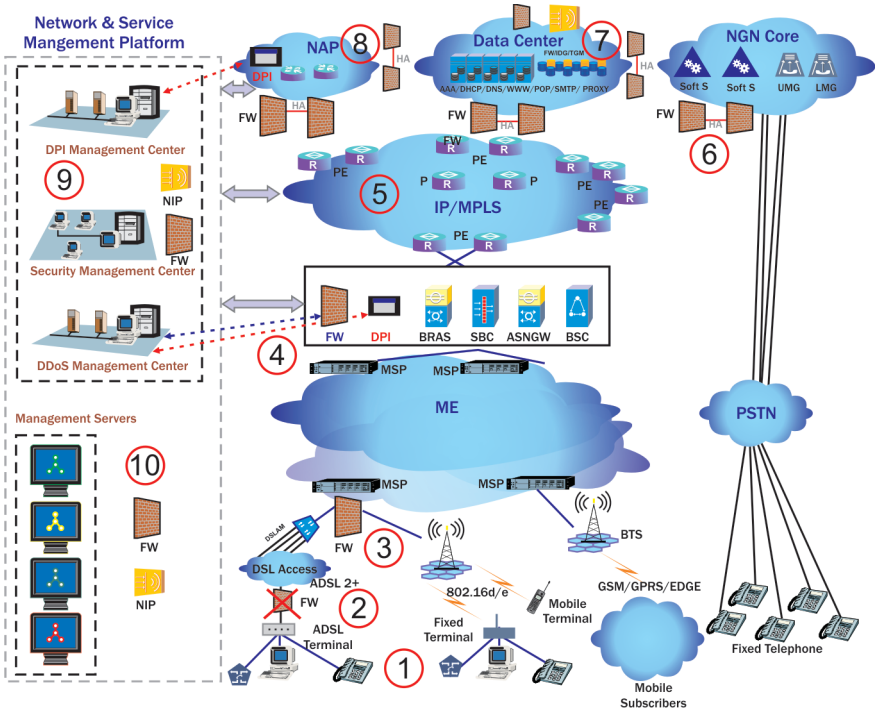

Figura 1 Arquitectura de seguridad para la red NGN (Fuente: [8]).

Capa de terminales:

- Los usuarios o clientes pueden establecer por sí mismos su seguridad, adoptar las medidas apropiadas para este nivel (Figura 1, punto 1) de acuerdo a sus necesidades, y deben cumplir los requerimientos de autenticación y autorización que demanden los servicios de la red que se les brinde. Entre las medidas posibles a emplear están los sistemas antivirus, "parcheo" de seguridad, compartimentación de recursos, empleo de técnicas de tunelización y cifrado de extremo a extremo para la protección de la información, uso de cortafuegos (*firewall*) y detectores de intrusos, etc. No obstante, el operador de telecomunicaciones deberá estar en condiciones de proveer estas medidas a aquellos usuarios o clientes que no tengan posibilidades o no deseen asumir su seguridad.
- Considerar el empleo de un *firewall* a la salida del equipo terminal del usuario o CPE (Figura 1, punto 2) como elemento de protección perimetral de la red del cliente sólo de manera excepcional a petición de este, concretado

en el proceso contractual del servicio. Esto se fundamenta en la posibilidad que tiene el operador de telecomunicaciones de emplear las diferentes opciones de seguridad implícitas en el CPE si son necesarias —funciones de FW (*firewall*), DMZ (*Demilitarized Zone*), filtrado de IP del cliente, bloqueo de URL y filtrado de direcciones MAC— y que en otros puntos de mayor agregación de la capa de acceso podrá instalar dispositivos de mayores prestaciones que perfectamente pueden garantizar la seguridad de las redes de los clientes.

Capa de acceso:

- Considerar el empleo de un *cortafuegos* en los puntos de agregación para el acceso a la red Metroethernet (Figura 1, punto 3) en aquellas etapas ulteriores de desarrollo en que se haya hecho un despliegue masivo de la red NGN con presencia de la red Metroethernet, siempre que los resultados de un estudio de tráfico y evaluación de riesgos lo justifiquen.
- Utilizar las potencialidades de la tecnología de acceso desplegada en cuanto a la posibilidad de implementar diferentes tipos de VPN, desde los terminales de usuarios (CPE) hasta el borde de la red IP/MPLS o red Metroethernet (Figura 1, entre los puntos 2 y 4).

Capa de transportación:

- Implementar en el borde de la red IP/MPLS (Figura 1, punto 4) las funcionalidades de seguridad de un *firewall*, inspección profunda de paquetes —*Deep Packet Inspection* (DPI)— y controlador de sesión de borde mediante los dispositivos correspondientes, en los tipos y cantidades requeridos según sus potencialidades y las cantidades de líneas de abonados previstas para las diferentes etapas del despliegue de la red.
- Concebir el uso de un centro de gestión para la detección de posibles ataques de negación de servicios DoS y DDoS, en interacción con los elementos cortafuego y DPI del borde de la red IP/MPLS, cuyas funciones, con su equipamiento, deberán integrarse al centro de gestión de la seguridad de la red —figura 1, punto 9—.
- Implementar en el borde de la red IP/MPLS (Figura 1, punto 4) las funcionalidades de servidor remoto de banda ancha (BRAS) para el acceso xDSL, pasarela de red de servicio de acceso (ASN-GW) para el acceso Wimax y controlador de estaciones base (BSC) para el acceso GSM/GPRS, mediante los dispositivos correspondientes, en los tipos y cantidades requeridos según sus potencialidades y las cantidades de líneas de abonados previstas para las diferentes etapas del despliegue de la red. Estos dispositivos serán empleados para garantizar funciones de seguridad vitales como la autenticación y autorización de los terminales y usuarios finales, bien de manera autónoma a partir de sus posibilidades o actuando como clientes o intermediarios de los servidores AAA y DHCP de la capa de servicios (aplicaciones).
- Utilizar las potencialidades de la tecnología de la red de transporte IP/MPLS desplegada en cuanto a la posibilidad de implementar los tipos de VPN permisibles, para la segregación y protección de los diferentes tipos de tráficos que se trasmitan por la misma (Figura 1, punto 5).

Capa de control:

- Ubicar de cara a los SS (figura 1, punto 6) un dispositivo cortafuego u otro que cumpla similar función, con las potencialidades requeridas para el control de tráfico.

Capa de gestión y aplicación:

- Concebir el funcionamiento de la red con la presencia de los servidores AAA y DHCP ubicados en la capa de aplicaciones —en una DMZ o en el centro de datos, como se muestra en el punto 7 de la figura 1— para garantizar el control de acceso de los usuarios que se conectan a la red mediante el proceso de autenticación y autorización, y permitir su conexión y facturación una vez verificada su identidad.
- Aplicar como soluciones de seguridad en el centro de datos (Figura 1, punto 7) el uso de dispositivos de seguridad cortafuegos y sistemas IDS/IPS, como los sistemas de detección de intrusiones inteligentes, de red o NIP-IDS. Al mismo tiempo, concebir la redundancia necesaria en la conectividad de acceso externo y la implementación de un centro de datos secundario como respaldo activo.
- Aplicar como soluciones de seguridad en el NAP las funcionalidades de cortafuego y DPI. Este último en interacción con un sistema de gestión de DPI integrado al centro de gestión de la seguridad de la red (Figura 1, puntos 8 y 9).
- Aplicar como concepción de seguridad para la red de gestión NGN el empleo de cortafuegos, IDS/IPS, servidor AAA y uso de las VPN, soportada en una red EoSDH independiente o, en su defecto, en

la propia red IP/MPLS (Figura 1, punto 10).

Repercusión social y económica

La aplicación integral de esta arquitectura de seguridad tiene una importante repercusión social y económica pues proporciona la protección adecuada para que la red NGN pueda enfrentar el número elevado de amenazas de seguridad ya enunciadas, y así evitar o minimizar sus posibles impactos que van desde las pérdidas económicas, asociadas por la interrupción y afectación de los servicios, hasta la consiguiente repercusión negativa de la imagen de la Empresa y del país.

Entre las principales amenazas y sus correspondientes impactos se destacan:

- Ataques de denegación de servicio a los servidores de la red que pueden paralizar total o parcialmente su funcionamiento por un tiempo determinado.
- Ataques de suplantación de identidad que posibilitan la ejecución de fraudes telefónicos.
- Ataques de manipulación y corrupción de la información que viaja por la red con la consiguiente usurpación de la privacidad de los datos de los clientes y de la Empresa.
- Ataques de virus, *spam* y otros intrusos que pueden afectar la infraestructura tecnológica y de programas de la red, así como la información que se transmite y se conserva por los medios informáticos y de comunicación.

La tecnología NGN instalada en Cuba ofrece servicios a un grupo amplio de usuarios con perspectivas inmediatas de crecer de acuerdo al desarrollo previsto. Una caída de los servidores de esta red, provocada por un simple ataque de denegación de servicios, significaría la interrupción o la no disponibilidad de las comunicaciones a la totalidad de los usuarios por el tiempo que dure la misma.

Conclusiones

Las redes de próxima generación soportadas en familias de protocolos IP son herederas de las vulnerabilidades y amenazas de seguridad típicas de las redes de datos tradicionales, además de las específicas de la telefonía IP presentes en la capa de servicios. Esto constituye un escenario propicio para los posibles ataques de denegación de servicios y otros incidentes de seguridad que pueden afectar la funcionalidad del sistema y propiciar la posibilidad de ejecución de fraudes telefónicos, con la secuela de la afectación económica y del impacto social para la Empresa y el país. Por tales motivos, la necesidad de implementar un sistema de seguridad adecuado se convierte en un imperativo de las nuevas tecnologías de telecomunicaciones para su protección y defensa.

La arquitectura de seguridad para la red NGN expuesta constituye una referencia apropiada para la proyección e implementación de un sistema de seguridad para esta red, con un enfoque genérico y personalizado conforme a las condiciones de nuestro entorno y a las diferentes etapas de desarrollo y despliegue previstas.

Referencias bibliográficas

1- UIT-T. "Recomendación Y.2201. Redes de la próxima generación – Aspectos relativos a los servicios: capacidades y arquitectura de servicios". 2009. http://www.itu.int/rec/T-REC-Y.2201-200909-I/es (acceso: septiembre, 2010).

2- UIT-T. "Recomendación M.3016.0. Visión general de la seguridad en la red de gestión de las telecomunicaciones". 2005. http://www.itu.int/rec/T-REC-M.3016.0-200505-I (acceso: septiembre, 2010).

3- UIT-T. "Recomendación M.3016.1. Seguridad para el plano de gestión: requerimientos de seguridad". 2005. http://www.itu.int/rec/T-REC-M.3016.1-200504-I (acceso: obtubre, 2010).

4- Gutiérrez, R. "Seguridad en VoIP: Ataques, Amenazas y Riesgos". Universidad de Valencia. 2007. http://www.uv.es/montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf (acceso: octubre, 2010).

5- UIT-T. "Recomendación X.805. Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo". 2003. http://www.itu.int/rec/T-REC-X.805-200310-I (acceso: octubre, 2005).

6- UIT-T. "Recomendación X.1205. Aspectos generales de la ciberseguridad". 2008. http://www.itu.int/rec/T-REC-X.1205-200804-I/es (acceso: julio, 2009).

7- UIT. "La seguridad en las telecomunicaciones y las tecnologías de la información". 2004. http://www.veeduriadistrital.gov.co/es/grupo/g285/web/Archivo4AS.pdf (acceso: noviembre, 2010).

8- Pérez S., R. y Reyes R., D. "Dictamen Técnico sobre Arquitectura de Seguridad de la red NGN". ETECSA. Cuba. Abril 2010.

9- Baluja G., W. "Arquitectura y Sistema para la Gestión de Seguridad de las Redes de Telecomunicaciones". Tesis de Doctorado. Departamento de Telemática. ISJAE. Cuba. 2006.

10- Baluja G., W. y Arias C.,C. "Propuesta de Arquitectura de Seguridad para las redes de Telecomunicaciones". CUJAE. Cuba. Diciembre, 2006. http://www.criptored.upm.es/guiateoria/gt_m189h.htm (acceso: enero, 2007).