

Convergencia IP: elementos clave para asegurar las redes de convergencia



Jorge Fernandez

Director Técnico de Enterasys

Los primeros sistemas de voz sobre IP propietarios han logrado proporcionar servicios de voz de calidad, pero no han sido capaces de hacer frente a los nuevos riesgos asociados a redes de convergencia. Esta primera generación de sistemas tampoco ha conseguido abrir los protocolos e interfaces para crear verdaderas redes de convergencia.

Superar esta barrera implica crear un verdadero sistema de comunicaciones que proporcione servicios eficientes, predecibles, tal como exigen la amplia gama de aplicaciones que utilizarán la red común. Para este objetivo, se tiene que revisar y actualizar el diseño de la arquitectura de red.

La seguridad, en el más amplio sentido de la palabra, implica capacidad de predecir. Cuando se estudia la implantación de una red de convergencia capaz de soportar VoIP junto al resto de las aplicaciones de negocio, se puede utilizar un enfoque lógico para definir las capacidades de la red. Mientras que los diseños de red clásicos, basados en redes “rápidas pero tontas” eran adecuados para tráfico que no exigen ejecución en tiempo real, como el correo electrónico o la navegación web, la creciente amenaza de virus y gusanos, junto con la introducción de aplicaciones en tiempo real como la Voz sobre IP, exigen

un modelo de red no sólo rápido, sino también inteligente y eficiente.

Tres son las claves para dotar de seguridad una red de convergencia: la capacidad de controlar el acceso, la capacidad de la red de ofrecer protección a los dispositivos y aplicaciones en uso, y la incorporación de una arquitectura de respuesta dinámica.

CONTROL DE ACCESO

La mayoría de las redes de hoy en día no son capaces de decir quién o qué se conecta y lo que debería estar o no permitido hacer en ellas. Tampoco ofrecen la capacidad de distinguir entre usos adecuados e inadecuados de la infraestructura.

Hay tres características críticas para un control de acceso efectivo en una red de convergencia:

- **Autenticación o detección de personas y dispositivos conectados a la red.** Mientras que los

protocolos como el 802.1x son apropiados para el control de accesos en PC's con usuarios humanos, las redes de convergencia permitirán a dispositivos autónomos como cámaras, teléfonos IP, y aparatos multimedia el acceso a la misma red. En muchos casos, estos dispositivos no pueden usar el modelo tradicional de autenticación, consistente en presentar una credencial de identidad al sistema. Adaptarse a estas tecnologías requiere un nuevo conjunto de técnicas de autenticación.

- **Autorización de los dispositivos conectados.** La autorización es el proceso de asociar un dispositivo autenticado a un determinado rol dentro de la organización. Por ejemplo, una red puede saber que un teléfono IP tiene permiso para utilizar la red, pero debería también saber lo que ese teléfono sólo está autorizado a ser usado por un departamento o usuario espe-

cífico, y no se trata de un teléfono de recepción o de uso para visitas.

- **Asociación de políticas.** Se produce una vez que se ha llevado a cabo la autenticación y autorización. Este paso asegura que cada dispositivo conectado tendrá un mapeado dinámico de los servicios, privilegios y accesos correctos para el mismo. Si un sistema puede reconocer un teléfono IP mediante autenticación, pero no puede ser asociado de forma dinámica a las funciones y servicios de calidad y seguridad adecuados para este dispositivo, el objetivo de lograr una red segura y predecible no se consigue

PROTECCIÓN DE DISPOSITIVOS Y APLICACIONES

El segundo elemento crítico de una red de convergencia segura es la capacidad de ofrecer protección proactiva a los dispositivos y aplicaciones en uso. Dado que la voz sobre IP es una aplicación bien definida que usa protocolos claramente aceptados y niveles de tráfico, el sistema de comunicaciones debería ser capaz de definir mecanismos proactivos para prevenir el uso inadecuado de dispositivos y aplicaciones, no permitiendo el uso de protocolos que no tienen relevancia en los sistemas de voz sobre IP. Los elementos que proporcionan esto son:

- La capacidad de definir políticas de uso aceptable para el sistema de red, que impiden el acceso a la red de todos aquellos protocolos y aplicaciones no deseados
- La capacidad de crear y aplicar dinámicamente una definición de servicio que permita el uso del sistema de la Voz sobre IP al mismo tiempo que lo protege de los usos inadecuados.

La capacidad de proteger a los dispositivos de VoIP de otros protocolos que pueden ser utilizados para poner en riesgo o hacer mal uso de ellos.

El crecimiento imparable de la telefonía IP



Javier González

Director de marketing de COLT España

El mundo de las comunicaciones ha sufrido, a lo largo de la historia, una tremenda transformación. Este desarrollo, todavía en curso, ha sido más rápido en el mercado empresarial, innovador nato en el mundo de la tecnología. Las comunicaciones empresariales han entrado de un tiempo a esta parte en una nueva era en la que la telefonía y soluciones IP adquieren cada vez mayor protagonismo.

De hecho, se espera que el mercado europeo de telefonía basado en redes IP alcance los 1.400 millones de dólares para el 2008. Unas previsiones que, según Ovum, permiten afirmar que este mercado se dirige hacia una nueva fase de crecimiento favorecida, en cierta medida, por la confianza que ha despertado esta tecnología.

La telefonía IP se presenta como una alternativa real a la telefonía tradicional ya que tanto el soporte tecnológico, como el entorno económico y el regulatorio están lo suficientemente maduros. Esta situación está animando a las operadoras a integrar esta tecnología en su portfolio, ofreciendo un servicio de valor añadido y apostando por futuros desarrollos.

Soluciones competitivas que respondan a las demandas de las empresas es la baza de las operadoras en este mercado emergente. Así, la posibilidad de tener una única red homogénea y de calidad, que soporte todo el tráfico y, de este modo, suponga un ahorro en los costes, entre otras ventajas (mayor funcionalidad, flexibilidad y versatilidad de las herramientas de comunicación) es la piedra angular de estos servicios. Sin embargo, las inversiones que deben afrontar las compañías en una primera fase hace que algunas se muestren cautelosas y decidan posponer la adopción de esta tecnología, ya que no ven la manera de rentabilizar a corto plazo esta inversión. Pero a día de hoy las empresas ya tienen la oportunidad real de adoptar estas tecnologías pensando en la adecuación de sus redes al futuro, haciéndolas más seguras, unificándolas, estableciendo calidades de servicio y dando cabida a las necesidades actuales, pero sobre todo las futuras.

Ofertas como la tarifa plana de telefonía IP hacen más jugosos estos servicios y animan a los empresarios a decantarse por esta opción de comunicación convergente. Tal es así que los analistas se atreven a afirmar que un servicio gestionado de telefonía IP en el que las empresas sólo paguen una cuota mensual por usuario en la que se incluye llamadas, mantenimiento, gestión y soporte de la solución puede favorecer la entrada de las organizaciones en lo que ya se atreven en calificar como el futuro de las comunicaciones. De esta manera, los empresarios saben perfectamente lo que gastan y pueden hacer previsiones ajustadas de sus gastos en comunicación.

Pero la voz sobre IP no es sólo ahorro en costes y facilidad de gestión, mantenimiento y uso de una única red que transmite voz y datos, sino también el paso a un amplio abanico de funcionalidades de valor añadido para empresas. Desde la posibilidad del nomadismo, gracias al uso de un mismo número independientemente de donde se encuentre físicamente el usuario, hasta el routing inteligente de llamadas que evitan el colapso de líneas, pasando por conferencias de larga distancia, modificación de sistemas o administración sencilla de líneas, factores que convierten a las soluciones de voz sobre IP en servicios polivalentes capaces de soportar las actuales necesidades de comunicación de las empresas.

Las compañías se muestran receptivas a adoptar esta tecnología; de hecho, según prevé Ovum, en 2008 el 80% de las empresas europeas habrán migrado sus redes de telefonía tradicional a redes de VoIP. En Europa, ya está desarrollada e implantada en muchas empresas, y en España son muchas las que la han probado y demandan la ampliación de este servicio a toda su red. Según el informe «Evolución del negocio de la voz», encargado desde el Ministerio de Industria, Comercio y Turismo al Grupo de Análisis y prospectiva del Sector de las Telecomunicaciones, este año se espera consumir un total de 605 millones de minutos, un 222% más que los gastados en 2003. Lo que pone de manifiesto el futuro de este mercado. <<<

INCORPORAR UNA ARQUITECTURA DE RESPUESTA DINÁMICA

El último elemento de una red de convergencia segura debería ser la incorporación de una arquitectura de respuesta dinámica. Con este mecanismo, cuando se produce en la red algún evento impredecible que puede afectar la fiabilidad o integridad de los sistemas de convergencia, la red puede identificar la amenaza, localizar su punto de origen y aislar dinámicamente, eliminar o controlar la amenaza en tiempo real. De este modo se evita un amplio y adverso impacto sobre el sistema.

Los elementos de una respuesta dinámica son:

- La capacidad de detectar ataques detallados y complejos en la red o en el sistema de convergencia. Basándose en la detección de eventos críticos por el sistema de detección de intrusiones, la red puede comunicar el evento a los sistemas de gestión de la red, y localizar el punto de entrada del puesto desde el que se realiza el ataque. Este tipo de servicio de localización es vital. Cuando los IDS pueden detectar un problema, el asunto más urgente es localizar rápidamente su origen de modo que la acción correctora pueda ser aplicada en tiempo real.
- La capacidad de alterar el comportamiento de la red en el punto de conexión en el que se origina un ataque. Esto se hace ajustando la política para aislar, deshabilitar o estrangular los servicios proporcionados a dicho dispositivo. Es importante señalar que la clave para el éxito en esta área es poder proporcionar una respuesta proporcionada al problema, más que simplemente cerrar el puerto afectado.
- La voluntad de aprovechar una infraestructura para una aplica-

gama de aplicaciones, incluyendo VoIP cada vez es más común en muchas organizaciones. En general, el último escollo significativo para llevar a cabo este despliegue es el miedo a que la red no está preparada para soportar voz y otras aplicaciones sin comprometer la seguridad y la predictibilidad de cualquiera de las aplicaciones compartidas.

Adoptando un modelo de red que este enfocado en la seguridad, y centrándose en el control de acceso, la protección proactiva y la respuesta dinámica, es posible incorporar servicios de voz en una red de convergencia, al tiempo que se establecen los cimientos igualmente aplicables para casi cualquier aplicación o servicio futuro que se añada al sistema

VOIPSA

VOIPSA es la primera organización creada para hacer frente a la enorme cantidad de asuntos relacionadas con la seguridad en redes de voz y datos. Enterasys es un miembro activo de la organización, cuyo objetivo es ayudar a las empresas a comprender y evitar los riesgos de seguridad, a través de listas de discusión, informes, patrocinio de la Voz sobre IP, proyectos de investigación en seguridad y el desarrollo de herramientas y metodologías para uso público. VOIPSA es el primer y único grupo dedicado enteramente y en exclusiva a la seguridad en VoIP, y está respaldado por un amplio espectro de organizaciones tales como universidades, investigadores en seguridad, fabricantes de VoIP, y proveedores de servicios de VoIP. La formación de este grupo está vinculada a los potenciales problemas a los que pueden enfrentarse las empresas que adoptan redes VoIP, en un nuevo entorno de convergencia. <<<