



¿Cómo proteger Servidores de Aplicaciones en Internet?

Questión Importante: Conectividad, Protección, Aceleración y Presupuesto.

El gran reto del personal IT, es sin duda crear medidas de seguridad que sean eficientes, no solo para los usuarios locales, sino para aquellos que están fuera de la red LAN, esto ha sido cubierto por varias tecnologías, y que sin duda han propuesto una solución viable al problema de conectividad, sin embargo muchas de estas tecnologías ha dejado a un lado otras cuestiones de gran importancia.



El gran aumento de ataques a nivel Aplicativo ha traído consigo una innumerable lista de vulnerabilidades en aplicaciones comunes para muchas empresas, estas aplicaciones no pueden ser detenidas o cambiadas por otras así por que si, el dilema del costo en la inversión siempre esta presente, a lo que se suma que nadie puede asegurar que otra aplicación pueda ser 100% invulnerable.

Ataques a la orden del día.

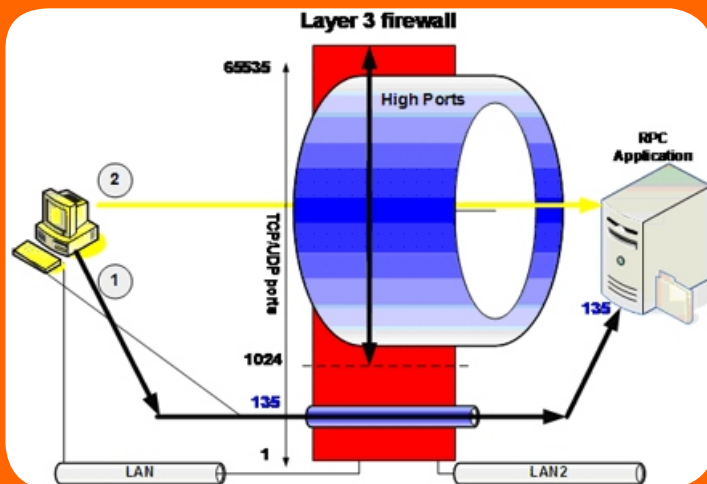
Casi todas las organizaciones hoy en día utilizan aplicaciones compartidas entre toda la organización, estas aplicaciones en algunos casos utilizan ciertos protocolos que permiten que estas aplicaciones puedan ser utilizadas por los usuarios desde distintos puntos geográficos, protocolos como RPC (Remote Procedure Call) permiten que estas aplicaciones ayuden a los usuarios a ser mas productivos, sin embargo un gran numero de personal IT, incluyendo los administradores de red y firewalls, no entienden como trabaja estos protocolos y los problemas potenciales que estos generan y lo mas importante no conocen como proteger su infraestructura de Servidores ante cualquier problema derivado de utilizar estos protocolos.

La gran mayoría piensa por ello que estos protocolos son inseguros por defecto, pero no saben que estos pueden llegar a ser utilizados de una manera segura y confiable.

Soluciones tecnológicas

La mayoría de las organizaciones creen que con el simple hecho de implementar un sistema perimetral de los denominados Stateful Inspection es suficiente, sin embargo estos sistemas lo único que hacen es abrir o cerrar puertos TCP o UDP. La constante evolución de los ataques, han sobre pasado estas defensas, ahora estos se enfocan a capas superiores, para ser exactos a nivel aplicación.

Si usted necesita filtrar trafico RPC y se utilizara un firewall stateful Inspection, sería necesario abrir el Puerto TCP 135(que es el puerto utilizado por los clientes de RPC para localizar el puerto del servicio RPC remoto) y como no es posible conocer cual es el puerto utilizado por la aplicación, será necesario abrir los puertos superiores desde 1024 hasta 65535.



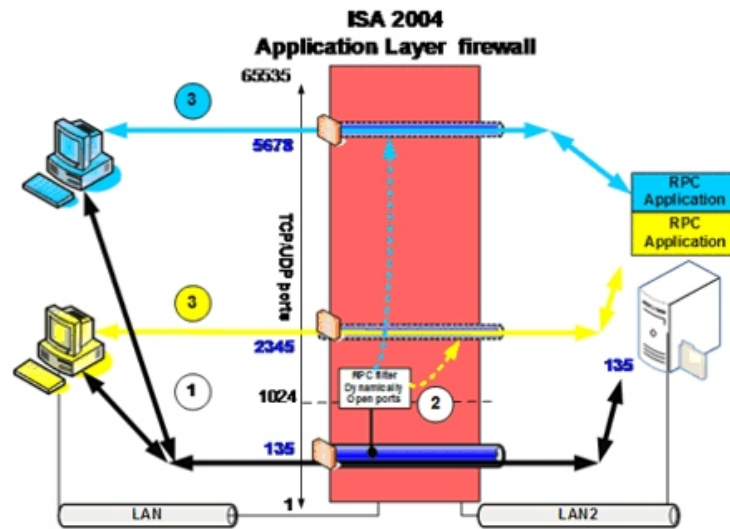
Como en realidad no es posible validar todos los orígenes desde los que se pudieran intentar conectar a nuestras aplicaciones, es necesario proteger nuestros servidores y servicios de una manera mas inteligente. Esto es posible gracias a sistemas de inspección completa a nivel aplicativo, este es el caso del sistema firewall ISA 2004.

El filtrado o inspección a nivel aplicativo significa que el contenido de la trama es revisado y se confirma que la información transmitida es autorizada, valida y que no signifique una amenaza para la compañía.

Cuando los sistemas Stateful Inspection realizan la inspección, ellos ven la información mas como un montón de caracteres siendo transportados por un medio, ISA 2004 realiza la inspección de la trama como un protocolo de red, validando no solo las cabeceras, sino la información en si misma.

Por ejemplo, un filtro de aplicación SMTP puede detener todas las tramas que contengan el commando RSET, o las tramas con mas de un cierto numero de caracteres, por decirlo así no solo revisa que tipo de trafico es transmitido sino también que cosas están dentro de ese trafico.

Cuando el firewall ISA 2004 realiza la inspección, analiza la trama llamada UUID (Identificador Único Universal), el cual es el identificador del servicio RPC que se esta corriendo en un servidor.



1. En la grafica de arriba, la estación de color Amarillo, en la parte izquierda, necesita entablar una conexión con el servidor RPC con una aplicación definida. El cliente RPC primero contacta al servidor por el puerto 135, y luego por decirlo así dice: "hola, cual es el puerto TCP para el UUID E1AF8308-5D1F-11C9-91A4-08002B14A0FA", el cual es el identificador único para la aplicación RPC con la que Necesita comunicarse. El firewall ISA crea el filtro de seguridad, y autoriza el trafico por que el sabe que el UUID esta autorizado.
2. El servidor responde con el puerto TCP asignado (2345) y con el cual se puede iniciar la comunicación.
3. Entonces la estación responde con el Puerto 2345 y entonces el servidor permite la comunicación con la aplicación.

Es entonces cuando se hace una inspección exacta de las comunicaciones permitidas y no solo de los puertos abiertos, esto es posible por que verdaderamente entiende como funcionan las comunicaciones a nivel aplicativo.

El mismo proceso es utilizado por la estación azul, donde esta intentando conectarse con la aplicación de color azul. La única diferencia esta en que el UUID es diferente, y el servicio no esta escuchando en el puerto 2345, sino por otro puerto (5678), en este caso si la estación trata de conectarse al servidor RPC con su propio UUID, este identificador no esta permitido en las reglas del ISA y por lo tanto esta comunicación será detenida.

Con esta visión de seguridad, es posible detener todas las conexiones RPC invalidas o no autorizadas y brindar un excepcional nivel de protección de los servidores internos tanto de zonas externas como Internet e incluso de peticiones internas.



Para más información acerca de este y más productos contáctenos o visite nuestra página de Internet.

RealNet, S.A. de C.V.
 "Administración y Seguridad de Redes"
 Guaymas 11bis Col. Roma C.P. 06700
 México, D.F.
 info@realnetsa.com.mx
 Tel: (01 55) 5219 8656
 Fax: (01 55) 5208 8201

www.realnet.com.mx