



Empresa Asociada: **Mediatrunk**

Autor: **Jose M^a Gómez Pinto**. Dtr. Ventas y Desarrollo de Negocio

Fecha de Publicación: Septiembre 2009. Boletín 72 @asLAN

BENEFICIOS PARA LA INDUSTRIA CON LA ADOPCIÓN DE UNA SOLUCIÓN DE "VISIBILIDAD TOTAL" EN SUS REDES DE DATOS.

Desde Mediatrunk quisiéramos exponer algunos problemas relacionados con las redes de datos que soportan el negocio en las compañías del sector industrial, de distribución y de servicios, y que necesitan una solución urgente; señalando los beneficios que obtendrán con la adopción de una solución de visibilidad total como la que describimos a continuación

Las redes IP se han convertido desde hace tiempo para estas empresas en una infraestructura crítica para el soporte y la continuidad del negocio, y se necesitan soluciones eficaces y polivalentes para su operación, su administración y su seguridad. Mejor una herramienta con varios usos que varias herramientas para cada uso, si se mantiene la eficacia.

Desde luego una visibilidad total del tráfico de Red con una alta granularidad se considera ya por muchos como indispensable. Y respecto a la seguridad es fundamental también una solución con un alcance también total, y no solo circunscrita al perímetro. Pasan más cosas en los pasillos de la empresa que en vestíbulo, por importante que sea esta pieza.

A la vez, en estos tiempos son frecuentes algunas dificultades como la limitación de la inversión para disponer de esa monitorización en toda la Red LAN y WAN (Interna y Perímetros), o la aparición costes excesivos por los cambios en la Red Interna para monitorizarla; y desde luego es común la limitación de los gastos de operación para gestionar mas sistemas en toda la Red. En definitiva, hay que hacer MÁS con MENOS.

Desde Mediatrunk proponemos como SOLUCIÓN la implantación de un Servicio Gestionado orientado a la eficiencia de la operación de la Red Interna y de su Seguridad, con la misma plataforma.

Pero hay más. También en estos tiempos existen problemas técnicos que necesitan una solución urgente en las redes de datos de las compañías del sector industrial, de distribución y de servicios.

Y es que no solo hace falta más ancho de banda y alta disponibilidad en la Red. Las amenazas en la Red aumentan en tamaño, frecuencia y complejidad; y la mayor amenaza es de naturaleza interna.

Pongamos como ejemplos el acceso no autorizado a los recursos en red y el uso indebido de aplicaciones. Hay muchos sitios donde vigilar. Así, encontramos otra vez

que monitorizar toda la red vuelve a ser una necesidad, que debería ser resuelta evitando distribuir sondas o agentes por todas partes.

Mediatrunk propone que la SOLUCIÓN a esto también sea la implantación de un Servicio Gestionado que dé visibilidad total de la Red interna y permita una gestión inteligente del tráfico y las amenazas de Red, de forma no intrusiva y sin sondas.

¿Pero cómo hacerlo? ¿Extendiendo a la Red interna las soluciones del perímetro? Desde luego que no.

Y ¿Por qué un Servicio Gestionado? Más allá de solución técnica empleada, de la que en seguida hablaremos, hay que plantear en un principio como gestionarla. En Mediatrunk creemos en el valor de la especialización. Disponer o no de los especialistas para mantener y gestionar las soluciones, no siempre está al alcance de una compañía, y no sólo es cuestión de dinero. Ambas cuestiones se pueden resolver eficazmente mediante la contratación de un servicio gestionado especializado.

Pero volvamos a la solución para ver el tráfico en toda la Red de una industria u organización de servicios desplegada por un amplio territorio con diferentes sedes, oficinas, centros de datos y puntos de acceso a/de otras organizaciones. Hay que considerar entonces una serie de características propias de las redes LAN/WAN que llevan a considerar soluciones diferentes de las del perímetro.

La Red interna, al contrario que el perímetro, tiene miles de blancos vulnerables y cientos de aplicaciones enviando datos. Las amenazas de la Red interna son diferentes de las del perímetro. Como ya se ha

mencionado, están el uso indebido de la Red, o la actividad maliciosa, entre otros.

Por último, consideremos que la Red interna de una empresa industrial mediana o grande es también grande y exige una cobertura amplia pero a un bajo coste.

Hay que añadir a lo anterior, que los retos actuales de la seguridad de la Red Interna aumentan porque el perímetro se vuelve difuso por la utilización de tecnologías de acceso inalámbrico de forma masiva.

El cambio continuo en las empresas trae la constante rotación de nuevos/ antiguos empleados, contratistas, consultores, auditores y clientes, que usan nuestra Red LAN/WAN con ciertos privilegios. La necesidad de cumplir leyes y regulaciones de seguridad y también normas internas o sectoriales sobre buenas prácticas en las TIC es un objetivo indiscutible, que llevado a toda la Red interna supone un autentico reto.

SOLUCIÓN DE MONITORIZACIÓN Y SEGURIDAD PARA REDES INTERNAS

Veamos ahora cómo funciona la solución técnica que proponemos para el servicio de monitorización y seguridad de las redes internas y que trata de dar respuesta a los requerimientos citados.

Primero, se va a recolectar la información estadística de tráfico generada por los elementos de red, conmutadores o routers. Tras eliminar flujos redundantes, se convierten los flujos unidireccionales en conversaciones bidireccionales. Después se modelan las conversaciones.

En un segundo paso, se realiza la correlación, análisis e identificación de la información, para generar un modelo relacional de "quién habla con quién y cómo". Así se proporciona a la empresa visibilidad de las conversaciones entre usuarios, redes y aplicaciones. Para ello se utilizan modelos de detección múltiple.

En un tercer paso, se defiende la Red mediante la generación de filtros con reglas para conmutadores o routers (ACLs) o políticas de cortafuegos. En general, para elementos que admitan scripts de comandos con una sintaxis típica.

Esto permite utilizar los elementos de Red como parte de la solución de seguridad, así como ajustar la configuración de los elemento de seguridad ante los incidentes que aparecen en la Red.

Los modelos de detección múltiple que antes citábamos son:

- Detección de patrones de propagación de comportamiento anormal como gusanos.
- Detección por huella de tráfico que viola un comportamiento: "malware", "phishing", "botnet".
- Detección de Anomalías por Ancho de Banda por cambios repentinos en los niveles del tráfico con respecto al nivel normal como un ataque DoS sobre una cadena de suministro.
- Detección de barridos tipo "slow scans", "fast scans", "stealth scans" y barrido de hosts.

- Uso interno indebido, detectando violaciones de políticas de seguridad específica, como un usuario del helpdesk accediendo a la base de datos de nómina.
- Caídas o indisponibilidad, detectando caídas en el tráfico de enlaces y servidores críticos.

De esta forma se consigue disponer de una visibilidad y capacidad de generar alertas e informes de forma no-intrusiva y en toda la Red LAN/WAN, en tiempo real y en forma estadística, sobre los participantes, las conversaciones y las aplicaciones que circulan por la Red que soporta el negocio.

El Análisis del Comportamiento en Red determina qué es "normal" en la Red y avisa de las "anomalías" que aparecen. Así tenemos información de "quién habla con quién y cómo". Y con esa información se pueden generar alertas y una amplia gama de informes para operación de red y planificación de capacidades.

Además esta solución ayuda a la administración de Red mediante el análisis del tráfico y permite la verificación de las políticas existentes. La solución también puede contribuir al Análisis Forense y al Cumplimiento Normativo, porque es posible verificar políticas y normas públicas o de la Industria como SOX, PCI, HIPAA, ITIL, ISO27001-2005 y otras.

Y ¿Cómo ayudamos al cumplimiento normativo? La solución asesora en el uso de la Red, detecta cambios, anomalías y ataques, así que refuerza el control sobre la Red y permite el seguimiento y trazado de los incidentes.

MÓDULO DE INTELIGENCIA DE APLICACIONES Y GESTIÓN DE HUELLAS DE AMENAZAS

Vamos ahora a describir otros dos aspectos importantes de la solución técnica que tienen gran importancia, por el valor que aportan a la operación y sobre todo a la seguridad de red: El módulo de inteligencia de aplicaciones y la gestión de huellas de amenazas.

El modulo de inteligencia de aplicaciones es el que da visibilidad en la capa de aplicación, necesaria para gestionar las aplicaciones en Red críticas para una industria como son VoIP, HTTP, BBDD o IM. Aquí se recurre a capturar el tráfico de paquetes al completo para inspeccionarlos, aunque sin llegar a procesar todo el paquete. De esta forma, se combinan las ventajas de la detección por flujos a partir de información estadística, con la visibilidad a nivel aplicación.

Este módulo permite saber cómo circulan por su Red las aplicaciones, cuánto tráfico utilizan y quién las usa. También permite tener informes por aplicación, independientemente del puerto y del usuario, identifica tráfico tunelizado o clandestino, mide y protege el tráfico crítico y aplica políticas para proteger la información.

El módulo detecta y clasifica más de cien aplicaciones, entre las que se encuentran protocolos como los ya citados de HTTP, IM, VoIP, BBDD, más P2P, Juegos, aplicaciones estándar como SMTP, Telnet, FTP, SSH, SSL y otras. Dentro de la solución que venimos

describiendo el módulo permite, para las aplicaciones detectadas, buscar tráfico, ver conexiones, generar estadísticas y crear alertas o informes.

La gestión de huellas de amenazas es un concepto basado en tres elementos:

Primero, un equipo de especialistas en seguridad que recolecta información sobre las más recientes amenazas presentes en Internet como BotNets, Worms, Trojans, Malware, Scans, Phishing/Pharming, o vulnerabilidades de aplicaciones, o protocolos muy populares, Skype, Peer-to-Peer, y otros.

El segundo elemento formado por las huellas de amenazas que se construyen como las trazas compuestas para identificarlas.

En tercer lugar, tenemos el uso de esas huellas directamente en la solución. La actualización es automática. Las huellas se emplean en la solución para reconocer las amenazas presentes en el tráfico de la Red monitorizada. No son firmas de bits y bytes. Son patrones de comportamiento.

Con los elementos ya descritos ahora podemos plantear nuevos Servicios de Seguridad desde la Red Interna como los siguientes:

- Detectar amenazas conocidas y nuevas.
- Descubrir hosts infectados.
- Prevenir y detectar el uso interno indebido.
- Controlar el acceso de usuarios a aplicaciones de la Empresa.
- Segmentar y fortalecer la Red Interna.
- Gestionar Perímetros Virtuales.

La solución de Visibilidad y Seguridad de la Red Interna que gestionamos para el cliente refuerza la seguridad usando los equipos de Red como defensa; detecta y notifica amenazas conocidas y desconocidas a través de huellas actualizadas y proporciona información valiosa para la segmentación y mitigación.

Ante el problema del Mal Uso de la Red Interna, la solución detecta accesos no autorizados a los recursos, detecta aplicaciones, usuarios o servidores maliciosos, avisa de la violación de políticas de uso aceptable de la Red, y relaciona tráfico con usuarios mediante Identity Tracking.

Acerca de...Mediatrunk:

Como parte de la estrategia de innovación impulsada por el grupo AL Holding (fundado en 1986), MediaTrunk nace en el 2001 para posicionarse en el mundo de las aplicaciones multimedia con el objetivo principal de atender a los mercados de Empresa, Operadores e ISP's. Con la visión de un mercado español marcado por la necesidad de mejorar la productividad y competitividad empresarial mediante la implantación de nuevas tecnologías, MediaTrunk da respuesta a este mercado aportando soluciones tecnológicas de última generación, con un espíritu de servicio al cliente caracterizado por la proximidad, la experiencia y la cualificación de su equipo de profesionales.,

La Asociación @asLAN. www.aslan.es

@asLAN, la Asociación de proveedores de sistemas de red, internet y telecomunicaciones, desde su constitución en el año 1989 ha tenido como misión la promoción y difusión de las tecnologías de redes y telecomunicaciones en España en el ámbito empresarial. Actualmente la Asociación @asLAN, agrupa más de 100 empresas, entre las que se encuentran los principales fabricantes de red, integradores, distribuidores y operadores de telecomunicaciones. @asLAN organiza y colabora en iniciativas dirigidas al desarrollo del Sector TIC y difusión de nuevas tecnologías en diversos sectores: Industria, AAPP, Banca, Educación, etc...Entre sus principales actividades se encuentra la organización de SITI/@asLAN, el evento profesional y especializado en Soluciones Tecnológicas para la Administración Pública, Gran Cuenta y Pyme.

En el importante capítulo de la Seguridad del servicio de VoIP, podemos gestionar y proteger el despliegue de VoIP con el módulo de Inteligencia de Red, proporcionando orientación y soporte para el despliegue actual de VoIP o una próxima ampliación, realizar monitorización continua, ayudando a la localización y resolución de problemas, dar visibilidad del Call Center e identificar rápidamente los Gateways más cargados o presentar los top-callers y las llamadas interrumpidas, entre otros. Por último, es interesante citar que se dispone de un Registro Histórico sobre grandes periodos de tiempo.

En resumen, proponemos a las industrias y empresas de servicios la adopción de un Servicio Gestionado para Redes Internas LAN/WAN que les proporciona:

- Un nuevo enfoque DUAL para la seguridad interna y la operación de red.
- Una Visión Global de la Red.
- Un modelo de "Quién hace Qué y Cómo".
- Qué aplicaciones están siendo usadas.
- Alertas en base a desviaciones del comportamiento normal.
- Informes de puertos abiertos sin usar.
- Descubrimiento Pasivo de Hosts.
- Detección y Protección ante amenazas (nuevas o conocidas).
- Identificación y documentación de uso inadecuado de recursos protegidos.
- Mitigación.
- Ayuda al Cumplimiento de Legislación y Normativa.

Además, otros Beneficios para su Industria serán:

- Despliegue reducido.
- Adaptación al Cambio Continuo en la Red de su organización.
- Mayor Flexibilidad de Operación.
- Gran contribución a: la Continuidad de su Negocio; la Gestión del Riesgo; la Inteligencia de su Negocio

Esperamos haber aportado un enfoque innovador al problema de la visibilidad del tráfico y la seguridad en la Red LAN/WAN con una solución económica, no intrusiva y de amplias posibilidades, gestionada por especialistas, para que la empresa usuaria obtenga los mejores resultados de la tecnología mientras se enfoca en su actividad industrial o de prestación de servicios.