Arquitecturas avanzadas para los sistemas de detección de intrusos

Los sistemas de detección de intrusos (IDS), son utilizados por numerosas organizaciones que los consideran, cada día más, una pieza indispensable de su arquitectura de seguridad perimetral. En este artículo se analiza en detalle la evolución de estos sistemas, desde las arquitecturas más sencillas, hasta las últimas novedades con las que, al entrar en juego nuevos elementos (taps, balanceadores, etc.), pueden diseñarse soluciones para aquellos clientes a los que un IDS, en su concepción tradicional, normalmente causaba más problemas de los que resolvía.

Alfonso Franco

Introducción

Antes de profundizar en las nuevas arquitecturas conviene dar un breve repaso a lo que todos conocemos como arquitecturas tradicionales de IDS.

Los IDS, más en concreto las sondas de red (NIDS), se instalan en aquellas redes a las que, por diferentes motivos, se desea dotar de un nivel de seguridad adicional al que proporcionan los cortafuegos. Para garantizar un correcto funcionamiento de estos sistemas es necesario que existan medios técnicos que garanticen que todo el tráfico de red va a poder llegar al IDS para su análisis.

Por lo tanto, a la hora de plantearse una solución para este tipo de entornos tradicionalmente existían dos opciones para lograr la replicación del tráfico:

– La conectividad mediante medios compartidos, *hubs*.

– Las técnicas *spanning* de puertos en los *switches* de comunicaciones.

La primera de las alternativas no debería aconsejarse en prácticamente ningún caso debido a la congestión de tráfico que genera un medio de red compartido y a los problemas de seguridad que este tipo de soluciones de conectividad introducen en las redes.

La segunda opción, pese a los inconvenientes que puede llegar a ocasionar en la configuración y el rendimiento de la electrónica de red, suele ser la opción más habitual puesto que constituye un punto de equilibrio razonable entre prestaciones, seguridad y funcionalidad.

Evolución tecnológica

Las arquitecturas de IDS tradicionales se han visto obligadas a evolucionar hacia nuevos escenarios que permitan a los IDS cumplir con su objetivo en las nuevas arquitecturas donde el volumen de tráfico (escenarios con redes GB) y la criticidad de los servicios que se ofrecen a los usuarios exigen nuevas soluciones. Uno de estos avances son los denominados *TAP (Test Access Point)*.

Los taps son unos dispositivos que mediante conexiones hardware, replican el tráfico de ambos sentidos de una comunicación. Estos dispositivos son, generalmente, tolerables a fallos de alimentación, es decir, ante una caída de la alimentación del tap, el tráfico no se interrumpe sino que únicamente dejaría de funcionar la replicación del tráfico a los puertos de tap.

Como se muestra en la **Figura 1**, el dispositivo extrae una "copia" de las señales de transmisión y recepción de la conexión entre dos equipos. La conectividad entre los equipos está asegurada ya que no se interrumpe la conexión física entre ambos. Como se puede ver, la conexión es unidireccional, no siendo posible la comunicación a través del tap de los sistemas que analizan el tráfico (en nuestro caso los IDS) con los equipos que se están comunicando.

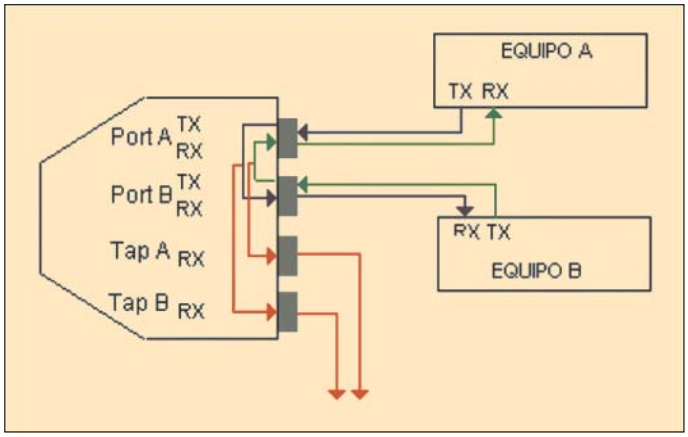

Figura 1: esquema de funcionamiento de un tap

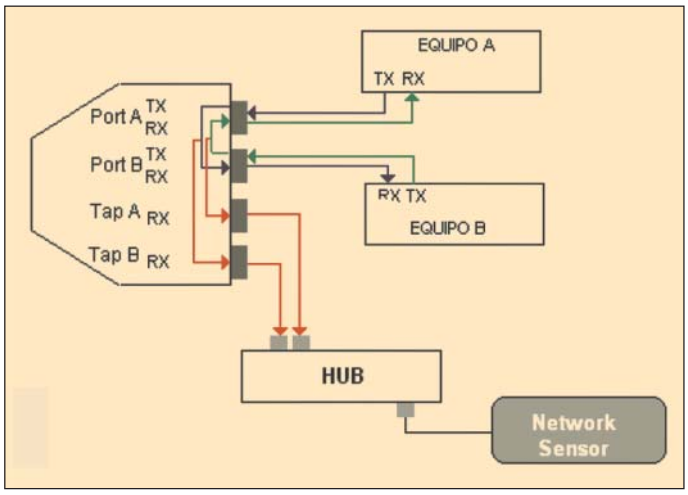

Figura 2: esquema de conexión de un TAP a un NIDS

La única consideración a tener en cuenta es que cada dispositivo de tap proporciona dos puertos de salida. Hasta el momento, la tecnología software empleada no dispone de capacidades de agregación de ambos tráficos en una única instancia de sensor, por lo que entre el tap y el sensor debe habilitarse un mecanismo adicional para agregar dicho tráfico, esto es, un medio compartido o un balanceador de IDS, tal y como puede verse en la **Figura 2**.

No debe confundirse la utilización de un *hub* como medio de conexión entre el TAP y el NIDS con la utilización de un HUB para la conexión entre los servidores y el NIDS, que se comentaba en la introducción de este artículo.

Fundamentalmente existen dos tipos de taps:

– Taps monopuerto: réplica del tráfico de un punto concreto de la red

– Taps multipuerto: réplica de varios puntos de la red a una única salida de *tapping* (problema de saturación de

los puertos de *tapping*).

Como se ha podido constatar, los taps son elementos orientados a resolver la problemática asociada a la replicación del tráfico de red a consecuencia de la instalación y configuración de un NIDS.

Sin embargo, ¿qué ocurre cuando el tráfico de una determinada red supera los límites de un NIDS? En estos casos el problema surge por la imposibilidad de que un determinado sensor de red pueda analizar todo el volumen de tráfico que recibe.

La solución a estos problemas es posible mediante la incorporación dentro de la arquitectura de IDS de elementos balanceadores de tráfico.

Como ocurre en otros sistemas, un balanceador de IDS es un elemento encargado de repartir el tráfico entre varios sensores de red, de forma que entre ellos puedan analizar todos los datos recibidos.

La combinación de estos elementos con las soluciones descritas anteriormente de replicación de tráfico utilizando *taps*, permite la instalación y configuración de arquitecturas de detección de intrusos con una capacidad de análisis, rendimiento y escalado muy superior a las soluciones tradicionales. Sobre todo porque en la mayor parte de los casos va a ser posible ampliar el rendimiento de la infraestructura simplemente añadiendo nuevos sensores de red, simplificando de esta forma la operación, gestión y el mantenimiento de las soluciones implantadas.

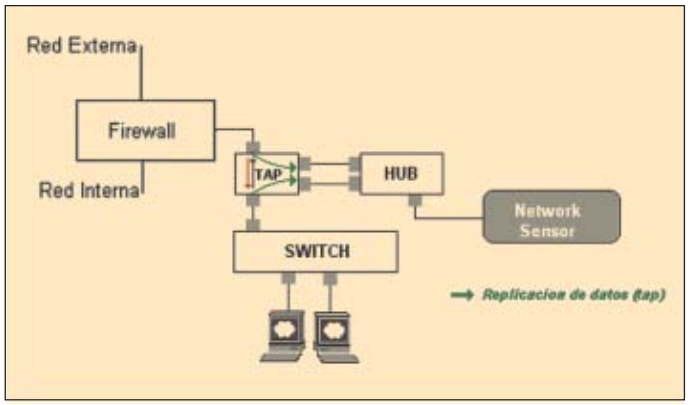

Figura 3: arquitectura con tap monopuerto

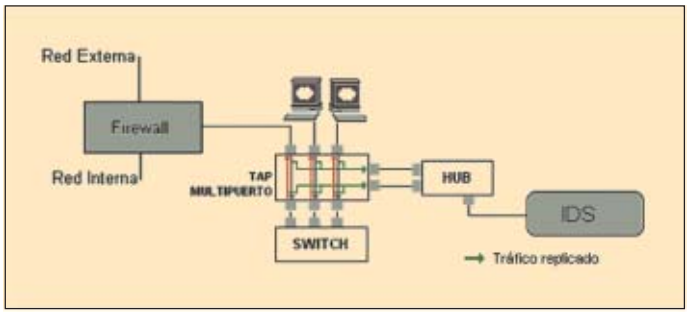

Figura 4: arquitectura ejemplo con taps multipuerto

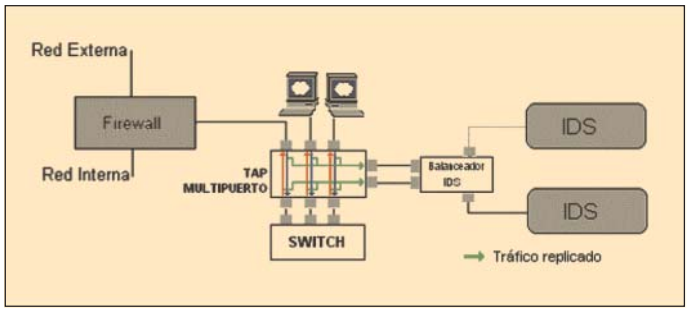

Figura 5: solución con taps y balanceadores de IDS

Ejemplos de arquitecturas

En este punto se comentan algunas arquitecturas de IDS combinando taps y balanceadores de carga entre distintos IDS.

Para cada una de estas arquitecturas partimos de una configuración clásica como puede ser la instalación de un NIDS en una DMZ de un cortafuegos.

En primer lugar, se propone una arquitectura sencilla con la utilización de un tap monopuerto como elemento de interconexión entre el cortafuegos y el *switch* tal y como puede verse en la **Figura 3**.

Esta arquitectura presenta las siguientes ventajas:

– El NIDS detectaría ataques originados en las redes externas con destino a cualquiera de los servidores instalados en dicha red.

– Para la instalación del NIDS no es necesaria ninguna configuración específica del *switch* que proporciona la conectividad.

– En caso de que el tap dejase de funcionar no se pierde la comunicación entre el cortafuegos y los servidores puesto que el tap seguiría proporcionando conectividad.

– Al no ser necesario realizar *port spanning* en el *switch*, no se perjudica el rendimiento de la electrónica de red.

Sin embargo, el inconveniente principal de este tipo de soluciones es que no sirven de protección frente a ataques entre equipos de la misma red, y por lo tanto, en caso de que un atacante obtuviese un acceso a un equipo de la DMZ podría intentar accesos al resto de los sistemas sin que el IDS los detectase.

La solución a este inconveniente consistiría en sustituir el tap monopuerto que aparece en el diagrama propuesto, por un tap multipuerto de forma que el tráfico entre los distintos equipos también atraviese el tap, tal y como puede observarse en el siguiente ejemplo.

En este caso, el inconveniente principal se encuentra en una posible saturación del puerto de salida del tap.

A la vista de estas arquitecturas, se observa claramente que proporcionar una solución para aquellos entornos con un tráfico de red elevado es una tarea relativamente sencilla puesto que bastaría con sustituir el *hub* que se utiliza como sistema de agregación de tráfico por un equipo con la funcionalidad de realizar el balanceo de IDS.

En este caso, tal y como puede apreciarse en la siguiente ilustración, añadir nuevas sondas de IDS es una tarea sencilla que permite aumentar la capacidad de análisis de los IDS de la arquitectura.

Las nuevas arquitecturas de servicios Internet arrastran de forma inevitable a todos los elementos que forman parte de las mismas, y los sistemas de seguridad no podrían ser menos, hacia nuevas soluciones tecnológicas que mantengan o mejoren los niveles de seguridad actuales. La combinación de taps con sistemas de balanceo de carga permiten que los sistemas de detección de intrusos puedan instalarse prácticamente en cualquier arquitectura de red, evitando los problemas de sobrecarga de los elementos de seguridad y perdida de tráfico en las sondas de red. ■

Alfonso Franco Gómez
División de Seguridad
Responsable de Preventa y Tecnología
Germinus Solutions
afranco@germinus.com