INFORME

ELEMENTOS PRINCIPALES DE LA ESTRATEGIA CISCO SELF-DEFENDING NETWORK

Gracias en parte a la campaña de publicidad que Cisco® ha realizado durante la presentación de Cisco Self-Defending Network (por ejemplo, el anuncio de TV en la que una niña descargaba ingenuamente un virus en el equipo de su padre), muchos usuarios se han dado cuenta de la necesidad de una seguridad de red integrada.

Pero ¿puede realmente una red defenderse a sí misma?

La respuesta rápida es "Sí, puede". La seguridad de red ha evolucionado desde productos desplegados de forma independiente (como los firewalls) al concepto de soluciones globales de sistema. Y Cisco Systems® está en la vanguardia del desarrollo tecnológico que ha hecho que la autodefensa de las redes sea una realidad.

La razón es sencilla: En las empresas de hoy en día, especialmente en esta era de actividad reguladora, preservar la integridad, confidencialidad y longevidad de la información empresarial es un factor esencial para lograr el éxito. A medida que nos dirigimos a una economía global basada en la información, tanto el valor de la información como el acceso controlado a ella son cada vez más importantes. El objetivo de una infraestructura TI es crear sistemas que puedan detectar y protegerse contra los accesos no autorizados y, al mismo tiempo, ofrecer acceso eficiente a los usuarios legítimos. La simple denegación del acceso frente a un ataque ya no es suficiente. Las redes actuales deben ser capaces de responder a los ataques de forma que se mantenga la disponibilidad y confiabilidad de la red, y permitir que la empresa continúe con sus funciones. En muchos aspectos, la meta de la seguridad es crear redes más robustas haciéndolas también más *flexibles*. En lugar de sucumbir a los ataques, las redes deben tener la capacidad de absorberlos y permanecer operativas, de la misma forma que el sistema inmunológico del ser humano nos permite seguir haciendo nuestras tareas aunque hayamos contraído un virus y las infecciones bacteriales relacionadas.

Este documento describe las razones de Cisco Self-Defending Network, sus fundamentos y los métodos incrementales que Cisco Systems ha adoptado para ofrecer este conjunto de capacidades.

EL CAMBIANTE PAISAJE DE LA SEGURIDAD

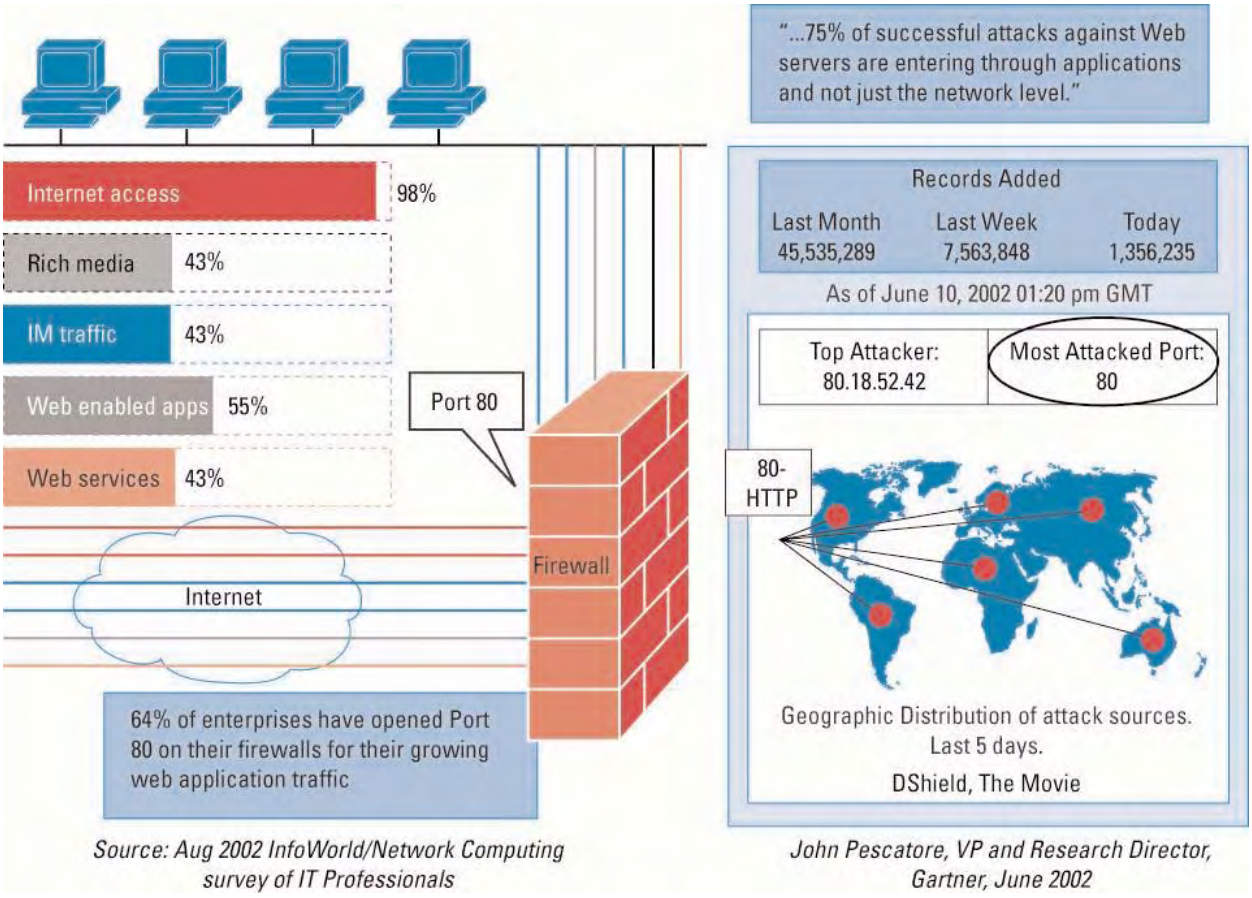
Nos guste o no, el futuro de la tecnología de la seguridad ha cambiado más en los últimos tres años que en los diez anteriores. La extensión de estos cambios, así como su dirección, ha complicado las tareas de los departamentos de seguridad TI. Antes de considerar el control, debemos comprender la evolución de este paisaje cambiante.

El perímetro de seguridad de red. Se trata de uno de los mayores cambios en la forma en que el sector enfocaba la seguridad de las redes y que ha sido resultado de un cambio en la naturaleza de las propias redes. Una red ya no puede protegerse simplemente mediante la seguridad de su perímetro de red; a medida que las empresas han ido consolidando sus centros de datos, creando redes convergentes y adoptando Internet, lo que una vez fue un entorno controlado y autocontenido está ahora abierto a los socios a través de las extranets intercorporativas, las conexiones con los puntos de venta y los empleados que trabajan en casa, por nombrar unos pocos ejemplos. Al ampliar la red de la empresa de esta forma, se amplía los limites de confianza a las redes intermediarias y a entornos no controlados. Con frecuencia, los dispositivos que se conectan a la red empresarial a través de estas rutas de acceso no son compatibles con las directivas de la empresa. Además, los dispositivos compatibles se utilizan frecuentemente para acceder a otras redes no controladas antes de conectarse a la red empresarial. Como resultado, los dispositivos de estas redes externas pueden convertirse en canales por los que llegan los ataques o los errores por el uso inadecuado.

Tecnología inalámbrica y movilidad. Relacionado con la idea de perímetro de seguridad, las redes inalámbricas y la movilidad en las empresas admiten ahora los equipos portátiles, asistentes personales (PDA) y teléfonos móviles que tienen más de una conexión de red. Estos hosts múltiples son capaces de establecer redes inalámbricas ad-hoc para habilitar la comunicación entre pares. Además, los paquetes se pueden enviar eficazmente entre los dispositivos en el nivel de la aplicación. Como resultado, es mucho más ambiguo conocer dónde empiezan o terminan los límites de una red. Las empresas necesitan ser capaces de ampliar un punto de control sobre estos dispositivos móviles a fin de administrar el sistema de forma segura y mantener la disponibilidad de la red.

Comercio electrónico, Extranets y operaciones comerciales basadas en Web. La aparición de interfaces comunes de aplicaciones basadas en protocolos de mensajería, como Extensible Markup Language (XML) y Simple Object Access Protocol (SOAP), ha significado un catalizador para el comercio electrónico y la productividad empresarial. Sin embargo, como pasa con la mayoría de las nuevas tecnologías, estos nuevos protocolos de mensajería han traído consigo un nuevo conjunto de vulnerabilidades y vectores de ataque que las empresas deben enfrentar. Los datos que antes se difundían a través de varios protocolos de red y podían filtrarse con facilidad a través de directivas de firewall, están ahora combinados dentro de unos pocos (si no uno solo) protocolos de transporte como, por ejemplo, HTTP en el puerto 80 de TCP. Como resultado, gran parte de los datos que solían residir en las cabeceras de los paquetes residen ahora en la carga útil. Esto crea importantes problemas de procesamiento que permiten a un atacante sortear con relativa facilidad las defensas clásicas de la red (Ilustración 1). Además, a fin de cumplir con los requisitos de confidencialidad e integridad de los datos empresariales, cada vez más tráfico de este nivel de aplicación se cifra a través de los protocoles SSL/TLS (Secure Socket Layer/Transport Layer Security) y HTTP Secure socket (HTTPS). Un efecto colateral de esta tendencia es que resulta mucho más difícil para los departamentos TI forzar el cumplimiento de las directivas empresariales de acceso en la red, debido a que no pueden inspeccionar la carga útil de los paquetes de estos flujos cifrados.

Ilustración 1. Las redes se enfrentan a nuevas vulnerabilidades a través del puerto 80



Virus, gusanos y el índice de propagación. El número y la variedad de virus y gusanos que han aparecido en los últimos tres años es, en si mismo, asombroso. Pero hay dos factores que tienen un enorme impacto en las empresas y su eficacia operativa: el lapso cada vez menor entre el momento en que se detecta la vulnerabilidad y el momento en que se da el ataque, y el *índice* en que estos ataques se expanden en toda la empresa. Esto ha llevado a niveles inaceptables de interrupciones en las empresas, así como a caros proyectos de recuperación que consumen tiempo, personal y fondos que no estaban originalmente presupuestados para esas tareas.

Normas de regulación. Las brechas conocidas y el comportamiento malicioso que se genera de forma interna en la empresa han exigido que los organismos de regulación de muchos sectores dicten reglas para la administración del riesgo de la información empresarial. En Estados Unidos, las normas resultantes, las más conocidas son *Sarbanes-Oxley*, *Gramm-Leach-Bliley (GLB)* y *Health Insurance Portability and Accountability Act, (HIPAA)*, han forzado cambios fundamentales en la forma en que se organizan las redes, los servidores, bases de datos y hosts empresariales.

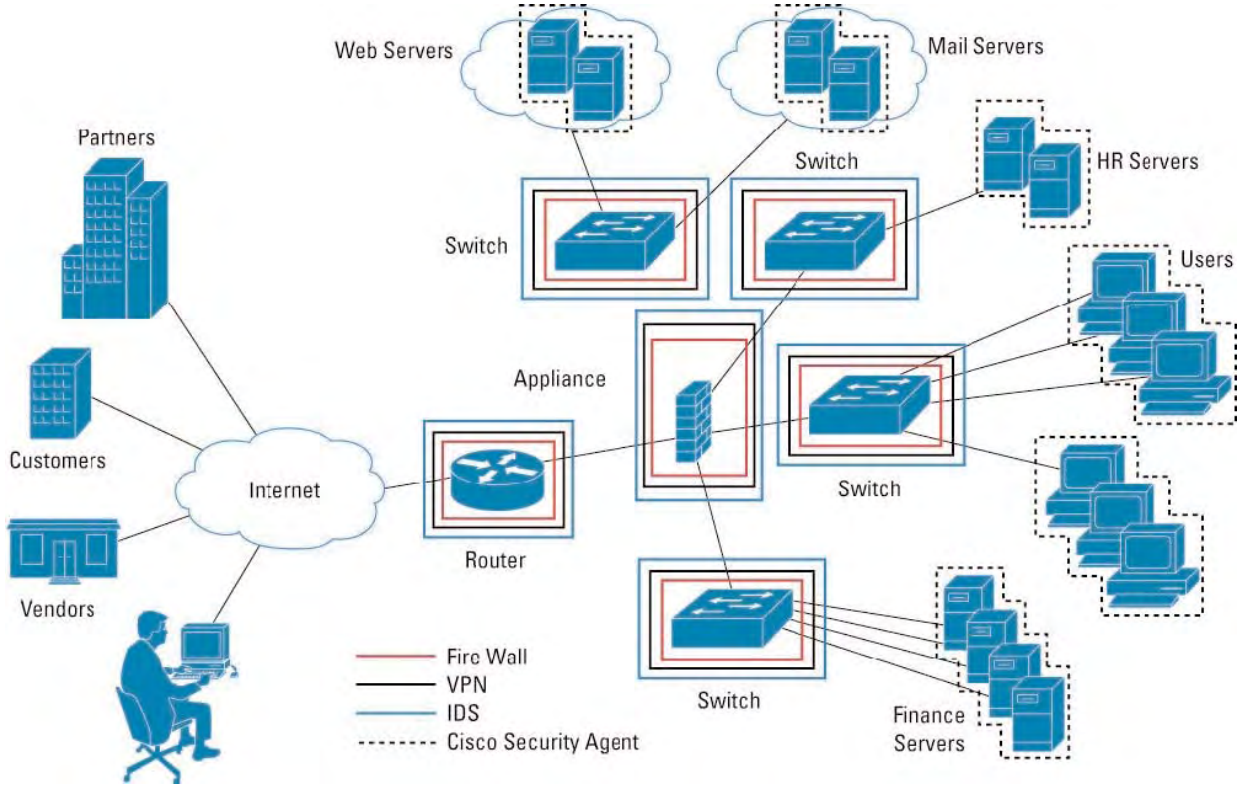
Aunque muchas organizaciones asumen de forma errónea que si cumplen con las regulaciones su infraestructura será más segura, no siempre es así. La ley de las consecuencias involuntarias hace que el propio hecho de crear una norma pueda introducir nuevas vulnerabilidades. Por ejemplo, los gusanos y virus pueden expandirse con mayor eficacia en una red que admita las VPN de extremo a extremo, dado que los nodos intermedios no tienen visibilidad del tráfico transversal. Este tráfico puede llevar gusanos a los servidores empresariales en un paquete cifrado y seguro. Además de que hacer un diagnóstico del ataque lleva un tiempo más largo, estas VPN de extremo a extremo puede dificultar la solución del problema.

PRINCIPIOS DE UNA RED MODERNA Y SEGURA

Las empresas que tratan de asumir este cambio en el paisaje de la seguridad sólo pueden adaptarse hasta cierto punto antes de que se convierta en algo operativamente inaceptable. De forma ideal, las mejoras en la seguridad deben tener un mínimo impacto en la infraestructura de enrutamiento y switching, las técnicas de control de acceso y segmentación, y las estructuras organizativas relacionadas que admiten estos sistemas. Esta sección explica los elementos fundamentales de Self-Defending Network para conseguir este objetivo: *Presencia*, *Contexto*, *Vínculación* y *Confianza*.

Presencia. Algo fundamental para un sistema seguro es el concepto de puntos de control, que se definirá como *presencia* (Ilustración 2). Así como los sistemas inmunológicos de nuestro cuerpo dependen de detectores y respondedores distribuidos por todo el cuerpo para conseguir presencia, una red depende de la disponibilidad de algunas capacidades dentro de nodos discretos de la red. Estas capacidades incluyen las tecnologías de identidad clásica, control de acceso, inspección de datos y seguridad de comunicación; así como de las más recientes capacidades orientadas a las aplicaciones, que deben hacer frente al crecimiento del contenido punto a punto, los servicios Web y el contenido móvil dinámico.

Ilustración 2. Presencia en una red con autodefensa



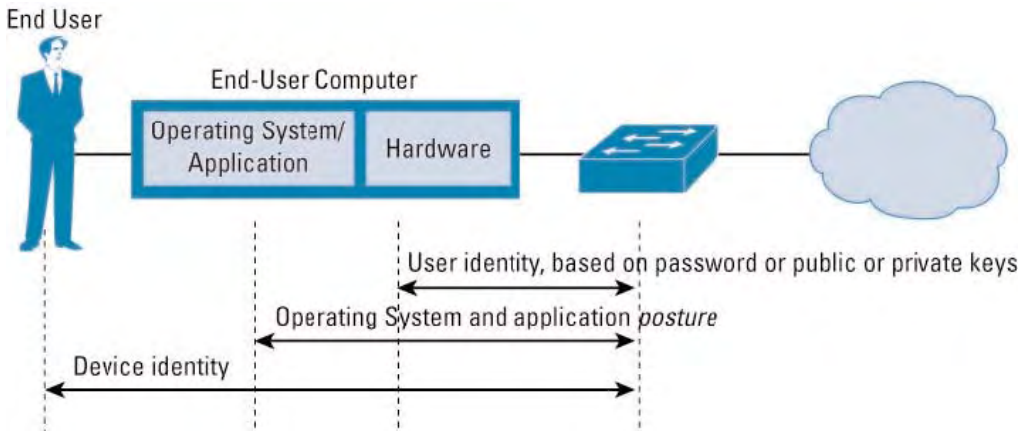
Contexto. Cuando un usuario se registra en la red, ésta solicita y obtiene acceso a un conjunto de credenciales para el usuario y el host que constituyen una *entidad* de extremo. Es importante tener en cuenta que estas credenciales pueden cambiar a lo largo del tiempo en respuesta a las acciones del host durante el periodo de conexión a la red. En conjunto, esta información representa el *contexto*. En tanto que los sistemas de seguridad de red actuales tienden a centrarse sólo en los permisos para el momento en que el usuario entra a una red, una red con autodefensa concede o revoca los permisos basándose en los cambios en el comportamiento y el contexto asignado durante la asociación de la entidad con la red. Por ejemplo, si la red detecta que un virus ha infectado un host, reacciona poniendo en cuarentena al host en un segmento de reparación de la red. Debido a que la información se puede falsificar, es posible que asegurar un sistema requiera obtener el contexto de otros sistemas, a fin de evaluar con precisión los derechos y privilegios del host en un momento dado.

Vinculación. Los nexos entre las entidades discretas es lo que permite compartir un contexto y crear un "sistema". Tradicionalmente, las redes han establecido vinculaciones entre los dispositivos a través de protocolos de enrutamiento como Border Gateway Protocol (BGP). A fin de hacer frente a las más recientes formas de amenazas y uso inadecuado, debemos ampliar estas vinculaciones de red hasta el origen y el destino del tráfico de la red. Además, dada una continua presencia de dispositivos móviles con múltiples redes, estas vinculaciones han empezado a sobrepasar las demarcaciones que hasta hace poco se veían como externas al ámbito de las redes tradicionales. Los privilegios que recibe una entidad cuando entra en una red y cómo cambian a lo largo de la duración de esa conexión, están estrechamente relacionados con el contexto de esa entidad y sus vinculaciones en una red o redes.

Confianza. Un sistema seguro es tan bueno como la información que se pone en él, y funciona mucho más eficazmente cuando está acompañado de relaciones de plena *confianza*. En el pasado, la confianza dependía principalmente de la identidad del dispositivo o usuario. Los avances recientes han demostrado que los sistemas seguros deben ampliarse para incluir la comprensión del estado o *postura* y la ubicación de un dispositivo.

En muchos aspectos, las actividades de los usuarios y dispositivos dentro de una red se pueden comparar a como se conduce un automóvil por una carretera. Al obtener el permiso de conducir que nos permite manejar cierta clase de vehículo, los usuarios deben poseer algún tipo de identidad a fin de unirse a una red. Así como el coche contiene un número de identificación de vehículo que debe registrarse en el ayuntamiento correspondiente, una red y los dispositivos extremo dispondrán pronto de un certificado digital instalado en el momento de la fabricación y se les requerirá algún tipo de registro cuando se implemente en una empresa. Sin embargo, debido a que las credenciales apropiadas no siempre están presentes en una ubicación determinada o en un momento concreto, una red con autodefensa utiliza métodos innovadores de *confianza inferida* y *máximo esfuerzo* para identificar y autorizar a una entidad. Como mínimo, una red con autodefensa debe ser capaz de adquirir credenciales para cada identidad de dispositivo o usuario, debe poder evaluar la postura del dispositivo y determinar la ubicación del dispositivo en el entorno (Ilustración 3). La tecnología necesaria para hacer esto será necesariamente ubicua y se habilitará a través de formatos de mensaje y protocolos bien definidos y basados en estándares, como los métodos 802.1x y Extensible Authentication Protocol (EAP).

Ilustración 3. Las credenciales son fundamentales para la seguridad de la red



Ninguno de estos conceptos resulta especialmente valioso por sí solo. No obstante, logran ser altamente eficaces cuando se combinan en una red con autodefensa. En el resto del documento, mostraremos algunas de las formas cómo estos conceptos funcionan dentro del modelo Self-Defending Network.

LA NECESIDAD DE SELF-DEFENDING NETWORK

Las redes empresariales, y los métodos que se usan para atacarlas, no son tan complejos, pero tampoco es posible depender de un solo mecanismo para mantenerlas seguras. Esto nos ha llevado al concepto de "defensa en profundidad". Hasta hace poco, este concepto se había basado en la noción de *defensas proactivas*. Sin embargo, dado el tipo de vulnerabilidades y ataques que han surgido en las redes en continuo cambio, Cisco Systems cree que es necesaria la construcción de defensas adaptativas. Como resultado, Cisco ha empezado a buscar ejemplos relacionados con el mundo real, como nuestro sistema inmunológico, a fin de utilizarlos como modelo para Self-Defending Network. Otros sistemas del mundo real que también se han mostrado instructivos pueden encontrarse en el campo de la epidemiología y en la forma en que las comunidades se protegen a sí mismas. Un tema común en todos estos sistemas es que emplean defensas ***adaptativas*** y ***proactivas***.

Si llevamos esta observación un paso más allá, las defensas para salvaguardar un sistema de esta naturaleza tienden a construirse en bloques funcionales. Las capacidades principales de estas defensas adaptativas son que:

- Permanecen constantemente activas
- Se ejecutan de forma no obstrusiva
- Minimizan la propagación de los ataques
- Responden con rapidez a ataques aún no conocidos

Estos sistemas se basan en la premisa de que esos recursos son finitos y deben utilizarse cuidadosamente para evitar el agotamiento de los recursos. También se han diseñado para usar de forma óptima la infraestructura actual con un mínimo de interrupciones en las operaciones del cliente TI.

Self-Defending Network de Cisco Systems *ofrece soluciones basadas en sistemas que permiten a los usuarios utilizar su infraestructura de forma novedosa para reducir los espacios de vulnerabilidad, minimizar el impacto de los ataques y mejorar la disponibilidad y confiabilidad global de la infraestructura. También ayuda a crear sistemas autónomos que pueden reaccionar rápidamente ante un ataque con poca o ninguna intervención humana. Este tipo de respuesta rápida permite contrarrestar las formas más recientes de uso indebido, mucho más virulentas que las anteriores.*

Cisco Self-Defending Network continúa mejorando su capacidad de responder a las nuevas amenazas. La primera fase, **Integrated Security**, incorpora elementos de seguridad en los elementos de red como los switches y los routers. La segunda fase, **Collaborative Security**, implica la construcción de nexos entre los elementos de seguridad y la extensión de la presencia de la red más allá de los extremos que se conectan a una red. La última fase de Cisco Self-Defending Network presenta las capacidades **Adaptive Threat Defense (ATD)**, que mejoran la capacidad de una red para responder a las amenazas basándose en un nuevo conjunto de tecnologías *Anti-X*.

LOS BLOQUES DE CONSTRUCCIÓN DE SELF-DEFENDING NETWORK

La mayoría de los clientes no adoptarán todos los componentes de Cisco Self-Defending Network de una vez, ya que puede ser difícil revisar todos los subsistemas necesarios de forma inmediata y sin causar interrupciones en la integridad de los servicios TI. Es posible que algunos clientes duden en cambiar sus controles de seguridad por un sistema automatizado hasta que no logren convencerse plenamente en que el sistema funciona de forma fiable. La iniciativa Cisco Self-Defending Network solventa estas preocupaciones mediante, primero, la oferta de productos que pueden implementarse útilmente de modo independiente unos de otros y, después, proporcionando soluciones que vinculen estos productos, a medida que cada producto y subsistema establezca un entorno de confianza: un método eficaz que se basa en una combinación de desarrollo y adquisición de productos, desarrollo de sistemas y asociación. Teniendo esto en cuenta, vale la pena revisar los hitos principales de la iniciativa Cisco Self-Defending Network hasta la fecha.

Protección del extremo. Una de las realidades de virus y gusanos es que, con frecuencia, crean congestión de red como un producto derivado de rápida propagación, así como infecciones de los extremos. Cisco determinó que ambos problemas podían solventarse ofreciendo a sus clientes un método de prevención de intrusiones denominado Cisco Security Agent. Cisco Security Agent utiliza formas nuevas de seguridad de comportamiento para detectar los virus y gusanos, y evitar que establezcan una cabeza de puente en un extremo y, a partir de ahí, puedan propagarse por toda la red. En efecto, Cisco Security Agent se convierte en un *amortiguador de primer orden* para el efecto de propagación de virus y gusanos.

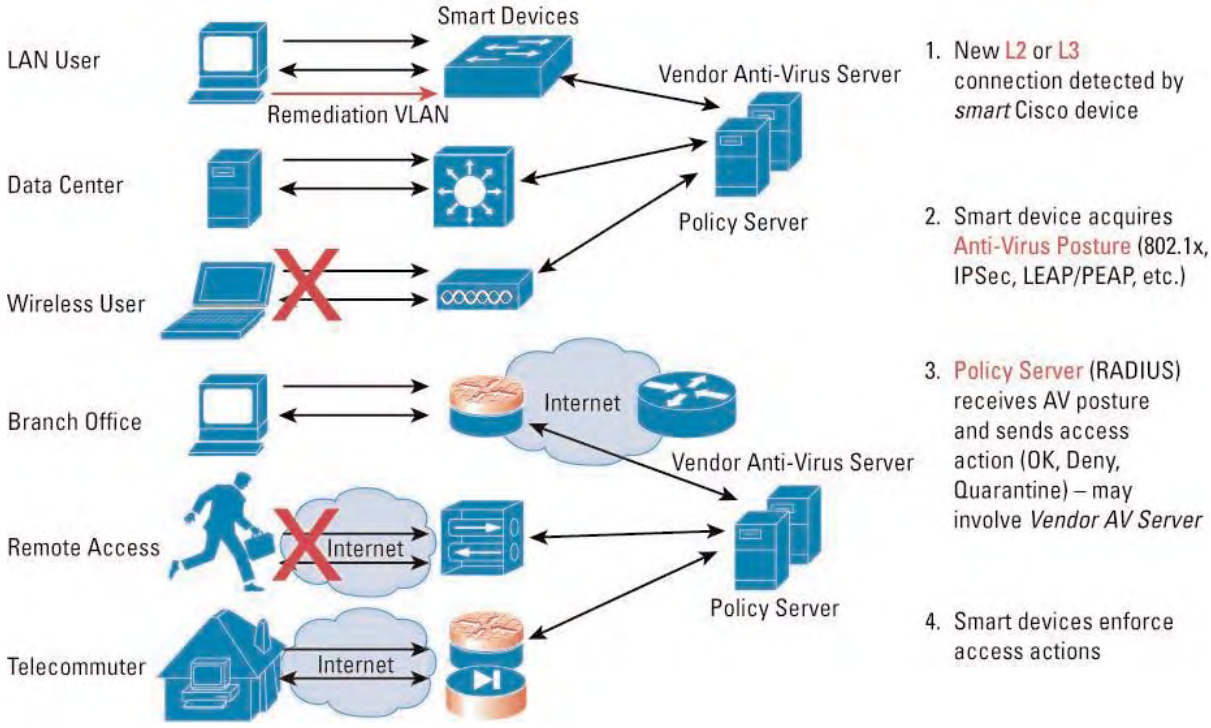
Una segunda y atractiva razón para la implementación de Cisco Security Agent es que establece una presencia en los extremos que se puede utilizar para desplegar un bucle de retroalimentación entre el extremo y la red, dando como resultado un red que se adapte rápidamente a las amenazas emergentes.

Control de admisión. Hasta la fecha, una de las iniciativas de perfil alto de Cisco Self-Defending Network es el programa Cisco Network Admission Control (NAC). NAC permite a los clientes determinar qué niveles de acceso de red desean conceder a un extremo basándose en su *postura* de seguridad, la cual se basa en el estado de seguridad del sistema operativo y las aplicaciones asociadas. Además de controlar el acceso, NAC proporciona a los administradores TI una forma de poner en cuarentena y reparar los extremos no compatibles. Garantizar que los extremos son compatibles con los parches SO y las actualizaciones del software antivirus es un eficaz *amortiguador de segundo orden* ante el efecto de propagación de gusanos y virus. Otra forma de considerar NAC es como una herramienta de evaluación de vulnerabilidades y de administración de parches *bajo demanda*.

Una característica especial de NAC es que proporciona interfaces de cliente y AAA respaldadas que permiten a los clientes conectarse a productos de sus proveedores favoritos de directivas y seguridad de extremo, a fin de determinar el plan de NAC.

Actualmente, más de 30 proveedores líderes del sector han integrado NAC de forma activa en sus tecnologías.

Ilustración 4. Control de admisión en la red



Es importante ampliar la capacidad de NAC a las pequeñas y medianas empresas (PYME). Para este fin, Cisco ha adquirido recientemente Perfigo, Inc., un desarrollador de paquetes de soluciones de control de acceso de red que proporciona capacidad de análisis de directivas, compatibilidad y control de acceso de extremo, y ahora ofrece un paquete de soluciones bajo el nombre de Cisco Clean Access para este segmento del mercado.

Contención de la infección. Las robustas directivas de admisión no lo curan todo ni eliminan la necesidad de continuar supervisando los dispositivos una vez que entran en la red. Algunos atacantes pueden evadir cualquier comprobación de admisión y la red no siempre puede depender, o *confiar*, en que un elemento infectado se delate a sí mismo. Los dispositivos que cumplen las normativas también se pueden infectar a través de una variedad de factores una vez que se ha hecho miembros de una red; por ejemplo, una llave USB con contenido infectado. Para una mayor protección de la red, Cisco Self-Defending Network se ha diseñado para ampliar las comprobaciones de seguridad que se ejecutan en el momento de la admisión a toda la duración de una conexión de red. Además, Self-Defending Network puede depender de otros elementos de la red, incluyendo *otros* extremos, para la detección cuando un extremo (o extremos) no resulta ya confiable; así como la fuerza policial supervisa la delincuencia en una comunidad a través de un centro de llamadas 911. Cisco considera la contención de la infección como un *amortiguador de tercer orden* ante el efecto de propagación de virus y gusanos.

Sin embargo, los protocolos actuales de autenticación no se han diseñado para trabajar más allá del intercambio inicial. Es por esto que Self-Defending Network debe ofrecer nuevas formas de comunicar el estado de un dispositivo (contexto) y nuevos métodos de medir la veracidad de esa información basándose en formas directas e inferidas de confianza. Por ejemplo, un administrador puede crear una regla que determine que la notificación recibida desde un extremo que ejecute Cisco Security Agent es más confiable que una notificación de un extremo no protegido. Como resultado, Cisco ha empezado el desarrollo de nuevos tipos de correlación y retroalimentación que se basan en atributos inferidos.

Correlación inteligente y respuesta a las incidencias. A fin de que mecanismos de retroalimentación de régimen permanente, como la contención de infecciones, funcionen de forma eficaz, Self-Defending Network necesita proporcionar servicios como la correlación en tiempo real de eventos, la evaluación rápida del impacto de seguridad de un evento, la capacidad de decidir qué acción llevar a cabo, la capacidad de identificar el punto de control de acceso más cercano para la implementación de una respuesta, etc. Para esto, Cisco anunció recientemente la adquisición de Protego Networks, cuya familia de productos MARS ofrece métodos para superponer la retroalimentación de una variedad de puntos de presencia (POP) de la red (firewalls, sistemas de detección de intrusiones [NIDS], routers, switches y hosts) con el contexto que se obtiene del aprendizaje de la topología de red L2 y L3. Esta capacidad ayuda a que el equipo de respuesta a los incidentes de seguridad identifique con rapidez el lugar de la red donde se realizan los ataques.

Cisco trabaja también con netForensics y otros partners para mejorar sus capacidades de correlación y la auditoria de Self-Defending Network.

IDS en línea y detección de anomalías. Un área importante en el desarrollo de la seguridad continua en Cisco ha sido el área de sistemas de detección de intrusiones (NIDS). Una de las primeras innovaciones de Cisco en este área fue integrar NIDS en sus plataformas de conmutación y routers. Sin embargo, para que NIDS consiga ofrecer con eficacia todas sus capacidades, es necesario trasformarlo en un sistema de *prevención de intrusiones* (IPS) con capacidades de filtrado en línea. Esto proporciona un mecanismo para eliminar el tráfico no deseado con sofisticados motores de clasificación programable.

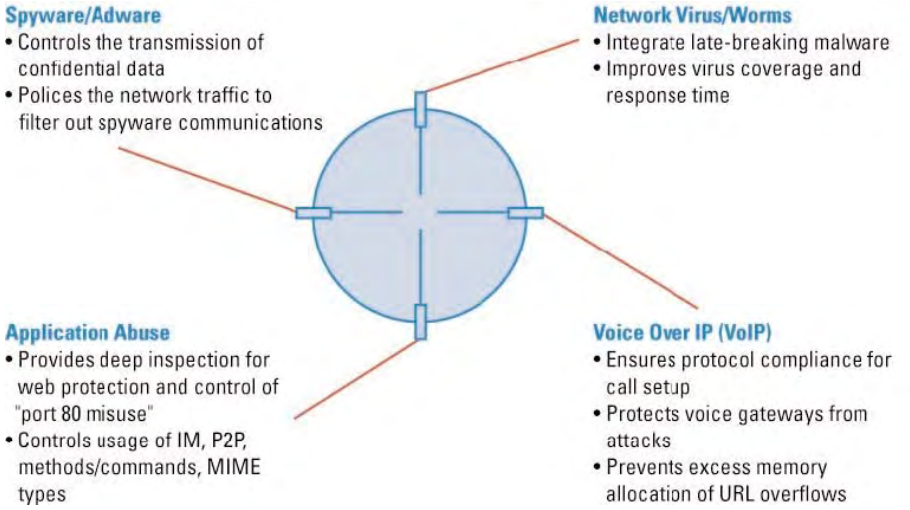
Por desgracia, la mayoría de NIDS generan demasiados falsos positivos como para funcionar de forma confiable como servicios de seguridad en línea. Parte del problema es que se debe ensamblar y procesar una gran cantidad de información (contexto) dentro de un lapso temporal relativamente corto, es particular, con la cantidad de contexto que se acumula con los protocolos basados en aplicaciones. Esto resulta especialmente cierto con aplicaciones de telefonía IP, que son muy sensibles a los retrasos en la transmisión de los paquetes. Para solventar este problema, Cisco está desarrollando varios métodos que ofrecen señalización de alta fidelidad a estos motores de clasificación en línea.

Muchas actividades legítimas pueden ser consideradas erróneamente como anómalas por la red, sobre todo en redes donde el número de variables es significativo. Como resultado, Cisco ha adoptado intencionalmente un método conservador e incremental para la detección de anomalías, empezando con Cisco Security Agent, debido a la certeza de que los sistemas operativos son más sencillos de modelar que los entornos de red. Cisco adquirió Riverhead, un sistema de prevención en línea que presentaba bajos índices de falsos positivos debido a que la actividad de denegación de servicio (DoS) se diferencia claramente de cualquier otra actividad de red. Los ataques DoS se pueden identificar con mayor precisión mediante el despliegue de la tecnología de Cisco que proviene de la adquisición de la red Riverhead. El resultado son índices bajos de falsos positivos en la identificación de un ataque DoS.

Basándose en la lección aprendida de Cisco Security Agent y las capacidades DoS adquiridas con la familia de productos DoS Guard de Riverhead, Cisco ha presentado un IPS que reduce el índice de falsos positivos a través de la aplicación de innovadoras técnicas de detección de anomalías y el uso compartido del estado (contexto) entre los extremos y los elementos de red (nexos). También ofrece identificación de amenazas multivector y correlación de meta-eventos para la evaluación rápida de vulnerabilidades y ataques. Mediante la introducción incremental de estas tecnologías en el mercado, Cisco establece una mayor confianza del cliente en sus capacidades y, por extensión, en las redes con sistemas de autodefensa.

Seguridad de aplicaciones y defensa anti-X. A lo largo de los años anteriores, han aparecido un número de nuevos productos de red de la capa de aplicación que sirven de ayuda para tratar nuevas clases de amenazas que no se resolvían adecuadamente mediante los productos firewall y NIDS clásicos, incluyendo *virus y gusanos*, *SPAM basado en correo electrónico* y *"phishing"*, *spyware*, *abuso de servicios Web*, *abuso de telefonía IP* y *actividad no autorizada punto a punto* (Ilustración 5). Cisco ha desarrollado la nueva generación de servicios de seguridad de inspección de paquetes y contenido para tratar este tipo de amenazas y uso inadecuado. Esta convergencia ofrece servicios de inspección de tráfico granulares en puntos cruciales de la seguridad de red, a fin de contener el tráfico malintencionado antes de que se propague a través de la red.

Ilustración 5. Mejoras en la seguridad a través de la identificación de amenazas multivector y anti-X



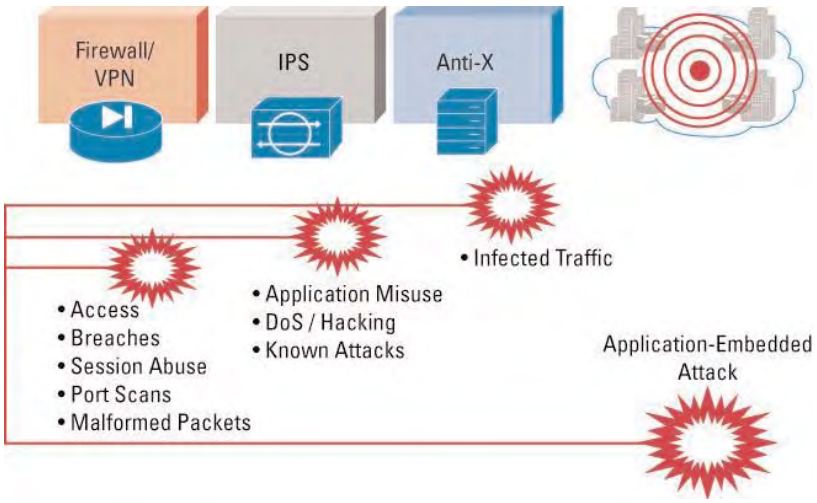
La consolidación de estos servicios en varias plataformas multiservicio representa una oportunidad de innovación para los fabricantes, así como la reducción de los costes de propiedad de los clientes. Self-Defending Network también estará mejor preparada para las aplicaciones una vez que estos servicios se integren dentro de su modelo.

Tenga en cuenta que cuando estas aplicaciones emplean cifrado de extremo a extremo, Self-Defending Network puede recopilar información desde los extremos para compensar la pérdida de visibilidad en el borde de la red.

PASOS SIGUIENTES

Cisco continuará realizando grandes inversiones en la construcción de las redes con autodefensa que crean nexos entre los POP a lo largo de todas las redes e incluyendo los sistemas de extremo (Ilustración 5). Con esto, Cisco ayuda a que las organizaciones obtengan una mayor visibilidad y control de los dispositivos, usuarios y aplicaciones que se comunican a través de sus infraestructuras. Es una evolución necesaria e importante de lo que se considera una red clásica, así como la introducción de protocolos inteligentes de enrutamiento lo fueron con respecto a la distribución de paquetes a través del tejido de comunicaciones.

Ilustración 6. Cisco continúa desarrollando las capacidades de una red con autodefensa



La breve descripción de Cisco Self-Defending Network que ofrece este documento debe examinarse con mayor profundidad, tanto para obtener una comprensión más detallada de lo que es posible hacer actualmente, como para establecer los fundamentos de seguridad en los proyectos de diseño de redes. La elección que haga cada organización dependerá de los problemas de seguridad, riesgo y compatibilidad que enfrentan:

- Para el personal de seguridad de perímetro, las nuevas plataformas Cisco PIX® 7.0 Firewall e Integrated Service Router ofrecen control e inspección detallada de datos a través de una amplia variedad de protocolos y sus factores de ataque respectivos, así como otras características de seguridad y red.
- Los grupos de operaciones de seguridad que emplean un enorme esfuerzo en responder a los incidentes deben investigar la nueva tecnología que proviene de Protego, así como aprender más sobre las nuevas capacidades de la protección de intrusiones en línea en la infraestructura y los dispositivos de seguridad.
- Los responsables de entornos de uso intensivo de datos que enfrentan constantemente ataques de DoS y DDoS deben revisar la tecnología Anomaly Guard adquirida de Riverhead.
- Las organizaciones que continúan sufriendo los ataques de gusanos y virus, o para aquellas que requieren de soluciones de compatibilidad de extremo, deben examinar las soluciones Cisco Security Agent, Network Admission Control y Cisco Clean Access que se han adquirido de Perfigo.
- Los auditores responsables de evaluar el cumplimiento de las regulaciones deben investigar NAC, así como CiscoWorks Security Information Management System (SIMS), una herramienta que proporciona información detallada con relación al uso de toda la infraestructura de comunicación.

Finalmente, los profesionales TI responsables del diseño e implementación de los sistemas de seguridad y la infraestructura de red, deben contactar con su representante de Cisco para obtener más detalles sobre las redes con autodefensa y cómo pueden tener un impacto positivo en el entorno TI.

Sede central
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
EE.UU.
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Sede en Europa
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
Países Bajos
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Sede en América
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
EE.UU.
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Sede en Asia Pacifico
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems tiene más de 200 oficinas en los siguientes países y regiones.
Las direcciones, números de teléfono y de fax se pueden encontrar en el
sitio Web Cisco.com en www.cisco.com/go/offices.

Alemania • Arabia Saudí • Argentina • Australia • Austria • Bélgica • Brasil • Bulgaria • Canadá • Chile • China • Chipre • Colombia • Corea • Costa Rica • Croacia • Dinamarca • Dubai, EAU • Escocia • Eslovaquia • Eslovenia • España • Estados Unidos • Filipinas • Finlandia • Francia • Grecia • Hong Kong o Hungría • India • Indonesia • Irlanda • Israel • Italia • Japón • Luxemburgo • Malasia • México • Noruega o Nueva Zelanda • Países Bajos • Perú • Polonia • Portugal • Puerto Rico o Reino Unido • República Checa • Rumanía • Rusia • Singapur o Sudáfrica • Suecia • Suiza • Tailandia • Taiwán • Turquía • Ucrania • Venezuela • Vietnam • Zimbabue

Impreso en Estados Unidos