INFORME

Cisco SAFE:
Un modelo de seguridad para las redes de las empresas

ÍNDICE

INFORME

Cisco SAFE: Un modelo de seguridad para las redes de las empresas

Autores

Los autores de este informe son Sean Convery (CCIE nº 4232) y Bernie Trudel (CCIE nº 1884). El primero es el arquitecto jefe de la implementación de referencia de esta arquitectura en las oficinas centrales de Cisco en San Jose, California (EE.UU). Ambos son miembros del equipo de marketing técnico de las arquitecturas de VPN y de seguridad de la línea empresarial de negocios de Cisco.

Resumen

El objetivo principal del modelo de seguridad para redes de empresas (SAFE) de Cisco es ofrecer información sobre las mejores prácticas a las partes interesadas en el diseño e implementación de redes seguras. SAFE sirve de guía a los diseñadores de red que están planteándose los requisitos de seguridad de su red. SAFE adopta un enfoque de defensa en profundidad para el diseño de la seguridad de las redes. Este tipo de diseño se centra en las amenazas que se esperan y en sus medios para combatirlas, en lugar de en "Coloque aquí el firewall o ponga allí el sistema de detección de intrusos". El resultado de esta estrategia es un enfoque por capas de la seguridad, donde no es probable que el fallo de un sistema de seguridad ponga en peligro los recursos de la red. SAFE se basa en los productos de Cisco y en los de sus empresas asociadas.

Este documento comienza con una descripción de la arquitectura y, a continuación, detalla los módulos específicos que conforman el diseño real de la red. Las tres primeras secciones de cada módulo describen los flujos de tráfico, los dispositivos clave y las amenazas que se esperan con diagramas de soluciones básicas. Después encontrará un análisis técnico del diseño, junto con más técnicas para combatir las amenazas y estrategias de migración. El anexo A explica con detalle el laboratorio de validación de SAFE e incluye instantáneas de configuraciones. El anexo B es un manual sobre la seguridad de redes. Es aconsejable que los lectores que no conozcan los conceptos básicos de seguridad de redes lean esta sección antes que el resto del documento. El anexo C contiene un glosario con definiciones de los términos técnicos empleados en este documento y una leyenda de las figuras que se incluyen.

Este documento se centra principalmente en las amenazas encontradas en los entornos empresariales. Los diseñadores de redes que conocen estas amenazas pueden decidir mejor dónde y cómo instalar las tecnologías antivirus. Sin un conocimiento completo de las amenazas implicadas en la seguridad de redes, las instalaciones tienden a configurarse incorrectamente, están muy centradas en los dispositivos de seguridad o la carencia de opciones de respuesta ante las amenazas. Al adoptar el método de combate de amenazas, este documento debería ofrecer a los diseñadores de redes información suficiente para tomar decisiones sólidas con respecto a la seguridad de las redes.

Público objetivo

Aunque la naturaleza de este documento es técnica, cada lector puede leerlo con diferentes niveles de detalle. Por ejemplo, un administrador de redes puede leer las secciones introductorias de cada área para lograr una buena perspectiva general de las estrategias y las consideraciones sobre el diseño de la seguridad de las redes. Un ingeniero o diseñador de redes puede leer todo el documento y obtener información sobre diseño y detalles de los análisis de las amenazas, que están respaldados por la información de la configuración de los dispositivos implicados.

Advertencias

En este documento se supone que ya tiene instalada alguna normativa de seguridad. Cisco Systems no recomienda instalar tecnologías de seguridad sin ninguna normativa asociada. Este documento afronta directamente las necesidades de las empresas grandes. Aunque la mayoría de los principios explicados aquí se aplican directamente a pequeñas y medianas empresas, e incluso a teletrabajadores, lo hacen a otra escala. El análisis detallado de estos tipos de empresas está fuera del ámbito de este documento. Sin embargo, para solucionar el problema en redes de menor escala de forma limitada, las secciones "Alternativas" y "Opciones para empresas" muestran los dispositivos que se pueden eliminar si se desea reducir el coste de la arquitectura.

El hecho de seguir las directrices de este documento no garantiza un entorno seguro ni que se puedan evitar absolutamente todos los intrusos. La verdadera seguridad absoluta sólo se puede lograr desconectando el sistema de la red, cubriéndolo con hormigón y guardándolo en el sótano de Fort Knox. Sus datos serán totalmente seguros, pero no podrá acceder a ellos. Sin embargo, puede lograr una seguridad razonable estableciendo una buena normativa de seguridad, siguiendo las directrices de este documento, estando al día de los desarrollos más recientes de las comunidades de hackers y de seguridad, y manteniendo y controlando todos los sistemas con prácticas sólidas de administración de sistemas. Esto incluye el conocimiento de los problemas de seguridad de aplicaciones que no se explican exhaustivamente en este informe.

Aunque las redes virtuales privadas (VPN) se incluyen en esta arquitectura, no se describen con gran detalle. No se incluye determinada información, como los detalles de las ampliaciones, las estrategias de resistencia y otros temas relacionados con las VPN. Igual que sucede con las VPN, las estrategias de identidad (incluyendo las autoridades de certificación [CA]) no se explican en este informe con ningún nivel de detalle. De igual forma, las CA requieren un nivel de atención que este documento no puede proporcionar, sin dejar de afrontar correctamente las restantes áreas importantes de seguridad de las redes. Además, dado que las redes de la mayoría de las empresas instalan entornos de CA totalmente funcionales, es importante explicar cómo instalar de forma segura redes sin ellos. Por último, determinadas aplicaciones y tecnologías de red avanzadas (como las redes de contenidos, el almacenamiento en caché y el balanceo de carga de los servidores) no están incluidas en este documento. Aunque se espera que se utilicen en SAFE, este artículo no cubre sus necesidades de seguridad específicas.

SAFE usa los productos de Cisco Systems y de sus empresas asociadas. Sin embargo, este documento no hace referencia de forma específica a los productos por nombre. Más bien, se hace referencia a los componentes por su función, en lugar de por su número de modelo o nombre. Durante la validación de SAFE, los productos reales se configuraron en la implementación de red exacta que se describe en este documento. Las instantáneas específicas de la configuración se incluyen en el anexo A, "Laboratorio de validación".

A lo largo de todo el documento, el término "hacker" señala a un individuo que intenta lograr acceso no autorizado a los recursos de las redes con intenciones perversas. Aunque por lo general el término "cracker" se considera la palabra más precisa para este tipo de personas, aquí utilizamos hacker para facilitar la lectura y comprensión.

Visión general de la arquitectura

Fundamentos del diseño

SAFE emula todo lo posible los requisitos funcionales de las actuales redes empresariales. Las decisiones de implementación variaron en función de la funcionalidad necesaria de la red. Sin embargo, los siguientes objetivos de diseño, mostrados en orden de prioridad, guiaron el proceso de toma de decisiones:

- Seguridad y defensa contra ataques basadas en normativas.
- Implementación de la seguridad en toda la infraestructura (no solamente en los dispositivos de seguridad especializados).
- Gestión y generación de informes seguros.
- Autenticación y autorización de usuarios y administradores a los recursos más importantes de la red.
- Detección de intrusos en los recursos y las subredes más importantes.
- Compatibilidad con las aplicaciones de red emergentes.

Lo primero y más importante es que SAFE es una arquitectura de seguridad. Debe evitar que la mayor parte de los ataques afecten a los recursos de red más valiosos. Los ataques que consiguen traspasar la primera línea de defensa o que parten desde dentro de la red deben detectarse con precisión y contenerse rápidamente para minimizar su efecto en el resto de la red. Sin embargo, además de ser segura, la red debe seguir ofreciendo todos los servicios que los usuarios esperan de ella. Es posible ofrecer al mismo tiempo una buena seguridad y funcionalidad de red. La arquitectura SAFE no es una forma revolucionaria de diseñar redes, sino meramente un modelo para asegurarlas.

SAFE también es resistente y ampliable. La resistencia de las redes incluye redundancia física que las protege de los fallos de los dispositivos debidos a una configuración errónea, a un fallo físico o a un ataque a la red. Aunque es posible realizar diseños más sencillos, sobre todo si la red no necesita un rendimiento excelente, este documento emplea un diseño complejo como ejemplo, ya que diseñar la seguridad de entornos complejos es más complicado que hacerlo en entornos simples. En este documento se explican las opciones para limitar la complejidad del diseño.

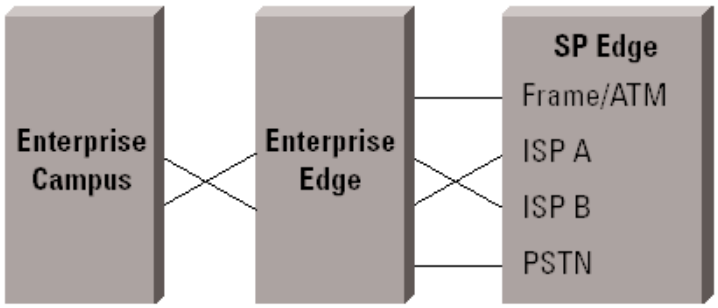
En muchas etapas del proceso de diseño de la red hace falta escoger entre utilizar una funcionalidad integrada en un dispositivo de la red o utilizar un dispositivo con funciones especializadas. A menudo la funcionalidad integrada es atractiva, ya que puede implementarse en el equipo existente o porque las características pueden interoperar con el resto del dispositivo para ofrecer una solución más funcional. Los dispositivos se suelen utilizar cuando la profundidad de la funcionalidad necesaria es muy avanzada o cuando las necesidades de rendimiento exigen el uso de hardware especializado. Tome las decisiones en función de la capacidad y funcionalidad del dispositivo, en lugar de en función del beneficio que produce su integración. Por ejemplo, a veces puede elegir un router Cisco IOS™ integrado de mayor capacidad con el software de firewall de IOS en lugar del router IOS con un firewall independiente, que es más pequeño. En esta arquitectura se emplean ambos sistemas. La mayor parte de las funciones de seguridad más importantes migran a dispositivos dedicados debido a los requisitos de rendimiento de las redes de las empresas grandes.

Concepto de módulos

Aunque las redes de la mayoría de las empresas evolucionan con los crecientes requisitos de tecnologías de información de la empresa, la arquitectura SAFE utiliza un enfoque modular green-field. El enfoque modular tiene dos ventajas principales. En primer lugar, permite a la arquitectura afrontar la relación de seguridad entre los distintos bloques funcionales de la red. Y, en segundo lugar, permite a los diseñadores evaluar e implementar la seguridad módulo a módulo, en lugar de intentar completar la arquitectura en una sola fase.

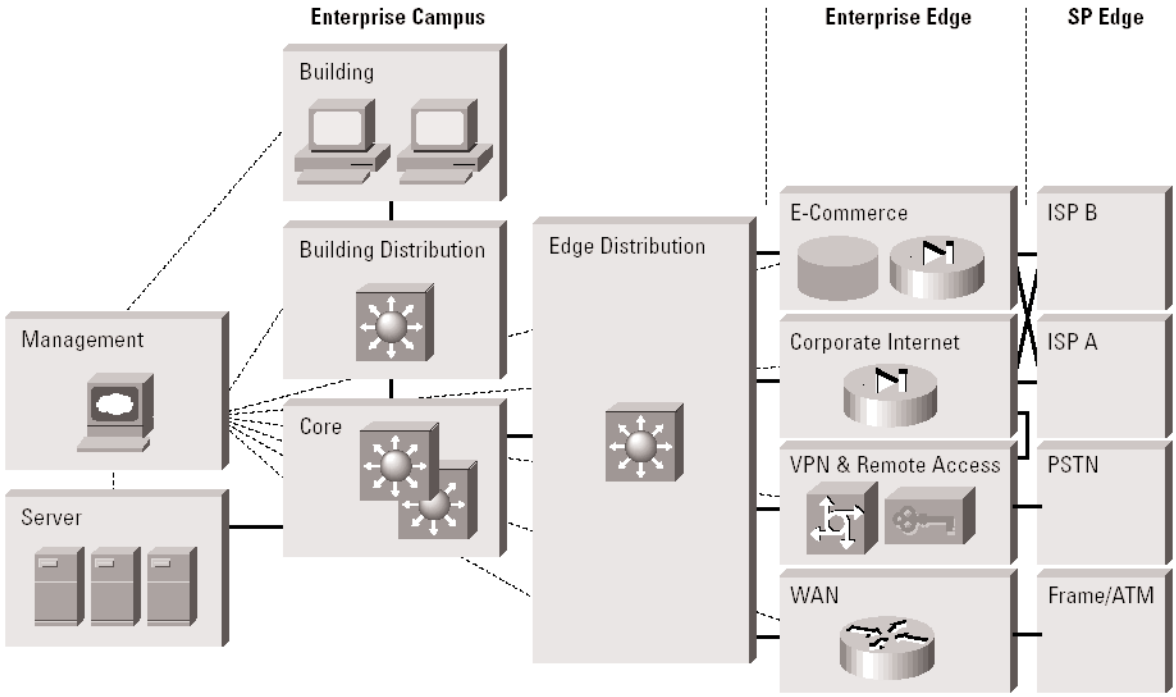
La ilustración 1 muestra la primera capa de modularidad de SAFE. Cada bloque representa un área funcional. El módulo del proveedor de servicios de Internet (ISP) no lo implementa la empresa, sino que está incluido hasta el punto de que para combatir ciertos ataques habría que pedir determinadas características de seguridad al ISP.

Ilustración 1 Módulo compuesto de la empresa



La segunda capa de modularidad, que se muestra en la ilustración 2, representa una vista de los módulos de cada área funcional. Estos módulos realizan funciones específicas en la red y tienen unos requisitos de seguridad específicos, pero sus tamaños no parecen preparados para reflejar su escala en una red real. Por ejemplo, el módulo del edificio, que representa los dispositivos de los usuarios finales, puede incluir un ochenta por ciento de los dispositivos de red. El diseño de la seguridad de cada módulo se describe por separado, pero se valida como parte del diseño de toda la empresa.

Ilustración 2 Diagrama de bloques de SAFE de la empresa



Si bien es cierto que las redes existentes en la mayor parte de las empresas no se pueden diseccionar fácilmente en módulos tan limpios, este enfoque proporciona una guía para implementar distintas funciones de seguridad en toda la red. Los autores no esperan que los ingenieros de red diseñen sus redes idénticas a la implementación de SAFE, sino que utilicen una combinación de los módulos descritos y los integren en la red existente.

Axiomas de SAFE

Los routers son el objetivo

Los routers controlan el acceso desde cada red a cada red. Anuncian redes y filtran quiénes pueden utilizarlas, y son potencialmente los mejores amigos de los hackers. La seguridad de los routers es un elemento crítico de cualquier instalación de seguridad. Por su naturaleza, los routers proporcionan acceso y, por consiguiente, hay que asegurarlos para reducir la posibilidad de que se pongan directamente en peligro. Puede consultar otros documentos que se han escrito acerca de la seguridad de los routers. Estos documentos ofrecen más información sobre los siguientes temas:

- Bloqueo del acceso por telnet a un router.
- Bloqueo del acceso por el protocolo Simple Network Management Protocol (SNMP) a un router.
- Control del acceso a un router a través del uso de Terminal Access Controller Access Control System Plus (TACACS+).
- Desactivación de los servicios no necesarios.
- Registro a los niveles apropiados.
- Autenticación de las actualizaciones del enrutamiento.

El documento más actual sobre la seguridad de routers se puede encontrar en la dirección URL siguiente: http://www.cisco.com/warp/customer/707/ 21.html

Los switches son el objetivo

Al igual que los routers, los switches (tanto de Capa 2 como de Capa 3) tienen su propio conjunto de consideraciones de seguridad. A diferencia de los routers, no se ha hecho pública tanta información acerca de los riesgos de seguridad en los switches y lo que puede hacerse para combatirlos. La mayoría de las técnicas de seguridad indicadas en la sección anterior, "Los routers son objetivos", se aplican también a los switches. Además, debería tomar las siguientes precauciones:

- En los puertos que no necesiten enlaces troncales, deberían desactivarse, en lugar de dejar la configuración en auto. Esto evita que un host se convierta en un puerto troncal y que reciba todo el tráfico que normalmente llegaría a dicho puerto.
- Asegúrese de que los puertos troncales usan un número de LAN virtual (VLAN) que no se emplea en ninguna otra parte del switch. Esto evita que los paquetes marcados con la misma VLAN que el puerto troncal lleguen a otra VLAN sin cruzar ningún dispositivo de Capa 3. Para obtener más información, consulte la siguiente dirección URL: http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
- Asigne todos los puertos no utilizados de un switch a una VLAN que no tenga conectividad de Capa 3. Mejor aún, desactive todos los puertos que no necesite. Esto evita que los hackers se conecten a los puertos no utilizados y se comuniquen con el resto de la red.
- Evite utilizar VLAN como único método para asegurar el acceso entre dos subredes. La posibilidad de un error humano, combinada con la certidumbre de que las VLAN y los protocolos de marcas de VLAN no se diseñaron pensando en la seguridad, hace que no sea aconsejable utilizarlos en entornos sensibles. Cuando se necesitan VLAN en las instalaciones de seguridad, asegúrese de prestar mucha atención a las configuraciones y directrices ya mencionadas.

Dentro de una VLAN, las VLAN privadas proporcionan cierta seguridad añadida a determinadas aplicaciones de red. Las VLAN privadas funcionan limitando los puertos de una VLAN que pueden comunicarse con otros puertos de la misma VLAN. Los puertos aislados de una VLAN sólo pueden comunicarse con puertos promiscuos. Los puertos de una comunidad sólo pueden comunicarse con los restantes puertos de la misma comunidad y con los puertos promiscuos. Los puertos promiscuos pueden comunicarse con todos los puertos. Ésta es una forma eficaz de mitigar los efectos de un solo host en peligro. Piense en un segmento estándar de servicios públicos con una Web, FTP y un servidor DNS. Si el servidor DNS está en peligro, un hacker puede perseguir los otros dos hosts sin pasar por el firewall. Si se instalan VLAN privadas, una vez que un sistema está en peligro, no puede comunicarse con los restantes sistemas. Los únicos objetivos que pueden perseguir los hackers son los hosts que están al otro lado del firewall.

Los hosts son el objetivo

Los hosts son los objetivos más probables durante los ataques y presentan algunos de los retos más difíciles desde la perspectiva de la seguridad. Hay muchas plataformas de hardware, sistemas operativos y aplicaciones, y todas ellas tienen actualizaciones y parches disponibles en distintos momentos. Dado que los hosts proporcionan los servicios de aplicaciones a los restantes hosts que los soliciten, son perfectamente visibles en la red. Por ejemplo, mucha gente ha visitado http://www.whitehouse.gov, que es un host, pero muy pocos han intentado acceder a s2-0.whitehouseisp.net, que es el router. A causa de esta visibilidad, los hosts son los dispositivos atacados con más frecuencia en cualquier intento de intrusión a la red.

En parte, debido a los retos de seguridad ya mencionados, los hosts también son los dispositivos que más se ponen en peligro. Por ejemplo, un servidor Web determinado de Internet podría ejecutarse en una plataforma de hardware de un fabricante, una tarjeta de red de otro, un sistema operativo de un tercero y un servidor Web que sea de código fuente abierto o de otro fabricante distinto al resto. Además, el mismo servidor Web podría ejecutar aplicaciones que se distribuyen libremente a través de Internet y que podría comunicarse con un servidor de bases de datos que vuelve a comenzar las variaciones. Eso no significa que los puntos vulnerables en la seguridad se provoquen específicamente por la naturaleza de varias fuentes de todo esto, sino que a medida que aumenta la complejidad de los sistemas, también aumenta la probabilidad de fallos.

Para asegurar los hosts, preste especial atención a cada uno de los componentes de los sistemas. Mantenga los sistemas actualizados con los parches y las actualizaciones más recientes. En particular, preste atención al modo en que estos parches afectan al funcionamiento de los restantes componentes del sistema. Evalúe todas las actualizaciones en sistemas de prueba antes de implementarlos en un entorno de producción. Si no lo hace, existe la posibilidad de que el propio parche cause una denegación de servicio (DoS).

Las redes son el objetivo

El peor ataque es el que no se puede detener. Si se realiza correctamente, la denegación distribuida de servicio (DDoS) es uno de esos ataques. Como se indica en el anexo B, "Manual de seguridad de redes", DDoS funciona haciendo que decenas o cientos de máquinas envíen simultáneamente datos falsos a una dirección IP. El objetivo de dicho ataque no suele ser echar abajo un host determinado, sino que deje de funcionar toda la red. Por ejemplo, piense en una organización con una conexión DS3 (45 Mbps) a Internet, que proporciona servicios de comercio electrónico a los usuarios de su sitio Web. Dicho sitio está muy preocupado por la seguridad y tiene detección de intrusos, firewalls, registro y control activo. Lamentablemente, todos estos dispositivos de seguridad no sirven de ninguna ayuda cuando un hacker lanza un ataque DDoS con éxito.

Piense en 100 dispositivos en todo el mundo, cada uno de ellos con conexiones DS1 (1,5 Mbps) a Internet. Si se indica de forma remota a estos sistemas que desborden la interfaz serie del router de Internet de la organización de comercio electrónico, pueden desbordar muy fácilmente a la conexión DS3 con datos erróneos. Aunque cada host sólo pueda generar 1 Mbps de tráfico, (las pruebas de laboratorio indican que una estación de trabajo Unix puede generar fácilmente 50 Mbps con una herramienta conocida de DDoS), dicha cantidad sigue siendo el doble de la cantidad de tráfico que puede gestionar el sitio de comercio electrónico. Como resultado, se pierden las solicitudes de Web legítimas y la mayoría de los usuarios creen que el sitio no funciona. El firewall local elimina todos los datos erróneos, pero para entonces el daño ya está hecho. El tráfico ha atravesado la conexión WAN y ha llenado el enlace.

Solamente a través de la cooperación con su ISP puede esperar frustrar dicho ataque esta empresa ficticia de comercio electrónico. Un ISP puede configurar la limitación de la velocidad en la interfaz saliente del sitio de empresa. Esta limitación de la velocidad puede eliminar la mayor parte del tráfico no deseado cuando supera una cantidad previamente especificada del ancho de banda disponible. La clave es marcar correctamente el tráfico como no deseado.

Las formas más habituales de ataques DDoS son los desbordamientos de ICMP, los desbordamientos de TCP SYN o los desbordamientos de UDP. En un entorno de comercio electrónico, este tipo de tráfico es bastante sencillo de clasificar. Sólo al limitar un ataque TCP SYN al puerto 80 (http) cualquier administrador corre el riesgo de bloquear a usuarios legítimos durante un ataque. Incluso entonces, es mejor bloquear temporalmente a los nuevos usuarios legítimos y mantener las conexiones de enrutamiento y gestión a que el router esté sobrecargado y pierda todas las conexiones.

Los ataques más sofisticados utilizan el tráfico del puerto 80 con el conjunto de bits ACK para que el tráfico parezca ser transacciones Web legítimas. Es improbable que un administrador pueda clasificar dicho ataque, ya que las comunicaciones TCP reconocidas son exactamente del tipo que se deja entrar en la red.

Un método para limitar este tipo de ataque es seguir las pautas indicadas en RFC 1918 y RFC 2827. RFC 1918 especifica las redes que están reservadas para uso privado y nunca deberían verse a través de Internet pública. Los filtros de RFC 2827 se explican en la sección "Ataques de falsificación (spoofing) de IP" del anexo B, "Manual de seguridad de redes". Para el tráfico que entra a un router conectado a Internet, puede emplear los filtros de RFC 1918 y 2827 para evitar que el tráfico no autorizado llegue a la red de la empresa. Cuando se implementan en el ISP, estos filtros evitan que los paquetes de los ataques de DDoS que utilicen estas direcciones como fuentes atraviesen el enlace WAN, lo que potencialmente ahorra ancho de banda durante el ataque. Colectivamente, si los ISP de todo el mundo tuvieran que implementar las directrices de RFC 2827, los ataques de falsificación a las direcciones de origen disminuirían considerablemente. Aunque esta estrategia no evita directamente los ataques de DDoS, evita que dichos ataques enmascaren su origen, lo que facilita mucho el seguimiento de las redes que realizan el ataque.

Las aplicaciones son el objetivo

Las aplicaciones las codifican seres humanos (la mayor parte) y, como tales, están sujetas a numerosos errores. Estos errores pueden ser benignos (por ejemplo, un error que hace que el documento no se imprima bien) o malignos (por ejemplo, un error que hace que se pueda acceder a través FTP anónimo a los números de tarjetas de crédito de su servidor de bases de datos). Son los problemas malignos, así como otros puntos vulnerables de la seguridad más generales, lo que los sistemas de detección de intrusos (IDS) pretenden detectar. La detección de intrusos actúa igual que los sistemas de alarmas en el mundo físico. Cuando un IDS detecta algo que considera un ataque, puede adoptar medidas correctoras automáticamente o enviar una notificación a un sistema de gestión para que sea el administrador el que tome las medidas. Algunos sistemas están más o menos equipados para responder y prevenir dicho ataque. La detección de intrusos basada en host puede funcionar interceptando las llamadas al sistema operativo y a las aplicaciones de un host individual. También puede funcionar mediante un análisis a posteriori de los archivos del registro local. El primer método permite prevenir mejor los ataques, mientras que el último dicta un rol de respuesta más pasiva a los mismos. A causa de la especificidad de su función, los sistemas IDS basados en host (HIDS) suelen ser mejores para evitar ciertos ataques que los IDS de red (NIDS), que normalmente sólo emiten una alerta al descubrir un ataque. Sin embargo, dicha especificidad provoca una pérdida de perspectiva en la red global. Y ahí es donde se ve superado por NIDS. Para lograr un sistema de detección de intrusos completo, Cisco recomienda una combinación de ambos sistemas (HIDS en los hosts mas importantes y NIDS supervisando toda la red).

Una vez instalado, hay que ajustar una implementación de IDS para aumentar su eficacia y eliminar "falsos positivos".

Los falsos positivos son las alarmas que desencadenan el tráfico o las actividades legítimas. Los falsos negativos son ataques que el sistema IDS no consigue ver. Una vez ajustado el sistema IDS, puede configurarlo más específicamente para su función, combatir amenazas. Como ya hemos indicado, debe configurar HIDS para que detenga la mayor parte de las amenazas válidas a nivel de host, ya que está preparado para determinar que cierta actividad es indudablemente una amenaza.

Al decidir sobre las funciones de combate de NIDS hay dos opciones principales:

La primera opción y, potencialmente, la más dañina si no se instala correctamente, es "rechazar (shun)" el tráfico a través de la incorporación de filtros de control de acceso en los routers. Cuando un NIDS detecta un ataque de un host específico sobre un protocolo determinado, puede impedir el acceso de dicho host en la red durante un periodo de tiempo predeterminado. Aunque a primera vista esto pudiera parecer de gran ayuda para los administradores de seguridad, en realidad si se implementa, hay que hacerlo con extremo cuidado. El primer problema es el de las direcciones falsificadas. Si el NIDS ve tráfico que coincide con algún ataque y dicha alarma específica desencadena una respuesta de rechazo, el NIDS instalará la lista de accesos en el dispositivo. Sin embargo, si el ataque que provocó la alarma utilizaba una dirección falsificada, el NIDS ha atacado a una dirección que nunca inició ningún ataque. Si da la casualidad que la dirección IP que utilizó el hacker era la de un servidor proxy HTTP saliente de un ISP importante, es posible que un inmenso número de usuarios quedara bloqueado. Esto, por si mismo, podría ser una interesante amenaza de DoS en manos de un hacker con dotes creativas.

Para reducir los riesgos del rechazo, normalmente debería utilizarlo solamente en tráfico de TCP, que es mucho más difícil de falsificar que el de UDP. Utilícelo solamente en caso de que la amenaza sea real y de que la oportunidad de que el ataque sea un falso positivo sea muy baja. Sin embargo, en el interior de las redes existen muchas más opciones. Con una correcta instalación de los filtros de RFC 2827, el tráfico falsificado sería muy limitado. Además, dado que los clientes no suelen estar en la red interna, puede adoptar una postura más restrictiva contra los intentos de ataque de origen interno. Otra razón para esto es que las redes internas no suelen tener el mismo nivel de filtro con estado que la que tienen las conexiones del contorno. Como tal, hay que confiar mucho más en el IDS que en el entorno externo.

La segunda opción para combatir las amenazas de NIDS es el uso de reinicios de TCP. Los reinicios de TCP funcionan solamente en el tráfico de TCP y terminan los ataques activos enviando mensajes de restablecimiento del TCP tanto al host que ataca como al atacado. Teniendo en cuenta que el tráfico de TCP es más difícil de falsificar, es posible que sea mejor utilizar resets TCP con más frecuencia que rechazos.

Desde el punto de vista del rendimiento, NIDS observa los paquetes que hay en el cable. Aunque los paquetes se envíen más rápidamente de lo que el NIDS puede procesarlos no empeora el funcionamiento de la red, ya que el NIDS no se asienta directamente sobre los flujos de datos. Sin embargo, el NIDS perderá efectividad y pueden perderse paquetes, lo que provoca tanto falsos negativos como falsos positivos. Asegúrese de no superar las capacidades de IDS para que pueda obtener sus beneficios. Desde el punto de vista del enrutamiento, IDS, como muchos motores que controlan el estado, no funciona correctamente en entornos enrutados asimétricamente. Los paquetes que salen de un conjunto de routers y switches vuelven a través de otro harán que los sistemas IDS vean solamente la mitad del tráfico, lo que provoca falsos positivos y falsos negativos.

Gestión y generación de informes seguros

"Si va a registrarlo, léalo". Ésta es una propuesta tan simple que casi todo el mundo que sabe de seguridad de redes la ha efectuado al menos una vez. Aun así el registro y la lectura de la información de más de cien dispositivos puede demostrar ser una propuesta desafiante, ¿qué registros son más importantes?, ¿cómo se separan los mensajes importantes de las meras notificaciones?, ¿cómo me aseguro de que los registros no se interceptan en tránsito?, ¿cómo me aseguro de que las etiquetas de hora coinciden entre sí cuando varios dispositivos informan de la misma alarma?, ¿qué información es necesaria si se solicitan los datos de los registros para una investigación criminal?, ¿cómo se trata el volumen de mensajes que puede generar una red grande? Para gestionar los archivos de registro eficazmente hay que solucionar todas estas preguntas. Desde el punto de vista de la gestión, hay que responder a otro conjunto de preguntas: ¿cómo se gestionan con seguridad los dispositivos?, ¿cómo se pueden enviar contenidos a servidores públicos y garantizar que no se interceptan en tránsito?, ¿cómo se puede hacer un seguimiento de los cambios en los dispositivos para solucionar los problemas que surgen cuando se producen ataques o fallos en la red?

Desde el punto de vista de la arquitectura, ofrecer gestión fuera de banda de los sistemas de red es el mejor primer paso que se puede dar en cualquier estrategia de gestión y generación de informes. Fuera de banda (OOB), como su nombre implica, hace referencia a una red que no tiene tráfico de producción. Los dispositivos deberían tener una conexión local directa a dicha red donde sea posible y, donde sea imposible (debido a problemas geográficos o relacionados con el sistema), el dispositivo debería conectarse a través de un túnel privado cifrado sobre la red de producción. Dicho túnel debería preconfigurarse para comunicarse sólo a través de los puertos específicos necesarios para la gestión y la generación de informes. El túnel también debería bloquearse para que solo sean los hosts apropiados los que pueden iniciar y terminar túneles. Asegúrese de que la propia red fuera de banda no crea problemas de seguridad. Para obtener más información al respecto, consulte la sección "Módulo de gestión" de este documento.

Tras implementar una red de gestión de OOB, es mucho más sencillo y directo tratar con los registros y con la generación de informes. La mayoría de los dispositivos de red puede enviar datos syslog, que pueden ser inestimables al solucionar los problemas de la red o las amenazas a la seguridad. Envíe estos datos a uno o varios hosts de análisis de syslog de la red de gestión. En función del dispositivo implicado, puede elegir entre varios niveles de registro para asegurarse de que se envía la cantidad de datos correcta a los dispositivos de registro. También tiene que marcar en el software de análisis los datos de registro del dispositivo para permitir la vista y la generación de informes granular. Por ejemplo, durante un ataque, es posible que los datos de registro que proporcionan los switches de Capa 2 no sean tan interesantes como los que proporciona el sistema de detección de intrusos. Las aplicaciones especializadas, como IDS, suelen utilizar sus propios protocolos de registro para transmitir información de las alarmas. Normalmente, estos datos deberían registrarse en hosts de gestión independientes que estén mejor equipados para tratar las alarmas de

ataques. Si se combinan, los datos de las alarmas de muchas fuentes distintas pueden ofrecer información acerca del estado global de la red. Para asegurarse de que los mensajes de registro están sincronizados entre sí, los relojes de los hosts y de los dispositivos de red deben estar sincronizados. Para los dispositivos que lo admiten, el protocolo Network Time Protocol (NTP) permite garantizar que todos los dispositivos tienen la hora exacta. Al enfrentarse a ataques, los segundos cuentan, ya que es importante identificar el orden en que tuvo lugar el ataque especificado.

Desde el punto de vista de la gestión, que a efectos de este documento hace referencia a cualquier función que lleva a cabo un administrador en un documento, salvo grabar registros y generar informes, hay otros problemas y soluciones. Igual que sucede con los registros e informes, la red OOB permite el transporte de información destinada a mantener un entorno controlado donde no pueda haber intercepciones. Aun así, siempre que sea posible una configuración segura, como por ejemplo mediante el uso de Secure Socket Layer (SSL) o Secure Shell (SSH), habría que optar por ella. SNMP debe tratarse con el máximo cuidado, ya que el protocolo subyacente tiene su propio conjunto de puntos vulnerables de seguridad. Estudie la posibilidad de ofrecer acceso de sólo lectura a los dispositivos a través de SNMP y a tratar la cadena de la comunidad SNMP con el mismo cuidado con que trataría a una contraseña root en un host Unix muy importante.

La gestión de los cambios de configuración es otro problema relacionado con una gestión segura. Cuando una red sufre un ataque, es importante conocer el estado de los dispositivos más importantes de la misma y cuándo se produjeron las últimas modificaciones conocidas. La creación de un plan para la gestión de modificaciones debería formar parte de las normativas de seguridad global, pero, como mínimo, hay que grabar las modificaciones utilizando los sistemas de autenticación de los dispositivos y archivar las configuraciones a través de FTP o TFTP.

Módulo de la empresa

La empresa se compone de dos áreas funcionales: las oficinas centrales y el contorno. A su vez, ambas áreas están divididas en módulos que definen detalladamente las distintas funciones de cada área. Después de la explicación detallada de los módulos de las secciones "Oficinas centrales de la empresa" y "Contorno de la empresa", la sección "Opciones de las empresas" describe varias opciones de diseño.

Amenazas que se esperan

Desde el punto de vista de las amenazas, la red de la empresa es como la mayor parte de las redes conectadas a Internet. Hay usuarios internos que necesitan acceso saliente y usuarios externos que necesitan acceso entrante. Hay varias amenazas comunes que pueden generar el peligro inicial que necesita cualquier hacker para penetrar en la red con exploits secundarios.

En primer lugar está la amenaza de los usuarios internos. Aunque las estadísticas difieren en el porcentaje, es un hecho establecido que la mayor parte de los ataques provienen de la red interna. Los trabajadores descontentos, los espías industriales, los visitantes y la torpeza de algunos usuarios son los orígenes potenciales de dichos ataques. Al diseñar la seguridad, es importante ser consciente del potencial de las amenazas internas.

En segundo lugar está la amenaza a los hosts públicos conectados a Internet. Es probable que estos sistemas se ataquen por los puntos vulnerables de la capa de aplicaciones y con ataques de DoS.

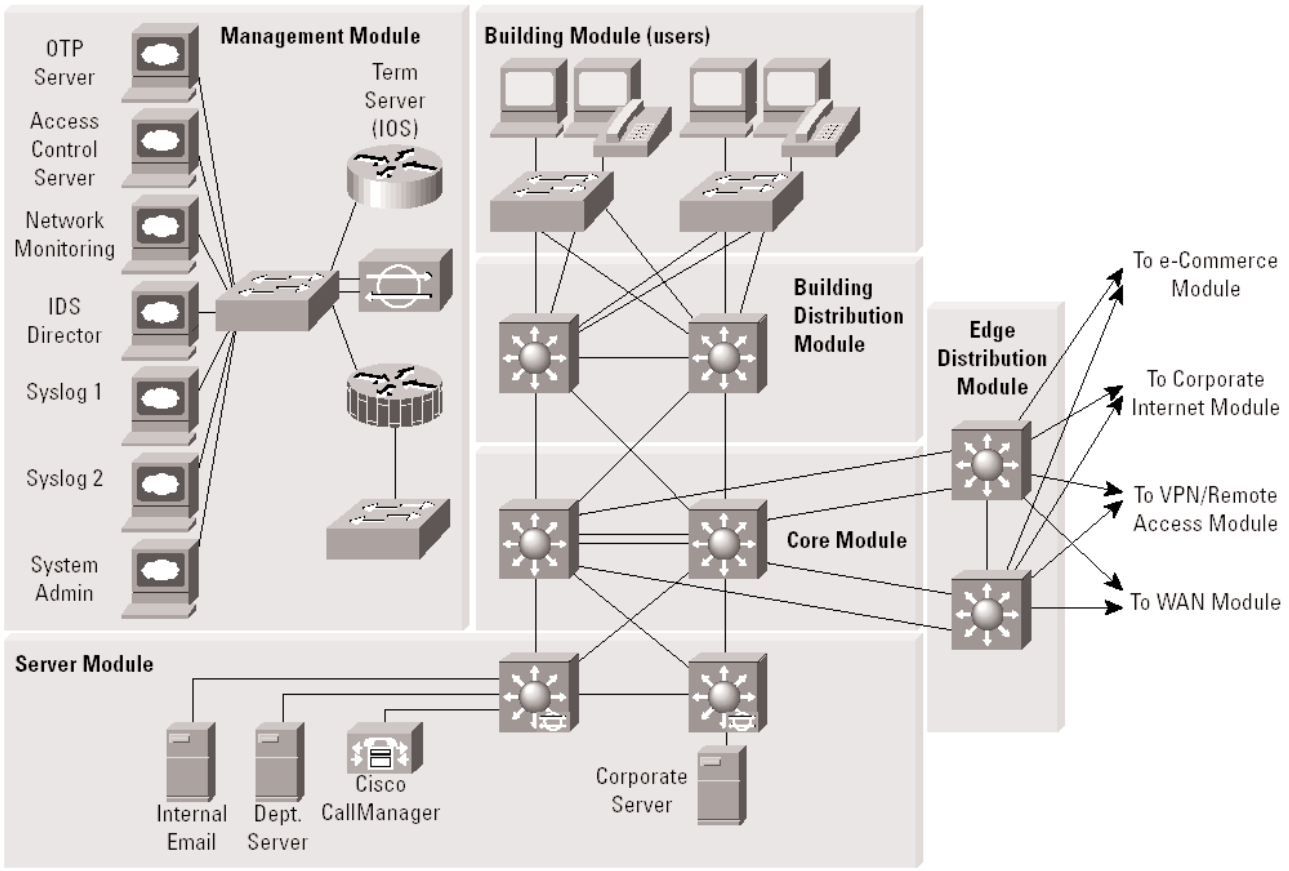
La amenaza final es que un hacker pueda intentar determinar sus números de teléfonos de datos utilizando un "war-dialer" e intente obtener acceso a la red. Los war-dialers son elementos de software o de hardware que están diseñados para marcar muchos números de teléfono y determinar el tipo de sistema del otro extremo de la conexión. Los sistemas personales con software de control remoto instalado por el usuario son los más vulnerables, ya que no suelen ser muy seguros. Dado que estos dispositivos están detrás del firewall, una vez que los hackers han accedido a través del host al que llamaron, pueden hacerse pasar por usuarios de la red.

Si deseas una explicación completa de los detalles de las amenazas, consulte el anexo B, "Manual de seguridad de redes".

Oficinas centrales de la empresa

A continuación encontrará un análisis detallado de todos los módulos que contienen las oficinas centrales de la empresa.

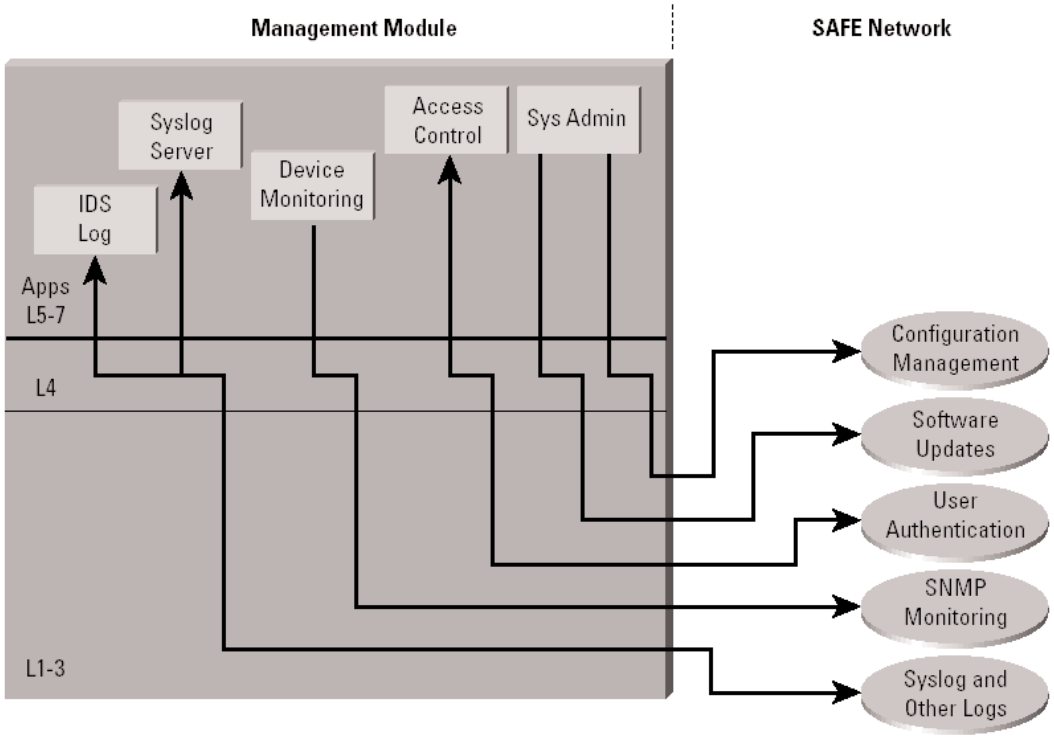
Ilustración 3 Detalle de las oficinas centrales de la empresa



Módulo de gestión

El objetivo principal del módulo de gestión es facilitar la gestión segura de todos los dispositivos y hosts de la arquitectura SAFE de la empresa. La información de registros e informes fluye desde los dispositivos hasta los hosts de gestión, mientras que el contenido, las configuraciones y el nuevo software fluyen desde los hosts de gestión a los dispositivos.

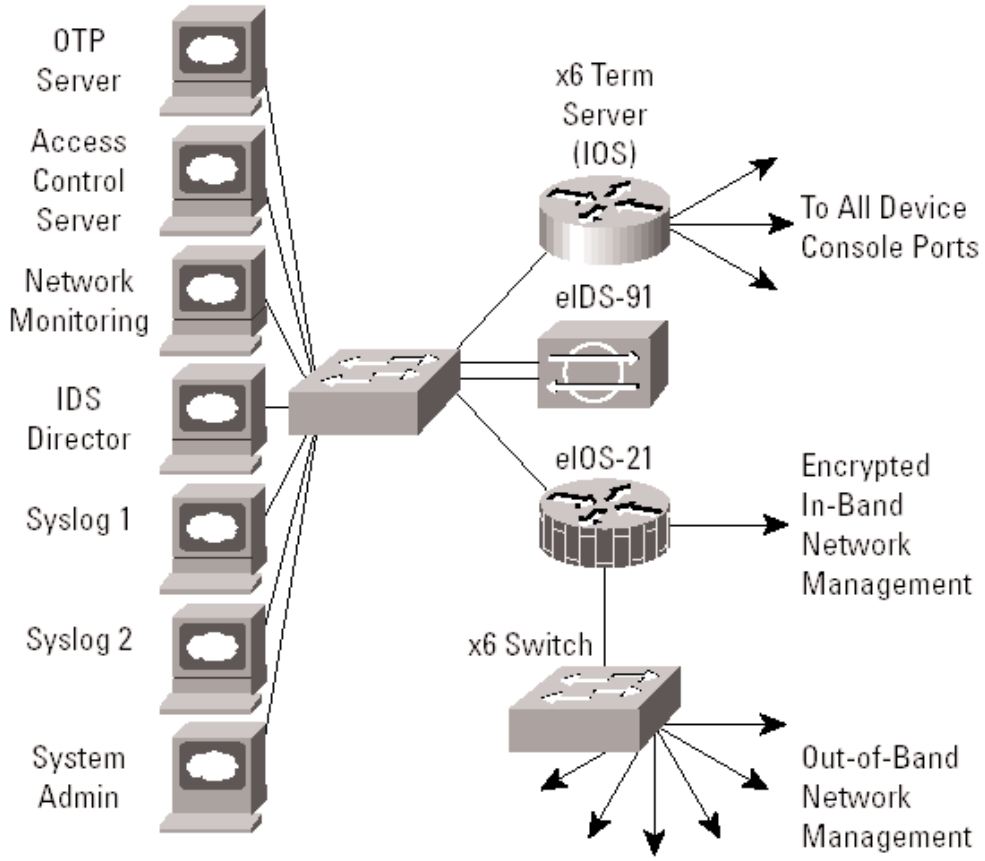
Ilustración 4 Flujo del tráfico de gestión



Dispositivos principales

- *Host de gestión de SNMP:* proporciona gestión de SNMP a los dispositivos.
- *Host de NIDS:* proporciona agregación de alarmas a todos los dispositivos NIDS de la red.
- *Hosts de syslog:* agrega información de registro al firewall y a los hosts de NIDS.
- *Servidor de control de accesos:* ofrece a los dispositivos de la red servicios de autenticación con dos factores que sólo hay que instalarlos una vez.
- *Servidor de contraseñas únicas (OTP):* autoriza la información de las contraseñas únicas transmitida desde el servidor de control de accesos.
- *Host de administración del sistema:* proporciona los cambios de configuración, software y contenidos de los dispositivos.
- *Dispositivo de NIDS:* proporciona supervisión de la Capa 4 a la Capa 7 de los elementos de red clave del módulo.
- *Firewall Cisco IOS:* permite el control granular de los flujos de tráfico entre los hosts de gestión y los dispositivos gestionados.
- *Switch de Capa 2 (con compatibilidad con VLAN privada):* garantiza que los datos de los dispositivos gestionados sólo pueden pasar directamente al firewall IOS

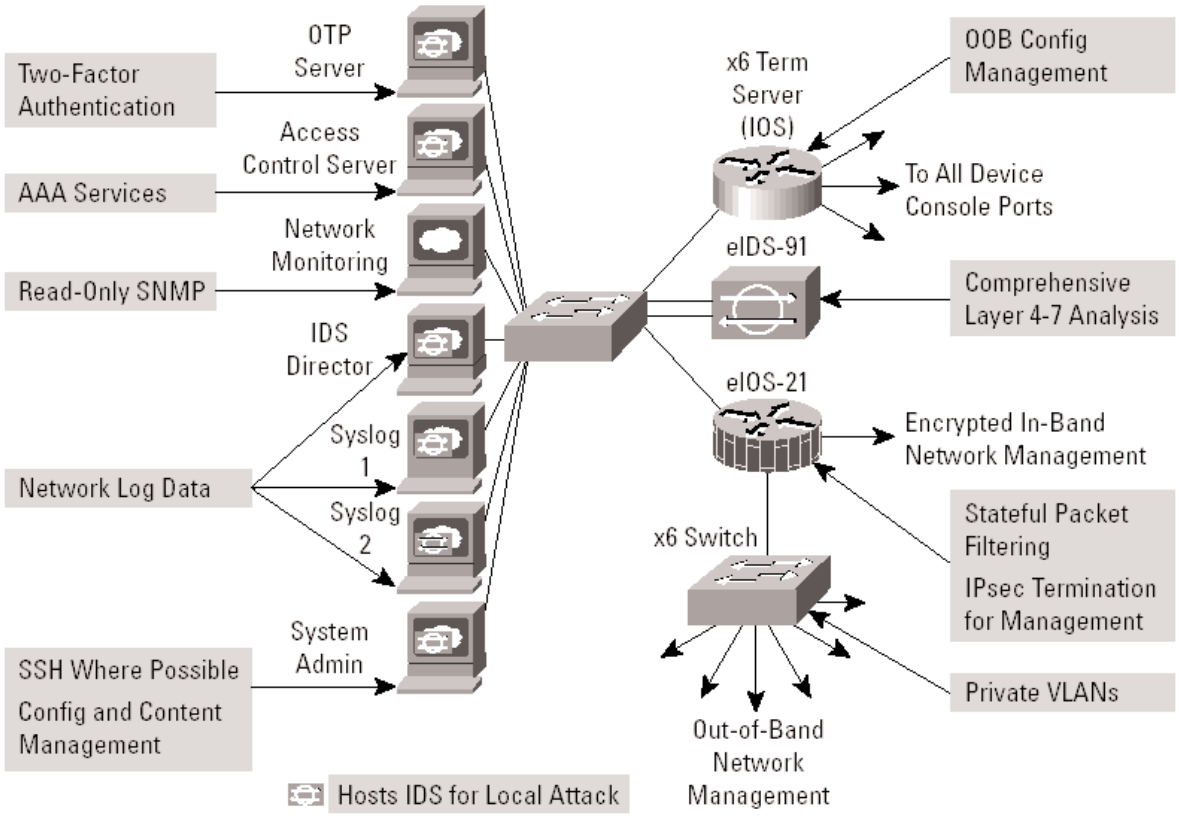
Ilustración 5 Módulo de gestión: detalle



Amenazas que combate

- *Acceso no autorizado:* los filtros del firewall IOS detienen la mayor parte del tráfico no autorizado que circula en ambas direcciones.
- *Ataques del tipo Man in the Middle:* los datos de gestión van a atravesar una red privada lo que hace que los ataques del tipo man in the middle sean difíciles.
- *Reconocimiento de la red:* dado que todo el tráfico de gestión cruza esta red, no cruza la red de producción, donde podría interceptarse.
- *Ataques a contraseñas:* el servidor de control de accesos permite una fuerte autenticación con dos factores en cada dispositivo.
- *Ataques de falsificación (spoofing) de IP:* el tráfico falsificado se detiene en ambas direcciones en el firewall IOS.
- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada limita la efectividad del rastreo.
- *Abuso de confianza:* las VLAN privadas impiden que un dispositivo que esté en peligro se haga pasar por un host de gestión.

Ilustración 6 Funciones en el combate de ataques del módulo de gestión



Directrices del diseño

Como se puede apreciar en los diagramas anteriores, la red de gestión de empresas SAFE tiene dos segmentos de red que están separados por un router IOS que actúa como firewall y como dispositivo de terminación de VPN. El segmento que está fuera del firewall conecta con todos los dispositivos que requieren gestión. El segmento que está dentro del firewall contiene los propios hosts de gestión y los routers IOS que actúan como servidores de terminal. El resto de la interfaz conecta con la red de producción, pero solamente para el tráfico de gestión protegido por IPSec de los hosts predeterminados. Esto permite la gestión de un dispositivo de Cisco que no tenía suficientes interfaces para soportar la conexión de gestión normal. El firewall IOS está configurado para dejar entrar la información de syslog en el segmento de gestión, así como telnet, SSH y SNMP, siempre que se inicien desde dentro de la red.

Ambas subredes de gestión funcionan en un espacio de direcciones que es completamente independiente del resto de la red de producción, lo que garantiza que ningún protocolo de enrutamiento publicitará la red de gestión. También permite a los dispositivos de la red de producción bloquear todo el tráfico de las subredes de gestión que aparezca en los enlaces de dicha red.

El módulo de gestión proporciona gestión de la configuración a casi todos los dispositivos de la red, para lo que utiliza dos tecnologías principales: los routers Cisco IOS que actúan como servidores de terminales y un segmento de la red dedicado a la gestión. Los routers proporcionan una función de telnet inverso a los puertos de consola de los dispositivos de Cisco de toda la empresa. Las características de gestión más amplias (cambios de software, actualizaciones de contenidos, agregación de registros y alarmas, y gestión de SNMP) se proporcionan a través del segmento de red dedicado a la gestión. Los restantes dispositivos no gestionados y los hosts se gestionan a través de túneles IPSec que parten del router de gestión.

Al tener acceso administrativo a casi todas las áreas de la red, la red de gestión es un objetivo que atrae mucho a los hackers. El módulo de gestión se ha creado con varias tecnologías diseñadas para combatir dichos riesgos. El primer reto importante es un hacker intentando obtener acceso a la propia red de gestión. Esta amenaza sólo puede combatirse con la instalación eficaz de características de seguridad en los restantes módulos de la empresa. Las restantes amenazas suponen que se ha abierto una brecha en la línea principal de defensa Para combatir la amenaza de un dispositivo en peligro, se implementa el control de accesos en el firewall, y en cualquier otro dispositivo posible, para impedir la explotación del canal de gestión. Los dispositivos en peligro ni siquiera pueden comunicarse con otros hosts de la misma subred, ya que las VLAN privadas de los switches del segmento de gestión obligan a todo el tráfico de los dispositivos gestionados a pasar directamente al firewall IOS, donde tiene lugar el filtro. El rastreo (sniffing) de contraseñas sólo muestra información inútil debido al entorno de contraseña única. Las IDS de host y de red también se implementan en la subred de gestión y se configuran de forma muy restrictiva. Teniendo en cuenta que los tipos de tráfico de esta red deberían ser muy limitados, cualquier coincidencia de firma de este segmento debe tratarse con una respuesta inmediata.

La gestión de SNMP tiene su propio conjunto de necesidades de seguridad. El hecho de mantener el tráfico SNMP en el segmento de gestión permite que atraviese segmentos aislados al extraer información de gestión de los dispositivos. Con SAFE, la gestión de SNMP sólo extrae información de los dispositivos, no le permite realizar cambios. Para garantizarlo, los dispositivos se configuran solamente con una cadena de "sólo lectura".

La agregación y el análisis correcto de la información de syslog es vital para una gestión adecuada de las redes. Desde una perspectiva de seguridad, syslog ofrece información importante relativa a las violaciones de la seguridad y a los cambios en las configuraciones. Dependiendo del dispositivo en cuestión pueden ser necesarios distintos niveles de información de syslog. El envío de todos los registros con todos los mensajes podría proporcionar demasiada información para que una persona o un algoritmo de análisis de syslog la clasificara. Guardar registros por el mero hecho de guardarlos no mejora la seguridad.

En el laboratorio de validación de SAFE, todas las configuraciones se realizaron utilizando aplicaciones de gestión independientes y la interfaz de línea de comandos (CLI). No obstante, no hay nada en SAFE que impida el uso de sistemas de gestión de normativas para la configuración. El establecimiento de este módulo de gestión hace que las instalaciones de dicha tecnología sean totalmente viables. Tanto CLI como las aplicaciones de gestión independientes se eligieron porque la mayoría de las instalaciones de redes actuales emplean este método de configuración.

Alternativas

La gestión completamente fuera de banda no siempre es posible porque algunos dispositivos quizá no la admitan o porque puede haber diferencias geográficas que dicten la gestión en banda. Cuando es necesaria la gestión en banda, hay que poner más énfasis en asegurar el transporte de los protocolos de gestión, lo que se puede realizar mediante el uso de IPSec, SSH, SSL o cualquier otro transporte cifrado y autenticado que permita que la información de gestión lo atraviese. Cuando la gestión se produce en la misma interfaz que algún dispositivo utiliza para los datos de los usuarios, hay que conceder importancia a las contraseñas, cadenas de comunidad, claves criptográficas y listas de acceso que controlan las comunicaciones a los servicios de gestión.

Objetivos a corto plazo de la arquitectura

La implementación actual de informes y alarmas está dividida entre varios hosts. Algunos hosts tienen inteligencia para analizar los datos del firewall y del IDS, mientras que otros son más apropiados para analizar los datos de los routers y de los switches. En el futuro, todos los datos se agregarán al mismo conjunto de hosts redundantes, con el fin de que se pueda producir la correlación de eventos entre todos los dispositivos.

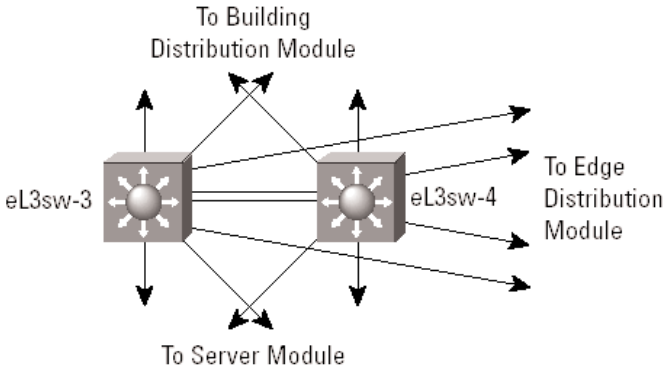
Módulo central

El módulo central de la arquitectura SAFE es casi idéntico al de cualquier otra arquitectura de red. Solamente enruta y conmuta el tráfico lo más rápidamente posible de una red a otra.

Dispositivos principales

- *Conmutación de Capa 3:* enruta y conmuta datos de la red de producción de un módulo a otro.

Ilustración 7 Módulo central: detalle



Amenazas que combate

- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada limita la efectividad del rastreo.

Directrices del diseño

Se siguieron las directrices de implementación estándar de acuerdo con las instalaciones del "núcleo, la distribución y la capa de acceso" que se suelen ver en las redes basadas en Cisco bien diseñadas.

Aunque la arquitectura SAFE no define requisitos únicos para el núcleo de las redes de las empresas, los switches centrales siguen el axioma de seguridad de switches de la sección "Los switches son el objetivo" para asegurarse de que están bien protegidos contra ataques directos.

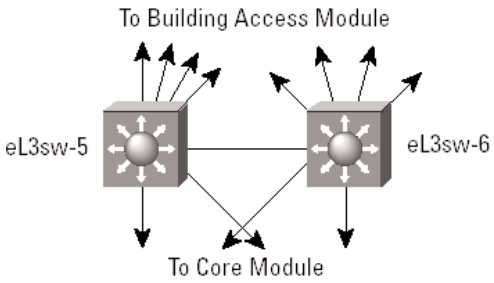
Módulo de distribución del edificio

El objetivo de este módulo es proporcionar servicios de la capa de distribución a los switches del edificio, entre los que se incluyen el enrutamiento, la calidad de servicio (QoS) y el control de accesos. Las solicitudes de datos entran en estos switches y en el núcleo, mientras que las respuestas siguen el camino inverso.

Dispositivos principales

- *Switches de Capa 3:* agregan switches de Capa 2 al módulo del edificio y proporcionan servicios avanzados.

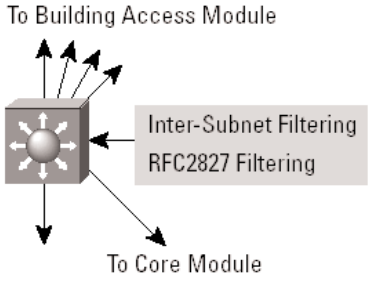
Ilustración 8 Módulo de distribución del edificio: detalle



Amenazas que combate

- *Acceso no autorizado:* los ataques contra los recursos del módulo del servidor se limitan mediante el filtrado en la Capa 3 de determinadas subredes.
- *Ataques de falsificación (spoofing) de IP:* los filtros de RFC 2827 detienen la mayoría de los intentos de falsificación.
- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada limita la efectividad del rastreo.

Ilustración 9 Funciones de mitigación de ataques del módulo de distribución del edificio



Directrices del diseño

Además de los fundamentos estándar del diseño de redes, las optimizaciones descritas en la sección "Los switches son el objetivo" se implementaron para proporcionar mas seguridad en la comunidad de usuarios de la empresa. La detección de intrusos no se implementa en el módulo de distribución del edificio, ya que se implementa en los módulos que contienen los recursos que es probable que sean atacados por su contenido (servidor, acceso remoto, Internet, etc.). El módulo de distribución del edificio proporciona la primera línea de defensa y protección contra los ataques que se originan internamente. Puede reducir la posibilidad de que un departamento acceda a información confidencial del servidor de otro departamento a través del uso del control de acceso. Por ejemplo, una red que contenga marketing e investigación y desarrollo puede sacar de la misma el servidor de I+D a una VLAN específica y filtrar el acceso a él, con lo que se garantizaría que sólo puede acceder el personal de I+D. Por cuestiones de rendimiento, es importante que este control de acceso se implemente en una plataforma de hardware que pueda ofrecer tráfico filtrado a velocidades cercanas al cable. Esto generalmente dicta el uso de la conmutación de Capa 3, frente a los dispositivos de enrutamiento dedicados más tradicionales. Este mismo control de accesos también puede evitar la falsificación de direcciones de origen locales, para lo que utiliza los filtros de RFC 2827. Por último, el aislamiento de subredes se utiliza para enrutar tráfico de voz a través de IP (VoIP) al gestor de llamadas y a todas la gateways asociadas. Esto impide que el tráfico de VoIP cruce los mismos segmentos que atraviesa el tráfico de datos restante, con lo que se reduce la probabilidad de rastreo de las comunicaciones de voz, y permite una implementación mas suave de QoS.

Alternativas

Dependiendo de los requisitos de tamaño y de rendimiento de la red, la capa de distribución puede combinarse con la capa central para reducir el número de dispositivos necesarios en el entorno.

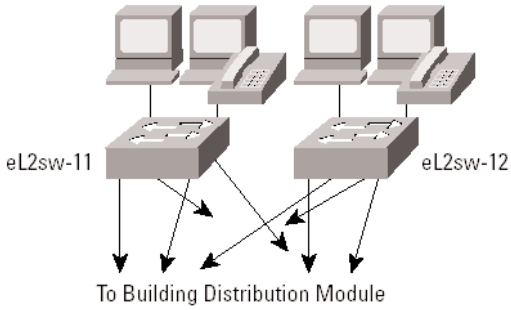
Módulo del edificio

SAFE define el módulo del edificio como la parte amplia de la red que contiene las estaciones de trabajo de los usuarios finales, los teléfonos y sus puntos de acceso de Capa 2 asociados. Su objetivo principal es ofrecer servicios a los usuarios finales.

Dispositivos principales

- *Switch de Capa 2:* proporciona servicios de Capa 2 a los teléfonos y a las estaciones de trabajo de los usuarios.
- *Estación de trabajo de usuario:* proporciona servicios de datos a los usuarios autorizados de la red.
- *Teléfono IP:* proporciona servicios de telefonía por IP a los usuarios de la red.

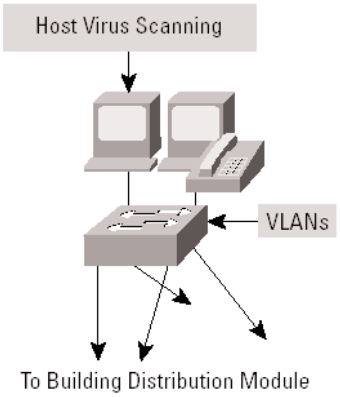
Ilustración 10 Módulo de acceso al edificio: detalle



Amenazas que combate

- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada y servicios VLAN predeterminados limitan la efectividad del rastreo.
- *Virus y troyanos:* el rastreo de virus basado en host evita la mayor parte de los virus y muchos troyanos.

Ilustración 11 Funciones de mitigación de ataques del módulo de acceso al edificio



Directrices del diseño

Teniendo en cuenta que los dispositivos de los usuarios suelen ser el elemento individual más grande de la red, la implementación de la seguridad en ellos de forma eficaz y concisa es un reto. Desde la perspectiva de la seguridad, es el módulo de distribución del edificio, más que ninguna otra cosa del módulo del edificio, el que proporciona la mayor parte del control de acceso que se utiliza a nivel de usuario final. Esto se debe a que el switch de Capa 2 con el que conectan las estaciones de trabajo y los teléfonos no tiene capacidad para el control de accesos a la Capa 3. Además de las pautas para la seguridad de la red descritas en el axioma de seguridad de switches, el rastreo de virus basado en host se implementa a nivel de estación de trabajo.

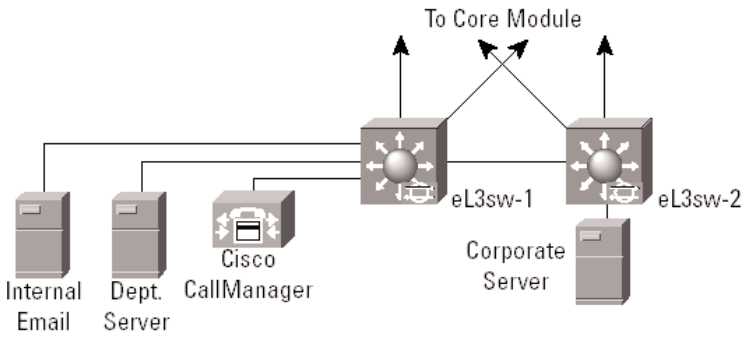
Módulo de servidores

El objetivo principal del módulo de servidores es proporcionar servicios de aplicaciones a los usuarios finales y a los dispositivos. Los flujos de tráfico del módulo de servidores los inspecciona la detección de intrusos a bordo en los switches de Capa 3.

Dispositivos principales

- *Switch de Capa 3:* proporciona servicios de Capa 3 a los servidores e inspecciona los datos que cruzan el módulo de servidores con NIDS
- *Gestor de llamadas:* realiza funciones de enrutamiento de llamadas para los dispositivos de telefonía por IP de la empresa.
- *Servidores de la empresa y de los departamentos:* ofrece servicios de archivos, impresión y DNS a las estaciones del módulo del edificio.
- *Servidor de correo electrónico:* proporciona servicios SMTP y POP3 a los usuarios internos.

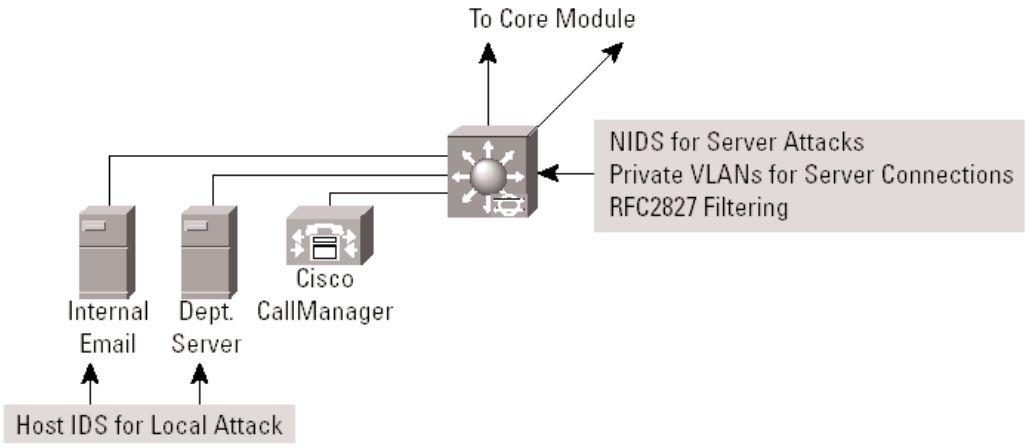
Ilustración 12 Módulo de servidores: detalle



Amenazas que combate

- *Acceso no autorizado:* combatido mediante el uso de detección de intrusos basada en hosts y del control de accesos.
- *Ataques a la capa de aplicaciones:* los sistemas operativos, los dispositivos y las aplicaciones se mantienen actualizados con las actualizaciones más recientes de seguridad y protegidos mediante IDS basado en host.
- *Ataques de falsificación (spoofing) de IP:* los filtros de RFC 2827 evitan la falsificación de direcciones de origen.
- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada limita la efectividad del rastreo.
- *Abuso de confianza:* las organizaciones de confianza son muy explícitas, las VLAN privadas evitan que los hosts de la misma subred se comuniquen a menos que sea necesario.
- *Redireccionamiento de puertos:* el IDS basado en host evita que se instalen agentes de redireccionamiento de puertos.

Ilustración 13 Funciones en el combate de ataques del módulo de servidores



Directrices del diseño

A menudo, el módulo de servidores se ignora a efectos de seguridad. Cuando se examinan los niveles de acceso que tienen la mayoría de los empleados a los servidores a los que están conectados, a menudo los servidores pueden convertirse en el objetivo principal de los ataques originados internamente. El mero uso de contraseñas eficaces no es suficiente para una estrategia global de combate de ataques. El uso de IDS basado en host y en red, VLAN privadas, control de accesos y buenas prácticas de administración de sistemas (como mantener los sistemas actualizados con los últimos parches) proporciona una respuesta mucho mas exhaustiva a los ataques.

Dado que el sistema NIDS tiene límites en la cantidad de tráfico que puede analizar, es importante enviarle solamente el tráfico sensible a ataques. Esto varía de una red a otra, pero probablemente debería incluir SMTP, Telnet, FTP y WWW. El NIDS basado en switch se eligió a causa de su capacidad para examinar solamente el tráfico interesante que cruza todas las VLAN, tal como lo definen las normativas de seguridad. Una vez ajustado correctamente, este IDS se puede configurar de forma restrictiva, ya que los flujos de tráfico necesarios deben conocerse bien.

Alternativas

Al igual que el módulo de distribución del edificio, el módulo de servidores se puede combinar con el módulo central si las necesidades de rendimiento no dictan la separación. Para entornos de servidores de alto rendimiento muy sensibles, la capacidad del NIDS en el switch de Capa 3 puede ampliarse instalando más de un módulo NIDS y dirigiendo el tráfico que coincide con las normativas a los módulos específicos.

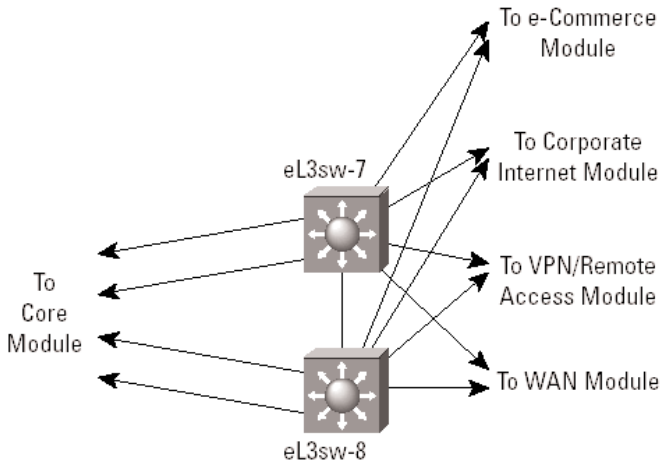
Módulo de distribución de contorno

El objetivo de este módulo es agregar la conectividad de los distintos elementos al contorno. El tráfico se filtra y se enruta desde los módulos de contorno al núcleo.

Dispositivos principales

- *Switches de Capa 3:* agregan conectividad de contorno y proporcionan servicios avanzados.

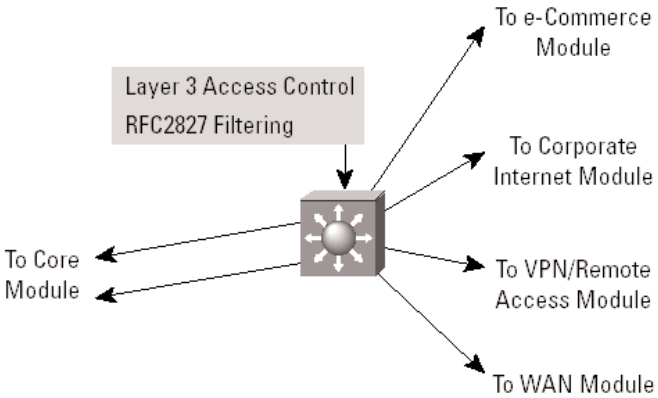
Ilustración 14 Módulo de distribución del contorno: detalle



Amenazas que combate

- *Acceso no autorizado:* los filtros proporcionan control granular a través de subredes específicas del contorno y su capacidad para acceder a áreas dentro de las oficinas centrales.
- *Ataques de falsificación (spoofing) de IP:* los filtros de RFC 2827 limitan los ataques de falsificación iniciados localmente.
- *Reconocimiento de la red:* los filtros limitan que el tráfico no esencial entre a las oficinas centrales limitando la capacidad de los hackers para realizar el reconocimiento de la red.
- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada limita la efectividad del rastreo.

Ilustración 15 Funciones de mitigación de ataques del módulo de distribución del contorno



Directrices del diseño

El módulo de distribución del contorno es similar, en algunos aspectos, al módulo de distribución del edificio en términos de función global. Ambos módulos emplean el control de acceso para filtrar tráfico, aunque el módulo de distribución del contorno puede confiar de algún modo en todo el área funcional del contorno para realizar otras funciones de seguridad. Ambos módulos utilizan la conmutación de Capa 3 para lograr un alto rendimiento, pero el módulo de distribución del contorno puede añadir otras funciones de seguridad, ya que los requisitos de rendimiento no son tan grandes. El módulo de distribución del contorno proporciona la última línea de defensa para todo el tráfico destinado al módulo de las oficinas centrales desde el módulo del contorno. Esto incluye la defensa contra los paquetes falsificados, actualizaciones erróneas de enrutamientos y provisiones para el control de acceso a las capas de la red.

Alternativas

Al igual que los módulos de servidores y de distribución del edificio, el módulo de distribución del contorno se puede combinar con el módulo central si los requisitos de rendimiento no son tan rigurosos como la implementación de referencias de SAFE. NIDS no está presente en este módulo, pero se podría colocar en él mediante el uso de tarjetas de línea IDS en los switches de Capa 3. Con eso se reduciría la necesidad de dispositivos NIDS a la salida de los módulos de contorno más importantes cuando se conectan con las oficinas centrales. Sin embargo, el rendimiento puede dictar, como hizo en el diseño de referencia de SAFE, que la detección dedicada de intrusos se coloque en los distintos módulos de contorno, al contrario que el módulo de distribución del contorno.

Contorno de la empresa

A continuación encontrará un análisis detallado de todos los módulos que contiene el contorno de la empresa.

Ilustración 16 Detalle del contorno de la empresa - Parte 1

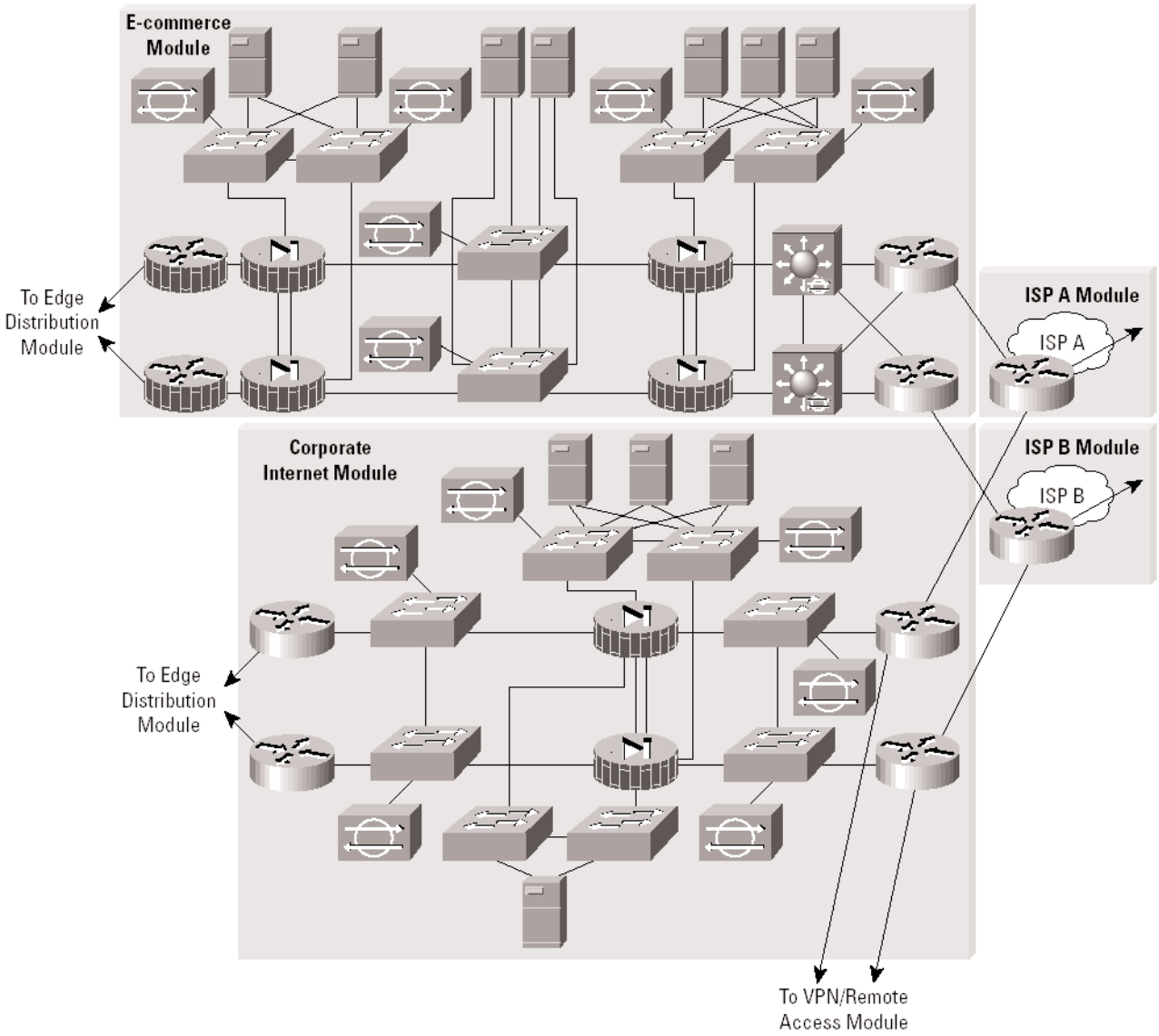
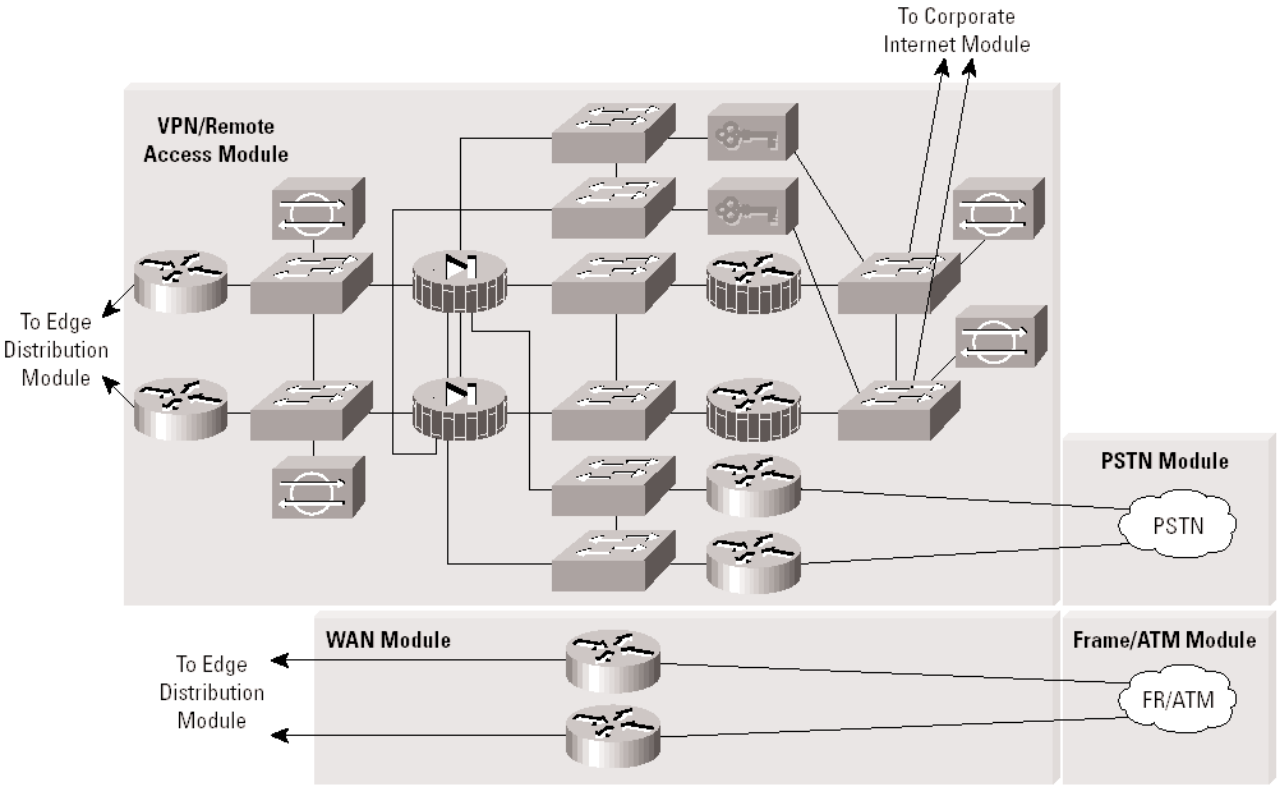


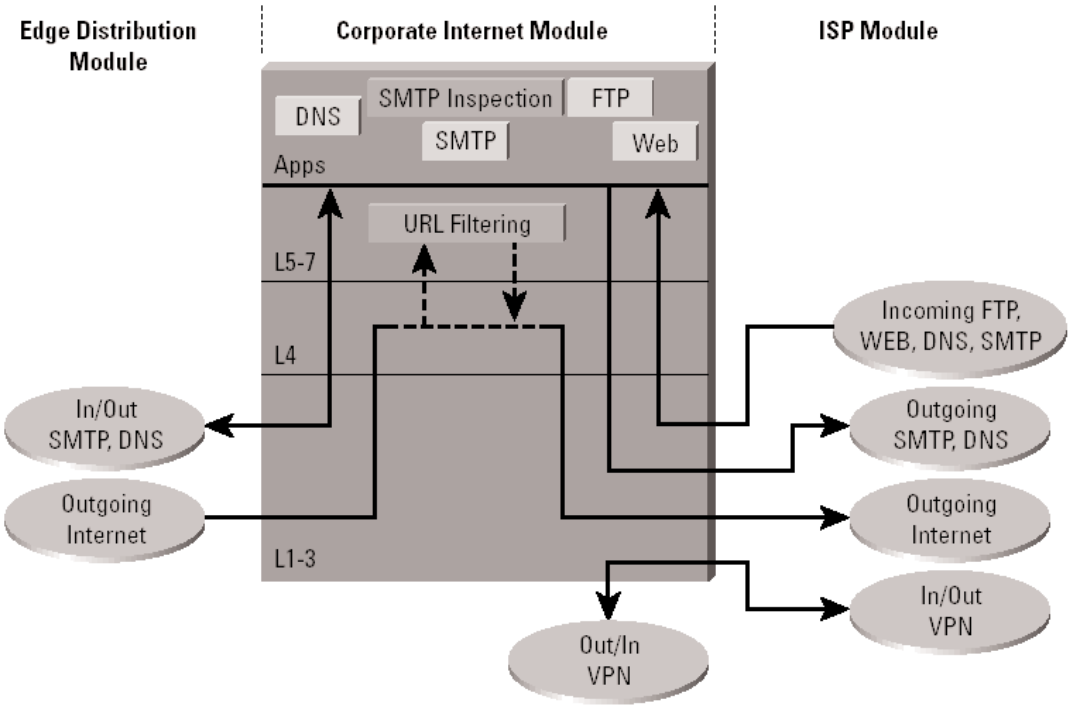
Ilustración 17 Detalle del contorno de la empresa - Parte 2



Módulo de Internet de la empresa

El módulo de Internet de la empresa proporciona a los usuarios internos conexión a los servicios de Internet y acceso a los usuarios de Internet a la información de los servidores públicos. El tráfico también fluye de este módulo de VPN y de acceso remoto en que tiene lugar la terminación de la VPN. Este módulo no está diseñado para servir aplicaciones de comercio electrónico. Para obtener más información sobre cómo ofrecer comercio por Internet, consulte la sección "Módulo de comercio electrónico" de este mismo documento.

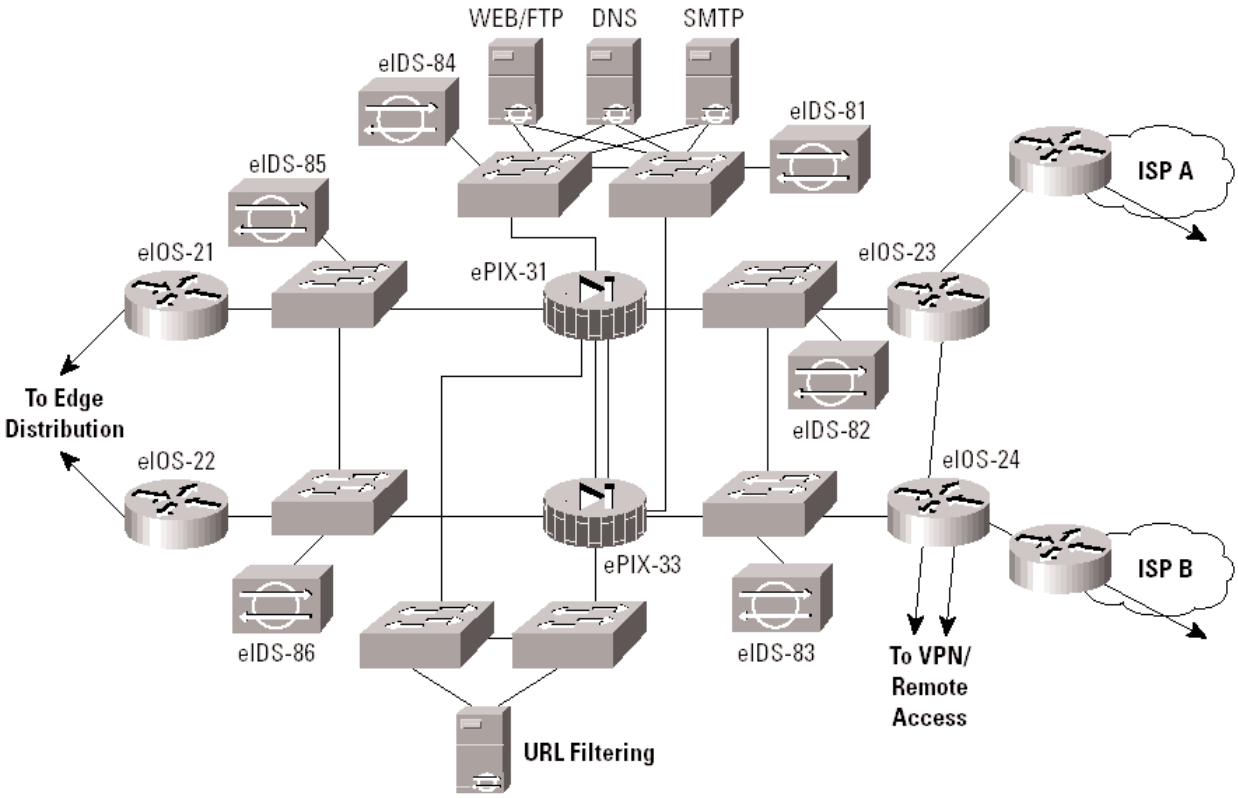
Ilustración 18 Flujo del tráfico de Internet de la empresa



Dispositivos principales

- *Servidor SMTP:* actúa como relay entre Internet y los servidores de correo de Internet (inspecciona los contenidos).
- *Servidor DNS:* sirve como servidor DNS externo autorizado de la empresa, transmite las solicitudes internas a Internet.
- *Servidor FTP/HTTP:* proporciona información pública acerca de la organización.
- *Firewall:* proporciona protección a nivel de red de los recursos y filtro con estado del tráfico.
- *Dispositivo de NIDS:* proporciona supervisión de la Capa 4 a la Capa 7 de los elementos de red clave del módulo.
- *Servidor de filtro de direcciones URL:* filtra las solicitudes de direcciones URL no autorizadas que provienen de la empresa.

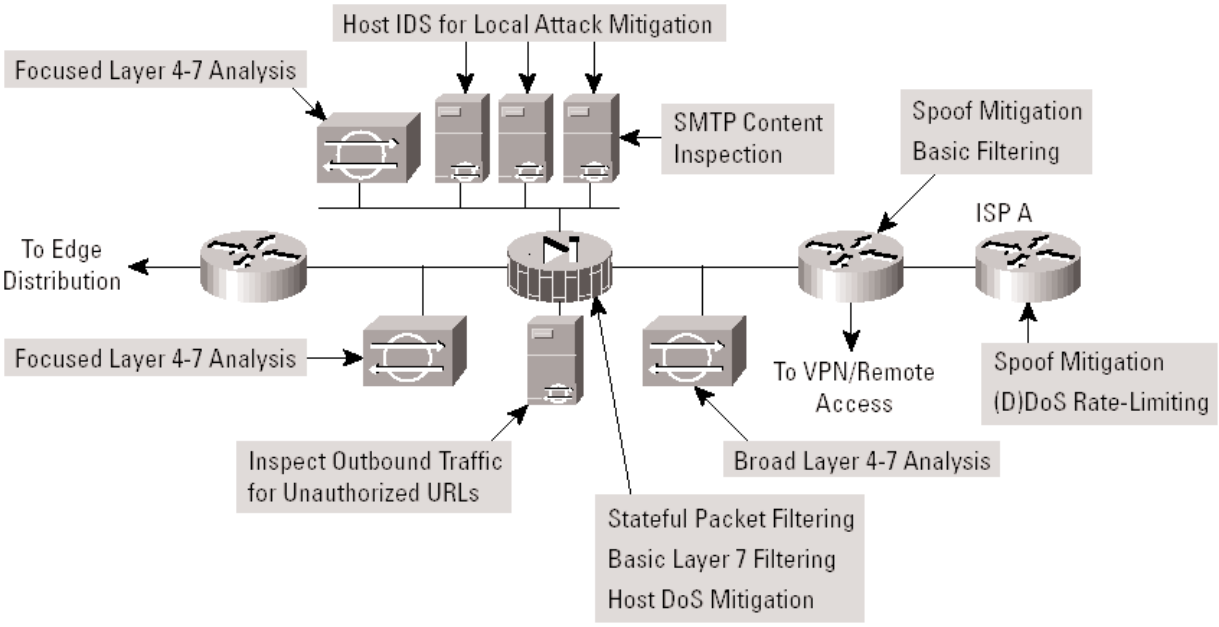
Ilustración 19 Módulo de Internet de la empresa: detalle



Amenazas que combate

- *Acceso no autorizado:* combatido a través de los filtros del ISP, del router del contorno y del firewall de la empresa.
- *Ataques a la capa de aplicaciones:* combatidos a través de IDS a los niveles de host y de red.
- *Virus y troyanos:* combatidos a través del filtro de los contenidos de los correos electrónicos y de IDS de los hosts.
- *Ataques a contraseñas:* servicios limitados disponibles para ataques por fuerza bruta, el sistema operativo e IDS pueden detectar la amenaza.
- *Denegación de servicio:* CAR en el contorno del ISP y los controles de configuración de TCP en el firewall
- *Ataques de falsificación (spoofing) de IP:* los filtros de RFC 2827 y 1918 en el contorno de ISP y del router de contorno de la empresa.
- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada e IDS de hosts limita la exposición.
- *Reconocimiento de la red:* IDS detecta el reconocimiento, se filtran los protocolos para limitar la eficacia.
- *Abuso de confianza*: un modelo de confianza restrictivo y VLAN privadas limitan los ataques basados en la confianza.
- *Redireccionamiento de puertos:* los filtros restrictivos y el IDS de hosts limitan el ataque

Ilustración 20 Funciones en el combate de ataques del módulo de Internet de la empresa



Directrices del diseño

El corazón del módulo es un par de firewalls resistentes que proporcionan protección a los servicios públicos de Internet y a los usuarios internos. La inspección con estado examina el tráfico en todas las direcciones asegurándose de que solo el tráfico legítimo atraviesa el firewall. Además de la resistencia de la Capa 2 y de la Capa 3 integrada en el módulo y la capacidad de recuperación con estado del firewall, las restantes consideraciónes del diseño se centran en la seguridad y la defensa contra ataques.

Comenzando en el router del contorno del cliente que hay en el ISP, la velocidad de salida del ISP limita el tráfico no esencial que supera los umbrales previamente especificados para combatir los ataques de (D)DoS. Además, en la salida del router del ISP, los filtros de RFC 1918 y RFC 2827 combaten la falsificación de las redes locales y de los rangos de redes privadas.

En la entrada del primer router de la red de la empresa, los filtros básicos limitan el tráfico al esperado (direcciones y servicios IP), proporcionando así un filtro tosco para los ataques más básicos. Aquí también se proporcionan los filtros de RFC 1918 y 2827 a modo de verificación de los filtros de ISP. Además, dada la enorme amenaza que crean contra la seguridad, el router está configurado para eliminar la mayoría de los paquetes fragmentados que normalmente no deberían verse de los tipos de tráfico estándar de Internet. Toda pérdida de tráfico legítimo perdido a causa de estos filtros se considera aceptable al compararla con el riesgo de permitir dicho tráfico. Por último se enruta adecuadamente el tráfico IPSec destinado al módulo de VPN y de acceso remoto. Los filtros de la interfaz conectada al módulo de VPN se configuran para que permitan pasar exclusivamente tráfico IPSec y sólo cuando el origen y el destino de dicho tráfico son pares autorizados. En el caso de las VPN de acceso remoto normalmente no se conoce la dirección IP del sistema entrante, por lo que los filtros sólo pueden ser específicos de los pares del extremo con los que se comunican los usuarios remotos.

El dispositivo NIDS de la parte pública del firewall controla los ataques basándose en el análisis de la Capa 4 a la Capa 7 y en las comparaciones con firmas conocidas. Teniendo en cuenta que el ISP y el filtro del contorno de la empresa filtran determinados rangos de direcciones y puertos, el dispositivo NIDS puede centrarse en algunos de los ataques más complejos. Las alarmas de dicho NIDS deben estar a un nivel menor que el de los dispositivos de dentro del firewall, ya que las alarmas que se ven aquí no representan brechas reales, solamente intentos de acceso.

El firewall proporciona cumplimiento del estado de las conexiones y filtros detallados para las sesiones iniciadas a través del firewall. Los servidores con direcciones públicas tienen cierta protección contra desbordamientos SYN de TCP a través del uso de límites de conexiones medio abiertas en el firewall. Desde el punto de vista de los filtros, además de limitar el tráfico en el segmento de servidores públicos a las direcciones y puertos pertinentes, también tiene lugar el filtro en la dirección opuesta. Si algún ataque pone en peligro a uno de los servidores públicos (sorteando el firewall, el IDS basado en host y el IDS basado en red) dicho servidor no podría atacar la red. Para combatir este tipo de ataque, el filtrado específico evita que los servidores públicos generen peticiones no autorizadas en otra ubicación. Como ejemplo, el servidor Web debería filtrarse para que no pueda originar solicitudes propias, sino meramente responder a las peticiones de los clientes. Esto ayuda a evitar que los hackers descarguen más utilidades en el equipo en peligro tras el ataque inicial. También ayuda a impedir que el hacker inicie sesiones no deseadas durante el ataque primario. Un ataque que genere un xterm desde el servidor Web a través del firewall a la máquina del hacker es un ejemplo de dicho ataque. Además, las VLAN privadas evitan que los servidores públicos que estén en peligro ataquen a otros servidores del mismo segmento. Este tráfico no lo detecta ni el firewall, que es el motivo por el que las VLAN privadas son vitales.

El tráfico del segmento de inspección de contenidos se limita a las solicitudes de filtro de direcciones URL desde el firewall al dispositivo de filtro de direcciones URL. Además, se permiten direcciones autenticadas desde el dispositivo de filtro de direcciones URL de la empresa a un servidor maestro para actualizar la base de datos. El dispositivo de filtro de direcciones URL inspecciona el tráfico saliente en busca de solicitudes no autorizadas de WWW. Comunica directamente con el firewall y aprueba o rechaza las solicitudes de direcciones URL que envía el firewall a su motor de inspección. Su decisión se basa en una normativa gestionada por la empresa que utiliza la información de clasificación de la WWW proporcionada por un servicio de terceros. La inspección de direcciones URL se prefirió sobre el filtro de acceso estándar, ya que las direcciones IP a menudo cambian en los sitios Web no autorizados y dichos filtros pueden crecer hasta ser muy grandes. El software de IDS basado en host de este servidor protege contra posibles ataques que, de algún modo sortean el firewall.

El segmento de servicios públicos incluye un dispositivo NIDS para detectar ataques a puertos que el firewall está configurado para permitir. Muy a menudo, éstos son ataques a la capa de aplicaciones contra un servicio específico o un ataque de contraseña contra un servicio protegido. Este NIDS debe definirse de una forma más restrictiva que el NIDS del exterior del firewall, ya que firmas que coinciden aquí han pasado correctamente a través del mismo. Todos los servidores tienen software de detección de intrusos en hosts para controlar cualquier actividad delictiva a nivel de sistema operativo, así como actividad en aplicaciones de servidor comunes (HTTP, FTP, SMTP, etc.). El host de DNS debe bloquearse para que responda solamente a los comandos deseados y elimine todas las respuestas innecesarias que puedan ayudar a los hackers en el reconocimiento de la red. Aquí se incluye impedir que realice transferencias de zona desde cualquier parte que no sean los servidores DNS internos. El servidor SMTP incluye servicios de inspección de los contenidos del correo que combaten los ataques de virus y troyanos generados contra la red interna y que suelen introducirse a través del sistema de correo. El propio firewall filtra los mensajes de SMTP en la Capa 7 para permitir solamente los comandos necesarios en el servidor de correo.

El dispositivo NIDS de la interfaz interna del firewall proporciona un análisis final de los ataques. En este segmento se deberían detectar muy pocos ataques, ya sólo se permiten respuestas a solicitudes iniciadas y unos pocos puertos seleccionados del segmento de servicios públicos. En este segmento sólo deberían verse los ataques sofisticados, ya que suele significar que se ha puesto en peligro un segmento de los servicios públicos y que el hacker está intentando hacer uso de este punto de apoyo para atacar la red interna. Por ejemplo, si el servidor SMTP público estuviera en peligro, un hacker podría intentar atacar el servidor de correo interno a través del puerto 25 de TCP, lo que se permite para que haya transferencias de correo entre dos hosts. Si se ven ataques en este segmento, las respuestas a dichos ataques deberían ser más severas que las de los restantes segmentos, ya que probablemente indican que ya se ha producido algún peligro. El uso de reinicios de TCP para frustrar, por ejemplo, el ataque SMTP mencionado antes, debería considerarse seriamente.

Alternativas

Hay varios diseños alternativos para este módulo. Por ejemplo, en función de su actitud hacia el conocimiento de los ataques, es posible que no hagan falta los dispositivos de NIDS delante del firewall. De hecho, sin filtros básicos en el router de acceso, este tipo de supervisión no es aconsejable. Con los filtros básicos apropiados, que existen en este diseño, el IDS externo del firewall puede ofrecer información importante sobre las alarmas que en caso contrario omitiría el firewall. Teniendo en cuenta que el número de alarmas generadas en este segmento es grande, deberían tener menos importancia que las generadas detrás de un firewall. Además, plantéese la posibilidad de registrar las alarmas de este segmento en una estación de gestión independiente, con el fin de garantizar que las alarmas legítimas de otros segmentos reciben la atención adecuada. Con la visibilidad que proporciona el NIDS de fuera del firewall, se ve mejor la evaluación de los tipos de ataques que atrae su organización. Además, se puede realizar la evaluación de la eficacia del ISP y de los filtros del contorno de la empresa.

Otra posible alternativa al diseño propuesto es la eliminación del router entre el firewall y el módulo de distribución del contorno. Aunque estas funciones pueden integrarse en el módulo de distribución del contorno, la separación funcional entre los módulos se perdería debido a que los switches de distribución del contorno necesitarían conocer toda la topología del módulo de Internet de la empresa para garantizar un enrutamiento apropiado. Además, esto limita la capacidad para instalar esta arquitectura de forma modular. Por ejemplo, si el núcleo actual de una empresa es la Capa 2, sería necesario el enrutamiento que se proporciona en el módulo de Internet de la empresa.

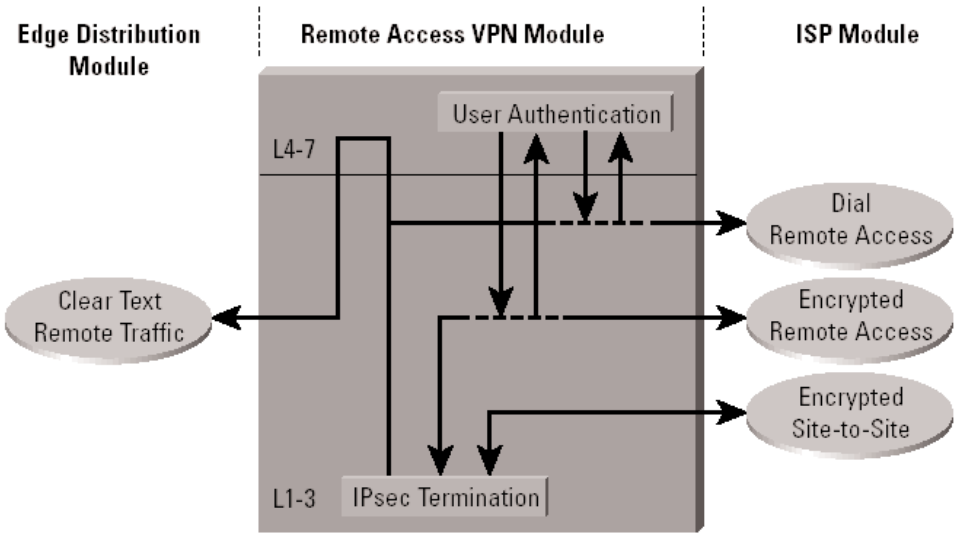
Objetivos de la arquitectura a corto plazo

Es necesario desarrollar la tecnología de firewalls de Cisco que se puedan comunicar directamente con otros dispositivos de inspección de contenidos (por ejemplo el rastreo de virus en toda la red). Actualmente, el filtro de direcciones URL es la única función de filtro de contenidos admitida que se integra directamente con la tecnología de firewalls de Cisco. Los productos no integrados descansan en los usuarios que funcionan en un modo proxy que no se escala correctamente.

Módulo de VPN y de acceso remoto

Como su nombre implica, el objetivo principal de este módulo se divide en tres: terminar el tráfico VPN de los usuarios remotos, proporcionar un hub para terminar el tráfico VPN de los sitios remotos y terminar los usuarios de acceso telefónico tradicionales. Todo el tráfico que se envía a la distribución del contorno es de los usuarios remotos de la empresa que están autenticados de alguna forma antes de que puedan pasar por el firewall.

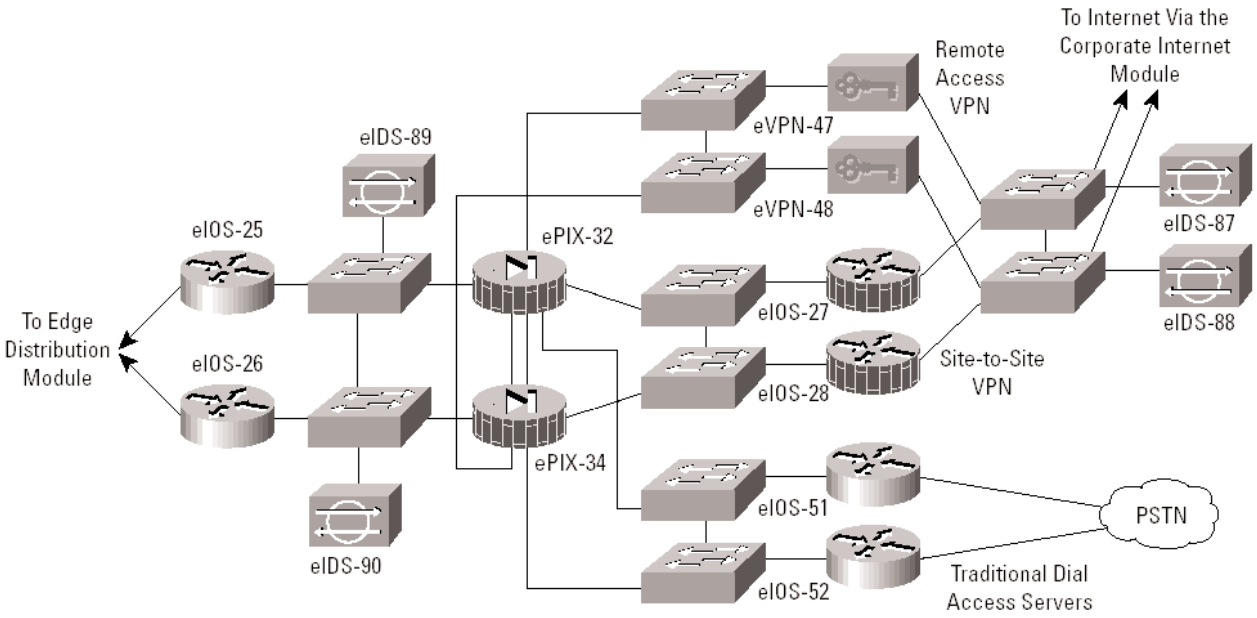
Ilustración 21 Flujo de tráfico del módulo de VPN de acceso remoto



Dispositivos principales

- *Concentrador de VPN:* autentica a los usuarios individuales remotos que utilicen Extended Authentication (XAUTH) y termina sus túneles IPSec.
- *Router VPN:* autentica los sitios remotos en los que se confía y proporciona conectividad utilizando túneles GRE/IPSec.
- *Servidor de acceso telefónico:* autentica a los usuarios remotos individuales utilizando TACACS+ y termina sus conexiones analógicas.
- *Firewall:* proporciona seguridad diferenciada para los tres tipos diferentes de acceso remoto.
- *Dispositivo de NIDS:* proporciona supervisión de la Capa 4 a la Capa 7 de los segmentos de red claves del módulo.

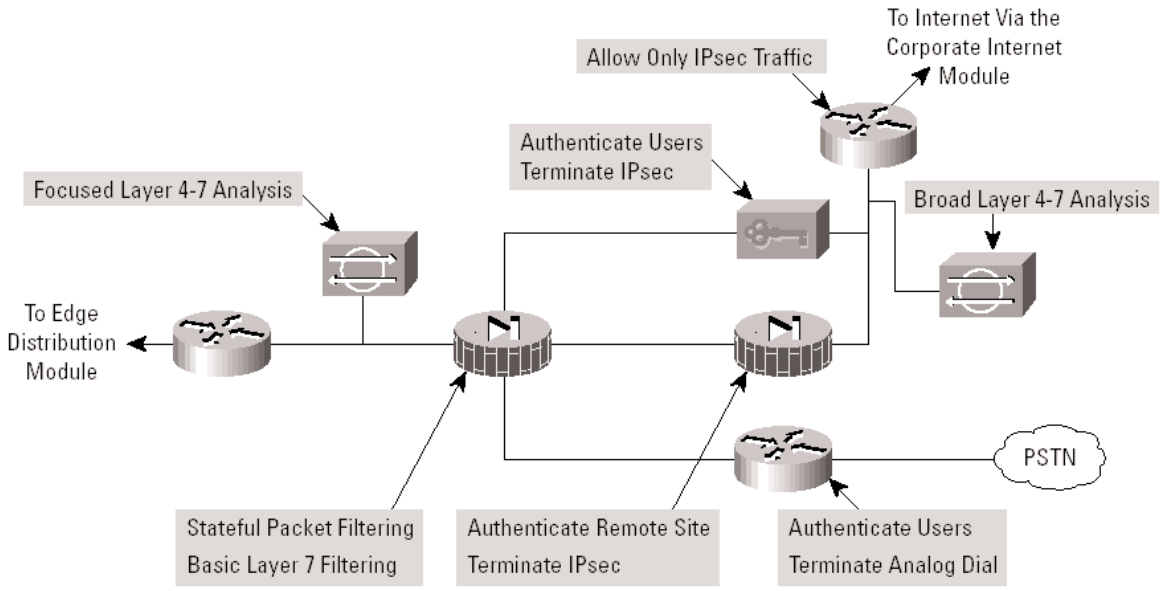
Ilustración 22 Módulo VPN de acceso remoto: detalle



Amenazas que combate

- *Descubrimiento de la topología de la red:* en este segmento sólo se permiten Internet Key Exchange (IKE) y Encapsulating Security Payload (ESP) de Internet
- *Ataque a contraseñas:* la autenticación de OTP reduce la probabilidad de se produzca un ataque a contraseñas con éxito.
- *Acceso no autorizado:* los servicios del firewall después del descifrado de paquetes evitan que haya tráfico en los puertos no autorizados.
- *Ataques del tipo Man in the Middle:* se combaten a través de tráfico remoto cifrado.
- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada limita la efectividad del rastreo.

Ilustración 23 Funciones de mitigación de ataques del módulo VPN de acceso remoto



Directrices del diseño

Dejando aparte la resistencia, el requisito principal de este módulo es tener tres servicios de usuarios externos autenticados e independientes. Teniendo en cuenta que el tráfico proviene de distintas fuentes de fuera de la red de la empresa, la decisión se tomó para proporcionar una interfaz independiente en el firewall para cada uno de estos servicios. La consideración del diseño de cada uno de los servicios se muestra a continuación.

VPN de acceso remoto

El tráfico de la VPN se reenvía desde los routers de acceso del módulo de Internet de la empresa, donde se filtra por primera vez en el punto de salida a las direcciones IP y los protocolos que forman parte de los servicios de VPN. Las actuales VPN de acceso remoto pueden utilizar distintos protocolos de tunelización y seguridad. Aunque IPSec es el protocolo de tunelización elegido, muchas organizaciones emplean los protocolos Point-to-Point Tunneling Protocol (PPTP) y Layer 2 Tunneling Protocol (L2TP), ya que los sistemas operativos de sobremesa más usados los admiten de forma nativa. En SAFE, se eligió IPSec porque la configuración que necesitan los clientes es mínima y porque, al mismo tiempo, proporciona mucha seguridad.

El tráfico VPN de acceso remoto se direccionará a una dirección pública específica utilizando el protocolo IKE (UDP 500). Teniendo en cuenta que la conexión IKE no está completa hasta que se proporciona la información de autenticación correcta, esto proporciona cierta disuasión para el hacker potencial. Como parte de las extensiones (borrador de RFC) de IKE, XAUTH proporciona un mecanismo de autenticación de usuarios adicional antes de que se asignen los parámetros de IP al usuario remoto. El concentrador de VPN está "conectado" al servidor de control de accesos de la subred de gestión a través de su interfaz de gestión. Las contraseñas fuertes se proporcionan a través del servidor de contraseñas únicas.

Una vez autenticado, se proporciona acceso al usuario remoto al recibir los parámetros de IP utilizando otra extensión de IKE, MODCFG. Aparte de una dirección IP y la ubicación de los servidores de nombres (DNS y WINS), MODCFG también proporciona servicios de autorización para controlar el acceso del usuario remoto. Por ejemplo en SAFE se impide a los usuarios activar la tunelización de splits, obligando de esa forma al usuario a acceder a Internet a través de la conexión de la empresa. Los parámetros de IPSec que se van a utilizar son Triple DES para el cifrado y SHA-HMAC para la integridad de los datos. Los módulos de cifrado por hardware del concentrador de VPN permiten instalar de forma ampliable a miles de usuarios remotos. Tras la terminación del túnel de VPN, el tráfico se envía a través de un firewall para garantizar que los usuarios de VPN se filtran correctamente.

La gestión segura de este servicio se logra llevando todos los parámetros de IPSec y de seguridad a los usuarios remotos desde el sitio central. Además, las conexiones a todas las funciones de gestión se encuentran en una interfaz de gestión dedicada.

Usuarios con acceso telefónico

Los usuarios de acceso telefónico tradicionales se terminan en uno de los dos routers de acceso con modems integrados. Una vez que se establece la conexión de la Capa 1 entre el usuario y el servidor, se utiliza un CHAP a tres para autenticar al usuario. Al igual que en el servicio de VPN de acceso remoto, los servidores de AAA y de contraseñas únicas se utilizan para autenticar y proporcionar contraseñas. Una vez autenticados, se proporcionan direcciones IP a los usuarios desde un grupo de IP a través de PPP.

VPN de ubicación a ubicación

El tráfico VPN asociado con las conexiones de ubicación a ubicación se compone de túneles GRE protegidos por un protocolo IPSec en modo de transporte utilizando Encapsulated Security Payload (ESP). Como en el caso del acceso remoto, el tráfico que se reenvía desde el módulo de Internet de la empresa se puede limitar a las direcciones de destino específicas de los dos routers VPN y a las direcciones de origen que se esperan de los sitios remotos. Los protocolos ESP (IP 50) e IKE serán los dos únicos que se esperan en esta conexión.

GRE se utiliza para proporcionar una conexión remota con todos los servicios que transportará tráfico multiprotocolo, con enrutamiento de protocolo y multidifusión. Dado que los protocolos de enrutamiento (el protocolo Enhanced Interior Gateway Routing Protocol [EIGRP] se va a usar entre sitios remotos) pueden detectar fallos en la conexión, el túnel GRE proporciona un mecanismo de resistencia para los sitios remotos si crean dos conexiones de encapsulado de enrutamiento genérico (GRE), una a cada uno de los routers VPN centrales.

Como en las VPN de acceso remoto, 3DES y SHA-HMAC se utilizan para que los parámetros de IKE y de IPSec proporcionen la máxima seguridad sin que ello afecte casi al rendimiento. Los aceleradores de IPSec por hardware se emplean en los routers VPN.

El resto del módulo

El firewall agrega el tráfico de los tres servicios a una interfaz privada antes de enviarlo al módulo de distribución del contorno a través de dos routers. El firewall debe configurarse con el tipo correcto de limitación en el control de acceso para que sólo permita pasar el tráfico apropiado de cada uno de los servicios a la interfaz interna del firewall. Un par de dispositivos NIDS están colocados en la parte pública del módulo para detectar cualquier actividad de "reconocimiento" de la red dirigida a los dispositivos de terminación de la VPN. En este segmento, solo debería verse el tráfico de IPSec (IKE/ESP). Teniendo en cuenta que el sistema NIDS no puede ver la parte interior de los paquetes IPSec, cualquier alarma de esta red indica que los dispositivos circundantes están en peligro o están fallando. Como tales, deben definirse niveles de seguridad muy altos en dichas alarmas. Un segundo par de NIDS están colocados detrás del firewall para detectar cualquier ataque que pase al resto del módulo. Este dispositivo NIDS también tiene una normativa restrictiva. Todos los usuarios que crucen este segmento deben estar enlazados o provenir de una ubicación remota, con el fin de que los rechazos o reinicios de TCP sólo afecten a dichos usuarios.

Alternativas

En VPN y en la tecnología de autenticación, hay muchas alternativas disponibles en función de los requisitos de la red. Estas alternativas se indican a continuación a modo de referencia, pero los detalles no se muestran en este documento.

- Autenticación con tarjeta inteligente y/o biométrica.
- Túneles VPN de acceso remoto L2TP y/o PPTP.
- Autoridades de certificación (CA).
- Mecanismo de resistencia keep-alive IKE.
- VPN con Multiprotocol Label Switching (MPLS)

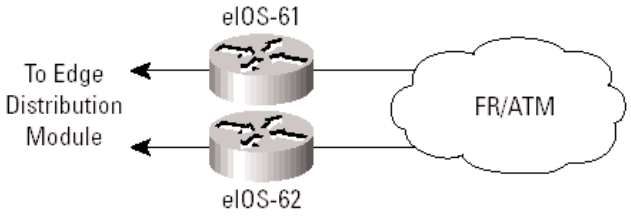
Módulo de WAN

En lugar de incluir todos los diseños potenciales de WAN, este módulo muestra la resistencia y la seguridad de la terminación de WAN. Utilizando la encapsulación de Frame Relay, el tráfico se enruta entre los sitios remotos y el sitio central.

Dispositivos principales

- *Router IOS:* utiliza el enrutamiento, el control de accesos y mecanismos de QoS.

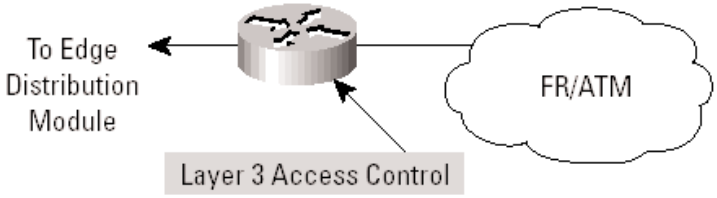
Ilustración 24 Módulo de WAN: detalle



Amenazas que combate

- *Ataques de falsificación (spoofing) de IP:* combatidos a través de los filtros de la Capa 3.
- *Acceso no autorizado:* el control de acceso simple del router puede limitar los tipos de protocolos a los que tienen acceso las sucursales.

Ilustración 25 Funciones de mitigación de ataques del módulo de WAN



Directrices del diseño

La resistencia la proporciona la conexión dual desde el proveedor de servicios, a través de los routers y al módulo de distribución del contorno. La seguridad se proporciona utilizando las características de seguridad de IOS. Las listas de accesos de entrada se utilizan para bloquear todo el tráfico no deseado de las sucursales remotas.

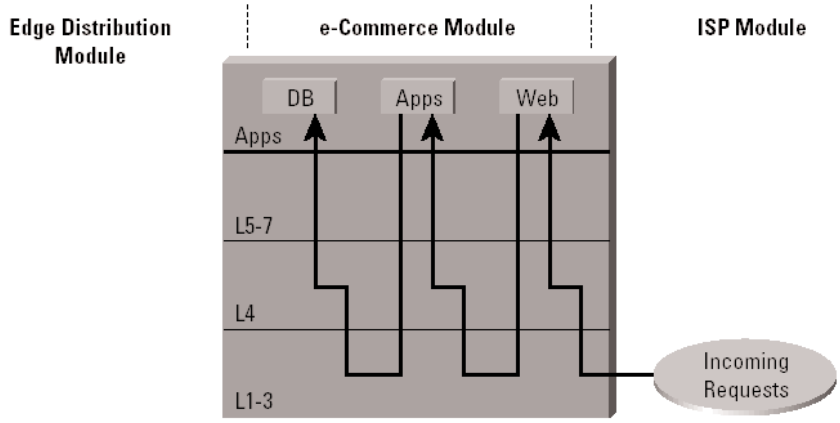
Alternativas

Algunas organizaciones que cuidan mucho la privacidad de la información cifran el tráfico muy confidencial de sus conexiones WAN. De forma parecida a las VPN de ubicación a ubicación, se puede emplear IPSec para lograr esta privacidad de la información.

Módulo de comercio electrónico

Dado que el comercio electrónico es el objetivo principal de este módulo, hay que ponderar con sumo cuidado el equilibrio entre el acceso y la seguridad. La división de la transacción del comercio electrónico en tres componentes permiten que la arquitectura proporcione varios niveles de seguridad sin impedir el acceso.

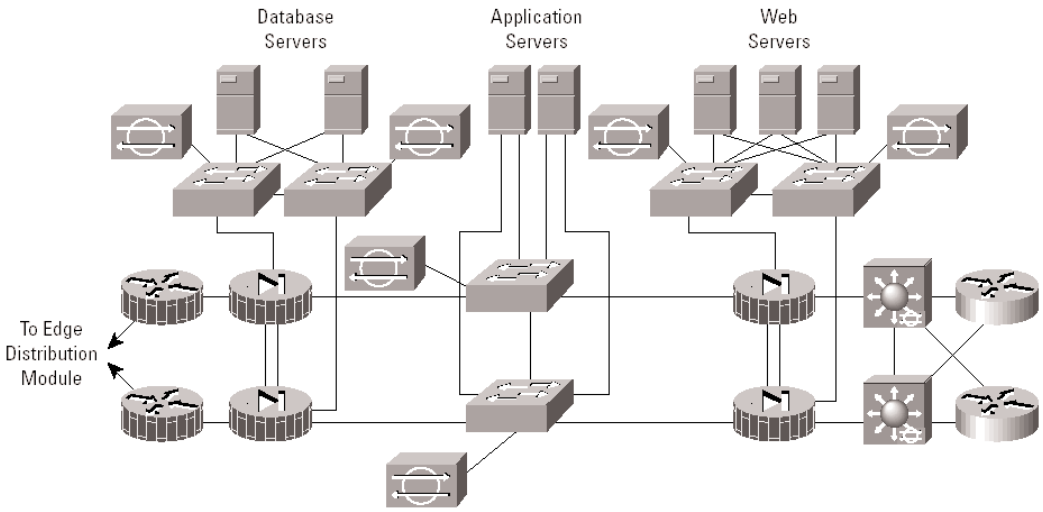
Ilustración 26 Flujo de tráfico del comercio electrónico



Dispositivos principales

- *Servidor de Web:* actúa como interfaz principal del usuario para el desplazamiento por el almacén del comercio electrónico.
- *Servidor de aplicaciones:* es la plataforma para las distintas aplicaciones que necesita el servidor de Web.
- *Servidor de bases de datos:* es la información crítica que está en el centro de la implementación del comercio electrónico.
- *Firewall:* gobierna la comunicación entre los distintos niveles de seguridad y de confianza del sistema.
- *Dispositivo de NIDS:* proporciona supervisión de los elementos de red clave del módulo.
- *Switch de Capa 3 con módulo de IDS:* es el dispositivo ampliable de entrada de comercio electrónico con control integrado de la seguridad.

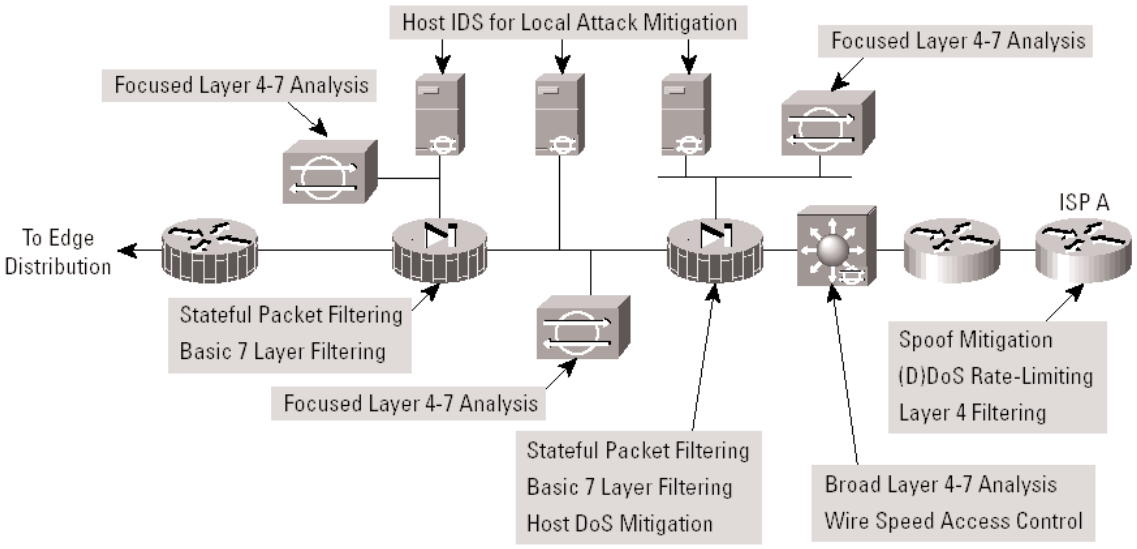
Ilustración 27 Módulo de comercio electrónico: detalle



Amenazas que combate

- *Acceso no autorizado:* los firewall con estado y las ACL limitan la exposición de ciertos protocolos.
- *Ataques a la capa de aplicaciones:* los ataques se combaten mediante el uso de IDS.
- *Denegación de servicio:* los filtros y la limitación de velocidad del ISP reducen el potencial de (D)DoS.
- *Ataques de falsificación (spoofing) de IP:* RFC 2827 y 1918 evitan los paquetes falsificados con origen local y limitan los intentos de falsificación remota.
- *Rastreadores de paquetes (Packet Sniffers):* una infraestructura conmutada y HIDS limitan la efectividad del rastreo.
- *Reconocimiento de la red:* los puertos se limitan a lo que sea necesario, el protocolo ICMP está restringido.
- *Abuso de confianza:* los firewalls garantizan que la comunicación fluye solamente en la dirección correcta del servicio apropiado.
- *Redireccionamiento de puertos:* HIDS y los filtros de los firewalls limitan la exposición a estos ataques.

Ilustración 28 Funciones en el combate de ataques del módulo de comercio electrónico



Descripción de la implementación del diseño

El corazón del módulo son dos pares de firewalls resistentes que proporcionan protección a los tres niveles de servidores: Web, aplicación y base de datos. Los routers de contorno del ISP proporcionan más protección al propio ISP y a la empresa. El diseño se entiende mejor si se tiene en cuenta la secuencia de flujo y la dirección del tráfico de las transacciones típicas de comercio electrónico.

El cliente de comercio electrónico inicia una conexión HTTP con el servidor de Web tras recibir la dirección IP de un servidor DNS alojado en la red del ISP. El DNS se aloja en otra red para reducir la cantidad de protocolos que necesita la aplicación de comercio electrónico. El primer conjunto de firewalls debe configurarse para que este protocolo pueda pasar a dicha dirección específica. Se permite que vuelva el tráfico de retorno de esta conexión, pero no hay necesidad de que ninguna comunicación que inicie el servidor de Web vuelva a Internet. El firewall debería bloquear esta ruta para limitar las opciones de los hackers si tuvieran control de uno de los servidores de Web.

A medida que el usuario se desplaza por el sitio Web, determinadas elecciones de conexiones hacen que el servidor de Web inicie una petición al servidor de aplicaciones de la interfaz interna. El primer firewall debe permitir tanto esta conexión como el tráfico de retorno asociado. Como ocurre con el servidor de Web, no hay ningún motivo para que el servidor de aplicaciones inicie una conexión con el servidor de Web o, incluso, con Internet. De igual modo, toda la sesión del usuario funciona sobre HTTP y SSL sin la posibilidad de comunicarse directamente con el servidor de aplicaciones ni con el servidor de bases de datos.

En algún momento, el usuario deseará llevar a cabo una transacción. El servidor de Web querrá proteger esta transacción y será necesario el protocolo SSL desde Internet al servidor de Web. Al mismo tiempo, es posible que el servidor de aplicaciones desee realizar alguna consulta o pasar la información al servidor de bases de datos. Éstas son las consultas SQL típicas que inicia el servidor de aplicaciones y llegan al servidor de bases de datos y no viceversa. Estas consultas pasan por el segundo firewall hasta el servidor de bases de datos. Dependiendo de las aplicaciones determinadas que estén en uso, es posible que el servidor de bases de datos no necesite comunicarse con los sistemas de nodos situados en el módulo de servidores de la empresa.

En resumen, los firewalls sólo deben permitir tres rutas de comunicación específicas, cada una de ellas con su propio protocolo, y bloquear las restantes comunicaciones, a menos que sean los paquetes de la ruta de retorno que están asociados con las tres rutas originales.

Los propios servidores deben estar perfectamente protegidos, sobre todo el servidor de Web, que es un host con direcciones públicas. Tanto el sistema operativo como la aplicación del servidor de Web deben actualizarse con las últimas versiones de los parches y debe controlarlos el software de detección de intrusos. Esto debería combatir la mayoría de los ataques principales y secundarios a la capa de aplicaciones, como el redireccionamiento de puertos y root kits. Los restantes servidores deberían tener una seguridad similar, por si el primer servidor o el firewall están en peligro.

Después del firewall

Los firewalls de comercio electrónico están protegidos inicialmente por el router de contorno del cliente en el ISP. En el punto de salida del router, hacia la empresa, el ISP puede limitar el tráfico al pequeño número de protocolos necesarios para el comercio electrónico cuya dirección de destino sea solamente servidores de Web. Los routers de contorno necesitan actualizaciones de los protocolos de enrutamiento (normalmente el protocolo Border Gateway Protocol [BGP]) y el tráfico restante debería bloquearse. El ISP debe implementar la limitación de la velocidad, como se especifica en la sección "Axiomas de SAFE" para combatir los ataques de (D)DoS. Además, el ISP también debe implementar los filtros según RFC1918 y RFC2827.

En las instalaciones de la empresa, el router inicial sólo sirve de interfaz con el ISP. El switch de Capa 3 realiza todo el procesamiento de la red, ya que tiene características descargadas a los procesadores por hardware. Los switches de Capa 3 participan en toda la decisión de enrutamiento por BGP para decidir qué ISP tiene la mejor ruta para el usuario determinado. Los switches de Capa 3 también proporcionan filtros de verificación que funcionan a la vez que los filtros del ISP ya descritos; esto proporciona una seguridad que se solapa. En tercer lugar, los switches de Capa 3 proporcionan control IDS integrado. Si la conexión con Internet supera la capacidad de la tarjeta de línea de IDS, es posible que haya que fijarse solamente en las solicitudes de Web que entran desde Internet de la tarjeta de línea de IDS. Aunque esto omitirá algunas firmas de alarmas de http (aproximadamente un diez por ciento), es mejor que examinar todo el flujo en ambas direcciones, donde podrían producirse muchas omisiones. Los restantes dispositivos NIDS que están detrás de las distintas interfaces del firewall controlan en los segmentos si algún ataque ha penetrado en la primera línea de defensa. Por ejemplo, si el servidor de Web está anticuado, los hackers podrían ponerlo en peligro con un ataque a la capa de aplicaciones, suponiendo que fueran capaces de eludir el HIDS. Como en el módulo de Internet de la empresa, hay que eliminar los falsos positivos para que todas las detecciones de ataques se traten con el nivel de prioridad correcto. De hecho, dado que sólo ciertos tipos de tráfico existen en segmentos determinados, se puede ajustar mucho NIDS.

Desde el punto de vista de las aplicaciones, las rutas de comunicaciones entre las distintas capas (web, apps, dbase) deberían estar cifradas, ser transaccionales y tener mucha autenticación. Por ejemplo, si el servidor de aplicaciones tuviera que obtener datos de la base de datos a través de algún tipo de sesión interactiva con scripts (SSH, FTP, Telnet, etc.), los hackers podrían hacer uso de dicha sesión interactiva para iniciar un ataque a la capa de aplicaciones. Mediante el uso de comunicaciones seguras se pueden limitar las amenazas potenciales.

Los switches de Capa 2 que admiten los distintos segmentos del firewall permiten implementar VLAN privadas, con lo que implementan un modelo de confianza que coincide con la comunicación deseada del tráfico de un segmento específico y elimina el restante. Por ejemplo, no suele haber ninguna razón para que un servidor de Web se comunique con otro.

La gestión de todo el módulo se realiza totalmente fuera de banda, como en el resto de la arquitectura.

Alternativas

La alternativa principal a esta instalación es la colocación de todo el sistema en un ISP. Aunque el diseño sigue siendo el mismo, hay dos diferencias principales. La primera es que el ancho de banda suele ser mayor en el ISP y emplea una conexión LAN. Aunque no es aconsejable, con esto se elimina potencialmente la necesidad de los routers de contorno en el diseño propuesto. El ancho de banda adicional también crea distintos requisitos para combatir ataques (D)DoS. La segunda es la conexión de vuelta a la empresa, que hay que gestionar de forma distinta. Las alternativas incluyen el cifrado y las líneas privadas. El uso de estas tecnologías crea más consideraciones de seguridad, en función de la ubicación de las conexiones y su uso deseado.

Hay varias variaciones en el diseño principal de este módulo. Aparte de mostrar las alternativas, este informe no explicará más detalles, ya que están fuera de su ámbito.

- El uso de más firewalls es una alternativa. Las comunicaciones de ejemplo serían: enrutamiento de contorno -> firewall -> servidor de web -> firewall -> servidor de aplicaciones -> firewall -> servidor de bases de datos. Esto permite que cada firewall controle solamente las comunicaciones de un sistema primario.
- El balanceo de cargas y las tecnologías de almacenamiento en caché no se explican en este informe, pero pueden integrarse en esta arquitectura sin modificaciones importantes. En un próximo informe se explicarán estas necesidades.
- Para requisitos de seguridad muy exigentes, es posible que haya que pensar en el uso de varios tipos de firewall.

Tenga en cuenta que esto crea una sobrecarga adicional en la gestión, ya que duplica la normativa en sistemas dispares. El objetivo de este diseño es evitar que cualquier vulnerabilidad en un firewall permita sortear la seguridad de todo el sistema. Estos tipos de diseños suelen centrarse mucho en los firewalls y no utilizan correctamente el IDS ni otras tecnologías de seguridad para combatir el riesgo de un solo punto vulnerable en un firewall.

Opciones de las empresas

A menudo, el proceso de diseño es una serie de intercambios. Esta breve subsección del documento resalta alguna de las opciones de alto nivel que pueden implementar los diseñadores de red si se encuentran con grandes restricciones presupuestarias. Algunos de estos intercambios se realizan a nivel de módulos, mientras que otros se realizan a nivel de componentes.

Una primera opción es contraer los módulos de distribución en el módulo central, lo que reduce el número de switches de Capa 3 al cincuenta por ciento. El ahorro de costes se compensaría con los requisitos de memoria del núcleo de la red y con la flexibilidad para implementar todos los filtros de seguridad de la distribución.

Una segunda opción es combinar la funcionalidad del módulo de VPN y de acceso remoto con el módulo de Internet de la empresa. Su estructura es muy similar, con un par de firewalls en el centro del módulo rodeados por dispositivos NIDS. Esto puede conseguirse sin pérdida de funcionalidad si el rendimiento de los componentes coincide con los requisitos de tráfico combinados de los módulos y si el firewall tiene suficientes interfaces para acomodar los diferentes servicios. Tenga en cuenta que a medida que se agregan funciones a dispositivos individuales aumenta el potencial de errores humanos. Algunas organizaciones van incluso más allá e incluyen las funciones de comercio electrónico en el módulo de Internet de la empresa/VPN. Los autores creen que el riesgo de esta práctica supera los ahorros de costes, a menos que las necesidades de comercio electrónico sean mínimas. La separación del tráfico de comercio electrónico del tráfico general de Internet permite optimizar más el ancho de banda del comercio electrónico, ya que permite al ISP poner filtros más restrictivos y utilizar la tecnología de limitación de velocidad para combatir ataques de DDoS.

Una tercera opción es eliminar algunos de los dispositivos de NIDS. Dependiendo de la estrategia de respuestas a las amenazas operativas, es posible que necesite menos dispositivos de NIDS. Este número también resulta afectado por la cantidad de ID de hosts instaladas, ya que esto puede reducir la necesidad de NIDS en ciertas ubicaciones. Esto se explica, donde es pertinente, en los módulos específicos.

Indudablemente, el diseño de redes no es una ciencia exacta. Las opciones siempre deben elegirse en función de los requisitos específicos a los que se enfrenta el diseñador. Los autores no proponen que ningún diseñador implemente esta arquitectura al pie de la letra, pero animan a los diseñadores a realizar elecciones acerca de la seguridad de red fundadas en esta implementación probada.

Estrategias de migración

SAFE es una guía para implementar la seguridad en la red de la empresa. No está pensado para servir de normativa de seguridad de las redes de las empresas ni tampoco como diseño global para proporcionar una seguridad total a todas las redes existentes. Mas bien, SAFE es una plantilla que permite a los diseñadores de redes pensar cómo diseñar e implementar las redes de las empresas para satisfacer sus requisitos de seguridad.

El establecimiento de una normativa de seguridad debe ser la primera actividad a la hora de migrar la red a una infraestructura segura. Las recomendaciones básicas para una normativa de seguridad se pueden encontrar al final del documento, en el anexo B, "Manual de seguridad de redes". Tras establecer la normativa, el diseñador de la red debería tener en cuenta los axiomas de seguridad descritos en la primera sección de este documento y ver cómo proporcionan más detalles para asignar la política a la infraestructura de red existente.

Hay suficiente flexibilidad en la arquitectura e información sobre las consideraciones que se deben tener en cuenta al realizar el diseño como para permitir que los elementos de la arquitectura de SAFE se adapten a las redes de la mayoría de las empresas. Por ejemplo, en el módulo de VPN y de acceso remoto, se asigna a los distintos flujos de tráfico de las redes públicas un par de dispositivos de separación independientes y una interfaz independiente en el firewall. El tráfico de la VPN se podría combinar en un par de dispositivos, siempre que los requisitos lo permitieran y que la normativa de seguridad fuera la misma para ambos tipos de tráfico. En otra red, los usuarios de acceso telefónico tradicional y de VPN de acceso remoto pueden entrar directamente en la red, ya que la normativa de seguridad confía suficientemente en los mecanismos de autenticación que permiten la primera conexión con la red.

SAFE permite al diseñador afrontar los requisitos de seguridad de cada función de red de forma casi independiente. Cada módulo suele disponer de todo lo que necesita y supone que los módulos interconectados se encuentran solamente en un nivel de seguridad básico, lo que permite a los diseñadores de redes utilizar un método por fases para asegurar la red de la empresa. Pueden afrontar la seguridad de la mayor parte de las funciones más importantes de la red tal como lo determina la normativa y sin tener que volver a diseñar toda la red. La excepción es el módulo de gestión. Durante la implementación inicial de SAFE, el módulo de gestión se debe implementar en paralelo con el primer módulo. A medida que se migra el resto de la red, el módulo de gestión puede conectarse con las restantes ubicaciones.

La primera versión de la arquitectura está pensada para afrontar la implementación de la seguridad de una red empresarial genérica. Los autores saben que hay muchas áreas que necesitan una mayor investigación, exploración y mejora. Entre estas áreas se incluyen las siguientes, aunque hay más:

- Análisis e implementación en profundidad de la gestión de la seguridad.
- Información de diseños especiales para redes pequeñas.
- Análisis e implementación en profundidad de identidades, de servicios de directorios, de tecnologías de AAA y de autoridades de certificación.
- Versiones a escala del extremo final de VPN y del diseño de WAN.

Anexo A: Laboratorio de validación

Existe una implementación de SAFE de referencia para validar las funciones descritas en este documento. En este anexo se detallan las configuraciones de los dispositivos específicos de cada módulo, así como las directrices globales para la configuración general de los dispositivos. A continuación encontrará instantáneas de la configuración de los dispositivos obtenidas en el laboratorio. Los autores de este informe no recomiendan la aplicación de estas configuraciones directamente a ninguna red de producción.

Pautas generales

La configuración que se presenta a continuación forma parte de los axiomas de SAFE, a los que ya se ha hecho mención en este documento.

Routers

Éstas son las opciones básicas de configuración presentes en casi todos los routers del laboratorio de SAFE:

```
! desactivación de los servicios no necesarios
!
no ip domain-lookup
no cdp run
no ip http server
no ip source-route
no service finger
no ip bootp server
no service udp-small-s
no service tcp-small-s
!
!activación del registro y de snmp
!
service timestamp log datetime localtime
logging 192.168.253.56
logging 192.168.253.51
snmp-server community Txo~QbW3XM ro 98
!
!establecimiento de contraseñas y de restricciones de acceso
!
service password-encryption
enable secret %Z<)|z9~zq
no enable password
no access-list 99
access-list 99 permit 192.168.253.0 0.0.0.255
access-list 99 deny any log
no access-list 98
access-list 98 permit host 192.168.253.51
access-list 98 deny any log
line vty 0 4
access-class 99 in
login
password 0 X)[^j+#T98
exec-timeout 2 0
line con 0
login
password 0 X)[^j+#T98
exec-timeout 2 0
line aux 0
transport input none
password 0 X)[^j+#T98
no exec
exit
banner motd #

                This is a private system operated for and by Cisco VSEC BU.
Authorization from Cisco VSEC management is required to use this system.
                Use by unauthorized persons is prohibited.

#
!
!Activación de NTP
!
clock timezone PST -8
clock summer-time PST recurring
```

```
ntp authenticate
ntp authentication-key 1 md5 -UN&/6[oh6
ntp trusted-key 1
ntp access-group peer 96
ntp server 192.168.254.57 key 1
access-l 96 permit host 192.168.254.57
access-l 96 deny any log
!
!Activación de AAA
!
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs line
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting network start-stop tacacs+
aaa accounting exec start-stop tacacs+
tacacs-server host 192.168.253.54 single
tacacs-server key SJj)j~t]6-
line con 0
login authentication no_tacacs
```

La siguiente instantánea de la configuración define los parámetros de la autenticación y de los filtros de OSPF de todos los routers OSPF de la red. Observe la autenticación MD5 y las listas de distribución que garantizan que la red OOB no está anunciada.

```
interface Vlan13
ip address 10.1.13.3 255.255.255.0
ip ospf authentication message-digest
        ip ospf message-digest-key 1 md5 7 024D105641521F0A7E
ip ospf priority 3
!
router ospf 1
        area 0 authentication message-digest
network 10.1.0.0 0.0.255.255 area 0
distribute-list 1 out
distribute-list 1 in
!
access-list 1 deny  192.168.0.0 0.0.255.255
access-list 1 permit any
```

La siguiente instantánea de la configuración define el control de acceso presente en todas las interfaces de OOB de la red.

No olvide que se suma a las VLAN privadas que bloquean el acceso entre direcciones IP de hosts gestionados.

```
interface FastEthernet1/0
ip address 192.168.254.15 255.255.255.0
ip access-group 101 in
ip access-group 102 out
no cdp enable
!
access-list 101 permit icmp any any
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.15 established
access-list 101 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.15 gt 1023
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.15 eq telnet
access-list 101 permit udp host 192.168.253.51 host 192.168.254.15 eq snmp
access-list 101 permit udp host 192.168.253.53 host 192.168.254.15 eq tftp
access-list 101 permit udp host 192.168.254.57 host 192.168.254.15 eq ntp
access-list 101 deny            ip any any log
access-list 102 deny            ip any any log
```

Switches

Ésta es la configuración básica de seguridad presente en casi todos los switches del sistema operativo CAT en el laboratorio de SAFE. Los switches IOS utilizan una configuración casi idéntica a la configuración de los routers.

```
!
!Activación de NTP
!
set timezone PST -8
set summertime PST
set summertime recurring
set ntp authentication enable
set ntp key 1 trusted md5 -UN&/6[oh6
set ntp server 192.168.254.57 key 1
set ntp client enable
!
! desactivación de los servicios no necesarios
!
set cdp disable
set ip http server disable
!
!activación del registro y de snmp
!
set logging server 192.168.253.56
set logging server 192.168.253.51
set logging timestamp enable
set snmp community read-only Txo~QbW3XM
set ip permit enable snmp
set ip permit 192.168.253.51 snmp
!
!Activación de AAA
!
set tacacs server 192.168.253.54 primary
set tacacs key SJj)j~t]6-
set authentication login tacacs enable telnet
set authentication login local disable telnet
set authorization exec enable tacacs+ deny telnet
set accounting exec enable start-stop tacacs+
set accounting connect enable start-stop tacacs+
!
!establecimiento de contraseñas y de restricciones de acceso
!
set banner motd <c>
      This is a private system operated for and by Cisco VSEC BU.
   Authorization from Cisco VSEC management is required to use this system.
         Use by unauthorized persons is prohibited.
<c>
!la contraseña de la consola la define 'set password'
!introduzca la contraseña antigu y después la nueva
!contraseña consola = X)[^j+#T98
!
!la contraseña de activación la define 'set enable'
!introduzca la contraseña antigu y después la nueva
!contraseña activación = %Z<)|z9~zq
!
!la siguiente configuración de contraseña sólo funciona la primera vez
!
```

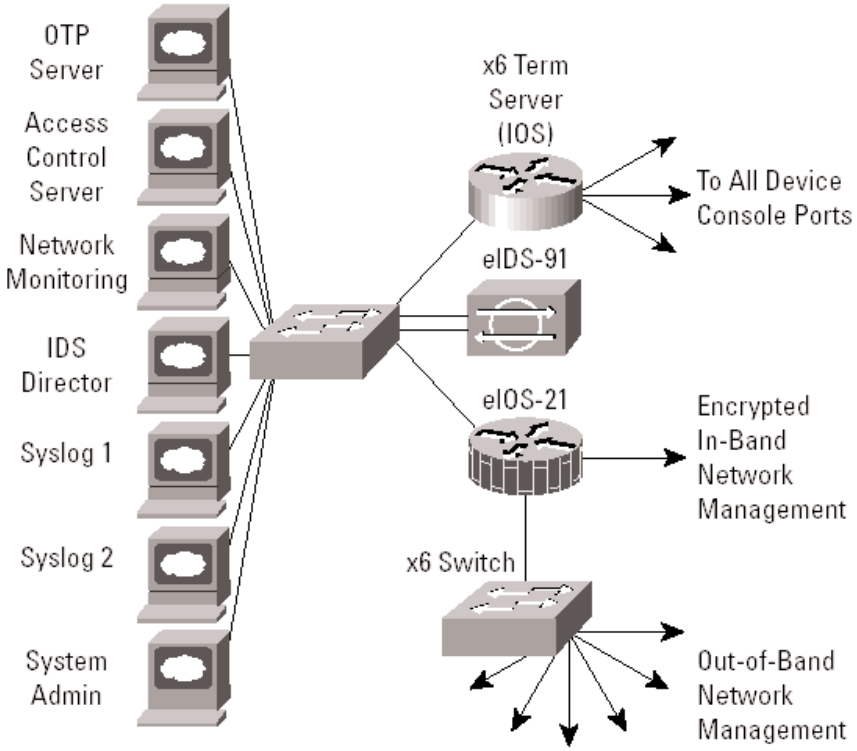
```
set password
X)[^j+#T98
X)[^j+#T98
set enable
cisco
%Z<)|z9~zq
%Z<)|z9~zq
!
!la anterior configuración de contraseña sólo funciona la primera vez
!
set logout 2
set ip permit enable telnet
set ip permit 192.168.253.0 255.255.255.0 telnet
```

Hosts

Se han incorporado los parches más recientes a los hosts. También se ha aplicado HIDS. La aplicación HIDS utilizada en el laboratorio es Entercept, de ClickNet. Puede encontrar más información en: http://www.clicknet.com

Módulo de gestión

Ilustración 29 Módulo de gestión: detalle



Productos utilizados

Switches de Capa 2 Cisco Catalyst 3500XL (toda la conmutación)

Router IOS Cisco 3640 con el conjunto de características de firewall (eIOS-21)

Router IOS Cisco 2511 (servidores terminales)

Sensor de Cisco Secure Intrusion Detection System (CSIDS)

Servidor OTP RSA SecureID

Servidor de control de acceso Cisco Secure

Cisco Works 2000

Cisco Secure Policy Manager

Herramienta de análisis de syslogs netForensics

HIDS ClickNet Entercept

EIOS-21

La configuración siguiente define los parámetros predeterminados del firewall IOS:

```
ip inspect audit-trail
ip inspect max-incomplete low 150
ip inspect max-incomplete high 250
ip inspect one-minute low 100
ip inspect one-minute high 200
ip inspect udp idle-time 20
ip inspect dns-timeout 3
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 3
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 40 block-time 0
ip inspect name mgmt_fw tcp timeout 300
ip inspect name mgmt_fw udp
ip inspect name mgmt_fw tftp
ip inspect name mgmt_fw http
ip inspect name mgmt_fw fragment maximum 256 timeout 1
ip audit notify log
ip audit po max-events 100
```

La configuración siguiente configura la gestión cifrada de redes en banda:

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key A%Xr)7,_) address 172.16.224.24
crypto isakmp key A%Xr)7,_) address 172.16.224.23
!
crypto ipsec transform-set vpn_module_mgmt esp-3des esp-sha-hmac
!
crypto map mgmt1 100 ipsec-isakmp
set peer 172.16.224.24
        set transform-set vpn_module_mgmt
        match address 111
crypto map mgmt1 200 ipsec-isakmp
set peer 172.16.224.23
        set transform-set vpn_module_mgmt
        match address 110
access-list 110 permit ip 192.168.253.0 0.0.0.255 host 172.16.224.23
access-list 110 permit udp 192.168.254.0 0.0.0.255 host 172.16.224.23
access-list 111 permit ip 192.168.253.0 0.0.0.255 host 172.16.224.24
access-list 111 permit udp 192.168.254.0 0.0.0.255 host 172.16.224.24
```

La configuración siguiente define el control de acceso de entrada desde la red de hosts gestionados. El puerto 45000 es para CSIDS y el puerto 5000 es para el HIDS de Click Net.

```
access-list 114 permit icmp 192.168.254.0 0.0.0.255 192.168.253.0 0.0.0.255 echo-reply
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.56 eq syslog
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.51 eq syslog
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.50 eq 45000
access-list 114 permit tcp 192.168.254.0 0.0.0.255 host 192.168.253.50 eq 5000
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.53 eq tftp
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.254.57 eq ntp
access-list 114 permit tcp 192.168.254.0 0.0.0.255 host 192.168.253.54 eq tacacs
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.54 eq 1645
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.52 eq syslog
access-list 114 deny              ip any any log
```

La configuración siguiente define el control de acceso de entrada desde la red de hosts de gestión:

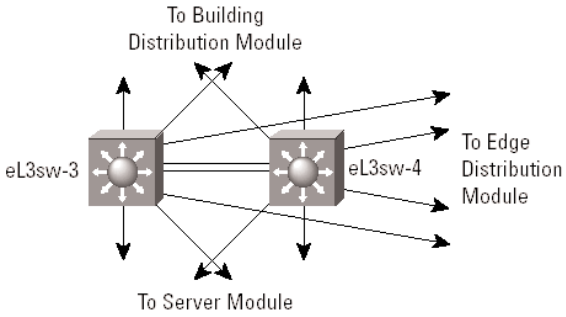
```
access-list 113 permit icmp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 192.168.253.57
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 192.168.253.57 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq 443
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq 22
access-list 113 permit udp host 192.168.253.50 192.168.254.0 0.0.0.255 eq 45000
access-list 113 permit tcp host 192.168.253.50 192.168.254.0 0.0.0.255 eq 5000
access-list 113 permit udp host 192.168.253.51 192.168.254.0 0.0.0.255 eq snmp
access-list 113 permit udp host 192.168.253.53 gt 1023 host 192.168.253.57 gt 1023
access-list 113 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.57 eq ntp
access-list 113 permit tcp host 192.168.253.54 eq tacacs host 192.168.253.57 gt 1023
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 172.16.224.23
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 172.16.224.24
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.24 eq telnet
access-list 113 permit udp host 192.168.253.51 host 172.16.224.23 eq snmp
access-list 113 permit udp host 192.168.253.51 host 172.16.224.24 eq snmp
access-list 113 deny              ip any any log
```

La configuración siguiente define el control de acceso de entrada desde la red de producción. Este acceso solo permite tráfico cifrado, ya que es la única comunicación que se permite que entre en el módulo de gestión de la red de producción. Las cuatro primeras líneas definen el acceso del tráfico cifrado. Tras descifrarlo, el tráfico debe volver a pasar por la lista de accesos para poder entrar en el módulo de gestión.

```
access-list 112 permit esp host 172.16.224.23 host 10.1.20.57
access-list 112 permit esp host 172.16.224.24 host 10.1.20.57
access-list 112 permit udp host 172.16.224.24 host 10.1.20.57 eq isakmp
access-list 112 permit udp host 172.16.224.23 host 10.1.20.57 eq isakmp
access-list 112 permit udp host 172.16.224.24 host 192.168.253.56 eq syslog
access-list 112 permit udp host 172.16.224.23 host 192.168.253.56 eq syslog
access-list 112 permit udp host 172.16.224.24 host 192.168.253.51 eq syslog
access-list 112 permit udp host 172.16.224.23 host 192.168.253.51 eq syslog
access-list 112 permit udp host 172.16.224.24 host 192.168.253.53 eq tftp
access-list 112 permit udp host 172.16.224.23 host 192.168.253.53 eq tftp
access-list 112 permit udp host 172.16.224.24 host 192.168.253.57 eq ntp
access-list 112 permit udp host 172.16.224.23 host 192.168.253.57 eq ntp
access-list 112 permit tcp host 172.16.224.24 host 192.168.253.54 eq tacacs
access-list 112 permit tcp host 172.16.224.23 host 192.168.253.54 eq tacacs
access-list 112 permit icmp host 172.16.224.24 192.168.253.0 0.0.0.255 echo-reply
access-list 112 permit icmp host 172.16.224.23 192.168.253.0 0.0.0.255 echo-reply
access-list 112 deny              ip any any log
```

Módulo central

Ilustración 30 Módulo central: detalle

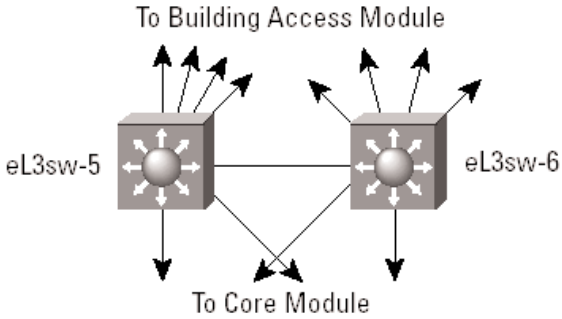


Productos utilizados

Switches de Capa 3 Cisco Catalyst 6500

Módulo de distribución del edificio

Ilustración 31 Módulo de distribución del edificio: detalle



Productos utilizados

Switches de Capa 3 Cisco Catalyst 6500

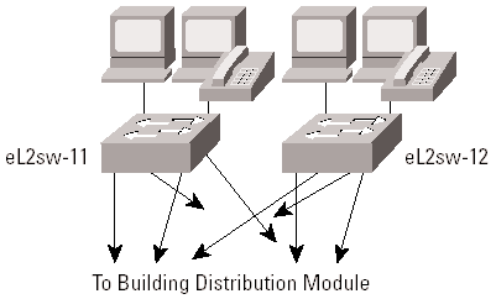
EL3SW-5

La siguiente instantánea de la configuración define el control de acceso de Capa 3 entre las subredes de este módulo. VLAN 5 define la subred de marketing, VLAN 6 define la subred de I+D, VLAN 7 define los teléfonos IP de marketing y VLAN 8 define los teléfonos IP de I+D.

```
interface Vlan5
        ip address 10.1.5.5 255.255.255.0
        ip access-group 105 in
!
interface Vlan6
        ip address 10.1.6.5 255.255.255.0
        ip access-group 106 in
!
interface Vlan7
        ip address 10.1.7.5 255.255.255.0
        ip access-group 107 in
!
interface Vlan8
        ip address 10.1.8.5 255.255.255.0
        ip access-group 108 in
!
access-list 105 deny  ip 10.1.5.0 0.0.0.255 10.1.6.0 0.0.0.255
access-list 105 deny  ip 10.1.5.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 105 deny  ip 10.1.5.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 105 deny  ip 10.1.5.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 105 permit ip 10.1.5.0 0.0.0.255 any
access-list 105 deny          ip any any log
access-list 106 deny  ip 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
access-list 106 deny  ip 10.1.6.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 106 deny  ip 10.1.6.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 106 deny  ip 10.1.6.0 0.0.0.255 10.1.15.0 0.0.0.255
access-list 106 deny  ip 10.1.6.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 106 permit ip 10.1.6.0 0.0.0.255 any
access-list 106 deny          ip any any log
access-list 107 permit ip 10.1.7.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 107 permit ip 10.1.7.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 107 permit ip 10.1.7.0 0.0.0.255 host 10.1.11.50
access-list 107 deny          ip any any log
access-list 108 permit ip 10.1.8.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 108 permit ip 10.1.8.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 108 permit ip 10.1.8.0 0.0.0.255 host 10.1.11.50
access-list 108 deny          ip any any log
```

Módulo de acceso al edificio

Ilustración 32 Módulo de acceso al edificio: detalle



Productos utilizados

Switches de Capa 2 Cisco Catalyst 4003

Telefono IP de Cisco

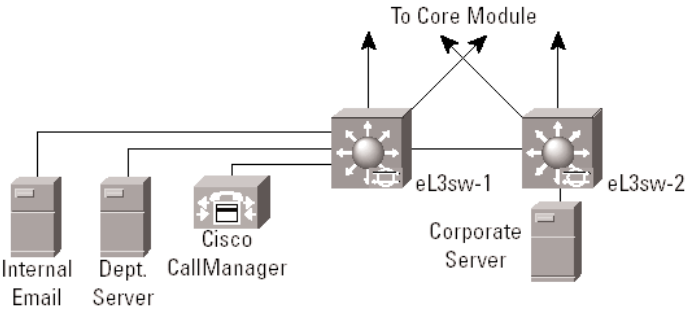
EL2SW-11 y 12

La siguiente instantánea de la configuración muestra algunos de los parámetros de VLAN de los switches de Capa 2 de este módulo. Observe que los puertos innecesarios se desactivan y se asignan a una VLAN no enrutable. Además, los enlaces troncales están desactivados en todos los puertos, excepto en los que conectan con teléfonos IP que utilizan enlaces troncales para la separación de la VLAN entre el teléfono y la estación de trabajo.

```
set vlan 5              2/5,2/17
set vlan 6              2/6,2/18
set vlan 99  2/34
set vlan 999 2/1-3,2/7-16,2/19-33
set port disable  2/7-33
set trunk 2/1-34 off
set trunk 2/4 on dot1q 1,5-8
```

Módulo de servidores

Ilustración 33 Módulo se servidores: detalle



Productos utilizados

Switches de Capa 3 Cisco Catalyst 6500

Blade de detección de intrusos Cisco Catalyst 6500

Cisco Call Manager

HIDS ClickNet Entercept

EL3SW-1 y 2

La configuración siguiente define las asignaciones de la VLAN privada para varios de los puertos de la misma VLAN. Este configuración impide que el servidor de correo electrónico interno se comunique con el servidor de la empresa.

```
! Config sistema operativo CAT
!
#private vlans
set pvlan 11 437
set pvlan 11 437 3/3-4,3/14
set pvlan mapping 11 437 15/1
!
! Config MSFC
!
interface Vlan11
        ip address 10.1.11.1 255.255.255.0
        ip access-group 111 in
no ip redirects
```

La configuración siguiente define los filtros de varias de las interfaces de este módulo. Incluye los filtros de RFC 2827.

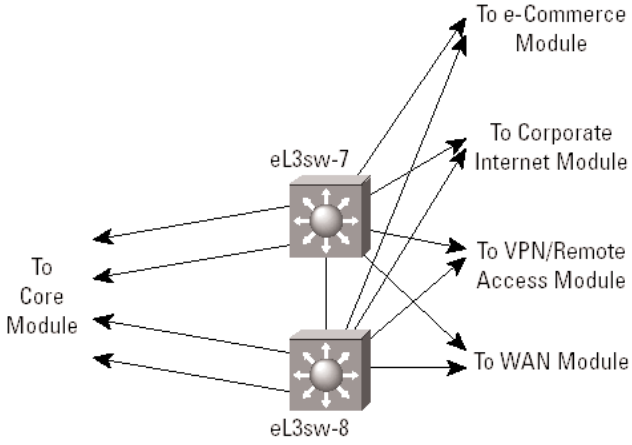
```
interface Vlan11
        ip address 10.1.11.1 255.255.255.0
        ip access-group 111 in
!
interface Vlan15
        ip address 10.1.15.1 255.255.255.0
        ip access-group 115 in
!
interface Vlan16
        ip address 10.1.16.1 255.255.255.0
        ip access-group 116 in
ip access-group 126 out
!
access-list 111 permit ip 10.1.11.0 0.0.0.255 any
access-list 111 deny        ip any any log
access-list 115 permit ip 10.1.15.0 0.0.0.255 any
access-list 115 deny        ip any any log
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.11.0 0.0.0.255
access-list 116 deny        ip any any log
access-list 126 permit ip 10.1.7.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 126 permit ip 10.1.8.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 126 permit ip 10.1.11.0 0.0.0.255 10.1.16.0 0.0.0.255
```

La configuración siguiente configura el puerto de capturas del módulo IDS de Cat 6000:

```
#module 4 : 2-port Intrusion Detection System
set module name  4
set module enable 4
set vlan 1          4/1
set vlan 99         4/2
set port name       4/1 Sniff-4
set port name       4/2 CandC-4
set trunk 4/1 nonegotiate dot1q 1-1005,1025-4094
set security acl capture-ports 4/1
```

Módulo de distribución de contorno

Ilustración 34 Módulo de distribución del contorno: detalle

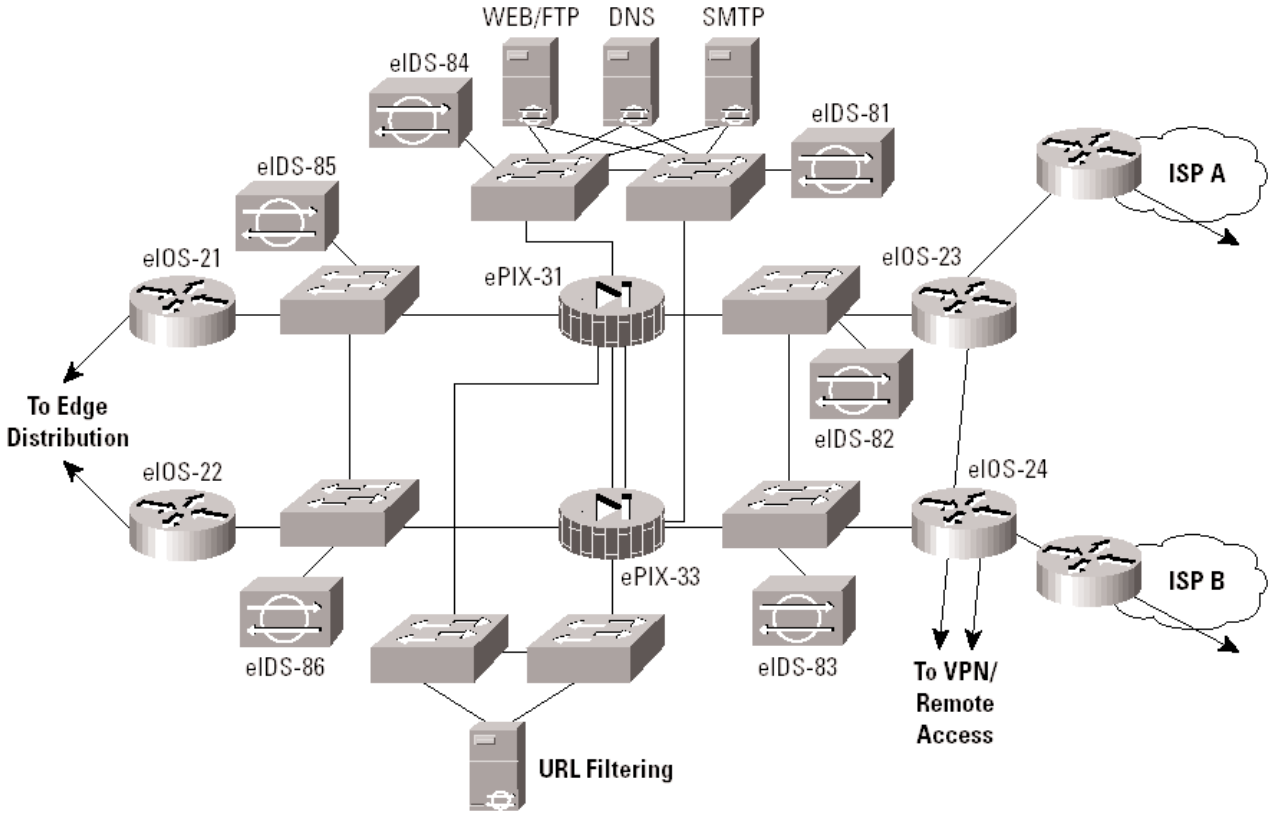


Productos utilizados

Switches de Capa 3 Cisco Catalyst 6500

Módulo de Internet de la empresa

Ilustración 35 Módulo de Internet de la empresa: detalle



Productos utilizados

Firewall PIX Cisco Secure

Sensor de CSIDS

Switches de Capa 2 Catalyst 3500

Router IOS Cisco 7100

HIDS ClickNet Entercept

Servidor de filtros de direcciones URL Websense

EPIX-31 y 33

La siguiente instantánea de la configuración detalla el control de acceso que se coloca en el firewall PIX. El nombre de la lista de acceso indica el lugar en que está colocado el ACL de entrada. "In" es entrante, "out" es saliente, "pss" es el segmento de servicios públicos (DMZ), "url" es el segmento de filtro de contenidos y "mgmt" es la interfaz de OOB.

```
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out permit icmp any any echo-reply
access-list out permit tcp any host 172.16.225.52 eq www
access-list out permit tcp any host 172.16.225.52 eq ftp
access-list out permit tcp any host 172.16.225.50 eq smtp
access-list out permit udp any host 172.16.225.51 eq domain
access-list out permit esp host 172.16.224.23 host 172.16.224.57
access-list out permit esp host 172.16.224.24 host 172.16.224.57
access-list out permit udp host 172.16.224.23 host 172.16.224.57 eq isakmp
access-list out permit udp host 172.16.224.24 host 172.16.224.57 eq isakmp
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in permit icmp any any echo
access-list in permit udp host 10.1.11.50 host 172.16.225.51 eq domain
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.1.103.50 eq 15871
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq smtp
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq 20389
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq ftp
access-list in deny ip any 172.16.225.0 255.255.255.0
access-list in permit ip 10.0.0.0 255.0.0.0 any
access-list in permit esp host 10.1.20.57 host 172.16.224.23
access-list in permit esp host 10.1.20.57 host 172.16.224.24
access-list in permit udp host 10.1.20.57 host 172.16.224.23 eq isakmp
access-list in permit udp host 10.1.20.57 host 172.16.224.24 eq isakmp
access-list pss deny ip any 192.168.254.0 255.255.255.0
access-list pss deny ip any 192.168.253.0 255.255.255.0
access-list pss permit tcp host 172.16.225.50 host 10.1.11.51 eq 20025
access-list pss permit tcp host 172.16.225.50 host 10.1.11.51 eq 20389
access-list pss deny ip 172.16.225.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list pss permit tcp host 172.16.225.50 any eq smtp
access-list pss permit udp host 172.16.225.51 any eq domain
access-list url permit udp host 10.1.103.50 host 172.16.225.51 eq domain
access-list url permit ip any any
access-list mgmt permit icmp 192.168.253.0 255.255.255.0 any
```

EIOS-23 y 24

Esta instantánea de la configuración detalla los comandos del protocolo Hot Standby Router Protocol (HSRP) en muchos routers que utilizan HSRP para aumentar la disponibilidad.

```
interface FastEthernet0/0
 ip address 172.16.226.23 255.255.255.0
 standby 2 timers 5 15
 standby 2 priority 110 preempt delay 2
 standby 2 authentication k&>9NG@6
 standby 2 ip 172.16.226.100
 standby 2 track ATM4/0 50
```

La configuración siguiente configura la conexión de la gestión de red cifrada en banda al módulo de gestión:

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key A%Xr)7,_) address 172.16.224.57
!
crypto ipsec transform-set vpn_module_mgmt esp-3des esp-sha-hmac
!
crypto map mgmt1 100 ipsec-isakmp
set peer 172.16.224.57
        set transform-set vpn_module_mgmt
match address 103
access-list 103 permit ip host 172.16.224.23 192.168.253.0 0.0.0.255
access-list 103 permit udp host 172.16.224.23 192.168.254.0 0.0.0.255
```

La siguiente ACL permanece en el interior desde la red de la empresa:

```
access-list 112 permit udp host 172.16.224.57 host 172.16.224.23 eq isakmp
access-list 112 permit esp host 172.16.224.57 host 172.16.224.23
access-list 112 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 established
access-list 112 permit udp 192.168.253.0 0.0.0.255 host 172.16.224.23 gt 1023
access-list 112 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 eq telnet
access-list 112 permit udp host 192.168.253.51 host 172.16.224.23 eq snmp
access-list 112 permit udp host 192.168.254.57 host 172.16.224.23 eq ntp
access-list 112 permit icmp any any
access-list 112 deny  ip any host 172.16.224.23 log
access-list 112 deny  ip any host 172.16.226.23 log
access-list 112 deny  ip any host 172.16.145.23 log
access-list 112 permit ip 172.16.224.0 0.0.0.255 any
access-list 112 permit ip 172.16.225.0 0.0.0.255 any
```

La siguiente ACL permanece en el interior desde el ISP: Observe que el filtro de RFC 1918 no está completo, ya que estas direcciones se emplean como direcciones de producción en el laboratorio. Las redes actuales deberían implementar todos los filtros de RFC 1918.

```
access-list 150 deny  ip 10.0.0.0 0.255.255.255 any
access-list 150 deny  ip 192.168.0.0 0.0.255.255 any
access-list 150 deny  ip 172.16.224.0 0.0.7.255 any
access-list 150 permit ip any 172.16.224.0 0.0.7.255
access-list 150 permit ip any 172.16.145.0 0.0.0.255
access-list 150 permit esp any 172.16.226.0 0.0.0.255 fragments
access-list 150 deny  ip any any fragments
access-list 150 deny  ip any any log
```

El siguiente filtro existe hacia fuera, al módulo de acceso remoto y de VPN. Observe que sólo se permiten IKE y ESP:

```
access-list 160 permit esp any host 172.16.226.27
access-list 160 permit esp any host 172.16.226.28
access-list 160 permit esp any host 172.16.226.48
access-list 160 permit udp any host 172.16.226.27 eq isakmp
access-list 160 permit udp any host 172.16.226.28 eq isakmp
access-list 160 permit udp any host 172.16.226.48 eq isakmp
access-list 160 deny  ip any any log
```

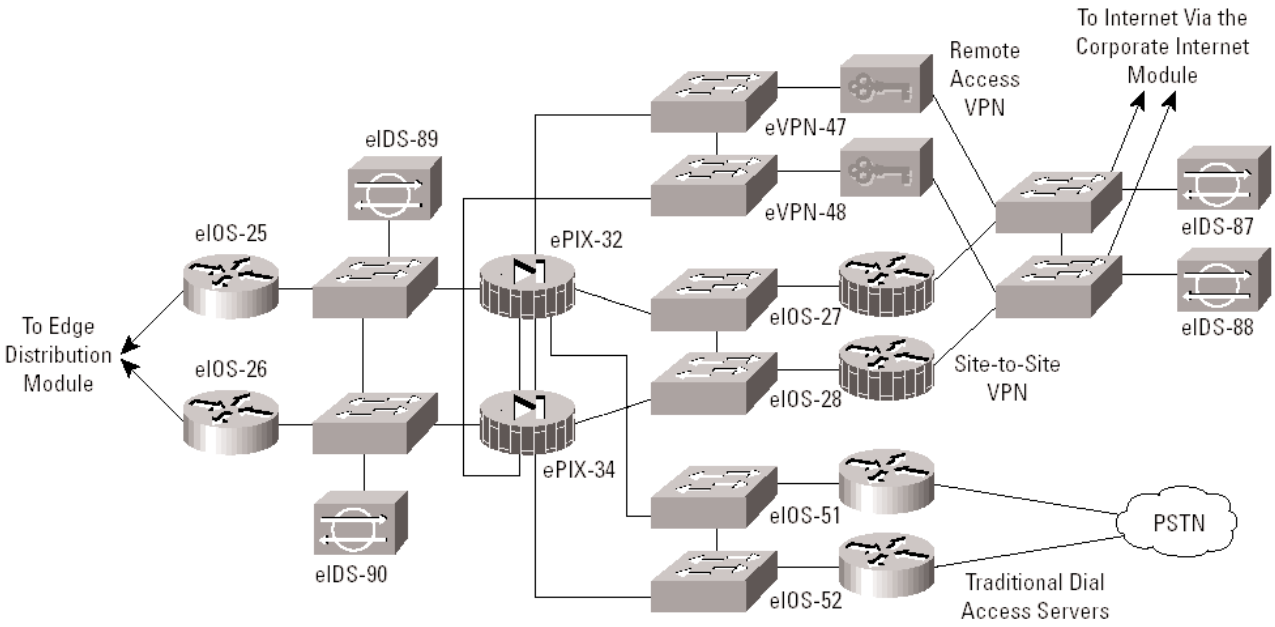
VLAN privadas Catalyst 3500XL

Esta instantánea de la configuración detalla la configuración de las VLAN privadas del segmento de servicios públicos:

```
interface FastEthernet0/1
        port protected
!
interface FastEthernet0/2
        port protected
```

Módulo de VPN y de acceso remoto

Ilustración 36 Módulo de VPN y de acceso remoto: detalle



Productos utilizados

Firewall PIX Cisco Secure

Sensor de CSIDS

Switches de Capa 2 Catalyst 3500

Router IOS Cisco 7100

Concentrador Cisco VPN 3060

Servidor de acceso de Cisco IOS

HIDS ClickNet Entercept

Servidor de filtros de direcciones URL Websense

EPIX-32 y 34

La siguiente instantánea de la configuración detalla el control de acceso que se coloca en el firewall PIX. El nombre de la lista de acceso indica el lugar en que está colocado el ACL de entrada. "In" es entrante, "out" es la VPN de ubicación a ubicación, "dun" es el acceso telefónico PSTN, "ra" es la VPN de acceso remoto y "mgmt" es la interfaz de OOB.

```
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in permit icmp any any
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq smtp
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq pop3
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq ftp
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq domain
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out permit icmp any any
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq smtp
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq pop3
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq www
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq ftp
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq domain
access-list out permit tcp 10.0.0.0 255.0.0.0 172.16.255.0 255.255.255.0 eq www
access-list out permit tcp 10.0.0.0 255.0.0.0 172.16.255.0 255.255.255.0 eq ftp
access-list ra deny ip any 192.168.253.0 255.255.255.0
access-list ra deny ip any 192.168.254.0 255.255.255.0
access-list ra permit icmp any any
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq smtp
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq pop3
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq www
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq ftp
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq domain
access-list ra deny ip 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0
access-list ra permit tcp 10.1.198.0 255.255.254.0 172.16.225.0 255.255.255.0 eq www
access-list ra permit tcp 10.1.198.0 255.255.254.0 172.16.225.0 255.255.255.0 eq ftp
access-list ra deny ip 10.1.198.0 255.255.254.0 172.16.224.0 255.255.248.0
access-list ra permit ip 10.1.198.0 255.255.254.0 any
access-list dun deny ip any 192.168.253.0 255.255.255.0
access-list dun deny ip any 192.168.254.0 255.255.255.0
access-list dun permit icmp any any
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq smtp
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq pop3
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq www
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq ftp
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq domain
access-list dun deny ip 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0
access-list dun permit tcp 10.1.196.0 255.255.255.0 172.16.225.0 255.255.255.0 eq www
access-list dun permit tcp 10.1.196.0 255.255.255.0 172.16.225.0 255.255.255.0 eq ftp
access-list dun deny ip 10.1.196.0 255.255.254.0 172.16.224.0 255.255.248.0
access-list dun permit ip 10.1.196.0 255.255.254.0 any
access-list mgmt permit icmp 192.168.253.0 255.255.255.0 any
```

Esta instantánea de la configuración detalla las conversiones NAT estáticas necesarias para que el tráfico de VPN salga del módulo de Internet de la empresa a Internet:

```
static (inside,ravpn) 128.0.0.0 128.0.0.0 netmask 128.0.0.0 0 0
static (inside,ravpn) 64.0.0.0 64.0.0.0 netmask 192.0.0.0 0 0
static (inside,ravpn) 32.0.0.0 32.0.0.0 netmask 224.0.0.0 0 0
static (inside,ravpn) 16.0.0.0 16.0.0.0 netmask 240.0.0.0 0 0
static (inside,ravpn) 8.0.0.0 8.0.0.0 netmask 248.0.0.0 0 0
static (inside,ravpn) 4.0.0.0 4.0.0.0 netmask 252.0.0.0 0 0
static (inside,ravpn) 2.0.0.0 2.0.0.0 netmask 254.0.0.0 0 0
static (inside,ravpn) 1.0.0.0 1.0.0.0 netmask 255.0.0.0 0 0
```

EIOS-27 y 28

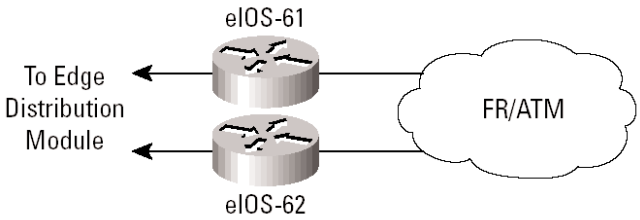
Esta instantánea de la configuración detalla la configuración de la criptografía para la VPN de ubicación a ubicación:

```
!
! Información básica criptografía
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.132.2
crypto isakmp key 52TH^m&^qu address 172.16.131.2
!
!
crypto ipsec transform-set smbranch esp-3des esp-sha-hmac
mode transport
!
crypto map secure1 100 ipsec-isakmp
set peer 172.16.132.2
set transform-set smbranch
match address 105
crypto map secure1 300 ipsec-isakmp
set peer 172.16.131.2
set transform-set smbranch
match address 107
!
!
! Información túnel GRE
!
interface Tunnel0
 ip address 10.1.249.27 255.255.255.0
 tunnel source 172.16.226.27
 tunnel destination 172.16.132.2
 crypto map secure1
!
interface Tunnel1
 ip address 10.1.247.27 255.255.255.0
 tunnel source 172.16.226.27
 tunnel destination 172.16.131.2
 crypto map secure1
!
!
! Enrutamiento EIGRP para mantener las conexiones activas
!
router eigrp 1
redistribute static
 passive-interface FastEthernet0/1
 passive-interface FastEthernet4/0
 network 10.0.0.0
```

```
 distribute-list 2 out
 distribute-list 2 in
!
! Crypto ACLs
!
access-list 105 permit gre host 172.16.226.27 host 172.16.132.2
access-list 107 permit gre host 172.16.226.27 host 172.16.131.2
!
! Inbound ACLs from Internet
!
access-list 110 permit udp 172.16.0.0 0.0.255.255 host 172.16.226.27 eq isakmp
access-list 110 permit esp 172.16.0.0 0.0.255.255 host 172.16.226.27
access-list 110 permit gre 172.16.0.0 0.0.255.255 host 172.16.226.27 access-list 110 deny  ip any any log
```

Módulo de WAN

Ilustración 37 Módulo de WAN: detalle



Productos utilizados

Router IOS Cisco 3640

EIOS-61

La configuración siguiente detalla el control de acceso de los routers del módulo de la WAN.

```
!
! Entrante desde la WAN
!
access-list 110 deny            ip any 192.168.253.0 0.0.0.255 log
access-list 110 deny            ip any 192.168.254.0 0.0.0.255 log
access-list 110 permit ospf any any
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.4.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 172.16.224.0 0.0.7.255
access-list 110 deny            ip any any log
!
! Entrante desde las oficinas centrales
!
access-list 111 deny            ip any 192.168.253.0 0.0.0.255 log
access-list 111 deny            ip any 192.168.254.0 0.0.0.255 log
access-list 111 permit ospf any any
access-list 111 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 10.3.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 10.4.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 172.16.224.0 0.0.7.255 10.2.0.0 0.0.255.255
access-list 111 deny            ip any any log
```

Anexo B: Manual de seguridad de redes

La necesidad de seguridad en la red

Internet está cambiando nuestra forma de trabajar, vivir, jugar y aprender. Estos cambios se producen tanto en las formas que utilizamos actualmente (comercio electrónico, acceso a la información en tiempo real, aprendizaje electrónico, más opciones de comunicación, etc.) y en las que aún tenemos que empezar a utilizar. Imagine el día en que las empresas puedan realizar todas sus llamadas telefónicas a través de Internet de forma gratuita. O quizá, de forma más personal, piense en la posibilidad de conectarse al sitio Web de una guardería para ver qué hacen sus hijos a lo largo del día. Como sociedad, no estamos más que empezando a desplegar el potencial de Internet. Pero con el crecimiento sin parangón de Internet llega una exposición sin precedentes de los datos personales, de los recursos más importantes de las empresas, de los secretos gubernamentales, etc. Todos los días, los hackers plantean cada vez más amenazas a estas entidades con distintos tipos de ataques. Estos ataques, que se explican en la siguiente sección, son cada vez más prolíficos y fáciles de implementar. Hay dos razones principales para ello.

En primer lugar, la ubicuidad de Internet. Con los millones de dispositivos que están actualmente conectados a Internet y más millones que están a punto de hacerlo, el acceso de los hackers a dispositivos vulnerables seguirá creciendo. La ubicuidad de Internet también ha permitido a los hackers compartir conocimientos a escala global. Una simple búsqueda en Internet de las palabras "hack", "crack" o "phreak" da como resultado miles de sitios, muchos de los cuales contienen código malicioso o los medios con los que utilizar dicho código.

En segundo lugar se encuentra la penetrabilidad de sistemas operativos fáciles de utilizar y los entornos de desarrollo. Este factor ha reducido la ingenuidad y los conocimientos globales que necesitan los hackers. Un buen hacker puede desarrollar aplicaciones fáciles de utilizar que pueden distribuirse a las masas. Varias herramientas de hackers que son de dominio público sólo requieren una dirección IP o un nombre de host y un clic de ratón para ejecutar un ataque.

Taxonomía de los ataques a redes

Los ataques a redes pueden ser tan variados como los sistemas en los que intentan penetrar. Algunos ataques son elaboradamente complejos, mientras que otros los pueden llevar a cabo, sin saberlo, los que manejan los dispositivos. Al evaluar los tipos de ataques es importante conocer algunas de las limitaciones inherentes al protocolo TCP/IP. Cuando se formó Internet, conectó varias entidades gubernamentales y universidades entre sí con el propósito de facilitar el aprendizaje y la investigación. Los arquitectos originales de Internet nunca llegaron a prever el tipo de adopción generalizada que Internet ha logrado en la actualidad. Como resultado, en los primeros días del Protocolo de Internet (IP), la seguridad no se diseñaba siguiendo ninguna especificación. Por este motivo, la mayor parte de las implementaciones de IP son inherentemente inseguras. Sólo después de muchos años y miles de RFC (Requests for Comments), por fin tenemos las herramientas para empezar a instalar IP de forma segura. Dado que las provisiones específicas para la seguridad de IP no se diseñaron desde el principio, es importante aumentar las implementaciones de IP con prácticas, servicios y productos de seguridad de red para combatir los riesgos inherentes del Protocolo de Internet. A continuación encontrará una breve explicación de los tipos de ataques que normalmente se ven en las redes IP y de cómo se pueden combatir dichos ataques.

Rastreadores de paquetes (Packet Sniffers)

Un rastreador de paquetes es una aplicación de software que utiliza una tarjeta adaptadora de red en modo promiscuo (un modo en el que la tarjeta adaptadora de red envía todos los paquetes recibidos en la red física a una aplicación para que los procese) para capturar todos los paquetes de red que se envían a través de un dominio de colisiones determinado. Los rastreadores se utilizan legítimamente en la redes actuales para facilitar la solución de problemas y el análisis del tráfico. Sin embargo, dado que varias aplicaciones de red envían datos en texto sin formato (telnet, FTP, SMTP, POP3, etc.), los rastreadores de paquetes pueden proporcionar información con sentido y, a veces, sensible, como nombres de usuario y contraseñas.

Un problema serio al adquirir los nombres de usuario y las contraseñas es que los usuarios a menudo reutilizan sus nombres de acceso y su contraseñas en varias aplicaciones y sistemas. De hecho, muchos usuarios emplean una sola contraseña para acceder a todas las cuentas y aplicaciones. Si una aplicación se ejecuta en modo cliente-servidor y la información de autenticación se envía a través de la red en texto sin formato, es probable que esta misma información de autenticación se pueda utilizar para obtener acceso a otros recursos de la empresa o externos. Dado que los hackers

conocen y usan características humanas (métodos de ataque conocidos colectivamente como ataques de ingeniería social), como utilizar una sola contraseña para varias cuentas, suelen conseguir acceder a la información sensible. En el peor de los casos, los hackers obtienen acceso a las cuentas de usuario a nivel de sistema, que utilizan para crear una cuenta nueva que puede utilizarse en cualquier momento como puerta trasera para entrar en una red y en sus recursos.

La amenaza de los rastreadores de paquetes se puede combatir de varias formas:

- *Autenticación:* el uso de una autenticación fuerte es la primera opción para defenderse contra los rastreadores de paquetes. La autenticación fuerte se puede definir en líneas generales como un método de autenticación de usuarios que no es fácil de esquivar. Un ejemplo común de autenticación fuerte son las contraseñas únicas (OTP). Una OTP es un tipo de autenticación de dos factores. La autenticación de dos factores implica el uso de algo que se tiene en combinación con algo que se conoce. Los cajeros automáticos utilizan la autenticación de dos factores. Los clientes necesitan una tarjeta y un número de identificación personal (PIN) para realizar transacciones. Con OTP se necesita un PIN y una tarjeta token para autenticarse en un dispositivo o en una aplicación. Una tarjeta token es un dispositivo de hardware o de software que genera contraseñas nuevas, aparentemente aleatorias, a intervalos especificados (normalmente 60 segundos). Los usuarios combinan dicha contraseña aleatoria con un PIN para crear una contraseña única que solo funciona para una instancia de autenticación. Aunque un hacker descubra dicha contraseña con un rastreador de paquetes, la información es inútil, ya que la contraseña ya ha expirado. Tenga en cuenta que esta técnica de defensa sólo es eficaz contra una implementación de rastreador diseñada para capturar contraseñas. Los rastreadores instalados para obtener información importante (como los mensajes de correo electrónico) seguirán siendo ineficaces.
- *Infraestructura conmutada:* otro método para contrarrestar el uso de rastreadores de paquetes en su entorno es instalar una infraestructura conmutada. Por ejemplo si toda una organización instala Ethernet conmutado, los hackers sólo pueden obtener acceso al tráfico que fluye en el puerto específico al que se conectan. Obviamente, las infraestructuras conmutadas no eliminan la amenaza de los rastreadores de paquetes, pero reducen considerablemente su eficacia.
- *Herramientas anti-rastreadores:* un tercer método que se utiliza contra los rastreadores es emplear software y hardware diseñado para detectar el uso de rastreadores en una red. Dicho software y hardware no eliminan totalmente la amenaza, pero como muchas otras herramientas de seguridad de la red, forman parte del sistema global. Estos "anti-rastreadores" detectan los cambios en el tiempo de respuesta de los hosts y determinan si los hosts están procesando tráfico que no es el suyo. Una de estas herramientas de seguridad de la red por software, que se puede obtener de LOpht Heavy Industries, se llama AntiSniff™. Para obtener más información, consulte la dirección URL http:// www.l0pht.com/antisniff/.
- *Criptografía:* el método más eficaz para contrarrestar los rastreadores de paquetes ni los evita ni los detecta, sino que hace que carezcan de importancia. Si un canal de comunicación es criptográficamente seguro, los únicos datos que detectarán los rastreadores de paquetes es texto cifrado (una cadena de bits aparentemente aleatorios) y no el mensaje original. La instalación de Cisco de criptografía a nivel de red se basa en IP Security (IPSec). IPSec es un método estándar para que los dispositivos de red se comuniquen de forma privada utilizando IP. Otros protocolos criptográficos para la gestión de redes son: Secure Shell (SSH) y Secure Sockets Layer (SSL).

Falsificación (spoofing) de IP

Un ataque de falsificación de IP se produce cuando un hacker de dentro o fuera de una red finge ser una computadora de confianza. Esto se puede lograr de uno de los dos modos siguientes. El hacker emplea una dirección IP que está dentro del rango de direcciones IP de confianza de una red o una dirección IP externa autorizada en la que se confíe y a la que se permite acceder a determinados recursos de la red. Los ataques de falsificación de IP suelen ser un punto de partida para otros ataques. El ejemplo clásico es lanzar un ataque de DoS utilizando direcciones de origen falsificadas para ocultar la identidad del hacker.

Normalmente, un ataque de falsificación de IP se limita a la inyección de datos o comandos dañinos a un flujo de datos existente que se pasan entre una aplicación cliente y una servidora o una conexión de red entre pares. Para activar la comunicación bidireccional, el hacker debe cambiar todas las tablas de enrutamiento para que apunten a la dirección IP falsificada. Otro enfoque que a veces adoptan los hackers es simplemente no preocuparse de recibir respuestas de las aplicaciones. Si un hacker intenta obtener un archivo importante de un sistema, las respuestas de las aplicaciones carecen de importancia.

Sin embargo, si un hacker logra cambiar las tablas de enrutamiento para que apunten a la dirección IP falsificada, dicho hacker puede recibir todos los paquetes de la red que vayan dirigidos a la dirección falsificada y responder como lo haría un usuario de confianza.

La amenaza de la falsificación de IP puede reducirse, pero no eliminarse, con las siguientes medidas.

Control de acceso: el método más común para evitar la falsificación de IP es configurar correctamente el control de acceso. Para reducir la eficacia de la falsificación de IP, configure el control de acceso para rechazar todo el tráfico de la red externa que tenga una dirección de origen que debería estar en la red interna. Tenga en cuenta que esto sólo evita los ataques de falsificación si las direcciones internas son las únicas direcciones en las que se confía. Si se confía en algunas direcciones externas, este método no es eficaz.

Filtros de RFC 2827: otra forma de evitar que los usuarios de una red ataquen mediante falsificaciones a otras redes (y al mismo tiempo ser un buen ciudadano de la red) es evitando todo el tráfico saliente de la red que no tenga una dirección de origen en el propio rango de IP de la organización. Su ISP también puede este tipo de filtros, que en conjunto se denominan filtros de RFC 2827. Estos filtros rechazan todo el tráfico que no tenga la dirección de origen que se esperaba en una interfaz determinada. Por ejemplo, si un ISP proporciona una conexión a la dirección IP 15.1.1.0/24, el ISP puede filtrar el tráfico, de forma que solamente aquel cuya dirección de origen sea 15.1.1.0/24 pueda entrar en el router del ISP desde dicha interfaz. Tenga en cuenta que, a menos que todos los ISP implementen este tipo de filtros, su eficacia se reduce considerablemente. Además, cuanto más se consigue de los dispositivos que se desean filtrar, más difícil es realizar el filtro a nivel granular. Por ejemplo, el uso de los filtros de RFC 2827 en el router de acceso a Internet requiere que permita que todo el número de su red principal (es decir, 10.0.0.0/8) atraviese el router de acceso. Si los filtros se utilizan en la capa de distribución, como en esta arquitectura, se puede lograr un filtro más específico (es decir, 10.1.5.0/24).

El método más eficaz para combatir la amenaza de falsificación de IP es el mismo que el que se utiliza para los rastreadores de paquetes: a saber, eliminar su eficacia. La falsificación de IP sólo puede funcionar correctamente cuando los dispositivos utilizan autenticación basada en direcciones IP. Por tanto, si utiliza otros métodos de autenticación, los ataques de falsificación de IP carecen de importancia. La autenticación criptográfica es la mejor forma de autenticación adicional, pero cuando no es posible, también puede ser muy eficaz la autenticación fuerte de dos factores con OTP.

Denegación de servicio

Los ataques de denegación de servicio (DoS) son, sin duda alguna, la forma de ataque más difundida y también están entre los más difíciles de eliminar totalmente. Incluso entre la comunidad de hackers, los ataques de DoS se consideran triviales y no tienen mucho prestigio porque se ejecutan con poco esfuerzo. Aun así, dado lo fácil que es implementarlos y el daño potencialmente importante que realizan, los ataques de DoS merecen una atención especial por parte de los administradores de seguridad. Si desea más información sobre estos ataques, puede resultarle muy útil investigar los métodos que emplean algunos de los ataques más conocidos. Entre estos ataques se incluyen los siguientes:

- Desbordamiento SYN de TCP
- Ping of Death
- Tribe Flood Network (TFN) y Tribe Flood Network 2000 (TFN2K)
- Trinco
- Stacheldraht
- Trinity

Otra fuente excelente sobre el tema de la seguridad es el Computer Emergency Response Team (CERT). Han publicado un excelente informe relacionado con los ataques de DoS, que puede encontrarse en la siguiente dirección URL: http://www.cert.org/tech_tips/ denial_of_service.html

Los ataques de DoS son distintos de la mayoría de los restantes ataques porque, por lo general, no ven encaminados a obtener acceso a una red o la información de una red. Estos ataques se centran en inutilizar un servicio para el uso normal, lo que suele llevarse a cabo agotando algunos límites de recursos de la red o de un sistema operativo o aplicación.

Cuando implican a aplicaciones servidoras de red específicas, como un servidor Web o un servidor FTP, estos ataques pueden centrarse en capturar y mantener abiertas todas las conexiones disponibles que admite dicho servidor, con lo que bloquea eficazmente a los usuarios válidos del servidor o del servicio. Los ataques de DoS también se pueden implementar utilizando protocolos de Internet comunes, como TCP e Internet Control Message Protocol (ICMP). La mayor parte de los ataques de DoS explotan una debilidad de la arquitectura global del sistema que se ataca, en lugar de algún error del software o un agujero en la seguridad. Sin embargo, algunos ataques ponen en peligro el rendimiento de la red inundándola con paquetes de red no deseados y, a menudo, inútiles y ofreciendo información falsa sobre el estado de los recursos de la red. Este tipo de ataque suele ser el más difícil de impedir, ya que para ello hay que estar coordinado con el proveedor de red de flujo ascendente. Si el tráfico dirigido a consumir el ancho de banda disponible no se detiene ahí, rechazarlo en el punto de entrada a la red no servirá de mucho porque el ancho de banda disponible ya se ha consumido. Cuando este tipo de ataque se lanza desde muchos sistemas diferentes al mismo tiempo suele denominarse ataque de denegación de servicio distribuido (DDoS).

La amenaza de este tipo de ataques se puede reducir a través de estos tres métodos:

- *Características anti-falsificación:* la configuración correcta de las características anti-falsificación de los routers y firewalls puede reducir el riesgo. Aquí se incluyen, como mínimo, los filtros de RFC 2827. Si los hackers no pueden enmascarar sus identidades, no pueden atacar.
- *Características anti-DoS:* la configuración correcta de las características anti-DoS de los routers y firewalls puede ayudar a limitar la eficacia de un ataque. Estas características a menudo implican poner límites en la cantidad de conexiones medio abiertas que permite abrir un sistema en un momento dado.
- *Limitación de la velocidad del tráfico:* una organización puede implementar la limitación de la velocidad del tráfico con su ISP. Este tipo de filtro limita la cantidad de tráfico no esencial que atraviesa los segmentos de la red a una velocidad determinada. Un ejemplo común es limitar la cantidad de tráfico ICMP que se permite entrar en la red, ya que sólo se emplea para realizar diagnósticos. Los ataques de (D)DoS basados en ICMP son frecuentes.

Ataques a contraseñas

Los hackers pueden implementar ataques a contraseñas utilizando varios métodos distintos, entre los que se incluyen ataques por fuerza bruta, troyanos, falsificación de IP y rastreadores de paquetes. Aunque con los dos últimos se pueden obtener cuentas de usuarios y contraseñas, los ataques a contraseñas suelen referirse a intentos repetidos para identificar cuentas de usuario y/o contraseñas. Estos repetidos intentos reciben el nombre de ataques por fuerza bruta.

A menudo, los ataques por fuerza bruta se realizan utilizando un programa que funciona a través de la red e intenta conectarse a un recurso compartido, como un servidor. Cuando los hackers consiguen obtener acceso a los recursos, tienen los mismos derechos que los usuarios cuyas cuentas han estado en peligro para obtener acceso a dichos recursos. Si las cuentas en peligro tienen suficientes privilegios, los hackers pueden crear puertas traseras para poder acceder más adelante sin preocuparse de los cambios de estado o de contraseña en las cuentas de usuario en peligro.

Existe otros problema por el que los usuarios tienen la misma contraseña en todos los sistemas a los que se conectan. A menudo, aquí se incluyen los sistemas personales, los sistemas de empresa y los sistemas de Internet. Dado que dicha contraseña es solo tan segura como el host administrado con más debilidad que la contiene, si dicho host está en peligro, los hackers tiene una amplia gama de hosts en los que pueden probar la misma contraseña.

Para eliminar los ataques a contraseñas fácilmente, lo primero es no utilizar contraseñas de texto sin formato. El uso de OTP y/o de autenticación criptográfica puede eliminar virtualmente la amenaza de ataques a contraseñas. Lamentablemente, no todas las aplicaciones, hosts y dispositivos admiten estos métodos de autenticación. Cuando se emplean contraseñas estándar, es importante elegir una que sea difícil de averiguar. Las contraseñas deben tener un mínimo de ocho caracteres y contener mayúsculas, minúsculas, números y caracteres especiales (#%$, etc.). Las mejores contraseñas se generan aleatoriamente, pero son muy difíciles de recordar, lo que a menudo conduce a los usuarios a apuntar sus contraseñas.

Se han realizado varios avances en relación al mantenimiento de las contraseñas (tanto para el usuario como para el administrador). Ya hay aplicaciones de software que cifran las listas de contraseñas que se almacenan en equipos portátiles. De esta forma, el usuario sólo tiene que recordar una contraseña compleja y, a cambio, tiene las restantes contraseñas almacenadas con total seguridad en la aplicación. Desde el punto de vista del administrador, existen varios métodos para realizar ataques por fuerza bruta a las contraseñas de sus propios usuarios. En uno estos métodos se utiliza una herramienta que emplea la comunidad de hackers llamada L0phtCrack. L0phtCrack realiza ataques por fuerza bruta a las contraseñas de Windows NT y puede señalar si un usuario ha elegido una contraseña muy fácil de averiguar. Para obtener más información, consulte la siguiente dirección URL: http://www.l0pht.com/l0phtcrack/

Ataques del tipo Man in the Middle

Los ataques del tipo Man in the Middle requieren que el hacker tenga acceso a los paquetes que atraviesan la red. Un ejemplo de dicha configuración podría ser alguien que trabaje para un ISP y que tenga acceso a todos los paquetes de red transferidos entre la red de su empresa y cualquier otra red. Dichos ataques se suelen implementar con rastreadores de paquetes de red y con protocolos de enrutamiento y transporte. Los posibles usos de dichos ataques son: el robo de la información, la apropiación de una sesión en curso para obtener acceso a los recursos privados de la red, el análisis del tráfico para derivar la información de una red y de sus usuarios, la denegación de servicio, el daño a los datos transmitidos y la introducción de información nueva en las sesiones de la red.

Los ataques del tipo Man in the Middle sólo se pueden combatir eficazmente mediante el uso de la criptografía. Si alguien se apropia de los datos del centro de una sesión privada criptográfica, lo único que verá el hacker es texto cifrado, no el mensaje original. Tenga en cuenta que si un hacker puede obtener información sobre la sesión criptográfica (como la clase de la sesión) puede realizar este tipo de ataques.

Ataques a la capa de aplicaciones

Los ataques a la capa de aplicaciones se pueden implementar utilizando varios métodos distintos. Uno de los métodos más comunes es explotar debilidades conocidas del software que suele encontrarse en los servidores, como sendmail, HTTP y FTP. Mediante la explotación de estas debilidades, los hackers pueden obtener acceso a una computadora con los permisos de la cuenta que ejecuta la aplicación, que suele ser una cuenta privilegiada del nivel del sistema. Estos ataques a la capa de aplicaciones suelen divulgarse profusamente en un esfuerzo por permitir al administrador solucionar el problema con un parche. Lamentablemente, también hay muchos hackers que se suscriben a estas mismas listas de correo, con lo que obtienen la información al mismo tiempo que los administradores (si no la han descubierto antes).

El principal problema de los ataques a la capa de aplicaciones es que suelen utilizar puertos que pueden pasar por un firewall. Por ejemplo, si un hacker ejecuta una vulnerabilidad conocida contra un servidor de Web, suele emplear el puerto 80 de TCP para efectuar el ataque. Teniendo en cuenta que el servidor de Web sirve páginas a los usuarios, algún firewall tiene que permitir el acceso a dicho puerto. Desde la perspectiva del firewall, no es más que tráfico estándar del puerto 80.

Los ataques a la capa de aplicaciones nunca se pueden eliminar por completo. Constantemente se están descubriendo y divulgando vulnerabilidades nuevas en la comunidad de Internet. La mejor forma de reducir el riesgo es realizar una buena administración del sistema. Éstas son algunas medidas que pueden adoptarse para reducir los riegos:

- Lea los archivos de registro del sistema operativo y de la red, o analícelos con aplicaciones de análisis de archivos de registro.
- Suscríbase a las listas de correo que divulgan las vulnerabilidades, como Bugtraq (http://www.securityfocus.com) y CERT (http://www.cert.org).
- Mantenga el sistema operativo y las aplicaciones actualizadas con los últimos parches.
- Además de una correcta administración del sistema, el uso de sistemas de detección de intrusiones (IDS) puede resultar de gran ayuda. Hay dos tecnologías de IDS complementarias:
- IDS basado en red (NIDS) funciona vigilando todos los paquetes que atraviesan un dominio específico de colisiones. Cuando NIDS ve un paquete o serie de paquetes que coinciden con un ataque conocido o sospechoso, puede marcar una alarma y/o terminar la sesión.
- IDS basado en host (HIDS) funciona insertando agentes en el host que se va a proteger. A partir de ese momento, sólo se preocupa de los ataques que se generan contra ese host.
- Los sistemas IDS funcionan con firmas de ataques. Estas firmas son el perfil de un ataque específico o de un tipo de ataque. Especifican determinadas condiciones que debe cumplir el tráfico para que se le considere un ataque. IDS tiene muchas semejanzas con un sistema de alarmas o con las cámaras de seguridad del mundo físico. La mayor limitación del sistema IDS es la cantidad de alarmas con falsos positivos que genera un sistema determinado. Para que IDS funcione correctamente en una red, es fundamental ajustarlo para evitar dichas alarmas falsas.

Reconocimiento de la red

Reconocimiento de la red hace referencia al acto de obtener información de una red objetivo empleando información y aplicaciones disponibles públicamente. Cuando los hackers intentan penetrar en una red determinada, a menudo necesitan obtener tanta información como sea posible sobre ella antes de lanzar los ataques. Esto se puede lograr en forma de consultas de DNS, barridos de pings y rastreos de puertos. Las consultas de DNS pueden revelar información como quién posee un dominio específico y qué direcciones se han asignado a dicho dominio. Los barridos de pings de las direcciones revelados por las consultas de DNS pueden presentar una imagen de los hosts vivos en un entorno determinado. Tras la generación de dicha lista, las herramientas de rastreo de puertos pueden recorrer los puertos conocidos para proporcionar una lista completa de todos los servicios que se ejecutan en los puertos descubiertos por el barrido de pings. Por último, los hackers pueden examinar las características de las aplicaciones que se están ejecutando en los hosts. Esto puede llevar al hacker a información que puede serle útil para intentar poner en peligro dicho servicio.

El reconocimiento de la red no puede evitarse en su totalidad. Por ejemplo, si el eco ICMP y la respuesta al eco se desactiva en los routers de contorno, se pueden detener los barridos de pings, pero a expensas de los datos de diagnóstico de la red. Sin embargo, los rastreos de puertos pueden ejecutarse fácilmente sin barridos de pings completos, aunque tardarán más en finalizar ya que necesitan rastrear direcciones IP que quizá no estén vivas. IDS a los niveles de red y de host puede informar normalmente al administrador cuando se vaya a producir un ataque de este tipo, lo que permite al administrador prepararse mejor para combatirlo, o indicar al ISP quién está alojando al sistema que está lanzando la sonda de reconocimiento.

Abuso de confianza

Aunque no es un ataque en si mismo, el abuso de confianza indica un ataque en el que un individuo se aprovecha de una relación de confianza dentro de una red. El ejemplo clásico es una conexión de red de perímetro de una empresa. Estos segmentos de red suelen albergar servidores DNS, SMTP y HTTP. Dado que todos ellos se encuentran en el mismo segmento, el hecho de que un sistema esté en peligro puede poner en peligro a los restantes sistemas, ya que pueden confiar en otros sistemas conectados a la misma red. Otro ejemplo es un sistema del exterior de la red que tenga una relación de confianza con un sistema que esté dentro de la red. Si el sistema externo está en peligro, puede hacer uso de dicha relación de confianza para atacar la parte interior de la red.

Los ataques basados en abuso de confianza pueden combatirse a través de férreas limitaciones en los niveles de confianza de la red. Los sistemas que estén dentro de un firewall nunca deberían confiar plenamente en los sistemas que estén fuera de él. Dicha confianza debe limitarse a determinados protocolos y, siempre que sea posible, debe autenticarla algo que no sea una dirección IP.

Redireccionamiento de puertos

Los ataques de redireccionamiento de puertos son un tipo especial de abuso de confianza que utiliza un host que está en peligro para pasar tráfico que en condiciones normales sería rechazado a través de un firewall. Piense en un firewall con tres interfaces y un host en cada interfaz. El host del exterior puede acceder al host del segmento de servicios públicos (normalmente denominado DMZ), pero no al host interno. El host del segmento de servicios públicos puede acceder tanto al host externo como al interno. Si los hackers fueran capaces de poner en peligro al host del segmento de servicios públicos, podrían instalar software que redireccionara el tráfico del host externo directamente al interno. Aunque ninguna comunicación viola las reglas implementadas en el firewall, el host externo ya ha conseguido conectividad con el interno a través del proceso de redireccionamiento en el host de servicios públicos. Un ejemplo de una aplicación que puede proporcionar este tipo de acceso es netcat. Para obtener más información, consulte la siguiente dirección URL: http:// www.avian.org

El redireccionamiento de puertos se puede combatir principalmente a través del uso de los modelos de confianza apropiados (como ya se ha indicado). Si un sistema sufre un ataque, el IDS basado en host puede ayudar a detectar al hacker y evitar que instale dichas utilidades en ningún host.

Acceso no autorizado

Aunque no es un tipo de ataque específico, el acceso no autorizado hace referencia a la mayoría de los ataques que se realizan actualmente a las redes. Para que alguien realice un ataque por fuerza bruta a una conexión por telnet, antes debe lograr el indicativo de telnet en un sistema mediante conexión al puerto de telnet, un mensaje puede indicar: "authorization required to use this resource". Si el hacker sigue intentando acceder, sus acciones pasan a ser "no autorizadas". Estos tipos de ataques pueden iniciarse tanto en el exterior como en el interior de una red.

Las técnicas para combatir los ataques de accesos no autorizados son muy sencillas. Implican la reducción o la eliminación de la posibilidad que tiene un hacker para obtener acceso a un sistema utilizando un protocolo no autorizado. Un ejemplo sería evitar que los hackers tuvieran acceso al puerto de telnet de un servidor que necesite proporcionar servicios de Web al exterior. Si los hackers no pueden acceder a dicho puerto, es muy difícil que lo ataquen. La función principal de los firewalls de las redes es evitar ataques de acceso no autorizado.

Virus y troyanos

Los principales puntos vulnerables de las estaciones de trabajo de los usuarios finales son los ataques de virus y de troyanos. Los virus son elementos de software dañinos que están vinculados a otro programa para ejecutar una función determinada no deseada en la estación de trabajo de un usuario. Un ejemplo de virus es un programa que esté

vinculado a command.com (el principal intérprete de los sistemas Windows) y que elimine determinados archivos e infecte las restantes versiones de command.com que encuentre. Los troyanos sólo difieren de los virus en que toda la aplicación se ha escrito para parecer otra cosa, cuando de hecho es una herramienta de ataque. Un ejemplo de troyano es una aplicación de software que ejecuta un simple juego en la estación de trabajo del usuario. Mientras el usuario está entretenido con el juego, el troyano envía por correo una copia de si mismo a todas las direcciones de la libreta de direcciones del usuario. A continuación, otros usuarios reciben el juego y vuelve a iniciarse la cadena, con lo que se extiende el troyano.

Estos tipos de aplicaciones pueden contenerse a través de un uso eficaz del software antivirus a nivel de usuario y, potencialmente, a nivel de red. El software antivirus puede detectar la mayoría de los virus y muchos de los troyanos, y evitar que se diseminen por la red. Mantenerse al día de los últimos desarrollos en este tipo de ataques también puede conducir a una postura más eficaz frente a estos ataques. A medida que aparecen nuevos virus o troyanos, las empresas deben actualizarse con el software antivirus y con las versiones de las aplicaciones más recientes.

¿Qué es una "normativa de seguridad"?

Una normativa de seguridad puede ser tan simple como una normativa de uso aceptable de los recursos de la red y puede llegar a tener varios cientos de páginas y detallar cada elemento de la conectividad y las normativas asociadas con él. Aunque su alcance es, hasta cierto punto, limitado, RFC 2196 define perfectamente las normativas de seguridad:

"Una normativa de seguridad es una declaración formal de las reglas que deben acatar las personas a las que se otorga acceso a la tecnología y a la información de una organización".

Este documento no pretende entrar en profundidad en el desarrollo de una normativa de seguridad. En RFC 2196 puede encontrar información disponible sobre el tema y un gran número de lugares de la Web tienen normativas y pautas de ejemplo. Las siguientes páginas Web pueden servir de ayuda a los lectores interesados en el tema:

- RFC 2196 "Site Security Handbook"

  http://www.ietf.org/rfc/rfc2196.txt

- Un ejemplo de normativa de seguridad de la Universidad de Illinois
  http://www.aits.uillinois.edu/security/securestandards.html

- Diseño e implementación de la normativa de seguridad de la empresa
  http://www.knowcisco.com/content/1578700434/ch06.shtml

La necesidad de una normativa de seguridad

Es importante saber que la seguridad de la red es un proceso en evolución. Ningún producto puede lograr que una organización sea "segura". La verdadera seguridad de la red se consigue mediante una combinación de productos y servicios, junto con una normativa de seguridad exhaustiva y el compromiso de observar dicha normativa empezando por la cúpula de la organización y llegando hasta el último trabajador. De hecho, una normativa de seguridad implementada correctamente sin hardware de seguridad dedicado puede ser más eficaz para combatir las amenazas a los recursos de la empresa que la implementación exhaustiva de un producto de seguridad sin ninguna normativa asociada.

Anexo C: Taxonomía de la arquitectura

Servidor de aplicaciones: proporciona servicios de aplicaciones directa o indirectamente a los usuarios finales de la empresa. Los servicios son los siguientes: flujo de trabajo, oficina en general y aplicaciones de seguridad.

Firewall (con estado): el dispositivo de filtro de paquetes con estado que mantienen las tablas de los estados de los protocolos basados en IP. El tráfico sólo puede atravesar el firewall si se ajusta a los filtros de control de acceso definidos o si forma parte de una sesión ya establecida de la tabla de estados.

IDS de host : Host Intrusion Detection System es una aplicación de software que controla la actividad en los hosts individuales. Las técnicas de control pueden incluir la validación del sistema operativo y de las llamadas a aplicaciones, la comprobación de los archivos de registro, la información del sistema de archivos y las conexiones de la red.

IDS de red: Network Intrusion Detection System. Este dispositivo se suele emplear sin interrupciones y captura el tráfico de un segmento de la LAN e intenta comparar el tráfico en tiempo real con las firmas de ataques conocidos. Las firmas oscilan entre atómicas (un solo paquete y una sola dirección) y compuestas (varios paquetes), y requieren tablas de estados y seguimiento de las aplicaciones de Capa 7.

Firewall IOS: un firewall de filtro de paquetes con estado que funciona de forma nativa en Cisco IOS (Internetwork Operating System).

Router IOS: un amplio espectro de dispositivos de red flexibles que proporcionan muchos servicios de enrutamiento y de seguridad para todos los requisitos de rendimiento. La mayoría de los dispositivos son modulares y tienen varias interfaces físicas de LAN y WAN.

Switch de Capa 2: proporciona ancho de banda y servicios de VLAN a los segmentos de red a nivel de Ethernet. Normalmente, estos dispositivos ofrecen puertos conmutados individuales 10/100, enlaces ascendentes Ethernet Gigabit, enlaces troncales VLAN y características de filtro L2.

Switch de Capa 3: ofrece funciones de transferencias similares a las de los switches de Capa 2 y añade las características de enrutamiento, QoS y seguridad. Estos switches a menudo tienen las capacidades de los procesadores de funciones especiales.

Servidor de gestión: proporciona servicios de gestión de red a los operadores de las redes de las empresas. Los servicios son los siguientes: gestión de la configuración general, control de los dispositivos de seguridad de la red y manejo de las funciones de seguridad.

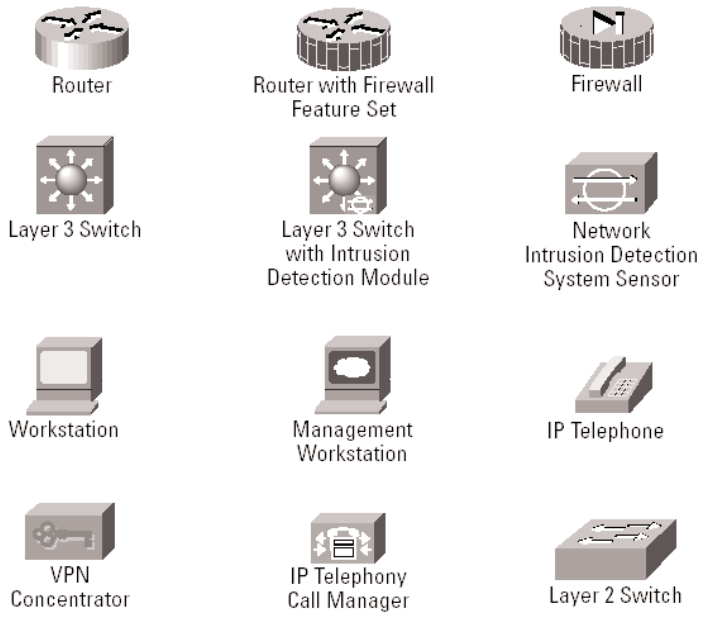
Servidor de filtro de contenidos de SMTP: una aplicación que suele funcionar en un servidor SMTP externo que controla el contenido (incluyendo los archivos adjuntos) del correo entrante y saliente para decidir si dicho correo está autorizado para enviarse tal cual, alterarlo y reenviarlo, o eliminarlo.

Servidor de filtro de direcciones URL: una aplicación que suele funcionar en un servidor independiente que controla las solicitudes de direcciones URL que le reenvía un dispositivo de red e informa al dispositivo de red de si la solicitud debería reenviarse a Internet. Esto permite a las empresas implementar una normativa de seguridad que indique las categorías de los sitios de Internet que no están autorizadas.

Dispositivo de terminación de VPN: termina los túneles IPSec de las conexiones sitio a sitio o de VPN de acceso remoto. El dispositivo debe proporcionar más servicios para ofrecer las mismas funciones de red que una conexión WAN clásica o de acceso telefónico.

Estación de trabajo o terminal de usuario: cualquier dispositivo de la red que utilice directamente el usuario final. Entre estos se incluyen los PC, teléfonos IP, dispositivos inalámbricos, etc.

Leyenda de los diagramas



Referencias

RFC

RFC 2196 "Site Security Handbook" - http://www.ietf.org/rfc/rfc2196.txt

RFC 1918 "Address Allocation for Private Internets" - http://www.ietf.org/rfc/rfc1918.txt

RFC 2827 "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" - http://www.ietf.org/rfc/rfc2827.txt

Otras referencias

"Mejora de la seguridad de los routers de Cisco" - http://www.cisco.com/warp/customer/707/21.html

"Informe de las pruebas de la seguridad de VLAN" - http://www.sans.org/newlook/resources/IDFAQ/vlan.htm

"AntiSniff" - http://www.l0pht.com/antisniff/

"L0phtCrack" - http://www.l0pht.com/l0phtcrack/

"Ataques de denegación de servicio" - http://www.cert.org/tech_tips/denial_of_service.html

"Computer Emergency Response Team" - http://www.cert.org

"Security Focus (Bugtraq)" - http://www.securityfocus.com

"Avian Research (netcat)" - http://www.avian.org

"Normativa de seguridad de la Universidad de Illinois" - http://www.aits.uillinois.edu/security/securestandards.html

"Diseño e implementación de la normativa de seguridad de la empresa" - http://www.knowcisco.com/content/1578700434/ch06.shtml

Referencias de productos de empresas asociadas

IDS basado en host Entercept de ClickNet - http://www.clicknet.com

Sistema OTP SecureID de RSA - http://www.rsasecurity.com/products/securid/

Sistema de filtro de correo electrónico MIMESweeper de Content Technologies - http://www.contenttechnologies.com

Filtro de direcciones URL Websense - http://www.websense.com/products/integrations/ciscopix.cfm

Análisis de syslogs netForensics - http://www.netforensics.com/

Agradecimientos

Los autores de este documento quieren dar las gracias públicamente a aquellas personas que han contribuido a la arquitectura SAFE y a la creación de este documento. Indudablemente, la correcta creación de esta arquitectura no habría sido posible sin la valiosa información y revisión de todos los trabajadores de Cisco, tanto de las oficinas centrales como sobre el terreno. Además, muchas personas han contribuido a la implementación y validación en laboratorio de la arquitectura. La parte central de este grupo estaba compuesta por Roland Saville, Floyd Gerhardt, Majid Saee, Mark Doering, Charlie Stokes, Tom Hunter, Kevin McCormick y Casey Smith. Gracias a todos por los especiales esfuerzos realizados.

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

Oficinas centrales en Europa
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les- Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

Oficinas centrales en Asia Pacífico
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems tiene más de 200 oficinas en los siguientes países y regiones. Las direcciones, números de teléfono y de fax pueden encontrarse en el

sitio Web de Cisco www.cisco.com/go/offices

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