Diseño de red segura

Las organizaciones aprovechan el poder de Internet para conectarse con todo tipo de entidades externas, como clientes, organizaciones de clientes y proveedores, por nombrar algunas. Este acceso está destinado a permitir un mecanismo simple y fluido para intercambio de información, para llevar a cabo una variedad de funciones de negocio, y para proporcionar acceso remoto a los sistemas y datos.

Sería bastante difícil que usted encuentre una organización, no importa dónde o cuán pequeña sea, que no aprovecha la Internet en algún aspecto como parte de su operación. Impulsada por los avances en las redes sociales, el alto rendimiento y la computación de bajo costo, la revolución tecnológica móvil y la creciente cantidad de ancho de banda disponible para los dispositivos portátiles, esta tendencia continuará acelerándose en el futuro.

Un acceso global sin precedentes está disponible, y proporcionar un vehículo virtual para que las personas conectadas y operando de la manera más eficiente posible es una parte estándar de las responsabilidades modernas de ti. Para decirlo de otra manera, las empresas deben hacer que sus propiedades y plataformas de información estén disponibles de forma remota a terceros, a menudo incluyendo material y datos sensibles. Si bien en muchos casos es importante que un negocio pueda proporcionar este acceso, también es muy importante trazar una línea entre donde la responsabilidad de la administración de la seguridad de ti no es un rol meramente para grandes organizaciones sino una necesidad de la actualidad.

El diseño subyacente de la red desempeña un papel fundamental en la capacidad de una organización para administrar y proteger eficazmente el acceso a sus datos.

Introducción al diseño de redes seguras

Todos los sistemas de información crean riesgos para una organización, y si el nivel de riesgo introducido es aceptable es en última instancia una decisión empresarial. Se pueden usar controles como firewalls, aislamiento de recursos, configuraciones que endurezca los sistemas, sistemas de autenticación, control de acceso y cifrado para ayudar a mitigar los riesgos identificados a niveles aceptables.

Riesgo aceptable

Lo que constituye un nivel aceptable de riesgo, depende de la organización y de su capacidad para tolerar el riesgo. Una organización que no les teme a los riesgos, en última instancia, aceptará niveles más bajos de riesgo y requerirá más controles de seguridad en los sistemas implementados. La tolerancia al riesgo de la gerencia se expresa a través de las políticas, procedimientos y pautas emitidas al personal. Un conjunto completo de políticas que describen las preferencias de la administración y su tolerancia a los riesgos de seguridad de la información permite a los empleados tomar decisiones de infraestructura apropiadas al diseñar y proteger nuevos sistemas y redes. Por lo tanto, el diseño y la configuración de la infraestructura se convierte en la observancia de esos documentos.

Algunas organizaciones toman involuntariamente más riesgo de lo que pretenden al no ser conscientes de los instrumentos legislativos a los que están sometidos dentro de una jurisdicción legal.

Las leyes informáticas y de información han evolucionado y cambiado rápidamente, y abarcan cientos de volúmenes de material y miles de páginas web solo para Estados Unidos. Eso ni siquiera está considerando los desafíos que enfrentan las corporaciones multinacionales cuando operan en el suelo de muchas naciones. Durante el desarrollo de las políticas que guiarán el diseño de los sistemas y redes, la gerencia debe dedicar el tiempo y el esfuerzo necesarios para determinar si alguna de estas consideraciones legales especiales se aplica.

Muchas empresas violan inadvertidamente ciertas leyes sin siquiera saber que lo están haciendo (por ejemplo, almacenar números de tarjetas de crédito sin tener en cuenta el estándar de seguridad de datos de la industria de tarjetas de pago [PCI DSS], o almacenar datos de pacientes sin tomar en cuenta la ley de portabilidad y rendición de cuentas de seguros de salud [HIPAA]. Esto modifica el nivel de riesgo residual realmente producido después de que se apliquen los controles, ya que los controles planificados pueden no abordar los riesgos que no están claramente definidos antes del desarrollo del plan de control.

Diseñar la seguridad en una red

La seguridad es a menudo un aspecto ignorado del diseño de red, y los intentos de reequipar la seguridad sobre una red existente pueden ser costosos y difíciles de implementar correctamente.

La separación de los activos de diferentes requisitos de confianza y seguridad debe ser un objetivo integral durante la fase de diseño de cualquier proyecto nuevo. La agregación de activos que tienen requisitos de seguridad similares en zonas dedicadas permite a una organización utilizar un pequeño número de dispositivos de seguridad de red, como firewalls y sistemas de detección de intrusiones, para proteger y supervisar varios sistemas de aplicaciones.
Otras influencias en el diseño de red incluyen presupuestos, requisitos de disponibilidad, tamaño y alcance de la red, expectativas de crecimiento futuras, requisitos de capacidad y tolerancia de riesgos de la administración.

Por ejemplo, los enlaces WAN dedicados a oficinas remotas pueden ser más fiables que las redes privadas virtuales (VPNs), pero cuestan más, especialmente cuando cubren grandes distancias. Las redes totalmente redundantes pueden recuperarse fácilmente de los fallos, pero con el hardware duplicado aumenta los costos y cuantas más rutas de enrutamiento estén disponibles, más difícil será proteger y segregar los flujos de tráfico.

Un factor significativo, pero a menudo omitido o subconsiderado en la determinación de una estrategia de diseño de seguridad adecuada es identificar cómo se utilizará la red y lo que se espera de la empresa que apoya. Esta diligencia de diseño puede ayudar a evitar cambios costosos y difíciles después de la implementación de la red. Consideremos algunas estrategias clave de diseño de red.

Modelos de diseño de red

Para pintar una imagen más clara de cómo el diseño global afecta a la seguridad, examinemos los diseños de un centro comercial y un aeropuerto. En un centro comercial, para hacer la entrada y salida lo más conveniente posible, se proporcionan numerosas entradas y salidas. Sin embargo, el gran número de entradas y salidas hace que los intentos de controlar el acceso al centro comercial sean costoso y difícil. Se requerirían mecanismos de vigilancia en cada puerta para identificar y bloquear a los visitantes no deseados. Además, la implementación de un mecanismo de vigilancia no es el único obstáculo; después de que se implemente, cada mecanismo debe mantenerse configurado y actualizado correctamente para asegurarse de que una persona no autorizada no se deslice a través de la entrada.

En cambio, un aeropuerto está diseñado para canalizar a todos los pasajeros a través de un pequeño número de puntos de control bien controlados para la inspección. Las redes construidas en el modelo del centro comercial son inherentemente más difíciles de asegurar que las redes diseñadas alrededor del modelo del aeropuerto. Las redes creadas con muchas conexiones a otras redes serán intrínsecamente más difíciles de proteger debido al número de mecanismos de control de acceso (como firewalls) que deben implementarse y mantenerse.

El diseño de un aeropuerto hace mucho más que simplemente facilitar la detección de pasajeros realizada justo dentro de una terminal. En general, el aeropuerto tiene un diseño altamente compartimentado que requiere que un individuo pase a través de un chequeo de seguridad cada vez que pasa entre compartimentos. No todos los exámenes son explícitos — algunos monitoreos son pasivos, involucrando cámaras y policías encubiertos estacionados en todo el aeropuerto.

Hay puntos de control explícitos entre la terminal principal y las áreas de la puerta, así como entre el área de la puerta y el avión. Hay controles de seguridad para los movimientos internos del aeropuerto, así, y el personal necesita llaves de acceso especiales para entrar en las áreas internas, tales como el procesamiento de equipaje y la pista.

Diseñar una red adecuada

Existen invariablemente numerosos requisitos y expectativas colocados en una red, como satisfacer y exceder los requisitos de disponibilidad y rendimiento de la organización, proporcionando una plataforma que sea segura para proteger los activos sensibles de la red, y permitiendo enlaces efectivos y seguros a otras redes. Además de eso, el diseño de red global debe proporcionar la capacidad de crecer y apoyar los futuros requisitos de red. Como se ilustra anteriormente con las analogías del aeropuerto y el centro comercial, el diseño general de la red afectará la capacidad de una organización para proporcionar niveles de seguridad acordes con los riesgos asociados con los recursos o en esa red.

Para diseñar y mantener una red que apoye las necesidades de sus usuarios, los arquitectos e ingenieros de redes deben tener una sólida comprensión de cuáles son esas necesidades. La mejor manera de hacerlo es involucrar a los arquitectos e ingenieros en el proceso de desarrollo de aplicaciones. Al involucrarse al principio del ciclo de desarrollo, los ingenieros pueden sugerir diseños y topologías más seguros, y además pueden asegurar al equipo del proyecto que tienen una comprensión clara de las consideraciones y capacidades de seguridad. Además, pueden garantizar que los nuevos proyectos son más compatibles con la infraestructura corporativa existente.

Los pasos comunes para obtener dicha información incluyen la reunión con las partes interesadas del proyecto, los propietarios de aplicaciones y sistemas, los desarrolladores, la administración y los usuarios. Es importante comprender sus expectativas y necesidades con respecto al rendimiento, la seguridad, la disponibilidad, el presupuesto y la importancia general del nuevo proyecto. La comprensión adecuada de estos elementos garantizará que se cumplan los objetivos del proyecto y que se incluyan en el diseño los controles de seguridad y rendimiento de red apropiados. Uno de los problemas más comunes encontrados en una implementación de red son las expectativas no satisfechas resultantes de una diferencia de suposiciones. Es por eso que las expectativas deben dividirse en hechos mutuamente observables (y medibles) tanto como sea posible, por lo que los diseñadores de seguridad se aseguran de que exista un acuerdo explícito con cualquier propuesta funcional claramente entendida y acordada.

El costo de la seguridad

Los mecanismos de control de seguridad tienen gastos asociados con su compra, despliegue y mantenimiento, y la implementación de estos sistemas de manera redundante puede aumentar los costos significativamente. Al decidir sobre los controles de redundancia y seguridad apropiados para un sistema o red determinado, es útil crear una serie de escenarios negativos en los que se produzca una infracción de seguridad o una interrupción, para determinar los costos de la Corporación para cada ocurrencia. Este enfoque de modelo de riesgo debería ayudar a la gerencia a determinar el valor para la Corporación de los diversos mecanismos de control de seguridad.

Rendimiento

La red desempeñará un gran papel al cumplir los requisitos de rendimiento de una organización.

Las redes son cada vez más rápidas, evolucionando de 10 megabit a 100 megabit a velocidades de Gigabit, con 10GE comúnmente implementado y 40GE, 100GE, y tecnologías InfiniBand disponibles en la actualidad. Al determinar la tecnología de red adecuada, asegúrese de que puede cumplir los requisitos de ancho de banda proyectados durante tres a cinco años en el futuro. De lo contrario, es posible que se requieran reemplazos o actualizaciones costosas.

Las aplicaciones y redes que tienen baja tolerancia para la latencia, como las que soportan el streaming de vídeo y voz, obviamente requerirán conexiones de red y hardware de mayor rendimiento. ¿Qué sucede con las aplicaciones que mueven datos en fragmentos grandes (por ejemplo, instantáneas de almacenamiento o replicación fuera del sitio de disco a disco)? En lugar de una costosa, dedicada, conexión de alto ancho de banda, puede ser más económico para implementar enlaces que son *con ráfagas*, lo que significa que el proveedor permitirá ráfagas cortas de tráfico por encima de la tasa de suscripción normal.

Si las aplicaciones compartirán componentes de infraestructura de red comunes, el equipo de diseño también puede considerar la implementación de tecnologías de calidad de servicio (QoS) para evitar que una aplicación consuma demasiado ancho de banda, o para garantizar que la mayor prioridad de las aplicaciones siempre tiene suficiente ancho de banda disponible.

El modelo jerárquico de Internetworking de Cisco heredado (Ciso Internetworking H), que la mayoría de los ingenieros de la red están íntimamente familiarizados, es un diseño comúnmente implementado en las redes a gran escala hoy en dia, aunque muchos nuevos tipos de diseños propuestos se han desarrollado que apoyan tecnologías emergentes, Ethernet sin pérdidas, capa dos bridging con trill o IEEE 802.1 AQ, y otras tecnologías centradas en centros de datos.

• **Core layer** Forma la red troncal y se centra en mover datos lo más rápido posible entre las capas de distribución. Dado que el rendimiento es el foco principal de la capa base, no debe utilizarse para realizar operaciones intensivas de CPU, como filtrar, comprimir, cifrar o traducir direcciones de red para el tráfico.

• **Distribution layer** Se encuentra entre el núcleo y la capa de acceso. Esta capa se utiliza para agregar el tráfico de la capa de acceso para la transmisión dentro y fuera del núcleo.

• **Access layer** Compuesto de las conexiones de red del usuario.

Los siguientes son fundamentos de red de dos niveles (la terminología de tres niveles se utiliza con fines comparativos):

• **Core** El núcleo de la red de dos niveles es un elemento de alta disponibilidad y escalabilidad horizontal que se utiliza para el tránsito y la mudanza de datos entre diferentes áreas o zonas de la red, al igual que el núcleo del modelo de tres niveles. La única diferencia importante es que, en general, el núcleo de una red de dos niveles no ve el 100 por ciento del tráfico, ya que gran parte del tráfico de host a host transita sin necesidad de ser manejado por el núcleo.

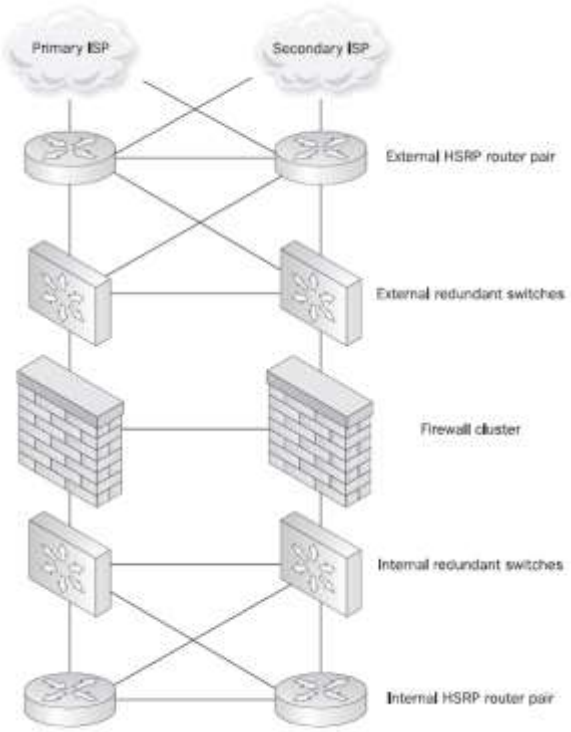
• **Distribution** La capa de distribución en algunas redes colapsadas se elimina completamente o se combina con la capa de acceso. Aunque una capa de la "distribución" puede existir literalmente, no existe lógicamente, pues es parte del switch o del cluster de la conmutación como la conmutación de acceso.

• **Access** La capa de acceso se contrae en la capa de distribución, así que mientras que los dispositivos físicamente separados pueden proporcionar la agregación y la función de acceso, ambos pueden ser parte del mismo dominio de la capa-dos. Estas capas combinadas ofrecen conectividad activa/activa a través de múltiples switches mediante clustering para una alta disponibilidad y rendimiento. Esto introduce una nueva dimensión para la seguridad, como la comunicación de servidor a servidor, de servidor a almacenamiento y de host virtual ahora se puede fusionar de formas que antes no era posible.

Disponibilidad

La disponibilidad de la red requiere que los sistemas sean adecuadamente resilientes y estén disponibles para los usuarios de forma oportuna (es decir, cuando los usuarios los requieran). Lo contrario de la disponibilidad es la denegación de servicio, que es cuando los usuarios no pueden acceder a los recursos que necesitan de forma oportuna. La denegación de servicio puede ser intencional (por ejemplo, el acto de personas malintencionadas) o accidental (como cuando falla el hardware o el software). Los sistemas no disponibles cuestan dinero real a las corporaciones en ingresos perdidos y productividad de los empleados, y pueden lastimar a las organizaciones de maneras intangibles a través de la confianza perdida del consumidor y la publicidad negativa. Las necesidades de disponibilidad empresarial han impulsado a algunas organizaciones a construir centros de datos duplicados que realizan espejo en tiempo real de sistemas y datos para proporcionar failover y reducir el riesgo de un desastre natural o un ataque terrorista destruyendo su único centro de datos
.

La mejor práctica para garantizar la disponibilidad es evitar puntos de falla dentro de la arquitectura. Esto puede requerir funcionalidades redundantes y/o de failover en las funciones de hardware, red y aplicación. Una solución totalmente redundante puede ser extremadamente costosa de implementar y mantener, porque a medida que aumenta el número de mecanismos de conmutación por error, aumenta la complejidad del sistema, que solo puede aumentar los costos de soporte y complicar la solución de problemas.



Como se mencionó anteriormente, los requisitos de disponibilidad de la aplicación deben evaluarse para determinar los impactos financieros y empresariales de los sistemas que no están disponibles. La realización de esta evaluación ayudará a la administración a llegar al equilibrio óptimo entre los mecanismos de conmutación por error, el costo y la complejidad de la red o aplicación concreta. Numerosos proveedores de dispositivos de seguridad tienen mecanismos de conmutación por error que permiten a un firewall secundario asumir responsabilidades de procesamiento en caso de que falle el Firewall principal. Además de los firewalls, los enrutadores también se pueden implementar en una configuración de alta disponibilidad.

Seguridad

Cada elemento de una red realiza funciones diferentes y contiene datos de diferentes requisitos de seguridad. Algunos dispositivos contienen información altamente confidencial que podría dañar a una organización si se difundió a personas no autorizadas, como registros de nómina, memorandos internos, listas de clientes e incluso documentos internos de cálculo del coste del trabajo.

Otros dispositivos tienen más exposición debido a su ubicación en la red. Por ejemplo, los servidores de archivos internos se protegerán de manera diferente que los servidores web disponibles públicamente. Al diseñar e implementar la seguridad en las arquitecturas de red y de sistema, resulta útil identificar los controles de seguridad críticos y comprender las consecuencias de un error en esos controles. Por ejemplo, los firewalls protegen a los hosts limitando los servicios a los que los usuarios pueden conectarse en un sistema determinado. Los firewalls pueden permitir que diferentes conjuntos de usuarios accedan de forma selectiva a diferentes servicios, como permitir a los administradores del sistema acceder a los servicios administrativos y evitar que los usuarios no administrativos accedan a esos mismos servicios. Esto proporciona un nivel adicional de control sobre el que proporcionan los propios mecanismos administrativos.

Al negar a un usuario no administrativo la capacidad de conectarse al servicio administrativo, se impide al usuario montar un ataque directamente en ese servicio sin eludir primero el firewall.

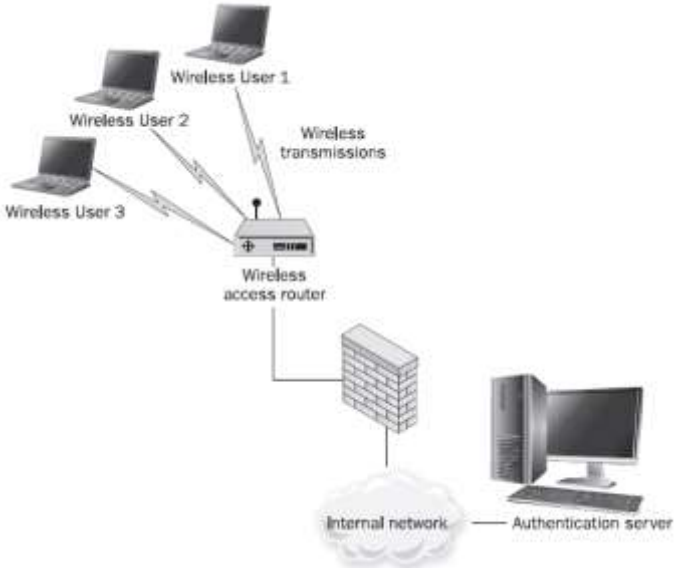
Sin embargo, simplemente restringir a los usuarios a servicios específicos puede ser insuficiente para lograr el nivel de seguridad deseado. Por ejemplo, es necesario permitir que el tráfico a través del firewall se conecte a varios servicios autorizados. Para que una organización envíe y reciba correo electrónico, los firewalls deben configurarse de permitir el tráfico de correo electrónico. Los firewalls tienen capacidad limitada en la prevención de ataques dirigidos a aplicaciones autorizadas, por lo que la seguridad global de la red depende de la operación adecuada y segura de esas aplicaciones.

Impacto de las redes inalámbrica en el perímetro

La seguridad perimetral de red solo es útil si hay controles de seguridad físicos adecuados para evitar que un usuario no autorizado simplemente se acerca y se conecte a la red interna. Por lo tanto, sin acceso físico a la red, un usuario malintencionado puede explotar una debilidad en los controles de seguridad del perímetro corporativo para obtener acceso. Las organizaciones que implementan soluciones inalámbricas deben

reconocer y mitigar los riesgos asociados con un individuo no autorizado que obtiene conectividad a la LAN corporativa a través de fugas de señal inalámbrica fuera de las instalaciones controladas por las empresas. Simplemente consiguiendo estar físicamente lo suficientemente cerca, un usuario malicioso con un ordenador portátil y una tarjeta LAN inalámbrica puede ser capaz de obtener una dirección IP en la red.

Mientras que las señales de los puntos de acceso inalámbricos se degradan rápidamente al pasar a través de paredes y a lo largo de la distancia, las antenas direccionales más potentes y especializadas pueden captar señales a distancias significativas. Estas antenas, llamadas antenas Yagi, pueden captar señales inalámbricas a distancias que se aproximan a una milla. Mientras que las antenas comerciales Yagi pueden ser costosas



Además de los problemas de la señal-salida, los defectos se han descubierto en los mecanismos de encripción usados para proteger el tráfico sin hilos. Por lo tanto, las redes inalámbricas corren un riesgo significativo de que las comunicaciones de red sean interceptadas y monitoreadas por partes no autorizadas.

Para mitigar los riesgos creados por la deficiente encriptación y la monitorización de señales, se ha convertido en algo común segregar la conectividad inalámbrica del resto de la LAN corporativa. Como se muestra, los administradores han aumentado los mecanismos de control inalámbrico con las soluciones VPN para proporcionar una autenticación segura y el cifrado del tráfico inalámbrico para lograr niveles adecuados de seguridad para los datos inalámbricos y para acceder a los Recursos.

Consideraciones sobre el acceso remoto

La mayoría de las redes corporativas permiten el acceso de usuarios a recursos internos desde ubicaciones remotas.

Mientras que algunas corporaciones todavía mantienen acceso telefónico como una solución de respaldo o secundaria, el acceso remoto ahora se proporciona generalmente a través de una solución VPN. Este tipo de VPN, que conecta a las personas ubicadas remotamente a la red de la organización, es una VPN de acceso remoto (como se distingue de una VPN de sitio a sitio o LAN a LAN, que conecta dos redes juntas).

Las VPNs proporcionan un medio para proteger los datos mientras viaja a través de una red que no es de confianza, proporcionan servicios de autenticación antes de permitir el tráfico VPN y funcionan a velocidades de red.

A pesar de su utilidad, las VPNs tienen un impacto significativo en el perímetro de la red corporativa. En función de cómo se configuran, las VPNs pueden permitir que las estaciones de trabajo remotas se conecten como si estuvieran conectadas físicamente a la red local, aunque permanecen fuera de la protección de la infraestructura de seguridad corporativa. Cuando los pares VPN consisten en usuarios remotos que acceden a la red corporativa a través de Internet, la seguridad general de la red corporativa depende de la seguridad del equipo remoto de ese empleado. Si un hacker obtiene acceso a un PC sin protección, la VPN se puede utilizar para tunelar el tráfico más allá de los firewalls corporativos y la protección que proporcionan.

Para proteger la red corporativa cuando se utilizan VPNs para el acceso de usuarios remotos, los administradores de seguridad deben asegurarse de que la protección adecuada se implementa a través de los puntos de conexión. La mayoría de los principales proveedores de firewall y VPN incluyen la funcionalidad de cortafuegos en sus clientes.

Prácticas de seguridad interna

Las organizaciones que implementan firewalls estrictamente alrededor del perímetro de su red se dejan vulnerables a los ataques iniciados internamente, que son estadísticamente las amenazas más comunes hoy en día. Los controles internos, como los firewalls y los sistemas de detección temprana (IDS, IPS y SIEM), deben ubicarse en puntos estratégicos dentro de la red interna para proporcionar seguridad adicional para recursos especialmente sensibles como redes de investigación, repositorios que contienen propiedad intelectual y bases de datos de recursos humanos y nóminas.

Intranets, Extranets, and DMZs

Las organizaciones deben proporcionar información a los usuarios internos y externos y conectar su infraestructura a redes externas, por lo que han desarrollado topologías de red y arquitecturas de aplicaciones que soportan esa conectividad mientras mantienen niveles adecuados de seguridad. Los términos más prevalentes para describir estas arquitecturas son *Intranet*, *Extranet*Y *zona desmilitarizada (DMZ)*. Las organizaciones a menudo segregan las aplicaciones desplegadas en sus intranets y extranets de otros sistemas internos mediante el uso de firewalls. Una organización puede ejercer niveles más altos de control a través de la protección contra incendios para garantizar la integridad y la seguridad de estos sistemas.

Intranets

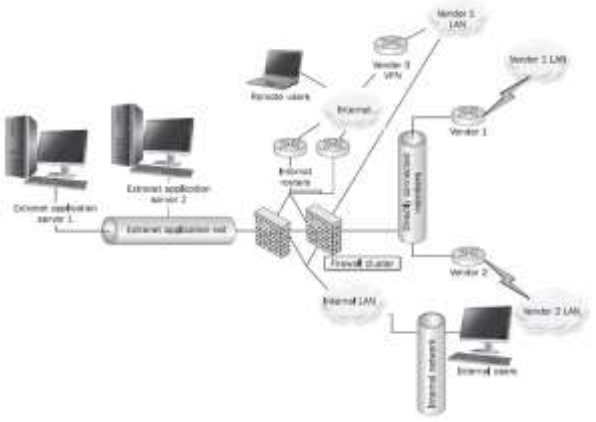
El objetivo principal de un *Intranet* es proporcionar a los usuarios internos acceso a las aplicaciones y la información. Las intranets se utilizan para albergar aplicaciones internas que generalmente no están disponibles para entidades externas, como sistemas de tiempo y gastos, bases de conocimiento y tablones de anuncios de organización. El objetivo principal de una Intranet es compartir la información de la organización y los recursos informáticos entre los empleados. Para lograr un mayor nivel de seguridad, los sistemas de intranet se agregan a una o más subredes dedicadas y son cortafuegos.

Desde el punto de vista de la conectividad lógica, el término *Intranet* no significa necesariamente una red interna. Las aplicaciones de intranet pueden diseñarse para ser universalmente accesibles. Por lo tanto, los empleados pueden ingresar sus sistemas de tiempo y gastos mientras están en sus escritorios o en la carretera. Cuando las aplicaciones de intranet se hacen accesibles públicamente, es una buena práctica segregar estos sistemas de sistemas internos y asegurar el acceso con un firewall. Además, dado que la información interna se transferirá como parte de la función de aplicación normal, es común cifrar dicho tráfico. No es infrecuente implementar aplicaciones de intranet en una configuración DMZ para mitigar los riesgos asociados con la provisión de acceso universal.

Extranets

Las extranets son redes de aplicaciones controladas por una organización y que están disponibles para las partes externas de confianza, como proveedores, proveedores, socios y clientes.

Los usos posibles para las extranets son variados y pueden incluir proporcionar el acceso de la aplicación a los socios comerciales, a los parnert, a los proveedores, a los vendedores, a los socios, a los clientes, y así sucesivamente. Sin embargo, debido a que estos usuarios son externos a la Corporación, y la seguridad de sus redes está fuera del control de la Corporación, las extranets requieren procesos de seguridad adicionales y procedimientos más allá de los de intranets. Los métodos de acceso a una extranet pueden variar considerablemente: las VPNs, las conexiones directas e incluso los usuarios remotos pueden conectarse.

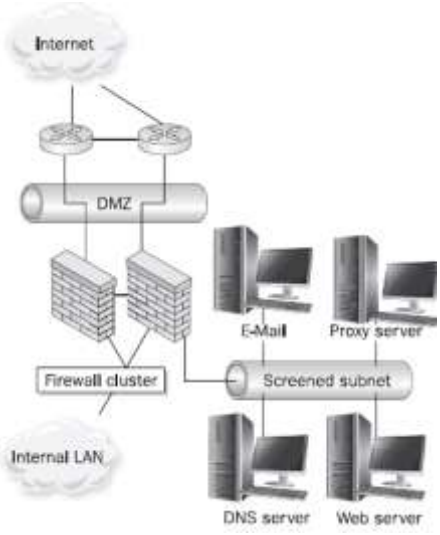


Redes DMZ y subredes filtradas

Una organización puede querer proporcionar acceso público a Internet a ciertos sistemas. Por ejemplo, para que una organización reciba correo electrónico de Internet, el servidor de correo electrónico debe estar disponible en Internet. es recomendable desplegar estos sistemas en una subred dedicada, comúnmente denominada *zona desmilitarizada (DMZ)* O *subred filtrada*, separada de los sistemas internos. Debido a que estos sistemas son accesibles públicamente, pueden y serán atacados por usuarios malintencionados. Al

alojarlos en una red segregada, un ataque exitoso contra estos sistemas todavía deja un firewall entre el atacante exitoso y los recursos internos más sensibles.

Filtrado saliente



Hasta este punto, nos hemos centrado casi enteramente en asegurar el acceso entrante a una red corporativa. Aunque no puede ser inicialmente obvio, el filtrado saliente del tráfico de red puede ser casi tan importante. El hecho de no restringir el acceso saliente crea una serie de riesgos significativos para la Corporación y su infraestructura, como los usuarios que acceden a servicios que no cumplen con las políticas de seguridad corporativas o que no tienen fines comerciales legítimos.

Web Access Considerations

Como se discute en el capítulo 15, es posible evitar conexiones directas entre usuarios internos y externos a través de servicios proxy o filtrado web. Los servidores proxy se pueden configurar para bloquear las conexiones a direcciones URL que se consideran susceptibles de ser maliciosas o innecesarias para el funcionamiento normal, como las que contienen ciertos scripts u otros archivos ejecutables. Los servicios proxy son procesos endurecidos que pueden ejecutarse internamente en un firewall o ser proporcionados por separado por un servidor dedicado. El filtrado web hoy en día se puede manejar a través de una variedad de productos y electrodomésticos especializados, incluyendo algunas ofertas basadas en la nube.

El uso de un servicio Proxy proporciona a una corporación varias opciones adicionales al controlar el tráfico de usuarios. Por ejemplo, es posible que la Corporación desee escanear los archivos descargados en busca de virus antes de la transmisión al usuario final. Un servidor proxy también puede registrar, registrar e informar sobre el uso de Internet del usuario, lo que puede disuadir a los empleados de desperdiciar sus días navegando por sitios web o visitando sitios web no apropiados o relevantes para su función de trabajo.

Filtrado de puertos salientes

El filtrado saliente va mucho más allá del simple filtrado de sitios Web. Otra razón para filtrar el tráfico saliente es asegurarse de que solamente el tráfico autorizado atraviesa los links controlados. Si bien esto puede parecer una declaración terriblemente obvia, los usuarios y los desarrolladores de aplicaciones que se quedan en sus propios dispositivos compilarán y desplegará aplicaciones sin comprender los riesgos de seguridad que están derribando en la organización (y otras organizaciones para que la empresa está conectada).

Para restringir el acceso saliente, es necesario implementar filtros salientes en firewalls perimetrales. Al igual que con el acceso entrante, los filtros restrictivos limitarán los servicios que se pueden usar de forma predeterminada. Esto también requerirá que los administradores de seguridad relajen los filtros a medida que se implementan nuevas aplicaciones y los requisitos empresariales exigen acceso a nuevos servicios.

Al limitar el tráfico saliente a las aplicaciones autorizadas, el filtrado saliente impedirá que los usuarios utilicen aplicaciones peligrosas o que no estén relacionadas con el negocio en el entorno corporativo. También puede reducir la posibilidad de que la red de la organización se pueda utilizar para lanzar un ataque contra otra red — tal ataque podría dañar o causar pérdidas para su víctima, y la organización podría terminar siendo demandada. Independientemente del resultado de ese procedimiento, es costoso y consume mucho tiempo montar una defensa, y puede centrarse publicidad negativa sobre las prácticas de seguridad de la organización. Para simplemente evitar el riesgo de una demanda, es prudente bloquear el acceso no necesario en el perímetro corporativo.

Cumplimiento con los estándares

Si está siguiendo un marco de seguridad específico, aquí está cómo NIST, ISO 27002 y COBIT se vinculan. NIST se centra en la tecnología inalámbrica, COBIT tiene algunas orientaciones generales de alto nivel sin entrar en detalles, y ISO 27002 proporciona la guía más específica para las consideraciones de diseño de red.

NIST

Las siguientes publicaciones especiales del NIST ofrecen orientación específica para proteger las redes inalámbricas:

• SP 800-153: Directrices para la protección de redes de área local inalámbricas (WLAN)
• SP 800-120: Recomendación para los métodos EAP utilizados en el acceso de red inalámbrica Autenticación
• SP 800-97: Establecer redes de seguridad robustas inalámbricas: una guía para IEEE 802.11 i
• SP 800-48: Guía para proteger las redes inalámbricas IEEE 802,11 de Legacy

ISO 27002

La norma ISO 27002 contiene las siguientes disposiciones, a las que los contenidos de este capítulo son relevantes:

• **10.1.4** Las instalaciones de desarrollo y pruebas están separadas de las instalaciones operativas. Cuando sea necesario, las redes de desarrollo y producción deben separarse de mutuamente.
• **10.4.1** Todo el tráfico procedente de redes que no son de confianza se comprueba en busca de malware.
• **11.4.3** El acceso a la red está limitado a dispositivos o ubicaciones específicamente identificados.
• **11.4.5** Los grupos de equipos, usuarios y servicios se segregan en dominios de red lógicos protegidos por perímetros de seguridad.
• **11.4.6** El tráfico de red se filtra por tipo de conexión, como mensajería, correo electrónico, transferencia de archivos, acceso interactivo y acceso a aplicaciones.
• **10.6.1** Los controles de red, incluida la administración y el acceso remoto, deben tener controles operativos efectivos, como instalaciones de administración de sistemas y redes separadas; se establecen las responsabilidades y procedimientos para la gestión de los equipos; y controles especiales protegen la confidencialidad y la integridad del procesamiento de datos a través de la red pública.
• **10.6.2** Las características de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red se identifican e incluyen en cualquier acuerdo de servicios de red.
• **11.4.1** Se define la protección de los servicios de red, incluidas las partes de la red a las que se accede, los servicios de autorización para determinar quién puede hacer qué y los procedimientos para proteger el acceso a las conexiones de red y los servicios de red.
• **11.4.2** La autenticación de usuario para las conexiones externas se realiza con un mecanismo de autenticación para las conexiones externas desafiantes.
• **11.4.3** El equipo se identifica antes de que se permita en las conexiones remotas.
• **11.4.4** El acceso (físico y lógico) a los puertos de diagnóstico está protegido por un mecanismo de seguridad.
• **11.4.5** Las redes se segregan mediante mecanismos de seguridad perimetral como firewalls.
• **11.4.6** Los controles de conexión de red se usan para servicios que se extienden más allá de los límites organizativos.
• **11.4.7** El control de enrutamiento de red, basado en la identificación de origen y destino positiva, se utiliza para garantizar que las conexiones del equipo y los flujos de información no infrinjan la Directiva de control de acceso de las aplicaciones empresariales.
• **11.6.1 and 11.1.1** El acceso está restringido en función de una directiva de control de acceso definida.
• **11.6.2** Los sistemas de la red están segmentados y aislados en función de su riesgo o sensibilidad.

COBIT

COBIT contiene las siguientes disposiciones, a las cuales los contenidos de este capítulo son relevantes:

• **DS5.9** Utilice medidas preventivas, detectoras y correctivas, especialmente parches de seguridad regulares y control de virus, en toda la organización para protegerse contra malware como virus, gusanos, spyware y spam.
• **DS5.10** Utilice firewalls, dispositivos de seguridad, segmentación de red y detección de intrusión para administrar y supervisar el acceso y la información entre redes.