Universidad Nacional Autónoma de Honduras

(UNAH)

Facultad de Ingeniería

Departamento de Ingeniería en Sistemas

Tema:

Tecnologias de seguridad para las redes de datos

Catedrático:

Aula Virtual

Asignatura:

Seguridad Informática

Alumno:

Jared Misael Castro Paguada 20151020512

Fecha:

11 de agosto del 2020

Contenido

INTRODUCCION

Se describen a continuación las categorías de productos que proporcionan seguridad perimetral: principalmente la categoría denominada CORTAFUEGOS, VPN e IPS/IDS, con todas sus subcategorías, y la categoría de GESTIÓN y CONTROL de ACCESO E IDENTIDAD, en particular la subcategoría de Control de acceso a red.

Los productos de las categorías seleccionadas para este monográfico están orientados en particular a la Seguridad en las redes si bien dada la diversidad de productos que existen en el mercado, como se explica a continuación, este ámbito no es exclusivo, y muchos productos incluyen también funcionalidades propias de otros alcances

PROBLEMA

Los productos de las categorías seleccionadas para este monográfico están orientados en particular a la Seguridad en las redes si bien dada la diversidad de productos que existen en el mercado, como se explica a continuación, este ámbito no es exclusivo, y muchos productos incluyen también funcionalidades propias de otros alcances.

OBJETIVOS

Generales

Mantener nuestros datos lo mas seguro osible pero entender que nunca estarán un 100% asegurados.

Específicos

- Investigar cuales son las herramientas y productos que mejor nos vienen para este comentido
- Entender el de cada una de las herramientas

MARCO TEORICO

Este tipo de productos está destinado a proteger los sistemas y dispositivos conectados a una red. Permiten establecer un perímetro de seguridad y garantizar las comunicaciones seguras para evitar accesos no autorizados y ataques procedentes de redes externas y de Internet. Esta categoría agrupa a productos que aseguran que las comunicaciones hacia y desde la red, corporativa o doméstica, cumplen las políticas de seguridad establecidas. Para ello rastrean y controlan las comunicaciones, bloqueando el tráfico, detectando comportamientos anómalos y ataques, y evitando intrusiones no autorizadas. Funcionalmente establecen una política de seguridad entre una red segura y otra insegura (Internet) y establecen los servicios que serán accesibles desde el exterior y a los que se puede acceder desde el interior. También se integran en esta categoría las herramientas que permiten extender la red corporativa a entornos distantes (sedes remotas, oficinas) creando enlaces de comunicación seguros. En general son herramientas destinadas a crear un perímetro de seguridad en la red de cualquier organización.

Cortafuegos de nivel de red que se caracterizan por controlar las comunicaciones entre redes a nivel de «capa de red». Implementan en tiempo real políticas de seguridad entre redes, estableciendo diferentes niveles de confianza. Dentro de esta subcategoría están los routers o enrutadores con funcionalidad de filtrado de paquetes. Cortafuegos de nivel de aplicación que operan por encima de la capa de red, a «nivel de aplicación» y son capaces de controlar protocolos específicos y aplicaciones, por ejemplo los cortafuegos para mensajería instantánea o de aplicaciones web y P2P (del inglés Peer to Peer). Dentro de este tipo se incluyen los cortafuegos-proxy (filtran protocolos de nivel de aplicación HTTP, FTP, SMTP,..). Dentro de esta subcategoría están los Gateways y Proxys a nivel de aplicación. Otra forma de clasificarlos es según su ámbito de protección, es decir, si están destinados a proteger un puesto de trabajo o toda una organización: Cortafuegos personales para uso particular, en un ordenador personal o en un puesto de trabajo que generalmente vienen incorporados a los Sistemas Operativos. Cortafuegos corporativos pensados para la protección completa de la red de una organización. Se diferencian de los personales o de puesto de trabajo en la potencia y capacidad de proceso que incorporan, necesaria para controlar y gestionar las miles de conexiones que entran y salen a diario de una red corporativa. Este tipo de cortafuegos puede trabajar tanto a nivel de red como de aplicación. En cuanto a su formato pueden presentarse integrados en software de aplicación, como en el caso de navegadores, formando parte de sistemas operativos, formando parte de dispositivos de red, o como dispositivos
hardware específico o integrado con otras funcionalidades de seguridad. Cortafuegos software que suelen estar incorporados en sistemas operativos y generalmente también los que se distribuyen de forma gratuita (véase INTECOCERT Útiles gratuitos>Cortafuegos). También se puede encontrar en este formato software cortafuegos que incorporan funcionalidad Anti-DoS (del inglés Denial of Service) o Anti-DDoS (del inglés Distributed Denial of Service) que contrarrestan los ataques de

denegación de servicio. Router/Proxy/Gateway - con funcionalidad de cortafuegos: son equipos de red que incorporan funcionalidades propias de cortafuegos y según su funcionalidad son cortafuegos de red o de aplicación. Cortafuegos UTM o Gestión unificada de amenazas (del inglés Unified Thread Management,), consisten en servidores o dispositivos que integran distintas soluciones de seguridad con un único interfaz de gestión. Los UTMs, suelen estar destinados a la protección de redes de pequeño, mediano o gran tamaño. Existen soluciones con funcionalidad de cortafuegos unidas a otras categorías, como antimalware o anti-fraude en este formato. Cortafuegos en formato appliance: el término appliance se refiere a plataformas hardware diseñadas con una funcionalidad específica; en el caso de appliances de seguridad esta funcionalidad suele estar destinada a la protección del correo electrónico, la navegación o ambas, pero no disponen necesariamente de gestión También en esta categoría se incluyen otro tipo de productos: Redes privadas virtuales o VPNs (del inglés Virtual Private Network) que permiten extender el perímetro seguro de la organización interconectando sedes y oficinas remotas o usuarios distantes, situados en distintas localizaciones geográficas, mediante la creación de túneles cifrados a través de Internet y utilizando técnicas de traducción de direcciones. Sistemas de prevención y detección de intrusiones IPS/ IDS (del inglés Intrusion Prevention System / Intrusion Detection System) que llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente. Son herramientas utilizadas para detectar y prevenir accesos no autorizados a un equipo o a una red, es decir hay IPS/IDS de equipo y de red, ambos monitorizan el tráfico para determinar y prevenir comportamientos sospechosos. Se integran con frecuencia con cortafuegos que realizan la función de bloquear el tráfico sospechoso. Filtro de contenidos: son herramientas para controlar, restringir y limitar el acceso a contenidos web. Sirven para configurar condiciones en los accesos a Internet a través de navegadores. En esta categoría están las herramientas de control parental que evitan que los menores accedan a páginas no adecuadas a su edad.

CONCLUSIONES

Ejemplos de este nivel de dependencia son tiendas en línea, servicios financieros, servicios de transporte de viajeros y mercancías, asociaciones, franquicias de cadenas comerciales, etc. cuyos procesos de negocio se basan en redes TIC externas con otras empresas (proveedores, distribuidores.

En conclusión contar con la mayoría de estas herramientas nos mucha seguridad a la hora de confiar que nuestros datos estén fielmente asegurados.

Referencias

Concepto.com
https://www.incibe.es/extfrontinteco/img/File/demostrador/monografico_catalogo_seguridad_perimetral.pdf