UNIVERSITAT POLITÈCNICA DE VALÈNCIA

CAMPUS D'ALCOI

Configuración básica de un cortafuegos para PYMES

MEMORIA PRESENTADA POR:

Miguel Catalá Ramirez

GRADO DE INGENIERÍA INFORMÁTICA

Tutor: Carlos Sastre Mengual

Co-Tutor: Pau Micó Tormo

Convocatoria de defensa: Alcoy, Junio de 2016

Resumen

Este trabajo ha sido propuesto por Carlos Sastre Mengual (tutor del proyecto) y Pau Micó Tormo (co-tutor), ambos Profesores en Informática en la Universidad Politécnica de Valencia - Campus Alcoy.

El propósito del siguiente trabajo es ayudar en la elección de un cortafuegos adecuado y su posterior configuración en una PYME, así como intentar ayudar a comprender por qué es tan importante la utilización de un cortafuegos para la protección de los datos de una empresa.

El trabajo consta de dos partes, una primera que hace referencia al estudio de los sistemas actuales para llevar a cabo la securización a nivel perimetral de una empresa, y posteriormente en una segunda parte se realizará la implementación de la solución elegida (firewall ASA de CISCO), donde se configurarán tres zonas típicas en una PYME (Inside, Outside y DMZ).

Tabla de contenidos

Tabla de Imágenes

Acrónimos

- **PYME**: Pequeña y Mediana Empresa.
- **UTM**: Unified Threat Management - Gestión unificada de amenazas.
- **NGFW**: Nueva generación de firewalls.
- **IPS**: Sistema de prevención de intrusiones.
- **NGIPS**: Nueva generación de sistema de prevención de intrusiones.
- **VPN**: Virtual Private Network.
- **VLAN**: Virtual Local Area Network.
- **NAT**: Network Address Translation.
- **DMZ**: DeMilitarized Zone.
- **ACL**: Access Control List.
- **OSI**: Open Systems Interconnect.
- **TCP**: Transmission Control Protocol.
- **UDP**: User Datagram Protocol.
- **ICMP**: Internet Control Message Protocol.
- **HTTP:** HyperText Transfer Protocol.
- **HTTPS:** HyperText Transfer Protocol Secure.
- **DNS:** Domain Name System.
- **FTP:** File Transfer Protocol.
- **LDAP:** Lightweight Directory Access Protocol.
- **SMTP:** Simple Mail Transfer Protocol.
- **CLI**: Command-Line Interface.
- **ASDM**: Adaptive Security Device Manager.

1. Motivación y objetivos

Internet se creó sólo con unos 4.000 millones de direcciones IP, es decir, 2 elevado a 32 (IPv4). Hoy en día están aumentando tanto los usuarios de internet que estas direcciones IPv4 se están agotando y se está implantando IPv6 para aumentar el número de direcciones IP.

Entre esos 4.000 millones de dispositivos se esconden multitud de personas que crean códigos maliciosos con “malas intenciones”.

Antiguamente la motivación de los creadores de estos códigos maliciosos era mayoritariamente por el reconocimiento público, pero hoy en día, la tendencia actual de estos códigos maliciosos suelen tener un objetivo lucrativo.

Existen grupos mafiosos organizados con un único fin económico que se dedican a infectar los equipos de los usuarios o empresas, centrándose principalmente en el robo de datos y credenciales bancarias. Estos son los 7 ataques más grandes en la historia enumerados por número de usuarios afectados:

1. **El gran hack de EE.UU.: 160 millones de usuarios**
   No tiene nombre oficial porque no afectó a una sola compañía, sino a una larga lista de ellas. El ataque se prolongó durante siete años desde 2005, y robó los datos de tarjetas bancarias de 160 millones de clientes.

2. **Adobe: 152 millones de usuarios**
   En octubre de 2013, Adobe reconoció haber sufrido un robo de cuentas bancarias a gran escala.

3. **eBay: 145 millones de usuarios**
   Este ataque obligó a cambiar sus contraseñas a 145 millones de personas. Aún no se ha podido calcular el volumen de la información filtrada.

4. **Heartland: 130 millones de usuarios**

   Este ataque se llevó datos de 130 millones de tarjetas de débito y crédito de la multinacional de pagos Heartland Payment Systems. Ocurrió en 2008, pero no se hizo público hasta mayo de 2009.

5. **TJX: 94 millones de usuarios**

   En enero de 2007, TJX hizo público un ataque informático que puso en peligro los datos bancarios de 94 millones de clientes entre sus cadenas de tiendas Marshals, Maxx y T.J.

6. **AOL: 92 millones de usuarios**

   Este ataque comenzó desde dentro en 2004. Un ingeniero de la compañía que había sido despedido utilizó sus conocimientos de la empresa para infiltrarse en la red interna de AOL, y robar la lista con los correos de sus 92 millones de usuarios. Después vendió la lista online a un grupo de spammers.

7. **Sony PlayStation Network: 77 millones de usuarios**

   El ataque robó información de las cuentas de 77 millones de usuarios de los servicios PlayStation en todo el mundo. Tuvo que compensar a los usuarios y recibió varias sanciones en países como Reino Unido.

Uno de los últimos ataques en España en 2016 ocurrió contra un sindicato de los Mossos d´Escuadra. Los atacantes filtraron información personal y bancaria de más de 5.600 agentes de policía.

Cada vez son más sofisticados los ataques y nunca estaremos cien por cien protegidos, los atacantes siempre buscarán un modo de acceder a la información.

Por ello, es necesario que los usuarios y empresas sean conscientes de la importancia de utilizar herramientas de seguridad como cortafuegos, antivirus, antiespías, etc., para intentar protegerse al máximo de estos ataques.

Objetivos

El presente trabajo de fin de grado tiene como objetivo principal realizar la configuración de un cortafuegos hardware en el entorno de una PYME, para aumentar la seguridad y conocer la importancia de la protección de los datos.

Se realizarán comparativas entre los diferentes tipos de implementación que existen, donde se llegará a la conclusión de que la mejor opción es utilizar un cortafuegos hardware mediante los dispositivos UTM, siendo nuestra mejor opción en el mercado de hoy en día el dispositivo UTM de CISCO, comparándolo con sus principales competidores.

Listado de objetivos:

- Reconocer la importancia de los cortafuegos.
- Conocer cómo trabaja un cortafuegos y sus formas de implementación.
- Llegar a la conclusión de que se necesita un cortafuegos hardware para mayor protección.
- Analizar y seleccionar un cortafuegos hardware UTM adecuado, de entre las diferentes opciones que existen en el mercado actual.
- Realizar la implementación de la solución en una PYME.

2. Introducción

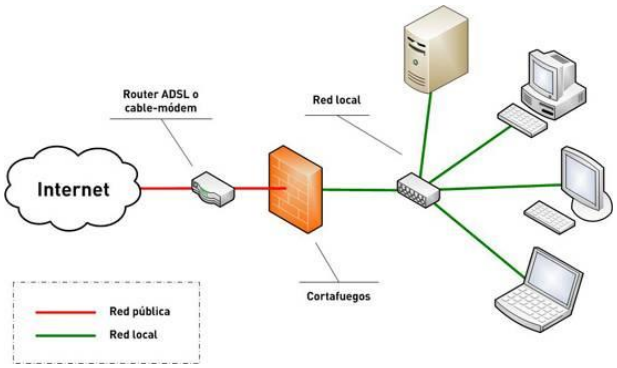

Imagen 1: Cortafuegos

2.1. ¿Qué es un cortafuegos (Firewall)?

El cortafuegos, también conocido como firewall, es nuestra primera línea de defensa ante los ataques provenientes de internet. Examina todos los mensajes que entran y salen de nuestra red, bloqueando los que no cumplen los criterios de seguridad establecidos, también conocidos como políticas (ACLs, IPTables).

Los cortafuegos se sitúan dentro de nuestra red, para separar la red interna de la red externa (internet). Además, también es frecuente conectar al cortafuegos una tercera red, llamada "zona desmilitarizada" o DMZ, en la que se ubican los servidores que serán accesibles desde la red externa.

Un cortafuegos **NO es un antivirus,** no elimina problemas de virus, así que es recomendable utilizarlo junto con un buen antivirus y tener actualizado nuestro sistema operativo para aumentar nuestra seguridad y protección.

2.1.1. Funciones principales de un cortafuegos

El modelo de International Standards Organization (ISO) Open Systems Interconnect (OSI) define siete capas, donde cada una de ellas proporciona los servicios que las capas superiores requieren de ellas.

Imagen 2: Modelo OSI

Filtrado de paquetes de datos

Se analiza el tráfico en la capa 3 (Nivel de Red), aunque a veces tiene en cuenta características generadas en las capas 1, 2 y 3.

Para decidir si un paquete es válido o no, influyen los siguientes elementos de decisión:

- Dirección de origen del paquete (Capa 3).
- Dirección del host de destino (Capa 3).
- Protocolo utilizado para la comunicación, normalmente Ethernet o IP (Capas 2 y 3).
- Tipo de trafico: TCP, UDP o ICMP (Capas 3 y 4).
- Puertos de origen y destino de la sesión (Capa 4).
- El interfaz físico del firewall de entrada y salida (Capa 1).

Filtrado por aplicación

Trabajan en la capa 7 (Nivel de Aplicación), suelen prestar servicios de autenticación de usuarios y servicios de Proxy.

Un Proxy es un servicio que permite controlar el tráfico, controlar el acceso y registrar detalladamente los sucesos de un protocolo determinado (HTTP, DNS, FTP, etc.).

Los servicios o agentes típicos que suelen utilizar estos cortafuegos son: HTTP, HTTPS, DNS, Finger, FTP, LDAP, NMTP, SMTP y Telnet.

2.1.2. Políticas de un cortafuegos

Existen dos tipos de políticas en un cortafuegos:

- **Política restrictiva:** Se deniega todo el tráfico excepto el que esta explícitamente permitido.

- **Política permisiva:** Se permite todo el tráfico excepto el que esta explícitamente denegado.

La política restrictiva es la más segura ya que debemos permitir el tráfico explícitamente y es difícil que permitamos tráfico peligroso por error.

2.1.3. Bastión y contención

Una configuración más segura y óptima es utilizar dos cortafuegos diferentes para implementar dos barreras de protección, de manera que si un atacante consigue burlar la seguridad del primer cortafuegos (bastión), por causa de algún agujero de seguridad del sistema operativo, el segundo cortafuegos (contención) al disponer un sistema operativo diferente, cortará el ataque.

2.2. Implementación

Los cortafuegos pueden ser implementados de tres formas:

- Software
- Hardware
- Hardware/Software

Los cortafuegos Hardware y Hardware/Software ofrecen protección perimetral, cuando se mencione a los cortafuegos perimetrales se hará referencia a estos dos tipos de implementación.

En primer lugar se hará una elección entre cortafuegos software o perimetral, posteriormente se detallarán los dos tipos de cortafuegos perimetral para realizar otra selección entre ellos.

2.2.1. Cortafuegos perimetral vs. Software

Cortafuegos perimetral

Los cortafuegos perimetrales son dispositivos utilizados para controlar las conexiones de toda una red local, este cortafuegos se sitúa entre internet y nuestra red local y proporcionan una fuerte protección contra la gran mayoría de formas de ataque provenientes de internet.

Son llamados cortafuegos perimetrales, ya que protegen todos los equipos situados en un perímetro (nuestra red local) y suelen unificar varios servicios en un solo dispositivo, lo cual ahorra espacio y centraliza las configuraciones.

Cortafuegos software

Son los más utilizados por los usuarios particulares. Es una aplicación que se instala en los equipos que queremos proteger.

A comparación del cortafuegos perimetral donde solo debemos configurar un único cortafuegos, en el cortafuegos software, al estar instalado en cada equipo de nuestra red, debemos configurar cada uno de estos equipos.

Su principal problema suele estar en los agujeros de seguridad del sistema operativo del equipo, que al estar basado en software puede ser atacado.

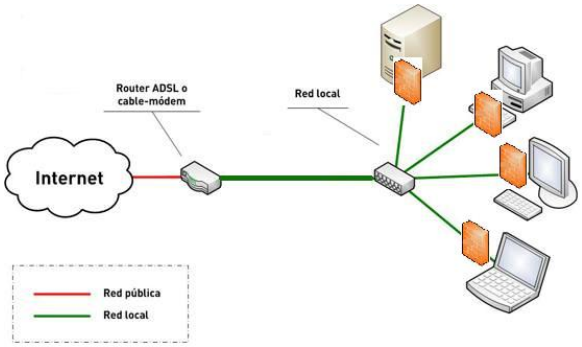

Imagen 3: Ubicación cortafuegos software

Ejemplos Software:

El más utilizado es el cortafuegos que ya suele incorporar cualquier sistema operativo Windows. Además, tenemos otras opciones líderes en el mercado como:

- ZoneAlarm
- Comodo

Son gratuitas, pero también disponen de versión de pago con funciones avanzadas.

Elección Cortafuegos perimetral o Software

Para una PYME, la mejor opción es adquirir un cortafuegos perimetral, ya que nuestra empresa puede disponer de una gran cantidad de equipos y con un cortafuegos perimetral centralizamos la configuración de todos ellos en un solo dispositivo.

Sin este tipo de cortafuegos, si tenemos 150 equipos en nuestra empresa debemos configurar uno a uno estos equipos por separado, lo que nos resultaría bastante más costoso y difícil de mantener.

Es recomendable la utilización de ambos juntos (perimetral + software) a modo de bastión y contención, para mayor protección de nuestra red, o si nuestro presupuesto lo permite podemos utilizar dos cortafuegos perimetrales diferentes (perimetral + perimetral).

2.2.2. Tipos de cortafuegos perimetrales

Los cortafuegos perimetrales pueden ser:

- Hardware/Software (Equipo dedicado LINUX-UNIX)
- Hardware (Dispositivos UTM)

Se realizará una comparativa de los diferentes tipos para seleccionar el más adecuado para nuestra PYME.

Hardware/Software (PC Linux)

Unas de las posibles soluciones, aunque más costosa de implementar y necesita un alto nivel de conocimientos, es utilizar un ordenador con un sistema operativo Linux-Unix instalado y al menos dos tarjetas de red, donde mediante IPtables (ACLs) podemos configurar un cortafuegos 100% funcional y seguro.

En él se pueden implementar los mismos servicios que ofrece un dispositivo UTM como veremos en el siguiente punto.

Ventajas:

- Precio.
- Bien configurado = alta seguridad.

Inconvenientes:

- Tiempo de configuración y pruebas.
- Cuello de botella.
- Posibles fallos en disco duro, memoria, Sistema Operativo…
- Tamaño del equipo.
- Consumo energético.
- Soporte

Ejemplos:

Estos son ejemplos de firewalls opensouce:

- ClearOS, IPcop, Zentyal, PFsense, Monowall y Smoothwall express.

Hardware (Dispositivos UTM)

UTM viene de las siglas en ingles de: Unified Thread Management (Gestión unificada de amenazas). Son dispositivos reducidos, que unifican varios sistemas independientes en uno único centralizando su configuración. Estos cortafuegos además de la función de firewall también suelen dar servicio para:

- **VPN** (para hacer túneles o redes privadas)
- **Antispam** (para evitar los correos spam)
- **Antiphishing** (para evitar el robo de información)
- **Antispyware**
- **Filtrado de contenidos** (para el bloqueo de sitios web, correo, etc…)
- **Antivirus** de perímetro
- **IDS/IPS (**Detección/Prevención de Intrusos)

Tienen un coste de mantenimiento al necesitar una licencia, normalmente anual en la que pagamos por un servicio de soporte y mantenimiento, donde hay un equipo de empleados encargados de buscar agujeros de seguridad y mejorar los dispositivos ofreciendo actualizaciones de software.

Ventajas:

- Tamaño y robustez.
- Servicio técnico.
- Consumo energético.
- Escalabilidad

Inconvenientes:

- Precio de dispositivo.

Ejemplos: (Más adelante se realiza una comparativa de los dos más implantados)

- Cisco ASA, Juniper, Check Point, Fortinet, Paloalto…

Elección de solución perimetral (UTM vs. Linux)

En cuanto a protección pueden llegar a estar al mismo nivel si los configuramos correctamente.

Una posible elección para una microempresa o para uso personal, donde las conexiones de usuarios son reducidas, sería implementar un PC con un sistema operativo Linux-Unix y su configuración mediante IPTables.

En cambio, para una PYME donde ya toma más importancia la seguridad y protección de datos de los clientes, lo más recomendable es utilizar un firewall UTM.

Las diferencias más significativas entre ambos son las siguientes:

- **Tiempo de mantenimiento y configuración:** En un PC Linux firewall, es mucho más complicado de configurar correctamente, necesitamos una persona con alto nivel de conocimiento encargada día a día de su mantenimiento (Actualizaciones, pruebas, reparaciones…).
- **Tamaño:** Un firewall UTM tiene un tamaño más reducido.
- **Robustez:** el PC es más susceptible a tener fallos (Disco duro, ram, fuente de alimentación…), en cambio el UTM es más robusto.
- **Consumo energético:** El PC tiene un consumo energético elevado (40 – 60 W) a comparación de un firewall UTM (10 – 20 W).
- **Rendimiento:** Si existe un alto número de conexiones, el tráfico que tiene que analizar el firewall puede hacer un cuello de botella en el PC Linux.
- **Soporte técnico:** Un dispositivo UTM, al ser un equipo dedicado únicamente a la seguridad, dispone de un equipo de trabajadores encargado día a día de buscar y corregir fallos o agujeros de seguridad, para dar soporte y actualización a sus dispositivos. En cambio un PC Linux-Unix al ser una comunidad abierta, nadie está obligado a prestar ayuda o soporte, hay que buscar soluciones si es que alguien las ha publicado y perder mucho tiempo en pruebas.

2.3.Estudio de mercado UTM

Ya hemos llegado a la conclusión de que necesitamos un firewall UTM para mejorar la seguridad de nuestra empresa y en el mercado hay varias compañías que comercializan estos tipos de dispositivos UTM, pero para saber cuáles son las mejores del mercado nos podemos ayudar observando los resultados de las pruebas que realiza anualmente el famoso laboratorio NSS Labs y los análisis de mercado que actualiza trimestralmente IDC.

Imagen 4: NSS Labs y IDC

IDC (International Data Corporation), es el principal proveedor mundial de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumo. IDC ayuda a los profesionales en las decisiones sobre compra de tecnología y estrategia de negocio.

Ha realizado un estudio de mercado titulado *Worldwide Quarterly Security Appliance Track Study*, el cual va actualizando trimestralmente para saber cuáles son los dispositivos UTM más implantados en las empresas de todo el mundo.

En estos resultados se cita al cortafuegos de Cisco ASA como el firewall más implementado del mundo con un 14,7% del mercado, seguido por Checkpoint en segunda posición con un 12,9%, tercera posición para PaloAlto con un 9,8%.

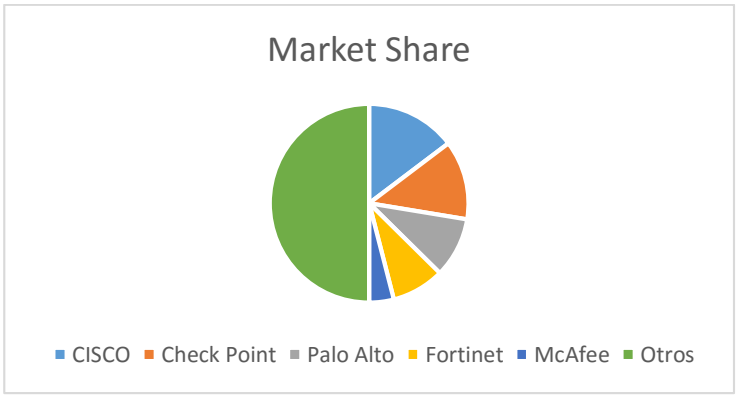

Imagen 5: Estudio de IDC

Nos centraremos en los dos dispositivos más implantados en el mundo (CISCO y CheckPoint), ya que siendo un estudio que se actualiza trimestralmente, si los dos primeros siguen siendo los más implantados, es de suponer que son unas buenas opciones de seguridad para nuestra PYME.

NSS Labs, es la organización líder en pruebas a productos de seguridad, realiza informes de pruebas muy valorados por los profesionales de seguridad.

En sus informes sobre firewalls UTM siempre ponen a prueba los mejores firewalls del mercado, en los que siempre se sitúan en la parte alta de los resultados de las pruebas, marcas como Cisco, CheckPoint, Juniper, Paloalto o Fortinet.

Nuestras dos opciones a comparar CISCO y CheckPoint, en los resultados de estas pruebas ambos superan el 99% de efectividad en la detección y bloqueo de amenazas, con lo cual ambos siguen siendo dos grandes opciones de seguridad para nuestra PYME.

2.4.CISCO Vs. CheckPoint

Ambos dispositivos UTM son excelentes opciones de seguridad, pero para decantarnos por uno u otro dispositivo, vamos a comparar los servicios que ofrecen ambos.

Imagen 6: Logos de Cisco y Checkpoint

2.4.1. CheckPoint

Check Point Software Technologies Ltd. es un proveedor global de soluciones de seguridad en redes desde 1993. Sus productos más conocidos son los cortafuegos y los sistemas VPN, Check Point fue pionero en la industria de los cortafuegos con la primera generación de firewalls al incorporar una tecnología patentada de inspección de estado. Desde 1993 hasta hoy, la compañía ha desarrollado, comercializado y soportado una amplia gama de productos que cubren todo tipo de aspectos de seguridad de IT, incluyendo seguridad de red, seguridad endpoint, seguridad de datos y gestión de seguridad.

CheckPoint cuenta con certificaciones propias, como:

- CPCS - Check Point Certified Specialist
- CCSA - Check Point Certified Security Administrator
- CCSE - Check Point Certified Security Expert
- CCSE+ - Check Point Certified Security Expert Plus
- CCMSE - Check Point Certified Managed Security Expert
- CCMA - Check Point Certified Master Architect

Aunque en España son algo menos conocidas que las certificaciones de Cisco.

Check Point 700 Appliances

Checkpoint dispone de una amplia gama de cortafuegos UTM capaces de proteger desde una pequeña empresa hasta un Data Center. La familia de appliances UTM de Check Point incluye las Series 600, 700, 1100, 2200 y 4000.

Imagen 7: Familia dispositivos Checkpoint

Los dispositivos de la familia de gama más baja (600 Appliances) están diseñados para pequeñas empresas con hasta 10 usuarios, nos centraremos en la familia 700 Appliances que está diseñada para pequeñas y medianas empresas.

Estos dispositivos ofrecen las funciones de:

- Firewall
- VPN
- IPS
- Control de aplicaciones
- Filtrado de URL
- Antivirus
- Anti-spam

2.4.2. CISCO

CISCO es líder global en redes y comunicaciones, su tecnología está implantada en la gran mayoría de empresas grandes, medianas y pequeñas de todo el mundo.

Principalmente está dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones como:

- Routers, switches y hubs.
- Cortafuegos y VPN.
- Productos de telefonía IP.
- Software de gestión de red como
- Equipos para redes de área de almacenamiento.

Además dispone de uno de los mejores servicios técnicos, ya que CISCO tiene una alianza con instituciones universitarias en 128 países, para formar a los estudiantes en sus conocidas y valoradas certificaciones de CISCO NETWORKING ACADEMY:

- CCDA (Cisco Certified Design Associate)
- CCDP (Cisco Certified Design Professional)
- CCIE (Cisco Certified Internetwork Expert)
- CCIP (Cisco Certified Internetwork Professional)
- CCNA (Cisco Certified Network Associate)
- CCNP (Cisco Certified Network Professional)
- CCSP (Cisco Certified Security Professional)

Otra ventaja de Cisco son sus conocidas herramientas de emulación y configuración de redes, **Packet Tracer** y **GNS3,** que son de gran ayuda para experimentar y simular redes, comprobando su correcto funcionamiento antes de implantarlo físicamente en nuestra empresa.

Cisco ASA 5500-X with FirePOWER Services

Cisco dispone de una gama de firewalls de última generación que dependiendo el modelo, puede protegernos desde una pequeña empresa o sucursal, a una empresa proveedora de servicios o Data Center.

Dispone hoy en día de 16 modelos diferentes, de los cuales 10 de ellos pertenecen a la gama Cisco ASA 5500-X with FirePOWER Services, y los otros 6 modelos pertenecen a la gama Cisco ASA 5585-X with FirePOWER Services.

Imagen 8: Familia ASA de Cisco

Nos centraremos en la gama Cisco ASA 5500-X with FirePOWER Services, que son los dispositivos más económicos de Cisco y disponen de funciones de protección frente a amenazas, como:

- Firewall
- Control de aplicaciones
- NGIPS
- Filtrado de URL
- Protección frente a malware avanzado (AMP)
- VPN.

Estos firewalls proporcionan un conocimiento contextual y controles dinámicos que ayudan a evaluar automáticamente las amenazas, hacer correlaciones inteligentes y optimizar la defensa para proteger todas las redes.

2.4.3. Elección CISCO Vs. CheckPoint

CISCO es la mejor solución para la protección firewall de nuestra PYME hoy en día, además de ser el dispositivo UTM más implantado en las empresas de todo el mundo, cosa que indica que es una gran elección, nos ofrece mayores ventajas en comparación a CheckPoint como:

- Innovación (NGIPS – Nueva generación de IPS).
- Herramientas de simulación propias (GNS3 y Packet Tracer).
- Mayor calidad en servicio de soporte (CCNA).
- Estabilidad.

Al juntar NGIPS y AMP se proporciona una defensa integrada frente a las amenazas en todas las etapas de los ataques: antes, durante y después.

NGIPS

Utilizado durante el ataque para ***Detectar – Bloquear – Defender.***

Sistema de Prevención de Intrusiones de Generación Avanzada o (singla en inglés de Next Generation Intrusion Prevent System).

El objetivo del Intrusion Prevention System (IPS) es el de ser desplegado a través en nuestra red para detectar, clasificar y detener amenazas. IPS identifica y detiene tráfico malicioso a través del uso de firmas, que se usan para detectar actividades.

NGIPS es una mejora de IPS con la habilidad de identificar aplicaciones y usuarios, en la que se detectan las amenazas mediante reconocimiento de contexto en tiempo real.

Ventajas del NGIPS:

- Detección de amenazas y capacidad de interrumpir violaciones en tiempo real.
- Mejor visibilidad de dispositivos, aplicaciones, usuarios y comunicaciones.
- Permite correlacionar eventos de diferentes orígenes para identificar hosts posiblemente comprometidos.
- Una seguridad amplia que proporciona tanto protección avanzada contra malware, como visibilidad y control de aplicaciones.

AMP

Utilizado después del ataque para ***Examinar – Contener – Remediar.***

Cisco Advanced Malware Protection, es la protección frente a malware avanzado.

Proporciona capacidad de detección, análisis, detención y remediación de malware y de amenazas que han pasado desapercibidas para las otras capas de seguridad.

AMP es un motor de minería de datos que identifica archivos maliciosos mediante la extracción de metadatos, para determinar el riesgo que suponen, basándose no en firmas como IPS, sino en el comportamiento.

El filtrado de URL

El filtrado de URL se basa en la reputación de las webs, bloquea las webs de alto riesgo. Cisco analiza las URL y asigna una puntuación de reputación a cada web, lo que permite a los usuarios evitar las direcciones web de alto riesgo.

VPN

Los cortafuegos ASA proporcionan IPsec/SSL VPN.

Estas redes privadas virtuales (VPN) se utilizan para conectar de manera segura oficinas y usuarios a nuestra empresa, cifrando la conexión de datos mediante Seguridad IP cifrada (IPSec) o túneles VPN Secure Sockets Layer (SSL).

Cisco dispone de la aplicación Cisco AnyConnect 4.0 que permite crear y gestionar VPN de manera segura tanto para ordenadores como para smartphones Androd o iOS.

2.5. Elección del modelo de CISCO ASA

Cisco ha renovado su gama de cortafuegos durante el año 2015, hasta entonces su dispositivo más económico era el firewall ASA 5505, que era un dispositivo muy vendido y utilizado. Ahora lo sustituye en el mercado su nuevo dispositivo ASA 5506-X que utiliza una configuración idéntica al dispositivo anterior, pero mejorando en todos los sentidos.

En cuanto a precios, la mejor opción es buscar un Partner de nuestra zona y adquirir un dispositivo nuevo y con la seguridad de ser el "oficial" junto a su garantía, lo podemos encontrar entre 500 – 700 €.

Todos los modelos disponen del mismo software y el mismo nivel de protección, sus principales diferencias se basan en:

- Trafico máximo (300 Mbps).
- Número de conexiones por segundo que pueden proteger (5.000cps)

- Número de conexiones máximas (20.000)
- Número de clientes VPN (50)
- Número de clientes VPN IPSec (10)
- Numero de VLANS (5)

El resto de diferencias son menos significativas, como los puertos Fast-ethernet o Gigabit-ethernet, numero de puertos RJ-45, Slot de expansión, memoria…

Depende de las necesidades y el tamaño de la empresa nos decantaremos por uno u otro modelo. Por lo tanto, nuestra elección para una PYME donde tendremos menos de 250 empleados, es el firewall ASA 5506-X.

3. Desarrollo

3.1. Conocimientos previos

Los dispositivos CISCO utilizan un Sistema Operativo llamado **Cisco IOS** (Internetworks Operating System) y se configuran mediante la interfaz de línea de comandos (IOS CLI).

Necesitamos tener conocimientos básicos de configuración de dispositivos CISCO. Lo ideal sería disponer al menos de la certificación básica CCNA de CISCO, o tener practica configurando estos dispositivos.

Además de controlar los comandos básicos de configuración, ACL, NAT, rutas por defecto… necesitamos saber diferenciar entre las tres zonas que vamos a configurar en nuestro firewall para la red de nuestra PYME:

- **Inside:** o LAN, es nuestra red interna y donde tendremos el máximo nivel de seguridad, con lo que aquí situaremos los servidores de datos importantes y todos los equipos de nuestra empresa.

- **Outside:** Será el trafico proveniente del exterior (internet).

- **DMZ:** (De-Militarized Zone) En esta zona tendremos los servidores que queremos que sean accesibles desde internet y estén instalados físicamente en nuestra red. Con la DMZ se crea una subred independiente y en caso de que alguien vulnere la seguridad de un servidor, no pueda acceder a la LAN.

El firewall ASA trabaja con niveles de seguridad (0-100), automáticamente le asignara un nivel 0 a la interfaz outside, y un nivel 100 a la interfaz inside. A la DMZ le asignaremos manualmente, por ejemplo un nivel 50.

3.2. Guía de configuración básica

Configuración Realizada en un modelo ASA 5505, esta configuración es aplicable a cualquier dispositivo de la gama de Cisco.

3.1.1. Contenido de la caja

El firewall ASA 5505 incluye en la compra 2 cables Ethernet, 1 cable para la administración desde consola, un adaptador con cable de alimentación y documentación en CD y en papel.

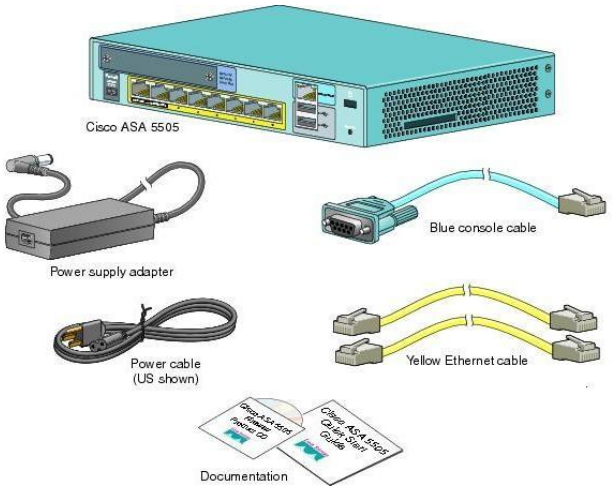

Imagen 9: Contenido caja ASA

Conectamos el ASA a la corriente y los leds frontales nos indicarán si el dispositivo esta encendido iluminando almenos el led power.

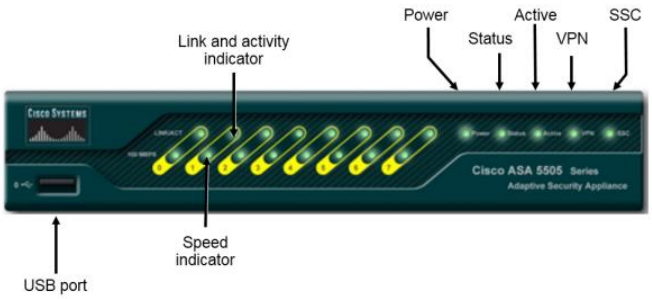

Imagen 10: Parte delantera dispositivo ASA 5505

Si ha adquirido el dispositivo de segunda mano, vamos a resetearlo de fábrica para eliminar las posibles configuraciones que tuviera el anterior usuario.

(PRECAUCIÓN, esto borrará toda la configuración del dispositivo)

Buscamos el botón reset en la esquina inferior derecha del panel trasero del ASA, con la ayuda de un clip, alfiler, bolígrafo… presionaremos el botón reset manteniéndolo pulsado durante unos 20-30 segundos, los leds del panel frontal parpadearán y ya dispondremos del dispositivo limpio de configuraciones y listo para empezar nuestra configuración desde 0.

En caso de haber adquirido el dispositivo nuevo, no es necesario hacer un reset ya que en esta guía vamos a realizar la configuración desde el dispositivo limpio de fábrica.

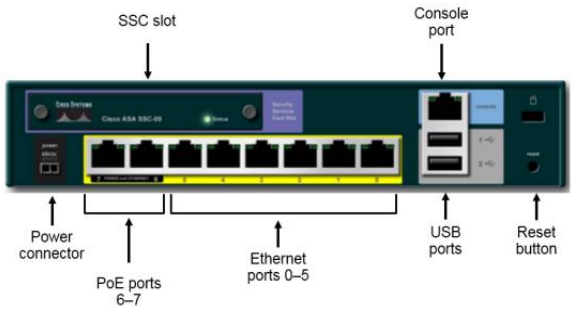

Imagen 11: Parte trasera dispositivo ASA 5505

Por defecto, el ASA viene configurado con el puerto Ethernet 0 para OUTSIDE y el resto de puertos Ethernet (1-7) para INSIDE.

Esta configuración la podemos cambiar y utilizar el puerto que queramos para cada zona (inside, outside y dmz), pero en esta guía utilizaré los puertos 0 y 1 por defecto y el puerto 2 lo configuraremos para la DMZ con los que nos quedará:

Puerto Ethernet 0 – OUTSIDE

Puerto Ethernet 1 – INSIDE

Puerto Ethernet 2 – DMZ

3.1.2. Topología

Esta es la topología básica que utilizaré.

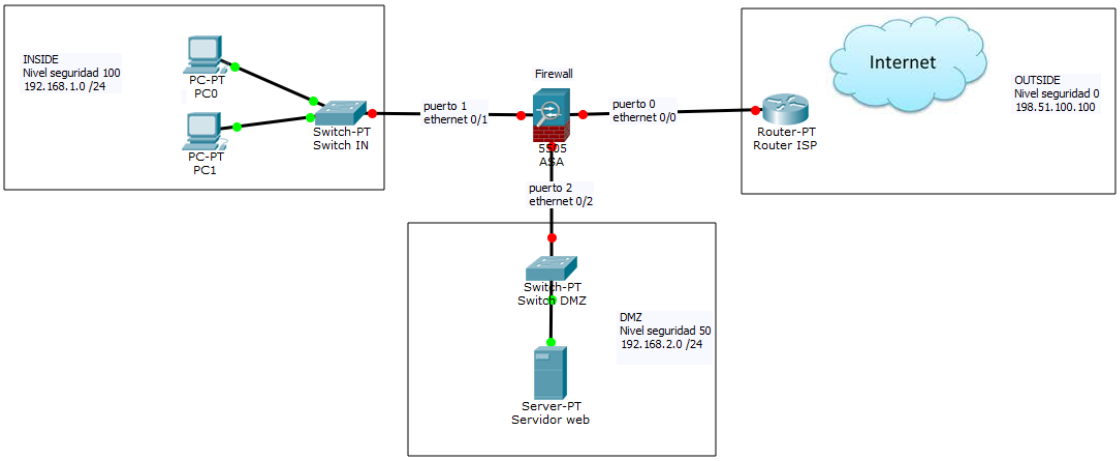

Imagen 12: Topología de red utilizada

OUTSIDE – irá del puerto 0 del firewall a nuestro router que sale a internet (router de nuestra compañía de internet o ISP). Un nivel de seguridad 0 ya que es la red con la mínima seguridad.

Vamos a suponer que nuestro ISP nos da la IP 198.51.100.100.

INSIDE – irá del puerto 1 del firewall a un switch donde tendremos los equipos de nuestra empresa con un nivel de máxima seguridad 100 y utilizaremos una dirección de red 192.168.1.0 /24.

DMZ – irá del puerto 2 del firewall a un switch donde tendremos el servidor web de nuestra empresa, el cual queremos que sea accesible desde internet por otros usuarios externos a la empresa.

Configuraremos un nivel de seguridad 50 y utilizaremos una dirección de red 192.168.2.0 /24.

3.1.3. Abrir terminal ASA

Conectamos el cable de consola que viene con el dispositivo en la caja, es un cable azul con un conector RJ-45 que va al puerto de consola del firewall y el otro extremo es una conexión serie que conectaremos a nuestro pc.

Necesitaremos el programa gratuito Putty (http://www.putty.org/), lo abrimos y seleccionamos el tipo de conexión "Serial", automáticamente se cambia el puerto a COM1. Hacemos click en "Open" y se nos abrirá la terminal de nuestro firewall ASA.

NOTA: Desde el administrador de dispositivos podemos comprobar si nos ha detectado el cable como COM1, COM2…

3.1.4. Entrar en modo configuración

Una vez en la terminal del ASA procedemos a configurar:

*Lo escrito en color **azul** será el texto de la terminal que debemos escribir.*

Accedemos a modo administrador

```
ciscoasa> enable
```

El password inicial está en blanco, intro y continuamos

```
Password:
```

Accedemos al modo de configuración global

```
ciscoasa# configure terminal
ciscoasa(config)#
```

3.1.5. Configurar hostname y password

El hostname por defecto en este caso es “ciscoasa”, si queremos modificarlo lo hacemos con el comando hostname.

```
ciscoasa(config)#hostname ASA5505
ASA5505(config)#
```

El password viene vacío por defecto, para añadir un password lo hacemos con el comando:

```
ciscoasa(config)#password [contraseña]
```

3.1.6. Configurar las interfaces y Vlans

Configuramos la VLAN 1 (inside):

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

Configuramos la VLAN 2 (outside):

```
ciscoasa(config)# interface vlan 2
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 198.51.100.100 255.255.255.0
```

Configuramos la VLAN 3 (DMZ):

```
ciscoasa(config)# interface vlan 3
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#nameif DMZ
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)# ip address 192.168.2.1 255.255.255.0
```

3.1.7. Configurar ruta por defecto

Configuramos la ruta por defecto para salir a internet:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

3.1.8. Asignar VLANs a interfaces

Asignamos las interfaces o puertos a las vlans creadas.

La interfaz Ethernet 0/0 a la vlan 2 (viene por defecto):

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 2
```

La interfaz Ethernet 0/1 a la vlan 1 (viene por defecto):

```
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 1
```

La interfaz Ethernet 0/2 a la vlan 3:

```
ciscoasa(config)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 3
```

3.1.9. Activar paquetes ICMP (Ping)

Un ping iniciado en un nivel de seguridad superior llega correctamente a una Vlan con un nivel de seguridad inferior, pero no puede volver ya que de un nivel inferior no se puede realizar conexión con un nivel de seguridad superior.

Para poder realizar estos pings debemos añadir los paquetes ICMP a la lista de inspección de tráfico del firewall.

Si se desea activar la inspección de paquetes ICMP para la realización de pruebas de conectividad entre equipos, debemos de añadir las siguientes líneas:

```
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#service-policy global_policy global
```

3.1.10. Configuración de NAT Dinámico

Configurando el NAT, conseguimos que los hosts internos de la red LAN o de la DMZ puedan salir a internet con una IP pública.

Vamos a crear dos objetos de red para representar las subredes inside y dmz, para aplicar un tipo de NAT dinámico.

```
ciscoasa(config)#object network inside-subnet
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

ciscoasa(config)#object network dmz-subnet
ciscoasa(config-network-object)#subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)#nat (dmz,outside) dynamic interface
```

3.1.11. Configuración de NAT estático (Web Server)

Ahora configuramos el NAT estático para nuestro servidor Web.

Nuestro ISP nos proporcionará una IP pública estática, como por ejemplo la 198.51.100.101, la asignamos a nuestro servidor web (IP interna 192.168.2.10) para que sea accesible desde internet con esta IP Publica.

```
ciscoasa(config)#object network webserver
ciscoasa(config-network-object)#host 192.168.2.10
ciscoasa(config-network-object)#nat (dmz,outside) static
192.51.100.101
```

3.1.12. Creación de ACL para conectar Outside-DMZ

Ahora mismo podemos iniciar una conexión desde la DMZ hacia internet, pero de internet no podemos acceder a la DMZ. Esto necesita de una ACL para su funcionamiento.

Creamos una ACL para que solo se pueda acceder al servidor web de nuestra DMZ utilizando el protocolo TCP por el puerto 80 (web), y asignamos esta ACL a la interfaz outside (accesos desde el exterior).

```
ciscoasa(config)# access-list OUTSIDE-DMZ extended permit tcp any any eq 80
ciscoasa(config)#access-group OUTSIDE-DMZ in interface outside
```

Puertos para ACL más utilizados

Estos son algunos puertos típicos que podemos necesitar abrir:

21 - ftp (el servidor FTP).

22 - ssh (el acceso al shell criptado).

23 - telnet (el acceso al shell no criptado).

25 - smtp (el servidor de correo entrante).

53 - dns (el servidor DNS).

80 - http (servidor web).

110 - pop3 (el acceso a los e-mails).

143 - imap (acceso a los mails).

443 - https (acceso al web criptado).

3.1.13. Activar configuración web (ASDM)

Adaptive Security Device Manager (ASDM) es la interfaz web de configuración del ASA, desde ella se puede realizar cualquier configuración, controlar tráfico, aplicar ACLs, etc.

Por defecto viene desactivada, debemos activarla desde CLI e indicarle desde que red o host se puede acceder a esta interfaz.

```
ciscoasa(config)#http server enable
ciscoasa(config)#http 192.168.1.0 255.255.255.255 inside
```

De esta manera queda activada la interfaz gráfica ASDM del ASA y solo es accesible desde los equipos de nuestra red inside, accediendo desde un navegador web a la dirección IP del frewall (https://192.168.1.1) y descargando el ASDM en nuestra maquina presionando el botón *"Install ASDM Launcher and RUN ASDM"*.

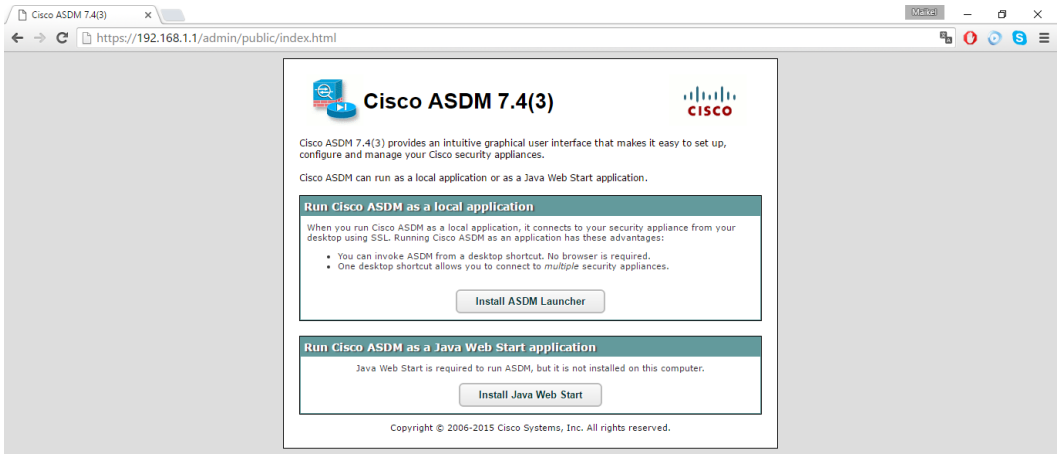

Imagen 13: Interfaz web ASDM

3.1.14. Guardar configuración

Para guardar la configuración modificada, escribimos el comando:

```
ciscoasa(config)#write memory
```

Si no guardamos la configuración, en el próximo reinicio del ASA se borrará.

3.1.15. Copiar configuración (Backup)

Existen varias formas de realizar una copia de seguridad de la configuración del dispositivo ASA.

Utilizaremos el comando *"copy"* para almacenar la configuración almacenada en RAM "running-config" (configuración actual del router) o la configuración almacenada en NVRAM "startup-config" (configuración que se carga al arranque).

```
ciscoasa#copy startup-config ?
```

Esto nos mostrara una lista de las opciones de copia que hay, como ftp, tftp, flash, etc…

En caso de tener un servidor FTP en nuestra red, copiaremos la configuración de la siguiente manera:

```
ciscoasa#copy startup-config ftp
```

Nos preguntará la dirección IP de nuestro servidor FTP y el nombre de archivo con el que queremos guardar la configuración.

3.1.16. Restaurar un backup

Es recomendable copiar la configuración en "running-config" para comprobar que todo funciona bien antes de copiar la configuración en el "startup-config".

```
ciscoasa#copy ftp startup-config
```

3.1.17. Actualizar ASA y ASDM

Podemos actualizar desde CLI o desde el ASDM, la manera más simple es utilizar el ASDM ya que lo tenemos habilitado.

Descargaremos las actualizaciones de software desde la página web oficial de Cisco, donde podemos encontrar la descarga para el ASDM y para el software del ASA 5505.

Una vez encontrado nuestro dispositivo, descargaremos:

- Adaptive Security Appliance (ASA) Device Manager
- Adaptive Security Appliance (ASA) Software

Ahora desde nuestro ASDM vamos a la pestaña de "Tools" y a la opción "Upgrade Software…" e instalaremos por separado ambas actualizaciones.

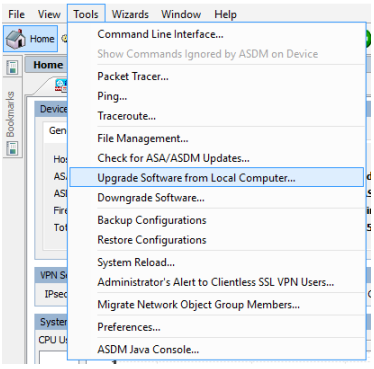

Imagen 14: Lista de herramientas, actualizar ASDM

3.3. Fin de la configuración

Estos son los pasos y configuraciones básicas para hacer funcionar este dispositivo ASA 5505 en una PYME, pero este dispositivo dispone de muchas más opciones de configuración que pueden ser interesantes para nuestra empresa.

Otra configuración muy utilizada por las empresas que tienen oficinas remotas y teletrabajadores suelen ser las VPN, y el cortafuegos ASA 5505 proporciona IPsec/SSL VPN.

4. Futuro: Seguridad en IoT

El término "Internet de las cosas" (Internet of things, IoT), parte de que estamos cada vez más rodeados de nuevas tecnologías dedicadas a conectar los dispositivos electrónicos que nos rodean, entre ellos y con nosotros.

El ejemplo más cercano es el propio hogar, donde ya existen neveras, lavadoras, televisores, videoconsolas e incluso coches que disponen de conexión a internet. También en las empresas son cada vez más utilizados estos dispositivos de IoT como por ejemplo en impresoras, cámaras de videovigilancia, control de luces, temperatura, etc.

El principal problema de estos dispositivos es la seguridad, ya que un estudio realizado por HP reveló en 2015 que el 70% de estos dispositivos "inteligentes" son vulnerables a los ataques más simples, ya que sus fabricantes se han centrado en el número de ventas y han dejado algo olvidado el apartado de la seguridad como:

- El acceso sin contraseñas.
- Contraseñas simples.
- Sistemas de control remoto fácilmente explotables.
- O sistemas que revelan información confidencial.

Las consecuencias de estos “agujeros” de seguridad pueden llevar a:

- Que un atacante controle estos dispositivos.
- Roben información confidencial.
- Desconfigurar los dispositivos, alterando el funcionamiento de la empresa.
- Los utilicen para acceder a sistemas más sensibles…

Otro inconveniente es que la mayoría de estos dispositivos no permiten la instalación de un cortafuegos o antivirus, con lo que disponer de un cortafuegos hardware UTM como es el de Cisco Firepower, resulta una mejora en la seguridad ya que permite identificar y detener ataques con mayor rapidez e independencia de dónde se encuentren, algo especialmente importante para las empresas que adoptan nuevos entornos virtuales y Cloud, soluciones IoT y terminales móviles.

Cisco además ofrece sistemas de seguridad del IoT específicos con la introducción de un nuevo dispositivo de seguridad dedicado (ISA-3000 para visibilidad de aplicaciones, aplicación de políticas y defensa ante amenazas) y una solución de seguridad antiniebla para servicios de datos.

En este año 2016, la empresa ICSA Labs ha presentado un programa que permitirá analizar la seguridad del IoT de los productos. Las pruebas a los dispositivos con IoT examinarán seis componentes de seguridad, para asegurar una protección adecuada: alertas e inicio de sesión, criptografía, autenticación, comunicaciones, seguridad física y plataformas de seguridad.

Si los productos pasan estas pruebas recibirán un sello de reconocimiento, el cual, unido a un buen cortafuegos hardware mejorará la seguridad del internet de las cosas en nuestra PYME.

5. Conclusiones

Un firewall hardware es un requisito indispensable para la seguridad de una PYME, no es un antivirus, con lo cual debemos combinarlo con un buen antivirus para aumentar la seguridad de nuestra red.

La mejor opción es utilizar dos firewalls diferentes unidos a modo de bastión y contención, el bastión se encargara de parar todos los ataques de internet y el de contención será la segunda barrera por si el primero pudiera fallar.

En cuanto a la elección del tipo de cortafuegos, la mejor opción es elegir un cortafuegos hardware UTM para nuestra PYME, ya que son dispositivos compactos fabricados únicamente para este propósito y tienen detrás un equipo de personas trabajando día a día para crear actualizaciones del dispositivo y mejorar su seguridad.

Otra opción, aunque más difícil de implementar y mantener es utilizar un equipo Linux a modo de cortafuegos, su mayor inconveniente es la falta de robustez, ya que tiene más probabilidad de fallos y por lo cual no es una solución óptima para la continuidad de una PYME.

Para la elección del cortafuegos UTM existen en el mercado multitud de compañías que fabrican estos tipos de dispositivos. Mi elección se ha basado en las pruebas que realiza NSS Labs cada año a los mejores equipos firewall del mercado y un estudio de mercado realizado por IDC donde se nombran los dispositivos UTM más implantados mundialmente.

Se ha realizado una comparación los dos dispositivos más implantados en el mundo (CISCO y CheckPoint), siendo un claro ganador y elección final el cortafuegos de CISCO al disponer de la nueva generación de IPS (NGIPS) que mejora la visibilidad del IPS típico.

Además, Cisco dispone de otras ventajas como la calidad de servicio técnico, estabilidad y por sus herramientas de emulación de redes como GNS3 o Packet Tracer.

En cuanto a la elección del modelo del cortafuegos dentro de la gama de productos de Cisco, la elección es el firewall ASA 5506-X, que es el modelo más económico de la gama de cisco pero utiliza el mismo software que sus hermanos mayores, con lo que el nivel de protección es idéntico, y por sus características (5000 conexiones por segundo, 5 VLANs, 50 VPNs, 20000 conexiones máximo, etc…) es más que suficiente para ser utilizado en una PYME de menos de 250 trabajadores.

En cuanto a la implementación y configuración, necesitamos unos conocimientos mínimos sobre configuración de equipos Cisco, listas de control de acceso (ACL), NAT, rutas, VPN, etc.

La configuración se puede realizar por línea de comandos (CLI) o por interfaz web (ASDM) con una visualización más rápida de la configuración global.

Lo más recomendable, ofreciendo mayor nivel de seguridad, es utilizar una política de configuración restrictiva, en la que por defecto esta todo denegado y solo se permitirá el acceso mediante las ACL que especifiquemos nosotros manualmente.

La conclusión definitiva es que los ciberataques van evolucionando y no existe una protección 100% efectiva en internet, con lo que debemos de “blindar” al máximo posible nuestra red y para ello necesitamos un cortafuegos hardware UTM, además de un buen antivirus en cada una de las máquinas de nuestra red.

6. Bibliografía

Las fuentes y herramientas utilizadas para este trabajo de fin de grado han sido además del material de las asignaturas de redes realizadas durante estos cuatro años de carrera, información de páginas web como:

Documentación oficial de Cisco:

- http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/interface_start_5505.html
- http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html
- https://www.cisco.com/web/ES/assets/pdf/asa_firepower_services_aag_es.pdf

Documentación no oficial:

- http://www.redescisco.net/sitio/2013/08/11/cisco-asa-configurando-interfaces/

Estudios de mercado y pruebas:

- https://www.idc.com/getdoc.jsp?containerId=prUS41078516
- https://www.nsslabs.com/

Herramienta de simulación Packet Tracer:

- https://www.netacad.com/es/about-networking-academy/packet-tracer/

Mayores ataques en la historia:

- http://es.gizmodo.com/los-10-mayores-ataques-informaticos-de-la-historia-1580249145

Internet de las cosas IoT:

- http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf
- http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

Además de utilizar un dispositivo físico ASA 5505 del laboratorio de DSIC de la Universidad Politécnica de Valencia – Campus de Alcoy (EPSA).