laSalle
UNIVERSIDAD RAMON LLULL

Curs d´Implantació i Gestió de la Seguretat

Módulo 2

Herramientas Básicas de Prevención

Práctica de laboratorio: Firewalls

Profesor: Víctor Verdú

Alumno: Julián Gordon

Indice

Curs d´Implantació i Gestió de la Seguretat

Alumno: Julián Gordon

Práctica de laboratorio: Firewalls

Objetivos

Contestar las siguientes preguntas en la que se debe identificar y analizar las soluciones pioneras de firewalls.

Preguntas

1. ¿Cuáles son los principales fabricantes de seguridad que tienen soluciones de Firewalls NGFW pioneras en el mercado?
2. ¿Qué funcionalidades ofrecen cada uno de estos fabricantes en sus productos de Firewalls?
3. ¿Qué diferencias existen entre fabricantes de seguridad?
4. Lista otras soluciones de seguridad comunes para la prevención de amenazas en una red corporativa.

Firewalls

Los firewalls next generation (NGFW), son esenciales para la seguridad moderna de las redes, ya que ofrecen capacidades avanzadas más allá del simple filtrado de paquetes. Los principales fabricantes que lideran el mercado de NGFW incluyen Palo Alto Networks, Fortinet, Cisco, Check Point, y Sophos.

A continuación, se describen las funcionalidades que ofrecen cada uno de estos fabricantes en sus productos de firewalls y sus diferencias.

1. Palo Alto Networks

Funcionalidades:

- **Application Identification (App-ID):** Identificación y control de aplicaciones de manera granular, independientemente del puerto o protocolo.
- **User Identification (User-ID):** Asociar tráfico de red con usuarios específicos.
- **Content Identification (Content-ID):** Prevención avanzada de amenazas, incluyendo la inspección de tráfico cifrado.
- **Threat Prevention:** Protección contra malware, exploits y amenazas conocidas y desconocidas mediante tecnologías como WildFire.
- **GlobalProtect:** Solución de seguridad para acceso remoto que extiende la protección NGFW a usuarios móviles y sucursales.

Diferencias:

- Palo Alto Networks es conocido por su tecnología de identificación de aplicaciones, que proporciona un control muy detallado y granular del tráfico de red.
- La integración con WildFire para la detección y prevención avanzada de amenazas, incluyendo el análisis en la nube, es una característica distintiva.

2. Fortinet

Funcionalidades:

- **FortiOS:** Sistema operativo unificado para la gestión de seguridad en todos los dispositivos Fortinet.
- **Application Control:** Identificación y control de aplicaciones.
- **Advanced Threat Protection:** Soluciones como FortiSandbox para análisis de amenazas en tiempo real.
- **Integrated SD-WAN:** Optimización de la red y mejora del rendimiento.
- **Security Fabric:** Integración de múltiples soluciones de seguridad para una visibilidad y gestión centralizadas.

Diferencias:

- Fortinet destaca por su enfoque en el rendimiento y la integración, ofreciendo una amplia gama de productos de seguridad que trabajan en conjunto bajo la plataforma Security Fabric.
- La incorporación de SD-WAN en sus NGFW proporciona capacidades avanzadas de optimización de red y seguridad en una sola solución.

3. Cisco

Funcionalidades:

- **Cisco Secure Firewall (anteriormente Firepower):** Ofrece protección avanzada contra amenazas, visibilidad, y control de aplicaciones.
- **Advanced Malware Protection (AMP):** Protección contra malware sofisticado y ataques de día cero.
- **Threat Intelligence:** Integración con Cisco Talos para inteligencia de amenazas.
- **VPN:** Soporte para VPN tanto en sitio a sitio como para usuarios remotos.
- **Network Analytics:** Monitorización y análisis del tráfico de red para la detección de anomalías y amenazas.

Diferencias:

- Cisco es conocido por su enfoque en la integración con otros productos y servicios de red, proporcionando una solución de seguridad que se integra bien con las infraestructuras de red existentes.
- La inteligencia de amenazas proporcionada por Cisco Talos es una de las más completas y avanzadas del mercado.

4. Check Point

Funcionalidades:

- **Threat Prevention:** Protección avanzada contra amenazas mediante tecnologías como SandBlast.
- **Identity Awareness:** Identificación y control basado en usuarios y grupos.
- **ThreatCloud:** Red global para la inteligencia de amenazas.
- **Unified Management:** Gestión centralizada de seguridad para todos los dispositivos Check Point.
- **Scalable Platforms:** Soluciones que escalan desde pequeñas oficinas hasta grandes centros de datos.

Diferencias:

- Check Point es conocido por su fuerte enfoque en la prevención de amenazas y la inteligencia de amenazas global a través de ThreatCloud.
- Su capacidad para escalar y la gestión unificada son características que atraen a grandes organizaciones y entornos complejos.

5. Sophos

Funcionalidades:

- **Synchronized Security:** Integración y comunicación entre endpoint y red para una mejor protección.
- **Advanced Threat Protection:** Protección contra amenazas avanzadas mediante tecnologías como Sophos Sandstorm.
- **Application Control:** Control detallado de aplicaciones.

- **Web Protection:** Filtrado y control de acceso web.
- **Centralized Management:** Gestión centralizada a través de Sophos Central.

Diferencias:

- Sophos se destaca por su enfoque en la seguridad sincronizada, donde sus soluciones de endpoint y red trabajan juntas para mejorar la detección y respuesta a amenazas.
- La simplicidad en la implementación y gestión, especialmente para pequeñas y medianas empresas, es una de sus principales ventajas.

Soluciones de seguridad para la prevención de amenazas

Además de los NGFW, existen varias otras soluciones de seguridad que son fundamentales para la prevención de amenazas en una red corporativa:

1. **Sistemas de Prevención de Intrusiones (IPS):**
   - Detectan y previenen actividades maliciosas o violaciones de políticas dentro de la red.
2. **Sistemas de Detección de Intrusiones (IDS):**
   - Monitorean la red en busca de actividades sospechosas y generan alertas.
3. **Sistemas de Gestión de Información y Eventos de Seguridad (SIEM):**
   - Recopilan y analizan datos de seguridad en tiempo real para la detección de amenazas, incidentes y cumplimiento normativo.
4. **Antivirus y Antimalware:**
   - Protegen contra software malicioso y virus en endpoints y servidores.
5. **Control de Acceso a la Red (NAC):**
   - Controla el acceso a la red y asegura que solo los dispositivos autorizados y compatibles puedan conectarse.
6. **VPN (Virtual Private Network):**
   - Proporciona acceso seguro y cifrado a la red corporativa para usuarios remotos.
7. **DLP (Data Loss Prevention):**
   - Protege contra la pérdida y exfiltración de datos sensibles.

8. **Filtrado de Contenidos Web y Correo Electrónico:**
   - Bloquea sitios web maliciosos y filtra el correo electrónico para detectar y prevenir amenazas de phishing y spam.
9. **Segmentación de Red:**
   - Divide la red en segmentos más pequeños para limitar el alcance de las amenazas y mejorar la seguridad interna.
10. **Autenticación Multifactor (MFA):**
    - Añade una capa adicional de seguridad mediante la verificación de la identidad de los usuarios a través de múltiples métodos.