Documento de especificaciones del producto

Contoso CipherGuard Sentinel X7

1. Información general del producto

1.1 Introducción

Contoso CipherGuard Sentinel X7 es un producto de seguridad avanzado y resistente diseñado meticulosamente para fortalecer la infraestructura de la red informática frente a una amplia gama de amenazas y vulnerabilidades. Este documento profundiza en las especificaciones técnicas, características y funcionalidades de Contoso CipherGuard Sentinel X7.

1.2 Características principales

- **Protección de firewall:** Contoso CipherGuard Sentinel X7 utiliza un firewall de inspección con estado y técnicas de inspección profunda de paquetes. Inspecciona y analiza paquetes de red en la capa de aplicación y ofrece un control detallado de los flujos de datos. El firewall adapta su conjunto de reglas de forma dinámica según el contexto de red en evolución y mitiga los riesgos asociados a los ataques en la capa de aplicación.

- **Sistema de detección y prevención de intrusiones (IDPS):** con tecnología de algoritmos de aprendizaje automático, nuestro IDPS supervisa de forma continua los patrones y anomalías del tráfico de red. Saca provecho de la detección basada en firmas, la detección de anomalías y el análisis heurístico para identificar e impedir amenazas potenciales. El sistema utiliza fuentes de inteligencia sobre amenazas y garantiza que se mantiene actualizado con los modelos de ataque conocidos más recientes.

- **Asistencia de la red privada virtual (VPN):** Contoso CipherGuard Sentinel X7 admite protocolos VPN estándar del sector, como Ipsec y OpenVPN. Facilita una comunicación segura en redes públicas al cifrar los datos en tránsito. El módulo VPN utiliza algoritmos criptográficos avanzados, como AES-256, lo que garantiza un canal de comunicación sólido y seguro para los usuarios remotos y sucursales.

- **Seguridad de los puntos de conexión:** nuestro módulo de seguridad de los puntos de conexión utiliza un enfoque de defensa en varias capas e incorpora capacidades de prevención de intrusiones basadas en antivirus, antimalware y host. Realiza análisis del comportamiento y detección heurística en tiempo real, por lo que garantiza una detección proactiva y la contención de las actividades malintencionadas. Además, se integra con plataformas de inteligencia sobre amenazas para dar una respuesta rápida a las amenazas emergentes.

- **Registro y supervisión:** el subsistema de registro y supervisión captura datos completos acerca de las actividades de la red. Incluye registros detallados de los modelos de tráfico, eventos de autenticación de usuarios y violaciones de las directivas de seguridad. Al integrarse con SIEM (Administración de eventos e información de seguridad), esta característica facilita la supervisión y análisis centralizados, lo que permite los administradores de seguridad responder con velocidad a los incidentes de seguridad potenciales.

- **Autenticación del usuario y control de acceso**: Contoso CipherGuard Sentinel X7 admite mecanismos de autenticación multifactor (MFA), como la autenticación biométrica y la integración de tarjetas inteligentes. Las directivas de control de acceso se basan en los roles de usuario, que sacan provecho de la integración de LDAP y Active Directory. La aplicación dinámica de directivas garantiza que solo los usuarios autorizados tengan acceso a los recursos confidenciales.

2. Especificaciones técnicas

2.1 Requisitos de hardware

- **Procesador:** cuatro núcleos de 2,5 GHz o superior con asistencia de aceleración de hardware
- **RAM:** 16 GB mínimo, se recomienda ECC (código de corrección de errores)
- **Almacenamiento:** 200 GB mínimo, SSD para un rendimiento óptimo
- **Tarjetas de interfaz de red (NIC):** Gigabit Ethernet doble con asistencia para tramas jumbo

2.2 Requisitos de software

- **Sistema operativo:** compatible con Windows Server 2019 y versiones posteriores, CentOS 8 o equivalente
- **Base de datos:** PostgreSQL 13 para el almacenamiento de datos, optimizado para indexación de alto rendimiento
- **Actualizaciones de seguridad:** actualizaciones automatizadas para las fuentes de inteligencia sobre amenazas y parches de seguridad regulares

2.3 Compatibilidad de red

- **Protocolos:** admitir TCP/IP, UDP, ICMP, IPv6
- **Integración:** integración perfecta con los protocolos de enrutamiento BGP y OSPF
- **Compatibilidad:** interoperabilidad con Cisco, Juniper y otros proveedores de redes importantes

3. Plan de implementación

3.1 Pasos de implementación

1. **Evaluación anterior a la implementación:** llevar a cabo una evaluación completa de la vulnerabilidad de la red, en la que se incluyen pruebas de penetración y análisis de riesgos.

2. **Instalación:** implementar Contoso CipherGuard Sentinel X7 en servidores dedicados o Virtual Machines, lo que garantiza un uso óptimo del hardware y la asignación de recursos.

3. **Configuración:** personalizar las directivas de seguridad, controles de acceso y reglas de firewall en base a los requisitos de la organización. Ajustar los parámetros de detección de intrusiones para la máxima precisión.

4. **Pruebas:** ejecutar un plan de pruebas completo, que incluya escenarios de ataques simulados y pruebas de carga para validar la eficacia y rendimiento de la solución.

5. **Aprendizaje:** ofrecer sesiones de aprendizaje en profundidad para el personal de TI que traten las operaciones diarias, los procedimientos de respuesta a incidentes y las tareas de mantenimiento.

3.2 Mantenimiento y asistencia

- **Actualizaciones regulares:** Contoso garantiza actualizaciones continuas del producto, que incorporan las mejoras de seguridad e inteligencia sobre amenazas más recientes.

- **Soporte técnico:** Contoso ofrece un equipo de soporte técnico dedicado las 24 horas para garantizar una asistencia veloz para cualquier problema técnico o consulta sobre Contoso CipherGuard Sentinel X7.