Documento de especificações do produto

# Contoso CipherGuard Sentinel X7

# 1. Visão geral do produto

## 1.1 Introdução

O Contoso CipherGuard Sentinel X7 é um produto de segurança avançado e resiliente meticulosamente projetado para fortalecer a infraestrutura de rede de computadores contra um espectro de ameaças e vulnerabilidades. Este documento explora as complexidades das especificações técnicas, características e funcionalidades do Contoso CipherGuard Sentinel X7.

## 1.2 Principais recursos

* **Proteção de firewall:** utilizando um firewall de inspeção com estado, o Contoso CipherGuard Sentinel X7 emprega técnicas de inspeção avançada de pacotes. Ele inspeciona e analisa pacotes de rede na camada de aplicativo, fornecendo controle granular sobre os fluxos de dados. O firewall adapta dinamicamente seu conjunto de regras com base no contexto de rede em constante evolução, mitigando os riscos associados a ataques à camada de aplicativo.
* **IDPS (Sistema de Detecção e Prevenção de Intrusão):** com algoritmos de machine learning, nosso IDPS monitora continuamente os padrões e anomalias de tráfego de rede. Ele utiliza detecção baseada em assinaturas, detecção de anomalias e análise heurística para identificar e neutralizar ameaças potenciais. O sistema emprega feeds de inteligência contra ameaças, garantindo que esteja atualizado com os últimos padrões de ataque conhecidos.
* **Compatibilidade com a VPN (Rede Virtual Privada):** o Contoso CipherGuard Sentinel X7 é compatível com os protocolos VPN padrão do setor, como IPsec e OpenVPN. Ele facilita a comunicação segura em redes públicas, criptografando dados em trânsito. O módulo VPN utiliza algoritmos de criptografia avançados, incluindo AES-256, garantindo um canal de comunicação robusto e seguro para usuários remotos e filiais.
* **Segurança de ponto de extremidade:** empregando uma abordagem de defesa em várias camadas, nosso módulo de segurança de ponto de extremidade incorpora recursos de prevenção de intrusão antivírus, antimalware e baseado em host. Ele realiza análises de comportamento em tempo real e verificação heurística, garantindo detecção proativa e contenção de atividades maliciosas. Além disso, integra-se a plataformas de inteligência contra ameaças para resposta imediata a ameaças emergentes.
* **Registro e monitoramento:** o subsistema de registro e monitoramento captura dados abrangentes sobre as atividades da rede. Inclui registros detalhados sobre padrões de tráfego, eventos de autenticação de usuários e violações de políticas de segurança. Integrado ao SIEM (gerenciamento de eventos e informações de segurança), esse recurso centraliza o monitoramento e a análise, capacitando os administradores da segurança a responder rapidamente a possíveis incidentes de segurança.
* **Autenticação de usuário e controle de acesso**: o Contoso CipherGuard Sentinel X7 é compatível com os mecanismos de MFA (autenticação multifator), incluindo autenticação biométrica e integração de cartão inteligente. As políticas de controle de acesso se baseiam em funções de usuário, aproveitando a integração com o LDAP e o Active Directory. A aplicação dinâmica de políticas garante que apenas os usuários autorizados tenham acesso a recursos confidenciais.

# 2. Especificações técnicas

## 2.1 Requisitos de hardware

* **Processador:** Quad-core 2,5 GHz ou superior compatível com aceleração de hardware
* **RAM:** mínimo de 16 GB, ECC (código de correção de erros) recomendado
* **Armazenamento:** mínimo de 200 GB, SSD para desempenho ideal
* **NIC (placa de interface de rede):** Dual Gigabit Ethernet compatível com quadros jumbo

## 2.2 Requisitos de software

* **Sistema operacional:** compatível com Windows Server 2019 e mais recentes, CentOS 8 ou equivalente
* **Banco de dados:** PostgreSQL 13 para armazenamento de dados, otimizado para indexação de alto desempenho
* **Atualizações de segurança:** atualizações automatizadas para feeds de inteligência contra ameaças e aplicação de patches de segurança regulares

## 2.3 Compatibilidade de rede

* **Protocolos:** compatível com TCP/IP, UDP, ICMP e IPv6
* **Integração:** integração direta com os protocolos de roteamento BGP e OSPF
* **Compatibilidade:** interoperabilidade com Cisco, Juniper e outros grandes fornecedores de rede

# 3. Plano de Implementação

## 3.1 Etapas de implantação

1. **Avaliação pré-implantação:** faça uma avaliação abrangente da vulnerabilidade da rede, incluindo testes de penetração e análise de risco.
2. **Instalação:** implante o Contoso CipherGuard Sentinel X7 em servidores dedicados ou máquinas virtuais, garantindo a alocação de recursos e a utilização de hardware ideais.
3. **Configuração:** personalize políticas de segurança, controles de acesso e regras de firewall com base nos requisitos organizacionais. Ajuste os parâmetros de detecção de invasões para máxima precisão.
4. **Teste:** execute um plano de teste completo, incluindo cenários de ataque simulados e testes de carga, para validar a eficácia e o desempenho da solução.
5. **Treinamento:** forneça sessões de treinamento aprofundadas para o pessoal de TI, abrangendo operações diárias, procedimentos de resposta a incidentes e tarefas de manutenção.

## 3.2 Manutenção e suporte

* **Atualizações regulares:** a Contoso garante atualizações contínuas para o produto, incorporando os aprimoramentos de segurança e inteligência contra ameaças mais recentes.
* **Suporte técnico:** a Contoso oferece uma equipe de suporte dedicada 24 horas por dia, 7 dias por semana, para garantir assistência imediata para quaisquer problemas técnicos ou dúvidas relacionadas ao Contoso CipherGuard Sentinel X7.