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 uma variedade 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 por firewall:** utilizando um firewall de inspeção com monitoração de estado, o Contoso CipherGuard Sentinel X7 emprega técnicas profundas de inspeção 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.
* **Sistema de Detecção e Prevenção de Intrusões (IDPS):** Alimentado por algoritmos de aprendizado de máquina, nosso IDPS monitora continuamente 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.
* **Suporte à rede virtual privada (VPN): o Contoso CipherGuard Sentinel X7 oferece suporte a 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.
* **Endpoint Security:** Empregando uma abordagem de defesa em várias camadas, nosso módulo de segurança de endpoint 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 oferece suporte a mecanismos de autenticação multifator (MFA), 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 com suporte a aceleração de hardware
* **RAM:** mínimo de 16 GB, ECC (Código de Correção de Erros) recomendado
* **Armazenamento:** mínimo de 200 GB, SSD para desempenho ideal
* **Placas de Interface de Rede (NIC):** Ethernet Gigabit dupla com suporte para quadros jumbo

## 2.2 Requisitos de software

* **Sistema operacional:** Compatível com Windows Server 2019 e superior, 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 de ameaças e patches de segurança regulares

## 2.3 Compatibilidade de rede

* **Protocolos:** TCP/IP, UDP, ICMP, IPv6 suporte
* **Integração:** integração perfeita com 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:** conduza 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 utilização ideal de hardware e alocação de recursos.
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. **Testes:** 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 detalhadas para o pessoal de TI, cobrindo 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 de ameaças mais recentes.
* **Suporte técnico: a Contoso fornece uma equipe de suporte dedicada 24 horas por dia, 7 dias por semana,** para garantir assistência imediata para quaisquer problemas técnicos ou consultas relacionadas ao Contoso CipherGuard Sentinel X7.