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 de firewall:** utilizando um firewall de inspeção com estado, o Contoso CipherGuard Sentinel X7 aplica técnicas de inspeção profunda 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 prevenção e detecção de invasões (IDPS):** possibilitado por algoritmos de aprendizado de máquina, nosso IDPS monitora continuamente os padrões de tráfego de rede e anomalias. 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 dá 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.

- **Segurança do ponto de extremidade:** utilizando uma abordagem de defesa em várias camadas, nosso módulo de segurança do ponto de extremidade incorpora antivírus, antimalware e recursos de prevenção de invasões baseados 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.

- **Monitoramento e registro em log:** o subsistema de registro em log e monitoramento captura dados abrangentes sobre atividades de 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 do usuário e controle de acesso**: o Contoso CipherGuard Sentinel X7 dá 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 à aceleração de hardware
- **RAM:** mínimo de 16 GB, ECC (Error-Correcting Code) recomendado
- **Armazenamento:** mínimo de 200 GB, SSD para desempenho ideal
- **Placa de interface de rede (NIC):** Dual Gigabit Ethernet com suporte a 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 automáticas para feeds de inteligência contra ameaças e patches de segurança regulares

2.3 Compatibilidade de rede

- **Protocolos:** suporte a TCP/IP, UDP, ICMP, IPv6
- **Integração:** integração perfeita com protocolos de roteamento BGP e OSPF
- **Compatibilidade:** interoperabilidade com Cisco, Juniper e outros grandes fornecedores de redes

3. Plano de implementação

3.1 Etapas de implantação

1. **Avaliação antes da implantação:** realize uma avaliação abrangente de vulnerabilidades de rede, incluindo testes de penetração e análises 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 recurso.

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 testes 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, 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 as últimas melhorias de segurança e inteligência contra ameaças.

- **Suporte técnico:** a Contoso disponibiliza uma equipe de suporte dedicada em tempo integral para garantir assistência rápida a quaisquer problemas técnicos ou dúvidas relacionadas ao Contoso CipherGuard Sentinel X7.