SERVIÇO: 02.06 – Firewall CP_MTI

Diretoria/Unidade/Gerência Responsável: DTIC/UGITI/GSUP

Descrição:
O **Firewall CP_MTI** oferece aos clientes de todos os portes a mais recente proteção de dados e segurança de rede em uma próxima geração integrando plataformas de prevenção de ameaças, reduzindo a complexidade e diminuindo o custo total de propriedade.

Diferenciais MTI:
A segurança é pré requisito para serviço "Conectividade a Rede INFOVIA MT" para atender as Política de Segurança da Informação MTI, a Política de Gestão Integrada de Riscos Corporativos que estabelece o modelo, os princípios, as diretrizes e as responsabilidades da Gestão Integrada dos Riscos Corporativos da Empresa Mato-grossense de Tecnologia da Informação – MTI e a resolução do Cosint 003/2010 que dispõe sobre as Políticas e Diretrizes de Segurança da Informação no âmbito do Poder Executivo do Estado de Mato Grosso.

Detalhamento do produto:

1. **Firewall CP_MTI_Appliance:** appliance dedicado para função de firewall de nova geração. **001CPAP-SG7000-PLUS-SNBT** - Modelo Check Point Quantum 7000 Next Generation Firewalls (CPAP-SG7000-PLUS-SNBT).
Datasheet: Check Point 7000 Security Gateway Datasheet

2. **Firewall CP_MTI_Virtual:** instância virtual de firewall hospedada em appliance dedicado para virtualização de firewalls de nova geração que possui todas as funcionalidades listadas acima nos itens 1 e 2.
0010040500250* - instância virtual sob as configurações abaixo:
   4 vCpu
   50k conexões simultâneas
   Até 250GB de LOG
   A estruturação do código tecnológico(AAABBBCCCDDDD) do produto reporta o seguinte significado:
   AAA - "001": identificação sequencial.
   BBB - "004": configuração vCpu.
   CCC - "050": configuração Conexões Simultâneas.
   DDD - "0250": configuração de capacidade de armazenamento de LOG.

Detalhamento das Funcionalidades:

1. **Funcionalidades Firewall CP_MTI:**

- **Firewall:** solução que provê alto nível de segurança de gateway.
- **IPsec VPN:** Integra controle de acesso, autenticação e criptografia para garantir conectividade segura para redes corporativas para usuários remotos e móveis, filiais e parceiros de negócios na Internet.
- **Advanced Networking and Clustering:** simplifica a implantação e gerenciamento de segurança de rede dentro de redes complexas, maximizando o desempenho da rede - ideal para empresas de ponta, datacenter e ambientes onde o desempenho e a disponibilidade são essenciais.
- **Mobile Access:** fornece acesso remoto simples e seguro a e-mail, calendários, contatos e aplicativos corporativos pela Internet, por meio de smartphones, tablets ou laptops.

- **Identity Awareness:** fornece visibilidade granular de usuários, grupos e máquinas, proporcionando incomparável controle de acesso por meio da criação de políticas precisas e baseadas em identidade.
- **Application Control:** permite que as equipes de TI criem facilmente políticas granulares - com base em usuários ou grupos - para identificar, bloquear ou limitar o uso de mais de 8.500 aplicativos.
- **URL Filtering:** integra ao application control, permitindo aplicação e gerenciamento unificados de todos os aspectos da segurança na web.
- **Content Awareness:** é uma solução leve de Prevenção de Perda de Dados (DLP) que ajuda as empresas a proteger preventivamente as informações confidenciais contra perda não intencional, educando os usuários sobre políticas de manuseio adequado de dados e dando poder de corrigir incidentes em tempo real.
- **Intrusion Prevention System:** oferece prevenção de intrusão proativa e completa - tudo com as vantagens de implantação e gerenciamento de uma solução de firewall de próxima geração unificada e extensível.
- **Anti-Bot:** detecta máquinas infectadas por bot, evita danos por bots, bloqueando as comunicações C&C do bot, é continuamente atualizado a partir do ThreatCloud ™, a primeira rede colaborativa para combater o crime cibernético.
- **Antivírus:** bloqueia a entrada de arquivos maliciosos. Usando assinaturas de vírus em tempo real e baseadas em anomalias de proteções do ThreatCloud ™, a primeira rede colaborativa para combater o crime cibernético.
- **Anti-Spam and Email Security:** oferece proteção abrangente para a infraestrutura de mensagens de uma organização.
- **SandBlast Threat Emulation:** evita infecções de ameaças de dia zero, novos malwares e ataques direcionados. Como parte da solução SandBlast ™ Zero-Day Protection, este inovador mecanismo de sandbox oferece a melhor taxa de detecção possível para ameaças e é virtualmente imune às técnicas de evasão dos invasores**.**
- **SandBlast Threat Prevention:** remove conteúdo explorável, incluindo conteúdo ativo e objetos incorporados, reconstrói arquivos para eliminar ameaças potenciais e entrega prontamente conteúdo higienizado aos usuários para manter o fluxo de negócios.

2. Funcionalidades da Gerência:

- **Networking Management:** fornece uma política de segurança de rede abrangente e centralizada no gerenciamento de gateways Check Point por meio de um console único e unificado que fornece controle sobre as mais complexas implantações de segurança.
- **Next-Generation SmartEvent:** consolida monitoramento, registro, relatórios e análise de eventos em um único console - para oferecer visibilidade de ameaças de fácil compreensão. Então, ao invés de se afogar no dilúvio de dados, sua equipe de segurança pode concentrar seus esforços nas ameaças críticas.
- **Logging and Status:** transforma dados em inteligência de segurança com SmartLog, um avançado analisador de log que fornece resultados de pesquisa em frações de segundo, proporcionando visibilidade em tempo real de bilhões de registros de log em vários períodos de tempo e domínios.
- **Compliance:** oferece uma solução de monitoramento de conformidade e segurança integrada e totalmente automatizada. A conformidade permite o monitoramento contínuo, fortalece a conformidade regulatória, mantém uma política segura e reduz o tempo e os custos de auditoria.

- **Monitoring:** apresenta uma imagem completa do desempenho da rede e da segurança, permitindo respostas rápidas às mudanças nos padrões de tráfego ou eventos de segurança. Monitore dispositivos Check Point e alertas de alterações em gateways, endpoints, túneis, usuários remotos e atividades de segurança.
- **SmartView:** permite o gerenciamento de eventos via navegador. Use o aplicativo SmartView Web para ter um overview geral das informações de segurança do seu ambiente. Possui o mesmo monitoramento e análise de eventos em tempo real tais como o SmartConsole.
- **User Directory:** aproveita os servidores LDAP para obter informações de identificação e segurança sobre os usuários da rede, eliminando os riscos associados à manutenção e sincronização manual de armazenamentos de dados redundantes, e permitindo o gerenciamento centralizado de usuários em toda a empresa.

Excluído:

- Capacitação na ferramenta;
- Administração da rede do cliente;
- Licenças de uso de sistemas de qualquer tipo (operacional, firewall, aplicativos, banco de dados, etc.);
- Solução de Segurança de Computadores **(Serviço específico no Catálogo);**
- Conectividade a Rede INFOVIA-MT **(Serviço específico no Catálogo);**

Excluído para o serviço CP_MTI_Virtual_Gerenciado:

- Permissão de login na gerência do firewall e administração do firewall

Excluído para o serviço CP_MTI_Virtual_NÃO_Gerenciado:

- Permissão para criação de interfaces (realizado apenas através de abertura de chamado para a equipe técnica da MTI);
- Permissão para criação de roteamento (realizado apenas através de abertura de chamado para a equipe técnica da MTI);
- Permissão para habilitar blades (realizado apenas através de abertura de chamado para a equipe técnica da MTI);
- Permissão para login direto na caixa Fisica.

Serviço Final:

Solução **Firewall CP_MTI** disponibilizado.

SLA:

- Abertura de chamados: 24x7
- Atendimento serviço e suporte 8 x 5
- Disponibilidade do Serviço 99,9% ao mês;
- Tempo para disponibilizar o serviço ao cliente será conforme cronograma de implantação definido na fase de planejamento.

Pré-requisito:

- Formalização da demanda junto a MTI caracterizando as necessidades do cliente;
- Documento com as especificações técnicas das necessidades de configuração dos Serviços conforme documento de dimensionamento link:
- https://docs.google.com/forms/d/1v6iA0rQFgekVUMy7O_ixva8DKTp1wNbjcclB4-FlKro/viewform?edit_requested=true
- Contrato da prestação do Serviço assinado;
- Disponibilidade de ambiente seguro dotado de energia estabilizada e climatização, referente ao produto no formato de appliance.

Responsabilidades:

Cliente

- Estabelecer contrato comercial assinado entre as partes, incluindo o acordo do Nível de Serviço, antes do início da prestação de serviços;

- Prover a MTI de todas as informações necessárias à consecução do serviço, dentro dos prazos e condições definidos na negociação do serviço;
- Indicar representante junto à MTI para tratar de assuntos relacionados ao serviço, acompanhar e validar sua execução, além de atestar as alterações e/ou implementações;
- Contratar previamente o serviço de Conectividade a Rede INFOVIA-MT;
- Instalar e manter a infraestrutura interna (física e lógica) para garantir a segurança e controle de acessos dos seus usuários;
- Comunicar, de imediato, via SAC, a ocorrência de qualquer anormalidade na operação do serviço.

MTI

- Estabelecer contrato comercial assinado entre as partes, incluindo o acordo do Nível de Serviço, antes do início da prestação de serviços;
- Comunicar ao cliente, com a antecedência possível ou de acordo com o contrato de Nível de Serviço, qualquer anormalidade na prestação do serviço ou paralisação para manutenção, referente ao produto no formato virtual.
- Manter a prestação do serviço conforme acordado em contrato;
- Atender os chamados de incidentes e problemas dirigidos ao SAC dentro dos níveis de serviço acordados.

Modalidade

Descrição do Item	Métrica
Firewall CP MTI Appliance Gerenciado	Equipamento
Firewall CP MTI Appliance NÃO Gerenciado	Equipamento
Firewall CP MTI Virtual Gerenciado	Instância
Firewall CP MTI Virtual NÃO Gerenciado	Instância