Tribunal de Justiça Militar do Estado de Minas Gerais

ESTUDOS PRELIMINARES DA STIC

INTRODUÇÃO

Este Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Resolução CNJ Nº 182 /2013.

1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

Identificação das necessidades de negócio

Pretende-se, com a solução segurança de redes, manter a segurança do ambiente computacional do TJMMG, por meio das funcionalidades de Firewall, filtro de conteúdo, filtro de aplicação, inspeção SSL, Intrusion prevention system - IPS, antivírus, AntiSpam.

O Tribunal de Justiça Militar de Minas Gerais (TJMMG), assim como outros órgãos governamentais, está sujeito a ataques cibernéticos, que podem comprometer a infraestrutura tecnológica e os sistemas disponibilizados. O surgimento diário de novas ameaças e a crescente complexidade desses ataques aumenta a dificuldade de detecção, análise e resposta em tempo hábil. Essa situação pode ocasionar vazamentos de dados sigilosos e comprometer a disponibilidade de sistemas críticos do TJMMG.

A segurança das informações e de todo parque computacional do TJMMG depende das funcionalidades de firewall, filtro de aplicações, filtro WEB, controle de trafego, antivírus e AntiSpam executadas por essa solução. Por tratar-se do principal elemento de segurança aplicado ao ambiente deste Tribunal, seu pleno funcionamento é essencial para a implementação das políticas de segurança definidas no órgão.

A solução que está sendo analisada neste estudo técnico possui de forma geral duas vertentes, e deve contemplar pelo menos os requisitos com que já contamos na solução atual. Primeiramente temos a solução de firewall em si, com todas as funcionalidades necessárias à proteção de rede e estabelecimento de regras. Além disso, há o escopo do registro, tratamento e análise dos logs, que é contemplado através de módulos ou funcionalidades complementares à funcionalidade primária.

Dentre as funcionalidades exercida pela solução de segurança, podemos citar:

- os filtros de pacotes, que restringem o trafego baseado no endereço IP de origem ou destino, ou, através das portas utilizadas pelos serviços.
- os filtros de estado e sessão, que são mais especializados e utilizam uma característica do principal protocolo de transporte utilizado, o Transmission Control Protocol (TCP), que é sua tabela de estados de conexão.
- o filtro de conteúdo, capaz de permitir ou negar acessos baseado em categorização ou em palavras-chaves definidas em uma lista.
- o filtro de aplicação, que possibilita o bloqueio de aplicações como Facebook, Youtube, Netflix, entre outros, de forma dinâmica e baseada em atributos, incluindo categorias, subcategorias e tecnologia.
- as funções de intrusão e detecção de intrusão, Intrusion prevention system - IPS e Intrusion detection system - IDS, que analisam o trafego prevenindo atividades potencialmente maliciosas por meio de assinaturas ou comportamento conhecidos.
- a funcionalidade de inspeção SSL que permite a verificação de trafego de rede criptografados, o que proporciona um nível maior de segurança ao ambiente.

Necessidade 1: Funcionalidade de Firewall
Requisito 1.1: Possuir controle de acesso à Internet por endereço /porta de origem e destino;
Requisito 1.2: Possuir integração com Servidores de Autenticação Microsoft Active Directory;
Requisito 1.3: Permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP;
Requisito 1.4: Possuir alta disponibilidade (High-Availability - HA), trabalhando no esquema de redundância do tipo ativo-passivo ou Ativo-Ativo com divisão de carga, com todas as licenças de firmware/software habilitadas para tal sem perda de conexões.
Necessidade 2: Funcionalidade de Filtro Web
Requisito 2.1: Possuir solução de filtro de conteúdo web integrado a solução de segurança;
Requisito 2.2: Deverá permitir a criação de listas de URL específicas para serem bloqueadas ou liberadas;
Requisito 2.3: Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável.
Necessidade 3: Funcionalidade de Controle de Aplicação
Requisito 3.1: Possuir solução de controle de aplicação integrado a solução de segurança;
Requisito 3.2: Deverá permitir a criação de listas de aplicações específicas para serem bloqueadas ou liberadas;
Requisito 3.3: Possuir categorias de aplicações definidas.
Necessidade 4: Funcionalidade de IPS
Requisito 4.1: Deverá permitir funcionar em modo transparente;
Requisito 4.2: Possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
Requisito 4.3: Deverá permitir a criação de padrões de ataque manualmente.
Necessidade 5: Funcionalidade de Controle de Utilização dos Links de Internet
Requisito 5.1: Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações ou serviços (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS (Quality of Service);
Requisito 5.2 Limitar individualmente a banda utilizada por programas tais como peer-to-peer, streaming, chat, VoIP e web;
Requisito 5.3: Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory.
Necessidade 6: Funcionalidade de VPN (Virtual Private Network)
Requisito 6.1: Possuir suporte a VPNs IPSec site-to-site e client-to-site;
Requisito 6.2: Possuir algoritmos de criptografia para túneis VPN: AES, 3DES;
Requisito 6.3: A VPN deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança implementada.
Necessidade 7: Funcionalidades de Gerenciamento Centralizado de Logs e Relatórios
Requisito 7.1: Throughput mínimo de 25 GB/dia de Logs;
Requisito 7.2: Capacidade de armazenamento de no mínimo 10TB;
Requisito 7.3: Permitir relatórios customizados na solução;
Requisito 7.4: Permitir geração de relatórios agendados ou sob demanda;
Requisito 7.5: Possuir relatórios pré-definidos na solução;
Requisito 7.6: Possuir console única de gerenciamento.
Necessidade 8: Garantia Técnica
Requisito 8.1: Suporte técnico remoto/presencial, com supervisão e autorização do fabricante da solução, baseado em níveis de serviço para tempos de atendimento, tratamento de incidentes e resolução de problemas, tudo sob demanda;
Requisito 8.2: Atualização tecnológica incluindo correções de erros e incremento de funcionalidades do firmware/software, acesso a base de conhecimento do fabricante da solução para todos os seus recursos e substituição eventual de peças/equipamentos, tudo sob demanda.
Requisito 8.3: Estar disponível por um período de 36 (trinta e seis) meses de acordo os termos contratuais vigentes.

2 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Para atendimento da demanda são necessárias 02 soluções de Firewall de Rede de Próxima Geração (NGFW), incluindo suporte e assinaturas de segurança por 36 meses e 02 comissionamento da solução.

Essa estimativa leva em conta a quantidade de equipamentos instalados atualmente no TJMMG e que são necessários para prover a solução.

3 – ANÁLISE DE SOLUÇÕES POSSÍVEIS

Solução 1: contratação de nova solução de Segurança UTM/NGFW Firewall, contemplando serviço de suporte técnico, manutenção e garantia, implantação, todos os componentes de software e hardware integrantes da solução, e todo o licenciamento, assinaturas e atualizações que se fizerem necessários.

Essa solução envolve a aquisição de uma solução totalmente nova, o que implica na aquisição de novos bens, que se configurariam como os novos ativos de Firewall. Neste cenário além de novos equipamentos, teríamos que levar em consideração os licenciamentos da solução, bem como implantação e capacitação no mínimo, o que se mostra pouco viável.

Solução 2: renovação da solução de segurança utilizada no TJMMG, incluindo suporte e assinaturas de segurança, devendo ser compatível com o concentrador de logs e geração de relatórios FortiAnalyzer.

Em 2017, o Tribunal de Justiça Militar de Minas Gerais aderiu à ata da UFSJ através do processo SEI 17.0.000001096-0, que contemplou a compra de duas unidades da solução Firewall de Rede de Próxima Geração Fortigate 300D da fabricante Fortinet. Essa aquisição representou um importante salto para a segurança de rede da instituição pois a solução anterior permitia apenas a execução de regras básicas de roteamento. Dentre os ganhos que foram proporcionados podemos citar filtros de navegação WEB granulares, integração com o LDAP Active Directory, balanceamento de carga entre links de Internet, QoS de saída de internet(priorizando banda para realização de vídeo-audiências), VPN para acesso remoto/teletrabalho seguro, IPS (detecção e prevenção de intrusão) etc. Concomitante ao appliance, a adesão incluiu o software de análise de logs FortiAnalyzer, pelo qual é possível extrair relatórios de utilização da rede com bastante detalhamento, tornando o estudo de utilização de rede e averiguação de incidentes de segurança bastante facilitado. A partir disso, é possível inferir a importância da atual solução de segurança composta pelos equipamentos Fortigate 300D e FortiAnalyzer.
De acordo com o site da fabricante, o modelo 300D atingirá fim de vida útil (*End of Life*) em Outubro do presente ano. Sendo assim após esse período, não é possível estender a garantia e suporte do equipamento, bem como subscrições de segurança fornecidas pelo fabricante, sendo inviável tanto do ponto de vista técnico, já que não há manutenção de equipamento que não possui mais suporte do fabricante, quanto do ponto de vista econômico, visto ser dispendioso para a Administração reservar recursos financeiros para equipamento descontinuado.

A solução Firewall, da fabricante Fortinet, em uso no TJMMG desde 2017, foi adquirida, portanto, em processo licitatório regular, fruto da adesão a uma ata de registro de preço. Está, em funcionamento há 6 anos e, como já dito, tem apresentado desempenho plenamente satisfatório e não há registro de danos ou prejuízos causados por invasões ou falhas de segurança durante seu período de uso.
Sendo assim, a manutenção da marca do equipamento Fortigate se baseia no princípio da padronização do ambiente e unificação das ferramentas. Desta forma, utilizando equipamentos de firewall do mesmo fabricante, possibilita a aplicação de regras integradas e homogêneas, eliminando prejuízos causados por eventuais incompatibilidades. Além disso, os servidores técnicos responsáveis pela operação da ferramenta já dominam o seu funcionamento, não sendo necessária nova capacitação, o que demandaria tempo e recurso.

Essa solução, portanto, atende aos requisitos elencados no item 1, mostrando-se viável.

4 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Os custos dos equipamentos foram estimados com base em pesquisa de mercado, em lojas de e-commerce:

- TI Mix, disponível em https://www.timix.com.br/fc-10-f200f-950-02-36.html: R$71.878,11, 01 licença Fortinet UTP - 3 anos - FC-10-F200F-950-02-36

- Firewall 1, disponível em https://www.firewall1.com.br/firewall/fortinet-fortigate-200f-unified-threat-protection-utp--p?gclid=CjwKCAjwt52mBhB5EiwA05YKo6ey9wPbp2P33oQLm3sR-D0ga12l5uxeBwkNXS1uDUwuegyplQqJ4hoCD7UQAvD_BwE: R$140.628,00, 01 licença Fortinet Fortigate 200F + Unified Threat Protection (UTP) 3 anos

Valor médio 01 licença: R$106.253,05

Valor estimado para 02 licenças Fortinet UTP - 3 anos - FC-10-F200F-950-02-36: R$212.506,11.

5 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Renovação da solução de Firewall de Rede de Próxima Geração (NGFW), incluindo suporte e assinaturas de segurança por 36 meses, com comissionamento da solução.

6 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Considerando a presente análise e a criticidade da demanda para a estratégia do TJMMG, declaramos viável a solução apontada, para renovação da solução de Firewall de Rede de Próxima Geração (NGFW), incluindo suporte e assinaturas de segurança por 36 meses e comissionamento da solução, nos termos descritos neste estudo.

Documento assinado eletronicamente por **WILLIAM MARCONDES DE FREITAS SANTOS**, **Analista Judiciário/Administrador de Redes**, em 16/08/2023, às 16:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **OTALINO GERALDINO SOARES JUNIOR**, **Analista Judiciário**, em 16/08/2023, às 16:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOANA EMÍLIA ROSA MEIRA**, **Assistente Judiciária**, em 22/08/2023, às 13:41, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://www.tjmmg.jus.br/servicos informando o código verificador **0271457** e o código CRC **41FD4A46**.