Estudo Técnico Preliminar 8/2023

1. Informações Básicas

Número do processo: 23060002324/2022-97

2. Descrição da necessidade

Este Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda de implantação de Firewalls, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

A constante modernização dos aparatos de Tecnologia da Informação e a evolução das aplicações da Internet trazem a necessidade da adoção de soluções de segurança da informação que garantam a integridade dos dados trafegados e armazenados dentro do ambiente de rede do IFS.

É incontestável, em termos técnicos, que o IFS precisa manter atualizada toda a sua infraestrutura de segurança da informação, visando proteger toda rede de dados com uma solução de firewall que atenda todas as demandas necessárias da instituição. Um simples acesso à internet pela comunidade do IFS pode sujeitá-los ao risco de trazerem softwares mal-intencionados (malwares) para rede local. Esses softwares podem causar interrupção do funcionamento dos computadores e, consequentemente, a interrupção de serviços administrativos executados pelos usuários da rede do IFS.

Firewalls são conjuntos de Softwares e Hardwares responsáveis por isolar o perímetro de uma rede de computadores, possibilitando um controle do tipo de tráfego que entra e que sai da mesma, além de gerenciar permissões de conteúdo e outras funcionalidades de segurança cibernética, tema basilar em uma boa gestão de TIC.

Um sistema de firewall de próxima geração funciona como um filtro eletrônico que examina o trafego da rede sinalizando quais operações de transmissão e recebimento de dados tem a possibilidade de serem executadas em determinado momento, garantido a integridade e a segurança dos dados pessoais ou corporativos. Além disso, o firewall evita que os usuários acessem conteúdos ilícitos, protegendo contra ameaças originadas deste tipo de conteúdo.

O firewall de próxima geração, além de impedir que hackers ou softwares mal-intencionados obtenham acesso indevido a uma rede ou computadores através da internet, também impede que um computador propague um software mal-intencionado para outros computadores

3. Área requisitante

Área Requisitante	Responsável
Diretoria de Tecnologia da Informação - DTI	Itauan Silva Eduão Ferreira

4. Necessidades de Negócio

Continuidade dos negócios;
Economia com ganho e crescimento de desempenho da rede da instituição, sem grandes saltos de investimentos com pessoal e capacitação;
Manter a disponibilidade, integridade e confiabilidade dos sistemas e aplicações da instituição;

Manter a integridade da imagem desta instituição;
Garantir uma infraestrutura segura para proteção dos dados institucionais;
Continuidade dos negócios;
Economia com ganho e crescimento de desempenho da rede da instituição, sem grandes saltos de investimentos com pessoal e capacitação;
Manter a disponibilidade, integridade e confiabilidade dos sistemas e aplicações da instituição;
Manter a integridade da imagem desta instituição;
Garantir uma infraestrutura segura para proteção dos dados institucionais.

5. Necessidades Tecnológicas

Atendimento de um número maior de dispositivos atendidos pela rede;
Gerenciamento através de interface Web e linha de comando (CLI);
Atendimento das demandas de desempenho dos serviços institucionais;
Gerenciamento unificado através de um único painel (gerenciador);
Gerenciamento microsegmentado do tráfego de rede.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

A Solução deve ser capaz de ser implementada, em caso de necessidade, por provisionamento zero-touch;
A solução deve ser capaz de ser gerenciada através de uma plataforma de gerenciamento;
A solução deve permitir acessos gerenciados através perfis com permissões distintas de acordo com um nível categorizado.
A solução deve permitir integração entre os itens que a compõe.

7. Estimativa da demanda - quantidade de bens e serviços

Atualmente a instituição faz uso do sistema de firewall da Fortinet, adquirido em 2017, e com base no sistema atual, a Instituição utiliza 11 Firewalls físicos, sendo que próxima aquisição ou renovação será feita nesta mesma quantidade acrescidos de 3 licenças de Firewalls virtuais para ambientes de Cloud, assim totalizam-se 14 Firewalls.

Objeto: Aquisição de Firewall e suporte técnico On-line para uso da solução de segurança		
Unidade do IFS	Métrica	Quantitativo
Reitoria	UND	02
Campus Aracaju	UND	01
Campus Socorro	UND	01
Campus Propriá	UND	01
Campus Tobias Barreto	UND	01
Campus Glória	UND	01
Campus São Cristóvão	UND	01
Campus Poço Redondo	UND	0
Campus Estância	UND	01
Campus Lagarto	UND	01
Campus Itabaiana	UND	01
Ambiente Cloud	UND	03
Total		14 UND

CAMPI	QUANTIDADE	OBS

Reitoria	2	Firewall da Matriz, onde será necessário mais de um firewall para manter redundância
CLOUD	3	São necessárias três licenças para os ambientes de nuvem.
Lagarto	1	Será somente um com SLA 24x7
Glória	1	Será somente um com SLA 24x7
Aracaju	1	Será somente um com SLA 24x7
Socorro	1	Será somente um com SLA 24x7
Itabaiana	1	Será somente um com SLA 24x7
Estância	1	Será somente um com SLA 24x7
Tobias	1	Será somente um com SLA 24x7
Própria	1	Será somente um com SLA 24x7

8. Levantamento de soluções

3.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

ID	Descrição da solução (ou cenário)

1	Aquisição de uma nova solução
2	Expansão da solução atual

SOLUÇÃO 1: Aquisição de uma Nova Solução

A aquisição de uma nova solução, em muitos casos, visa à economicidade e a renovação tecnológica de um parque de equipamentos. Sendo estes mais modernos e de maior capacidade de processamento.

A escolha por esta opção pode ser motivada, pelo fato que há fabricantes que cobram o suporte técnico e as atualizações aos seus sistemas operacionais através de subscrições, mensais ou anuais, o que acaba não sendo uma prática facilitadora para as instituições que realizam os planejamentos financeiros para aquisição de uma solução de forma anual e no ano subsequente, fica sem o devido suporte técnico básico, para as atualizações. Deixando assim os equipamentos sem correção de falhas, novas funcionalidades e até mesmo vulneráveis no quesito da segurança digital.

Muito embora exista um conjunto de protocolos abertos, conhecido como Ethernet e diversos fabricantes que atendem essa especificação, existe aqueles que conseguem se diferenciar. Esta diferenciação acontece de diversas maneiras, mas a principal delas é a característica ou facilidade de gerenciamento que a solução entrega.

SOLUÇÃO 2: Expansão da Solução Atual

O IFS possui um parque de soluções de rede da fabricante Fortinet. Estas soluções estão instaladas no ponto que a rede local é conectada à internet, assim todo o tráfego que entra ou sai para a internet passa pelo firewall. A infraestrutura de segurança da informação do Instituto Federal de Sergipe utiliza, atualmente, uma solução de firewall que atende aos requisitos de segurança de rede da instituição como: Solução baseada em appliance; A Solução de Segurança e Gerência de Redes NGFW em Cluster de Alta Disponibilidade, deve ser composto por no mínimo 02(dois) equipamentos ambos licenciados para operar em modo ATIVO-ATIVO. Está licenciado com as funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, Controladora Wireless e Virtualização; Firewall com capacidade mínima de processamento de 36(setenta) Gbps; IPS com capacidade mínima de processamento de 7 (treze) Gbps; Proteção a ameaças avançadas. interfaces Multiple 10 GE SFP+, GE SFP and GE RJ45,Onboard Storage 120 GB.

A renovação de soluções de segurança e equipamentos de rede é uma modalidade com grande aderência que os órgãos praticam para dar continuidade nos serviços com um mesmo fabricante de equipamento ou para aproveitar um legado já existente. Esta opção de solução possui grandes vantagens econômicas quando visa os investimentos feitos em sistemas (softwares) adquiridos para gerenciamento da solução e gastos feitos com a capacitação técnica da equipe de TI. E há também vantagens tecnológicas, sendo que algumas topologias de rede necessitam de um protocolo específico e poucos fabricantes possuem e aplicam este protocolo.

Levando em consideração o investimento já realizado em equipamentos, e que a equipe já é treinada nessa ferramenta, a continuidade deste serviço em fase as demais é vantajosa.

9. Análise comparativa de soluções

A existência de equipamentos de diferentes fabricantes implica em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessário a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações. Tal pensamento já foi manifestado no ACÓRDÃO 2789/2019 – PLENÁRIO do Tribunal de Contas da União (TCU), ao grafar:

“A falta de padronização das tecnologias afeta o acúmulo de conhecimento e a disseminação de boas práticas, o que poderia reduzir as necessidades de capacitação de pessoal e tornar a troca de experiências e movimentação de pessoal mais eficiente. Além disso, diminui a possibilidade de o Estado tirar proveito do efeito escala como grande comprador de tecnologia, aumentando a pressão sobre os custos. Por fim, dificulta a interoperabilidade entre os ambientes, tornando-se um incentivo perverso à criação de silos de informação, o que tanto emperra a integração de dados para a prestação de serviços públicos eficientes, sem contar com o esforço adicional que impõe às áreas de TI para lidar com tais complexidades.”

Outrossim, destacamos pontos relevantes no que tange à aspectos financeiros, técnicos e humanos, tal como expostas abaixo:

Financeira: Considerando-se que os equipamentos já adquiridos em 2017, e ainda em bom funcionamento, não seriam utilizados, o que ocasionaria mais custos com a compra de novos equipamentos, juntamente com a solução nova. Além disso, seria necessário e dispendioso cursos de treinamento para a equipe.

Técnica: Considerando-se que não seja possível a transferência de configurações para equipamentos de marcas distintas, sem a necessidade de alteração nas sintaxes das regras, o que impossibilita a substituição imediata, ocasionando maiores períodos de indisponibilidade em casos de falha.

Hoje a solução de firewall possui gerenciamento centralizado existente com o switch da core da instituição, esses equipamentos não terão compatibilidade com uma solução de outro fabricante, obrigando do IFS a adquirir uma nova ferramenta. Além do custo de aquisição, ainda existe o custo de operação e manutenção de mais uma ferramenta no Instituto Federal de Sergipe.

Outro fabricante ainda impediria a simples expansão da rede LAN (adição de novos switchs e licenciamento) e dificultaria ainda o estabelecimento de processos de gerência do equipamento, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Humana: Atualmente a equipe responsável pela administração da LAN e WLAN deste órgão conta com apenas 03 servidores, de forma que, ainda que fossem especializados separadamente estaríamos limitados a dois fabricantes, e mesmo assim não estaríamos garantindo a impessoalidade da equipe, sendo necessária a intervenção de um técnico específico de acordo com o fabricante do equipamento. Ficando ainda limitada a ação sempre que este mesmo técnico esteja ausente em razão dos afastamentos legais.

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X

	Solução 2			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

10. Registro de soluções consideradas inviáveis

Após análise técnica, financeira e humana, constatou-se que a SOLUÇÃO 1 - Aquisição de uma nova solução de FIREWALL é inviável, o que implica que a SOLUÇÃO 2 - Expansão da solução existente, é preferível.

11. Análise comparativa de custos (TCO)

5.1 – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Solução Viável 1
Descrição:
Expansão da Solução Atual
Custo Total de Propriedade – Memória de Cálculo
Custo Total: R$2.452.213,65 O valor acima é resultante da média de propostas enviadas por, no mínimo, três fornecedores, conforme pesquisa de preço, ANEXO I deste ETP.

5.2 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos				Total
	Ano 1	Ano 2	Ano 3	Ano 4	
Solução Viável 1 - Expansão da Solução Atual	R$2.452.213,65	R$ 0	R$ 0	R$ 0	R$2.452.213,65

Obs.: É importante esclarecer que o total é pretendido pelo prazo de vigência da ARP.

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas das soluções e observando seus benefícios, desvantagens e custos, a melhor e mais viável solução para o Instituto Federal de Sergipe é a SOLUÇÃO DE FIREWALL 2: Expansão da Solução Atual, pois além de melhor custo-benefício em questões técnicas apresentadas, atende na totalidade os requisitos esperados pela equipe de segurança da informação e necessidades do IFS.

13. Estimativa de custo total da contratação

Valor (R$): 2.452.213,65

A estimativa de custo total desta contratação é de R$2.452.213,65 (dois milhões, quatrocentos e cinquenta e dois mil, duzentos e treze reais e sessenta e cinco centavos).

14. Justificativa técnica da escolha da solução

Considerando que a Internet, a rede de dados e a mobilidade do IFS desempenham um papel crucial na missão institucional. O sistema de firewall possui componentes críticos para o bom funcionamento da rede e da produtividade dos colaboradores, pois além de impedir que hackers ou softwares mal-intencionados obtenham acesso indevido a uma rede ou computadores através da internet, também impede que um computador propague um software mal-intencionado para outros computadores.

A solução de firewall que o Instituto já possui, se mostrou eficiente e confiável desde a sua implementação, atendendo aos requisitos técnicos de performance, tendo em vista o alto volume de tráfego do Instituto, considerando ainda todos os requisitos de proteção contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises específica.

Outro aspecto importante que viabiliza a escolha dessa solução é o conhecimento que a equipe já possui, pois, não será necessário adquirir treinamentos para a equipe. Esses analistas possuem o conhecimento necessário para implementação de serviços de rede no NGFW. Caso fosse adquirida uma nova solução de outro fabricante, seria necessário que todos analistas que atuam diretamente no gerenciamento do NGFW realizassem novos treinamentos, ocasionando um custo adicional no valor final da contratação.

15. Justificativa econômica da escolha da solução

As soluções apresentadas nesse ETP foram avaliadas e, ainda que eventualmente apresentem preço de implantação substancioso em um primeiro momento, em médio e longo prazo trarão benefícios financeiros indiretos com a melhoria da prestação de serviços e execução dos processos institucionais.

16. Benefícios a serem alcançados com a contratação

Neste, pretende-se alcançar os seguintes resultados e benefícios:

1.

Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;

1.

Melhorar a qualidade e o *compliance* de segurança da informação

1.

Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

1.

Proteção do ambiente de rede contra ameaças tipo *Worms*, *vírus*, *malwares* entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.

1.

Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;

1.

Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);

1.

Simplificar a administração dos equipamentos;

1.

Minimização do esforço de aprendizagem por meio da padronização dos equipamentos;

1.

Garantia da segurança das informações que trafegam pela rede

17. Providências a serem Adotadas

As salas de equipamentos deverão possuir espaço para alocação dos novos Firewalls, disponibilizando a quantidade de U's (unidade de medida de espaços em racks) necessários para cada equipamento adquirido.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

As soluções aqui apresentadas, avaliadas e selecionadas consideram os pilares Financeiro, Técnico e Humano como critério de suas respectivas avaliações, portanto, as decisões foram tomadas com embasamento válido e relevante.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Despacho: Requisitante Técnico da Contratação

Documento assinado digitalmente
gov.br
DEMAIR DE SA RAMOS
Data: 11/04/2023 15:46:25-0300
Verifique em https://validar.iti.gov.br

DEMAIR DE SA RAMOS

Membro da comissão de contratação

Despacho: Diretor de TIC

MARCOS PEREIRA DOS SANTOS

Documento assinado digitalmente
gov.br
MARCOS PEREIRA DOS SANTOS
Data: 11/04/2023 16:29:01-0300
Verifique em https://validar.iti.gov.br

Documento assinado digitalmente
gov.br
ITAUAN SILVA EDUAO FERREIRA
Data: 11/04/2023 16:48:57-0300
Verifique em https://validar.iti.gov.br

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - TermoDeReferencia e Mapa de Rsicos Firewall.zip (154.93 KB)