Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Coordenação de Infraestrutura de TIC

HISTÓRICO DE REVISÕES			
Data	Versão	Descrição	Autor
25/04/2023	1.0	Finalização da primeira versão do documento	Equipe de Planejamento da Contratação
22/05/2023	2.0	Finalização da segunda versão (após revisão da CGL)	Equipe de Planejamento da Contratação

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. INFORMAÇÕES BÁSICAS

1.1 Número do processo: 08006.000158/2023-36

2. INTRODUÇÃO

2.1. Conforme previsto no artigo 11 da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019, a elaboração dos Estudos Técnicos Preliminares da Contratação serve essencialmente para definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição. A análise comparativa de soluções, deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

2.2. É na elaboração dos dos Estudos Técnicos Preliminares da Contratação que diversos aspectos devem ser levantados com maior profundidade para que os gestores se certifiquem, de que através de uma necessidade da área de negócio, claramente definida, há condições de atendê-la, tendo como premissa que os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente, além de embasar a elaboração do Termo de Referência ou o Projeto Básico, que somente é elaborado se a contratação for considerada viável.

2.3. A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da aquisição de equipamentos de rede de dados para a modernização e expansão da capacidade, incluindo novos ativos de camada de acesso, contemplando os serviços de instalação e suporte técnico com garantia pelo período de 60 meses para atendimento das necessidades do Ministério da Justiça e Segurança Pública (MJSP).

3. DESCRIÇÃO DA NECESSIDADE

3.1. VISÃO GERAL DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA E SEUS OBJETIVOS ESTRATÉGICOS:

3.1.1. O Ministério da Justiça e Segurança Pública (MJSP), órgão da Administração Pública Federal, tem, dentre outras, as competências para atuar no "combate ao tráfico de drogas e crimes conexos, inclusive por meio da recuperação de ativos que financiem ou sejam resultado dessas atividades criminosas", na "prevenção e combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo", na "coordenação de ações para combate a infrações penais em geral, com ênfase em corrupção, crime organizado e crimes violentos", na "coordenação e promoção da integração da segurança pública no território nacional, em cooperação com os entes federados", na "promoção da integração e da cooperação entre os órgãos federais, estaduais, distritais e municipais e articulação com os órgãos e as entidades de coordenação e supervisão das atividades de segurança pública" e, por fim, no "desenvolvimento de estratégia comum baseada em modelos de gestão e de tecnologia que permitam a integração e a interoperabilidade dos sistemas de tecnologia da informação dos entes federativos".

3.1.2. Atualmente o MJSP, é composto de várias unidades em sua estrutura:

- **Órgãos de assistência direta e imediata ao Ministro** (Assessorias Especiais, Gabinete do Ministro, Secretaria Executiva e Consultoria Jurídica);
- **Órgãos específicos singulares** (Secretaria Nacional de Justiça - SENAJUS, Secretaria Nacional do Consumidor - SENACON, Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos - SENAD, Secretaria Nacional de Segurança Pública - SENASP, Secretaria Nacional de Políticas Penais - SENAPPEN, Secretaria Nacional de Assuntos Legislativos - SAL, Secretaria de Acesso à Justiça - SAJU, Polícia Federal - PF, Polícia Rodoviária Federal - PRF);
- **Órgãos colegiados** (Conselho Federal Gestor do Fundo de Defesa dos Direitos Difusos - CFDD, Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual - CNPCP, Conselho Nacional de Políticas sobre Drogas - CONAD, Conselho Nacional de Política Criminal e Penitenciária - CNPCP, Conselho Nacional de Segurança Pública e Defesa Social - CNSP, Conselho Gestor do Fundo Nacional de Segurança Pública - CFNSP, Conselho Nacional de Imigração - CNI e Comitê Nacional para os Refugiados - CNR);
- **Entidade vinculada** (Conselho Administrativo de Defesa Econômica - CADE e Autoridade Nacional de Proteção de Dados - ANPD).

3.1.3. Como pode ser observado, a estrutura do MJSP é bastante considerável e complexa, possuindo diversas áreas de atuação que merecem tratamento diferenciado e proporcional às suas especificidades, tanto do ponto de vista de suas dimensões, quanto ao grau de sensibilidade e sigilo que as áreas necessitam para o desempenho de suas atividades.

3.1.4. Alguns temas sensíveis podem ser destacados de cada um dos Órgãos específicos singulares e de acordo com as competências do Ministério com base no decreto nº 11.348, de 01 de janeiro de 2023, como por exemplo:

Art. 14. À Secretaria Nacional de Justiça compete:

...

II - coordenar, em parceria com os órgãos da administração pública, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro - Enccla e outras ações do Ministério relacionadas com o enfrentamento da corrupção, da lavagem de dinheiro e do crime organizado transnacional;

III - coordenar a negociação de acordos e a formulação de políticas de cooperação jurídica internacional, civil e penal, e a execução dos pedidos e das cartas rogatórias relacionadas com essas matérias;

IV - coordenar as ações relativas à recuperação de ativos;

...

Art. 17. À Secretaria Nacional do Consumidor compete:

I - formular, promover, supervisionar e coordenar a política nacional de proteção e defesa do consumidor;

II - integrar, articular e coordenar o Sistema Nacional de Defesa do Consumidor;

...

X - receber e encaminhar consultas, denúncias ou sugestões apresentadas por consumidores, entidades representativas ou pessoas jurídicas de direito público ou privado;

...

Art. 20. À Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos compete:

I - assessorar e assistir o Ministro de Estado quanto às políticas sobre drogas relacionadas com a prevenção do uso indevido, a atenção e a reinserção social de usuários e dependentes de drogas, a redução da oferta e a repressão da produção não autorizada e do tráfico ilícito de drogas;

...

Art. 24. À Secretaria Nacional de Segurança Pública compete:

I - assessorar o Ministro de Estado: na articulação, na proposição, na formulação, na implementação, no acompanhamento e na avaliação de políticas, de estratégias, de planos, de programas e de projetos de segurança pública e defesa social;

II - estimular, propor, promover e coordenar a integração da segurança pública e defesa social no território nacional, em cooperação com os entes federativos, incluídas as organizações governamentais e não governamentais;

III - implementar, manter e modernizar redes de integração de banco de dados e de sistemas nacionais de informações de segurança pública e defesa social;

IV - coordenar e planejar as atividades da Força Nacional de Segurança Pública;

V - participar da elaboração de propostas de legislação em matérias relativas à segurança pública e defesa social;

VI - monitorar os riscos que possam impactar a implementação de políticas de segurança pública e defesa social e a consecução de seus objetivos;

VII - atuar no ciclo de gestão de recursos da segurança pública sob sua responsabilidade, em atividades de natureza técnica e finalística, em especial na propositura e na avaliação de políticas públicas e em seus instrumentos de implementação;

VIII - coordenar as atividades relacionadas à gestão dos recursos de segurança pública;

...

Art. 31. À Secretaria Nacional de Políticas Penais cabe exercer as competências estabelecidas nos art. 71 e art. 72 da Lei nº 7.210, de 11 de julho de 1984 - Lei de Execução Penal, e, especificamente:

I - planejar e coordenar a política nacional de serviços penais;

...

IV - prestar apoio técnico aos entes federativos quanto à implementação dos princípios e das regras da execução penal;

...

XII - promover a gestão da informação penitenciária e consolidar, em banco de dados nacional, informações sobre os sistemas penitenciários federal e dos entes federativos.

...

Art. 38. À Secretaria Nacional de Assuntos Legislativos compete:

I - promover o processo de articulação com o Congresso Nacional nos assuntos de competência do Ministério, observadas as competências dos órgãos que integram a Presidência da República;

II - providenciar o atendimento às consultas e aos requerimentos formulados, além de acompanhar a tramitação legislativa dos projetos de interesse do Ministério;

III - participar do processo de interlocução com os Governos estaduais, distrital e municipais, com as assembleias legislativas estaduais, com a Câmara Legislativa do Distrito Federal e com as câmaras municipais nos assuntos de competência do Ministério, com o objetivo de assessorá-los em suas iniciativas e de providenciar o atendimento às consultas formuladas, observadas as competências dos órgãos que integram a Presidência da República;

IV - auxiliar as comissões e grupos especiais de juristas constituídos pelo Ministro de Estado, com o objetivo de elaborar e consolidar leis; e

V - organizar e auxiliar as áreas temáticas nas consultas públicas de temas de competência do Ministério.

Art. 40. À Secretaria de Acesso à Justiça compete:

I - promover políticas públicas de modernização, aperfeiçoamento, transformação digital e democratização do acesso à justiça e à cidadania, inclusive no âmbito de plataformas digitais;

...

IV - promover ações para o aperfeiçoamento do sistema e da política de justiça, em articulação com os órgãos e as entidades dos Poderes Executivo e Judiciário e com o Ministério Público, a Defensoria Pública, a Ordem dos Advogados do Brasil, os órgãos e as agências internacionais e as organizações da sociedade civil;

...

VII - promover ações relacionadas ao Sistema de Justiça que contribuam para a redução da violência contra as mulheres, a população LGBTQIA+, os povos indígenas e as comunidades tradicionais e para o aprimoramento do Sistema de Justiça.

Art. 43. À Polícia Federal cabe exercer as competências estabelecidas no § 1º do art. 144 da Constituição, e, especificamente:

I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, além de outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, conforme previsto em lei;

II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas e o contrabando e o descaminho de bens e de valores, sem prejuízo da ação fazendária e de outros órgãos públicos, nas suas áreas de competência;

...

VI - acompanhar e instaurar inquéritos relacionados com direitos humanos e conflitos agrários ou fundiários e aqueles deles decorrentes, quando se tratar de crime de competência federal, além de prevenir e reprimir esses crimes.

Art. 58. À Polícia Rodoviária Federal cabe exercer as competências estabelecidas no § 2º do art. 144 da Constituição, no art. 20 da Lei nº 9.503, de 23 de setembro de 1997 - Código de Trânsito Brasileiro, no Decreto nº 1.655, de 3 de outubro de 1995, e, especificamente:

I - planejar, coordenar e executar o policiamento, a prevenção e a repressão de crimes nas rodovias e estradas federais e nas áreas de interesse da União;

II - exercer os poderes de autoridade de trânsito nas rodovias e nas estradas federais;

III - executar o policiamento, a fiscalização e a inspeção do trânsito e do transporte de pessoas, cargas e bens;

IV - planejar, coordenar e executar os serviços de prevenção de acidentes e de salvamento de vítimas nas rodovias e estradas federais;

...

3.1.5. Merecem também ser destacados os órgãos colegiados do Ministério, que atuam em temas sensíveis, e de importância nacional, como por exemplo o Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual (CNPCP). Esse órgão é a instância que trata do assunto pirataria no Brasil, sendo responsável pela aplicação de abordagens e metodologias inéditas para o tratamento da questão, elaborando diretrizes para a formulação e proposição de plano nacional para o combate à pirataria, à sonegação fiscal dela decorrente e aos delitos contra a propriedade intelectual.

3.1.6. Outro importante órgão colegiado é o Conselho Nacional de Políticas sobre Drogas - CONAD, sendo o órgão máximo brasileiro que regulamenta e pesquisa o uso de substâncias químicas e determina quais são drogas e quais não são e sua classificação. Este conselho também realiza campanhas de esclarecimento quanto às drogas e projetos como o de dano mínimo.

3.1.7. Destaca-se também o Conselho Nacional de Política Criminal e Penitenciária - CNPCP, que preconiza a implementação, em todo o território nacional, de uma nova política criminal e principalmente penitenciária a partir de periódicas avaliações do sistema criminal, criminológico e penitenciário, bem como a execução de planos nacionais de desenvolvimento quanto às metas e prioridades da política a ser executada.

3.1.8. O Ministério possui também em sua estrutura o Conselho Nacional de Segurança Pública e Defesa Social - CNSP, que tem o objetivo de propor diretrizes para prevenir e conter a violência e a criminalidade no País. O CNSP está previsto na lei nº 13.675, de 11 de junho de 2018, que instituiu o Sistema Único de Segurança Pública (SUSP) e a Política Nacional de Segurança Pública e Defesa Social (PNSPDS), o órgão será composto por representantes da União, dos estados, Distrito Federal, municípios e sociedade civil.

3.1.9. De acordo com o alinhamento ao plano estratégico institucional 2020-2023, o MJSP possui os seguintes objetivos estratégicos:

- **OE-PEI-01 -** Fortalecer o enfrentamento à criminalidade, com enfoque em crimes violentos, organizações criminosas, corrupção e lavagem de dinheiro, inclusive com atuação na faixa de fronteira;
- **OE-PEI-02 -** Promover o acesso à justiça e proteger os direitos do cidadão;
- **OE-PEI-03 -** Aperfeiçoar a coordenação estratégica e a integração dos órgãos de segurança pública;
- **OE-PEI-04 -** Aperfeiçoar a gestão do sistema prisional I;
- **OE-PEI-05 -** Promover a gestão e a alienação do produto de crimes;
- **OE-PEI-06 -** Ampliar a escala e a efetividade das ações de defesa da concorrência e do consumidor;
- **OE-PEI-07 -** Gerir políticas referentes aos povos indígenas;
- **OE-PEI-08 -** Aprimorar mecanismos de gestão do conhecimento e da preservação e difusão da memória arquivística nacional;
- **OE-PEI-09 -** Promover a valorização e o desenvolvimento dos servidores;
- **OE-PEI-10 -** Aprimorar e integrar a gestão e a governança institucional;
- **OE-PEI-11 -** Fortalecer e ampliar a estrutura e os serviços de TIC (Finalidade: Avaliar se os serviços de TIC considerados estratégicos estão em operação conforme acordado, quais sejam: 1) E-mail; 2) SEI; 3) mj.gov.br; 4) Rede Local; e 5) Acesso à Internet.);

3.1.20. Para que todos os órgãos da estrutura do Ministério possam atuar de maneira eficiente e eficaz, e com os recursos necessários para o pleno desenvolvimento de suas atividades, **são necessários mecanismos tecnológicos que sejam capazes de gerar valor e entregar as informações necessárias, de forma a permitir a produção de conhecimento útil e tempestivo à tomada de decisão**, seja em nível estratégico, tático ou operacional.

3.1.21. Uma unidade crucial para que o MJSP cumpra suas funções e missão é a Subsecretaria de Tecnologia da Informação e Comunicações - STI, criada por meio do DECRETO Nº 11.348, DE 1º DE JANEIRO DE 2023, que é responsável direta pelo planejamento, coordenação e execução das atividades relacionadas com o SISP no âmbito do Ministério, além de articulação com os órgãos centrais, elaborando e consolidando planos e programas de sua competência:

...

Art. 12. À Subsecretaria de Tecnologia da Informação e Comunicação compete:

I - planejar, coordenar e supervisionar a execução das atividades relacionadas com o Sistema de Administração dos Recursos de Tecnologia da Informação no âmbito do Ministério;

II - promover a articulação com os órgãos centrais do sistema federal referido no inciso I e informar e orientar os órgãos integrantes da estrutura do Ministério e da entidade a ele vinculada quanto ao cumprimento das normas estabelecidas;

III - elaborar e consolidar os planos e os programas das atividades de sua área de competência e submetê-los à decisão superior; e

IV - acompanhar e promover a avaliação de projetos e atividades, no âmbito de sua competência.

...

3.1.32. A busca por evolução dos serviços de informática vem resultando em mudanças no perfil de tráfego de suas aplicações internas e externas, exigindo uma revisão da arquitetura de ativos de segurança atualmente em funcionamento, requerendo dos equipamentos maiores taxas de transmissão e maior poder de processamento.

3.1.33. Tal implementação requer uma maior interatividade da parte de procedimentos de configuração, desempenho e qualidade, bem como a total interoperabilidade, visando uniformização dos recursos como um todo.

3.1.34. Nesse sentido, a adoção de tecnologias modernas e inovadoras, como solução de Firewall de alto desempenho, deixaram de ser uma tendência e passaram a ser uma realidade na Administração Pública Federal – APF, que deve estar alinhada às modernas e eficientes práticas do mercado.

3.1.35. Os Firewalls possuem funções fundamentais em uma rede de TIC, podendo evitar que pacotes indesejados e prejudiciais tenham acesso à rede interna e, portanto, às informações e recursos em posse da mesma. Assim também, os "filtros" implementados por esses equipamentos evitam que *hosts* internos tenham acesso a domínios e informações que não condizem com a política de segurança da rede.

3.1.36. Além disso, é um dos mecanismo de segurança utilizados para proteger a rede computacional contra acessos indevidos, através da identificação, análise, bloqueio, isolamento e tratamento das rotas de rede utilizadas pelo usuários e pelos sistemas computacionais sob responsabilidade do MJSP, além do gerenciamento das atividades que envolvam ameaças relacionadas à configuração de rotas. Com isso, diminui-se o risco de acessos indevidos aos sistemas do MJSP enquanto o desempenho geral da rede é otimizado através do gerenciamento mais eficaz do roteamento dos ativos de TI do órgão.

3.1.37. Existem muitas vantagens em manter uma solução de *Firewall* com poder de processamento robusto, com altas taxas de transmissão e em um ambiente de TIC totalmente coberto com suporte e garantia, cabendo destaque para os listados abaixo:

a) Manutenção da integridade dos dados;

b) Maior controle do acesso às informações;

c) Manutenção da integridade da rede;

d) Melhora a segurança da rede;

e) Proteção contra malwares;

3.1.41. Além dessas vantagens consideradas essenciais, deve-se observar os riscos que o MJSP correrá caso opte em não utilizar uma solução de *Firewall*:

a) **Comprometimento dos dados** - trata-se de um incidente de segurança em que dados pessoais e/ou informações privadas e sigilosas podem ser expostos publicamente ou a terceiros sem autorização.

b) **Sujeição aos ataques dos cibercriminosos** - atualmente, com o alto fluxo de informação, gera-se um aumento significativo de ataques, espionagem e roubo de dados cibernéticos. Ou seja, a maior conectividade trouxe com ela a maior exposição a risco e Malwares diversos, completamente dispersos pela rede ou tecnicamente planejados para atacar órgãos específicos.

c) **Comprometimento da integridade da rede** - acessos indevidos à rede podem ocorrer, afetando assim a garantia da integridade dos dados e informações essenciais.

d) **Descontrole da autorização de acesso às informações** - As políticas de segurança coincidem com as regras aplicadas no firewall, ditam as regras de permissões e proibições de acesso que um *firewall* deve implementar.

3.1.42. Em virtude dos aspectos abordados, é de fundamental importância a abordagem e entendimento da arquitetura atual da solução de firewall e sua topologia aplicada à rede do MJSP, assim como o entendimento do escopo dos projetos de segurança em infraestrutura realizados ao longo dos anos.

3.2. ATUAL ARQUITETURA DA SOLUÇÃO DE FIREWALL NA TOPOLOGIA DE REDE

3.2.1. Na atual conjuntura, a estrutura de Tecnologia da Informação do Ministério vem passando por mudanças de disposição física em suas unidades, o que tem provocado a necessidade de aquisição de equipamentos, processos de automatização e alta disponibilidade que suportem este dinamismo.

3.2.2. A atual plataforma de ativos de rede do MJSP, formada pela rede do núcleo central, é composta por três camadas:

- Camada Central;
- Camada de Distribuição e
- Camada de Acesso.

3.2.3. A Camada Central abriga os switches do tipo core, que são equipamentos de alto desempenho, os quais devem ser robustos para suportarem grande tráfego de pacotes. A arquitetura desta camada deve proporcionar alto grau de disponibilidade, capacidade, redundância e resiliência.

3.2.4. A Camada de Distribuição é responsável pela interconexão entre a camada Central e de Acesso, sendo responsável pela concentração dos pacotes de dados oriundos da Camada de Acesso para encaminhamento à Camada Central. A Camada de Distribuição controla o fluxo do tráfego da rede usando políticas e determina domínios de broadcast, realizando funções de roteamento entre VLANs, além de conectar os pontos de acesso da rede sem fio (APs).

3.2.5. A Camada de Acesso é a camada de switches mais próxima das máquinas dos usuários, sendo que os equipamentos ativos desta camada captam os pacotes de dados oriundos das máquinas de usuários, impressoras, telefones VoIP e outros equipamentos da ponta, e os encaminham à Camada de Distribuição. O principal propósito da camada de acesso é fornecer um meio de conectar dispositivos à rede e controlar quais têm permissão de comunicação na rede.

3.2.6. Dentre os projetos de aquisição de equipamentos para essas camadas, o de reestruturação e modernização de ativos de rede da Camada Central (Core), se relaciona diretamente com funcionamento da solução de firewall, pois trouxe inovação para os Data Centers do MJSP (Primário e Secundário), e ainda teve por objetivo a inserção da estrutura *Spine-Leaf,* a qual consiste em uma espinha dorsal formada pelo SPINE e os LEAFs, que servem de entrada dos diversos subsistemas de rede. A arquitetura proposta forma um único *Fabric,* que funciona de forma redundante em camada 3 (três) e com a utilização de roteamento dinâmico interno ao Data Center.

3.2.7. Nesse contexto, a topologia da Camada Central (Leaf Serviços) e topologia de Firewall implantada nos Data Centers do MJSP (Primário e Secundário) são divididas conforme imagem abaixo:

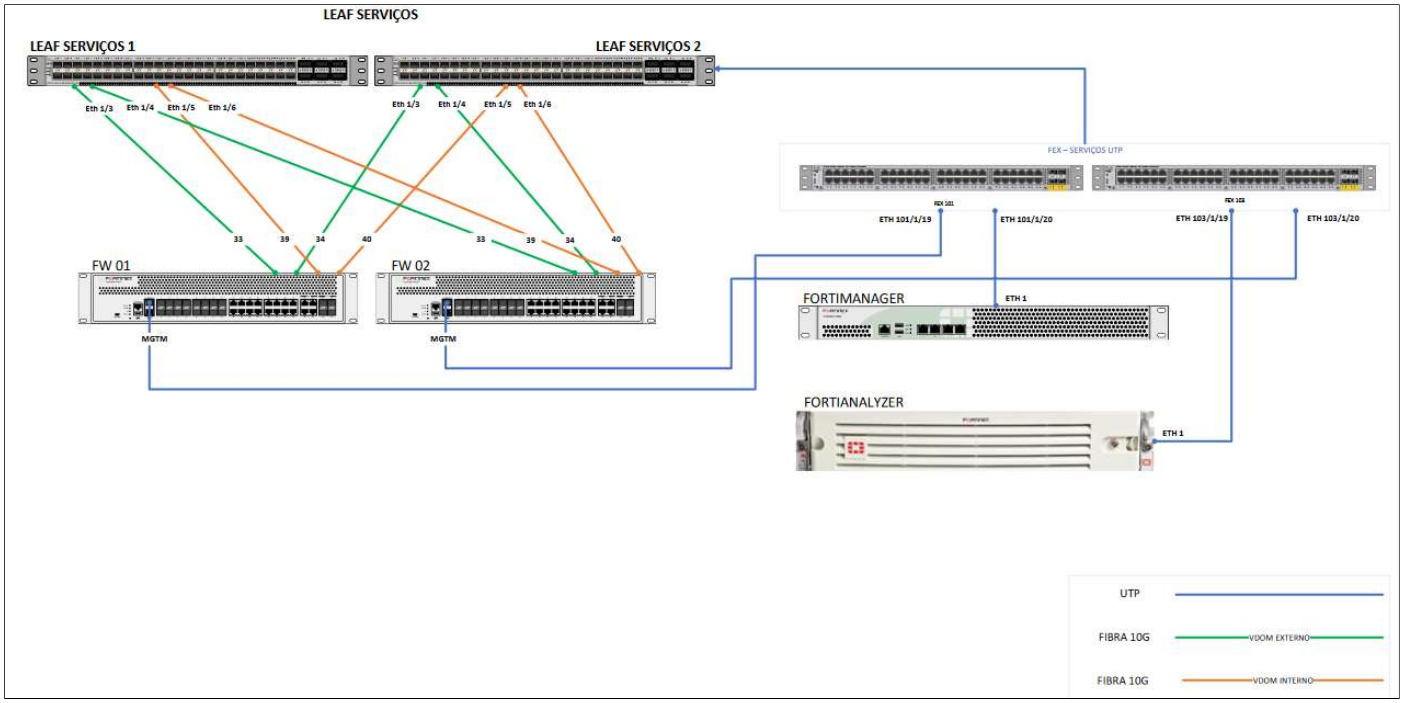

Figura 1 – Arquitetura da solução de firewall na topologia de rede

3.2.8. Na figura acima, encontra-se a solução de Firewall ligada ao Leaf de Serviços (que é a estrutura responsável por receber instalações de equipamentos relacionados aos serviços diversos de TIC, como Wireless, SERPRO, Load Balance, Videoconferência, etc.) com velocidade de link de 10 Gbps.

3.2.9. A estrutura de firewall do Ministério é composta pelos equipamentos instalados nos 2 (dois) Data Centers do MJSP, além de equipamentos localizados nas 05 (cinco) Penitenciárias Federais (Catanduvas (PR), Campo Grande (MS), Mossoró (RN), Porto Velho (RO) e Brasília (DF)). Importante salientar, que, a topologia de redes difere das implantada no MJSP e CICCN, tendo em vista que a rede de uma Penitenciária federal é menos complexa, utilizando somente switches de distribuição para ligar os equipamentos de firewall. Então, em cada Penitenciária foi instalado um Appliance Físico, contemplando assim 5 "caixas" desses ativos no total.

3.2.10. A tabela abaixo apresenta o quantitativo atual de equipamentos que atende a todo o MJSP (Data Centers Primário, Secundário e Penitenciárias):

Solução de Firewall Atual		
Descrição	**Tipo**	**Quantidade**
Appliance de Firewall para uso nos Datacenters do MJSP	Unidade	04
Appliance de Firewall para uso nas Penitenciárias Federais	Unidade	05
Appliance para análise do tráfego de dados para uso nos Datacenters do MJSP	Unidade	01
Appliance de gerenciamento centralizado para uso nos Datacenters do MJSP	Unidade	01

3.2.11. Esses equipamentos de Firewall foram adquiridos por meio do processo 08006.001190/2016-18, tendo o suporte e garantia prazos de expiração em 28/06/2023, o que requer atenção especial com a elaboração de pesquisas e análises de soluções voltadas ao atendimento da necessidade, considerando inicialmente algumas soluções como, manter a solução atual (renovando apenas o suporte e garantia), utilizar uma solução de firewall em software livre ou realizar a aquisição de uma solução por completo, sendo essas análises realizadas ainda neste estudo.

3.2.12. Outro fator importante em adquirir uma solução robusta e com alto desempenho, é a necessidade observada de utilizar links de internet redundantes em algumas unidades do MJSP, destacando-se as Penitenciárias Federais.

3.2.13. Atualmente, para a interligação das Penitenciárias Federais à infraestrutura do Ministério, é utilizada a tecnologia MPLS (Multiprotocol Label Switching, ou "Comutação de Rótulos Multiprotocolo") que é uma tecnologia de rede usada, em geral, por empresas a fim de conectar suas unidades remotas, ou por provedores de internet para a segmentação de tráfego de layer 2 e layer 3. A empresa contratada para fornecimento do MPLS é a Telebrás, sendo que o contrato prevê dupla abordagem de links, ou seja, um por fibra óptica outro por meio sem fio. Apesar disso, diversos incidentes na rede foram registrados nos anos de 2022 e agora em 2023, ocasionando que sistemas importantes para a segurança pública ficassem indisponíveis.

3.2.14. O quantitativo de incidentes foram relacionados e podem ser observados na imagem abaixo:

Incidentes TELEBRÁS			
Localidades	**Anos**		
Rótulos de Linha	**2022**	**2023**	**Total Geral**
Fortigate Forca Nacional Gama	37	35	72
PFBSB_CORE	23	31	54
Roteador_Telebras_Concentrador_MPLS_MJ_Brasilia	7	18	25
Roteador_Telebras_Concentrador_MPLS_MJ_Brasilia_Secundario	8	15	23
SW_CORE_CAMPO_GRANDE_172.22.16.10	18	34	52
SW_CORE_CATANDUVAS_172.22.80.10	31	34	65
SW_CORE_MOSSORO_172.22.144.10	63	58	121
SW_CORE_PORTO_VELHO_172.22.208.10	36	32	68
Total Geral	**223**	**257**	**480**

3.2.15. Sendo assim, percebe-se que foram 480 (quatrocentos e oitenta) incidentes relacionados à solução de internet/MPLS da Telebrás, contando todas as unidades do MJSP. Esta situação de recorrentes indisponibilidades traz transtornos e perdas consideráveis incalculáveis, levando em conta todos os

sistemas e serviços que estão afetados e deixando de ser prestados à população. Cabe destacar que muitos dos incidentes ocorrem em decorrência da Telebrás terceirizar a última milha do link, tendo em vista a capilaridade da operadora não chegar em algumas localidades.

3.2.16. Dito isso, a equipe de planejamento da contratação está analisando a possibilidade de implementação, em um futuro próximo, da tecnologia SD-WAN (WAN definida por software), com o objetivo de aumentar a disponibilidade, a velocidade do link e diminuir os custos com links MPLS. Vários benefícios podem ser elencados da SD-WAN em comparação com o MPLS, como por exemplo:

a) As **SD-WANs não dependem de hardware especializado**. As MPLS requerem a configuração de roteadores especializados para encaminhar pacotes corretamente. As SD-WANs podem ser executadas usando qualquer hardware de rede.

b) As **SD-WANs não têm limites de largura de banda inerentes**. Como as conexões MPLS são mais ou menos definidas (a menos que sejam reconfiguradas), há um limite rígido sobre quanta capacidade pode ser provisionada em uma conexão MPLS de uma só vez . As conexões SD-WAN podem adicionar capacidade conforme necessário, combinando várias conexões e aproveitando a conectividade mais rápida disponível.

c) As **SD-WANs são independentes do provedor de serviços**. As MPLS exigem que as organizações usem a mesma operadora em todos os sites conectados por WAN porque as conexões MPLS precisam ser configuradas em roteadores físicos na rede adjacente. As conexões SD-WAN são executadas pela internet comum; qualquer provedor pode ser compatível com uma conexão SD-WAN.

d) O **roteamento SD-WAN é mais flexível**. A SD-WAN pode aproveitar várias opções de conectividade, incluindo conexões de internet de banda larga, linhas privadas e 5G. Ela pode direcionar o tráfego e o failover entre todas as opções de conectividade disponíveis. Os serviços de MPLS normalmente exigem conexões de linha privada dedicadas do provedor de serviços.

e) As **SD-WANs se integram mais facilmente com a nuvem**. Conectar-se à nuvem via MPLS é um serviço especializado oferecido por alguns provedores de serviços MPLS para alguns provedores de nuvem. Com a MPLS, a conexão com a nuvem requer a construção de uma rota direta para a infraestrutura desse provedor de nuvem.

3.2.17. Diante dos motivos expostos e das necessidades apresentadas, se faz necessário uma análise sobre as possíveis soluções no mercado para a modernização e expansão da capacidade, incluindo novos appliances físicos de firewall, além de contemplar os serviços de instalação, suporte técnico e garantia.

4. ÁREA REQUISITANTE

Área Requisitante	Responsável
Coordenação-Geral de Infraestrutura e Serviços de TIC	Rodrigo Albernaz Bezerra

5. NECESSIDADES DE NEGÓCIO

ID	Principais necessidades de negócio
1	Reestruturar e modernizar a arquitetura de firewall do Ministério, provendo aquisição de equipamentos robustos e confiáveis.
2	Suportar o aumento no número de usuários e prestação de serviços a estes de maneira rápida, segura e eficaz.
3	Suportar a crescente demanda por conectividade de rede, internet e acesso a sistemas internos que estão hospedados em nuvem.
4	Garantir a continuidade dos negócios do MJSP por meio de melhorias, apoio técnico e manutenções da solução a ser adquirida.
5	Prover a mitigação de impactos para as áreas de negócios decorrentes de problemas no funcionamento dos equipamentos de segurança
6	Aumentar a segurança por meio da ativação novas funcionalidade técnicas à nova solução
7	Prover solução de firewall eficiente com a atualização dos ativos deste Ministério.

Tabela 1 **- Necessidades de negócio**

6. NECESSIDADES TECNOLÓGICAS

ID	Principais necessidades tecnológicas
1	Manter a integridade da rede em conjunto com a integridade dos dados
2	Permitir gestão centralizada de todos dos dispositivos de segurança e borda da rede das unidades remotas (Penitenciárias), otimizando o monitoramento do uso da rede local do MJSP, agilizando a recuperação de desastres (disaster recovery).
3	Assegurar estabilidade da rede e dos sistemas frente à ampliação da infraestrutura de rede existente nas Unidades do MJSP
4	Manter a compatibilidade tecnológica do parque de ativos de segurança em funcionamento na rede do Ministério
5	Prover maior proteção contra malwares;
6	Atender prontamente ao aumento de novos serviços online e em nuvem prestados pelo MJSP e na melhoria do acesso à Internet nas Unidades Penitenciárias
7	Garantir a continuidade da conexão da VPN entre o MJSP e diversas localidades e serviços
8	Assegurar disponibilidade entre links de internet em unidades do MJSP

Tabela 2 **- Necessidades tecnológicas**

7. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

ID	Demais requisitos necessários e suficientes à escolha da solução de TIC
1	Prover segurança da informação ao acessar os equipamentos e serviços do Ministério.
2	Arquitetura tecnológica de segurança compatível com a utilizada atualmente.

Tabela 3 **- Demais requisitos**

8. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Solução de Firewall		
Descrição	**Tipo**	**Quantidade**
Appliance de Firewall para uso nos Datacenters do MJSP	Unidade	04
Appliance de Firewall para uso nas Penitenciárias Federais	Unidade	05
Appliance para análise do tráfego de dados para uso nos Datacenters do MJSP	Unidade	01

Appliance de gerenciamento centralizado para uso nos Datacenters do MJSP	Unidade	01

Tabela 4 - Estimativa da Demanda

9. LEVANTAMENTO DAS SOLUÇÕES

9.1. **Solução 1 - Contratação de serviço de garantia e suporte técnico para a solução atual.**

9.1.1. O presente cenário tem o objetivo de analisar a possibilidade da contratação dos serviços de manutenção e suporte para os equipamentos existentes verificando sua viabilidade.

9.2. **Solução 2 - Contratação de toda uma solução em Software Livre.**

9.2.1. O presente cenário tem o objetivo de demonstrar a contratação por meio da instalação, configuração e mudança de todo o ambiente de firewall para uma solução de software livre.

9.3. **Solução 3 - Contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses.**

9.3.1. O presente cenário tem o objetivo de demonstrar a solução por meio da aquisição e modernização por completo da solução de firewall dos atuais ambientes do MJSP. O objetivo principal da análise é a possibilidade de aquisição de novos appliances, expandindo e reestruturando arquitetura de segurança do MJSP, de forma a dar continuidade às melhorias com uma topologia moderna, escalável e de alto desempenho.

10. ANÁLISE COMPARATIVA DE SOLUÇÕES

10.1 **Solução 1 - Contratação de serviço de garantia e suporte técnico para a solução atual.**

10.1.1. Atualmente, o Ministério da Justiça e Segurança Pública possui uma solução de Firewall adquirida através do Processo 08006.001190/2016-18, composta por 04 (quatro) equipamentos do modelo FortiGate 1500D, sendo que 02 (dois) desses equipamentos estão instalados no datacenter primário e 02 (dois) instalados no datacenter secundário do MJSP, além de 05 (cinco) equipamentos do modelo FortiGate 500D, instalado em cada uma das cinco Penitenciárias que compõem o Sistema Penitenciário Federal, localizadas em Catanduvas (PR), Campo Grande (MS), Mossoró (RN), Porto Velho (RO) e Brasília (DF).

10.1.2. Também faz parte da solução atual, 01 (um) equipamento de Gerenciamento de Firewall, modelo FortiManager 200D, responsável por controlar todos os produtos adquiridos, permitindo o gerenciamento centralizado de todos os equipamentos de Firewall.

10.1.3. Por fim, a solução atual também possui 01 (um) equipamento de relatório de Firewall, modelo FortiAnalyzer 1000E, responsável por coletar e armazenar os dados gerados pelos equipamentos de Firewall, permitindo realizar a análise do tráfego de dados a partir de relatórios customizados.

10.1.4. O fabricante dos equipamentos já estabeleceu datas específicas para descontinuidade de todos os produtos que compõem a solução atual (*end of life*) do MJSP, conforme consta na tabela 5.

Modelo	Data de descontinuidade	Link SEI
FortiGate 1500D	31/12/2026	23806105
FortiGate 500D	08/05/2023	23806064
FortiManager 200D	03/12/2024	23806087
FortiAnalyzer 1000E	22/03/2025	23806042

Tabela 5 - Data de descontinuidade (end of life) dos equipamentos que compõem a solução de Firewall atual

10.1.5. Diante disso, observa-se que os equipamentos FortiGate 500D, FortiAnalyzer 1000E e FortiManager 200D atingirão o *end of life* em breve, estando, dessa forma, desatualizados tecnologicamente. Logo, há um comprometimento na contratação de garantia e suporte para esses equipamentos, caracterizando-se como uma solução sem sustentabilidade a médio e longo prazo.

10.1.6. Cabe destacar, que além do fato dos referidos equipamentos se encontrarem em estado de obsolescência, estando descontinuados pelo fabricante, ainda é importante considerar as Boas Práticas e Acórdãos que tratam sobre o tema para embasar de forma positiva ou negativa o cenário proposto.

10.1.7. Nessa linha, existem as BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4 (Link), do Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação do STI/MP, que cita a contratação de manutenção dos ativos de TIC fora de garantia como mais onerosa para a Administração Pública, assim como define o ciclo de vida para esses equipamentos:

> *"....*
>
> *1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de* ***manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração*** *do que quando o bem é adquirido com garantia para toda sua vida útil. (grifo nosso)*
>
> *"....*
>
> *1.4. ORIENTAÇÕES ESPECÍFICAS SOBRE CICLO DE VIDA*
>
> 1.4.5. SERVIDORES DE REDE, APLICAÇÃO, EQUIPAMENTOS DE BACKUP, ARMAZENAMENTO, **SEGURANÇA**, ENTRE OUTROS
>
> 1.4.5.1. Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, **segurança**, entre outros, deve-se considerar o tempo de vida útil mínimo de **5 (cinco) anos** para fins de posicionamento da tecnologia e de garantia de funcionamento.*(grifo nosso)*

10.1.8. Assim como a apreciação da Egrégia Corte de Contas que exarou entendimento no sentido de condenara prática de atualizações tecnológicas em detrimento da aquisição de novos equipamentos. Para ilustrar cita-se o Acórdão TCU nº 2400/2006 que assim discorreu sobre os serviços de atualização tecnológica e suporte técnico:

"Acórdão TCU n. 2400/2006 – Plenário

> *"...*
>
> *2.9.2.4 .... do ponto de vista técnico, o fato de existir garantia para os equipamentos que sofrerem atualização nos mesmos níveis que os prestados a equipamentos novos não garante vantagem técnica ao upgrade. Pelo contrário, não se pode esperar que um servidor em gabinete desmontado e remontado em um rack com substituição de quase todos os componentes (ver listagem dos componentes que serão substituídos à fl. 70 do anexo 2), com a permanência de alguns componentes antigos, possa ter menor probabilidade de falha que um equipamento novo que, dependendo do fornecedor, pode ser montado e testado em fábrica. A garantia não diminui o risco de falha e necessidade de substituição de componentes (mais provável no caso do upgrade do que no caso de aquisição de novos servidores), caso em que os equipamentos, mesmo que por pouco tempo, permaneceriam indisponíveis. "*

"...

10.1.9. Uma observação importante também, é quanto aos equipamentos FortiGate 1500D, com data de descontinuidade em 31/12/2026, pois trata-se de equipamentos que na topologia atual (ligados nos Datacenter primário e secundário) já não atendem satisfatoriamente, conforme mencionado Nota Técnica 23657316:

> "...
>
> Diante do exposto, verifica-se que a capacidade do equipamento de Firewall do núcleo central do MJSP encontra-se próximo do seu limite máximo, representando um risco à segurança das informações sob responsabilidade do MJSP e à disponibilidade dos seus serviços.
>
> Além disso, é possível verificar que a ferramenta FortiAnalyzer também está operando próximo ao seu limite, contribuindo para aumentar os riscos à segurança da informação do MJSP.
>
> Cabe ressaltar que esses fatores decorrem do crescimento da rede do MJSP, que passou a disponibilizar mais serviços através da internet e do aumento de usuário que utilizam a internet para acessar tais serviços.
>
> Ao avaliar os resultados obtidos pela presente análise, constata-se a necessidade da substituição da solução atual de Firewall por uma de maior porte, para atender tanto às necessidade atuais do MJSP, quanto às expectativas de crescimento de sua rede computacional, de modo a garantir o correto controle sobre os acessos aos dados armazenados e trafegados pelo MJSP e evitar possíveis indisponibilidade de seus serviços.
>
> "...

10.1.10. Cabe destacar, que ao longo dos últimos anos, houve um crescimento expressivo da infraestrutura do Ministério devido à grande quantidade de projetos e aplicações que entraram em produção. Além disso, houve um aumento na utilização da nuvem e sua gama de aplicativos colaborativos, fato que sobrecarrega o tráfego, e sua capacidade de análise pelas ferramentas de segurança.

10.1.11. Essa sobrecarga nas soluções de segurança geram um consumo excessivo de recursos dos equipamentos, gerando a impossibilidade de analisar o tráfego de rede por completo, resultando em falhas de conexão à rede interna e externa do MJSP, além do risco de acessos indevidos a informações sensíveis sob a responsabilidade do MJSP. Sendo assim, os equipamentos de firewalls estão frequentemente entrando em um estado chamado de "*conserve mode*", que é uma proteção do próprio sistema pelo consumo excessivo de processamento. Importante salientar que o estado de "*conserve mode*", impacta o funcionamento geral da rede, gerando incidentes massivos para os usuários.

10.1.12. Para avaliar o desempenho destes Firewalls, foram realizadas duas medições, uma no dia 23/11/2022 às 9:00 horas (Figura 1) e outra no dia 29/11/2022 às 16:00 horas (Figura 2). Em ambas as medições, é possível verificar que o consumo médio de CPU alcança, respectivamente, 85,4% e 81,9% do limite da ferramenta.

10.1.13. Em uma situação de maior acesso aos serviços do MJSP ou no caso de um possível ataque cibernético, esse consumo pode alcançar valores que ultrapassam o limite da solução, podendo resultar em indisponibilidades de sistemas ou acesso indevido aos dados sob responsabilidade do MJSP, conforme imagens extraídas da solução:

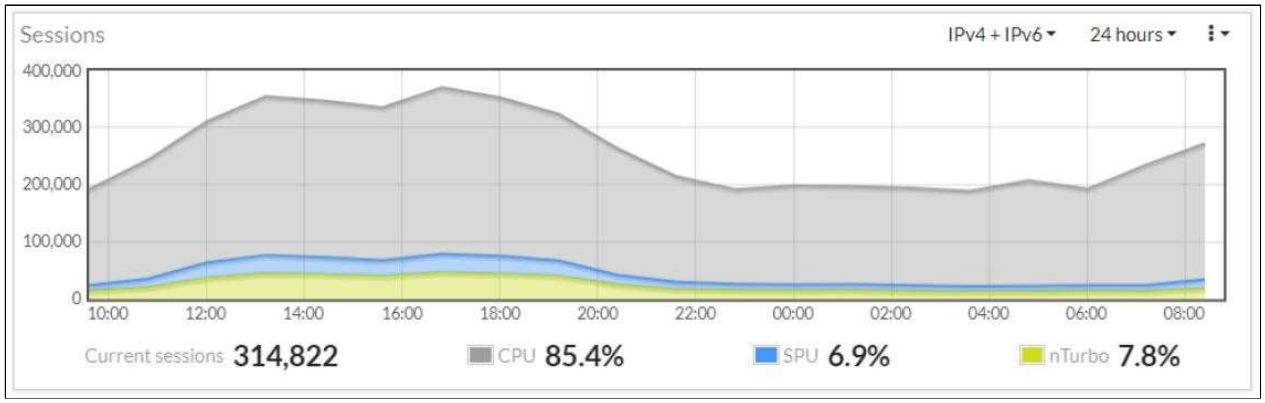

Figura 2 – Número de conexões e consumo de CPU e SPU do Firewall do núcleo central – Medição 01

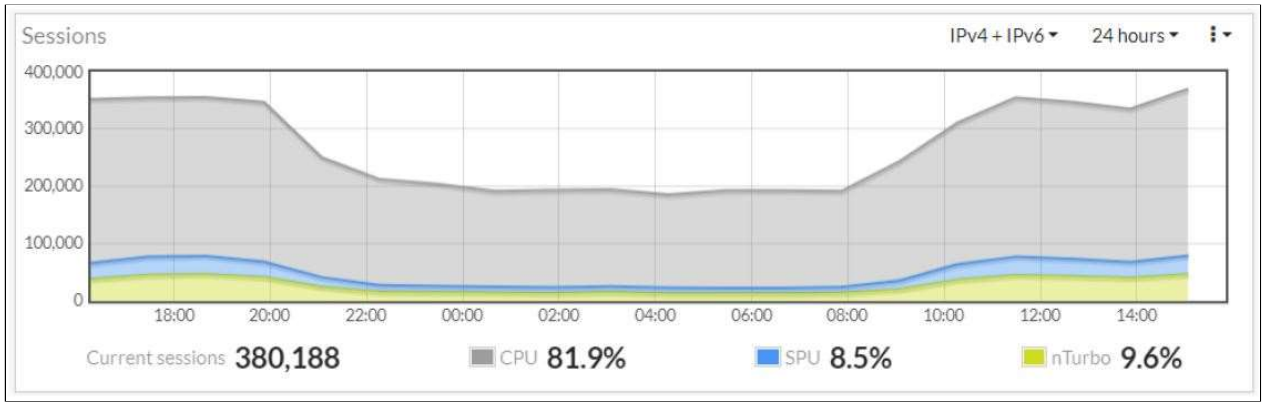

Figura 3 – Número de conexões e consumo de CPU e SPU do Firewall do núcleo central – Medição 02

10.1.14. Diante o exposto, a equipe de planejamento contratação entende que a contratação de serviço de garantia e suporte técnico para os ativos existentes, considerando a topologia atualmente implementada, o consumo elevado do tráfego de rede, as boas práticas, orientações e vedações para contratação de ativos de TIC e o acórdão TCU *n. 2400/2006,* **não é uma solução viável**, pois também implica em risco elevado para a operação dos serviços críticos de tecnologia da informação providos pelo MJSP devido à indisponibilidade de suporte aos equipamentos por parte do fabricante.

10.2. Solução 2 - Contratação de toda uma solução em Software Livre.

10.2.1. O presente cenário tem o objetivo de demonstrar uma possível utilização de solução em Software Livre nos atuais ambientes do MJSP (sede), CICCN-DF e Penitenciárias Federais . A disposição principal da análise é a viabilidade de implementação de toda uma solução de software livre, inclusive com suporte e garantia, de forma a tentar concretizar uma topologia de firewall moderna, escalável e de alto desempenho.

10.2.2. Nessa linha de soluções, destaca-se algumas forças e fraquezas observadas caso se implemente a solução em Software Livre:

Forças	Fraquezas
Open-Source	Interface não muito intuitiva
Permite a instalação de pacotes extras;	Demanda um conhecimento mais aprofundado para explorar suas funcionalidades
Execução de serviços como VPN, regras de NAT, geração de chaves RSA e monitoramento de tráfego	Suporte básico
Sistema leve	Necessário capacitação da equipe com frequência para configurações
	Funciona bem em pequenas e médias empresas
	Necessário Hardware adequado do cliente para sua instalação
	Necessário atualização e monitoramento tempestivos dos plugins por meio das comunidades

Tabela 6 - Forças e Fraquezas na Utilização de Solução em Software Livre

10.2.3. Apesar da solução possuir qualidades como ser Open Source (código projetado para ser acessado abertamente pelo público), permitir a utilização de VPN, NAT, chaves de segurança e ainda ser considerado um sistemas leve, há bastante fraquezas e necessidades específicas do MJSP que não são supridas pela solução.

10.2.4. Destaca-se nisso que a solução como um todo não possui nativamente uma empresa especializada/fabricante para manter a solução e prestar suporte especializado, sendo necessário aguardar a "comunidade" disponibilizar as atualizações sempre que considerar oportuno.

10.2.5. Além disso, a solução é disponibilizada, geralmente, em appliances virtuais, necessitando de servidores de processamento e espaço de armazenamento de dados nos nossos Datacenters e Penitenciárias para realizar a instalação e configuração. Nisso, cabe deslindar a carência desses equipamentos em nossos Datacenters e demais locais atualmente.

10.2.6. Outro fato importante é a dificuldade que poderá ser encontrada na configuração e implementação da solução de SD-WAN de forma a ter o gerenciamento centralizado, com automação do controle do caminho baseado em políticas, capacidade de segregar tráfego com base nas aplicações da camada 7 e utilizando topologia "full mesh".

10.2.7. Em virtude dos fatos mencionados, a solução de contratação de toda uma solução em Software Livre, contemplando serviços de instalação e suporte técnico, **não é uma solução viável** às áreas de negócio e técnicas do Ministério da Justiça e Segurança Pública.

10.3. Solução 3 - Contratação de uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses.

10.3.1. O presente cenário tem o objetivo de demonstrar a modernização necessária da topologia da nova solução de firewall dos atuais ambientes do MJSP (sede), CICCN-DF e Penitenciárias Federais . A disposição principal da análise é a possibilidade de aquisição de ativos novos contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, de forma a implementar uma topologia de firewall moderna, escalável e de alto desempenho.

10.3.2. A Figura 4 demonstra a topologia de firewall implementada junto aos equipamentos de redes presentes no Datacenter MJSP (SEDE) e CICCN-DF:

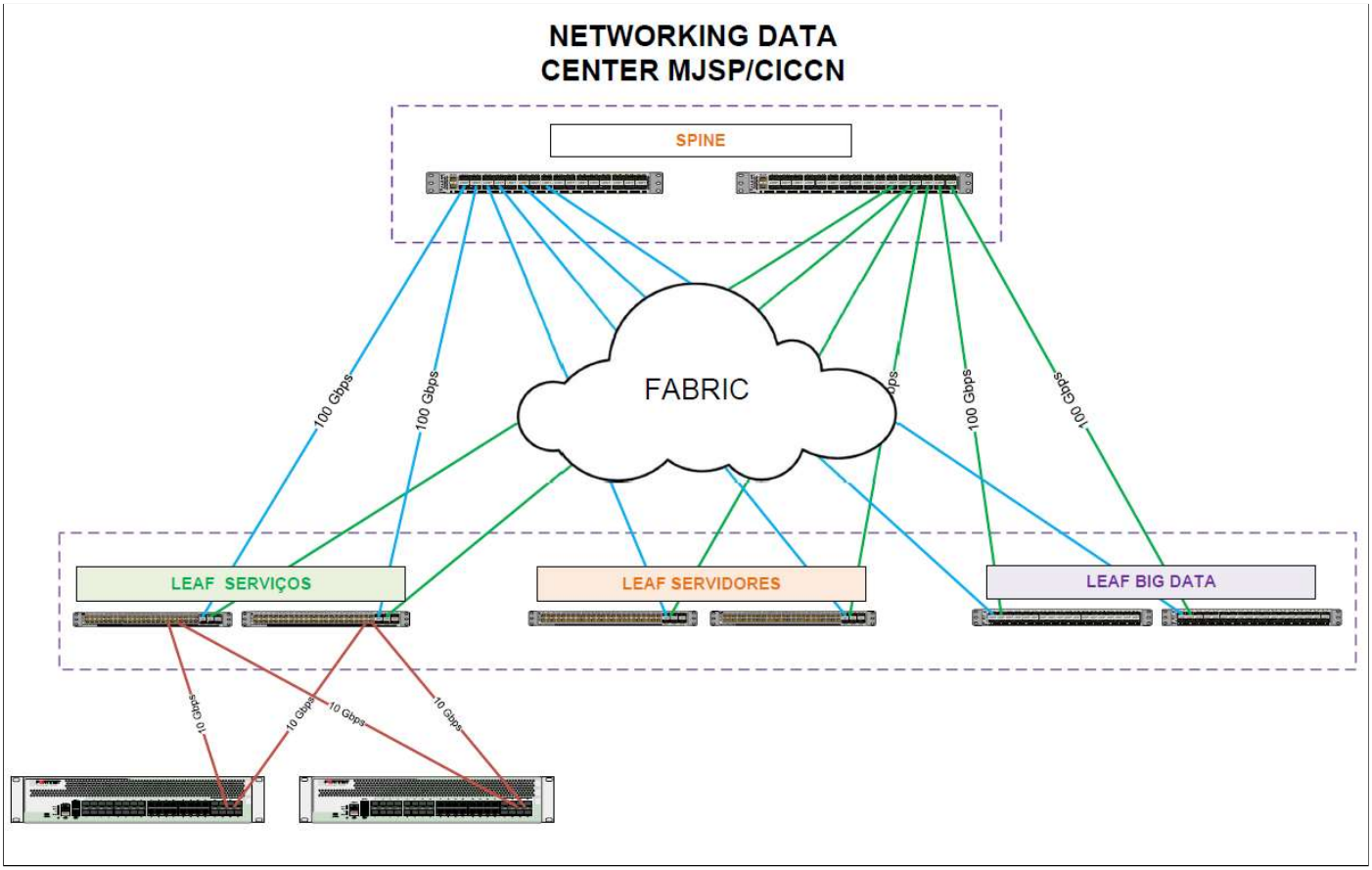

Figura 4 – Topologia MJSP e CICCN

10.3.3. De um modo geral, a topologia física não será alterada, permanecendo a nova solução também conectada aos switches Leafs de Serviços, proporcionando a padronização de topologia física, mitigando os riscos de uma parada da rede e obtendo a possibilidade de uma futura expansão tecnológica.

10.3.4. Destaca-se na nova solução, a importância em adquirir Firewalls considerados de Última Geração (Firewalls Next Generation - NGFW, que faz inspeção profunda de pacote que vai além da inspeção e do bloqueio de portas/protocolos para adicionar uma inspeção ao nível da aplicação, uma prevenção de intrusões e obter informações fora da firewall), com a implementação da tecnologia de SD-WAN, sendo listado abaixo as principais características e vantagens, como:

10.3.4.1. Os NGFWs são a evolução e ampliação das capacidades dos firewalls tradicionais. Inspeciona os dados em um nível mais profundo para identificar e bloquear ameaças que podem estar ocultas no tráfego normal.

10.3.4.2. Os NGFWs usam inspeção profunda de pacotes (DPI), ou seja, inspeciona o corpo de cada pacote, não apenas o cabeçalho, verificando os corpos dos pacotes em busca de assinaturas de malware e de outras ameaças em potencial. Durante essa inspeção, o conteúdo de cada pacote é comparado com o conteúdo de ataques maliciosos conhecidos.

10.3.4.3. Faz o controle do aplicativo e application awareness, isto é, bloqueiam ou autorizam pacotes com base em para qual aplicativo eles estão sendo encaminhados. Os NGFWs fazem isso analisando o tráfego na camada 7, a camada de aplicativos.

10.3.4.4. Maior capacidade em prevenção de intrusões (IPSs), utilizando métodos de detecção de assinaturas (verifica as informações dentro dos pacotes recebidos e as compara com ameaças conhecidas), detecção de anomalias estatísticas (verifica o tráfego para detectar mudanças incomuns de comportamento, em comparação com uma base de referência) e detecção de análise de protocolos stateful (semelhante à detecção de anomalias estatísticas, mas com foco nos protocolos de rede em uso, comparando-os com o uso normal dos protocolos).

10.3.4.5. Inteligência contra ameaças, ou seja, são capazes de receber e agir com base em informações de inteligência contra ameaças provenientes de fontes externas, mantendo a eficácia da detecção de assinaturas do provedor ao fornecer as assinaturas de malware mais recentes, também fornecendo informações sobre a reputação de IP. "A reputação de IP" identifica os endereços de IP de onde os ataques (especialmente ataques de bot).

10.3.4.6. Os NGFWs podem processar o tráfego em várias camadas no modelo OSI, não apenas nas camadas 3 (camada de rede) e 4 (a camada de transporte). Os NGFWs podem analisar o tráfego na camada 7 HTTP e identificar quais aplicativos estão sendo utilizados.

10.3.5. A Figura 5 demonstra a topologia de firewall implementada nas Penitenciárias junto aos principais equipamentos de redes presentes nas localidades:

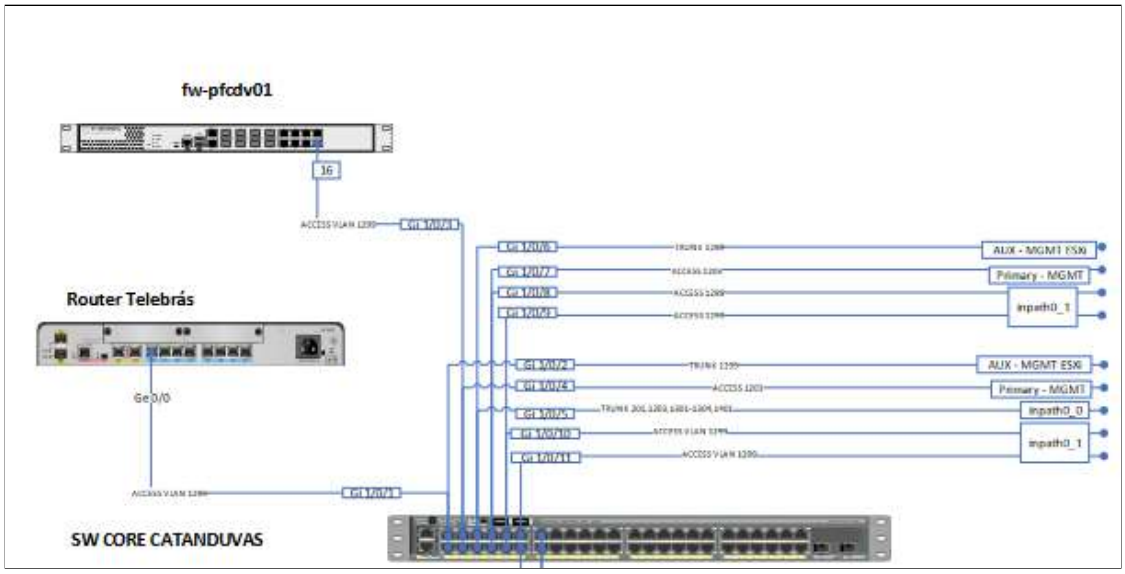

Figura 5 – Topologia de Firewall das Penitenciárias

10.3.6. A topologia de firewall implementada nas penitenciárias segue um padrão, utilizando-se de um appliance físico (de menor processamento e capacidade devido à quantidade de usuários na rede) ligado diretamente os Switch Core juntamente com outros serviços. Esta topologia física também será mantida, substituindo os atuais equipamentos por outros mais modernos, visando a utilização mais predominante da tecnologia de SD-WAN.

10.3.7. A SD-WAN pode ser entendida como uma WAN definida por software, ou seja, uma tecnologia de implantações de redes WAN baseadas em software via internet, oferecendo valor de utilidade significativo para os órgãos públicos e unidades distribuídas em termos de agilidade e capacidade de alavancar a economia da largura de banda da Internet.

10.3.8. A SD-WAN garante desempenho e resiliência consistentes de aplicativos, automatiza o direcionamento de tráfego de maneira orientada por aplicativos com base nos propósitos do MJSP, melhora a segurança da rede e simplifica a arquitetura WAN.

10.3.9. Além disso, a implantação rápida de serviços de WAN (como largura de banda e firewall) é menos complexa e muitas vezes sem a necessidade de enviar pessoal de TI no local, pois tem o gerenciamento centralizado (Centralizado no Datacenter Primário do MJSP). A largura de banda pode ser facilmente adicionada (com circuitos adicionais) ou reduzida à medida que os requisitos de negócios evoluem. A virtualização e a configuração automatizada de políticas de negócios e de segurança permitem serviços de direcionamento de tráfego automatizados, controlados centralmente com poucos cliques.

10.3.10. Sendo assim, adquirir uma nova solução de firewall (Firewall Next Generation (NGFW)), com implementação da solução de SD-WAN, vai otimizar implantações de links de dados e VPN nas unidades do MJSP, principalmente nas Penitenciárias Federais, e apresentam ainda outras funcionalidades, como:

10.3.10.1. Automatização do caminho das WANs e possibilidade de automação do controle do caminho baseado em políticas de negócios e aplicações;

10.3.10.2. Definição dinâmica de caminhos e métricas, baseadas na visibilidade em tempo real, sobre o destino desejado da aplicação, seu desempenho, a experiência do usuário final da aplicação e a qualidade das redes disponíveis no caminho;

10.3.10.3. Automação alinhada aos negócios e baseada em políticas para definir a qualidade do serviço e privilégios de acesso para todas as aplicações e todos os usuários, em combinação com a escolha automatizada do caminho;

10.3.10.4. Gerenciamento centralizado, com uma visualização integrada e topologia "full mesh" da estrutura de conectividade entre o datacenter e Unidades, tudo em uma plataforma de gerenciamento integrada e centralizada, que possibilite automatizar a implantação da VPN, com escolha do melhor

link de dados e melhor caminho para a VPN, possibilitar múltiplas VPN's e continuidade do serviço de VPN em caso de falhas ou degradação de um dos links de dados, melhorando a conectividade entre redes das Unidades e a Sede;

10.3.10.5. Monitoramento de desempenho integrado de ponta a ponta e otimização da WAN de forma segura.

10.3.10.6. Suporte a VLANs, capacidade de segregar tráfego pelas WANs e entre redes LANs sem fio, e com fio e capacidade de segregar tráfego com base nas aplicações da camada 7;

10.3.10.7. Capacidade de aplicar regras de controle de acesso, desempenho e segurança com base na política definida no console de gerenciamento central;

10.3.10.8. Implantação sem configurações na unidade remota " zero-touch" via ativação automatizada e segura de todos os gateways de WAN.

10.3.11. Em virtude dos fatos mencionados, a solução de contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses **é o cenário mais viável**, com vistas os benefícios técnicos e de padronização prestados às áreas de negócio do Ministério da Justiça e Segurança Pública.

11. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

11.1. Solução 1 - Contratação de serviço de garantia e suporte técnico para a solução atual.

11.1.1. Entende-se que este cenário não é viável em virtude das BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4, do Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação do STI/MP, o acórdão TCU *n. 2400/2006*, além da necessidade de expansão e atualização dos ativos de TIC.

11.2. Solução 2 - Contratação de toda uma solução em Software Livre.

11.2.1. Não é uma solução viável, considerando o escopo das necessidades do MJSP e por não se enquadrar nos aspectos técnicos de TIC do MJSP necessários para está contratação.

12. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

12.1.Não se aplica, pois apenas a **Solução 3 - contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses** encontra-se viável no momento, não sendo possível realizar comparação com outra, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019.

13. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

13.1 **Solução 3** - Trata-se da solução de **contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses**, que contempla plano de atualização, expansão tecnológica e contingência constituídos por uma série de ações e procedimentos.

13.2. A tabela abaixo traz o item e a localidade de instalação de cada equipamento:

Item	Descrição	Quantidade Total	Quantidade por localidade	Local de Instalação
1	Appliance de Firewall para uso nos Datacenters do MJSP	04	02	Datacenter Primário - SEDE do MJSP
			02	Datacenter Secundário - CICCN
2	Appliance de Firewall para uso nas Penitenciárias Federais	05	01	Penitenciária Federal Catanduvas (PR)
			01	Penitenciária Federal Campo Grande (MS)
			01	Penitenciária Federal Mossoró (RN)
			01	Penitenciária Federal Porto Velho (RO)
			01	Penitenciária Federal Brasília (DF)
3	Appliance para análise do tráfego de dados	01	01	Datacenter Primário - SEDE do MJSP
4	Appliance de gerenciamento centralizado	01	01	Datacenter Primário - SEDE do MJSP

Tabela 7 - Quantidade e localização para instalação

13.3. As principais especificações e requisitos da solução serão destacados nesta etapa do planejamento, as demais serão incluídas no Termo de Referência, em seu anexo.

13.3.1. **Appliance Físico de Firewall para uso nos Datacenters do MJSP.**

13.3.1. 1. Throughput de no mínimo, 15 (quinze) Gbps, com as funcionalidades de firewall, controle de aplicação, IPS, anti-malware e prevenção contra ameaças avançadas de dia-zero habilitadas e atuantes;

13.3.1. 2. O Throughput é a quantidade de tráfego que um único equipamento écapaz de encaminhar, não havendo soma entre os membros do cluster;

13.3.1. 3. Suporte a, no mínimo, 12.000.000 (doze milhões) de conexões simultâneas;

13.3.1. 4. Suporte a, no mínimo, 500.000 (quinhentos mil) novas conexões por segundo;

13.3.1. 5. Armazenamento de, no mínimo, 480GB SSD;

13.3.1. 6. Deve possuir fontes de alimentação AC 100-240VAC redundantes e hot-swappable;

13.3.1. 7. No mínimo, 16 (Dezesseis) interfaces de rede de 1GbE RJ-45;

13.3.1. 8. No mínimo, 02 (duas) interfaces de rede de 10 Gbps SFP+;

13.3.1. 9. No mínimo, 01 (uma) interface Gigabit dedicada para alta disponibilidade;

13.3.1. 10. 01 (uma) interface do tipo console ou similar;

13.3.1. 11. Deverão ser licenciados para suportar, pelo menos, 5.000 (cinco mil) usuários de VPN SSL;

13.3.1. 12. VPN com capacidade de, pelo menos, 40 (quarenta) Gbps de tráfego IPSec;

13.3.1. 13. Suportar, no mínimo, 2 instâncias de firewall (cluster) e permitir a expansão, através de aquisição futura de licenças;

13.3.1. 14. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

13.3.1. 15. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores do tipo SR.

13.3.1. 16. Não serão aceitos appliances virtualizados para os firewalls, somente equipamentos físicos.

13.3.2. **Appliance Físico de Firewall para uso nas Penitenciárias Federais**

13.3.2.1. Throughput de, no mínimo, 1Gbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas;

13.3.2.2. Throughput de, no mínimo, 8 Gbps de VPN IPSec para ser utilizado no SD-WAN;

13.3.2.3. Estar licenciado para, ou suportar sem o uso de licença, 500 túneis de VPN IPSEC Site-to-Site simultâneos;

13.3.2.4. Suporte a, no mínimo, 55 mil novas conexões por segundo;

13.3.2.5. Suportar no mínimo 1 Gbps de throughput de Inspeção SSL;

13.3.2.6. Possuir ao menos 16 interfaces 1 GE RJ45;

13.3.2.7. Possuir ao menos 4interfaces 1 GE SFP com transceivers inclusos;

13.3.2.8. Possuir ao menos 2 interfaces 10 GE SFP+ com transceivers inclusos;

13.3.2.9. Suportar a criação de no mínimo 5 instâncias virtuais;

13.3.2.10. Deve incluir porta USB compatível com modem 3G/4G, permitindo ainda que este link WAN seja utilizado nas regras de SD-WAN;

13.3.2.11. Possuir armazenamento de no mínimo de 480GB;

13.3.2.12. Possuir fonte de alimentação interna redundante;

13.3.2.13. Deve suportar a instalação em rack padrão 19”;

13.3.3. **SD-WAN**

13.3.3.1. Deve possuir capacidade para utilizar, pelo menos 3 (três) links de WAN, sendo no mínimo 2 (dois) links simultâneos.

13.3.3.2. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede da CONTRATANTE e dinamicamente. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

13.3.3.2.1. Endereço IP de origem e/ou destino;

13.3.3.2.2. Subredes de origem e/ou destino;

13.3.3.2.3. Métricas de Jitter, latência e perda de pacotes por aplicação;

13.3.3.2.4. Status da porta de WAN primários (UP ou DOWN);

13.3.3.2.5. Toda a comunicação Wan deve trafegar em um túnel VPN ponto-a-ponto estabelecido dinamicamente entre os PONTOS DE PRESENÇA da CONTRATANTE;

13.3.3.2.6. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation - RFC 2784);

13.3.3.2.7. A solução deve ter um tempo máximo de failover e failback de 300 segundos;

13.3.3.2.8. A topologia da rede WAN deve ser dentre outras possíveis, a de malha completa (full mesh);

13.3.3.2.9. O estabelecimento do túnel VPN entre os pontos de presença pode inicialmente ser orientado pelo concentrador, mas o tráfego de dados após o estabelecimento do túnel deve ser realizado diretamente entre os integrantes do túnel, sem consumir throughput do concentrador;

13.3.3.2.10. A solução de SD-WAN deverá ser integrada no próprio appliance de NGFW.

14. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

14.1. Conforme o "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" V 3.0 do SISP, o orçamento informado nesse momento é preliminar. Ele deverá ser suficiente na análise de custo total de propriedade para a escolha da solução. **O orçamento detalhado será realizado na confecção do Termo de Referência.**

Grupo	Item	Descrição	Unidade	QTDE	Estimativo unitário (R$)	Estimativo total (R$)
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	Unitário	04	R$ 1.195.000,00	R$ 4.780.000,00
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	Unitário	05	R$ 93.000,00	R$ 465.000,00
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	Unitário	01	R$ 210.000,00	R$ 210.000,00
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	Unitário	01	R$ 300.00,00	R$ 300.00,00
	ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO *(Art. 11, Inciso IV, da IN 01/2019 SGD/ME)* *				**R$ 5.755.000,00**	
	* Conforme o "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" V 3.0 do SISP (pág. 39), o orçamento estimado informado nesse momento é preliminar. **O orçamento detalhado será realizado na confecção do Termo de Referência.**					

Tabela 8 - Descrição dos itens

15. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

15.1. A escolha da solução de contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses se deu foi por vários motivos, podendo destacar os de âmbito técnico como fator importante dessa escolha.

15.2. De fato, para chegar a escolha da solução mais viável, foi necessário realizar a segmentação dos requisitos por localidade, o que remete a necessidades específicas para cada ambiente de TIC administrado pelo MJSP, sendo essas localidades os Datacenters primário e secundário e as Penitenciárias Federais (Catanduvas (PR), Campo Grande (MS), Mossoró (RN), Porto Velho (RO) e Brasília (DF)).

15.3. Os Datacenters primário e secundário e todas as penitenciárias possuem necessidades claras, a primeira é a substituição dos ativos da solução de firewall atuais, desatualizados tecnologicamente e que estão próximos do fim de vida ficando sem suporte e garantia, Já a segunda, trata-se da

necessidade de expansão da capacidade da solução de Firewall do núcleo central do MJSP, pois encontra-se próximo do seu limite máximo, representando um risco à segurança das informações sob responsabilidade do MJSP e à disponibilidade dos seus serviços.

15.4. Além disso, soma-se a necessidade de ativação da tecnologia de SD-WAN nas localidades onde há indisponibilidades de links constantemente, ou ainda nos locais que possuem sistemas e serviços sensíveis que precisem de uma maior mitigação de riscos.

15.5. Sendo assim, tecnicamente, ficou comprovado que a melhor solução para os Datacenters primário e secundário é a aquisição de ativos novos, levando em consideração, para a escolha das especificações dos equipamentos, o aumento de usuários na rede, serviços disponibilizados e acessos externos aos sistemas ofertados pelo MJSP.

15.6. Por fim, conclui-se que o benefício da aquisição de uma nova solução de firewall contemplando serviços de instalação e suporte técnico foi evidenciado e comprovado, uma vez que foram realizadas análises do ponto de vista técnico, trazendo com isso melhor administração e acompanhamento da equipe de fiscalização dos contratos.

15.7. Em vista dos argumentos técnicos levantados em todo este Estudo Técnico, contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses **foi considerado o cenário mais viável**, com vistas os benefícios técnicos e de atendimento da necessidades das áreas de negócio do Ministério da Justiça e Segurança Pública.

16. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

16.1. O aspecto econômico da solução escolhida (**contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses**) foi considerado no sentido do minucioso estudo da quantidade exata ou o mais próximo da realidade necessária, com requisitos, análises e comparações técnicas consideradas essenciais para os ativos de firewall em cada localidade, já que não foi possível realizar a comparação econômica com as demais soluções devido à singularidade atual do ambiente de TIC, dispensando a necessidade de cálculos comparativos entre soluções, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019: *"§ 1º As soluções identificadas no inciso II consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade."*

17. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

17.1. Os benefícios buscados com a substituição, expansão e atualização de equipamentos com o objetivo de mitigar os riscos, evitar impactos na segurança e na rotina dos usuários da rede do MJSP, se traduzem nas listadas abaixo:

a) Manter parque de ativos de segurança (Firewalls) com suporte, manutenção e garantia;

b) Prover a infra-estrutura de Firewalls necessária para suportar, de forma otimizada e flexível, as demandas de informações e serviços das áreas finalísticas;

c) Manter e aprimorar o método de gestão centralizada e comunicação de toda a infra-estrutura de Firewalls de forma a agilizar a sua operação;

d) Suportar a demanda futura por largura de banda e balanceamento de links nas Penitenciárias com a utilização da tecnologia SD-WAN;

e) Garantir soluções voltadas à segurança em redes de computadores;

18. PROVIDÊNCIAS A SEREM ADOTADAS

18.1. As próximas providências estão relacionadas as etapas referentes à contratação da solução escolhida, levando em consideração outras áreas envolvidas neste projeto.

18.2. Com isso, as demais etapas que envolvem diretamente a área técnica e requisitante são:

1. A Aprovação e Assinatura do Estudo Técnico Preliminar (ETP) pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, conforme previsto no art. 11, § 2º da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019.
2. Elaboração do Termo de Referência pela Equipe de Planejamento da Contratação a partir do Estudo Técnico Preliminar da Contratação, que será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.
3. Em paralelo a elaboração do Termo de Referência, realizar a pesquisa de mercado, que trará os esclarecimentos necessários sobre os parâmetros utilizados para a mensuração do preço médio de licitações realizadas e de mercado.
4. A composição do Mapa de Gerenciamento de Riscos (instrumento de registro e comunicação da atividade de gerenciamento de riscos ao longo de todas as fases da contratação).

19. DECLARAÇÃO DE VIABILIDADE

19.1. O presente Estudo Técnico Preliminar da Contratação evidencia que a forma de contratação que maximiza a probabilidade do alcance dos resultados pretendidos com a mitigação dos riscos e observância dos princípios da economicidade, eficácia e eficiência, seria a realização de processo de **contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses**, para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

19.2. Como principais objetivos a serem alcançados, entre outros, podem ser citados:

- Alinhamento estratégico com as iniciativas do MJSP, garantindo a entrega de valor para que as áreas finalísticas consigam atingir seus objetivos específicos;
- Melhoria da qualidade dos serviços prestados pela STIC a sua população cliente, com adoção das melhores práticas de mercado incorporadas à solução tecnológica que se pretende adquirir.
- Manter parque de ativos de segurança com suporte, manutenção e garantia;
- Prover a infraestrutura de firewall necessária para suportar, de forma otimizada e flexível, as demandas de informações e serviços das áreas finalísticas;
- Suportar a demanda futura por por maior proteção contra malwares;

19.3. Diante do exposto, a equipe de planejamento declara ser **viável** a contratação da solução pretendida.

Documento assinado eletronicamente por **Bruno Alves de Lima**, **Integrante Técnico(a)**, em 23/06/2023, às 14:46, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **RODRIGO ALBERNAZ BEZERRA**, **Coordenador(a)-Geral de Infraestrutura e Serviços**, em 23/06/2023, às 15:34, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Criado por bruno.alves, versão 5 por bruno.alves em 22/05/2023 21:32:40.