TERMO DE REFERÊNCIA

Contratação de solução de gerenciamento unificado de ameaças (UTM) e de rede WAN definida por software (SD-WAN) composta por hardware, software, licenciamento, suporte, implantação e garantia de 60 meses.

PROCESSO ADMINISTRATIVO PA-PRO-2021/02105

1. DO OBJETO

Contratação de solução de gerenciamento unificado de ameaças (UTM) e de rede WAN definida por software (SD-WAN) composta por hardware, software, licenciamento, suporte, implantação e garantia de 60 meses para atender o Tribunal de Justiça do Estado do Pará.

2. DA FUNDAMENTAÇÃO

2.1. Da motivação

Necessidade de prover uma camada adicional de segurança em cada unidade judiciária onde será implantada a solução, permitindo maior visibilidade do tráfego gerado em cada unidade, além da possibilidade de mitigar ameaças e riscos de segurança tanto no que se refere a sistemas e serviços de TI internos, além de ameaças externas que possam comprometer a confidencialidade, a integridade e a disponibilidade dos serviços oferecidos.

Soma-se ao fato supramencionado, a necessidade de gerenciar a conectividade WAN das unidades judiciárias de forma pró-ativa, por meio da priorização de demandas, melhor utilização dos links WAN e maior disponibilidade dos serviços demandados, tendo o objetivo de permitir que a atividade fim do Tribunal seja realizada com maior qualidade.

Houve a contratação de novos circuitos de internet, via fibra óptica, em diversas localidades do interior do estado, trazendo a necessidade de adicionar equipamento capaz de realizar a conexão segura via VPN entre a unidade judiciária e o Datacenter do TJPA, situado em Belém/PA.

Em função deste Tribunal já ter implementado a solução de SDWAN em algumas localidades na FASE 1 do projeto, observou-se a melhoria do uso dos circuitos de dados, além do aumento da disponibilidade da rede, o que motivou ainda mais a necessidade de ampliação da solução já existente, objeto desta contratação.

2.2. Dos objetivos a serem alcançados por meio da contratação:

Conforme o subitem 1.7, c, dos Estudos Preliminares, a presente contratação objetiva:

- Permitir instalação de circuitos de provedores locais via fibra óptica nas unidades do TJPA.
- Possuir infraestrutura que permita o uso simultâneo de circuitos de dados, trazendo maior disponibilidade na rede e velocidade nas transmissões dos dados.
- Implantar equipamento que garanta a segurança na rede de dados em todas as unidades do TJPA.
- Criar uma arquitetura de TI segura em todas as suas camadas.

- Melhorar no grau de satisfação dos usuários, jurisdicionados e órgãos conveniados pelo ganho de desempenho e de segurança nos serviços de TIC ofertados pelo TJPA.
- Viabilizar ferramentas para o monitoramento pró-ativo dos equipamentos que compõem a solução de UTM/SD-WAN pela equipe de Operações de TIC 24x7 do TJPA.
- Integrar políticas e ações que possam prover conformidade com os normativos que regem à segurança da informação no âmbito do TJPA.

Ademais também irá melhorar a segurança da informação de nível operacional no âmbito do TJPA, auxiliando na prevenção de riscos e ameaças, tanto internas quanto externas, além da mitigação dos efeitos de potenciais ataques virtuais que possam comprometer os dados institucionais tratados no Tribunal. Melhora da experiência do usuário na utilização de serviços que demandam conectividade WAN, além da redução de custos no que diz respeito a possibilidade de contratação de diversos tipos de conectividade WAN (MPLS, Internet, 4G, etc), o que possibilita pelas escolhas mais vantajosas para a Administração

2.3. Dos benefícios diretos e indiretos resultantes da contratação:

O principal objetivo do presente desta fase do projeto é ampliar e melhorar a experiência na utilização dos serviços e sistemas de TI para os magistrados e servidores que trabalham em unidades judiciárias localizadas no interior do Estado, e que carecem de melhores condições de trabalho no que se refere à conectividade WAN, possibilitando redução de custos para a Administração.

Como benefícios diretos, cita-se a possibilidade de garantir maior disponibilidade dos serviços e sistemas de TI, já que a solução de UTM/SD-WAN permite a utilização e o gerenciamento de diversos links WAN de diversas tecnologias diferentes (MPLS, Internet, 4G, etc) ao mesmo tempo, permitindo mitigar problemas de conectividade nas unidades de forma transparente para usuários e magistrados. Também a segurança operacional é um benefício direto, pois é possível mitigar diversas modalidades de ataques cibernéticos, o que auxilia na proteção de dados sensíveis que trafegam dentro da infraestrutura de TI do Tribunal.

Como benefício indireto, cita-se a possibilidade de melhoria na produtividade dos usuários internos da rede do TJPA e a entrega de serviços com maior valor agregado pelo Tribunal.

2.4. Do alinhamento entre a demanda e os instrumentos de planejamento do TJPA

Do Planejamento Estratégico do Poder Judiciário 2021/2026, em seu **MACRODESAFIO: FORTALECIMENTO DA ESTRATÉGIA NACIONAL DE TIC E DE PROTEÇÃO DE DADOS**, temos a **INICIATIVA ESTRATÉGICA: Aprimoramento do Domínio de Serviços de TIC**, que orienta para “Aprimorar o aparato tecnológico corporativo, envolvendo Segurança da Informação e Proteção de

Dados, Riscos, Software, Infraestrutura e Serviços, com foco na otimização das atividades jurisdicionais e administrativas, o que compreenderia o domínio de Serviços de TIC na Estratégia Nacional de TIC do Poder Judiciário."

A contratação está definida no Plano de Gestão Biênio 2021-2023, contemplada no **MACRODESAFIO 12: FORTALECIMENTO DA ESTRATÉGIA NACIONAL DE TIC E PROTEÇÃO DE DADOS**, tendo a **INICIATIVA ESTRATÉGICA 12.1: Aprimoramento do Domínio de Serviços de TIC**, alinhada ao item **12.1.1 Expandir a infraestrutura de telecomunicações** que descreve a necessidade em "Melhorar a infraestrutura da rede de comunicação de dados e voz das unidades judiciárias e administrativas da RMB e do interior, visando a otimização da utilização dos recursos tecnológicos, a adequação do desempenho e a disponibilidade dos sistemas de TIC em função do aumento significativo da necessidade de circuitos de dados com maior banda e menor latência". Tal iniciativa é contemplada com a **ETAPA 12.1.3.5: Expansão da solução de rede de Gerenciamento Unificado de Ameaças e Wan Definida por Software (UTM-SDWan)**.

A contratação também está prevista no Plano de Contratações de Soluções de TIC 2021 e no Plano Orçamentário para o exercício corrente.

2.5. Da referência aos Estudos Preliminares

O presente Termo de Referência foi elaborado a partir dos Estudos Preliminares elaborados no processo nº PA-PRO-2021/02105 do sistema SIGADOC.

2.6. Da relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados

A **ETAPA 12.1.3.5: Expansão da solução de rede de Gerenciamento Unificado de Ameaças e Wan Definida por Software (UTM-SDWan)** do Plano de Gestão Biênio 2021/2023 possui como meta a quantidade de 50 unidades a serem implantadas, porém por meio de levantamento da atual quantidade de unidades restantes para que toda a rede do TJPA seja atendida, houve a necessidade do aumento para 67 unidades, o que atenderá todas localidades do Estado.

O quadro abaixo representa o quantitativo necessário para atender a demanda.

Item	Descrição	Qtde inicial	Qtde atual	Critérios de definição da quantidade
1	**NGFW de pequeno porte com SDWAN integrada, garantia, suporte e todas as licenças necessárias para atendimento das especificações** Marca: Fortinet Fabricante: Fortinet Modelo: FortiGate 61F (FG-61F) Contempla também todos os acessórios, como Kit para instalação em rack, cabos de energia e cabos console, além de licenciamento de 60 meses do tipo UTP (FC-10-0061F-950-02-60), que contempla serviço de suporte e garantia 24x7, atualização de assinaturas de Controle de Aplicação, IPS, Antivirus, Filtro Web, Antispam, e FortiSandbox Cloud.	50	67	Atender todas unidades do TJPA

2.7. Da análise de mercado de TIC

A equipe técnica do TJPA teve a oportunidade de visitar entidades públicas e privadas em Belém e fora de Belém (PA-MEM-2019/18370 e PA-MEM-2019/30280) que já haviam implantado em seus ambientes tecnológicos, dentro das peculiaridades de cada entidade, a solução de UTM/SD-WAN, como por exemplo, o Supremo Tribunal Federal (STF), o Tribunal de Contas da União (TCU), a Procuradoria Geral da União (PGR), o Sistema de Cooperativas de Crédito do Brasil (SICOOB) e o Banco da Amazônia (BASA). Sem realizar visitas técnicas, também foram avaliadas outras soluções, como a do Ministério do Planejamento, Desenvolvimento e Gestão (MPDG), o Banco do Nordeste (BNB), a Polícia Civil do Distrito Federal (PCDF), o Tribunal de Contas do Estado do Pará (TCE/PA) e Companhia Brasileira de Trens Urbanos (CBTU).

Através das visitas técnicas e das análises das soluções, houve a oportunidade de avaliar duas modalidades de solução de UTM/SD-WAN, que foram a modalidade tradicional, onde a entidade adquiriu equipamentos próprios e a implantação e administração da solução fica a cargo da mesma, e a modalidade baseada em serviços, onde os equipamentos são “terceirizados”, normalmente vendidos como um serviço adicional a contratação de links de internet através das operadoras de telecomunicações, onde as operadoras administravam a solução de UTM/SD-WAN. Por exemplo, no Tribunal de Contas da União, a solução UTM/SD-WAN foi contratada através da modalidade serviços e administrada pela operadora vencedora, juntamente com links MPLS redundantes vindo das capitais para o prédio sede localizado em Brasília. Abaixo, na figura 1, consta a topologia desenhada pelo TCU.

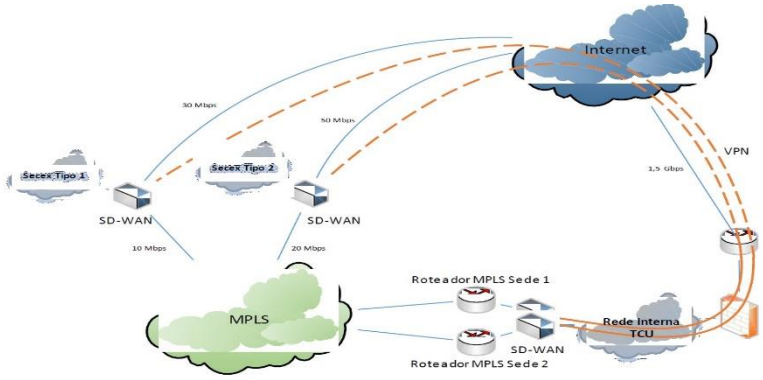

Figura 1 - Topologia da solução de UTM/SD-WAN do TCU (Fonte: Pregão Eletrônico 93/2018/TCU).

Outro exemplo, no Banco do Nordeste, a solução UTM/SD-WAN também foi contratada através da modalidade serviços e administrada pela operadora vencedora, juntamente com links MPLS e de internet vindo das unidades distribuídas para os sites primário e secundário do BNB, localizados em Fortaleza. Abaixo, na figura 2, consta a topologia desenhada pelo BNB.

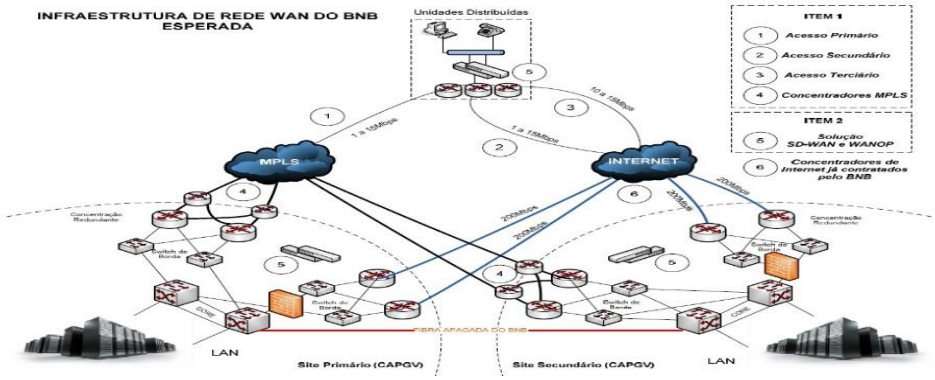

Figura 2 - Topologia da solução de UTM/SD-WAN do BNB (Fonte: Pregão Eletrônico 44/2018/BNB).

Comparada as duas modalidades e avaliando as peculiaridades dos dados que trafegam nas redes de comunicação do TJPA, foi tomada uma decisão estratégica pelo TJPA onde a modalidade de solução adotada seria a tradicional, devido a sensibilidade dos dados que trafegam através das redes de comunicação de dados do TJPA, não seria possível permitir que a solução fosse administrada por terceiros, onde serviços críticos poderiam ficar expostos de maneira desnecessária, decidiu-se que a administração desta solução ficaria a cargo da equipe técnica do TJPA.

Também por questões estratégicas, foi constatado que a contratação deste serviço juntamente com links de internet poderia resultar em um aprisionamento a fornecedores específicos e, por consequência, em maiores custos para a Administração.

Adicionalmente, dentro da modalidade tradicional, existem duas abordagens: a abordagem “On-Premise” onde a gerência dos equipamentos se dá através de software tradicional, implantado nas dependências do demandante, e a abordagem em nuvem, onde a gerência dos equipamentos se

dá através de um sistema de gerência em nuvem, fora das dependências do cliente. Por questões estratégicas e para prevenir possíveis vazamentos de dados para fora das dependências do TJPA escolheu-se, dentro da modalidade tradicional, a abordagem “On-Premise”. Abaixo, na figura 3, um esboço da topologia de UTM/SD-WAN nas unidades judiciárias do Tribunal.

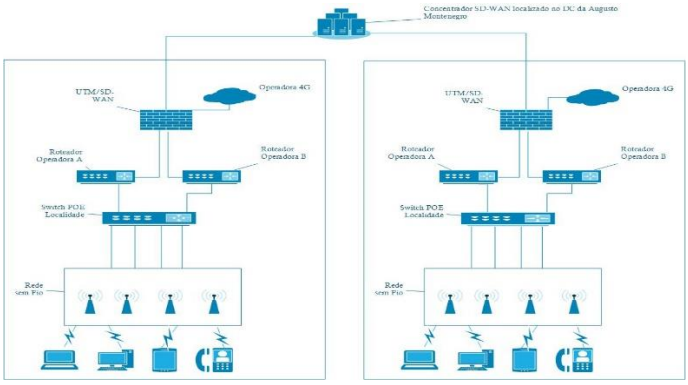

Figura 3 – Esboço de Topologia da solução de UTM/SD-WAN do TJPA nas unidades judiciárias.

Após análise de diversas soluções oferecidas pelo mercado, incluindo visitas técnicas em entidades públicas e privadas que já possuem a referida solução em funcionamento, respeitadas as peculiaridades de cada entidade, análises feitas pela equipe técnica do TJPA, além da recomendação emitida por entidades de nível internacional responsáveis pela análise de soluções de TIC, como o Gartner e o NSS Labs, a disponibilidade de atas de registro de preço para adesão imediata e o custo total em relação ao orçamento disponível para aquisição, além do custo benefício entre o valor que será pago e o que a solução oferece (capacidade dos equipamentos, tempo de licenciamento, suporte e garantia, implantação, SLA para suporte e garantia, dentre outras características), a solução do fabricante Fortinet, adquirida pelo Ministério Público do Estado do Pará (MPPA) por meio do Pregão Eletrônico 047/2020/MPPA foi escolhida.

Sendo de reconhecida qualidade, a solução traz benefícios importantes que podem auxiliar na manutenção e aumento da disponibilidade dos serviços oferecidos pelo TJPA que utilizam circuitos WAN, fazendo parte de um conjunto de soluções que tem como objetivo melhorar a experiência de trabalho dos magistrados e servidores deste Tribunal.

Ainda nesse sentido, a solução escolhida possui um conjunto de serviços que se mostra vantajoso em relação ao preço que será pago, como garantia, suporte e licenciamento por 60 meses, o que fornece um tempo de vida útil compatível com o tempo de vida médio para as soluções de TI existentes no mercado.

2.8. Da natureza do objeto

O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de Tecnologia de Informação, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste Termo de Referência.

Adicionalmente, admite-se que a execução do objeto possui natureza continuada, cujo escopo prevê o fornecimento em um período de até 60 (sessenta) meses.

2.9. Do parcelamento do objeto

Conforme § 1º, do Art. 23, da Lei Nº 8.666/93, os serviços deverão ser divididos em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

O disposto, no entanto, não se aplica na presente demanda, sendo necessário o agrupamento em Lote, tendo em vista a garantia da uniformidade na prestação dos serviços, uma vez que os itens agrupados possuem a mesma natureza e guardam relação entre si, afastando possíveis prejuízos à competitividade, ao mesmo tempo em que exerce maior atratividade perante os licitantes. Ademais, considerando o número de itens, a organização em lote evita que inúmeros contratos sejam celebrados com diferentes fornecedores, situação que, tecnicamente, afeta diretamente a rotina da Administração, prejudicando a eficiência administrativa, que passa pela otimização do gerenciamento de seus contratos de fornecimento, uma vez que lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação.

É importante salientar que o aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos, e essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública. Busca-se ainda, com o agrupamento, obtenção de preços mais vantajosos à Administração, em razão da economia de escala, eficiência e racionalização de custos.

Dessa forma a presente contratação será realizada por meio de lote único com 01 (um) item, considerando para efeito de adjudicação, o MENOR PREÇO GLOBAL POR LOTE

2.10. Da seleção do Prestador de Serviço

A seleção do fornecedor será feita para o licitante que apresentar menor preço por lote único, desde que sejam atendidos plenamente às condições do edital, com toda a documentação e comprovação técnica exigida.

2.10.1. Da forma e do critério de seleção

O critério de aceitabilidade de preços será realizado por LOTE ÚNICO, mediante a análise de proposta. Além disso, cita-se que não será aceita proposta, após a fase de lances e negociação, cujo valor do lote único esteja superior ao estimado pelo TJPA na fase de cotação de preços.

2.10.2. Da modalidade e do tipo de licitação

A contratação do objeto em questão deve ser efetuada em adesão à Ata de Registro de Preços nº 040/2021, oriunda do Pregão Eletrônico nº 047/2020 do Ministério Público do Estado do Pará, que apresentou o no valor global estimado de R$ 2.111.782,38 (dois milhões, cento e onze mil, setecentos e oitenta e dois reais e trinta e oito centavos).

2.10.3. Dos critérios de habilitação obrigatórios

A. Comprovação de aptidão para desempenho de atividade pertinente e compatível com o objeto deste Pregão, mediante atestado(s) ou declaração(ões) de Capacidade Técnica, expedido(s) por pessoa jurídica de direito público ou privado comprovando que a licitante prestou ou está prestando serviços objeto deste edital, conforme transcrição abaixo:

   i. Atestado de Capacidade Técnica, para fins de comprovação da capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa realizado ou estar realizando o fornecimento do objeto, compatível em características, quantidades e prazos com o objeto deste Termo de Referência;

   ii. Com a finalidade de tornar objetivo o julgamento da documentação de qualificação técnica, considera(m)-se compatível(eis) o(s) atestado(s) que expressamente certifique(m) que a empresa já forneceu solução de:

      - SOLUÇÃO DE GERENCIAMENTO UNIFICADA DE AMEAÇAS (UTM) E DE REDE WAN DEFINIDA POR SOFTWARE (SDWAN).
      - SUPORTE TÉCNICO EM SOLUÇÃO DE SDWAN, além de comprovar que executou a contento serviço de suporte técnico, pelo período de no mínimo 12 (doze) meses.

   iii. Admite-se a soma do quantitativo de serviços nos atestados apresentados, desde que tenham sido realizados de forma simultânea no período de 12 (doze) meses.

B. Apresentar documento probatório de que possui compromisso com a sustentabilidade ambiental, nos termos da Lei Distrital n° 4.770/2012, que poderá ser feito da seguinte forma:

i. Por Declaração, onde a licitante afirma possuir o compromisso e responsabilidade com a Sustentabilidade Ambiental, nos termos das exigências impostas pela Lei Distrital n° 4.770/2012, conforme modelo constante do Anexo deste edital, ou;

ii. Com a apresentação de documento probatório (atestado, declaração, certificado, registro, credenciamento etc.) emitido por Órgãos Públicos de qualquer ente da Federação que tenha competência legal na área ambiental que o produto ofertado, comercializado, ou o fornecedor, distribuidor ou fabricante está devidamente cadastrado, registrado etc. no respectivo Órgão, ou;

iii. Com a apresentação de documentos que o fornecedor está em fase de implantação de práticas sustentáveis, informando, no referido documento quais são as práticas já implantadas e, quais as metas pretendidas a atingir na questão da sustentabilidade ambiental.

iv. No caso de o licitante apresentar os documentos comprobatórios, conforme mencionado nas alíneas “i” e “iii” poderá ser designada pelo TJPA uma Comissão de Avaliadores que juntamente com o Pregoeiro e sua Equipe poderá inspecionar/vistoriar o estabelecimento ou o ponto comercial do licitante, a fim de verificar as informações e declarações apresentadas.

v. Caso seja detectado pelos inspetores/avaliadores que as informações declaradas pelo licitante não sejam verdadeiras, ou, que esteja de má fé, serão tomadas as medidas administrativas, e se for o caso, penal, cabível ao caso.

2.11. Do impacto ambiental

Considerando a análise apresentada nos Estudos Preliminares referenciados na SEÇÃO 2.5 deste TERMO DE REFERÊNCIA, não foram identificados riscos ambientais significativos, em decorrência do fornecimento dos bens e serviços da solução de UTM/SD-WAN.

A probabilidade de ocorrência dos impactos estudados (geração de resíduos sólidos, poluição sonora e poluição visual) poderá ser facilmente mitigada através de realização de vistorias técnicas durante o período da prestação dos serviços.

Neste sentido, é importante que todos os serviços previstos atendam rigorosamente às normas técnicas vigentes e os padrões adotados pelo TJPA. Assim como, estes serviços deverão ser entregues sem instalações provisórias e com os ambientes livres de entulho ou sujeira, sendo a CONTRATADA responsável por sua limpeza.

Ademais, é desejável que os equipamentos, ferramentas e materiais empregados na execução dos serviços em cena estejam em conformidade com a diretiva RoHS (Restriction of Hazardous Substances), relacionada à preservação do meio ambiente, por meio da restrição do uso

de metais pesados (mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs), etc.) durante a fabricação.

2.12. Da conformidade técnica e legal

Os procedimentos legais para a renovação contratual pretendida obedecerão, integralmente:

a) À Constituição da República Federativa do Brasil, promulgada em 5 de outubro de 1988;

b) Às disposições contidas na Lei Federal nº 8.666, de 21 de junho de 1993, com as respectivas alterações posteriores;

c) Às disposições contidas na Lei Federal nº 9.784, de 29 de janeiro de 1999, com as respectivas alterações posteriores;

d) À Resolução do CNJ nº 182, de 17 de outubro de 2013;

e) Às disposições contidas na Lei Federal nº 9.472, de 16 de julho de 1997, com as respectivas alterações posteriores.

Quando a conformidade técnica, a contratação em estudo deverá obedecerá às seguintes normas:

a) **ITU-T G.703 (11/2011)** – *Physical/electrical characteristics of hierarchical digital interfaces*;

b) **ANSI/TIA/EIA-568-B.3** – Commercial Building Telecommunications Cabling Standard – Part 3: *Optical Fiber Cabling components standard*;

c) **ANSI/TIA/EIA-568-B.3-1** – *Commercial Building Telecommunications Cabling Standard – Part* 3: *Optical Fiber Cabling components standard – Addendum* 1 – *Additional Transmission Performance Specifications for* 50/125 µm *Optical fiber cables*;

d) **ANSI/TIA/EIA-569-B** – *Commercial Building Standard for Telecommunications Pathways and Spaces*;

e) **RESOLUÇÃO ANATEL nº. 242, de 30/11/2000** – Regulamento para certificação e homologação de produtos para telecomunicações;

2.13. Das obrigações

2.13.1. Das obrigações do CONTRATANTE

a) Permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, o acesso às unidades para a execução das atividades, respeitadas as normas de segurança vigentes nas suas dependências.

b) Notificar a CONTRATADA quanto a defeitos ou irregularidades verificados na execução das atividades objeto deste Termo de referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o Tribunal.

c) Indicar os locais onde deverão ser instalados os equipamentos, caso necessários, e proporcionar à CONTRATADA as facilidades e instruções necessárias para a realização do serviço de instalação.

d) Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA conforme determina a lei, antes de efetuar o pagamento devido.

e) Promover a fiscalização do contrato, sob os aspectos quantitativo e qualitativo, por intermédio de profissional designado, anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos serviços, podendo ainda sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais.

f) Comunicar tempestivamente à CONTRATADA as possíveis irregularidades detectadas na execução das atividades.

g) Confeccionar Termo de Recebimento Definitivo para o item do LOTE.

h) Observar para que durante a vigência do contrato sejam cumpridas as obrigações assumidas pela CONTRATADA, bem como sejam mantidas todas as condições de qualificação exigidas no processo de contratação.

2.13.2. Das obrigações da CONTRATADA

a) Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD). Para a habilitação, o licitante deverá apresentar Declaração indicando o encarregado responsável pela proteção de dados, nos termos do art. 41 da Lei Federal nº 13.709/18.

b) Cumprir fielmente o instrumento contratual, de modo que os serviços sejam realizados com segurança e perfeição, executando-os sobre sua inteira e exclusiva responsabilidade, de acordo com as Especificações Básicas constantes neste Termo de Referência;

c) Fornecer os recursos materiais e humanos necessários à execução dos serviços objeto do contrato, responsabilizando-se por todas as despesas e encargos, de qualquer natureza,

exceto quando se tratar de atividades expressamente atribuídas ao TJPA, segundo a lei, o edital ou o contrato;

d) Designar preposto responsável pelo atendimento ao TJPA, devidamente capacitado e com poderes para decidir e solucionar questões pertinentes ao objeto do contrato;

e) Manter atualizados os dados bancários para os pagamentos e os endereços, telefones e e-mail para contato;

f) Solicitar, em tempo hábil, todas as informações de que necessitar para o cumprimento das suas obrigações contratuais, exceto aquelas que são de fornecimento obrigatório pelo TJPA, nos termos do contrato.

g) Prestar os esclarecimentos solicitados pelo TJPA, no prazo máximo de 05 (cinco) dias quanto à execução dos serviços;

h) Acatar integralmente as exigências do TJPA quanto à execução dos serviços, inclusive providenciando a imediata correção das deficiências apontadas;

i) Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento deste contrato;

j) Remeter as correspondências destinadas ao TJPA e decorrentes da execução deste contrato à atenção da Secretaria de Informática – SECINFO, mais especificamente ao gestor do Contrato, citando o número do contrato a que se referem;

k) Manter, durante toda a execução dos serviços, as condições de habilitação e qualificação exigidas na contratação, informando ao TJPA a superveniência de eventual ato ou fato que modifique aquelas condições;

l) Efetuar o pagamento de multas, indenizações ou despesas impostas por órgãos fiscalizadores da atividade da CONTRATADA, bem como suportar o ônus decorrente de sua repercussão sobre o objeto deste contrato;

m) Efetuar o pagamento de seguros, impostos, taxas e serviços, encargos sociais e trabalhistas, indenizações por acidente de trabalho e quaisquer despesas decorrentes de sua condição de empregadora, referente aos serviços, inclusive licença em repartições públicas, registros, publicação e autenticação do contrato e dos documentos a ele relativos, se necessário;

n) Fiscalizar o cumprimento do objeto do contrato, cabendo-lhe integralmente os ônus daí decorrentes, necessariamente já incluídos no preço contratado, independentemente da fiscalização exercida pelo TJPA;

o) Assegurar ao TJPA o direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o

recebimento de cada parcela, de forma permanente, permitindo ao TJPA distribuir, alterar e utilizar estes sem limitações;

p) Assegurar ao TJPA os direitos autorais da solução do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa do TJPA, sob pena de rescisão contratual e multa;

q) Comprovar a origem de bens importados e a quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega, sob pena de rescisão contratual e multa;

r) São de responsabilidade da CONTRATADA eventuais transtornos ou prejuízos causados ao TJPA, provocados por imprudência, imperícia, negligência, atrasos ou irregularidades cometidas na execução dos serviços contratados;

s) O TJPA fica autorizado a descontar o valor correspondente aos danos sofridos da garantia do Contrato ou dos pagamentos devidos à CONTRATADA.

3. ESPECIFICAÇÃO TÉCNICA DETALHADA

3.1. Dos papeis a serem desempenhados

Em atenção à legislação vigente, especialmente no que diz respeito a Resolução nº 182/2013 do CNJ e as Portarias nº 684/2020 e 685/2020, resume-se papeis e responsabilidades relacionados à contratação e fiscalização:

PAPEL	ENTIDADE	RESPONSABILIDADE
Equipe de Apoio da Contratação	TJPA	Equipe responsável por subsidiar a área de licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes.
Equipe de Gestão e Fiscalização do Contrato	TJPA	Equipe composta pelo gestor do contrato, responsável por gerir a execução contratual, e pelos fiscais demandante, técnico e administrativo, responsáveis por fiscalizar a execução contratual.
Fiscal Demandante do Contrato	TJPA	Servidor representante da área demandante da contratação, indicado pela referida autoridade competente, responsável por fiscalizar o contrato quanto aos aspectos funcionais do objeto, inclusive em relação à aplicação de sanções.
Fiscal Técnico do Contrato	TJPA	Servidor representante da área técnica, indicado pela respectiva autoridade competente, responsável por

		fiscalizar o contrato quanto aos aspectos técnicos do objeto, inclusive em relação à aplicação de sanções.
Fiscal Administrativo do Contrato	TJPA	Servidor representante da Secretaria de Administração, indicado pela respectiva autoridade, responsável por fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.
Gestor do Contrato	TJPA	Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente do órgão.
Preposto	Contratada	Funcionário representante da empresa contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

Equipe de apoio da contratação (quando se tratar de licitação)		
Integrante Demandante Nome: Arilson Galdino da Silva Matrícula: 183318 Telefone: 3289-7181 Email: arilson.silva@tjpa.jus.br	**Integrante Técnico** Nome: Claudio Luis da Silva Cabral Matrícula: 11646-7 Telefone: (91) 3289-7195 E-mail: claudio.cabral@tjpa.jus.br	**Integrante Administrativo** Nome: Lenne Chaves Pinto da Silva Torres Matrícula: 6499-8 Telefone: 3205-3275 Email: lenne.torres@tjpa.jus.br

Equipe de gestão e fiscalização da contratação			
Gestor do Contrato: Nome: Denison Leandro Serrão Soares Matrícula: 16231-1 Telefone: (91) 3289-7191 E-mail: denison.soares@tjpa.jus.br	**Fiscal Demandante:** Nome: Arilson Galdino da Silva Matrícula: 18331-8 Telefone: 3289-7181 Email: arilson.silva@tjpa.jus.br	**Fiscal Técnico** Nome: Claudio Luis da Silva Cabral Matrícula: 11646-7 Telefone: (91) 3289-7195 E-mail: claudio.cabral@tjpa.jus.br	**FISCAL ADMINISTRATIVO** Nome: Matrícula: Telefone: E-mail:

A CONTRATANTE, deverá indicar um servidor da Coordenadoria de Suporte Técnico (CST) para acompanhar a implantação, onde também, eventualmente e formalmente, delegará competências conforme as necessidades do projeto.

A CONTRATADA, deverá indicar um responsável técnico encarregado de dar suporte ao esclarecimento das exigências técnicas contratuais.

Para fins de contrato, a empresa contratada deverá designar seu “PREPOSTO”, ao qual serão transmitidas as instruções, orientações e normas para execução das obrigações contratuais.

Cabe ao PREPOSTO e ao RESPONSÁVEL TÉCNICO:

3.1.1. Coordenar, orientar e supervisionar toda a equipe técnica da CONTRATADA alocada para o cumprimento das obrigações contratuais, cabendo-lhe ainda, a delegação e distribuição das tarefas entre as equipes, garantindo o cumprimento dos níveis de serviço estabelecidos.

3.1.2. Responder prontamente a todos os questionamentos e solicitações do TJPA, informando-os das necessidades de intervenção, inclusive, se necessário, aquelas que sejam efetuadas através de terceiros.

3.1.3. Propor ao TJPA mudanças nas rotinas e procedimentos técnicos, quando julgar pertinente, visando a otimização de custos, a racionalização e melhoria de processos.

3.1.4. Participar, quando solicitado pelo Tribunal, de reuniões relativas às atividades sob sua gestão, fornecendo informações e relatórios, apresentando sugestões, e propondo soluções que julgue pertinentes e necessárias.

3.1.5. Acompanhar os resultados globais das atividades sob sua gestão, fornecendo subsídios e informações à Secretaria de Informática do TJPA, visando o tratamento das prioridades e do planejamento global.

3.1.6. Ser o ponto de contato entre o TJPA e a CONTRATADA, no que se refere as atividades executadas, posicionando os servidores da Secretaria de Informática quanto ao cumprimento das metas estabelecidas.

3.2. Da dinâmica de execução do contrato

3.3. Etapas

3.4. Dos prazos

3.4.1. Prazos de entrega dos bens/execução dos serviços

A CONTRATADA deverá executar todos os serviços correlatos à entrega, instalação e ativação da solução na Secretaria de Informática, localizada na Tv. Rui Barbosa, esquina com a Av. Nazaré, e também no Data Center do TJPA, localizado na Rod. Augusto Montenegro, no horário entre 08:00 e 14:00, de segunda a sexta-feira, ou em outros horários conforme a estrita necessidade técnico de eventual intromissão na infraestrutura do Data Center do TJPA que possa comprometer o bom

funcionamento dos serviços, ocasião em que os dias e horário serão formal, prévia e exclusivamente acordados com o responsável do TJPA pela coordenação da implantação.

O prazo de entrega dos bens adquiridos e de serviços prestados deverá ser executado de acordo com os prazos máximos definidos no cronograma abaixo:

#	EVENTO	RESPONSÁVEL	PRAZO
1	Assinatura do Contrato.	CONTRATANTE e CONTRATADA	Até 6 (seis) dias após a convocação pelo CONTRATANTE.
2	Entrega de todos os componentes da solução.	CONTRATADA	Até 60 (sessenta) dias após o evento 1.
3	Conferência dos componentes da solução e Emissão do Termo de Recebimento Provisório	CONTRATANTE	Até 05 (cinco) dias após o evento 2.
4	Entrega da versão inicial do Plano de Configurações e Testes	CONTRATADA	Até 10 (dez) dias após o evento 1.
5	Aceite do Plano de Configurações e Testes	CONTRATANTE	Até 05 (cinco) dias após o evento 4.
6	Entrega da versão final do Plano de Configurações e Testes.	CONTRATADA	Até 2 (dois) dias úteis após o evento 5.
7	Configurações e Testes da Solução	CONTRATADA	Até 10 (dez) dias úteis após o evento 6.
8	Emissão do Termo de Recebimento Definitivo (TRD) da solução.	CONTRATADA	Até 5 (cinco) dias úteis após o evento 7.

Os equipamentos fornecidos pela CONTRATADA ficarão sob guarda do TJPA, que deverá se responsabilizar pela integridade dos mesmos.

O TJPA será responsável em cada edificação pela infraestrutura interna das salas onde ficarão alguns dos equipamentos da solução de UTM/SD-WAN destinados as unidades judiciárias no interior, tal como especificado a seguir: energia elétrica, climatização, unidades de fornecimento ininterrupto de energia (nobreak), cabeamento para conexão à rede interna de dados e aos equipamentos das operadoras, bem como switches de acesso, além dos armários de telecomunicações (racks). Adicionalmente, o TJPA será responsável pela disponibilização do espaço físico em rack-padronizado da Sala Segura do seu Data Center e pelas infraestruturas elétrica e de conectividade Ethernet para fornecer as devidas quantidades de portas e conectividade aos respectivos elementos centrais, objetivando a melhor interoperabilidade do equipamento a ser implantado.

Todos os prazos constantes da contratação serão contabilizados em dias corridos e a sua contagem excluirá os dias de início e de vencimento.

A CONTRATADA deverá entregar equipes de trabalho suficientes, bem como adequada gestão logística para suprimento de materiais, equipamentos e serviços necessários ao cumprimento do objeto do contrato.

A CONTRATANTE poderá determinar à execução dos serviços em horários alheios ao comercial, em feriados ou finais de semana, sem qualquer ônus extra ao TJPA, em caso de atrasos no cronograma ou quando explicitamente solicitado pela CONTRATADA, com vistas a execução do objeto nos prazos especificados.

Caso aconteça algum fato superveniente não motivado pela CONTRATADA, o fato deve ser informado à CONTRATANTE, mediante ofício protocolado na sede da CONTRATANTE. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados em até 02 (dois) dias úteis antes do término do prazo de entrega, e aceitos pela CONTRATANTE, não serão considerados como inadimplemento contratual.

O prazo de entrega de todos os equipamentos nas dependências do TJPA é de 60 (sessenta) dias. Em conjunto com a entrega dos equipamentos deverão ser entregues todas as notas fiscais de hardware.

A etapa de conferência (Evento 3) engloba apenas o recebimento dos equipamentos, conferências técnicas, quantitativo, número de série e nota fiscal.

3.4.2. Prazo de vigência do contrato

O prazo de vigência do contrato assinado será de 60 (sessenta) meses, a partir da data da assinatura.

3.4.3. Logística de implantação

A CONTRATADA realizará as configurações iniciais e testes de todos equipamentos, devidamente acompanhada da equipe técnica da CONTRATANTE.

Somente após a configuração e teste da solução (conclusão da Etapa 7), a vigência da garantia dos equipamentos terá início, de forma que os equipamentos, prontos para receberem os dados de produção, já possuam essa cobertura contratual.

Após a entrega, instalação, ativação dos equipamentos e licenças e a entrega da documentação, a equipe técnica da CONTRATANTE fará a conferência final da solução de TI contratada, através da vistoria das instalações físicas, caso necessário, e via console de gerenciamento dos equipamentos, que deverá ser entregue junto com a solução, visando verificar se ainda restam pendências contratuais a serem cumpridas.

O aceite da solução, para efeito de emissão do Termo de Recebimento Definitivo (TRD), será dado após entrega, conferência, instalação, configuração, incluídas a documentação exigida e acesso ao suporte técnico. Todos os elementos que compõem o objeto deste edital deverão estar disponíveis para que seja emitido o TRD.

A logística e implantação dos equipamentos nas localidades é de responsabilidade da CONTRATANTE, que deve elaborar o cronograma a ser aprovado pela Secretaria de Informática.

3.4.4. Cronograma

O cronograma de implantação nas localidades será definido posteriormente pela equipe técnica do TJPA, a ser definido após a conclusão do Evento 7.

3.5. Dos instrumentos formais de solicitação

As comunicações formais ocorrerão, preferencialmente, por e-mail, especialmente no que tange à formalização de pedidos, prazos e intercâmbio de documentação, sem prejuízo da utilização de recursos telefônicos quando da prestação da garantia e dos seus serviços atrelados de suporte técnico ou quando couber a agilização do contato para a consecução de atividade específica, ficando estas discricionariamente a cargo da CONTRATANTE.

3.6. Garantia e Nível de Serviço

3.6.1 Garantia do produto/serviço

De acordo com o item 3.6.3 dos estudos preliminares, o prazo de garantia da solução deverá ser de 60 (sessenta) meses.

3.6.2 Garantia contratual

A CONTRATADA, no prazo de 10 (dez) dias corridos, após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, podendo optar por qualquer das modalidades previstas no Art. 56, da Lei n° 8.666, de 1993.

3.6.3 Nível de Serviço

O serviço de atendimento para abertura de chamados devem estar disponíveis 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, em horário integral.

Por início de atendimento entende-se o contato com técnico responsável pelo acompanhamento do chamado.

O prazo de atendimento deve começar a ser contabilizado a partir do momento de efetivação da abertura do suporte, através de telefone ou e-mail.

Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhar e controlar a execução dos chamados.

Os serviços de Suporte e Garantia do equipamento devem ser em regime de 5x8xNBD, modalidade Next Business Day (próximo dia útil comercial), durante o período mínimo de 60 (sessenta) meses para toda a solução, contados da data em que ocorrer recebimento definitivo dos bens.

O problema dos equipamentos defeituosos, caso comprovado, deverá ser sanado dentro dos tempos estipulados. Quando não for possível solucionar o problema no prazo estipulado, caso autorizado após avaliação por representante da Secretaria de Informática, deverá ser fornecido outro equipamento de igual configuração ou superior, até resolução definitiva do problema.

Os chamados deverão ser resolvidos em até 3 (três) dias úteis, contados do primeiro dia útil seguinte à abertura do mesmo. Findo o prazo de 3 (três) dias úteis, sem a resolução do problema, deverá a CONTRATADA disponibilizar em até 24 horas equipamento de especificação igual ou superior para operação temporária como substituição do equipamento em conserto, o qual deverá ser avaliada e autorizado por representante do Secretaria de Informática, não ultrapassando o prazo máximo de 30 (trinta) dias para a solução definitiva do problema.

Substituir qualquer equipamento durante o prazo de suporte se, em um período de 6 (seis) meses, ocorrer mais de 3 (três) chamados referentes ao mesmo problema (desde que a causa-raiz do mesmo tenha sido atribuída ao equipamento), ou mais de 5 (cinco) chamados referentes a problemas distintos (desde que a causa-raiz dos mesmos tenha sido atribuída ao equipamento).

3.7. Da forma de comunicação e acompanhamento da execução do contrato

A CONTRATADA deverá fornecer previamente os contatos de e-mail e telefone dos envolvidos na execução do objeto da contratação. Estes serão os principais canais de comunicação a serem utilizados durante a execução do contrato, devendo a comunicação ser realizada preferencialmente por e-mails, para geração de registros documentais. Pela CONTRATANTE, os componentes da Equipe de Gestão e Fiscalização da Contratação se encarregarão da comunicação com a CONTRATADA no tocante à execução do contrato.

3.8. Do recebimento

3.8.1 Do recebimento provisório e definitivo

Com o objetivo de verificar sua conformidade com as especificações constantes neste Termo de Referência, o recebimento dos bens será realizado:

Provisoriamente, no ato da entrega dos equipamentos, para posterior verificação de conformidade dos bens com as especificações constantes neste Termo de Referência.

Definitivamente, no prazo máximo de até 30 (trinta) dias corridos, contados a partir da data de assinatura do Termo de Recebimento Provisório.

O TJPA designará equipe específica para o recebimento e conferência dos produtos integrantes do objeto deste Termo de Referência.

A equipe técnica designada pelo TJPA será responsável pela conferência e avaliação dos serviços de instalação, configuração prestados pela empresa contratada, além de avaliar as atividades de gerenciamento da execução do projeto e a realização dos testes de todo ambiente implementado.

Os materiais que forem entregues em desacordo com o especificado deverão ser substituídos pela contratada em até 10 (dez) dias úteis. O seu descumprimento poderá acarretar sanções conforme previsto na legislação vigente;

Caso após o Recebimento Provisório constatar-se que os materiais possuem vícios aparentes ou redibitórios ou estão em desacordo com as especificações ou a proposta, serão interrompidos os prazos de recebimento e suspenso o pagamento até que sanado o problema;

O Recebimento Provisório ou Definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem a responsabilidade pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou por este instrumento

Em caso de treinamento, a contratada deverá apresentar os certificados de conclusão do curso emitidos para os participantes bem como, documento fiscal com a identificação do comprador (Tribunal), descrição do serviço entregue, quantidade, preços unitário e total.

3.9. Da forma de pagamento

Para efeito de pagamento, a Contratada deverá apresentar os seguintes documentos:

3.9.1 Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – FGTS, fornecido pela CEF – Caixa Econômica Federal, devidamente atualizado (Lei n.º 8.036/90);

3.9.2 Prova de regularidade com a Fazenda Federal por meio da Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais, inclusive contribuições previdenciárias, e a Dívida Ativa da União, expedida pelo Ministério da Fazenda/Secretaria da Receita Federal do Brasil (Portaria Conjunta RFB/PGFN nº 1.751/2014);

3.9.3 Certidão de Regularidade com as Fazendas Estaduais e Municipais da sede da licitante.

3.9.4 Certidão de regularidade relativa a débitos inadimplidos perante o Poder Judiciário do Pará, mediante a apresentação de certidão negativa, em plena validade.

O pagamento será efetuado em até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal, desde que o documento de cobrança esteja em condições de liquidação de pagamento.

Passados 30 (trinta) dias sem o devido pagamento por parte da Administração, a parcela devida será atualizada monetariamente, desde o vencimento da obrigação até a data do efetivo pagamento de acordo com a variação “pro rata tempore” do IPCA.

Nenhum pagamento será efetuado ao licitante enquanto pendente de liquidação qualquer obrigação que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

A retenção dos tributos não será efetivada caso a contratada apresente junto com sua Nota Fiscal a comprovação de que ele é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES.

Documentos de cobrança rejeitados por erros ou incorreções em seu preenchimento serão formalmente devolvidos à Contratada, no prazo máximo de 5 (cinco) dias úteis contados da data de sua apresentação.

Os documentos de cobrança, escoimados das causas que motivaram a rejeição, deverão ser reapresentados num prazo máximo de 2 (dois) dias úteis.

Em caso de rejeição da Nota Fiscal/Fatura, motivada por erro ou incorreções, o prazo de pagamento passará a ser contado a partir da data de sua reapresentação.

Esta contratação foi relacionada no Plano de Orçamentário deste Tribunal e no Plano de Contratações de Soluções de TIC para o referido exercício.

Os valores decorrentes dessa despesa foram previstos na dotação orçamentária própria do Tribunal de Justiça do Estado do Pará, referente a Secretaria de Informática, vigente para o exercício de 2021, na ordem de R$ 2.048.320,00 (dois milhões, quarenta e oito mil e trezentos e vinte reais) para adquirir apenas 50 unidades. Como houve a abrangência do projeto para atender mais unidades do TJPA, a quantidade de equipamentos passou a ser 67 unidades, o que onerou o valor em R$ 63.462,38 (sessenta e três mil, quatrocentos e sessenta e dois reais e trinta e oito centavos), devendo ser complementado pela SECINFO para perfazer o valor total da solução. As tratativas para a complementação deste valor seguem no expediente PA-MEM-2021/32616, onde as provisões orçamentárias se darão nas ações 8651, 8652 e 8653, elemento de despesa 4.4.90.52, a qual será rateada em 65% no 1º Grau, 9% no 2º Grau e 26% no Apoio Indireto.

3.10. Da transferência de conhecimento

Como se trata de uma solução já conhecida pela equipe técnica do TJPA que será implantada na infraestrutura tecnológica do Tribunal, não houve a necessidade em contratar o serviço específico de treinamento.

A CONTRATADA realizará as configurações inicias da solução, devendo apresentar toda documentação relacionada às configurações, topologia, endereçamento de rede e afins.

Adicionalmente, durante toda a configuração inicial da solução, os técnicos da CONTRATADA deverão demonstrar à Equipe Técnica de Acompanhamento da CONTRATANTE os procedimentos de instalação e configuração dos equipamentos e os procedimentos de operação dos componentes da solução. Todo o processo de instalação e configuração deverá ser documentado pela CONTRATADA sob a forma de relatório ou roteiro, de modo que a Equipe Técnica do TJPA possa absorver o conhecimento e aplica-lo quando for necessário.

3.11. Dos direitos de propriedade intelectual e autoral

Após a completa implantação da solução adquirida e atestado que a solução está em conformidade com todos os itens do contrato firmado, tanto em termo de qualidade, quando em quantidade, será emitido um TRD (Termo de Recebimento Definitivo) da solução, caracterizando a transferência definitiva da solução e de todos os componentes necessários para o seu total funcionamento, para o Tribunal.

Eventuais softwares que são necessários ao funcionamento da solução são de propriedade do fabricante e deverão ser fornecidos em conjunto com o respectivo hardware, sendo que os direitos de propriedade intelectual pertencem ao fabricante da solução, de acordo com a Lei 9609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador Concluída a execução dos serviços e comprovada a qualidade e a quantidade do objeto, bem como sua conformidade com todas as condições exigidas em contrato, será emitido o TERMO DE RECEBIMENTO DEFINITIVO da solução. Neste momento, ocorrerá a transferência de propriedade da solução (incluindo-se todos os equipamentos e softwares) para o TJPA.

Quanto à documentação produzida (projetos, relatórios, manuais, etc), os direitos de propriedade autoral sobre os projeto, planos, desenhos, diagramas e esboços produzidos durante a vigência contratual pertencerão à empresa contratada e, respeitadas as relações contratuais expressas entre o autor e outros interessados, ao profissional que os elaborar.

Vale ressaltar que a empresa contratada se limita a projetar a implantação da solução de UTM/SD-WAN idealizada pelo TJPA e constante nos projetos preliminares apresentadas antes da emissão de toda e qualquer ordem de fornecimento de serviço. Em resumo, as atividades compreendem a análise e a validação dos desenhos produzidos, bem como a estimativa dos quantitativos de materiais e serviços necessários para sua execução. Tal condição não apenas limita o direito autoral, mas também permite ao TJPA a manipulação e a modificação da referida documentação, respeitando-se a titularidade na autoria.

Eventuais softwares, necessários ao funcionamento da solução contratada, são próprios dos fabricantes e deverão ser fornecidos em conjunto com os equipamentos correspondentes. Os direitos

de propriedade intelectual sobre estes produtos pertencem à empresa fabricante da solução, tal como dispõe o art. 2ª, § 2º e § 3º da Lei Federal 9609/98 que versa sobre a propriedade intelectual dos programas de computador.

3.12. Da qualificação técnica dos profissionais

Sem prejuízo do especificado neste Termo de Referência, toda a documentação relativa à qualificação técnica dos representantes da CONTRATADA deverá ser apresentada e analisada quando da assinatura do contrato.

Ainda assim, o TJPA reserva-se ao direito de, a qualquer momento e a seu exclusivo critério, exigir o reenvio de documentação recente e atualizada, inclusive quanto ao registro ou inscrição da empresa na entidade profissional competente e quanto a qualificação profissional doas agentes envolvidos na execução dos serviços.

A não apresentação da documentação exigida caracterizará a falta e habilidades e competências mínimas para a execução do objeto contratual, dando a entender que pode representar risco ao processo e que não possui capacidade ou apoio do fabricante em sua proposição.

3.13. Das sanções

Pela inexecução total ou parcial do objeto contratual, a Administração do Tribunal de Justiça do Estado do Pará poderá aplicar a CONTRATADA as sanções de natureza pecuniárias e restritivas de direito pelo descumprimento das normas previstas neste Termo de Referência e dos contratos dele decorrentes, bem como pela prática das condutas tipificadas nos arts. 81, 86, 87 e 88 da Lei 8.666/93 e artigo 7º da Lei 10.520/2002, também obedecerão às prescrições do Decreto 26.851/2006 e alterações posteriores.

Aplicam-se aos Licitantes nessa aquisição todas as disposições referentes às Práticas Proibidas e à incorporação do reconhecimento recíproco de sanções por parte de Instituições Financeiras Internacionais (IFI), conforme disposto no Anexo deste Edital e no site do Banco (www.iadb.org/integrity).

3.13.1 Multa

- Multa moratória de 5% (cinco por cento) sobre o valor do Contrato, pela recusa da CONTRATADA em assinar contrato e pela não apresentação da documentação exigida no Edital para sua celebração, nos prazos e condições estabelecidas, caracterizando o descumprimento total da obrigação assumida, com base no art. 81 da Lei 8.666/93, independentemente das demais sanções cabíveis;
- Multa moratória de 0,33% (zero vírgula trinta e três por cento) sobre o valor do item ou conjunto de itens, por dia de atraso, no caso da CONTRATADA não entregar e/ou não

instalar os equipamentos no prazo estipulado no item 3.4.1, até o limite máximo de 30 (trinta) dias.

- Multa moratória de 5% (cinco por cento) sobre o valor do Contrato, pela inexecução parcial, total ou execução insatisfatória do contrato, aplicada em dobro na sua reincidência, ou pela interrupção da execução do contrato sem prévia autorização da CONTRATANTE, independentemente das demais sanções cabíveis;
- Multa moratória de 1% (cinco por cento) sobre o valor do Contrato, pela recusa em corrigir qualquer objeto rejeitado ou com defeito, caracterizando-se a recusa caso a correção não se efetive nos 10 (dez) dias que se seguirem à data de comunicação formal da rejeição ou defeito, independentemente das demais sanções cabíveis;
- Multa moratória de 1% (cinco por cento) sobre o valor do Contrato, pelo não cumprimento dos prazos estipulados nos Acordos de Níveis de Serviço (ANS), de acordo com o item 3.4.1, sem justificativa prévia aceita pela CONTRATANTE, independentemente das demais sanções cabíveis;
- Multa compensatória de 10% (dez por cento) sobre o valor do Contrato, sendo deste valor deduzido o(s) valor(es) referente(s) às multa(s) moratória(s), no caso de rescisão do Contrato por ato unilateral da administração, motivado por culpa da CONTRATADA, garantida a defesa prévia e o contraditório, independentemente das demais sanções cabíveis.

As multas previstas neste Termo de Referência poderão ser aplicadas, cumulativamente ou não com as demais sanções administrativas previstas na legislação aplicável e vigente.

A inobservância do prazo fixado para apresentação da garantia contratual acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento)

O atraso ou a suspensão injustificada na execução do objeto a ser contratado, por período superior a 30 (trinta) dias, poderá ensejar a rescisão do contrato emergencial.

As multas aplicadas serão descontadas do valor da garantia contratual. Se for insuficiente, além de perder a garantia, responderá a CONTRATADA pela sua diferença, que será descontada dos pagamentos eventualmente devidos pelo TJPA. Se preferir, poderá a CONTRATADA recolher as multas no prazo de 05 (cinco) dias úteis a contar da comunicação oficial.

Na ausência/insuficiência de garantia e de créditos para desconto das multas, e se estas não foram recolhidas no prazo estipulado anteriormente, as multas aplicadas serão cobradas judicialmente.

Em sendo a garantia utilizada para o pagamento de multas, compromete-se a empresa CONTRATADA a complementar ou apresentar nova garantia no prazo de 05 (cinco) dias úteis.

Da aplicação das previstas inicialmente caberá recurso, no prazo de 05 (cinco) dias úteis, contados da notificação oficial, que será dirigido à autoridade superior, por intermédio da que praticou o ato, a qual poderá reconsiderar a sua decisão ou fazê-lo subir devidamente informado.

As penalidades serão obrigatoriamente registradas no SICAF e, no caso de impedimento de licitar, por descumprimento parcial ou total do contrato, a CONTRATADA deverá ser descredenciada por igual período, ou seja, por prazo não superior a 5 (cinco) anos, conforme atr. 7º da Lei nº 10.520, de 17 de julho de 2002, sem prejuízo das multas previstas no instrumento convocatório e das demais combinações legais.

4. Da confidencialidade de informações

Os conhecimentos, dados e informações de propriedade do CONTRATANTE, tanto tecnológicos, como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.

Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento da execução das cláusulas e condições estabelecidas no contrato, sendo expressamente vedado à CONTRATADA:

a) Utilizá-las para fins não previstos no instrumento contratual;

b) Repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado.

5. DOS REQUISITOS TÉCNICOS ESPECÍFICOS

5.1. CARACTERISTICAS GERAIS

5.1.1. Solução de proteção de rede com características de Firewall Next Generation (NGFW) com SD-WAN integrada do tipo Appliance. A solução deve ser integralmente do mesmo fabricante, contemplando gerência centralizada, todos os softwares e suas licenças de uso, possibilitando atualização contínua. Deve incluir, além das funcionalidades citadas acima: Otimização de WAN, gerenciamento centralizada, zero-touch deployment, filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN, IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta. Na qual todos os links WANs e VPNs devem funcionar simultaneamente.

5.1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance com todas as licenças necessárias inclusas, o sistema operacional fornecido deve ser a versão mais nova disponível, devendo, entretanto, ser considerada estável pelo fabricante do equipamento.

5.1.3. Os hardwares e softwares ofertados na composição deste item não devem estar listados como “end-of-sale”, “end-of-support” ou “end-of-life” por seus respectivos fabricantes na data da abertura das propostas. Não serão aceitos equipamentos que entrem em modo End of Support durante a vigência da garantia ou que entre em modo End of Life pelo período de 1 ano após a assinatura do contrato.

5.1.4. A solução de NGFW deverá suportar mecanismos de redundância de dispositivos em modo ativo-passivo e ativo-ativo, em caso de falha de um dos equipamentos.

5.1.5. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelo firewall.

5.1.6. A solução deve contemplar gerenciamento centralizado e integrado de todos os dispositivos da sede e filiais, que possibilite que as configurações, controle de acesso, regras e políticas sejam executadas em um único ponto e replicadas para todos os dispositivos, grupos de dispositivos, usuários, grupos de usuários.

5.1.7. O equipamento deve permitir a gestão e monitoramento através da interface de gestão WEB no mesmo dispositivo de proteção da rede.

5.1.8. Permitir controle global e centralizado de políticas para todos os equipamentos que compõe a plataforma de segurança.

5.1.9. Deve possuir LEDs indicadores de status, atividade de rede, status dos links e alimentação.

5.1.10. A funcionalidade de Sandbox deve ser executada em nuvem pelo próprio fabricante, devendo o NGFW estar devidamente licenciado para possibilitar a execução desta função.

5.1.11. O hardware e software que executa as funcionalidades de proteção de rede firewall (NGFW) e SD-WAN deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

5.1.12. Os appliances que executarão a função de NGFW deverão ter altura máxima de 1 (um) U de espaço em rack.

5.1.13. O software deverá ser fornecido em sua versão mais atualizada e estável.

5.1.14. Deve ser fornecido com a versão de software mais recente disponível para o equipamento.

5.1.15. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento de todos os recursos descritos e exigidos neste termo para o prazo mínimo de 05 anos.

5.1.16. Os equipamentos deverão ser fornecidos de acordo com as características técnicas mínimas presentes neste Termo de Referência.

5.1.17. A solução deverá ser capaz de fechar túneis VPN do tipo IPSec com equipamentos de terceiros (Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall).

5.1.18. Todos os itens de hardware e software fornecidos pela PROPONENTE deverão ser da mesma marca e fabricante. A padronização da marca garante que os equipamentos adquiridos sejam 100% compatíveis entre si, permitindo a proteção de investimento a ser realizado por este órgão. Desta forma, faz-se necessária a aquisição de produtos de mesma marca e fabricante, com o fim de garantir a interoperabilidade e possibilidade de operar em Alta Disponibilidade entre si.

5.2. FUNCIONALIDADES

5.2.1. Suporte a 4094 VLAN Tags 802.1q.

5.2.2. Suporte a 4094 VLAN Tags 802.1q;

5.2.3. Agregação de links 802.3ad e LACP;

5.2.4. Policy based routing ou policy based forwarding;

5.2.5. Roteamento multicast (PIM-SM e PIM-DM);

5.2.6. DHCP Relay;

5.2.7. DHCP Server;

5.2.8. Jumbo Frames;

5.2.9. Os dispositivos de proteção de rede devem suportar sFlow;

5.2.10. Suportar sub-interfaces ethernet logicas.

5.2.11. Deve suportar os seguintes tipos de NAT:

5.2.11.1. Nat dinâmico (Many-to-1);

5.2.11.2. Nat dinâmico (Many-to-Many);

5.2.11.3. Nat estático (1-to-1);

5.2.11.4. NAT estático (Many-to-Many);

5.2.11.5. Nat estático bidirecional 1-to-1;

5.2.11.6. Tradução de porta (PAT);

5.2.11.7. NAT de Origem;

5.2.11.8. NAT de Destino;

5.2.11.9. Suportar NAT de Origem e NAT de Destino simultaneamente

5.2.12. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

5.2.13. Deve implementar o protocolo ECMP;

5.2.14. Portas UDP, uma ou um range;

5.2.15. Portas TCP, uma ou um range;

5.2.16. Deve implementar balanceamento de link por hash do IP de origem;

5.2.17. Deve implementar balanceamento de link por hash do IP de origem e destino;

5.2.18. Deve implementar balanceamento de link através do método round-robin;

5.2.19. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

5.2.20. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

5.2.21. Seleção do melhor caminho que o tráfego da sessão leva com base na qualidade do circuito baseado em Latência, Perda "Loss" e Jitter;

5.2.22. A solução deve ser capaz de detectar perda, aumento de latência e jitter de um caminho, quando este começa a degradar a qualidade de uma aplicação. Deslocando o tráfego da aplicação para outro circuito de dado que esteja com melhor desempenho de forma

transparente para os usuários, sem que seja percebido interrupção na continuidade do aplicativo ou dos pacotes perdidos;

5.2.23. Deve implementar balanceamento de link através de políticas por aplicação, conforme regras de negócio;

5.2.24. Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;

5.2.25. Enviar log para sistemas de monitoração externos, simultaneamente;

5.2.26. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

5.2.27. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

5.2.28. Proteção contra anti-spoofing;

5.2.29. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

5.2.30. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

5.2.31. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

5.2.32. Para IPv6, deve suportar roteamento estático e dinâmico (RIPv6, BGP4+, OSPFv3);

5.2.33. Suportar a OSPF graceful restart;

5.2.34. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, DHCPv6 Server, IPSec, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;

5.2.35. Dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);

5.2.36. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

5.2.37. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

5.2.38. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

5.2.39. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

5.2.40. Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

5.2.40.1. Em modo transparente;

5.2.40.2. Em Layer 3;

5.2.41. A configuração em alta disponibilidade deve sincronizar:

5.2.41.1. Sessões;

5.2.41.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

5.2.41.3. Certificados de-criptografados;

5.2.41.4. Associações de Segurança das VPNs;

5.2.41.5. Sincronizar tabelas FIB;

5.2.42. HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

5.2.43. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

5.2.44. As funcionalidades de NGFW e SD-WAN, controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

5.3. CONTROLE POR POLÍTICA DE FIREWALL

5.3.1. Deverá suportar controles por zona de segurança;

5.3.2. O Firewall deverá possuir controles de segurança de camada L4 - L7;

5.3.3. A solução de firewall deve atuar na camada de aplicação possibilitando ao administrador criar regrar e impedir a utilização de aplicações (deep packet inspection);

5.3.4. Controles de políticas por porta e protocolo;

5.3.5. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

5.3.6. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

5.3.7. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

5.3.8. Controle de políticas por código de País ou geolocalização (Por exemplo: BR, USA, UK, RUS);

5.3.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

5.3.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

5.3.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

5.3.12. Controle de inspeção e de-criptografia de SSH por política;

5.3.13. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

5.3.14. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

5.3.15. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

5.3.16. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

5.3.17. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

5.3.18. Suporte a objetos e regras IPV6;

5.3.19. Suporte a objetos e regras multicast;

5.3.20. Deve possibilitar a utilização de no mínimo 04 ações nas regras de controle como Permitir, Bloquear;

5.3.21. Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário e TCP-Reset para o cliente;

5.3.22. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

5.3.23. O controle por políticas de firewall deverá ser integrado no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

5.4. CAPACIDADE

5.4.1. Throughput de, no mínimo, 02 (dois) Gbps com a funcionalidade de firewall habilitada;

5.4.2. Throughput de no mínimo 450 (quatrocentos e cinquenta) Mbps com a funcionalidade de controle de aplicação e logs habilitada;

5.4.3. Throughput de no mínimo 160 (cento e sessenta) Mbps com as seguintes funcionalidades habilitadas: controle de aplicação, IPS, Antivírus e Anti-Spyware e log. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, todas deverão ter valor superior ao throughput requerido;

5.4.4. Capacidades (throughput) comprovadas por documento de domínio público disponibilizado pelo fabricante, não sendo admitida a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

5.4.5. Efetividade de Segurança mínima de 80%, classificados como recomendado em Security Value Map (SVM) Comparative Report para Next Generation Firewall (NGFW) da NSSLabs ou certificação ICSA Labs para o ano de 2018 ou posterior, seja para o modelo apresentado ou para equipamento da mesma linha que possua mesmo sistema operacional e engine de anti-vírus, comprovada por documento de domínio público;

5.4.6. Suporte a, no mínimo, 192 (Cento e noventa e dois) mil conexões simultâneas;

5.4.7. Suporte a, no mínimo, 13 (treze) mil novas conexões por segundo;

5.4.8. Fonte de alimentação automática 100-240V AC;

5.4.9. Possuir espaço em disco SSD interno com no mínimo 32 (trinta e dois) GB;

5.4.10. No mínimo 7 (sete) interfaces de rede gigabit Ethernet RJ45, devendo ser possível configurar ao menos 02 (duas) destas interfaces como WAN;

5.4.11. Possuir 01 (uma) interface do tipo console ou similar;

5.4.12. Suporte a, no mínimo, 20 (vinte) zonas de segurança;

5.4.13. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos;

5.4.14. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos.

5.5. CONTROLE DE APLICAÇÕES

5.5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

5.5.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

5.5.3. Reconhecer pelo menos 2000 (duas mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

5.5.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, onedrive, db2, mysql, oracle, active directory kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc .

5.5.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações customizadas e não somente sobre aplicações conhecidas;

5.5.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

5.5.7. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

5.5.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.5.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

5.5.10. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

5.5.11. Identificar o uso de táticas evasivas via comunicações criptografadas;

5.5.12. Atualizar a base de assinaturas de aplicações automaticamente;

5.5.13. Reconhecer aplicações em IPv6;

5.5.14. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

5.5.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

5.5.16. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

5.5.17. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

5.5.18. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

5.5.19. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, SMTP, Telnet, SSH, MS-SQL, IMAP, MS-RPC e RTSP.

5.5.20. Deve alertar o usuário quando uma aplicação for bloqueada;

5.5.21. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

5.5.22. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.) possuindo granularidade de controle/políticas para os mesmos;

5.5.23. Deve possibilitar a diferenciação de tráfegos para as seguintes aplicações e respectivas granularidades: Instagram (login, post, vídeo, upload de arquivo), YouTube (canais, streaming HD, pesquisa de vídeo, play vídeo), Facebook (upload e download de arquivos, login, chat, botão de like, chamadas VoIP, play vídeo, post, mensagem de voz), WhatsApp (transferência de arquivos, chamadas VoIP e whatsapp web);

5.5.24. Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para os mesmos;

5.5.25. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc); Nível de risco da aplicação; Categoria de aplicações;

5.5.26. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;

5.5.27. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

5.5.28. O controle de aplicações deverá ser integrado no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função

5.6. PREVENÇÃO DE AMEAÇAS

5.6.1. Para proteção do ambiente de redes contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;

5.6.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

5.6.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

5.6.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

5.6.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Anti-Spyware e Antivírus: permitir, permitir e gerar log, bloquear, e enviar tcp-reset;

5.6.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

5.6.7. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

5.6.8. Deve permitir o bloqueio de vulnerabilidades;

5.6.9. Deve permitir o bloqueio de exploits conhecidos;

5.6.10. Deve incluir proteção contra ataques de negação de serviços;

5.6.11. Fornecem proteção contra ataques de dia zero;

5.6.12. Deverá possuir os seguintes mecanismos de inspeção de IPS:

5.6.12.1. Análise de padrões de estado de conexões;

5.6.12.2. Análise de decodificação de protocolo;

5.6.12.3. Análise para detecção de anomalias de protocolo;

5.6.12.4. Análise heurística;

5.6.12.5. IP Defragmentation;

5.6.12.6. Remontagem de pacotes de TCP.

5.6.12.7. Bloqueio de pacotes malformados.

5.6.12.8. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;

5.6.12.9. Detectar e bloquear a origem de portscans;

5.6.12.10. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

5.6.12.11. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

5.6.12.12. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

5.6.12.13. Possuir assinaturas para bloqueio de ataques de buffer overflow;

5.6.12.14. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

5.6.12.15. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e Anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;

5.6.12.16. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

5.6.13. Suportar bloqueio de arquivos por tipo;

5.6.14. Identificar e bloquear comunicação com botnets;

5.6.15. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

5.6.16. Deve suportar referência cruzada com CVE;

5.6.17. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

5.6.17.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

5.6.18. Deve suportar a captura de pacotes (PCAP) por assinatura de IPS;

5.6.19. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

5.6.20. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

5.6.21. Os eventos devem identificar o país de onde partiu a ameaça;

5.6.22. Deve incluir proteção contra vírus em conteúdo HTML e Java script, software espião (Spyware) e worms;

5.6.23. Proteção contra downloads involuntários usando HTTP de arquivos executáveis;

5.6.24. Rastreamento de vírus em pdf;

5.6.25. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);

5.6.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem,

destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

5.6.27. A prevenção de ameaças deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

5.7. ANÁLISE DE MALWARE

5.7.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante sem custo adicional;

5.7.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

5.7.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

5.7.4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e suspeito;

5.7.5. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Android, MacOS, Windows 8, Windows 7 (32 bits) e Windows 7 (64 bits), Windows 10 (32bits) e Windows 10 (64 bits);

5.7.6. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

5.7.7. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

5.7.8. O sistema de análise “In Cloud” ou local deve gerar assinaturas de Antivírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

5.7.9. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (Sandbox) independentes para execução simultânea de arquivos suspeitos;

5.7.10. Caso seja necessário, licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (Sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

5.7.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

5.7.12. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em Sandbox com frequência;

5.7.13. A análise de Malware deverá ser integrada no próprio appliance de NGFW, não sendo aceito quaisquer componentes adicionais com esta função.

5.8. FILTRO URL

5.8.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

5.8.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

5.8.3. Incluir nativamente Explicit Web Proxy e proxy Web transparente;

5.8.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, base de dados local, inclusive em modo de proxy transparente e explicito;

5.8.5. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

5.8.6. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

5.8.7. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo). O Firewall deve ter mecanismo que implemente a navegação com o uso o Safe Search, independente da intervenção do usuário.

5.8.8. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

5.8.9. Possui pelo menos 60 categorias de URLs;

5.8.10. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

5.8.11. Suporta a criação categorias de URLs customizadas;

5.8.12. Suporta a criação de exceções nos bloqueios de filtro de URLs;

5.8.13. Permite a customização de página de bloqueio;

5.8.14. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

5.8.15. A funcionalidade de Filtro de URL, categorizada localmente, deve operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

5.8.16. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

5.8.17. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

5.8.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

5.9. IDENTIFICAÇÃO DE USUÁRIOS

5.9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, e base de dados local;

5.9.2. Deve possuir integração com Microsoft Active Directory e LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

5.9.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

5.9.4. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

5.9.5. Suporte a autenticação Kerberos;

5.9.6. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

5.9.7. Deve identificar usuários através de leitura do campo nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

5.9.8. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo de identificação do usuário;

5.9.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

5.9.10. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

5.10. QOS

5.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

5.10.2. Suportar a criação de políticas de QoS e traffic-shaping por:

5.10.2.1. Endereço de origem;

5.10.2.2. Endereço de destino;

5.10.2.3. Por usuário e grupo do LDAP/AD;

5.10.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

5.10.2.5. Por porta.

5.10.3. QoS deve possibilitar a definição de classes por:

5.10.3.1. Banda Garantida;

5.10.3.2. Banda Máxima;

5.10.3.3. Fila de Prioridade.

5.10.4. Suportar priorização Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

5.10.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

5.10.6. Deve implementar QoS (traffic-shaping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (Inbound e Outbound);

5.10.7. Disponibilizar estatísticas Real Time para classes de QoS;

5.10.8. Deve suportar QoS (traffic-shaping), em interface agregadas;

5.10.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

5.11. FILTRO DE DADOS

5.11.1. Permite a criação de filtros para arquivos e dados pré-definidos;

5.11.2. Os arquivos devem ser identificados por extensão, tipo e assinaturas (ou fingerprint);

5.11.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, SMTP, POP3, IMAP, MAPI, FTP e NNTP);

5.11.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

5.11.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

5.12. GEOLOCALIZAÇÃO

5.12.1. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

5.12.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

5.12.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

5.12.4. VPN

5.12.4.1. Suportar VPN Site-to-Site e Cliente-To-Site;

5.12.4.2. Suportar IPSec VPN;

5.12.4.3. Suportar SSL VPN;

5.12.4.4. A VPN IPSec deve suportar:

5.12.4.4.1. DES e 3DES;

5.12.4.4.2. Autenticação MD5 e SHA-1;

5.12.4.4.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

5.12.4.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);

5.12.4.4.5. AES 128, 192 e 256 (Advanced Encryption Standard);

5.12.4.4.6. Autenticação via certificado IKE PKI.

5.12.4.4.7. Deve possuir interoperabilidade com os seguintes fabricantes: Palo Alto Networks, Cisco, Check Point, Juniper, Fortinet, SonicWall;

5.12.4.4.8. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

5.12.4.5. VPN SSL deve suportar:

5.12.4.5.1. Usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

5.12.4.5.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente. Caso necessite de agente, deve estar licenciada para ou suportar sem o uso de licença, 50 (cinquenta) clientes de VPN SSL simultâneos;

5.12.4.5.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

5.12.4.5.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

5.12.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

5.12.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

5.12.7. Atribuição de DNS nos clientes remotos de VPN;

5.12.8. Deve suportar autenticação de clientes VPN a partir de diferentes sistemas operacionais remotos (Android, IOS, Mac Windows e Chrome OS);

5.12.9. A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;

5.12.10. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spywares e filtro de

5.12.11. URL para tráfego dos clientes remotos conectados na VPN SSL;

5.12.12. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

5.12.13. Suporta leitura e verificação de CRL (certificate revocation list);

5.12.14. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

5.12.15. Agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

5.12.16. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

5.12.17. Antes do usuário autenticar na estação;

5.12.18. Após autenticação do usuário na estação;

5.12.19. Sob demanda do usuário.

5.12.20. Deverá manter uma conexão segura com o portal durante a sessão;

5.12.21. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e Mac Osx.

6. PROPOSTA DE MODELOS A SEREM UTILIZADOS

O preço proposto para este fornecimento deve englobar os valores relativos a impostos, fretes, seguros, salários, suporte, garantia, encargos e demais despesas necessárias ao fornecimento completo do objeto.

As propostas comerciais deverão ser válidas, no mínimo, por 60 (sessenta) dias.

Deverá constar, obrigatoriamente, na proposta:

O preço unitário do item ofertado, considerando todos os componentes de hardware e software necessários à execução do serviço;

A descrição detalhada dos itens propostos, atendendo aos quantitativos e às especificações mínimas descritas neste Termo de Referência e em seus anexos, indicando os números de identificação dos serviços ofertados.

O fabricante poderá ser convocado a validar a compatibilidade dos itens e as declarações apresentadas, de modo a validar as condições de garantia existentes.

A proposta comercial, necessariamente, deverá atender a descrição dos itens propostos, conforme descrito neste Termo de Referência.

Todas as características técnicas obrigatórias deverão ser do fabricante e comprovadas por meio de folders, catálogos, manuais, impressão de páginas na Internet do fabricante ou testes realizados pelo CONTRATANTE, os quais deverão ser entregues juntamente com a proposta, em folhas numeradas e sequenciais.

7. INFORMAÇÕES COMPLEMENTARES

Não há

Belém, 19 de novembro de 2021

(ASSINATURA DOS MEMBROS DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO)

Local e data

_____