TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO

AQUISIÇÃO DE MATERIAIS

COMPANHIA DE SANEAMENTO DE SERGIPE – DESO

PREGÃO Nº_____/2021

(Processo Administrativo n.º 19717/2021)

1. DO OBJETO

Registro de Preços, pelo menor preço por lote, no prazo de 12 (doze) meses, para eventual e futura **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC), PARA AMPLIAÇÃO DA SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO, ENGLOBANDO O FORNECIMENTO DE TODO HARDWARE, SOFTWARE, SUBSCRIÇÕES, INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE TÉCNICO, TREINAMENTO, REPOSIÇÃO DE PEÇAS**, de acordo com as necessidades da Companhia de Saneamento de Sergipe – DESO, conforme quantidades e exigências estabelecidas neste termo.

2. JUSTIFICATIVA

2.1. Do objeto

O sistema e serviço de segurança de redes objeto desta contratação são essenciais para a DESO obter alto desempenho, segmentação das redes, segurança lógica, analítica, controle e conectividade para todos os usuários da unidade. Os equipamentos deverão fornecer segmentação segura, controle e visibilidade em toda infraestrutura da rede de dados da DESO.

A atual Solução de Segurança da Informação da DESO é composta por 82 equipamentos de único fabricante descritos nos **ANEXOS II e III**. Estes equipamentos são responsáveis por controlar o tráfego de entrada e saída da rede da DESO, protegendo-a contra ameaças, invasões e perdas de informação.

Dada a existência e disponibilidade dos equipamentos de firewalls citados no ANEXO I deste Termo de Referência, assim como a solução de concentração de Logs e geração de relatórios FortiAnalyzer, modelo: FAZ-VM, bem como de capacitação de pessoal na solução do fabricante Fortinet, considera-se que a compatibilidade da nova solução de segurança de firewall com a infraestrutura já existente trará benefícios de economicidade para

a Administração Pública, uma vez que, todos os recursos serão aproveitados, evitando-se a necessidade de novos treinamentos, bem como a redução do tempo para implantação da nova solução.

Atende ainda a justificativa ao princípio da economicidade nas compras públicas, uma vez que a padronização da solução evitará custos adicionais de treinamento para operação de nova solução e dos custos de operação e manutenção da segurança no ambiente por se tratar de plataforma única de gerenciamento, além de evitar possíveis incompatibilidades técnicas entre equipamentos de marcas diferentes em uma operação integrada, atingindo os objetivos esperados de redução dos custos de operação pela integração das diversas unidades da DESO.

2.2 Da modalidade

Sugerimos a realização desta licitação, na modalidade Pregão Eletrônico, via Sistema de Registro de Preços (SRP), haja vista que esta contratação se enquadra nas hipóteses do art. 3º, inciso IV do Decreto nº 7892/2013, visto a dificuldade em se definir os quantitativos ideais a serem adquiridos, em virtude da demanda. Portanto, tendo em vista a impossibilidade do quantitativo exato a ser demandado pela administração, bem como a conveniência de que as entregas sejam feitas de forma parcelada, o SRP demonstra-se opção viável ao processo licitatório.

Considerando a grande demanda do referido objeto e ao mesmo tempo a necessidade de controle e racionamento do gasto público, o Registro de Preços apresenta-se como ferramenta comprovadamente eficiente na busca por melhores preços, mantendo-os registrados para uma futura e eventual contratação, conforme a necessidade e disponibilidade de recursos orçamentários.

Justifica-se a não aplicação das disposições do *artigo 43* da Lei Complementar nº 123/2006, alterado pelo *artigo 48* da Lei Complementar nº 147/2014, para não incluir um lote com percentual de até 25% do objeto contratado a competição para microempresas e empresas de pequeno porte, visto que tal divisão não é economicamente vantajosa para a DESO. Uma vez que, trata-se de contratação de serviço específico na área de **TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO** e a mais ampla competição, faz-se necessária neste processo licitatório, para atingir a sua finalidade e efetividade, que é a de atender a contento as necessidades da Administração Pública.

Não obstante, para o regular fornecimento do objeto, necessário se faz o estabelecimento dos requisitos mínimos a serem considerados em conformidade com este

Termo de Referência, não eximindo a licitante vencedora de qualquer procedimento adicional necessário para a correta execução do objeto e tampouco servirá de pretexto para ilidir ou afastar sua responsabilidade pela execução contratual.

3. DO ESCOPO DA AQUISIÇÃO

Estão incluídas no escopo da aquisição:

3.1**. Embalagem de proteção, acessórios e dispositivos especiais,** que permitam a carga, transporte e descarga do referido objeto, protegidos de possíveis danos, de forma a atender a legislação específica, aos requisitos regulamentares e a este Termo de Referência.

3.2. **Os itens licitados deverão ser entregues embalados de forma adequada** com bom aspecto visual e de asseio.

3.3. **Carga, transporte e descarregamento dos itens até o local de entrega,** atendendo a legislação específica e aos requisitos regulamentares, englobando os custos inerentes a esses serviços, tais como: seguros, impostos, taxas e outros.

4. FONTE DE RECURSO

Os recursos financeiros para pagamento serão oriundos da RECEITA PRÓPRIA da DESO, **FR10.**

5. GENERALIDADES

5.1. As especificações do lote e itens encontram-se no **Anexo III** deste Termo de Referência.

5.2. O critério a ser utilizado na avaliação e julgamento das propostas de preço e adjudicação é a de menor preço por lote, observando o critério de aceitabilidade do item 14.1 deste Termo de Referência.

6. DA ENTREGA E DO RECEBIMENTO DO OBJETO

O objeto será fornecido de acordo com as quantidades solicitadas com base nas Ordens de Fornecimento – OF's, emitidas pela Gerência de Compras e Almoxarifado (GCAL), correndo o frete, a carga e o transporte do produto às expensas do fornecedor. As entregas ocorrerão mediante programação e conforme as necessidades da DESO.

6.1 Local de entrega e prazos

Os itens licitados deverão ser entregues no seguinte endereço: **GTIC – Gerência de Tecnologia da Informação e Comunicação, localizada na Sede da DESO, Rua Campo Do Brito, No 331, Bairro Praia 13 de Julho, Aracaju/Se**, nos seguintes horários: 07h:00 às 12h:00 e das 14h:00 às 16h:00;

6.1.1. Prazo de entrega: 60 (sessenta) dias sequenciais, contados a partir da data de cada solicitação, que será de acordo com a necessidade da DESO.

Serão de responsabilidade do fornecedor as despesas com carga e descarga dos materiais no local supracitado;

6.1.2. Não serão aceitas como justificativas de irregularidades no fornecimento, a paralisação da unidade fabril ou a quebra de equipamentos, a necessidade de manutenções na indústria, a falta de matéria-prima, problemas com o transporte etc. Nos referidos casos, o fornecedor deverá providenciar a aquisição do referido objeto em outras regiões e/ ou outros fornecedores, garantindo e comprovando sua qualidade em consonância com as especificações estabelecidas, entregando o produto no mesmo preço daquele ofertado para esta licitação.

6.1.3. O recebimento dos itens se dará pelo atesto no canhoto da nota fiscal por empregado da DESO, que deverá ter: nome legível, número de matrícula, data de recebimento, lotação e assinatura.

6.1.4. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 5 (cinco) dias sequenciais, antes do término do prazo de solicitação, e aceitos pela contratante, não serão considerados como inadimplemento contratual.

7. DO PAGAMENTO

7.1. Não será efetuado qualquer pagamento à contratada, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

7.2. É vedada a realização de pagamento se o objeto não estiver de acordo com as especificações deste instrumento ou antes da sua execução.

7.3. Serão pagos apenas os valores relativos aos quantitativos executados, conforme quantidade solicitada e atendimento as especificações descritas neste Termo de Referência.

7.4. O pagamento será efetuado em 30 (trinta) dias após o recebimento definitivo da nota fiscal/fatura, devidamente acompanhada da documentação exigida para a quitação.

7.5. Nenhum pagamento será efetuado a empresa, enquanto houver pendência de liquidação de obrigação financeira, em virtude de penalidade ou inadimplência contratual.

7.6. Caso se faça necessária a apresentação ou reapresentação de qualquer Nota Fiscal/Fatura ou documentação por culpa da contratada, o prazo de até 30(trinta) dias reiniciar-se-á a contar da data da respectiva apresentação ou reapresentação.

8. DAS OBRIGAÇÕES DA CONTRATADA

8.1. Executar o objeto em conformidade com as condições deste instrumento.

8.2. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

8.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos no máximo de 25%, tomando-se por base o valor contratual.

8.4. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade, o fato da contratante proceder à fiscalização ou acompanhar a execução do contrato.

8.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais, e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específica de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado para execução do contrato.

8.6. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipóteses estas que serão respondidas no prazo máximo de 6 (seis) horas.

8.7. Substituir os itens que apresentarem condições de defeito ou quaisquer problemas detectados ou que estejam em desconformidade com as especificações deste termo, no prazo máximo de 5 (cinco) dias, contados da sua notificação através de e-mail e/ ou telefone.

8.8. Cumprir as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

8.9. Entregar o objeto conforme todas as especificações do edital e seus anexos.

8.10. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

8.11. Indicar preposto para representá-la durante a execução do contrato.

9. OBRIGAÇÕES DA CONTRATANTE

9.1. Solicitar a execução do objeto à contratada, através da emissão da ordem de fornecimento.

9.2. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual.

9.3. Fiscalizar a execução do objeto contratual através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

9.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

9.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo de Referência.

9.6. Aplicar as penalidades e sanções previstas em lei e neste instrumento, na hipótese de a contratada não cumprir o contrato, mantidas as situações normais de disponibilidade e volume dos materiais, arcando a referida contratada com quaisquer prejuízos que tal ato acarretar à CONTRATANTE.

9.7. Assegurar-se de que os preços contratados estão compatíveis com àqueles praticados no mercado pelas demais empresas do mesmo ramo, de forma a garantir que os preços contratados continuem a ser os mais vantajosos para a Administração.

9.8. Assegurar os recursos financeiros necessários para contratação do objeto;

9.10. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do objeto, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

10. DA FISCALIZAÇÃO

A execução contratual será acompanhada e fiscalizada por empregado especialmente designado para este fim pela contratante, doravante denominada simplesmente de GESTORA.

11. INSPEÇÃO DE QUALIDADE

Os itens a serem fornecidos poderão ser inspecionados e analisados, a qualquer tempo pela DESO, procedendo de forma sistemática o controle de qualidade e de quantidade sobre o objeto. Caso não atenda às especificações constantes neste Termo, o quantitativo será devolvido e glosado através da nota fiscal.

12. DOS ANEXOS

ANEXO I – SUGESTÃO PARA APRESENTAÇÃO PROPOSTA DE PREÇO DETALHADA;

ANEXO II – DOS ITENS, PREÇOS UNITÁRIOS MÁXIMOS E TOTAIS MÁXIMOS;

ANEXO III – DA INSTALAÇÃO E ESPECIFICAÇÕES E SUPORTE.

13. REGULAMENTAÇÃO DOS FORNECIMENTOS E CRITÉRIOS DE MEDIÇÃO

13.1. A validade da ATA será de 12 meses.

13.2. O fornecimento do objeto se dará conforme necessidade da DESO.

13.3. O pagamento da fatura será 30 (trinta) dias após a entrega de cada parcela devidamente aprovada pela DESO.

14. CRITÉRIO DE ACEITABILIDADE DOS PREÇOS

14.1. Os preços unitários e global somente serão aceitos quando não superiores aos estimados no preço de referência da DESO, constantes no Anexo II – Especificações dos lotes, itens e preço máximo:

14.1.1. Nos casos em que forem apresentadas propostas com valor global dentro dos parâmetros especificados, mas que os valores unitários não atendam o critério estipulado no item 14.1, poderá a Administração promover junto a proponente a solicitação de revisão destes itens de forma que todos itens ofertados estejam dentro dos limites estabelecidos.

14.1.2. Em hipótese alguma será aceito o aumento dos valores inicialmente propostos.

14.1.3. Não havendo por parte da arrematante a revisão de sua proposta dentro do prazo estabelecido pelo Pregoeiro, a mesma terá sua proposta desclassificada.

14.2. A licitante deverá descrever o produto ofertado e indicar a marca e o modelo, conforme o caso, sob pena de desclassificação.

15. MODALIDADE DA LICITAÇÃO

A licitação será por meio de Pregão Eletrônico via Sistema de Registro de Preços.

16. DA PROPOSTA

16.1. Deverá constar na proposta:

16.1.1 Referência aos locais de entrega dos materiais;

16.1.2. Preços unitários e totais dos materiais, inclusos IPI, demais impostos, descarregamento, arrumação e montagem por conta do fornecedor;

16.1.3. Condições de pagamento: 30 DIAS após entrega do material;

16.1.4. Prazo de entrega: 60 (sessenta) dias sequenciais contados a partir da data de cada solicitação, que será de acordo com a necessidade da DESO;

16.1.5. Validade da Proposta: 60 DIAS;

16.1.6. Frete: CIF.

16.2. O licitante deverá estar ciente e levar em consideração, na apresentação da proposta, além das especificações dos produtos em anexo e a todas as condições e exigências estabelecidas neste Edital, o atendimento dos seguintes requisitos:

16.2.1. Nos preços propostos deverão estar inclusos todos os custos necessários para o atendimento do objeto da licitação, bem como todos os materiais, equipamentos, impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, deslocamentos de pessoal, treinamento, garantia, montagem e instalação e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado constante da proposta;

16.2.2. Os preços deverão ser cotados em moeda corrente nacional e neles deverão estar inclusas todas e quaisquer despesas, tais como: IPI e demais impostos, encargos sociais, seguros, taxas, tributos diretos e indiretos incidentes sobre o fornecimento dos materiais;

16.2.3 A proposta entregue será considerada com prazo de validade de 60 (sessenta) dias, contados da data da sessão pública de abertura desta licitação;

16.3. Serão desclassificadas as propostas:

a) que não atendam às exigências do ato convocatório ou que apresentem dispositivos contrários à lei e à regulamentação vigente;

b) que contiverem preços ou vantagens de qualquer natureza ou descontos não previstos neste Pregão, inclusive financiamentos subsidiados ou a fundo perdido;

c) que forem omissas, vagas, apresentarem irregularidades ou defeitos capazes de dificultar o julgamento, bem como as que apresentarem preços ou vantagens baseadas nas ofertas de outros licitantes;

d) que forem superiores ao valor orçado pela DESO.

16.4 A proposta deverá limitar-se ao objeto desta licitação, sendo desconsideradas quaisquer alternativas de preço ou qualquer outra condição não prevista.

16.5 Independentemente de declaração expressa, a simples apresentação das propostas implica submissão a todas as condições e exigências estipuladas no Edital e seus Anexos, sem prejuízo da estrita observância das normas contidas na legislação mencionada no preâmbulo do Edital.

17. QUALIFICAÇÃO TÉCNICA

O PROPONENTE, arrematante do objeto da licitação, na etapa de habilitação, para qualificação técnica, deverá apresentar os seguintes documentos, sob pena de NÃO QUALIFICAÇÃO TÉCNICA pela não apresentação:

17.1. Declaração da disponibilidade de uma Central de Atendimento para todas as soluções, com infraestrutura, aparelhamento e pessoal técnico especializado, em quantitativo adequado e disponível, para a realização do objeto da licitação, conforme especificações técnicas.

17.2. Atestado de fornecimento do produto/serviços: Deverá comprovar por meio de certidão(ões), atestado(s) ou declaração(ões) fornecido(s) por pessoa jurídica de direito público ou privado, que comprovem o fornecimento de forma satisfatória do objeto compatível e pertinente em quantidades, características e prazos com o objeto da licitação.

17.3. Não serão considerados atestados de capacidade técnica os emitidos por pessoas jurídicas integrantes do mesmo grupo comercial, industrial ou de qualquer atividade econômica de que faça parte a proponente. O(s) atestado(s) deverá(ão) estar, necessariamente, acompanhado(s) por original ou cópia autenticada.

17.4. A LICITANTE deverá garantir e comprovar ser representante dos fabricantes das soluções ofertadas em proposta comercial com base nos requisitos técnicos exigidos neste presente termo de referência.

17.5. A LICITANTE deverá apresentar documentos que comprovem a existência de técnico(s), no mínimo 1 (um), certificado(s) pelos fabricantes das soluções ofertadas para execução dos serviços de instalação e suporte das referidas soluções. O vínculo profissional deverá ser comprovado através de uma das seguintes formas, devidamente autenticadas:

- *Registro de Contrato de Trabalho, Contrato social e alterações consolidadas ou Contrato de prestação de serviços e demais formas comprobatórias.*

17.6. A LICITANTE deverá apresentar anexo a proposta prospecto/datasheets com as características técnicas de todos os componentes dos equipamentos, incluindo especificação de marca, modelo e outros elementos que, de forma inequívoca, identifiquem e comprovem as configurações cotadas, através de certificados, manuais técnicos, fôlderes e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em websites dos fabricantes na Internet, em que conste o respectivo endereço eletrônico.

17.7. Os componentes do equipamento e ou software deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação dos equipamentos.

17.8. Os equipamentos ofertados, deverão ser do modelo mais recente do fabricante (compatíveis com o equipamento ofertado). Modelos descontinuados, em vias de descontinuidade e versões anteriores não serão aceitos.

As exigências de modelo (versão) devem ser consideras a partir da entrega do produto e não da publicação do edital, pois o trâmite entre licitação e entrega poderá superar a liberação de versionamentos dos produtos.

18. QUALIFICAÇÃO ECONÔMICA

18.1. Conforme abaixo:

18.1.1. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo

ser atualizados por índices oficiais quando encerrados há mais de 03 (três) meses da data de apresentação da proposta.

18.1.2. O Balanço patrimonial e as demonstrações contábeis deverão ser apresentados da seguinte forma:

a) Para as sociedades anônimas, cópia autenticada da publicação em Diário oficial.
b) Para as demais empresas, cópias legíveis e autenticadas das páginas do Livro Diário, onde foram transcritos o balanço patrimonial e a documentação do resultado do último exercício social, com os respectivos termos de abertura e encerramentos registrados na Junta Comercial ou no Cartório de Títulos e Documentos;
c) Para as empresas constituídas a menos de um ano será exigido apenas o balanço de abertura e demonstrações contábeis na forma da lei.
d) No caso de ME/EPP, desde que optante pelo simples, será exigido contabilidade simplificada.
e) No caso de licitantes com apuração no lucro real, será exigido comprovante de entrega do SPED CONTÁBIL.

18.1.3. A capacidade econômico-financeira será verificada através de:

Liquidez Corrente: ≥ 1,20

Ativo Circulante

LC = ----------

Passivo Circulante

Liquidez Geral:≥ 1,10

Ativo Circulante + Realizável a Longo Prazo

LG = ----------

Passivo Circulante + Exigível a Longo Prazo

Grau de Endividamento Geral: ≤ 0,50

Passivo Circulante + Exigível a Longo Prazo

EG = ----------

Ativo Total

18.1.4. O Patrimônio líquido mínimo exigido será de 10% do valor de cada lote adjudicado, devendo a comprovação ser feita relativamente à data da apresentação da proposta.

19. JULGAMENTO

Critério a ser utilizado na avaliação e julgamento das propostas de preço será o de menor preço por lote.

20. SANÇÕES ADMINISTRATIVAS

20.1. A contratada, pelo inadimplemento de suas obrigações, terá o prazo de 05 (cinco) dias úteis, garantido a ampla defesa e o direito ao contraditório, sujeitando-se às seguintes sanções previstas no Regulamento Interno de Licitações e Contratos da DESO e na Lei 13.303/2016:

20.1.1 – Advertência;

20.1.2 – Multa moratória;

20.1.3 – Multa compensatória;

20.1.4 – Suspensão do direito de participar de licitação e impedimento de contatar com a DESO, pelo prazo de até 02 (dois) anos;

20.1.5 – Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

20.2. As sanções constantes no subitem 19.1 poderão ser aplicadas de forma cumulativa.

20.3. Ficará impedida de licitar e de contratar com a Administração Pública Estadual, pelo prazo de até 05 (cinco) anos, garantido a ampla defesa e o direito ao contraditório, o fornecedor que:

20.3.1 – Ensejar o retardamento da execução do objeto desta licitação;

20.3.2 – Não mantiver proposta, injustificadamente;

20.3.3 – Comportar-se de modo inidôneo;

20.3.4 – Fizer declaração falsa;

20.3.5 – Cometer fraude fiscal;

20.3.6 – Falhar ou fraudar no fornecimento do objeto.

20.4. São consideradas condutas reprováveis e passíveis de sanções, dentre outras, as previstas no art. 186 do RILC.

20.5. As multas estabelecidas serão entendidas como independentes e cumulativas e serão compensadas pela DESO com as importâncias em dinheiro, relativas às prestações a que corresponderem, ou da garantia do contrato, quando for o caso, cobradas judicialmente.

20.6. A aplicação de sanção de advertência se efetiva com o registro da mesma junto ao cadastro de fornecedores e no Sistema de Gerenciamento de Contratos da DESO, independentemente de tratar-se de pessoa cadastrada ao não.

20.7. A multa, correspondente a 5% do valor máximo estabelecido para a referida licitação, poderá ser aplicada nos seguintes casos:

20.7.1 – Em decorrência da interposição de recursos meramente procrastinatórios;
20.7.2 – Em decorrência da não regularização da documentação de habilitação, nos termos do artigo 43, § 1° da Lei Complementar n° 123/2006;
20.7.3 – Pela recusa em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido por este edital;
20.7.4 – No caso de atraso na entrega da garantia contratual, quando exigida, o instrumento convocatório deverá prever, mediante competente justificativa.

20.8. Além das situações acima, poderá incidir multa, nos seguintes casos:

20.8.1 – Inexecução parcial, incidirá multa na razão de 10% sobre o valor da parcela não executada;
20.8.2 – Inexecução total, incidirá multa na razão de 30% sobre o saldo remanescente do contrato;
20.8.3 – Nos demais casos de atraso, incidirá multa na razão de 10% sobre o valor da parcela em atraso.

20.9. Caso não haja o recolhimento da multa no prazo estipulado, a DESO descontará a referida importância de eventuais créditos a vencer da empresa contratada. Na ausência de créditos disponíveis para quitação da importância da multa, a DESO executará a garantia quando exigida, e quando for o caso, será cobrada judicialmente.
20.10. A DESO poderá quando do não pagamento da multa pela Contratada, aplicar a sanção de suspensão do direito de participar de licitação e impedimento de contratar com a DESO, por até 02 (dois) anos e demais cominações legais;
20.11. Cabe a sanção de suspensão em razão de ação ou omissão capaz de causar, ou que tenha causado danos à DESO, suas instalações, pessoas, imagem, meio ambiente ou a terceiros, aplicando a disposição do art. 189 e 190 do RILC em face da legislação fiscal, previdenciária, social ou trabalhista.

21 – GARANTIA CONTRATUAL

Para contratos superiores a R$ 100.000,00 (cem mil reais), a empresa contratada, para garantia da execução do Contrato, apresentará na 5.0.11.00/GFIN – Gerência Financeira desta Companhia, no prazo de 20 (vinte) dias da assinatura do contrato, a importância correspondente a 3% (três por cento) do valor Contratual, em uma das seguintes modalidades: 1 – Caução em Dinheiro 2 – Seguro Garantia; 3 – Fiança Bancária.

22 – REAJUSTAMENTO DE PREÇOS

22.1. Os preços são fixos e irreajustáveis pelo período de 12 (doze) meses a contar da apresentação da proposta.

23 – LEIS ANTICORRUPÇÃO – CONDUTA DA DESO

23.1. A DESO conduz os seus negócios de maneira legal, ética, transparente e profissional, em conformidade com os requisitos gerais das leis anticorrupção e estende aos seus colaboradores e aos terceiros, que a representam, a obrigação de assimilar, aceitar e executar estas diretrizes;

23.2. Em decorrência, a DESO exige que suas contratadas conduzam seus negócios de forma a coibir a prática de atos lesivos conta a Administração Pública, nacional ou estrangeira, que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou quaisquer outras leis e regulamentos aplicáveis ao suborno ou corrupção.

23 – CÓDIGO DE CONDUTA E INTEGRIDADE

Para a DESO o Código de Conduta e Integridade, compila o conjunto de princípios éticos e normas que se consolidam em enunciados para orientar e direcionar a forma como a Companhia se relaciona com os seus *stakeholders.* O referido Código de Conduta e Integridade encontra-se disponível na página da DESO https://www.deso-se.com.br ou acesse através do link abaixo:

- CÓDIGO DE CONDUTA E INTEGRIDADE – https://bit.ly//2OM7fLP

Aracaju, 31 de maio de 2021

Tatiana Franco da Silva
Líder da 2.0.06.00/GCAL
TERMO DE REFERÊNCIA elaborado por Cristiani Rocha de Andrade – Matrícula: 3067-7

ANEXO I - SUGESTÃO PARA APRESENTAÇÃO PROPOSTA DE PREÇO DETALHADA

À
DESO

Ref. Pregão Eletrônico nº ___/20__ – Lote xxxx

Prezados Senhores,

Pela presente formulamos proposta comercial para ---------- Objeto da Licitação ----------, conforme discriminado no Anexo XX do Termo de Referência, que integra o instrumento convocatório da licitação em epígrafe.

IDENTIFICAÇÃO DO LICITANTE	
RAZÃO SOCIAL:	
CNPJ:	INSCRIÇÃO ESTADUAL:
ENDEREÇO:	
TELEFONES:	
E-MAIL:	
DADOS BANCÁRIOS	
BANCO: (nome e código)	
AGÊNCIA:	CONTA CORRENTE:
DADOS DO RESPONSÁVEL PELA ASSINATURA DO INSTRUMENTO CONTRATUAL	
NOME:	
RG:	ÓRGÃO EMISSOR:
CPF:	CARGO:

LOTE X						
Item	**Especificação do Produto**	**Und**	**Marca**	**Quant. Total**	**Valor**	
					Unitário	**Total**
X.X					R$	R$
	TOTAL GERAL					R$

Valor da nossa proposta é de R$ xxxxxxxxxx (por extenso).

- **Validade da Proposta:** 60 dias corridos, contados a partir da data da sessão pública;
- **Validade da ATA:** 12 (doze) meses;
- **Prazo de entrega:** 60 dias sequenciais;
- **Local de Entrega: GTIC – Gerência de Tecnologia da Informação e Comunicação**, localizada na Sede da DESO, Rua Campo Do Brito, No 331, Bairro Praia 13 de Julho, Aracaju/Se;
- **Especificar detalhadamente cada item licitado, juntando portfólios e/ou catálogos com especificações precisas e ilustrações**;
- **Frete:** CIF

Declaramos que os preços ora propostos incluem todas as despesas diretas, indiretas, impostos, benefícios, tributos, contribuições, seguros e licenças de modo a se constituírem a única e total contraprestação pela execução do **FORNECIMENTO**.

Declaramos, ainda, que estamos cientes e de acordo que as intimações ou notificações decorrentes da contratação, caso seja necessário, serão formalizadas eletronicamente para o e-mail da empresa, informado nesta Proposta Comercial, sendo o único responsável em manter-lhe atualizado junto a DESO, verificar caixa de SPAM e não obstante assegurar que o mesmo não esteja com a caixa de entrada cheia.

Portanto, estamos ciente e de acordo com os termos estabelecidos no Edital e seus anexos.

_____, _____ de _____ de 20__

_____

Assinatura do representante legal

ANEXO II – DOS ITENS, PREÇOS UNITÁRIOS MÁXIMOS E TOTAIS MÁXIMOS

LOTE ÚNICO – AMPLA CONCORRÊNCIA.					
ITEM	**DESCRIÇÃO**	UNI.	**QTD.**	**VALOR UNITÁRIO MÁXIMO**	**VALOR TOTAL MÁXIMO**
1	Solução integrada de segurança de redes (UTM-NGFW) **Tipo I – Conforme ANEXO II.**	UN	04	R$ 82.288,06	R$ 329.152,24
2	Solução integrada de segurança de redes (UTM-NGFW) **Tipo II – Conforme ANEXO II.**	UN	04	R$ 25.319,41	R$ 101.277,64
3	Solução integrada de segurança de redes (UTM-NGFW) **Tipo III – Conforme ANEXO II.**	UN	40	R$ 13.366,93	R$ 534.677,20
4	Upgrade solução de repositório de log e relatoria **– Conforme ANEXO II.**	UN	02	R$ 84.432,74	R$ 168.865,48
5	Solução de Gestão e Gerenciamento de Equipamentos **– Conforme ANEXO II.**	UN	02	R$ 140.317,77	R$ 280.635,54
6	Solução de ativos de rede – SWITCH TIPO I **– Conforme ANEXO II.**	UN	04	R$ 21.119,04	R$ 84.476,16
7	Solução de ativos de rede – SWITCH TIPO II **– Conforme ANEXO II.**	UN	06	R$ 5.038,27	R$ 30.229,62
8	Solução de ativos de rede – SWITCH TIPO III **– Conforme ANEXO II.**	UN	80	R$ 3.664,19	R$ 293.135,20
9	Transceiver, SFP, 1GbE **– Conforme ANEXO II.**	UN	50	R$ 267,43	R$ 13.371,50
10	Dispositivo de rede sem fio – WIFI **– Conforme ANEXO II.**	UN	50	R$ 4.051,53	R$ 202.576,50
VALOR TOTAL					**R$ 2.038.397,08**

ANEXO III – DA INSTALAÇÃO E ESPECIFICAÇÕES E SUPORTE

1. INSTALAÇÕES

A instalação deve abranger a Solução de Segmentação e Segurança de Redes em Alta disponibilidade, Solução de Gestão e Gerenciamento de Dispositivos e a implementação do protocolo 802.1x como pré-requisito de conexões de rede, com ou sem fio, comunicando qualquer dispositivo de rede aos elementos ativos deste Termo de Referência.

Os serviços de Instalação deverão ser prestados de forma **presencial** e deverão contemplar as seguintes atividades:

- Registro e ativação de licenças;
- Atualização de software;
- Implantação da Solução de Segmentação e Segurança de Redes em Alta disponibilidade;
- Solução de Gestão e Gerenciamento de Dispositivos;
- Integração dos firewalls com software de gerenciamento;
- Configuração de rotinas de backup e atualizações de firmware;
- Implementação do protocolo 802.1x omo pré-requisito de conexões de rede, com ou sem fio, comunicando qualquer dispositivo de rede aos elementos ativos deste Termo de Referência.

Na apresentação da proposta comercial a Licitante deverá fornecer declaração do fabricante dos produtos ofertados, declarando que é credenciada para realizar a instalação, configuração, treinamento e suporte técnico pós-venda de seus produtos.

Os equipamentos deverão ser entregues com seus acessórios (equipamentos e demais componentes), cabos, conectores, armários e demais itens necessários à sua montagem, testes, perfeito e pleno funcionamento.

A CONTRATADA deverá instalar os equipamentos observando as exigências das normas reguladoras conforme as práticas aplicáveis.

A CONTRATADA deverá submeter à aprovação da CONTRATANTE, a programação de realização dos serviços.

Ficará por conta da CONTRATADA o fornecimento de todos os materiais e acessórios necessários à instalação dos equipamentos objeto destas especificações.

Os equipamentos deverão ser instalados de modo que esteja com sua capacidade inicial disponível para uso imediato.

Todos os componentes ofertados devem ser testados em conjunto com a CONTRATANTE.

Até 15 (quinze) dias antes do início dos serviços de instalação, a empresa CONTRATADA deverá submeter à aprovação a programação de realização dos serviços, composta de cronograma e descritivo dos serviços a serem executados.

Devem estar inclusas na instalação todas as configurações necessárias para o pleno funcionamento da Solução, inclusive a integração total com a solução já implantada, descrita no Anexo I deste Termos de Referência.

A CONTRATADA deve fazer a passagem de conhecimento básica para os técnicos da unidade, para que os mesmos possam operar as soluções de forma básica conforme detalhamento:

- Deverá ser realizado, para até 06 (seis) prepostos da DESO, treinamento ministrado por profissional certificado pelos fabricantes das soluções, abrangendo configuração de todos os equipamentos ativos e dos softwares a serem ofertados pela CONTRATADA. O treinamento deverá ser ministrado nas dependências da CONTRATANTE, ou em local adequado e definido por esta.
- Caso haja custos de translado, alimentação e hospedagem da equipe de treinamento, estes serão de responsabilidade da CONTRATADA.
- A carga horária mínima será de 16 (dezesseis) horas.
- A abordagem do treinamento deverá ser eminentemente prática, utilizando exemplos e exercícios para ilustrar os conceitos e capacitar os participantes a empregar os recursos oferecidos, dirigidos ao ambiente identificado na DESO.

A LICITANTE poderá realizar uma visita técnica na DESO, para vistoria do local e coleta de informações de forma que tenham conhecimento pleno das condições técnicas para a sua efetiva oferta, não sendo aceitas alegações posteriores de desconhecimento das condições necessárias à execução dos serviços.

Não caberá pleito posterior de indenização por despesas de serviços complementares por desconhecimento de informações e qualquer outro trabalho que a LICITANTE tenha realizado para poder participar do certame.

Caso a licitante manifeste interesse em realizar uma visita técnica, deverá agendá-la pelo telefone (79) 3226-1015. A visita deverá ocorrer em até 72 horas antes da data do certame.

Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela DESO.

A execução do Contrato deverá seguir metodologia de trabalho baseada no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela DESO.

Os serviços deverão ser realizados nas dependências da DESO, utilizando-se de equipamentos e infraestrutura com capacidade operacional.

Os serviços deverão ser realizados por profissionais certificados pelo fabricante.

Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela DESO, providenciando sua inspeção, conferência, classificação e prestação de contas.

Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela DESO.

2. EQUIPAMENTOS INTEGRANTES DA SOLUÇÃO

2.1. Solução integrada de segurança de redes (UTM-NGFW) TIPO I, possuindo licenciamento, suporte, garantia e atualizações por **48(quarenta e oito) meses**, e funcionalidades de: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Anti-Spam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention, Sandboxing (podendo ser físico ou virtualizado) e SD-WAN, incluindo todas as subscrições, garantias, atualizações de software e instalação local dos equipamentos e configuração em alta disponibilidade, conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

2.2. Solução integrada de segurança de redes (UTM-NGFW) TIPO II, possuindo licenciamento, suporte, garantia e atualizações por **48(quarenta e oito) meses**, e funcionalidades de: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Anti-Spam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention, Sandboxing (podendo ser físico ou virtualizado) e SD-

WAN, incluindo todas as subscrições, garantias, atualizações de software e instalação local dos equipamentos e configuração em alta disponibilidade, conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

2.3. Solução integrada de segurança de redes (UTM-NGFW) TIPO II, possuindo licenciamento, suporte, garantia e atualizações por **48(quarenta e oito) meses**, e funcionalidades de: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Anti-Spam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention, Sandboxing (podendo ser físico ou virtualizado) e SD-WAN, conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

2.4. Upgrade Solução de repositório de log e relatoria com gerência centralizada incluindo todas as subscrições, garantias e atualizações de software pelo período de **48 (quarenta e oito) meses** conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança e infraestrutura tecnológica da DESO.

2.5. Solução de Gestão e Gerenciamento de Dispositivos com gerência centralizada incluindo todas as subscrições, garantias e atualizações de software pelo período de **48 (quarenta e oito) meses**, com instalação e configuração local da solução, conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança e infraestrutura tecnológica da DESO.

2.6. Solução de ativos de rede SWITCH TIPO I com gerência centralizada incluindo todas as subscrições, garantias e atualizações de software por **48(quarenta e oito) meses**, instalação local dos equipamentos e configuração em alta disponibilidade conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

2.7. Solução de ativos de rede SWITCH TIPO II com gerência centralizada incluindo todas as subscrições, garantias e atualizações de software por **48(quarenta e oito) meses** conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

2.8. Solução de ativos de rede SWITCH TIPO III com gerência centralizada incluindo todas as subscrições, garantias e atualizações de software por **48(quarenta e oito) meses** conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

2.9. Transceiver, SFP, 1GbE, SX, 850nm, com garantia do fabricante por **12(doze) meses**, conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

2.10. Dispositivo de rede sem fio – WIFI, com garantia do fabricante por **48(quarenta e oito) meses**, conforme especificação técnica detalhada no item 7 deste Termo de Referência, para atender o projeto de segurança na infraestrutura tecnológica da DESO.

SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDES (UTM-NGFW), UPGRADE SOLUÇÃO DE REPOSITÓRIO DE LOG E RELATORIA, SOLUÇÃO DE GESTÃO E GERENCIAMENTO DE DISPOSITIVOS E SERVIÇOS PROFISSIONAIS.		
ITEM	**DESCRIÇÃO**	**QTD.**
01	Solução integrada de segurança de redes (UTM-NGFW) **TIPO I**	04
02	Solução integrada de segurança de redes (UTM-NGFW) **TIPO II**	04
03	Solução integrada de segurança de redes (UTM-NGFW) **TIPO III**	40
04	Upgrade solução de repositório de log e relatoria	02
05	Solução de Gestão e Gerenciamento de Equipamentos	02
06	Solução de ativos de rede – SWITCH TIPO I	04
07	Solução de ativos de rede – SWITCH TIPO II	06
08	Solução de ativos de rede – SWITCH TIPO III	80
09	Transceiver, SFP, 1GbE	50
10	Dispositivo de rede sem fio – WIFI	50

3 – ESPECIFICAÇÕES TÉCNICAS

Solução integrada de segurança de redes (UTM-NGFW), solução de repositório de log e relatoria, solução de gestão e gerenciamento de dispositivos e serviços profissionais.

ITEM – 01 – SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDES (UTM-NGFW) TIPO I COM LICENCIAMENTO POR 48 (QUARENTA E OITO) MESES

Requisitos Mínimos de Performance e quantidades:

- Throughput de Firewall (UDP 512 bytes): 27 Gbps;
- Conexões simultâneas: 2.8 Milhões;
- Novas conexões por segundo: 250 Mil;
- Throughput de VPN IPSec: 10 Gbps;
- Quantidade de túneis lan to lan: 2 mil;
- Quantidade de túneis client to lan: 15 mil;
- Throughput de VPN SSL: 1.8 Gbps;
- Quantidade de usuários VPN SSL licenciados: 500;

- Throughput de IPS: 4.5 Gbps;
- Throughput de Threat Protection (app. control e malware protection): 2.6 Gbps;
- Throughput de Controle de Aplicações: 12 Gbps;
- SSL Inspection Throughput: 3.7 Gbps;
- NGFW Throughput: 3.0 Gbps;
- Quantidade mínima de Switches Gerenciados: 60;
- Quantidade de interfaces 1Gbps – RJ45: 14;
- Quantidade de interfaces 1Gbps – SFP: 8;
- Quantidade de interfaces 10Gbps – SFP+: 4.

REQUISITOS DE FUNCIONALIDADES

Funcionalidades do Firewall

- Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- Deve possuir tecnologia de firewall do tipo Statefull;
- Deve permitir filtro de pacotes sem controle de estado “stateless” para verificação em camada 2;
- Deve ser otimizado para análise de conteúdo de aplicações em camada 7;
- Deve suportar forwarding multicast, inclusive em modo bridge;
- Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- Deve suportar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;
- Deve ser compatível com item SOLUÇÃO DE REPOSITÓRIO DE LOG E RELATORIA deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve ser compatível e gerenciado pelo dispositivo especificado no item SOLUÇÃO DE GESTÃO E GERENCIAMENTO DE EQUIPAMENTOS deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve possuir controle de acesso à internet por endereço IP de origem e destino;
- Deve possuir controle de acesso à internet por sub-rede;

- Deve suportar tags de VLAN (802.1q);
- Deve possuir ferramenta de diagnóstico do tipo TCPDump;
- Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deve suportar single-sign-on;
- Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
- Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
- Deve suportar roteamento estático para IPv4 e IPv6;
- Deve suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP);
- Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deve suportar aplicações multimídias, como: H.323 e SIP;
- Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo com a atual solução de integrada de segurança da DESO Marca Fortinet, Modelo FG500E;
- Deve permitir o funcionamento em modo transparente tipo “bridge”;
- Deve suportar PBR – Policy Based Routing;
- Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- Deve possuir mecanismo de anti-spoofing;
- Deve permitir criação de regras definidas pelo usuário;
- Deve suportar sFlow;
- Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- Deve permitir funcionamento em modo bridge, router, proxy explícito e sniffer;
- Deve possuir mecanismo de tratamento (session-helpers ou ALGs);
- Deve permitir a criação de administradores independentes, para cada um dos sistemas;

- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance, virtuais existentes, de maneira a possibilitar a criação de sistemas virtuais que podem ser administrados por equipes distintas;
- Deve suportar o protocolo padrão da indústria VXLAN;
- Deve permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;
- Deve possuir controle, inspeção e de criptografia de SSL por política;
- Deve continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos gerenciados com o serviço de gerência;
- Em caso de gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;
- Deve possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;
- Deve suportar ambientes multi-cloud;
- Deve possui a capacidade de criar automações através de gatilhos e ações;
- Deve ter a capacidade de criar políticas de firewall baseando-se em endereços MAC.

Funcionalidades de QoS

- Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.

Funcionalidades de Anti-Spam

- Deve possuir verificação na funcionalidade de anti-spam da verificação do cabeçalho SMTP do tipo MIME;
- Deve possuir filtragem de e-mail por palavras chaves;
- Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
- Deve possuir para a funcionalidade de Anti-Spam o recurso de DNSBL;
- Deve permitir a checagem de URL no corpo mensagens de correio eletrônico.

Funcionalidades de Webfilter

- Deve possuir solução de filtro de conteúdo web integrado a solução de segurança;
- Deve possuir pelo menos 50 categorias para classificação de sites web;
- Deve possuir base mínima contendo, 100 milhões de sites internet web já registrados e classificados;
- Deve possuir a funcionalidade de cota de tempo de utilização por categoria;
- Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de base de URL própria atualizável;
- Deve permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, endereço IP e sub-rede;
- Deve implementar roteamento WCCP e ICAP;
- Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
- Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deve possuir a função de exclusão de URLs do bloqueio;
- Deve permitir a customização de página de bloqueio;
- Deve permitir 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);
- Deve possuir em sua base de dados, uma blacklist contendo URLs de certificados maliciosos;
- Deve permitir além do Explicit Web Proxy, suportar proxy Web transparente.

Funcionalidades de IPS

- Possui base de assinaturas de IPS com pelo menos 2.000 ameaças conhecidas;
- Detecção de ataques de RPC (Remote procedure call);
- Deve prover mecanismos de Proteção contra ataques de Windows ou NetBios;
- Deve prover mecanismos de Proteção contra ataques DNS (Domain Name System);
- Deve prover mecanismos de Proteção contra ataques a FTP, SSH, Telnet e rlogin;
- Deve prover mecanismos de Proteção contra ataques de ICMP (Internet Control Message Protocol);
- Deve prover notificação via Alarmes na console de administração e correio eletrônico;
- Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- Deve permitir funcionar em modo transparente, one-arm e router;
- Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- Deve permitir a criação de padrões de ataque manualmente;
- Deve possuir integração à plataforma de segurança;
- Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a Web Server, para que seja usado para proteção específica de Servidores Web;
- Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Implementar os seguintes tipos de ações para ameaças detectadas pelo ips, antispyware e antivírus;
- Deve permitir, permitir e gerar log, bloquear, bloquear ip do atacante por um intervalo de tempo;
- Deve permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- Permitir o bloqueio de programas exploradores de vulnerabilidades (exploits) conhecidos.
-

Funcionalidades de Sandbox em Nuvem

- Deve ter a capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante.

Funcionalidades de VPN

- A VPN SSL deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- A VPN SSL deve suportar cliente para plataforma Windows, Linux e Mac OS X;
- Deve permitir a arquitetura de vpn hub and spoke;
- Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
- Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
- Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;
- Deve possuir suporte a VPN SSL e deverá manter uma conexão segura com o portal durante a sessão;
- Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- Solução deve ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN.

Funcionalidades de Antivírus

- Deve possuir funções de antivírus e anti-spyware;
- Deve possuir antivírus em tempo real, para ambiente de gateway internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;
- Deve permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, dentre outros);
- Deve possuir proteção contra conexões a servidores Botnet;
- Deve permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
- Deve permitir o bloqueio de download de arquivos por tamanho;

Funcionalidades de Application Control

- Deve possuir categoria exclusiva, no mínimo, para os tipos de aplicações: P2P, Instant Messaging, Web, Transferência de arquivos e VOIP;

- Deve reconhecer, no mínimo, 1700 (mil e setecentas) aplicações;
- Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deve ser capaz de controlar aplicações, independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
- Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deve permitir criação de padrões de aplicação manualmente;
- Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Hangouts chat e bloquear a chamada de vídeo;
- Deve Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Funcionalidades de Análise de Vulnerabilidades

- Deve permitir efetuar análises dos servidores e estações na rede, indicando vulnerabilidades encontradas nos mesmos;
- Deve possuir base de dados local atualizável com as vulnerabilidades;
- Deve permitir que tais análises sejam programadas e automáticas de forma diária, semanal e mensal, e que também possa ser executado via linha de comando de forma imediata;
- Deve permitir definir horários nos quais a análise deve ser interrompida automaticamente de forma a não afetar o desempenho da rede;
- Deve permitir definir quais os equipamentos que serão analisados. No caso de servidores, deve permitir que se defina um usuário e senha para que a análise seja mais completa;
- Deve prover como resultado final uma lista dos dispositivos analisados e as vulnerabilidades encontradas nos mesmos.

Gerenciamento Centralizado de Switches

- Deve permitir o gerenciamento de switches;
- Deve permitir a coleta de syslog;
- Deve permitir o gerenciamento dos switches através de interface gráfica;
- Deve permitir a visualização da topologia física e lógica da rede assim como usuários conectados;
- Deve permitir a autodescoberta de múltiplos switches;
- Deve permitir a atualização de software/firmware dos switches gerenciados;
- Deve permitir a configuração de VLANs de forma centralizada;
- Deve permitir o controle de PoE dos switches gerenciados;
- Deve permitir a configuração de link aggregation;
- Deve permitir a configuração de Spanning Tree;
- Deve permitir a configuração de LLDP/MED;
- Deve permitir habilitar recursos de DHCP snooping;
- Deve implementar descoberta de dispositivos;
- Deve permitir a configuração de autenticação 802.1x;
- Deve ter capacidade de apresentar, no mínimo, os seguintes parâmetros de acesso:
- – Switch através do qual o acesso foi solicitado, porta do switch em que o usuário estava conectado;
- – Endereço MAC da máquina usada pelo usuário;
- – Bytes transmitidos e recebidos durante o período de conexão.

Funcionalidades de SD-WAN

- Deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- Deve suportar Forward Error Connection (FEC);
- Deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- Deve poder adicionar e equilibrar, no mínimo, 6 interfaces de dados;
- Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;

- Deve suportar testar o link (probe) através do seguinte:
  - Ping;
  - HTTP;
  - TCP-Echo;
  - UDP-Echo.

Deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:

- Número de Sessões;
- Volume de Tráfego;
- IP de Origem e Destino;
- Transbordo de Link (Spillover).

Funcionalidades de Gerenciamento Wireless

- Deve suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;
- Deve suportar IPv4 e IPv6 por SSID;
- Deve permitir definir quais redes serão acessadas através da controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- Deve suportar a monitoração e supressão de ponto de acesso indevido;
- Deve prover autenticação para a rede wireless através de bases externas como LDAP ou RADIUS;
- Deve permitir a visualização dos clientes wireless conectados;
- Deve suportar configuração de Captive Portal por SSID;
- Deve permitir configurar o bloqueio de tráfego entre os clientes conectados a um SSID e AP específico;
- Deve ser compatível com Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de algoritmo AES e/ou TKIP;
- Deve permitir configurar parâmetros de rádio, como banda e canal;
- Deve possuir método de descoberta de novos Pontos de Acesso de maneira automática;
- Deve possuir método de descoberta de novos Pontos de Acesso baseados em IP estático;

- Deve possuir método de descoberta de novos Pontos de Acesso baseados em DHCP;
- Deve possuir proteção contra ataques do tipo ARP Poisoning na controladora wireless;
- Deve implementar Protected Management Frames de acordo com a norma da aliança WiFi e o padrão 802.11ac;
- Deve possuir WIDS integrado para detecção de ataques;
- Deve Implementar canais de aprovisionamento automático dos Access Points, de forma a minimizar interferência entre eles;
- Deve permitir definir em quais horários determinados SSID estará disponível;
- Deve possibilitar definir número máximo de clientes permitidos por SSID;
- Deve possibilitar definir número máximo de clientes permitidos por AP;
- Deve possibilitar número máximo de clientes permitidos por Radio;
- Deve permitir criar, gerenciar e disponibilizar redes wireless mesh;
- Deve possuir mecanismo de criação automática e/ou manual de usuários visitantes e senhas, que possam ser enviadas por e-mail ou SMS aos usuários, e com ajuste de tempo de expiração da senha;
- Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois pontos de acesso gerenciados;
- Deve permitir a identificação do firmware utilizado em cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
- Deve permitir que sejam desabilitados clientes wireless que possuam taxa de transmissão baixa;
- Deve permitir bloquear clientes wireless que tenham sinal fraco, definindo um limiar de sinal a partir do qual esses clientes serão ignorados;
- Deve permitir configurar o valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
- Deve permitir associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID;
- Deve permitir visualizar as aplicações e ameaças por dispositivo wireless;
- Deve permitir a visualização dos usuários conectados em forma de topologia lógica de rede;

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM – 02 – SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDES (UTM-NGFW) TIPO II COM LICENCIAMENTO 48 (QUARENTA E OITO) MESES

Requisitos Mínimos de Performance e quantidades:

- Throughput de Firewall (UDP 512 bytes): 9 Gbps;
- Conexões simultâneas: 1.4 Milhões;
- Novas conexões por segundo: 40 Mil;
- Throughput de VPN IPSec: 6 Gbps;
- Quantidade de túneis lan to lan: 200;
- Quantidade de túneis client to lan: 2.000;
- Throughput de VPN SSL: 950 Mbps;
- Quantidade de usuários VPN SSL licenciados: 200;
- Throughput de IPS: 1.3 Gbps;
- Throughput de Threat Protection (app. control e malware protection): 800 Mbps;
- Throughput de Controle de Aplicações: 1.6 Gbps;
- SSL Inspection Throughput: 700 Mbps;
- NGFW Throughput: 950 Mbps;
- Quantidade mínima de Switches Gerenciados: 16;
- Quantidade de interfaces 1Gbps – RJ45: 8;
- Quantidade de interfaces 1Gbps – SFP: 2.

REQUISITOS DE FUNCIONALIDADES

Funcionalidades do Firewall

- Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

- Deve possuir tecnologia de firewall do tipo Statefull;
- Deve permitir filtro de pacotes sem controle de estado “stateless” para verificação em camada 2;
- Deve ser otimizado para análise de conteúdo de aplicações em camada 7;
- Deve suportar forwarding multicast, inclusive em modo bridge;
- Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- Deve suportar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;
- Deve ser compatível com item SOLUÇÃO DE REPOSITÓRIO DE LOG deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve ser compatível e gerenciado pelo dispositivo especificado no item SOLUÇÃO DE GESTÃO E GERENCIAMENTO DE EQUIPAMENTOS deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve possuir controle de acesso à internet por endereço IP de origem e destino;
- Deve possuir controle de acesso à internet por sub-rede;
- Deve suportar tags de VLAN (802.1q);
- Deve possuir ferramenta de diagnóstico do tipo TCPDump;
- Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deve suportar single-sign-on;
- Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
- Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
- Deve suportar roteamento estático para IPv4 e IPv6;
- Deve suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP);
- Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deve suportar aplicações multimídias, como: H.323 e SIP;

- Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo;
- Deve permitir o funcionamento em modo transparente tipo “bridge”;
- Deve suportar PBR – Policy Based Routing;
- Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- Deve possuir mecanismo de anti-spoofing;
- Deve permitir criação de regras definidas pelo usuário;
- Deve suportar sFlow;
- Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TA-CACS;
- Deve permitir funcionamento em modo bridge, router, proxy explícito e sniffer;
- Deve possuir mecanismo de tratamento (session-helpers ou ALGs);
- Deve permitir a criação de administradores independentes, para cada um dos siste-mas
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance, virtuais existentes, de maneira a possibilitar a criação de sistemas virtuais que podem ser administrados por equipes distintas;
- Deve suportar o protocolo padrão da indústria VXLAN;
- Deve permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;
- Deve possuir controle, inspeção e de criptografia de SSL por política;
- Deve continuar tratando o tráfego corretamente, sem causar interrupção das comuni-cações, mesmo no caso de queda da comunicação dos equipamentos gerenciados com o serviço de gerência;
- Em caso de gerenciado de forma centralizada, o equipamento ofertado deverá conti-nuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de ge-rência centralizada;
- Deve possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;
- Deve suportar ambientes multi-cloud;
- Deve possui a capacidade de criar automações através de gatilhos e ações;

- Deve ter a capacidade de criar políticas de firewall baseando-se em endereços MAC.

Funcionalidades de QoS

- Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
-

Gerenciamento Centralizado de Switches

- Deve permitir o gerenciamento de switches;
- Deve permitir a coleta de syslog;
- Deve permitir o gerenciamento dos switches através de interface gráfica;
- Deve permitir a visualização da topologia física e lógica da rede assim como usuários conectados;
- Deve permitir a autodescoberta de múltiplos switches;
- Deve permitir a atualização de software/firmware dos switches gerenciados;
- Deve permitir a configuração de VLANs de forma centralizada;
- Deve permitir o controle de PoE dos switches gerenciados;
- Deve permitir a configuração de link aggregation;
- Deve permitir a configuração de Spanning Tree;
- Deve permitir a configuração de LLDP/MED;
- Deve permitir habilitar recursos de DHCP snooping;
- Deve implementar descoberta de dispositivos;
- Deve permitir a configuração de autenticação 802.1x;
- Deve ter capacidade de apresentar, no mínimo, os seguintes parâmetros de acesso:
- -Switch através do qual o acesso foi solicitado, porta do switch em que o usuário estava conectado;
- -Endereço MAC da máquina usada pelo usuário;
- -Bytes transmitidos e recebidos durante o período de conexão.

Funcionalidades de SD-WAN

- Deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;

- Deve suportar Forward Error Connection (FEC);
- Deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- Deve poder adicionar e equilibrar, no mínimo, 6 interfaces de dados;
- Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- Deve suportar testar o link (probe) através do seguinte:
  - Ping;
  - HTTP;
  - TCP-Echo;
  - UDP-Echo.
- Deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:
  - Número de Sessões;
  - Volume de Tráfego;
  - IP de Origem e Destino;
  - Transbordo de Link (Spillover).

Funcionalidades de Gerenciamento Wireless

- Deve suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;
- Deve suportar IPv4 e IPv6 por SSID;
- Deve permitir definir quais redes serão acessadas através da controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- Deve suportar a monitoração e supressão de ponto de acesso indevido;
- Deve prover autenticação para a rede wireless através de bases externas como LDAP ou RADIUS;
- Deve permitir a visualização dos clientes wireless conectados;
- Deve suportar configuração de Captive Portal por SSID;
- Deve permitir configurar o bloqueio de tráfego entre os clientes conectados a um SSID e AP específico;

- Deve ser compatível com Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de algoritmo AES e/ou TKIP;
- Deve permitir configurar parâmetros de rádio, como banda e canal;
- Deve possuir método de descoberta de novos Pontos de Acesso de maneira automática;
- Deve possuir método de descoberta de novos Pontos de Acesso baseados em IP estático;
- Deve possuir método de descoberta de novos Pontos de Acesso baseados em DHCP;
- Deve possuir proteção contra ataques do tipo ARP Poisoning na controladora wireless;
- Deve implementar Protected Management Frames de acordo com a norma da aliança WiFi e o padrão 802.11ac;
- Deve possuir WIDS integrado para detecção de ataques;
- Deve Implementar canais de aprovisionamento automático dos Access Points, de forma a minimizar interferência entre eles;
- Deve permitir definir em quais horários determinados SSID estará disponível;
- Deve possibilitar definir número máximo de clientes permitidos por SSID;
- Deve possibilitar definir número máximo de clientes permitidos por AP;
- Deve possibilitar número máximo de clientes permitidos por Radio;
- Deve permitir criar, gerenciar e disponibilizar redes wireless mesh;
- Deve possuir mecanismo de criação automática e/ou manual de usuários visitantes e senhas, que possam ser enviadas por e-mail ou SMS aos usuários, e com ajuste de tempo de expiração da senha;
- Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois pontos de acesso gerenciados;
- Deve permitir a identificação do firmware utilizado em cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
- Deve permitir que sejam desabilitados clientes wireless que possuam taxa de transmissão baixa;
- Deve permitir bloquear clientes wireless que tenham sinal fraco, definindo um limiar de sinal a partir do qual esses clientes serão ignorados;
- Deve permitir configurar o valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

- Deve permitir associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID;
- Deve permitir visualizar as aplicações e ameaças por dispositivo wireless;
- Deve permitir a visualização dos usuários conectados em forma de topologia lógica de rede.

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM – 03 – SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDES (UTM-NGFW) TIPO III COM SUPORTE E GARANTIA POR 48 (QUARENTA E OITO) MESES

Requisitos Mínimos de Performance e quantidades:

- Throughput de Firewall (UDP 512 bytes): 4.5 Gbps;
- Conexões simultâneas: 650 Mil;
- Novas conexões por segundo: 30 Mil;
- Throughput de VPN IPSec: 4 Gbps;
- Quantidade de túneis lan to lan: 200;
- Quantidade de túneis client to lan: 200;
- Throughput de VPN SSL: 450 Mbps;
- Quantidade de usuários VPN SSL licenciados: 200;
- Throughput de IPS: 950 Mbps;
- Throughput de Threat Protection (app. control e malware protection): 500 Mbps;
- Throughput de Controle de Aplicações: 900 Mbps;
- SSL Inspection Throughput: 300 Mbps;
- NGFW Throughput: 700 Mbps;

- Quantidade mínima de Switches Gerenciados: 6;
- Quantidade de interfaces 1Gbps – RJ45: 5.

REQUISITOS DE FUNCIONALIDADES

Funcionalidades do Firewall

- Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- Deve possuir tecnologia de firewall do tipo Statefull;
- Deve permitir filtro de pacotes sem controle de estado “stateless” para verificação em camada 2;
- Deve ser otimizado para análise de conteúdo de aplicações em camada 7;
- Deve suportar forwarding multicast, inclusive em modo bridge;
- Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- Deve suportar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;
- Deve ser compatível com item SOLUÇÃO DE REPOSITÓRIO DE LOG deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve ser compatível e gerenciado pelo dispositivo especificado no item SOLUÇÃO DE GESTÃO E GERENCIAMENTO DE EQUIPAMENTOS deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve possuir controle de acesso à internet por endereço IP de origem e destino;
- Deve possuir controle de acesso à internet por sub-rede;
- Deve suportar tags de VLAN (802.1q);
- Deve possuir ferramenta de diagnóstico do tipo TCPDump;
- Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deve suportar single-sign-on;

- Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
- Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
- Deve suportar roteamento estático para IPv4 e IPv6;
- Deve suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP);
- Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deve suportar aplicações multimídias, como: H.323 e SIP;
- Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo;
- Deve permitir o funcionamento em modo transparente tipo “bridge”;
- Deve suportar PBR – Policy Based Routing;
- Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- Deve possuir mecanismo de anti-spoofing;
- Deve permitir criação de regras definidas pelo usuário;
- Deve suportar sFlow;
- Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TA-CACS;
- Deve permitir funcionamento em modo bridge, router, proxy explícito e sniffer;
- Deve possuir mecanismo de tratamento (session-helpers ou ALGs);
- Deve permitir a criação de administradores independentes, para cada um dos siste-mas;
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance, virtuais existentes, de maneira a possibilitar a criação de sistemas virtuais que podem ser administrados por equipes distintas;
- Deve suportar o protocolo padrão da indústria VXLAN;
- Deve permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;
- Deve possuir controle, inspeção e de criptografia de SSL por política;

- Deve continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos gerenciados com o serviço de gerência;
- Em caso de gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;
- Deve possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;
- Deve suportar ambientes multi-cloud;
- Deve possui a capacidade de criar automações através de gatilhos e ações;
- Deve ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;

Funcionalidades de QoS

- Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

Funcionalidades de Anti-Spam

- Deve possuir verificação na funcionalidade de anti-spam da verificação do cabeçalho SMTP do tipo MIME;
- Deve possuir filtragem de e-mail por palavras chaves;
- Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
- Deve possuir para a funcionalidade de Anti-Spam o recurso de DNSBL;
- Deve permitir a checagem de URL no corpo mensagens de correio eletrônico.

Funcionalidades de Webfilter

- Deve possuir solução de filtro de conteúdo web integrado a solução de segurança;
- Deve possuir pelo menos 50 categorias para classificação de sites web;
- Deve possuir base mínima contendo, 100 milhões de sites internet web já registrados e classificados;
- Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

- Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de base de URL própria atualizável;
- Deve permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, endereço IP e sub-rede;
- Deve implementar roteamento WCCP e ICAP;
- Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
- Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deve possuir a função de exclusão de URLs do bloqueio;
- Deve permitir a customização de página de bloqueio;
- Deve permitir 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);
- Deve possuir em sua base de dados, uma blacklist contendo URLs de certificados maliciosos;
- Deve permitir além do Explicit Web Proxy, suportar proxy Web transparente;
-

Funcionalidades de IPS

- Possui base de assinaturas de IPS com pelo menos 2.000 ameaças conhecidas;
- Detecção de ataques de RPC (Remote procedure call);
- Deve prover mecanismos de Proteção contra ataques de Windows ou NetBios;
- Deve prover mecanismos de Proteção contra ataques DNS (Domain Name System);
- Deve prover mecanismos de Proteção contra ataques a FTP, SSH, Telnet e rlogin;
- Deve prover mecanismos de Proteção contra ataques de ICMP (Internet Control Message Protocol);

- Deve prover notificação via Alarmes na console de administração e correio eletrônico;
- Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- Deve permitir funcionar em modo transparente, one-arm e router;
- Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- Deve permitir a criação de padrões de ataque manualmente;
- Deve possuir integração à plataforma de segurança;
- Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a Web Server, para que seja usado para proteção específica de Servidores Web;
- Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Implementar os seguintes tipos de ações para ameaças detectadas pelo ips, antispyware e antivírus;
- Deve permitir, permitir e gerar log, bloquear, bloquear ip do atacante por um intervalo de tempo;
- Deve permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- Permitir o bloqueio de programas exploradores de vulnerabilidades (exploits) conhecidos.

Funcionalidades de Sandbox em Nuvem

- Deve ter a capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante.

Funcionalidades de VPN

- A VPN SSL deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- A VPN SSL deve suportar cliente para plataforma Windows, Linux e Mac OS X;
- Deve permitir a arquitetura de vpn hub and spoke;
- Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

- A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
- Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
- Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;
- Deve possuir suporte a VPN SSL e deverá manter uma conexão segura com o portal durante a sessão;
- Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- Solução deve ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN.
-

Funcionalidades de Antivírus

- Deve possuir funções de antivírus e anti-spyware;
- Deve possuir antivírus em tempo real, para ambiente de gateway internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;
- Deve permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, dentre outros);
- Deve possuir proteção contra conexões a servidores Botnet;
- Deve permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
- Deve permitir o bloqueio de download de arquivos por tamanho.

Funcionalidades de Application Control

- Deve possuir categoria exclusiva, no mínimo, para os tipos de aplicações: P2P, Instant Messaging, Web, Transferência de arquivos e VOIP;
- Deve reconhecer, no mínimo, 1700 (mil e setecentas) aplicações;
- Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deve ser capaz de controlar aplicações, independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
- Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

- Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deve permitir criação de padrões de aplicação manualmente;
- Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Hangouts chat e bloquear a chamada de vídeo;
- Deve Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Funcionalidades de Análise de Vulnerabilidades

- Deve permitir efetuar análises dos servidores e estações na rede, indicando vulnerabilidades encontradas nos mesmos;
- Deve possuir base de dados local atualizável com as vulnerabilidades;
- Deve permitir que tais análises sejam programadas e automáticas de forma diária, semanal e mensal, e que também possa ser executado via linha de comando de forma imediata;
- Deve permitir definir horários nos quais a análise deve ser interrompida automaticamente de forma a não afetar o desempenho da rede;
- Deve permitir definir quais os equipamentos que serão analisados. No caso de servidores, deve permitir que se defina um usuário e senha para que a análise seja mais completa;
- Deve prover como resultado final uma lista dos dispositivos analisados e as vulnerabilidades encontradas nos mesmos.

Gerenciamento Centralizado de Switches

- Deve permitir o gerenciamento de switches;
- Deve permitir a coleta de syslog;
- Deve permitir o gerenciamento dos switches através de interface gráfica;

- Deve permitir a visualização da topologia física e lógica da rede assim como usuários conectados;
- Deve permitir a autodescoberta de múltiplos switches;
- Deve permitir a atualização de software/firmware dos switches gerenciados;
- Deve permitir a configuração de VLANs de forma centralizada;
- Deve permitir o controle de PoE dos switches gerenciados;
- Deve permitir a configuração de link aggregation;
- Deve permitir a configuração de Spanning Tree;
- Deve permitir a configuração de LLDP/MED;
- Deve permitir habilitar recursos de DHCP snooping;
- Deve implementar descoberta de dispositivos;
- Deve permitir a configuração de autenticação 802.1x;
- Deve ter capacidade de apresentar, no mínimo, os seguintes parâmetros de acesso:
- -Switch através do qual o acesso foi solicitado, porta do switch em que o usuário estava conectado;
- -Endereço MAC da máquina usada pelo usuário;
- -Bytes transmitidos e recebidos durante o período de conexão.

Funcionalidades de SD-WAN

- Deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- Deve suportar Forward Error Connection (FEC);
- Deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;
- Deve poder adicionar e equilibrar, no mínimo, 6 interfaces de dados;
- Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- Deve suportar testar o link (probe) através do seguinte:
  - Ping;
  - HTTP;
  - TCP-Echo;
  - UDP-Echo.

- Deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:
  - Número de Sessões;
  - Volume de Tráfego;
  - IP de Origem e Destino;
  - Transbordo de Link (Spillover).

Funcionalidades de Gerenciamento Wireless

- Deve suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;
- Deve suportar IPv4 e IPv6 por SSID;
- Deve permitir definir quais redes serão acessadas através da controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- Deve suportar a monitoração e supressão de ponto de acesso indevido;
- Deve prover autenticação para a rede wireless através de bases externas como LDAP ou RADIUS;
- Deve permitir a visualização dos clientes wireless conectados;
- Deve suportar configuração de Captive Portal por SSID;
- Deve permitir configurar o bloqueio de tráfego entre os clientes conectados a um SSID e AP específico;
- Deve ser compatível com Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de algoritmo AES e/ou TKIP;
- Deve permitir configurar parâmetros de rádio, como banda e canal;
- Deve possuir método de descoberta de novos Pontos de Acesso de maneira automática;
- Deve possuir método de descoberta de novos Pontos de Acesso baseados em IP estático;
- Deve possuir método de descoberta de novos Pontos de Acesso baseados em DHCP;
- Deve possuir proteção contra ataques do tipo ARP Poisoning na controladora wireless;
- Deve implementar Protected Management Frames de acordo com a norma da aliança WiFi e o padrão 802.11ac;

- Deve possuir WIDS integrado para detecção de ataques;
- Deve Implementar canais de aprovisionamento automático dos Access Points, de forma a minimizar interferência entre eles;
- Deve permitir definir em quais horários determinados SSID estará disponível;
- Deve possibilitar definir número máximo de clientes permitidos por SSID;
- Deve possibilitar definir número máximo de clientes permitidos por AP;
- Deve possibilitar número máximo de clientes permitidos por Radio;
- Deve permitir criar, gerenciar e disponibilizar redes wireless mesh;
- Deve possuir mecanismo de criação automática e/ou manual de usuários visitantes e senhas, que possam ser enviadas por email ou SMS aos usuários, e com ajuste de tempo de expiração da senha;
- Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois pontos de acesso gerenciados;
- Deve permitir a identificação do firmware utilizado em cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
- Deve permitir que sejam desabilitados clientes wireless que possuam taxa de transmissão baixa;
- Deve permitir bloquear clientes wireless que tenham sinal fraco, definindo um limiar de sinal a partir do qual esses clientes serão ignorados;
- Deve permitir configurar o valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
- Deve permitir associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID;
- Deve permitir visualizar as aplicações e ameaças por dispositivo wireless;
- Deve permitir a visualização dos usuários conectados em forma de topologia lógica de rede;

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados;

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de

abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM 4 – UPGRADE SOLUÇÃO DE REPOSITÓRIO DE LOG E RELATORIA COM SUPORTE E GARANTIA POR 48 (QUARENTA E OITO) MESES

- Upgrade da solução baseado em appliance ou em servidor virtualizado. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- O upgrade deve ser compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+ and Open Source Xen 4.1+, KVM on Redhat 6.5+ and Ubuntu 17.04, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI);
- O Upgrade deve ampliar capacidade da solução atual para processar, no mínimo, 16 GB de logs por dia e armazenamento total de 9TB, atualmente a solução possui capacidade de 6 GB logs por dia e armazenamento total de 3TB;
- Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período mínimo de 48 (quarenta e oito) meses;
- Deve ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês;
- Deve ser compatível com item a atual solução de segurança de redes NGFW em funcionamento na DESO;
- Deve ser compatível com item SOLUÇÃO DE GESTÃO E GERENCIAMENTO DE DISPOSITIVOS deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve suportar Traps SNMP;
- Deve possibilitar a comunicação com os dispositivos monitorados através de IPSEC;
- Deve gerar alertas para os problemas de segurança encontrados pelos Dispositivos de Segurança especificados neste termo de referência;

- Deve possibilitar o armazenamento de páginas Web, E-mail, arquivos transferidos via FTP e conversas via Instant Message;
- Deve prover a geração de, pelo menos, os seguintes tipos de relatório: máquinas mais acessadas; serviços mais utilizados; usuários que mais utilizaram serviços; URLs mais visualizadas; categorias Web mais acessadas;
- Deve possuir uma ferramenta de relatórios integrada ao sistema de gerenciamento e monitoramento;
- Deve suportar a personalização e à criação de novos relatórios pelos administradores;
- Deve possibilitar a quarentena de arquivos infectados, que forem detectados pelos dispositivos de segurança especificados neste termo;
- Deve possibilitar as buscas nos logs de tráfego por usuários;
- Deve funcionar de forma independente do sistema de gerenciamento, garantindo o seu funcionamento mesmo com a parada do sistema de gerenciamento;
- Deve ser totalmente compatível com os demais itens descritos neste termo.

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM – 05 SOLUÇÃO DE GESTÃO E GERENCIAMENTO DE DISPOSITIVOS COM SUPORTE E GARANTIA POR 48 (QUARENTA E OITO) MESES

- Características Gerais:
- Deve ser do mesmo fabricante dos itens de firewall, a fim de garantir compatibilidade;
- Deve vir acompanhado de licença para gerenciar, no mínimo, 110 dispositivos;

- Deve ser compatível e permitir gerenciamento dos dispositivos da atual solução de segurança de redes NGFW em funcionamento na DESO;
- Deve ser compatível com item SOLUÇÃO DE REPOSITÓRIO DE LOG E RELATORIA deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve permitir e estar licenciado para operar em alta disponibilidade (HA) sincronizando as configurações, objetos e políticas entre as estações de gerência;
- Caso a solução de gerenciamento seja ofertada em appliance físico deverá possuir:
- Possuir ao menos 2 interfaces de 10Gbps RJ-45;
- Possuir ao menos 32GB de memória RAM;
- Possuir ao menos um processador octacore;
- Possuir ao menos 22TB de armazenamento, configurados em RAID 1;
- Caso a solução de gerenciamento seja ofertada em appliance virtual deverá:
  - Ser compatível com ambiente VMware ESXi 5.5;
  - Estar licenciada para pelo menos 3 TB de espaço em disco;
  - Não possuir limite na quantidade de múltiplas vCPU caso virtual;
  - Não possuir limite para suporte a expansão de memória RAM caso virtual;

Funcionalidades da Solução de Gerência

- Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS);
- Permitir acesso concorrente de administradores;
- Possuir interface baseada em linha de comando para administração da solução de gerência;
- Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Gerar alertas automáticos via Email;
- Gerar alertas automáticos via SNMP;

- Gerar alertas automáticos via Syslog;
- Deve suportar XML API;
- O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;
- O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;
- Deve permitir usar palavras chaves ou cores para facilitar identificação de regras;
- Permitir localizar quais regras um objeto está sendo utilizado;
- Deve atribuir sequencialmente um número a cada regra de firewall;
- Deve atribuir sequencialmente um número a cada regra de NAT;
- Deve atribuir sequencialmente um número a cada regra de QOS;
- Deve atribuir sequencialmente um número a cada regra de DOS;
- Permitir criação de regras que fiquem ativas em horário definido;
- Permitir criação de regras com data de expiração;
- Permitir backup das configurações e rollback de configuração para a última configuração salva;
- Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
- Um sistema de backup/restore de todas as configurações da solução de gerência deve estar incluso e deve permitir ao administrador agendar backups da configuração em um determinado dia e hora;
- Deve ser permitido ao administrador transferir os backups para um servidor FTP;
- Deve ser permitido ao administrador transferir os backups para um servidor SCP;
- As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;
- Caso os appliances percam comunicação com os servidores de gerência, os firewalls deverão continuar tratando o tráfego corretamente, sem causar interrupção das comunicações;

- A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;
- A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;
- Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;
- Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;
- Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;
- Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);
- Deve suportar sincronização do relógio interno via protocolo NTP;
- Deve registrar login ou tentativa de login de qualquer usuário;
- Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;
- Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;
- Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
- Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;
- Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;
- Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
- A solução de gerência deve permitir criar administradores que tenham acesso a todas as instâncias de virtualização;
- Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;
- Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;

- Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;
- Permitir criar os objetos que serão utilizados nas políticas de forma centralizada.

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM 6 – SOLUÇÃO ATIVOS DE REDE – SWITCH TIPO I

Requisitos Mínimos de Performance e quantidades:

- A solução deve ser composta de um único equipamento, montável em rack 19″ devendo este vir acompanhado dos devidos acessórios para tal;
- Deve possuir, no mínimo, 24 portas 1GE SFP para instalação de transceivers;
- Deve possuir, no mínimo, 4 portas 10GE SFP+ para instalação de transceivers;
- Detecção automática MDI/MDIX em todas as portas UTP RJ-45;
- Possuir altura máxima de 1U (1,75");
- Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes;
- Deve possuir capacidade de vazão de ao menos 120 Gbps;
- Deve possuir capacidade de encaminhamento de pacotes por segundo (pps) de, no mínimo, 200 Mpps;
- Deve possuir tabela para 30 mil endereços MAC;
- Deve suportar 4 mil VLAN´s 802.1q;

- Implementar agregação de links utilizando LACP. Deverá ser possível a formação de grupos com até 8 portas;
- Deve ser compatível com item SOLUÇÃO DE REPOSITÓRIO DE LOG E RELATORIA deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve ser compatível e gerenciado pelo item SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDES (UTM-NGFW) TIPO I deste termo;
- Deve implementar 802.1s – MSTP;
- Deve implementar autenticação 802.1x;
- Deve permitir autenticação em servidores RADIUS;
- Deve implementar IP multicast;
- Deve implementar associação automática de VLAN de acordo com usuário autenticado;
- Implementar SNMPv3 e SSH;
- Deve suportar HTTP REST APIs para configuração e monitoramento;
- Implementar TFTP e FTP em IPv4;
- Implementar LLDP e LLDP-MED;
- Deve implementar recurso de proteção contra loops de rede;
- Deve implementar storm control;
- Deve implementar DHCP snooping;
- Deve implementar Dynamic ARP Inspection;
- Deve possuir fonte de alimentação com tensão 110/220VAC;
- Deve possuir pelo menos 1GB de memória DRAM;
- Deve possuir pelo menos 256 MB de memória Flash;
- Deve possuir buffer de pacotes de, pelo menos, 4 MB;
- Deve implementar SNTP;
- Deve implementar os seguintes padrões IEEE: IEEE 802.1ab, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x;
- A solução de gerência centralizada deverá atender minimamente aos itens descritos abaixo:
  - Permitir total configuração dos equipamentos por meio de interface WEB em IP de gerência único;

- Permitir criação de vlans;
- Permitir roteamento entre vlans;
- Suportar IPV4 e IPV6;
- Ser compatível os seguintes protocolos de prevenção de loops:
  - Spanning tree;
  - Loop guard;

- Criar topologia física e lógica dos ativos de rede gerenciados de forma automática;
- Dhcp snooping;
- Igmp snooping;
- Profiles LLDP;
- Criar políticas de QOS;
- Permitir visualização dos seguintes dados dos usuários por porta conectada:
  - Mac address;
  - Pacotes enviados;
  - Pacotes recebidos;
  - Vlan configurada na porta conectada.

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM 7 – SOLUÇÃO ATIVOS DE REDE – SWITCH TIPO II

Requisitos Mínimos de Performance e quantidades:

- A solução deve ser composta de um único equipamento, montável em rack 19″ devendo este vir acompanhado dos devidos acessórios para tal;

- Deve possuir, no mínimo, 24 portas GE RJ45;
- Deve possuir, no mínimo, 4 portas 10GE SFP+ para instalação de transceivers;
- Detecção automática MDI/MDIX em todas as portas UTP RJ-45.
- Possuir altura máxima de 1U (1,75")
- Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.
- Deve possuir capacidade de vazão de ao menos 120 Gbps;
- Deve possuir capacidade de encaminhamento de pacotes por segundo (pps) de, no mínimo, 180 Mpps;
- Deve possuir tabela para 8 mil endereços MAC;
- Deve suportar 4 mil VLAN´s 802.1q;
- Implementar agregação de links utilizando LACP. Deverá ser possível a formação de grupos com até 8 portas;
- Deve ser compatível com item SOLUÇÃO DE REPOSITÓRIO DE LOG E RELATORIA deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve ser compatível e gerenciado pelo item SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDES (UTM-NGFW) TIPO I deste termo;
- Deve implementar 802.1s – MSTP;
- Deve implementar autenticação 802.1x;
- Deve permitir autenticação em servidores RADIUS;
- Deve implementar IP multicast;
- Deve implementar associação automática de VLAN de acordo com usuário autenticado;
- Implementar SNMPv3 e SSH;
- Deve suportar HTTP REST APIs para configuração e monitoramento;
- Implementar TFTP e FTP em IPv4;
- Implementar LLDP e LLDP-MED;
- Deve implementar recurso de proteção contra loops de rede;
- Deve implementar storm control;
- Deve implementar DHCP snooping;
- Deve implementar Dynamic ARP Inspection;
- Deve possuir fonte de alimentação com tensão 110/220VAC;

- Deve possuir pelo menos 512 MB de memória DRAM;
- Deve possuir pelo menos 64 MB de memória Flash;
- Deve possuir buffer de pacotes de, pelo menos, 2 MB;
- Deve implementar SNTP;
- Deve implementar os seguintes padrões IEEE: IEEE 802.1ab, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x;
- A solução de gerência centralizada deverá atender minimamente aos itens descritos abaixo:
  - Permitir total configuração dos equipamentos por meio de interface WEB em IP de gerência único;
  - Permitir criação de vlans;
  - Permitir roteamento entre vlans;
  - Suportar IPV4 e IPV6;
  - Ser compatível os seguintes protocolos de prevenção de loops:
    - Spanning tree;
    - Loop guard.
- Criar topologia física e lógica dos ativos de rede gerenciados de forma automática;
- Dhcp snooping;
- Igmp snooping;
- Profiles LLDP;
- Criar políticas de QOS;
- Permitir visualização dos seguintes dados dos usuários por porta conectada:
  - Mac address;
  - Pacotes enviados;
  - Pacotes recebidos;
  - Vlan configurada na porta conectada.

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM 8 – SOLUÇÃO ATIVOS DE REDE – SWITCH TIPO III

Requisitos Mínimos de Performance e quantidades:

- A solução deve ser composta de um único equipamento, montável em rack 19″ devendo este vir acompanhado dos devidos acessórios para tal;
- Deve possuir, no mínimo, 24 portas GE RJ45;
- Deve possuir, no mínimo, 4 portas GE SFP para instalação de transceivers;
- Detecção automática MDI/MDIX em todas as portas UTP RJ-45.
- Possuir altura máxima de 1U (1,75")
- Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.
- Deve possuir capacidade de vazão de ao menos 55 Gbps;
- Deve possuir capacidade de encaminhamento de pacotes por segundo (pps) de, no mínimo, 80 Mpps;
- Deve possuir tabela para 8 mil endereços MAC;
- Deve suportar 4 mil VLAN´s 802.1q;
- Implementar agregação de links utilizando LACP. Deverá ser possível a formação de grupos com até 8 portas;
- Deve ser compatível com item SOLUÇÃO DE REPOSITÓRIO DE LOG E RELATORIA deste termo ou por solução de gerência centralizada do mesmo fabricante dos demais itens deste termo, a ser fornecida em conjunto com o equipamento especificado neste item;
- Deve ser compatível e gerenciado pelo item SOLUÇÃO INTEGRADA DE SEGURANÇA DE REDES (UTM-NGFW) TIPO I deste termo;
- Deve implementar 802.1s – MSTP;
- Deve implementar autenticação 802.1x;
- Deve permitir autenticação em servidores RADIUS;

- Deve implementar IP multicast;
- Deve implementar associação automática de VLAN de acordo com usuário autenticado;
- Implementar SNMPv3 e SSH;
- Deve suportar HTTP REST APIs para configuração e monitoramento;
- Implementar TFTP e FTP em IPv4;
- Implementar LLDP e LLDP-MED;
- Deve implementar recurso de proteção contra loops de rede;
- Deve implementar storm control;
- Deve implementar DHCP snooping;
- Deve implementar Dynamic ARP Inspection;
- Deve possuir fonte de alimentação com tensão 110/220VAC;
- Deve possuir pelo menos 256 MB de memória DRAM;
- Deve possuir pelo menos 32 MB de memória Flash;
- Deve possuir buffer de pacotes de, pelo menos, 512 Kbps;
- Deve implementar SNTP;
- Deve implementar os seguintes padrões IEEE: IEEE 802.1ab, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x;
- A solução de gerência centralizada deverá atender minimamente aos itens descritos abaixo:
  - Permitir total configuração dos equipamentos por meio de interface WEB em IP de gerência único;
  - Permitir criação de vlans;
  - Permitir roteamento entre vlans;
  - Suportar IPV4 e IPV6;
  - Ser compatível os seguintes protocolos de prevenção de loops:
    - Spanning tree;
    - Loop guard;
- Criar topologia física e lógica dos ativos de rede gerenciados de forma automática;
- Dhcp snooping;
- Igmp snooping;
- Profiles LLDP;
- Criar políticas de QOS;

- Permitir visualização dos seguintes dados dos usuários por porta conectada:
  - Mac address;
  - Pacotes enviados;
  - Pacotes recebidos;
  - Vlan configurada na porta conectada.

Suporte Técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.

ITEM 9 – TRANSCEIVER, SFP, 1GE, SX, 850NM

Requisitos Mínimos de Performance e quantidades:

- Deve possuir garantia do fabricante de 12 (doze) meses;
- Deve possuir uma porta duplex 1Gbase-SX;
- Deve suportar distâncias de até 300 metros utilizando fibra multimodo;
- Deve possuir comprimento de onda de 850nm;
- Deve ser compatível com fibras ópticas multimodo;
- Deve possuir conector do tipo Duplex LC;
- Deve ser do compatível com os itens 01 e 02.

ITEM 10 – DISPOSITIVO DE REDE SEM FIO – WIFI COM LICENCIAMENTO POR 48 (QUARENTA E OITO) MESES

- Todo licenciamento, assinaturas e subscrições, necessárias para o completo funcionamento da solução em atendimento às características e especificações devem ser contemplados na oferta pelo prazo mínimo de 48 meses;

- Deverá ser gerenciado por controladora de forma centralizada, pela Solução integrada de segurança de redes Tipos I, II e III;
- Deverá possuir, ao menos, 1 interface de rede 10/100/1000 RJ45;
- Deverá suportar, ao menos, 16 SSIDs simultâneos por Ponto de Acesso, sendo, pelo menos, 8 por rádio;
- Deverá possuir potência de transmissão de, ao menos, 20 dBm;
- Deverá possuir ganho mínimo de 3 dBi por antena em 2.4 GHz e 4dBi por antena em
- 5 GHz;
- Deverá suportar operação na temperatura de 0 a 40 ºC;
- Suporte no mínimo 300 usuários por Ponto de Acesso;
- Deverá ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede;
- Deverá suportar os padrões 802.11a/b/g/n/ac;
- Deverá possuir 2 rádios para atuar nas frequências 2.4 GHz b/g/n e 5 GHz a/n/ac simultaneamente;
- Deverá possuir, ao menos, a tecnologia MIMO (Multiple-In/Multiple-Out) – 2x2;
- Deverá suportar taxas de transferência nominais de, no mínimo, 300 Mbps para o padrão 802.11n e 800 Mbps para o padrão 802.11ac;
- Deverá possuir PoE (Power over Ethernet), padrão 802.3af, possibilitando seu uso sem a necessidade de fontes de energia externas em qualquer porta ethernet;
- Deverá suportar extensão multimídia WME;
- Deverá ser capaz de encontrar automaticamente a Controladora Wireless;
- Deverá suportar o padrão 802.11n High-Throughput (HT) Support: HT 20/40;
- Deverá suportar a criação de redes mesh;
- Deverá suportar a criação de enlaces de bridge entre dois Access Point;
- Deverá permitir a configuração individual para cada SSID, se o tráfego será tunelado até a controladora ao qual ele está registrado e/ou se será comutado localmente;
- Deverá suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação;
- Deverá suportar Adaptive Radio Resource Provisioning (ARRP);
- Deverá possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais;
- Deverá implementar 802.11n A-MPDU e A-MSDU packet aggregation;
- Deverá implementar LPDC – Low Density Parity Checking;

- Deverá implementar MLD – Maximum Likelihood Demodulation;
- Deverá implementar TxBF – Transmit Beamforming;
- Deverá implementar MRC – Maximum Ratio Combining.

Suporte técnico

Todas as funcionalidades de segurança que necessitem de atualização deverão estar licenciadas para 48 (quarenta e oito) meses;

Na prestação do suporte técnico não poderá haver limites no quantitativo de abertura de chamados.

A CONTRATADA deverá disponibilizar telefone, e-mail ou sistema de abertura de chamado para resolução de problemas técnicos com disponibilidade 24 x 7. No caso de abertura através de telefone, o contato será efetuado através de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou números locais em cada município de entregados equipamentos; em ambos os casos, o atendimento deve ser efetuado em língua portuguesa.