CONTRATO N.º _____/2017

Contrato celebrado entre a Assembleia Legislativa do Estado do Rio Grande do Sul e a _____.
(Processo n.º 11403-0100/17-4)

A Assembleia Legislativa do Estado do Rio Grande do Sul, doravante designada CONTRATANTE, com sede na Praça Marechal Deodoro n.º 101, Centro Histórico, cidade de Porto Alegre – RS, inscrita no CNPJ sob o n.º 88.243.688/0001-81, por seu Superintendente Administrativo e Financeiro, Ricieri Dalla Valentina Junior e a _____, doravante designada CONTRATADA, com sede na _____, inscrita no CNPJ sob o n.º _____, representada por _____, celebram o presente Contrato de prestação de serviços, na forma de execução indireta, em regime de empreitada por preço unitário, nos termos da Lei Federal n.º 8.666/1993, da Lei Estadual n.º 13.191/2009, do Edital de Pregão Eletrônico n.º _____/2017, e a proposta vencedora a que se vincula, pelas cláusulas e condições a seguir expressas:

DO OBJETO

CLÁUSULA PRIMEIRA – O presente instrumento tem por objeto a contratação de pessoa jurídica para fornecimento de segurança de perímetro de rede, denominada Next Generation Firewall (NGFW), composta de elementos de hardware e software integrados de mesmo fabricante e que contemple instalação, configuração, customização inicial das políticas de segurança, garantia de 36(trinta e seis) meses, treinamento e serviços de consultoria a fim de atender às necessidades da CONTRATANTE, conforme detalhamento dos itens do objeto constantes no Anexo I.

Parágrafo primeiro – A solução deverá prover no mínimo as funcionalidades de filtro de quadros (L2), filtro de pacotes (L3 e L4), controle de aplicações, VNP IPSec (Site-to-Site) e SSL (Client-to-Site), IPS/IDS, prevenção contra ameaças de vírus, spywares, malwares e APTs, prevenção contra ameaças "Zero Day", Filtro de URL, funcionalidades básicas de controle de dados (DLP) e Anti-DoS. Além destas características, a solução deverá servir como gateway de redes IPv4 e IPv6, bem como, implementar os principais mecanismos de roteamento dinâmico disponíveis na atualidade.

Parágrafo segundo – As quantidades de que trata o objeto deste instrumento poderão ser alteradas pela CONTRATANTE, para mais ou para menos, até o limite de 25% do valor do Contrato, de acordo com o § 1.º do art. 65 da Lei Federal n.º 8.666/93.

DO GESTOR

CLÁUSULA SEGUNDA – O gestor do presente Contrato é o Coordenador das Divisões de Rede e Telecomunicações do Departamento de Tecnologia da Informação da CONTRATANTE.

DAS ESPECIFICAÇÕES TÉCNICAS DO OBJETO

CLÁUSULA TERCEIRA – O objeto deste contrato - solução de segurança de perímetro de rede, denominada Next Generation Firewall (NGFW)- deve atender as especificações constantes no ANEXO II – ESPECIFICAÇÕES TÉCNICAS – do presente instrumento.

DAS CONDIÇÕES DE ENTREGA, INTALAÇÃO E ACEITE

CLÁUSULA QUARTA – O prazo para **entrega, instalação e configuração** do objeto, será de até **100 (cem)** dias a contar do recebimento, pela CONTRATADA, da Ordem de Fornecimento (ou nota de empenho) emitida pelo gestor do contrato.

Parágrafo único – Todo regramento pertinente à entrega, instalação e aceite, está disposto no Anexo III deste Contrato.

DA CAPACITAÇÃO TÉCNICA

CLÁUSULA QUINTA- Após à conclusão da etapa de instalação e de configuração do sistema integrado de segurança para proteção de perímetro de rede em sua integralidade, a CONTRATADA deverá ministrar treinamento da equipe técnica da CONTRATANTE, destinado a transferir os conhecimentos relativos aos equipamentos, "softwares", arquitetura e as configurações da solução adquirida e implantada, bem como sobre a interconexão destes com os principais equipamentos da infraestrutura tecnológica do CONTRATANTE mediante as seguintes condições:

I-Fica a CONTRATADA obrigada a oferecer os treinamentos oficiais do fabricante de nível administrador da plataforma de segurança para no mínimo 02 (dois) analistas da CONTRATANTE;

II- Fica a CONTRATADA obrigada a oferecer os treinamentos oficiais do fabricante de nível de engenheiro da plataforma de segurança para no mínimo 02 (dois) analistas da CONTRATANTE;

III- Caso não exista a possibilidade de realização dos cursos no município de Porto Alegre, fica a CONTRATADA obrigada a custear, passagens aéreas e estadia dos analistas durante o período do treinamento;

IV- Caso seja necessário o deslocamento dos analistas para realização dos treinamentos, deverão ser disponibilizados ao menos duas opções de data para

realização dos respectivos cursos, a fim de garantir a disponibilidade dos serviços mantidos por estes na CONTRATANTE;

V- O treinamento deverá ser ministrado por profissional devidamente capacitado e certificado junto ao fabricante dos equipamentos, devendo este ser demonstrado mediante documento comprobatório de certificação;

VI- O treinamento deverá se constituir em curso oficial do fabricante abrangendo todas as funcionalidades do sistema;

VII-O treinamento poderá ser dividido em módulos de acordo com as funcionalidades disponíveis;

VIII-O treinamento deverá ser ofertado em Português e o material didático deverá ser em Português ou Inglês;

IX-O material didático impresso deverá ser oficial, sendo uma unidade para cada participante;

X-Deverá ser fornecido certificado de participação para cada participante que obtiver pelo menos 75% (setenta e cinco por cento) de frequência;

XI- As despesas inerentes ao treinamento (local, instrutor, "coffee-break", material, equipamentos, entre outros elementos não enumerados taxativamente) serão de responsabilidade da CONTRATADA.

DA ASSISTÊNCIA TÉCNICA E GARANTIA

CLÁUSULA SEXTA- Caberá à CONTRATADA a prestação dos serviços de manutenção corretiva e assistência técnica necessária para o conserto e perfeito funcionamento para todos os equipamentos e programas objeto deste contrato.

Parágrafo primeiro: A CONTRATADA deverá prestar serviços de garantia e assistência técnica, através do fabricante do sistema, em todos os produtos fornecidos, pelo período de 36 (trinta e seis) meses, a contar da data do aceite definitivo do objeto, compreendendo no mínimo:

I- Manutenção corretiva de "hardware" dos produtos fornecidos, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação, novos de primeiro uso e originais, de acordo com os manuais e normas técnicas específicas para os mesmos;

II- Atualizações corretivas, preventivas e evolutivas de "software" e "firmware", incluindo pequenas atualizações de "release", reparos de pequenos defeitos ("bug fixing" e "patches");

III- Ajustes e configurações conforme manuais e normas técnicas do fabricante;

IV- Demais procedimentos destinados a recolocar os equipamentos em perfeito estado de funcionamento;

V- Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos.

CLÁUSULA SÉTIMA: A garantia de 36 (trinta e seis) meses, para todos os componentes de "hardware" e de "software" ofertados na proposta, deverá ser comprovada pelo fabricante do equipamento (por meio de "site", portal ou documentação).

Parágrafo primeiro: Os serviços de garantia e de assistência técnica deverão ser prestados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, no local onde os equipamentos se encontrarem instalados ("on-site"), por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional.

Parágrafo segundo: A CONTRATADA deverá disponibilizar canal de atendimento para abertura de chamados técnicos, por meio de número do tipo 0800 ou número local (nas cidades onde se encontrarem instalados os equipamentos). Adicionalmente, poderá ser disponibilizado serviço de abertura de chamado via "site" ou "e-mail".

Parágrafo primeiro: Para cada chamado técnico, a CONTRATADA deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas.

Parágrafo segundo: Os chamados técnicos serão classificados por criticidade, de acordo com o impacto no ambiente computacional do CONTRATANTE, conforme abaixo:

a)Prioridade Alta: Sistema indisponível ou com severa degradação de desempenho;

b)Prioridade Média: Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema;

c) Prioridade Baixa: Sistema disponível, sem impacto em seu desempenho ou disponibilidade; consultas gerais sobre instalação, administração, configuração, otimização, "troubleshooting" ou utilização.

Parágrafo terceiro- O nível de severidade será informado pela CONTRATANTE no momento da abertura do chamado.

Parágrafo quarto- A CONTRATANTE poderá escalar os chamados para níveis mais altos ou baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de atendimento e de solução, bem como os prazos e percentuais de multa, serão automaticamente ajustados para o novo nível de prioridade. Os serviços de assistência técnica em garantia deverão atender, respectivamente, os seguintes prazos de atendimento inicial e de solução do incidente:

a) Os chamados de "**Prioridade Alta**" deverão ser atendidos em até 1 (uma) hora e solucionados em até 4 (quatro) horas;

b) Os chamados de "**Prioridade Média**" deverão ser atendidos em até 2 (duas) horas e solucionados em até 16 (dezesseis) horas;

c) Os chamados de "**Prioridade Baixa**" deverão ser atendidos em até 4 (quatro) horas e solucionados em até 48 (quarenta e oito) horas.

Parágrafo quinto: O prazo de atendimento começará a ser contado a partir da hora do acionamento do suporte a partir da central de atendimento da CONTRATADA.

I- Entende-se por início de atendimento a hora de chegada do técnico de suporte ao local onde está o produto ou sua intervenção remota.

I- Entende-se por término do atendimento a ocorrência de um dos eventos abaixo relacionados:

a) Solução definitiva;

b) Solução de contorno e escalonamento do chamado para um nível de menor severidade, mediante prévia aprovação do CONTRATANTE;

c) Solução de contorno e escalonamento do chamado para o fabricante, em caso de correção de falhas ("bugs") ou da liberação de novas versões e "patches" de correção, desde que comprovados pelo fabricante do sistema. Para esses problemas, a CONTRATADA deverá restabelecer o ambiente, por meio da adoção de uma solução paliativa, informando o CONTRATANTE em um prazo máximo de 24 (vinte e quatro) horas quando a solução definitiva será disponibilizada. A solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um "patch" ou "fix".

Parágrafo sexto: A CONTRATADA não poderá impor qualquer limitação de quantitativo de chamados, seja diário, mensal, anual, ou de tempo de duração dos chamados, durante o período de prestação dos serviços.

Parágrafo sétimo: O CONTRATANTE poderá acompanhar os chamados técnicos abertos pela CONTRATADA junto ao fabricante.

Parágrafo oitavo- O encerramento do chamado será dado por servidor do CONTRATANTE na conclusão dos serviços, após a disponibilização da solução para uso em perfeitas condições de funcionamento no local onde está instalada.

CLÁUSULA OITAVA- Caberá aos técnicos do fabricante ou da empresa autorizada pelo fabricante identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos fornecidos. Identificado o problema será adotado um dos procedimentos a seguir:

I- Em caso de falhas irrecuperáveis de "hardware" ou impossibilidade de solução pela assistência técnica, a CONTRATADA deverá providenciar a troca por equipamento idêntico.

II-Casos em que se tornará obrigatória a substituição de equipamentos pela CONTRATADA:

a) Falha de componente de "hardware" e/ou componente de "software" que interrompa o funcionamento do equipamento por mais de 3 (três) horas consecutivas;

b) Inoperância do equipamento, por tempo superior a 2 (duas) horas, em 2 (duas) ocasiões separadas por, no máximo, um período de 30 (trinta) dias corridos.

Parágrafo primeiro: Por questão de segurança, os equipamentos e "software" nunca deverão ser removidos das dependências da CONTRATANTE sem a remoção de dados ou regras sigilosas.

Parágrafo segundo: No caso de troca do produto em razão de defeito, não haverá qualquer ônus adicional para CONTRATANTE.

Parágrafo terceiro: Relativamente à manutenção corretiva de "hardware" e "software" os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências do CONTRATANTE, nos prazos do parágrafo quarto da cláusula sétima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.). Não haverá cobrança adicional para a execução dos serviços de garantia e suporte técnico, seus valores deverão estar incluídos no preço ofertado para os produtos adquiridos.

Parágrafo quarto: Concluída a manutenção, a CONTRATADA fornecerá à CONTRATANTE, documento em que conste a identificação do chamado técnico, data e hora de início e término da assistência técnica, descrição dos serviços executados, indicação da peça e/ou componente eventualmente substituído, assim como relato referente às condições inadequadas ao funcionamento do equipamento ou sua má utilização, fazendo constar a causa e as medidas para a sua correção;

Parágrafo quinto: Durante todo o período de garantia, a CONTRATADA atualizará ou disponibilizará para "download", sem ônus adicionais para a CONTRATANTE, os componentes de "softwares" necessários ao perfeito funcionamento dos produtos fornecidos, fornecendo as novas versões ou "releases" lançados. Os componentes de "softwares" tratados neste item incluem vacinas de "anti-virus" e "anti-malware", assinaturas do filtro de conteúdo "web", "software" de gerenciamento, "firmwares" de BIOS e "drivers".

Parágrafo sexto: Qualquer manutenção e/ou intervenção por solicitação da CONTRATADA ou do fabricante, mesmo não implicando em inoperância do sistema ou alteração de suas características, deverá ser agendada e acordada previamente com a CONTRATANTE.

Parágrafo sétimo: Nos casos em que os produtos operem em alta disponibilidade a CONTRATADA e/ou fabricante deverão realizar o reparo ou troca do equipamento que apresente falha ou defeito ainda que o serviço não seja interrompido, sendo contados normalmente os prazos de atendimento.

Parágrafo oitavo: Os serviços deverão ser prestados por equipe técnica qualificada pelo fabricante do sistema.

Parágrafo nono: Será admitida a subcontratação dos serviços de garantia e assistência técnica, desde que previamente autorizada por escrito pelo CONTRATANTE, por empresa comprovadamente autorizada pelo fabricante dos equipamentos;

CLÁUSULA NONA- A CONTRATADA garante por, no mínimo, 5 (cinco) anos de fornecimento dos componentes de hardware, firmware, e software, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas. Em caso de descontinuidade de algum de seus componentes por parte do fabricante, caso ocorra indisponibilidade de componentes de reposição no mercado, o proponente deverá providenciar a substituição do equipamento ou do componente defeituoso por outro que possua, no mínimo, todas as especificações e funcionalidades aqui definidas, sem custos adicionais para o CONTRATANTE.

Parágrafo primeiro: Toda e qualquer peça ou componente consertado ou substituído, ficará automaticamente garantido até o final da garantia;

Parágrafo segundo: Os equipamentos, componentes, peças e materiais que substituírem os defeituosos deverão ser novos, de primeiro uso, originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento, desde que compatíveis, com todas as atualizações e configurações necessárias ao seu funcionamento.

DAS OBRIGAÇÕES DA CONTRATADA

CLÁUSULA DÉCIMA – Além das obrigações já estabelecidas nas cláusulas sexta, sétima, oitava e nona a CONTRATADA obriga-se, também, a:

I) manter sigilo sobre quaisquer dados e informações contidos em quaisquer documentos e em quaisquer mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto e forma divulgar, reproduzir ou utilizar tais recursos;

II) observar que todas as informações geradas e armazenadas referentes aos atendimentos prestados serão de propriedade exclusiva da CONTRATANTE, não podendo a CONTRATADA, em nenhuma hipótese, as utilizar ou divulgar, para qualquer finalidade, sem prévia autorização formalizada da CONTRATANTE;

III) eximir-se de reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado ciência em razão da execução dos serviços previstos neste Termo, sem consentimento, por escrito, da CONTRATANTE;

IV) observar que os executores da CONTRATADA que atuarão na execução dos serviços previstos receberão acesso privativo e individualizado, não podendo repassá-los a terceiros, sob pena de responder, criminal e judicialmente, pelos atos e fatos que venham a ocorrer, em decorrência deste ilícito;

V) observar que será considerado ilícita a divulgação, o repasse ou utilização indevida de informações, bem como dos documentos, imagens, gravações e informações utilizados durante a prestação dos serviços;

VI) entregar ao gestor do contrato toda e qualquer documentação produzida decorrente da prestação de serviços, objeto deste termo, bem como, cederá, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzido, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e documentação, em papel ou em qualquer forma ou mídia;

VIII-atentar que todo e qualquer documento entregue em formato digital, deva estar em formato que permita sua futura edição e aprimoramento;

IX-designar, por escrito, um sócio ou empregado, que receberá a denominação de preposto, para ser o contato com o GESTOR da CONTRATANTE e responder pela execução do Contrato, bem como por seus direitos, deveres e obrigações;

X- responsabilizar-se pela idoneidade e pelo comportamento de seus empregados, prepostos ou subordinados, quando da execução das atividades, respondendo por quaisquer prejuízos ou danos que sejam causados por estes à CONTRATANTE ou a terceiros, quando da execução dos serviços do Contrato;

XI-fazer com que os seus empregados portem crachás de identificação, fornecidos pela CONTRATANTE, quando da execução das tarefas;

XII-fornecer, quando solicitado, para fins de identificação por parte do Departamento de Segurança do Legislativo, a relação dos seus empregados que necessitem acesso às dependências da CONTRATANTE para executar os serviços objeto do Contrato, contendo: nome completo, endereço residencial, telefones residencial e celular, e número da carteira de identidade.

DAS OBRIGAÇÕES DA CONTRATANTE

CLÁUSULA DÉCIMA PRIMEIRA – São obrigações da CONTRATANTE:

a) registrar, por intermédio do GESTOR, com a ciência do representante da CONTRATADA, todas as ocorrências relacionadas com a execução do presente Contrato, determinando o que for preciso para regularização das faltas ou defeitos observados;

b) proceder ao pagamento do preço, na forma e prazo contratados;

c) permitir o acesso dos técnicos da CONTRATADA às dependências da CONTRATANTE, para a execução dos serviços decorrentes do objeto deste Contrato;

d) dar todas as informações necessárias ao cumprimento do Contrato.

Parágrafo primeiro – Qualquer fiscalização exercida pela CONTRATANTE será feita em seu exclusivo interesse, não implicando corresponsabilidade pela execução das atividades e não eximindo a CONTRATADA de suas obrigações pela fiscalização e perfeita execução das atividades.

Parágrafo segundo - A qualquer momento, durante a vigência do contrato, a CONTRATANTE, poderá realizar diligências para comprovação de que a CONTRATADA, para a prestação dos serviços de suporte e garantia, adquiriu junto ao fabricante dos equipamentos em tela, o serviço de suporte e RMA (ou equivalente) do próprio fabricante para todos os itens de hardware e software constantes neste termo de referência;

Parágrafo segundo: A qualquer momento, durante a vigência do contrato, a CONTRATANTE, poderá realizar diligências para comprovação da certificação de cada profissional para a solução de segurança e tal comprovação se dará através da apresentação de cópia autenticada de seu certificado, emitido pelo fabricante dos equipamentos propostos, comprovando a aprovação em testes e requerimentos para tal certificação e especialização. Esta certificação e especialização deverá estar dentro de seu período de validade. Somente serão aceitos certificados de profissionais que

tenham prestado exames e avaliações. Não serão aceitos certificados de simples participação em treinamentos ou atividades similares.

Parágrafo terceiro: A qualquer momento, durante a vigência do contrato, a CONTRATANTE, poderá realizar diligências para comprovação de que a CONTRATADA é parceiro do fabricante e está habilitada a comercializar, dar suporte especializado, instalar e configurar os produtos objetos deste certame.

DO PREÇO E DO PAGAMENTO

CLÁUSULA DÉCIMA TERCEIRA - O valor do objeto do presente contrato, entendido como preço justo e suficiente para a plena execução contratual, deve observar a planilha de quantidades e preços discriminados na tabela a seguir:

ITEM	OBJETO	UNIDADE DE MEDIDA	QUANT.	MARCA/ MODELO	PREÇO UNITÁRIO
SOLUÇÃO DE SEGURANÇA DE REDE					
01	Sistema Integrado de Segurança de Rede.	conjunto	01		
02	Sistema de Gerência Centralizada.	conjunto	01		
SERVIÇOS					
03	Instalação, Configuração, migração e Gerenciamento Assistido.	conjunto	01		
04	Serviços de Capacitação Técnica.	conjunto	01		
05	Serviços de Consultoria e Suporte Técnico.	Valor por Hora Técnica	240	**Preço Unitário**	**Preço Total**
PREÇO GLOBAL				**R$ .....**	

Parágrafo único - O preço a ser pago pela CONTRATANTE deve englobar todas as despesas relativas e os respectivos custos diretos e indiretos, tributos, fretes, encargos trabalhistas, sociais, seguros, remunerações de mão de obra, despesas fiscais e financeiras, e qualquer outra necessária ao cumprimento do objeto.

CLÁUSULA DÉCIMA QUARTA - O pagamento dos itens constantes na tabela acima e na tabela do Anexo I deste termo será efetuado conforme regramento

disposto a seguir:

Parágrafo Primeiro – O pagamento dos itens 01(sistema integrado de segurança de rede) e 02 (sistema de gerência centralizada) será efetuado da seguinte forma:

a) Após homologada a entrega e gerado o Termo de Recebimento Físico, será efetuado pagamento de 30% do valor deste conjunto dentro de 15 dias mediante apresentação de documento fiscal de cobrança;

b) O valor restante será creditado em até 15 dias, após a emissão do Termo de Recebimento Definitivo;

Parágrafo segundo – O pagamento do item 3 (serviço de instalação, configuração, migração e gerenciamento assistido) será efetuado em 15 dias mediante apresentação de documento fiscal de cobrança e após a emissão do Termo de Aceite Definitivo. Não será emitido aceite parcial deste item.

Parágrafo terceiro – O pagamento do item 4 (Serviços de Capacitação Técnica) será efetuado após o recebimento definitivo dos serviços, sendo executados em 15 dias mediante apresentação de documento fiscal de cobrança.

Parágrafo quarto – No caso particular dos serviços de consultoria e de suporte técnico (**item 5** do objeto), os quais serão solicitados por demanda pelo CONTRATANTE, o pagamento será efetuado em parcelas mensais, proporcionais ao número de horas técnicas consumidas no período de apuração, após a efetiva comprovação da prestação dos serviços.

Parágrafo quinto – O pagamento do item 5 (serviço de consultoria e suporte técnico) será efetuado em parcela mensal e ocorrerá em conformidade com a efetiva prestação dos serviços, sendo proporcional ao número de horas técnicas consumidas no intervalo temporal em questão.

Parágrafo sexto – O preço a ser pago pela CONTRATANTE deve englobar todas as despesas relativas e os respectivos custos diretos e indiretos, tributos, encargos trabalhistas, sociais, seguros, remunerações de mão de obra, despesas fiscais e financeiras, e qualquer outra necessária ao cumprimento do objeto.

DA MORA

CLÁUSULA DÉCIMA QUINTA – Caso a CONTRATANTE não realize o pagamento dentro do prazo estabelecido, o valor da cobrança será acrescido de multa de mora, no percentual de 0,5% (meio por cento) ao mês, calculado *pro rata die*, limitado ao valor integral do documento de cobrança.

DA VIGÊNCIA

CLÁUSULA DÉCIMA SEXTA – O prazo de vigência do presente Contrato

tem início na data de assinatura, cuja eficácia é condicionada à publicação de sua súmula no Diário Oficial da Assembleia Legislativa, e perdurará por 36 (trinta e seis) meses, considerando o período de garantia, iniciando-se esta última contagem na data de emissão do aceite definitivo do objeto.

DA RESCISÃO

CLÁUSULA DÉCIMA SÉTIMA – O Contrato será rescindido:

I) por ato unilateral e escrito da CONTRATANTE, nas hipóteses relacionadas nos incisos I a XII e XVII, do artigo 78 da Lei Federal n.º 8.666/93;

II) amigavelmente, por acordo entre as partes, reduzido a termo no processo, e desde que haja conveniência para a CONTRATANTE; ou

III) judicialmente, em consonância com a legislação correspondente.

Parágrafo primeiro – A rescisão deste Contrato implicará a retenção dos créditos decorrentes, até o limite dos prejuízos ocasionados à CONTRATANTE.

Parágrafo segundo – A CONTRATADA reconhece os direitos da CONTRATANTE no caso de rescisão, prevista nos arts. 77 a 80 da Lei n.º 8.666/93.

DAS PENALIDADES E SUA APLICAÇÃO

CLÁUSULA DÉCIMA OITAVA– Ressalvados os casos fortuitos ou de força maior, devidamente comprovados e reconhecidos como tais pela CONTRATANTE, a inexecução parcial ou total das condições pactuadas neste Contrato, garantida a prévia defesa e o contraditório em regular processo administrativo, sem prejuízo da responsabilidade civil e criminal que os atos porventura ensejarem, submeterá a CONTRATADA à aplicação das seguintes sanções:

I) advertência, por escrito, sempre que ocorrerem faltas consideradas pela CONTRATANTE como sendo de pequena importância;

II) multa;

III) suspensão temporária do direito de licitar e de contratar com a Administração Pública do Rio Grande do Sul, pelo período de até 5 (cinco) anos;

IV) declaração de inidoneidade para licitar ou para contratar com a Administração Pública enquanto perdurarem as razões determinantes da punição ou até que seja concedida a reabilitação pela CONTRATANTE, desde que ressarcidos os prejuízos resultantes de sua conduta e após transcorridos 2 (dois) anos da punição.

Parágrafo primeiro – A multa poderá ser aplicada cumulativamente às demais penalidades estabelecidas, e a sua cobrança não isentará a CONTRATADA do dever de ressarcir os prejuízos eventualmente ocasionados.

Parágrafo segundo – Quando, no entender da CONTRATANTE, a falta perpetrada justificar a rescisão do contratual por justa causa, será aplicada à CONTRATADA multa de 10% (dez por cento) do valor integral deste Contrato.

Parágrafo terceiro – O desatendimento, pela CONTRATADA, às obrigações contratadas configura falta no cumprimento do presente Contrato.

Parágrafo quarto – Além de ensejarem a rescisão do Contrato, configuram justa causa para a aplicação da penalidade de suspensão temporária do direito de licitar e de contratar com a Administração Pública do Estado do Rio Grande do Sul, segundo a gravidade da falta incidida pela CONTRATADA:

I) o cometimento reiterado de faltas na execução dos serviços;

II) o descumprimento às determinações do gestor do presente Contrato para a resolução das faltas verificadas na realização destes serviços;

III) a paralisação injustificada dos serviços objeto deste Contrato;

IV) a prática de qualquer ato que vise a fraudar ou burlar o cumprimento das obrigações fiscais, sociais ou trabalhistas decorrentes do Contrato;

V) a utilização de mão de obra de pessoa menor de 18 (dezoito) anos de idade, em infração ao artigo 7.º, inciso XXXIII, da Constituição Federal.

Parágrafo quinto – A pena de declaração de inidoneidade para licitar ou para contratar com a Administração Pública poderá ser aplicada à CONTRATADA na hipótese de descumprir ou cumprir parcialmente o presente Contrato, e desde que deste ato resulte prejuízos à CONTRATANTE.

Parágrafo sexto – As penas de suspensão do direito de licitar e contratar com a Administração Pública do Estado do Rio Grande do Sul e de declaração de inidoneidade para licitar ou contratar com a Administração Pública podem ser aplicadas, à CONTRATADA, caso sofrer condenação definitiva por prática de fraude fiscal ou deixar de cumprir as suas obrigações fiscais ou parafiscais.

Parágrafo sétimo – Exceto na hipótese de fraude na execução do Contrato, as penalidades de suspensão do direito de licitar e de contratar com a Administração Pública do Estado do Rio Grande do Sul e de declaração de inidoneidade para licitar ou contratar com a Administração Pública não serão aplicadas enquanto a CONTRATADA não houver sido punida anteriormente com penalidade menos severa.

Parágrafo oitavo – A CONTRATANTE aplicará multa à CONTRATADA nos seguintes casos, sem prejuízo das demais cláusulas punitivas:

a)descumprimento injustificado do prazo de entrega e instalação do objeto, de 0,3% por dia corrido de atraso, sobre o valor total da solução de segurança;

b)inexecução injustificado do prazo de entrega da documentação de projeto (Aplicado ao PPI e/ou PDI), de 0,3% por dia corrido de atraso, sobre o valor global da solução de segurança;

c)não execução das horas de gerenciamento assistido, na ordem de 0,03% do valor global da solução de segurança, por hora de gerencia não executada;

Parágrafo nono- A CONTRATADA estará sujeita também às multas de:

I- **1% (um por cento)** do valor unitário do item do objeto nas seguintes situações:

a)Por dia de atraso na inexecução dos serviços de treinamento;

b)Por hora de atraso injustificado para a prestação dos serviços de consultoria e de suporte técnico;

c)Por hora de atraso injustificado para a prestação dos serviços de garantia e de assistência técnica.

II-**0,01% (um centésimo por cento)** do valor unitário do item 1 do objeto por hora de atraso no atendimento de chamado técnico cujo impacto foi categorizado como sendo de "Prioridade Baixa", **limitado a 1% (um por cento)**;

III-**0,05% (cinco centésimos por cento)** do valor unitário do item 1 do objeto por hora de atraso no atendimento de chamado técnico cujo impacto foi categorizado como sendo de "Prioridade Média", **limitado a 1% (um por cento)**;

IV-**0,1% (um décimo por cento)** do valor unitário do item 1 do objeto por hora de atraso no atendimento de chamado técnico cujo impacto foi categorizado como sendo de "Prioridade Alta", **limitado a 1% (um por cento)**;

V-**0,01% (um centésimo por cento)** do valor unitário do item 2 do objeto por hora de atraso no atendimento de chamado técnico cujo impacto foi categorizado como sendo de "Prioridade Baixa", **limitado a 1% (um por cento)**;

VI-**0,05% (cinco centésimos por cento)** do valor unitário do item 2 do objeto por hora de atraso no atendimento de chamado técnico cujo impacto foi categorizado como sendo de "Prioridade Média", **limitado a 1% (um por cento)**;

VII-**0,1% (um décimo por cento)** do valor unitário do item 2 do objeto por hora de atraso no atendimento de chamado técnico cujo impacto foi categorizado como sendo de "Prioridade Alta", **limitado a 1% (um por cento)**;

VIII-10% (dez por cento) sobre o valor global do contrato, em caso de inexecução total da obrigação assumida;

IX-10% (dez por cento) sobre o valor global do contrato, a critério da autoridade competente do CONTRATANTE, em razão de qualquer descumprimento das demais obrigações contratuais não previstas taxativamente nos itens supracitados.

X-A recusa da CONTRATADA em entregar o objeto acarretará a multa de 10% (dez por cento) sobre o valor total que lhe foi adjudicado.

Parágrafo nono: No caso de multa, cuja apuração ainda esteja em processamento, ou seja, na fase da defesa prévia, o CONTRATANTE poderá fazer a retenção do valor correspondente à multa, até a decisão final da defesa prévia. Caso a defesa prévia seja aceita, ou aceita parcialmente pelo CONTRATANTE, o valor retido correspondente será depositado em favor da CONTRATADA;

Parágrafo décimo: Os percentuais e valores referentes às multas serão apurados e encaminhados à CONTRATADA para as providências de recolhimento;

Parágrafo décimo primeiro: Não será aplicada multa se, justificada e comprovadamente, a entrega de qualquer um dos itens for decorrente de caso fortuito ou de força maior;

Parágrafo décimo segundo: Em qualquer hipótese de aplicação de sanções, serão assegurados à CONTRATADA o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA NONA – Caracterizada a hipótese ensejadora de aplicação de sanção, o GESTOR da CONTRATANTE notificará a CONTRATADA, abrindo-lhe o prazo de 5 (cinco) dias úteis para oferecer defesa sobre o fato descrito.

Parágrafo primeiro – Findo o prazo para a defesa previsto no *caput*, os autos do processo seguirão para o Superintendente Administrativo e Financeiro da CONTRATANTE, quem decidirá sobre a aplicação da pena, em 5 (cinco) dias úteis.

Parágrafo segundo – A decisão do Superintendente Administrativo e Financeiro deve ser avisada, por escrito, pela CONTRATANTE à CONTRATADA, com lançamento no registro de ocorrências relacionadas com a execução contratual.

Parágrafo terceiro – O montante da multa aplicada será deduzido do pagamento a que a CONTRATADA fizer jus, após a punição, ou pago diretamente à CONTRATANTE, no prazo de 10 (dez) dias úteis da notificação.

DA DOTAÇÃO ORÇAMENTÁRIA

CLÁUSULA VIGÉSIMA – As despesas correm por conta da Função 01 – LEGISLATIVA, Subfunção 0031 – AÇÃO LEGISLATIVA, Atividade 6351 –

APOIO ADMINISTRATIVO E QUALIFICAÇÃO DA INFRAESTRUTURA DA AL, Subtítulo 009 – AÇÕES DE INFORMÁTICA-INVESTIMENTO, Elemento 4.4.90.52 –EQUIPAMENTOS E MATERIAL PERMANENTE.

DO FORO

CLÁUSULA VIGÉSIMA PRIMEIRA - Fica eleito o foro da Comarca de Porto Alegre, capital do Estado do Rio Grande do Sul, para dirimir questões oriundas da interpretação do presente Contrato.

E, por estarem assim de acordo, as partes assinam este instrumento.

Porto Alegre, ___ de _____ de 2017.

_____,
Ricieri Dalla Valentina Junior,
Superintendente Administrativo e Financeiro da
Assembleia Legislativa do Estado do Rio Grande do Sul.

_____,
Representante legal da CONTRATADA.

ANEXO I DO CONTRATO

(DESCRIÇÃO DO OBJETO E QUANTIDADES)

SOLUÇÃO DE SEGURANÇA DE REDE			
Item	**Descrição**	**Unidade**	**Quantidade**
1	Sistema Integrado de Segurança de Rede	Conjunto	Um (01) Conjunto de licenças de hardware e de software que atenda às especificações do item em sua integralidade, considerando o emprego de um cenário em alta disponibilidade dos diversos componentes do sistema em configuração redundante.
2	Sistema de Gerência Centralizada	Conjunto	Um(1) conjunto de licenças de software que atenda às especificações do item em sua integralidade, considerando o emprego de um cenário em alta disponibilidade dos diversos componentes do sistema em configuração redundante.
3	Serviços de Instalação, Configuração, migração e Gerenciamento Assistido	Conjunto	Um(01) conjunto de serviços que atenda às especificações do item em sua integralidade.
4	Serviços de Capacitação Técnica	Conjunto	Um(01) conjunto de serviços que atenda às especificações do item em sua integralidade
5	Serviços de Consultoria e Suporte Técnico	Valor por hora técnica	240 horas

ANEXO II DO CONTRATO

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1) CARACTERÍSTICAS GERAIS

1.1. A solução deve consistir de no mínimo um cluster de appliance de proteção de rede que executem instancias virtuais com funcionalidades NGFW, e uma plataforma de gerencia e monitoramento;

1.2. Os equipamentos que compõem o sistema deverão ser implementados em sistema computacional dedicado do tipo "Appliance" físico, no qual os componentes de "hardware" e de "software" são fornecidos de forma integrada pelo mesmo fabricante, não sendo aceitos servidores convencionais ou máquinas virtuais para fins de implementação de tal papel.

1.3. O sistema operacional da solução deverá ser customizado ou desenvolvido pelo próprio fabricante do firewall, para garantir segurança e melhor desempenho ao firewall, permitindo o monitoramento de recursos no appliance;

1.4. Todos os módulos de software, residentes no appliance de proteção de rede, deverão ser desenvolvidos pelo próprio fabricante, ou seja, não serão aceitas soluções híbridas a partir da integração de diferentes módulos de software oriundos de desenvolvedores distintos;

1.4.1. Por plataforma de gerência e monitoramento, entende-se por software e hardware, bem como as respectivas licenças necessárias para operação das consoles que desempenham este conjunto de funcionalidades;

1.4.2. As consoles de gerencia e monitoramento deverão residir em appliance distinto ao de proteção de rede em esquema de alta disponibilidade, sendo permitido o uso de outro appliance físico (de mesmo fabricante) ou o fornecimento de appliance virtual homologado para as plataformas VmWare e Hyper-V. Tal exigência visa buscar um produto que efetivamente não apresente problemas de desempenho ao prestar o certe de suas funcionalidades em detrimento da execução de processos de gerenciamento da solução;

1.5. Deverá ser comprovado pela licitante que o sistema integrado de segurança de perímetro de rede ofertado foi aprovado no conjunto de critérios de avaliação contido nos testes da NSS Labs, ou da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades. Cabe nesse contexto salientar que, conforme entendimento jurisprudencial contido no acórdão n° 1605/2009 do TCU, "Tais certificações analisadas possuem correlação com o objeto licitado, o qual, pela sua descrição e destinação, deve implementar requisitos de segurança de TI. Portanto, elas estariam aptas a servir de critério para avaliação dos produtos a serem apresentados durante a licitação."

1.6. Devido ao nível de criticidade do ambiente que será atendido pela plataforma, a solução deverá ter figurado como leader ou challenger no quadrante mágico do Gartner na categoria Enterprise Firewalls nos últimos 3 anos. Este requisito

visa garantir que o fabricante da solução adquirida possua a capacidade de execução necessária para atender aos requisitos mínimos exigidos.

1.7. A plataforma de segurança deve ser otimizada para análise de conteúdo de aplicações em camada 7;

1.8. Os softwares deverão ser fornecidos em sua versão mais atualizada recomendada pelo fabricante;

1.9. .A atualização de todos os softwares que compões a plataforma deverá ser possível durante a validade do contrato de suporte com o fabricante;

1.10. Deverá ser possível realizar o downgrade de todos os softwares que compões a plataforma ao menos para a versão imediatamente anterior, sem que ocorra a perda da configuração ativa;

1.11. Nos casos em que o dispositivo não possua conectividade com a Internet, o administrador deverá ser capaz de atualizar os softwares e suas respectivas bases de assinaturas, mediante o upload local dos arquivos de atualização pelo fabricante através de um portal na internet;

1.12. O licenciamento das funcionalidades de Firewall de camada 2 (Filtro de Quadros), 3 e 4 (filtro de pacotes), identificação de usuários, VPN IPSec (site-to-site), VPN SSL e Roteamento Dinâmico deve ser vitalício;

1.13. O licenciamento das demais funcionalidades de segurança e a atualização das respectivas bases de assinatura deverão estar disponíveis durante o período de validade do contrato de suporte e garantia do objeto adquirido;

1.14. Em nenhuma hipótese, o término do período de garantia ou expiração de demais licenças deverá incorrer no não encaminhamento dos pacotes roteados pela plataforma;

1.15. A atualização das bases de assinaturas de identificação de ameaças não deverá requerer o reinício do sistema;

1.16. A solução deve permitir que seus usuários consumam e compartilhem, de forma anônima ou não, informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do Fabricante, a fim de acelerar a identificação de novas ameaças;

1.17. Quando o software estiver configurado em um esquema de alta disponibilidade, deverá ser possível realizar sua atualização sem que ocorra interrupção dos serviços fornecidos pelo cluster;

1.18. Todos os componentes da plataforma de segurança deverão ser capazes de atuar com data/hora sincronizados a partir de um servidor NTP;

1.19. Nos casos de plataformas de segurança baseadas exclusivamente em processadores de propósito geral, deve ser possível configurar núcleos específicos para o tratamento das interrupções geradas por cada interface de rede;

1.20. Nos casos de plataforma de segurança baseadas exclusivamente em processadores de propósito geral, deve ser possível determinar quantos núcleos serão utilizados para o tratamento de interrupções de rede e quantos serão utilizados pelos módulos de controle do NGFW, como IPS e Controle de Aplicações, de forma a permitir a reserva de recursos para garantir que a solução permaneça responsiva sob condições de sobrecarga;

1.21. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.21.1. Suporte à utilização simultânea de no mínimo 1024 VLANs Tags 802.1q mediante a criação de interfaces ou sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem ("Stateful Firewall") entre elas;

1.21.2. Implementar o padrão IEEE 802.3ad, "Link Aggregation Control Protocol" (LACP) mediante a criação de sub-interfaces lógicas;

1.21.3.Deve ser possível utilizar VLANs sob agregação de link;

1.21.4.Deve implementar roteamento por origem, por destino ou por serviço (Policy based routing (PBR) ou Policy based forwarding);

1.21.4.1. Deve permitir a criação de no mínimo 2000 regras de PBR;

1.21.5. Roteamento multicast (PIM-SM);

1.21.6. IGMP Versões 2 e 3;

1.21.7. DHCP Relay;

1.21.8. DHCP Server;

1.21.9. Jumbo Frames;

1.22. Deve suportar no mínimo 16.000 entradas em sua tabela ARP;

1.23. Deve suportar os seguintes tipos de NAT:

1.23.1. Dinâmico (Many-to-1);

1.23.2. Estático (1-to-1);

1.23.3. Estático (Many-to-Many);

1.23.4 Estático bidirecional (1-to-1);

1.23.5. Tradução de Porta (PAT);

1.23.6. Nat de Origem;

1.23.7. Nat de Destino;

1.23.8. Suportar NAT de Origem (SNAT) e NAT de Destino (DNAT) simultaneamente;

1.23.9. Deve suportar que um mesmo endereço possua mais de uma tradução configurada, baseando-se na origem, destino, porta da camada de transporte ou usuário associado ao fluxo de dados;

1.24. Deve permitir que redes ou faixas de endereços IP reservados acessem a Internet a partir de um ou mais endereços IP público (Masquerading);

1.25. Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;

1.26. Deve permitir a criação de no mínimo 4000 regras de NAT;

1.27. Deve suportar o balanceamento de links sem que seja necessária a utilização de protocolos de roteamento dinâmico, devendo implementar no mínimo:

1.27.1 O protocolo ECMP;

1.28. Deve ser capaz de monitorar a disponibilidade dos links mediante a configuração de endereços específicos em redes distintas dos enlaces diretamente conectados ao equipamento. Estes endereços deverão ser monitorados com um protocolo padrão de monitoramento de conectividade como o ICMP***;***

1.28.1 Nos casos de perda de conectividade com algum dos endereços monitorados o equipamento deverá migrar as conexões previamente estabelecidas através do link indisponível para os demais links disponíveis;

1.29. Ser capaz de enviar para ou ter seus logs de acesso coletados para/por sistema de monitoração externos utilizando protocolos de comunicação;

1.30. Proteção contra anti-spoofing;

1.31. Deve permitir bloquear sessões TCP que usarem variações de 3-way hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

1.32.Suportar roteamento estático e dinâmico em IPv4 (RIPv2, BGP e OSPFv2);

1.33.Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

1.34.Os protocolos de roteamento previamente enumerados deverão poder operar de forma simultânea e harmoniosa, mediante a atribuição automática de pesos (Distância Administrativa) para seleção das rotas aprendidas por cada um deles;

1.35.Suportar OSPF graceful restart;

1.36.Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos:

1.36.1.Modo Sniffer, para inspeção via porta espelhada do tráfego da rede;

1.36.2.Modo Camada 2(L2), para inspeção, visibilidade e controle do tráfego de dados no nível da aplicação em um esquema de instalação em linha, sem a necessidade de alteração da estrutura de roteamento para ativação;

1.36.3.Modo Camada 3(L3), para inspeção, visibilidade e controle do tráfego de dados no nível da aplicação em um esquema de instalação padrão de gateway das redes protegidas;

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

1.37.Os mecanismos de IPS, controle de aplicação, filtro de pacotes, filtro de URL e anti-malware devem possibilitar a análise e encaminhamento transparente dos protocolos RTSP, SIP, H.323, mesmo quando for necessário aplicar conversão de endereços (NAT) sobre o fluxo de dados analisado;

1.38.Deve possuir recursos de alta disponibilidade que atendem, no mínimo, aos seguintes requisitos:

1.38.1.Ativação do recurso de HA sem necessitar de licenciamento adicional ou estar licenciado de forma perpétua;

1.38.2.Deve ser capaz de operar em conjunto com dois ou mais equipamentos de mesma classe e do mesmo fabricante, constituindo um esquema de alta disponibilidade (HA) ou balanceamento de carga;

1.38.3.Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

1.38.3.1.Em modo Transparente;

1.38.3.2.Em Layer 3;

1.38.3.3.Suportar a implementação simultânea em todos os modos descritos acima (Transparente e Layer3) no mesmo equipamento.

1.38.4.Os grupos de alta disponibilidade e balanceamento de carga devem ser constituídos por no mínimo dois appliances distintos e independentes;

1.38.5.Os elementos de um grupo devem compartilhar e manter sincronizados:

1.38.5.1.Sessões;

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

1.38.5.3.Certificados;

1.38.5.4.Todas as Associações de Segurança, incluindo das VPNs;

1.38.5.5.Todas as assinaturas de "Anti-virus"/"Anti-spyware"/"Aplicações"/IPS;

1.38.5.6.Configurações de protocolos, tabelas de endereços e de roteamento;

1.39.Na ocorrência de falhas que inutilizem algum dos nós do cluster, as conexões direcionadas a este deverão ser tratadas pelo(s) outro(s) nó(s) sem que isso acarrete interrupções perceptíveis do fluxo de dados;

1.40.O Failover de um cluster (ativação de um novo nó mestre), deverá poder ocorrer mediante o monitoramento das seguintes condições:

1.40.1.Estado físico e administrativo dos links dos nós (up/down);

1.40.2.Comunicação com o no ativo do cluster;

1.40.3.Estado de funcionamento de processos críticos;

1.40.4.Deve ser possível suspender um dos nós do cluster para realização de tarefas de manutenção sem que seja necessário retirar o mesmo do conjunto de alta disponibilidade;

1.41.As funcionalidades de "Firewall", VPN IPSec e SSL Decryption e protocolos de roteamento devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que inexista contrato vigente de garantia de "software" com o fabricante.

1.42.Suportar, sem restrições, no mínimo as seguintes funcionalidades descritas neste termo em redes IPv6: SLAAC (address auto configuration), NAT64, IPv6 over IPv4 IPSec, Identificação de usuários, proteção básica contra DoS (Denial os Service), Descriptografia SSL, DHCPv6 Relay, IPSEc, Alta disponibilidade (Ativo/Ativo, Ativo/Passivo), DNS e controle de aplicação;

1.43. O módulo do sistema que implementa o mecanismo de rede privada virtual (VPN) deverá possuir interoperabilidade com pelo menos os fabricantes Cisco, Checkpoint, Palo Alto Networks, Fortinet, Juniper e Dell ou estar de acordo com as RFCs RFCs 4301 e RFCs 2403 a 2411, de modo a estabelecer canais de criptografia com outros produtos que também implementem tais especificações.

2. CAPACIDADES E QUANTIDADES

2.1.A plataforma de segurança deve ser composta por partes de peça de hardware (appliances) idênticas e independentes, configuradas em um esquema de alta disponibilidade. Cada um dos appliances deverá possuir a capacidade e as características abaixo, bem como as licenças necessárias, para o atendimento de tais requisitos, ao menos durante o período de vigência da garantia/contrato de suporte da plataforma:

2.1.1. Throughput mínimo de 20Gbps, por equipamento, para tráfego stateful inspection multiprotocolo somente com a funcionalidade de firewall ativa, considerando-se para fins de métrica ambiente de produção ou em condições ideais de teste 30Gbps de firewall throughput e pacotes UDP com tamanho de 1518 byte;

2.1.2. Throughput mínimo de 2Gbps, por equipamento, para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente (NGFW), considerando-se para fins de métrica ambiente de produção ou 7Gbps em condições ideais de teste;

2.1.3. Throughput mínimo de 800Mbps, por equipamento, para prevenção de ameaças (***Threat Prevention***), considerando neste contexto tráfego stateful inspection multiprotocolo com Firewall, Controle de Aplicações, IPS, anti-vírus, anti-spyware/anti-bot, habilitada para todas as assinaturas recomendadas pelo fabricante. Neste cenário considera-se para fins de métrica ambiente de produção ou 4Gbps de Throughput em condições ideais de teste

2.1.3.1. O Throughput de 800Mbps, apontado no subitem 5.2.1.3, poderá ser aferido em teste de bancada de acordo com as métricas estabelecidas na seção 9;

2.1.4.Os indicadores de Throughput devem constar do datasheet dos equipamentos ofertados. Este(s) deve(m) ser documento(s) de domínio público emitidos pelo(s) fabricante(s) da solução;

2.1.5.Em função da heterogenia das metodologias de aferição, e da falta de regulamentação sobre os itens apresentados em datasheet, o fabricante poderá complementar o detalhamento das características de capacidade da solução ofertada através de carta oficial do fabricante da solução. No entanto, não poderá haver discrepância entre valores caso ambos os tipos de documentos tratem sobre um mesmo recurso. Neste caso, será considerado o menor valor apresentado.

2.1.6.Descriptografia do Tráfego de Rede Criptografado

2.1.6.1.O sistema deverá descriptografar o tráfego de rede do protocolo HTTPS de saída ("outbound inspection" ou "outbound HTTPS") em conexões negociadas pelos protocolos criptográficos SSL e TLS para fins de controle e inspeção de conteúdo via criação de política de segurança. Por conseguinte, o sistema deverá implementar mecanismo de descriptografia de pacotes IP no tocante ao tráfego de saída criptografado em SSL ou TLS a fim de possibilitar a leitura do "payload" do pacote IP para fins de checagem de assinaturas de aplicações conhecidas pelo fabricante.

2.1.6.2.O sistema deverá implementar mecanismo de bloqueio de conexões com certificados de servidor não confiáveis (ou seja, o qual não possui uma relação de hierarquia com nenhum dos certificados contidos na lista de certificados de autoridades de certificação confiáveis armazenados localmente pelo sistema).

2.1.6.3.O sistema deverá permitir a criação de política de exclusão no contexto da inspeção de conteúdo baseado no protocolo HTTPS de serviços de atualização de "software" publicados na rede mundial de computadores.

2.1.6.4.O sistema deverá identificar o uso de táticas evasivas no contexto das comunicações criptografadas cujo destino seja a rede mundial de computadores.

2.1.6.5.O sistema deverá permitir a criação de uma lista de exceções para aplicações que não funcionam corretamente.

2.1.6.6.É permitido uso de appliances externos adicionais, específicos para descriptografia de SSL e TLS, desse que seja mantida a alta disponibilidade da solução.

2.1.7.Suporte a, no mínimo, 2.000.000 conexões simultâneas;

2.1.8.Suporte a, no mínimo, 120.000 novas sessões por segundo;

2.1.9.Deve possuir LED indicativo de ligado/desligado;

21.10.Deve possuir fonte capaz de operar com tensão de entrada na faixa de 110-240 Volts AC, frequência de operação entre 50 e 60 HZ, redundante, hot-swappble e com detecção automática de tensão e frequência;

2.1.11.Deve possuir, cabos de alimentação para as fontes com comprimento mínimo de 3 (três) metros;

2.1.12.Disco Solid State Drive (SSD) com no mínimo 200GB de capacidade de armazenamento;

2.1.13.Possuir Oito (8) interfaces 1000 Base-TX;

2.1.14.Possuir Duas (2) interfaces 10GBase-SR SFP+, já acompanhados dos tranceivers;

2.1.14.1. Deve suportar expansão futura, por appliance de segurança, em no mínimo 2 portas do tipo 10GBase-SR SFP+ e 1 porta do tipo 40GBase-F QSFP, visando ampliação de conectividade com os equipamentos responsáveis pelo core de rede da CONTRATADA

2.1.15.Possuir uma (1) interface dedicada para alta disponibilidade;

2.1.16.Possuir uma (1) interface 10/100/1000Base-T dedicada ao Gerenciamento;

2.1.17.Possuir uma (1) interface do tipo console ou similar;

2.1.18.Caberá à CONTRATADA o fornecimento de todos os cabos e suportes (se necessário, “gavetas”, “braços” e “trilhos”) para a instalação dos equipamentos;

2.1.19.Caberá a CONTRATADA o fornecimento de todos os módulos necessários para as conexões compatíveis fornecidas pelas interfaces disponíveis;

2.1.20.Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

2.1.21.Todas as interfaces de rede devem suportar a utilização de Jumbo Frames de até 9000 bytes;

2.1.22.Estar licenciado ou suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos;

2.1.23.Estar licenciado ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos e manter uma vazão de até 4Gbps de dados encapsulados;

2.1.24. Características de Virtualização

2.1.24.1. Deve suportar e estar licenciado para executar, no mínimo, 5 sistemas virtuais lógicos (Contextos) no firewall Físico

2.1.24.2. Deve permitir expansão futura para até 20 sistemas virtuais lógicos (Contextos) no firewall Físico;

2.1.24.3.Cada contexto virtual deverá suportar as seguintes funcionalidades, as quais deverão ser implementadas pelo sistema integrado de segurança de rede: filtragem de pacotes de rede ("firewall"), controle de aplicações, descriptografia do tráfego de rede criptografado, identificação de usuários, prevenção de intrusão e de ameaças (IPS), análise e remoção de "malwares" ("anti-virus" e "anti-spyware"), rede privada virtual (VPN), filtragem de URL e conversão de endereço de rede (NAT);

2.1.24.4.O sistema deverá permitir a criação de instâncias de roteadores virtuais em cada um dos contextos virtuais para viabilizar o uso de protocolos de controle no âmbito da camada de rede (em particular, o protocolo de roteamento dinâmico OSPF). Cada roteador virtual criado em cada contexto virtual deverá possuir a sua respectiva tabela de roteamento.

5.2.1.24.5.O sistema deverá permitir a criação de instâncias de comutadores virtuais no âmbito dos contextos virtuais criados previamente para viabilizar o uso de protocolos de controle no âmbito da camada de enlace (dentre os quais, cabe mencionar-se o protocolo LACP).

2.1.25.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;

2.1.26.O equipamento ofertado deverá estar no portfólio do fabricante no máximo a 3 anos, ou seja, o lançamento deste no mercado não poderá ser superior a este

3.POLITICA DE SEGURANÇA

3.1.Deve possibilitar a construção de uma base de objetos e atributos que identifique um fluxo de dados, que sejam utilizáveis para a construção das políticas de segurança da plataforma;

3.2.A base de objetos deverá atender aos seguintes requisitos**:**

3.2.1.Deve contemplar os seguintes tipos de objetos: endereços IPv4, endereços IPv6, intervalos de endereços IPv4, intervalo de endereços IPv6, grupos de endereços IPv4 e IPV6, aplicações, grupos de aplicações, serviços (relação protocolo e porta) e grupos de serviços;

3.2.2.Possuir base de regras singular sem separação de regras orientadas à versão de endereço IP utilizada;

3.2.3.Deve permitir a criação de regras baseadas em combinações irrestritas dos objetos enumerados anteriormente. Ademais, deverá permitir o controle baseados em aplicações, grupos de aplicações, categorias de aplicações, usuários ou grupos de usuários;

3.2.4.Deve possibilitar a criação de no mínimo 40000 objetos do tipo endereço;

3.2.5.Deve possibilitar a criação de no mínimo 2500 objetos do tipo grupo de endereços;

3.2.6.Deve possibilitar a criação de no mínimo 2000 objetos do tipo serviço, além dos serviços previamente cadastrados pelo fabricante;

3.2.7.Deve possibilitar a criação de no mínimo 200 objetos do tipo grupos de serviços, além dos grupos de serviços previamente cadastrados pelo fabricante;

3.3.A política de controle utilizada pelos mecanismos de filtro de pacotes, controle de aplicações e filtro de URL devem atender no mínimo aos seguintes requisitos:

3.3.1.Deve suportar a criação e operação simultânea de no mínimo 5.000 regras;

3.3.2.Deve permitir a criação de regras com data e hora de efetividade, período no qual estas serão consideradas habilitas para fins de controle;

3.3.3.O agendamento da efetividade de regras deverá permitir, além da especificação de datas de expirarão, intervalos recorrentes de validade;

3.3.4.Deve ser capaz de operar sobre uma base de regras mistas, que contenha objetos que referenciem endereços IPv4 e IPv6;

3.3.5.Todas as regras da política devem contar com um campo de texto livre associado para descrição do propósito da mesma;

3.3.6.Deve ser possível configurar a geração ou não de logs de acesso relacionados aos fluxos de dados de cada uma das regras da política;

3.3.7.Deve ser possível configurar se após a atualização da base de regras, as conexões previamente estabelecidas que não deveriam ser permitidas segundo a nova política, serão mantidas ou interrompidas.

4.FILTRO DE PACOTES

4.1.Deve permitir o controle do fluxo de dados por porta e protocolo, usuários grupos de usuários, endereços e redes IP;

4.2.Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário e Drop com envio de TCP-Reset ou mensagem ICMP do tipo Destination Unreachable para o cliente;

4.3.Deve prover mecanismos contra falsificação de endereços (IP Spoofing) e de inundação (SYN flooding);

4.4.O sistema deverá suportar a atribuição de agendamento das políticas de segurança para habilitar e desabilitar tais políticas em horários pré-definidos automaticamente;

4.5.O sistema deverá suportar a criação de políticas de acesso permitindo especificar o dia do mês para o seu funcionamento.

5.5.CONTROLE DE APLICAÇÕES

5.1.Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

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

5.1.2.Controle de políticas por aplicação, grupos de aplicações, categorias e subcategorias de aplicações;

5.1.3.Deve ser possível a liberação e bloqueio de aplicações sem que seja necessário informar portas e protocolos de forma explicita;

5.1.4.Deverá ser possível sobrescrever a porta padrão na qual um determinado serviço normalmente opera, sem que haja prejuízo da análise e identificação da mesma;

5.1.5.Reconhecer pelo menos as seguintes categorias de aplicações: peer-to-per, redes sociais, acesso remoto, update de software, protocolos de rede, voip, streaming de áudio, streaming de vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

5.1.6.Reconhecer no mínimo 1700 aplicações diferentes, incluindo necessariamente as seguintes: bittorrent, gnutella, Skype, facebook, linked-in, twitter, Citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, chat, facebook chat, gmail chat, WhatsApp, 4shared, dropbox, google drive, OneDrive, db2, Mysql, Oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, webex, google-docs, dentre outras aplicações não enumeradas taxativamente;

5.1.7.Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, bloquear o Gtalk chat e permitir o acesso ao gmail ou bloquear a

postagem de atualizações no Facebook mas permitir o acesso de leitura do conteúdo ou permitindo o Gtalk chat e bloquear a transferência de arquivo;

5.1.8.Deve ser possível realizar a inspeção e identificação de aplicações protegidas por SSL;

5.1.9.Deve ser possível criar exceções para inspeção SSL, a fim de evitar, por exemplo, a visibilidade dos dados de aplicações bancárias;

5.1.10.As aplicações deverão possuir um nível de risco, atribuído pelo fabricante segundo critérios objetivos e documentados;

5.1.11.Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicação criptografadas, tais como Skype e ataques mediante porta 443;

5.1.12.Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identifica funcionalidade específicas dentro de uma aplicação, incluindo, mas não limitado à transferência de arquivos dentro do Gtalk. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo com as regras de segurança implementadas;

5.1.13.Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittoorent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

5.1.14.Deve possibilitar a diferenciação de tráfego de Instant Messagin (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;

5.1.15.Deve possibilitar a diferenciação de aplicações Proxies (ultrasurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

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

5.1.16.1.O administrador do sistema deverá ser capaz de criar assinaturas próprias para identificação de aplicações não contempladas previamente pelo fabricante através da interface de administração do sistema ou mediante solicitação ao fabricante;

5.5.1.17.O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

5.5.1.18.No caso de aplicações baseadas no protocolo HTTP(S) que façam uso de um navegador para sua utilização, o usuário deverá ser alertado no caso do bloqueio da mesma;

5.5.1.19.Deve ser possível a criação de grupos de aplicações baseados em características como:

5.5.1.19.1.Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

5.5.1.19.2.Categorias e/ou subcategorias;

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

5.5.1.21.A solução deve ser capaz de bloquear uma conexão até a classificação da aplicação trafegada seja completada.

6.PREVENÇÃO DE AMEAÇAS

6.1.Para proteção efetiva do ambiente, os dispositivos de proteção devem possuir módulo de IPS, IDS, antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através da composição com outro equipamento de mesmo fabricante;

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

6.3.Devem suportar a criação e operação simultânea de no mínimo 15 perfis de proteção, onde um perfil de proteção é o conjunto de assinaturas que devem ser correlacionadas com um determinado fluxo de dados para identificação de ameaças;

6.4.O mecanismo de IPS deve realizar a inspeção de todo o pacote IP (camada 3), independentemente do tamanho do mesmo;

6.5.O mecanismo de IPS deve suportar a inspeção do fluxo de dados de forma bidirecional;

6.6.Nos casos de plataformas de segurança nas quais o módulo de IPS não disponha de hardware especializado e dedicado, o mesmo deverá possuir mecanismos configuráveis de fail-open baseados em valores de utilização de recursos de hardware;

5.6.6.1.Uma vez ativo o mecanismo de fail-open, os administradores do sistema deverão ser comunicados por e-mail e através da interface de gerenciamento centralizado. O software também deverá gerar logs de registro do evento;

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

6.8.Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, antispyware e Antivírus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por meio de um intervalo de tempo e enviar tcp-reset;

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

6.10.Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

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

6.12.Deve permitir o bloqueio de exploits conhecidos;

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

6.13.1.Analise de padrões de estado de conexões;

6.13.2.Analise de decodificação de protocolos;

6.13.3.Analise para detecção de anomalias de protocolo;

6.13.4.Analise heurística;

6.13.5.Bloqueio de pacotes malformados.

6.14.Deve incluir mecanismos de proteção contra-ataques de negação de serviço na camada 3;

6.14.1.Ser imune e capaz de impedir ataques básicos como: Synflood, UDPflood;

6.14.2.Possuir assinaturas específicas para a mitigação de ataques de DoS;

6.15.Detectar e bloquear a origem de portscans;

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

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

6.18.Permitir o bloqueio de conteúdo contendo vírus e spywares transmitidos através dos seguintes protocolos: HTTP, FTP, SMTP;

6.19.Suportar bloqueio de arquivos por tipo;

6.20.Identificar e bloquear a comunicação com botnets (Command & Control);

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

6.22.Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: O nome da assinatura do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

6.23.Deve suportar a captura de pacotes (PCAP), por assinaturas de IPS e Antispyware;

6.24.Deve realizar a captura de pacotes para um conjunto de assinaturas de IPS e Antispyware;

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

6.26.Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

6.27.Proteção contra downloads usando HTTP de arquivos executáveis maliciosos.

6.28.Rastreamento de vírus em pdf;

6.29.Deve permitir a inspeção em arquivos comprimidos que utilizem os formatos, zip e gzip;

6.30.As assinaturas contidas na base de assinaturas de ameaças deverão conter o(s) código(s) CVE (quando aplicável) relacionados à ameaça e um nível de risco atribuído pelo fabricante segundo critérios objetivos e documentados;

6.31.A base de assinaturas de ameaças deverá contemplar no mínimo proteções para as seguintes categorias de serviços: E-mail, DNS, FTP, Aplicações Web, Serviços de rede do Microsoft Windows (Microsoft Networking) e VoIP (H.323 e SIP).

6.32.O módulo de IPS deverá possuir resiliência contra técnicas de evasão avançadas comprovadas por uma entidade independente amplamente reconhecida como a NSS Labs, ICSA Labs ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades;

6.33.O mecanismo de IPS deve permitir a configuração de regras baseadas no posicionamento geográfico dos ips de origem ou destino dos fluxos de dados analisados;

6.34.O mecanismo de IPS deverá permitir a importação de certificados digitais para inspeção do tráfego HTTPS entrante;

6.35.Deve possuir capacidade de inspeção de tráfego SSL ao menos para os protocolos HTTP, FTP e SMTP;

6.36.Deve ser possível criar regras para que determinadas categorias de sites sejam ignoradas pelo mecanismo de inspeção SSL;

6.37.O mecanismo de antivírus deve operar sobre o fluxo de dados de forma transparente, sem que seja necessária a configuração de proxies, rotas estáticas ou qualquer outro mecanismo de redirecionamento explícito de tráfego;

6.38.O mecanismo de Anti-Malware deve ser capaz de analisar e bloquear malware e/ou códigos maliciosos contidos em arquivos com formatos compatíveis com as ferramentas do pacote Microsoft Office 2003 e suas versões subsequentes.

6.38.1. O emprego do termo "anti-malware" poderá contemplar de forma unificada as funcionalidades de "anti-virus" e "anti-spyware"/"anti-bot".

6.39.Além dos arquivos do pacote Office, o mecanismo de antivírus deverá ser capaz de analisar e bloquear malware e/ou códigos maliciosos contidos em arquivos ao menos dos seguintes formatos: bat, com, exe, dll, reg, ps1, js, vbs, jar, swf, cmd, png, jse, midi, mp3, hlp, php, tif, wav, htm, jpg.

6.40.Deve ser capaz de analisar arquivos trafegados ao menos sob os protocolos HTTP, SMTP, IMAP, POP3 e FTP, bem como, sob suas respectivas versões protegidas por SSL, quando houver.

6.41.Deve ser possível realizar a captura de amostra do tráfego cujo conteúdo seja considerado malicioso pelo mecanismo de antivírus. Esta configuração

deve ocorrer de forma granular, por regra, a fim de evitar o consumo excessivo de recursos do equipamento.

6.42.Deve ser capaz de identificar e prevenir a comunicação de ativos sob o escopo de proteção do software com centros de comando e controle (proteção pós-exploração) atendendo no mínimo os seguintes requisitos:

6.42.1.As bases de domínios de DNS, endereços IP e URLs maliciosas utilizadas pelo mecanismo de proteção pós-exploração deve ser atualizada a partir de uma nuvem de inteligência global alimentada de forma colaborativa por outros equipamentos de mesma natureza instalados ao redor do mundo;

6.42.2.Deve realizar a detecção e bloqueio de call-backs (comunicação do malware com os servidores de comando e controle);

6.43.Deve prover mecanismos de bloqueio ao menos para os seguintes tipos de malware/grayware: adware, spyware, hijackers, keyloggers;

6.44.Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de firewall considerando Usuários, Grupos de usuários, origem, destino, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuário, Grupos de usuários, origem e destino.

7.ANÁLISE DE MALWARES

7.1.A plataforma deve possuir funcionalidades de análise de Malwares não conhecidos;

7.2.A plataforma de segurança deve ser capaz e estar licenciada para enviar arquivos trafegados de forma automática para análise em nuvem (SaaS), onde o arquivo será executado e simulado em ambiente controlado (SandBox);

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

7.4.A plataforma de segurança deve ser capaz de identificar e enviar para o serviço de analise arquivos encapsulados ao menos nos protocolos HTTP(S), FTP(S) e SMTP(S);

7.5.O serviço de análise em nuvem deve atender aos seguintes requisitos:

7.5.1.Deve possuir a capacidade de diferenciar os arquivos analisados classificando-os ao menos como: malicioso, não malicioso e indesejáveis, ou empregar classificação equivalente;

7.5.1.1.Entende-se por software indesejável softwares que causem algum tipo de prejuízo de menor impacto para os sistemas afetados, como, lentidão e alteração de configurações;

7.5.2.Suportar análise baseada em comportamentos maliciosos para a identificação de ameaça;

7.5.3.Suportar a análise de arquivos maliciosos em ambientes controlados executando, no mínimo, o sistema operacional Windows 7(32/64 bits);

7.5.4.Ser capaz de analisar links presentes no corpo de mensagens encapsuladas no protocolo SMTP;

7.5.5.Deve prover informações sobre as ações do Malware na máquina infectada, informações sobre as quais aplicações são utilizadas para causar/propagar a infecção;

7.5.6.Detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

7.5.7.Deve permitir exportar o resultado das análises no formato PDF a partir da própria interface de gerencia da plataforma de gerenciamento e monitoração;

7.5.8.Deve permitir o download dos malwares identificados a partir da própria interface de gerencia da plataforma de gerenciamento e monitoração ou a identificação da URL de onde o malware foi acessado inicialmente;

7.5.9.Deve permitir visualizar os resultados das análises de malwares de dia zero (Zero-Day) nos diferentes sistemas operacionais suportados;

7.5.10.O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos;

7.5.11.Deve permitir informar ao fabricante quando a suspeita de ocorrência de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência da plataforma de gerência e monitoração ou através de portal WEB específico;

7.5.12.Caso sejam necessárias licenças de sistemas operacionais e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a CONTRATANTE;

7.5.13.Todas as atualizações das máquinas virtuais utilizadas na solução devem ser providas pelo fabricante da solução;

7.5.14.O sistema de emulação deve exibir quota de percentual (ou total) de arquivos scaneados;

7.5.15.Suportar a análise de arquivos executáveis para plataformas Windows, DLLs, ZIP e criptografados em SSL no ambiente controlado;

7.5.16.Suportar a análise de arquivos do pacote Microsoft Office (.doc, .docx, xls, .xlsx, ppt, pptx);

7.6.É permitida a composição da solução de análise de malwares não conhecidos com hardware especializado do mesmo fabricante da solução NGFW, desde que este seja integrado com a plataforma de gerencia e monitoramento. A

solução deverá ser capaz de avaliar ao menos 500 ameaças potenciais (arquivos suspeitos) por hora;

7.6.1.A solução de sandbox em appliance deve possibilitar a expansão da capacidade de avaliação de ameaças por hora com a inclusão de novos appliances físicos ou virtuais compatíveis com a plataforma VMware/Hyper-V.

8.FILTRO DE URL

8.1.A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

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

8.1.2.Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

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

8.1.4.Deve possibilitar a obrigatoriedade do não uso dos mecanismos de "Safe Search" dos seguintes sistemas de busca: Google, Bing e Yahoo, visando a verificação adequada da URL acessada pelo usuário;

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

.8.1.6.Possui pelo menos 60 categorias de URLs;

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

8.1.8.O fabricante deve fornecer uma descrição objetiva para cada uma das categorias de URL disponíveis;

8.1.9.Suporta a criação de categorias de URLs customizadas;

8.1.10.Suporta a exclusão de URLs do bloqueio, por categoria;

8.1.11.Deve fornecer mecanismos de (re) categorização de URL para os casos em que esta não se encontre categorizada ou não esteja categorizada corretamente;

8.1.12.Deve implementar ao menos as seguintes ações de controle de fluxo: permitir, bloquear e continuar;

8.1.12.1.A ação bloquear deve impedir o acesso do usuário a um determinado recurso da Web mediante a apresentação de uma página de bloqueio.

8.1.12.2.A página de bloqueio deve ser capaz de apresentar no mínimo as seguintes informações: endereço IP de origem da conexão, Identificador do usuário, categoria do recurso bloqueado e URL do recurso bloqueado.

8.1.12.3.A ação continuar deve possibilitar que o usuário acesse um determinado recurso da Web, mediante confirmação exigida por uma página Web apresentada pelo navegador do usuário anteriormente ao acesso;

8.1.12.4.As páginas apresentadas pelas ações bloquear e continuar devem ser personalizáveis pelos administradores do sistema, devendo ser possível editar o código fonte das mesmas com o uso de editores de texto gratuitos e amplamente disponíveis;

8.1.13.Deve suportar a geração de logs de acesso para todas as ações tomadas pelo filtro;

8.1.13.1.Os logs deverão conter no mínimo os seguintes campos do cabeçalho HTTP: UserAgent e Referer;

8.1.14.Deve dispensar a configuração de proxies explícitos nas máquinas clientes (operar em modo transparente) sem que haja perdas de funcionalidades do recurso de filtro de URL.

9.IDENTIFICAÇÃO DE USUÁRIOS

9.1.Deve possibilitar a identificação de usuários ao menos pelos mecanismos de controle de aplicação, filtro de pacotes e filtro de navegação Web, atendendo no mínimo aos seguintes requisitos:

9.1.1.Deve suportar ao menos os seguintes métodos de identificação: Captive Portal, Radius e integração com o Microsoft Active Directory;

9.1.2.Deve dispensar o uso de um usuário com poderes de Domain Admin para integração com o Active Directory;

9.1.3.A integração com o Microsoft Active Dirctory deve dispensar a necessidade de instalação de agentes;

9.2.Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes que utilizem o Microsoft Terminal Server;

.9.3.O Captive Portal deve suportar um esquema de Single Sign On baseado em Kerberos ou NTLMv2;

9.4.Deve suportar o recebimento de eventos de autenticação de dispositivos de rede, dispositivos compatíveis com o padrão 802.1x e soluções de NAC que façam uso de protocolo Radius ou syslog para a identificação de endereços IP e usuários;

9.5.Deve ser capaz de compartilhar a base de usuários identificados com outros componentes da solução;

9.6.Deve possibilitar, a fim de reduzir o uso desnecessário de recursos pelos ativos envolvidos no processo, a definição das redes de origem as quais terão seus fluxos de dados autenticados;

9.7.As especificações de autenticação previamente descritas também devem ser aplicáveis para o tráfego originado a partir de dispositivos móveis;

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

9.9.Deve suportar a autenticação de usuários via Captive Portal;

10.FILTRO DE DADOS

10.1.A plataforma de segurança deverá possuir um conjunto mínimo de recursos para prevenir a evasão de dados sensíveis da organização. Neste contexto, este módulo (Filtro de Dados) deverá atender no mínimo aos seguintes requisitos:

10.1.1.Permitir a criação de filtros para arquivos e dados pré-definidos;

10.1.2.Os arquivos analisados devem ser identificados por extensão e assinaturas;

10.1.3.Permitir identificar e opcionalmente prevenir a transferência sobre aplicações (HTTP, FTP, SMTP, etc) de vários tipos de arquivos (Microsoft Office, pdf, etc);

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

10.1.5.Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

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

11.GEO-LOCALIZAÇÃO

11.1.Suportar a criação de políticas por meio de mecanismo baseado em Geo Localização, permitindo que todo o tráfego gerado a partir de determinado país (ou conjunto de países) seja bloqueado.

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

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

11.4.Deverá possuir pelo menos 200 países previamente cadastrados em sua base;

11.5.Abase de referência geográfica deverá ser atualizada periodicamente pelo fabricante.

12.VPN

12. Baseada em IPSec

12.1.1.O sistema deverá suportar a configuração de rede privada virtual por meio de IPSec manual e IKE (IKEv1 ou IKEv2).

12.1.2.O sistema deverá suportar o gerenciamento centralizado de redes privadas virtuais, com a possibilidade de emprego de várias redes privadas virtuais simultaneamente.

12.1.3.O sistema deverá permitir a criação de políticas de controle de aplicações, IPS, "anti-virus", "anti-spyware" e filtro de URL no contexto do tráfego dos clientes remotos conectados na VPN IPSec.

12.1.4.O sistema deverá suportar a configuração de rede privada virtual IPSec nas modalidades "site-to-site" e "client-to-site".

12.1.5.O sistema deverá possibilitar o acesso a toda infraestrutura de rede interna em conformidade com política de segurança a ser definida pela equipe técnica do CONTRATANTE.

12.1.6.O sistema deverá oferecer acesso remoto seguro a toda a rede interna para qualquer aplicação baseada no protocolo IP via emprego dos protocolos de transporte TCP ou UDP.

12.1.7.O sistema deverá suportar os algoritmos de criptografia 3DES e AES-256 para fins de estabelecimento de associações seguras ("security association" - SA) no contexto do protocolo IKE em suas fases I e II.

12.1.8.O sistema deverá suportar os algoritmos de integridade de dados MD5 e SHA1 para fins de estabelecimento de associações seguras ("security association" - SA) no contexto do protocolo IKE em suas fases I e II.

12.1.9.O sistema deverá suportar pelo menos os seguintes grupos "Diffie-Hellman" para fins de troca de chaves de criptografia no contexto do protocolo IKE em suas fases I e II: grupo 1 (768 bits), grupo 2 (1024 bits), grupo 5 (1536 bits) e grupo 14 (2048 bits).

12.1.10.O sistema deverá suportar a configuração de VPN "site-to-site" nas seguintes topologias de conectividade: "full meshed" (todos para todos), "star" (escritórios remotos para "site" central) e "hub and spoke" ("site" remoto através de "site" central para outro "site" remoto).

12.1.11.O sistema deverá suportar o gerenciamento centralizado de redes privadas virtuais, permitindo a criação de várias redes privadas virtuais simultaneamente, sem que seja necessário efetuar tal tarefa por meio de CLI.

12.1.12.O sistema deverá permitir a criação de políticas de segurança para fins de controle do tráfego que transita no contexto do túnel ponto-a-ponto estabelecido pela rede privada virtual.

12.1.13.O sistema deverá prover mecanismos para mitigar ataques de rede ao protocolo IKE, fazendo a distinção entre "peers" conhecidos e desconhecidos.

12.1.14.O sistema deverá suportar o estabelecimento de redes privadas virtuais com "gateways" remotos que possuam endereços IP públicos e dinâmicos.

12.1.15.O sistema deverá ser fornecido com licenciamento para viabilizar a criação de uma quantidade ilimitada de redes privadas virtuais do tipo "site-to-site" e do tipo "client-to-site". Ou caso não exija licenciamento para tal finalidade, o sistema deverá suportar pelo menos 1.000 (mil) redes VPN do tipo "site-to-site" e do tipo "client-to-site".

12.1.16.O sistema deverá prover clientes para acesso remoto do mesmo fabricante para a plataforma Microsoft Windows.

12.1.17.O sistema deverá prover pacote de instalação de cliente para acesso remoto (agente), o qual poderá ser distribuído automaticamente por meio de plataformas de terceiros (por exemplo, Microsoft Configuration Manager). Tal agente deverá ser compatível pelo menos com os sistemas operacionais Windows 7 e 8.

12.2.Baseada em SSL

12.2.1.O sistema deverá suportar a configuração de rede privada virtual por meio do protocolo SSL.

12.2.2.O sistema deverá permitir a criação de políticas de controle de aplicações, IPS, "anti-virus", "anti-spyware" e filtro de URL no contexto do tráfego dos clientes remotos conectados na VPN SSL.

12.2.3.O sistema deverá suportar a configuração de rede privada virtual SSL na modalidade "client-to-site".

12.2.4.O sistema deverá possibilitar o acesso a toda infraestrutura de rede interna em conformidade com política de segurança a ser definida pela equipe técnica do CONTRATANTE.

12.2.5.O sistema deverá oferecer acesso remoto seguro a toda a rede interna para qualquer aplicação baseada no protocolo IP via emprego dos protocolos de transporte TCP ou UDP.

12.2.6.O sistema deverá possibilitar a customização da interface gráfica da página de "Login" e mensagens de apresentação ao usuário.

12.2.7.O sistema deverá suportar mecanismo de autenticação da categoria "single-sign-on" (SSO).

12.2.7.1.O sistema deverá ser capaz de viabilizar autenticação "single-sign-on" por meio dos protocolos Kerberos, LDAP ou integrado ao "Active Directory System" (ADS).

12.2.8.O sistema deverá possuir mecanismos de validação do grau de aderência de um dado dispositivo remoto com determinados requisitos técnicos de uma dada política de segurança da informação.

12.2.9.O sistema deverá validar o nível de conformidade de um dado cliente remoto para, no mínimo, os seguintes recursos:

12.2.9.1.Versão do sistema operacional e "patches" instalados;

12.2.9.2.Mecanismo de "firewall" ativado no "host";

12.2.9.3.Antivírus instalado e atualizado.

12.2.10.O sistema deverá ser capaz de autenticar usuários por meio do emprego dos seguintes mecanismos de autenticação:

12.2.10.1.Base de dados do próprio sistema;

12.2.10.2.Protocolo LDAP;

12.2.10.3.Protocolo RADIUS;

12.2.10.4.Serviço "Active Directory System" (ADS);

12.2.10.5.Certificado digital.

12.2.11.O sistema deverá suportar a autenticação de usuários por meio do uso de múltiplos fatores.

12.2.12.Os clientes do sistema deverão estar disponíveis para estações de trabalho e para dispositivos móveis.

12.2.13.O sistema deverá implementar mecanismo de acesso remoto aos recursos da rede interna via canal de comunicação baseado no protocolo SSL por meio de módulo cliente a ser baixado e instalado em cada estação de trabalho e dispositivo móvel.

12.2.14.O sistema deverá prover clientes para acesso remoto do mesmo fabricante para a plataforma Microsoft Windows, enquanto que para as demais plataformas (Linux e Apple OS), deverá ser utilizada tecnologia compatível com tais sistemas operacionais.

12.2.15.O sistema deverá prover clientes para acesso remoto para dispositivos móveis baseados nas plataformas Google Android e Apple iOS.

12.2.16.O sistema deverá implementar mecanismo de acesso remoto aos recursos da rede interna via canal de comunicação baseado no protocolo SSL por meio do emprego de "browser" (visualizador) web instalado em cada estação de trabalho.

12.2.17.O sistema deverá prover pacote de instalação de cliente para acesso remoto (agente), o qual poderá ser distribuído automaticamente por meio de plataformas de terceiros (por exemplo, Microsoft Configuration Manager) bem como deverá estar disponível para download diretamente por meio de portal provido pelo sistema. Tal agente deverá ser compatível pelo menos com os sistemas operacionais Windows 7 e 8.

13.SOLUÇÃO DE GERENCIA, MONITORAÇÃO E RELATÓRIOS

13.1.Como boa pratica de segurança e de mercado, a solução de gerencia deverá ser separada dos Gateway de segurança onde irá gerenciar políticas de segurança de todos os firewall e funcionalidades solicitadas neste projeto assim como logs e relatórios de forma unificada;

13.2.A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, WebGUI utilizando protocolo HTTPS;

13.3.Deverá centralizar a administração de regras e políticas da plataforma de segurança utilizando uma única console de gerenciamento;

13.4.Caso haja a necessidade de instalação de um cliente específico para administração da plataforma, o mesmo deverá ser compatível com no mínimo o sistema operacional Windows 7 ou superior;

13.5.A solução de gerencia centralizada deverá ser composta por única console de gerenciamento, sem a necessidade de consoles adicionais para qualquer tipo de administração dos appliances e funcionalidades solicita neste edital;

13.6.O gerenciamento de políticas deverá ser realizado em um único ponto centralizado, não sendo permitido aplicação de políticas de segurança através de dois pontos diferentes.

13.7.Deverá possuir validação da política avisando quando houver regras que ofusquem ou conflitem com outras regras;

13.8.O controle de acesso à console administrativa deve atender aos seguintes requisitos:

13.8.1.Autenticação integrada ao Microsoft Active Directory ou servidor Radius;

13.8.2.Implementar no mínimo 02 (dois) níveis de administração distintos (Administrador e usuário);

13.8.2.1.O nível de administrador deverá ter controle total sobre o sistema instalado no equipamento (read-write);

13.8.2.2.O nível usuário deverá ter acesso apenas às utilidades informativas e de mera visualização de dados (read-only);

13.9.Os recursos de gerenciamento da plataforma devem permitir/possuir:

13.9.1.A criação e administração de políticas de firewall e controle de aplicação;

13.9.2.A criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

13.9.3.A criação e administração de políticas de Filtro de URL;

13.9.4.A criação e administração de políticas de Filtro de DADOS;

13.9.5.A criação e administração dos recursos de VPN;

13.9.6.Mecanismo de busca global na base de objetos tais como aplicações e endereços IPs, permitindo a localização e uso dos mesmo na configuração dos ativos gerenciados;

13.9.7.O uso de cores e/ou marcações (tags) para facilitar a identificação de regras e objetos;

13.9.8.Bloquear alterações, no caso acesso simultâneo de dois ou mais administradores;

13.9.9.Localizar em quais regras um endereço IP, Range de IP, subnet ou objetos estão sendo utilizados;

13.9.10.A atribuição automática de um número para cada regra de firewall e NAT;

13.9.11.Backup das configurações e rollback de configuração para a última configuração salva;

13.9.12.O upgrade dos softwares que compões a plataforma de gerenciamento e respectiva plataforma de segurança gerenciada;

13.9.13.Validação automática de políticas, identificando regras que, ofusquem ou conflitem com outras com outras (shadowing);

13.9.14.A visualização e comparação de configurações Atuais, configuração anterior e configurações antigas;

13.9.15.A geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e horário da alteração;

13.10.Os recursos de monitoração da plataforma devem permitir/possuir:

13.10.1.A monitoração de logs de acesso;

13.10.2.Ferramentas de investigação de logs;

13.10.3.Ferramentas de debugging;

13.10.4.A captura de pacotes processados pelas plataformas de segurança;

13.10.5.Monitorar falhas de hardware, uso elevado de recursos de software, número de túneis de VPN estabelecidos, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões ativas;

13.10.6.Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);

13.10.7.Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

13.10.8.Geração de relatório com dados geográficos em tempo real para visualizações de origens e destinos do tráfego gerado na instituição;

13.10.9.Deve prover relatórios com visão correlacionadas de aplicação, ameaças (IPS, Antivírus e Anti-Spyware), URLs e filtro de arquivos, para melhor diagnóstico e reposta a incidentes;

13.10.10.Deve permitir a criação de Dash-Boards customizados

13.10.11.Coletar estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

13.10.12.Gerar relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, antivírus e Anti-Spyware), etc;

13.10.13.Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus e Anti-Spyware), e URLs que passam pela solução;

13.10.14.Deve possuir relatório de visibilidade e uso de aplicações. O relatório também deve mostrar os riscos associados ao uso de cada aplicação para a segurança do ambiente, tais como a entrega de malwares;

13.10.15.Deve ser possível exportar os logs de acesso para um arquivo CSV;

13.10.16.Deve ser capaz de processar e armazenar, para fins de consulta e geração de relatórios, o volume referente a 90 dias de logs gerados pela solução, sem que isso incorra em novos custos para o CONTRATANTE.

13.10.17.Não deve impor limites temporais rígidos e irreversíveis para o armazenamento de logs; como por exemplo, não ter limites diários para armazenamento de logs;

13.10.18.Deve permitir que os logs e relatórios sejam racionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco ocupado por estes;

13.10.19.Contador de hits ou sessões associadas às regras da política de segurança para auxiliar no processo de identificação de possíveis melhorias de desempenho e a possibilidade de anomalias;

13.10.20.Log em tempo real.

13.10.21.A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos.

13.10.22.Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referente a Malwares encontrados através de emulação, incidentes de vírus e Bots;

13.10.23.A exibição das seguintes informações, de forma histórica e em tempo real:

13.10.23.1. Situação do dispositivo e do cluster;

13.10.23.2.Principais aplicações;

13.10.23.3.Principais aplicações por risco;

13.10.23.4.Administradores autenticados na gerência da plataforma de segurança;

13.10.23.5.Número de sessões simultâneas;

13.10.23.6.Status das interfaces;

13.10.23.7.Uso de CPU;

13.10.23.8.Linha do tempo que permita ao administrador visualizar os eventos de segurança de forma correlacionada e consolidada para um determinado período, sem que haja a necessidade prévia de construção de consultas avançadas

13.10.24.A geração dos seguintes relatórios:

13.10.24.1.Resumo gráfico de aplicações utilizadas;

13.10.24.2.Principais aplicações por utilização de largura de banda de entrada e saída;

13.10.24.3.Principais aplicações por taxa de transferência de bytes;

13.10.24.4.Principais hosts por número de ameaças identificadas;

13.10.24.5.Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivítus e Anti-Spyware), de redes vinculadas a este tráfego;

13.10.25.Deve permitir a criação de relatórios personalizados;

13.11.Em cada critério de pesquisa do log, incluir múltiplas entradas (ex. 10 redes e IPs distintos; serviços HTP, HTTPS e SMTP) exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

13.12.O envio de alertas automáticos via:

13.12.1.Email;

13.12.2.SNMP;

13.12.3.Syslog;

13.13.Os processos de gerenciamento deverão ser priorizados de forma seja possível configurar a plataforma de segurança mesmo durante de alta carga de utilização dos componentes de hardware e software.

14.AQUISIÇÃO DE SERVIÇOS DE CONSULTORIA E SUPORTE TÉCNICO

Os serviços de consultoria e suporte técnico deverão atender aos requisitos enumerados a seguir:

14.1.Caberá a CONTRATADA a prestação dos serviços de consultoria e suporte técnico a todos os produtos fornecidos em utilização ou que venham a ser utilizados por esta casa Legislativa no que tange ao sistema integrado de segurança de-perímetro, pelo prazo de 12 (doze) meses, prorrogáveis por igual período até 36 (trinta e seis) meses, compreendendo suporte telefônico e local ("on-site");

14.2.Os serviços de consultoria e suporte técnico são distintos dos serviços de garantia e de assistência técnica dos equipamentos a serem fornecidos, os quais estão descritos no item 10. Em sua essência, tais serviços visam auxiliar a equipe técnica do CONTRATANTE na administração e na operação do sistema integrado de segurança, no âmbito das atividades que exijam conhecimentos com maior grau de complexidade e que possam impactar negativamente no negócio caso sejam executadas sem sucesso. Tal proposição encontra justificativa no fato de que tal sistema se mostra razoavelmente complexo em função da quantidade de componentes de "software" especializados que são implementados no conjunto de "appliances" do sistema, sendo que o provimento de todo e qualquer serviço de TIC na rede mundial de computadores depende do nível de disponibilidade da referida plataforma;

14.3.A CONTRATADA deverá disponibilizar 240 (duzentos e quarenta) horas técnicas de consultoria e de suporte técnico ao longo de cada período de vigência do contrato, podendo estas ser utilizadas a qualquer tempo, mediante solicitação do CONTRATANTE;

14.4.Os serviços serão solicitados sob demanda mediante a abertura de chamado efetuada por técnicos do CONTRATANTE, via chamada telefônica local, ou por e-mail, no horário das 8h30min às 18h30min, de segunda a sexta-feira, informando a modalidade de atendimento no momento da solicitação, local ou telefônico;

14.5.As horas utilizadas no mês serão pagas no mês subsequente mediante emissão de documento comprobatório da CONTRATADA e ateste de sua efetiva execução pelo gestor do contrato;

14.6.Os serviços prestados ao CONTRATANTE e que não atendam aos padrões de conformidade técnica serão notificados à CONTRATADA com a devida justificativa, não sendo objeto de faturamento e sujeitando-se, ainda, a CONTRATADA, às penalidades contratuais correspondentes;

14.7.As horas técnicas deverão ser prestadas por técnicos devidamente certificados para prestar serviços de consultoria no sistema implantado;

14.8.A CONTRATADA deverá prestar os serviços orientando-se pelos seguintes objetivos:

14.8.1.Utilização das melhores práticas recomendadas pela área de Segurança da Informação;

14.8.2.Adoção das melhores práticas para assegurar os melhores níveis de desempenho tecnicamente possíveis no que tange aos diversos componentes do sistema;

14.8.3.Uso otimizado e eficiente dos recursos tecnológicos empregados pelos diversos componentes do sistema;

14.8.4.Assegurar o melhor grau de integração entre os componentes do sistema entre si e com componentes de outros sistemas computacionais dos quais dependa o bom funcionamento do sistema integrado de segurança.

14.9.Os serviços de suporte técnico deverão ser prestados em plena conformidade com as seguintes condições:

14.9.1.Atendimento local ("on-site"):

14.9.1.1.Deverá ser prestado nas dependências da área técnica do CONTRATANTE, na cidade de Porto Alegre;

14.9.1.2.As horas técnicas a serem consumidas serão contabilizadas da seguinte forma:

14.9.1.2.1.Em dias úteis, de segunda a sexta-feira, das 8h30min às 18h30min, período em que cada hora de serviço prestado corresponderá a 1 (uma) hora técnica de consultoria e suporte técnico;

14.9.1.2.2.Em dias úteis, de segunda a sexta-feira, das 0h às 8h30min e das 18h30min às 23h59min, período em que cada hora de serviço prestado corresponderá a 1 e ½ (uma e meia) hora técnica de consultoria e suporte técnico;

14.9.1.2.3.Em sábados, domingos e feriados, das 0h às 23h59min, período em que cada hora de serviço prestado corresponderá a 2 (duas) horas técnicas de consultoria e suporte técnico.

14.9.1.3.O tempo mínimo contabilizado para fins de atendimento local será de 1 (uma) hora técnica;

14.9.1.4.No final do atendimento, o técnico da CONTRATADA deverá elaborar um relatório de atendimento onde conste, no mínimo, o problema que ocasionou à abertura do chamado, a solução encontrada, as pendências, a data e hora de abertura do chamado, do início e do fim do atendimento e a quantidade de horas despendidas. Esse relatório deve ter a concordância e a assinatura de um técnico do CONTRATANTE.

14.9.2.Atendimento remoto:

14.9.2.1.Prestado nas dependências da CONTRATADA;

14.9.2.2.Por telefone ou por meio de sistema de acesso remoto disponibilizado pelo CONTRATANTE à CONTRATADA;

14.9.2.3.Os atendimentos remotos serão considerados como horas-técnicas remotas e serão contabilizadas como atendimento da seguinte forma:

14.9.2.3.1.Em dias úteis, de segunda a sexta-feira, das 8h30min às 18h30min, período em que cada hora de atendimento remoto prestado corresponderá a 3/4 (três quartos) da hora técnica de suporte técnico;

14.9.2.3.2.Em dias úteis, de segunda a sexta-feira, das 0h às 8h30min e das 18h30min às 23h59min, período em que cada hora de atendimento remoto prestado corresponderá a 1 (uma) hora técnica de suporte técnico;

14.9.2.3.3.Em sábados, domingos e feriados, das 0h às 23h59min, período em que cada hora de atendimento remoto prestado corresponderá a 1 e ½ (uma e meia) hora técnicas de suporte técnico.

14.9.2.4.Os atendimentos remotos por telefone e e-mail serão limitados em 15 (quinze) chamados por mês de competência.

14.10.A prestação dos serviços de suporte técnico por meio telefônico e por e-mail deverá contemplar, no mínimo:

14.10.1.Esclarecimento de dúvidas de utilização, administração e operação dos componentes do sistema fornecido e utilizado pelo CONTRATANTE;

14.10.2.Poderá ser solicitado o envio de procedimentos para viabilizar a resolução de problemas de utilização, administração e operação dos componentes do sistema fornecido e utilizado pelo CONTRATANTE;

14.10.3.Fornecer orientação sobre a necessidade de realizar atualização de um dado componente de "software" do sistema para viabilizar a resolução de problemas reportados;

14.10.4.Fornecer orientação na utilização do suporte junto à fabricante do sistema para fins de envio de correções dos produtos contratados e acionamento de laboratório quando não houver correções disponíveis.

14.11.A prestação dos serviços de consultoria e de suporte técnico compreende, entre outras atividades não enumeradas taxativamente:

14.11.1.Análise, elaboração e implantação de projetos que envolvam componentes de "software" em uso e os que porventura venham a ser utilizados pelo CONTRATANTE;

14.11.2.Auxílio na gestão de políticas de segurança com vistas à prevenção e ao combate de ameaças, desde avaliação e projeto até a implementação tecnológica e reativa a emergências;

14.11.3.Avaliação de vulnerabilidades e prevenção de ameaças no contexto do ambiente computacional do CONTRATANTE;

14.11.4.A identificação e a solução de problemas em componentes de "software" do sistema;

14.11.5.A instalação e configuração de componente de "software" em computadores servidores de rede, caso necessário;

14.11.6.A instalação e configuração de atualizações de "firmware" e de "software" ("patches") nos componentes do sistema;

14.11.7.A implementação de filtros e de outros mecanismos disponíveis nos componentes de "software" do CONTRATANTE, a fim de impedir a proliferação de ameaças identificadas e que não disponham, em determinado momento, de mecanismo de proteção apropriado;

14.11.8.Auxílio na auditoria e análise de "logs".

CONSIDERAÇÕES GERAIS

a)Todos os equipamentos fornecidos devem ser do mesmo fabricante.

b)Todos os equipamentos fornecidos deverão ser entregues com sistema operacional e demais programas necessários ao seu funcionamento instalados e atualizados.

b) Os produtos ofertados deverão ser novos e estar em fase normal de fabricação.

d) os produtos que apresentarem quaisquer falhas que impossibilitem o seu uso ou não atenderem às especificações apresentadas neste termo, deverão ser substituídos sem qualquer ônus à Assembleia Legislativa, no prazo máximo de 20 (vinte) dias úteis após a notificação da CONTRATADA por parte do gestor.

e) somente após a aprovação da instalação e configuração dos produtos relacionados será assinado o termo de Recebimento definitivo para efeito de pagamento.

ANEXO III DO CONTRATO
(ENTREGA, INSTALAÇÃO E ACEITE)

1.SOBRE ENTREGA, INSTALAÇÃO E ACEITE

a)Local e Prazo para entregas

I-O prazo para **entrega, instalação e configuração** do objeto, descrito neste edital, será de até **100 (cem)** dias a contar do recebimento, pela CONTRATADA, da Ordem de Fornecimento (ou nota de empenho) emitida pelo gestor do contrato;

II-Os materiais deverão ser entregues no almoxarifado da Assembleia Legislativa, em embalagens lacradas, com identificação do fabricante ou fornecedor, não sendo aceito equipamentos com caixas violadas;

III-Juntamente da solução, deverá acompanhar documentação técnica, manuais necessários à sua instalação, configuração e operacionalização;

IV-Os equipamentos deverão ser novos, sem uso e em linha de fabricação. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração;

V-Após recebimento e conferencia dos itens, será gerado o Termo de Recebimento Físico do objeto;

b)Projeto Provisório de Instalação (PPI)

I-No PPI deverá constar a prévia de projeto de instalação, contendo, no mínimo, relação de materiais e serviços que vão compor a entrega, croquis e plantas de instalação, topologia física e lógica, detalhamento da configuração do equipamento, relatório de vistoria, planos de migração e ativação e plano de retorno (em caso de falhas);

II-Procedimentos que serão seguidos para a realização dos testes de funcionamento da nova configuração de rede e dos sistemas em instalação;

III-Plano de ativação das proteções;

IV-Informações adicionais, requeridas pelo CONTRATANTE;

V-Montagem completa dos equipamentos no datacenter da CONTRATANTE, cabendo a CONTRATADA o fornecimento de todos os conectores, cabos, e demais componentes que se façam necessários para o perfeito funcionamento das interfaces Ethernet LAN de cada "appliance" do sistema;

VI-Cabe a CONTRATADA verificar durante o planejamento da instalação e vistorias, o padrão da CONTRATANTE quanto à: arquitetura de cabeamento, padrão de conectores ópticos, patch panels, tomadas elétricas e entregar os equipamentos dentro desses padrões ou com as adaptações necessárias;

VII-A CONTRATADA será responsável por elaborar e entregar o PPI da solução de segurança em até **20 (vinte) dias**, a contar do recebimento, pela CONTRATADA, da Ordem de Fornecimento (ou nota de empenho) emitida pelo gestor do contrato;

VIII-A CONTRATANTE fará análise e validação do PPI, em até **3 (três) dias úteis**, apontando as devidas correções e ou ajustes no documento, ficando a CONTRATADA responsável por ajustar o plano em até **3 (três) dias úteis**, a partir da comunicação da CONTRATANTE das não conformidades e das alterações necessárias;

IX-Após entrega dos equipamentos e do Projeto Provisório de Instalação já ajustado pela CONTRATADA, a CONTRATANTE emitirá, em até 5 (cinco) dias úteis, a Ordem de Serviço da Instalação - OSI.

c)Da Instalação

I- Os equipamentos descritos neste termo deverão ser entregues instalados e operacionais, incluindo todos os acessórios necessários para o seu pleno funcionamento, dentro dos prazos contratuais;

II-Fica a critério da CONTRATANTE, definir o horário de instalação e configuração dos equipamentos e softwares, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno, conforme as necessidades da CONTRATANTE;

III-A CONTRATADA deverá fornecer todos os materiais necessários à instalação física completa, à configuração e ao perfeito funcionamento da totalidade dos itens adquiridos;

IV-Constatada a ocorrência de divergência na especificação técnica, falhas de componentes, defeitos de fabricação e operação ou qualquer outro defeito apresentado durante o transporte, a entrega e a instalação dos equipamentos, fica a CONTRATADA obrigada a providenciar a substituição do equipamento, conforme

prazos contratuais, sujeitando-se a CONTRATADA às penalidades previstas na legislação vigente e neste edital;

V-Eventuais despesas de custeio com deslocamento de técnicos da CONTRATADA ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da CONTRATADA;

VI-A CONTRATADA deverá comunicar a CONTRATANTE a conclusão da instalação dos equipamentos e entregar toda documentação técnica prevista, dentro dos prazos contratuais;

VII-A CONTRATADA deverá entregar o Projeto Definitivo de Instalação - PDI ("As Built"), que por sua vez deve contemplar todas as informações constantes previamente do PPI, juntamente com os ajustes, que se mostraram necessários quando da instalação de fato dos ativos;

VIII-A CONTRATADA entregará toda a documentação de instalação física dos equipamentos descritos no **ANEXO 1**, a qual deverá prover nível de informação suficiente para que um técnico possa entender e refazer, caso necessário, as instalações e configurações dos equipamentos adquiridos e implantados;

IX-Após a CONTRATADA concluir toda a instalação dos equipamentos, deixando-os completamente operacionais, e a entrega de toda documentação técnica e do PDI, conforme condições e prazos exigidos neste termo de referência, a CONTRATANTE emitirá o Termo de Recebimento Provisório, em até 5 (cinco) dias úteis, contados a partir do aceite do PDI;

X-Após 15 (quinze) dias úteis da emissão do Termo de Recebimento Provisório, sendo confirmada a operação e desempenho a contento dos equipamentos, nos termos das especificações técnicas e do atestado de homologação, a CONTRATANTE emitirá o Termo de Recebimento Definitivo.

d)Escopo do Serviço de Instalação

I-Fornecimento de ferragens e todos os acessórios necessários para instalação dos equipamentos em rack padrão 19" polegadas;

II-Fornecimento de todos os serviços necessários ao planejamento e a execução da instalação, incluindo projetos, configuração dos equipamentos, planos de retorno e contingenciamento, de acordo com as necessidades da CONTRATANTE.

III-A CONTRATADA deverá executar todas as atividades (físicas e lógicas) de migração dos serviços que se encontrem em operação, incluindo a elaboração do De/Para de portas e a configuração dos equipamentos. A CONTRATANTE deverá disponibilizar a topologia de rede existente para que estas atividades sejam efetuadas.

IV-O plano de retorno e contingenciamento visa garantir a disponibilidade total dos serviços durante e imediatamente após o processo de instalação dos novos equipamentos. Assim, a CONTRATADA, no caso de algum incidente que comprometa os serviços, deverá retornar toda solução conforme estado imediatamente anterior ao processo de instalação. Isso inclui fallback tanto de eventuais configurações alteradas (lógicas), bem como também do respectivo cabeamento (físico).

V-A CONTRATADA deverá ainda, independente de outras atividades necessárias para garantir a disponibilidade total dos serviços, executar:

a)Todos os backups necessários e relacionados à atividade em questão dos equipamentos da rede em produção;

b)Todos os testes, antes e após as atividades de intervenção e/ou instalação, dos serviços em funcionamento na ALRS e que tenham relação com os equipamentos em questão.

VI-Os serviços de instalação deverão ser executados e supervisionados por pelo menos 1 (um) técnico certificado pelo fabricante da solução proposta.

VII-Os acessórios, peças e manuais não utilizados durante a instalação, assim como as embalagens dos equipamentos deverão ser removidas pela CONTRATADA antes da emissão do Termo de Recebimento Definitivo, para que não permaneça no local de instalação nenhum resíduo da embalagem ou qualquer peça solta. Tal exigência é condicionante para emissão do Termo de Recebimento Definitivo;

VIII-Somente será considerado instalado o equipamento entregue, quando instalado no respectivo rack de 19´´ polegadas, cabeado, operacional, em plenas condições de funcionamento, integrado com a rede local e com capacidade de permitir acesso remoto por parte da equipe da CONTRATANTE;

IX-A CONTRATADA deverá realizar a configuração inicial do equipamento para acesso remoto, assim como prestar o fornecimento de quaisquer outros acessórios e serviços que sejam necessários para a completa operacionalização da rede, de acordo com as necessidades da CONTRATANTE;

X-Cabe à CONTRATADA realizar a instalação dos firmwares necessários para o funcionamento e a operação completa dos equipamentos, sendo obrigatória a inclusão no equipamento, no momento da instalação, da versão estável mais atual de todos os firmwares;

XI-Todos os softwares necessários à operação dos equipamentos e soluções devem, igualmente, ser entregues instalados e operacionais. Também devem estar incluídos e licenciados (se for o caso) todos os componentes de software básico necessários ao funcionamento dos equipamentos, tais como: sistemas operacionais, controladores de dispositivos, gerenciamento da solução e outros pertinentes ao objeto deste edital.

e)Transferência de Conhecimento e Gerência Assistida

I-No momento da entrega do PDI, fica a CONTRATADA obrigada a realizar, reunião de conclusão desta etapa com a equipe da Divisão de Redes e Telecomunicações para revisão total da configuração e apresentação do PDI (As-Built) da solução.

II-Além dos aspectos já mencionados, o PDI do deverá contemplar no mínimo os seguintes aspectos:

a)Topologia física e lógica da solução;

b)Mapeamento de Zonas;

c)Mapeamento de IPs;

d)Lista final de regras com a devida explicação para os seguintes recursos:

1.e.II.d.1.Filtro de Quadros;

1.e.II.d.2.Filtro de Pacotes;

1.e.II.d.3.NAT;

1.e.II.d.4.Filtragem de URL;

1.e.II.d.5.Controle de Aplicações;

1.e.II.d.6.IPS, AV e DLP;

e)Credenciais empregadas na integração da solução de segurança com bases de usuários da ALRS (AD, Radius, LDAP);

f)Levantamento de Configurações aplicadas na ativação do Captive Portal;

g)Demais definições, credenciais e configurações de acesso visando atualização das respectivas bases de assinatura de todos os módulos da solução (Ex: AV, IPS, Filtro de URL, Controle de Aplicações, etc);

III-Mapeamento do processo de configuração e validação do Cluster (HA);

IV-Mapeamento do processo de backup da solução;

V-Mapeamento de processos automatizados executados pela solução;

f)A CONTRATANTE terá prazo de 3 dias uteis para aprovação do As-Built, contados a partir da data de entrega deste documento;

I-Caso seja apontado algum detalhe que necessite de correção ou ajuste, a CONTRATADA terá 3 (três) dias uteis para executar tal execução;

g)Após aprovação do PDI, a CONTRATADA deverá iniciar um breve período de Gerenciamento Assistido contemplando os seguintes aspectos:

I-Duração de 5 dias uteis com carga horária diária de 6 horas;

II-A gerencia deverá ser executada nas dependências da CONTRATANTE;

III-Neste processo, as atividades de configuração e manutenção da solução deverão ser acompanhadas pelo profissional que estiver provendo o gerenciamento assistido;

IV-O período de Gerência Assistidas deverá contemplar no mínimo as seguintes atividades:

a)Configurações;

b)Otimização de processos;

c)Troubleshooting;

d)Automatização de Tarefas;

e)Revisão de Politicas;

f)Esclarecimento de dúvidas.