TERMO DE REFERÊNCIA

1. OBJETO

1.1 Fornecimento de solução de segurança de perímetro **utm** contra multi-ameaças, composto de um conjunto de componentes de segurança baseado em appliance de Hardware de Software integrados e de um mesmo fabricante, na modalidade de Pregão Eletrônico, para atender as necessidades do Município de Parnamirim, através do Gabinete Civil.

2. JUSTIFICATIVA

a) A Prefeitura Municipal de Parnamirim encontra-se em constante crescimento e expansão de sua infraestrutura tecnológica. O uso dos recursos tecnológicos, principalmente no que concerne a qualidade da navegação na internet na Prefeitura, é um dos principais fatores.

b) A Prefeitura Municipal de Parnamirim dispõe de uma infraestrutura de rede lógica com mais de 10TB de armazenamento de dados, entre folhas de pontos, usuários de máquinas, documentos e processos.

c) A implementação do firewall é uma necessidade obrigatória para proteger os ativos de tecnologia da informação contra-ataques cibernéticos e promover a continuidade dos sistemas institucionais que usam os ativos de tecnologia da informação do município.

d) Por meio da introspecção dos dados de rede, o firewall é capaz de bloquear acessos não autorizados ou nocivos, mediar o uso de internet, criar conexões de rede seguras, bem como oferecer atualizações para ameaças. A contratação objetiva a proteção de acessos à rede interna (LAN) e rede externa (WAN), visando garantir a Disponibilidade, Integridade, Confidencialidade, Autenticidade e Irretratabilidade dos dados transmitidos ou armazenados na infraestrutura de rede da Prefeitura Municipal de Parnamirim, bem como gerenciar os riscos e ameaças aos ativos de tecnologia da informação.

No que tange ao critério para julgamento do presente certame, informamos que trata-se de uma licitação em que a natureza do objeto não permite o parcelamento, em virtude de

desvantagem a administração pública no momento da fiscalização e da execução dos contratos, caso sejam feitas com empresas distintas. Vejamos dois acórdãos do TCU em que ressalta a legalidade da utilização do preço global:

> *[...] inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem relação entre si. – Acórdão – TCU5.260/2011-1ª Câmara. (Grifo nosso)*
>
> *Número interno do documento: AC-1214-17/13-P Número do Acórdão: 1214 Ano do Acórdão: 2013 – parcelamento do objeto*

Há que se avaliar, para cada tipo de contratação, se o parcelamento é benéfico ou não para a administração, sob os pontos de vista técnico e econômico. Assim, um eventual parcelamento não ampliaria a competitividade das licitações e potencialmente aumentaria o custo da contratação, uma vez que se empresas diversas ganharem a prestação de serviços dessa natureza, o custo fixo por posto de trabalho será maior. Além disso, aumentaria a dificuldade de gerenciamento dos contratos por parte da administração, que teria de se relacionar com um maior número de empresas.

Desse modo, entendemos que não há prejuízos para Administração Pública optar pelo Menor Preço Global, em virtude das suas características e suas obrigatórias interações, que impossibilitariam a atribuição, a diferentes contratadas, eventual responsabilidade por danos ou por defeito de execução dos serviços. Ressaltamos ainda que tal opção facilitará o gerenciamento do contrato, ensejará o planejamento e a racionalização do trabalho, melhor gestão dos contratos, o adequado cumprimento de prazos e padrões de qualidade e não implicará em desvantagens quanto a competitividade.

2.1 GLOSSÁRIO

Termos aplicados neste Termo de Referência:

a) NGFW = Next Generation Firewall, sendo Firewall de Próxima Geração;

b) UTM = Tecnologia embutida nos equipamentos que fornece a proteção contra multi-ameaças como: Vírus, Spam, Worms Spyware, ataques de rede, ameaças de e-mail e etc.

c) Renovação de subscrições = Termo utilizado para renovar as licenças, serviços, suporte, garantias, features e firmwares com o fabricante, mantendo o mesmo equipamento no ambiente.

3. ESPECIFICAÇÃO DOS EQUIPAMENTOS/SOFTWARES PARA AQUISIÇÃO

3.1 – Seguem discriminadas as especificações dos equipamentos/software a serem contratados:

LOTE ÚNICO				
ITEM	**COD. CATSER**	**DESCRIÇÃO**	UNIDADE DE MEDIDA	**QUANT.***
01	609340	Firewall TIPO 1 Solução de NGFW com Appliance de Firewall contra multi ameaças, hardware e software devidamente licenciado – Subscrição por 24 meses.	Unidade	01
02	21172	Serviços: Implantação da solução Onsite e treinamento de capacitação técnica.	Serviço	01

*** Referência para número mínimo de equipamentos a serem entregues.**

3.2 A descrição dos itens deverá ser a exigida neste termo de referência, independente da descrição a que faça referência o código CATMAT/CATSER. Não serão aceitas características diferentes ou inferiores às constantes no item 3, assim como, nos anexos deste termo de referência.

3.3 Projeto para 24 meses de atualizações. Probabilidade máxima de 75% de crescimento nos próximos 3 anos, o hardware e software deve contemplar o crescimento previsto sem necessidade de troca do aparelho.

3.4 Não serão aceitos equipamentos com softwares montados em servidores. Não será aceita solução não homologada no mercado e que não tenha certificados de qualidade e segurança de entidades reconhecidas internacionalmente e governamentais se for o caso, conforme exigência do presente Termo de Referência.

3.5 Não serão aceitos equipamentos que não possuam o recurso exigido do Termo de Referência, mesmo que tenha promessa que venha a ser lançado em um futuro release.

Todos os recursos e especificações técnicas precisam ser atendidos integralmente na data de publicação deste Termo de Referência.

3.6 O projeto busca a máxima segurança e relação custo-benefício com equipamentos que permitam evolução tecnológica.

3.7 Toda a solução ofertada deste Termo de Referência composto de Appliances, hardwares e softwares deve ser de único fabricante, não sendo aceito produtos que dependem de software ou hardware de terceiros para funcionar como ferramenta integrada, ou comprometendo um determinado recurso. Devem obrigatoriamente ser fornecidos como Appliance com finalidade específica e dedicada. O projeto contempla uma solução integrada, com gerenciamento centralizado por único console WEB.

3.8 O Firewall deve suportar ser gerenciado pelo browser de WEB (HTTPS e HTTP), não será aceito gerenciamento por console instalado em desktop ou servidor. Deve permitir ser gerenciado por console WEB único através do Appliance de gerência de rede;

3.9 A empresa vencedora deverá fornecer toda a infraestrutura e pessoal devidamente certificado conforme presente Termo de Referência para implementação, treinar e suportar todo o projeto, sendo obrigatoriamente autorizado do fabricante para a venda e execução dos serviços deste Termo de Referência, comprovando esta condição através de carta emitida pelo fabricante;

3.10 Não será aceito subcontratação por se tratar de uma solução complexa, que envolve muitos elementos técnicos e de muita complexidade, a subcontratação com certeza acarreta prejuízo à segurança e gerenciamento da solução;

3.11 O suporte será prestado exclusivamente pelo fabricante;

3.12 A empresa vencedora deverá apresentar documentos comprovando que atende a todos os itens do presente Termo de Referência. O CONTRATANTE a seu critério poderá chamar o licitante para homologação do projeto e comprovação que atende às exigências do presente Termo de Referência.

4. SERVIÇOS DE IMPLANTAÇÃO, TREINAMENTO E SUPORTE. PLANEJAMENTO DE IMPLANTAÇÃO DA INFRA-ESTRUTURA DE SEGURANÇA DE PERÍMETRO INTERNET

4.1 A implantação deverá ser executada Onsite pelo Fornecedor, com configuração das funcionalidades contratadas e migração do firewall atual. Execução dos seguintes serviços

referentes à implantação da solução:

- Instalação física dos equipamentos firewall de rede;
- Testes de compatibilidade com o ambiente atual do CONTRATANTE;
- Ativação dos equipamentos, registro das licenças no fabricante;
- Configurações das políticas de melhores práticas, para proteção ao console de gerência dos equipamentos;
- Regras de Firewall, visando portar as regras e configurações do firewall atual do CONTRATANTE para o novo ambiente a ser implantado;
- Regras e ações de IDS/IPS;
- Antivírus de Gateway e Filtro de Conteúdo;
- Configuração dos links de internet com o uso da tecnologia SD-WAN, com criação de regras SD-WAN, visando o melhor desempenho dos links no acesso aos serviços Web;
- Monitoramento dos links WAN, LAN, DMZ e outros configurados, visualizando uso do consumo de banda;
- DNS, Alarmes e Relatórios;
- Regras de saída para a internet, para os serviços de protocolos SMTP, WEB, FTP, Cloud;
- Conexões de banco de dados e outros serviços solicitados pelo CONTRATANTE durante a fase de planejamento;
- Autenticação de usuários integrada ao domínio da rede Windows, via ferramenta nativa de integração da solução.
- Configuração do IDS/IPS para monitoramento dos segmentos de rede definidos na fase de planejamento.
- Configuração do antivírus de gateway HTTP, FTP, SMTP e POP3;
- Configuração do Filtro de conteúdo HTTP / FTP;
- Configuração de IPs virtuais, políticas de balanceamento de carga, roteamento simétrico/assimétrico e sincronismo das configurações dos firewalls de rede.
- Migrar, adequar e definir, juntamente com a equipe do CONTRATANTE, as políticas para o controle de tráfego de entrada e saída de dados;
- Instalar e distribuir as políticas de segurança garantindo a proteção em todos os níveis da pilha de rede;

- Configurar NAT, DHCP, endereçamento IP, roteamento, DNS, alarmes, relatórios, regras para SMTP, WEB, FTP, Telnet, conexões de banco de dados e outros serviços solicitados pela equipe do CONTRATANTE durante a fase de projeto;
- Proporcionar uma alta segurança inicial e constante dos sistemas e da rede;
- Proteger a rede e os sistemas do CONTRATANTE contra ataques de negação de serviço (DoS, Denial of Service) e ameaças diversificadas e integradas;
- Configurar a VPN com a criação de túneis seguros, através da Internet, permitindo acesso via CONTRATANTE de VPN ou conexão padrão dos sistemas operacionais Windows, configurar SSL-VPN;
- Integrar o acesso VPN ao Active Directory;
- Configurar a autenticação de usuários integrada ao domínio Active Directory;
- Estabelecer proteção contra intrusão com respostas customizadas para incidentes através de regras customizadas;
- Documentar as configurações realizadas;
- Repassar tecnologia nas instalações da equipe do CONTRATANTE para atualização das informações quanto às tarefas de administração e operação do serviço de firewall implantado;
- Testar completamente e certificar a solução;
- Instalação e configuração da solução de ANTISPAM e ANTIVÍRUS para GATEWAY SMTP;
- Definir, juntamente com a equipe do CONTRATANTE, as políticas para gerenciamento e filtragem de SPAM;
- Definir, juntamente com a equipe do CONTRATANTE, as de políticas de combate a vírus;
- Definir, juntamente com a equipe do CONTRATANTE, uma política de controle de conteúdo de e-mail, (Blocking Policy);
- Instalar as políticas de gerenciamento de conteúdo visando melhorar o fluxo, disponibilidade e segurança da rede, assim como a maximização da produtividade do usuário eliminando qualquer SPAM;
- Testar completamente e certificar a solução.

5. SERVIÇOS DE GARANTIA/SUPORTE DA SOLUÇÃO

5.1 Disponibilização por parte do fabricante da solução, de suporte ilimitado Remoto regime 24x7 durante o período contratado.

5.2 Requisitos dos Serviços de Suporte

Os seguintes requisitos mínimos devem ser atendidos:

a. **Atendimento no local**: Caso identificada a necessidade de atendimento presencial por parte da CONTRATANTE, a CONTRATADA deverá se deslocar até o CONTRATANTE para realizar o atendimento presencial mediante disponibilidade da equipe da CONTRATANTE.
b. **Abertura de chamados:** Os chamados de suporte poderão ser feitos via telefone ou sistema de Help Desk via Internet, com interface WEB. O sistema WEB de HelpDesk, deverá permitir o controle, por parte da CONTRATANTE, de todos os chamados e atendimentos realizados, em aberto ou fechados, além de permitir a emissão de relatórios estatísticos.
c. **Horário de atendimento:** Os serviços de suporte serão executados em regime de 9x5 (Horas e dias úteis comerciais).
d. **Tempo de resposta aos chamados**: Os chamados de suporte realizados, deverão ser respondidos em um prazo compatível com o nível de urgência especificado pela CONTRATANTE no momento da abertura do chamado, conforme descrito a seguir:
e. **Tempo de solução:** o tempo de solução de problemas dependerá de sua extensão, gravidade, disponibilidade de recursos de hardware e software. A empresa contratada deverá fornecer uma estimativa de tempo para solução do problema dentro da primeira hora de atendimento.

Nível do Problema	***Descrição***	***Horário Comercial***		***Horários Alternativos***	
		Remoto	***In-Loco***	***Remoto***	***In-Loco***
Crítico	-Serviço completamente indisponível.	1h	2h	2h	4h
Severo	-Serviço operando parcialmente.	2h	4h	4h	8h
Alerta	-Serviço com degradação de performance ou funcionalidade.	4h	4h	8h	16h

Normal	-Aplicação de patches e hot fixes. -Resolução de dúvidas.	Agendamento com 48 horas

a. Em caso de defeito de equipamentos, (contanto que não acarrete o risco de paralisação dos serviços), o equipamento danificado deverá ser substituído em no máximo 30 (trinta.) dias.
b. Os equipamentos quando danificados, deverão ser substituídos por outros com iguais características ou superior com capacidade de atender ao ambiente da CONTRATANTE.
c. Quando acontecer de problema físico da CONTRATANTE, o deslocamento de equipamentos vai se dar através de transporte de mercado (aéreo ou terrestre) o que for mais rápido, sendo o custo por conta do CONTRATADO.
d. Sistema informatizado para controle e atendimento do suporte: Deverá ser utilizado um sistema informatizado, disponibilizado via Internet, para controle dos serviços de suporte, que funcionará como gerenciador de demandas, devendo possuir registro, acompanhamento e formação de estatísticas sobre a evolução das operações dos atendimentos de suporte.
e. A EMPRESA CONTRATADA deverá disponibilizar este sistema para o CONTRATANTE pelo tempo de duração do contrato.
f. A EMPRESA CONTRATADA deverá instalar os equipamentos na CONTRATANTE, sem nenhum custo adicional, todas as despesas vão correr por conta da CONTRATADA.
g. Durante o período de suporte nos casos que tiver deslocamento para a CONTRATANTE, o custo vai correr exclusivamente por conta da CONTRATADA.

6. QUALIFICAÇÃO TÉCNICA DA CONTRATADA

6.1 Comprovação de que a licitante executou, sem restrição, serviço de natureza compatível ao indicado no Termo de Referência e seus respectivos anexos, para empresa pública ou privada. A comprovação será feita por meio de apresentação de atestado(s), devidamente assinado(s), carimbado(s) e em papel timbrado da empresa ou órgão tomador do serviço, com contato, telefone e e-mail compatível com o objeto desta licitação;

6.2 Apresentar declaração do fabricante, certificando a qualificação técnica do licitante para participação. O fabricante deverá declarar que o licitante é revenda técnica autorizada do fabricante a fornecer suporte e comercializar suas soluções;

6.3 Catálogos e documentos com todas as características técnicas dos produtos propostos, de forma a comprovar atendimento às características técnicas mínimas desta especificação;

6.4 Documentação, manuais, folhetos, sites "impressos" da WEB, com suas respectivas URL´s para conferência, ou qualquer outro tipo de documento técnico, que efetivamente comprove a existência e aderência ao quesito ou padrão exigido ao longo dessas especificações. Um ponto a ponto de cada característica e onde se encontra a referida comprovação deverá ser apresentado juntamente com a proposta, sendo que não comprovação de tais características implicará na desclassificação da proponente;

6.5 Não será aceito equipamento que não atenda a todos os itens do Termo de Referência, nem mesmo promessa que venha a fornecer determinado recurso em um release, upgrade ou versão nova.

7. DO FORNECIMENTO DE SERVIÇOS E EQUIPAMENTOS

7.1. Os fornecimentos de materiais deverão prever todos os equipamentos, componentes e subcomponentes, objetivando garantir a total conectividade e interoperabilidade, que deverão resultar no perfeito funcionamento do conjunto, com níveis de desempenho adequados aos fins a que se destinam no contexto de melhorias nos Serviços de conexões da Prefeitura Municipal de Parnamirim.

7.2. Os equipamentos e serviços a serem utilizados para a execução do serviço, bem como para a sua manutenção em eventuais problemas, ficam sendo de total responsabilidade da empresa contratada. Devendo fornecer **TODOS** os equipamentos e os materiais necessários conforme o solicitado, ou de acordo com a demanda vigente.

7.3. Todos os componentes e subcomponentes objetos deste Termo de Referência deverão ser novos, de primeiro uso, sem previsão de descontinuidade anunciada, com tecnologia atualizada e avançada, em linha de produção atendendo às características técnicas presentes no anexo I.

8 . HOMOLOGAÇÃO DA SOLUÇÃO

8.1 Execução dos seguintes serviços referentes à homologação da solução:

a. Certificação final e otimização da solução;
b. Documentação AS-BUILT de todo o projeto;
c. Repasse de tecnologia para a operação e gerência da solução por parte da equipe

da CONTRATANTE;

9. CONDIÇÕES DE PAGAMENTO

9.1. O pagamento seguirá rigorosamente a Ordem Cronológica de Pagamentos estabelecida pela Resolução 032/2016 TCE/RN e Decreto Municipal nº 6.048/2019, contados a partir da data do atesto da CONTRATANTE.

9.2. Para execução do pagamento, a CONTRATADA deverá fazer constar da Nota Fiscal correspondente, emitida, sem rasura, em letra bem legível em nome do Órgão beneficiado com o devido n.º do CNPJ, informando o número de sua conta bancária, o nome do Banco e a respectiva Agência.

9.3. Havendo erro na Nota Fiscal ou circunstância que impeça a liquidação da despesa, aquela será devolvida à CONTRATADA e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para o Órgão beneficiado.

9.4. Por ocasião da apresentação da nota fiscal/fatura, a CONTRATADA deverá fazer prova do recolhimento mensal dos encargos sociais e previdenciários, quais sejam, INSS,CNDT, FGTS, Certidões Negativas das Fazendas Federal, Estadual e Municipal.

9.5. A CONTRATANTE reserva-se o direito de suspender o pagamento se os produtos forem entregues em desacordo com as especificações constantes neste certame.

9.6. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, acompanhado da nota fiscal, a devida comprovação, a fim de evitar a retenção na fonte, dos tributos e contribuições, conforme legislação em vigor.

10.7 Deverá ser obedecido os ditames do Decreto nº 7.202/2023, que dispõe sobre a retenção de Imposto de Renda nas contratações de bens e na prestação de serviços realizados.

10. DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS

10.1. As sanções administrativas serão impostas fundamentadamente nos termos da Lei nº 8.666/93, garantido o direito à ampla defesa sem prejuízo das cominações legais, ao contratado que:

a) Se recusar a assinar o termo do contrato/Ordem de Compra ou receber a nota de empenho;

b) Inexecução total ou parcial da nota de empenho ou contrato/Ordem de Compra;

c) Apresentar documentação falsa;

d) Ensejar o retardamento da execução do seu objeto;

e) Não mantiver a proposta dentro do prazo de validade;

f) Falhar ou fraudar na execução do contrato;

g) Comportar-se de modo inidôneo;

h) Fazer declaração falsa ou cometer fraude fiscal.

10.2 Independente da sanção aplicada, a inexecução total ou parcial do contrato poderá ensejar, ainda, a rescisão contratual, nos termos previstos na Lei nº. 8.666/93, bem como a incidência das consequências legais cabíveis, inclusive indenização por perdas e danos eventualmente causados à CONTRATANTE.

10.3 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

10.4 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado às secretarias municipais, observado o princípio da proporcionalidade.

11. OBRIGAÇÕES DA CONTRATANTE

11.1 Emitir a nota de empenho;

11.2 Prestar as informações e os esclarecimentos pertinentes aos objetos que venham a ser solicitados pela Contratada;

11.3 Exercer a fiscalização dos bens e serviços entregues, na forma prevista na Lei n° 8.666/1993, procedendo ao atesto das respectivas faturas, com as ressalvas e/ou glosas que se fizerem necessárias;

11.4 Proporcionar todas as facilidades para que a CONTRATADA possa cumprir suas obrigações dentro dos prazos e condições estabelecidas no contrato/Ordem de Compra e ou Ordem de Serviço;

11.5 Efetuar o pagamento do(s) serviço(s) prestado(s), conforme condições estabelecidas neste Termo;

12. DA FISCALIZAÇÃO

12.1 A execução contratual será acompanhada e fiscalizada pela ASCTI (GCTI), especialmente designada para este fim pela contratante, de acordo com o estabelecido no art. 67 da Lei Federal nº 8.666/1993, a ser informado quando da lavratura do instrumento contratual.

13. OBRIGAÇÕES DA CONTRATADA

13.1. As despesas com seguros, transportes, fretes, tributos, encargos trabalhistas e previdenciários e demais despesas envolvidas na entrega correrão por conta da CONTRATADA.

13.2. A CONTRATADA deverá comunicar, por escrito, imediatamente, a impossibilidade de execução de qualquer obrigação contratual, para adoção das providências cabíveis.

13.3. A CONTRATADA deverá manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação.

13.4. O representante da CONTRATADA ficará responsável pela execução dos itens deste Termo de Referência, cabendo acompanhar o cumprimento rigoroso dos prazos, entrega de documentos, elaboração de relatórios de acompanhamento e quaisquer atividades pertinentes à execução do contrato.

13.5. A empresa vencedora responsabiliza-se pela reposição, em caso de imperfeições de fabricação ou transporte, no prazo de até 30 (trinta) dias a partir da comunicação, sem prejuízos da garantia máxima exigida.

13.6. O material e a instalação do serviço deverá ser entregue dentro do prazo estabelecido e na qualidade solicitada, sob pena de responsabilidade contratual, salvo caso fortuito ou motivo de força maior.

13.7. Todos os equipamentos e serviços deverão ser entregues e funcionando perfeitamente.

13.8. A recusa da aceitação dos serviços deverá ser feita por escrito e conterá os elementos que motivaram a sua determinação. Assim, elencará os produtos ou serviços que estão em desacordo com as especificações e/ou os defeitos apresentados. Diante disso, a CONTRATADA se disporá a consertar, ajustar, substituir os produtos ou fazer os serviços apontados na correspondência do Grupo de Ciência e Tecnologia da Informação e

Inovação – GCTI e no término, apresentará o resultado à GCTI.

13.9. A CONTRATADA será responsável pelos seguintes encargos:

11.9.1. Assumir a responsabilidade e o ônus pelo recolhimento de todos os impostos, taxas, tarifas, contribuições ou emolumentos federais, estaduais, e municipais, trabalhistas, com a Regularidade de FGTS e os que incidam ou venham incidir sobre o objeto deste instrumento, bem como apresentar os respectivos comprovantes, quando solicitados pelo CONTRATANTE.

11.9.2. Responsabilizar-se pelos prejuízos causados à CONTRATANTE ou a terceiros por atos de seus empregados ou prepostos, durante a execução deste contrato.

11.9.3. Responder, integralmente, por perdas e danos que vier a causar ao órgão CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

14. REAJUSTAMENTO DOS PREÇOS.

14.1.Os preços registrados são fixos e irreajustáveis no prazo de um ano contado da data de assinatura do contrato.

13.2 Após o interregno de um ano, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do índice ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, , exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

R = V (I – Iº) / Iº, onde:

R = Valor do reajuste procurado;

V = Valor contratual a ser reajustado;

Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta na licitação;

I = Índice relativo ao mês do reajustamento;

14.2 Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, da data da apresentação da proposta, aplicando-se o índice da variação do ICTI exclusivamente para

as obrigações iniciadas e concluídas após a ocorrência da anualidade.

14.3 Os efeitos financeiros do reajuste serão devidos, exclusivamente a partir da data da solicitação, vedada a concessão de reajuste retroativo.

14.4 Nos reajustes subsequentes ao primeiro, o intervalo mínimo de um ano será contado a partir da data da apresentação da proposta.

14.5 No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

14.6 Caso o índice estabelecido para reajuste venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

14.7 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

15. DA DOTAÇÃO ORÇAMENTÁRIA

15.1 As despesas decorrentes da presente contratação serão custeadas com os recursos financeiros e a seguinte Dotação Orçamentária:

Unidade Orçamentária: 02.001 – Gabinete Civil;
Função: 04 – Administração;
Sub–função: 126 – Tecnologia da Informação;
Programa: 0008 – Gestão da Tecnologia da Informação e Comunicação;;
Ação: 1004 – Aquisição de Equipamentos Diversos para otimização de serviços do GCTI;
Natureza:44.90.52 – Equipamentos e Material Permanente
Fonte: 15000000 – Recursos Não Vinculados de Impostos

16. CRITÉRIO DE JULGAMENTO

16.1 A seleção do fornecedor ocorrerá através de Pregão Eletrônico, do tipo MENOR PREÇO GLOBAL, nos termos da Lei Federal n° 8.666/93, cumulada com a Lei nº 10.520 de 17 de julho de 2002.

17. PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

17.1 O contrato vigorará por 12 (doze) meses, a partir da assinatura do mesmo, podendo ser prorrogado, por iguais e sucessivos períodos, até o limite máximo de 60 (sessenta) meses, conforme previsão legal do Art. 57, II, da Lei 8.666/93 e suas modificações.

18. DA APROVAÇÃO DA AUTORIDADE COMPETENTE

18.1 A autoridade competente para aprovar o termo de referência e responder sobre as questões formuladas durante o certame e após sua conclusão, atinentes aos itens definidos neste Termo de Referência .

Parnamirim/RN, 18 de setembro de 2023.

FELIPE FERNANDES DA CUNHA
Coordenador de Redes e Internet - GCTI
Matrícula: 20680

RIJKAARD MELO
Assessor em Tecnologia da Informação
Matrícula: 56383

HABYS MIKAEL DE MORAIS BARROS
Assessor em Tecnologia da Informação - GCTI
Matrícula: 19160
Gestor Geral do GCTI
Em substituição legal

Aprovo o presente Termo de Referência, bem como estou de acordo com todas as informações prestadas nas declarações e assinaturas acima.

JONATHAN TARGINO DANTAS
Chefe de Gabinete Civil
Em substituição legal

Anexo I

ESPECIFICAÇÃO TÉCNICA

1.	**REQUISITOS DE PERFORMANCE E LICENCIAMENTO DE UTM**

1.1.	**Appliance Firewall TIPO 1**	**01 unidade**
1.1.1.	NGFW baseado em *appliance* . Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.	
1.1.2.	Deve-se ser entregue único equipamento com todas as funcionalidades requisitadas.	
1.1.3.	Possuir as seguintes funcionalidades listadas anteriormente neste documento: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Filtro de Conteúdo Web, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização Wan, DLP – Data Leak Prevention, Controladora Wireless, Virtualização e Controle de Endpoints	
1.1.4.	Suportar a tecnologia SD-WAN, sem a necessidade de equipamento ou software extra	
1.1.5.	Cada equipamento deve possuir Fonte de alimentação com chaveamento automático 110/240 V – 50-60Hz. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos	
1.1.6.	Firewall com capacidade de processamento de 9 Gbps	

1.1.7.	IPS com capacidade de processamento de 10.8Gbps	
1.1.8.	Suportar pelo menos 500 usuários ativos na rede com todas as funcionalidades solicitadas nesta especificação habilitadas e funcionais;	
1.1.9.	VPN com capacidade de pelo menos 50 Gbps de tráfego IPSec;	
1.1.10.	VPN SSL com capacidade de pelo menos 3.5Gbps de tráfego;	
1.1.11.	Suporte a 6 milhões de sessões simultâneas;	
1.1.12.	Permitir a criação de 250 VLANS no padrão IEEE 802.1q	
1.1.13.	Devem ser licenciados para suportar pelo menos 3000 usuários de VPN SSL	
1.1.14.	Suporte a pelo menos 400.000 novas sessões por segundo;	
1.1.15.	Suporte a pelo menos 2000 túneis de VPN Site-Site;	
1.1.16.	Suporte a pelo menos 10.000 túneis de VPN Client-Site;	
1.1.17.	Possuir ao menos 14 interfaces 1GbE RJ45;	
1.1.18.	Possuir ao menos 4 interfaces 1GE/10GE SFP+.	
1.1.19.	Possuir porta USB para conexão de modem 3G/4G	
1.1.20.	Possuir ao menos 480GB SSD de disco	
1.1.21.	Possuir licença para número ilimitado de usuários e endereços IP	
1.1.22.	Possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de UTM pelo período de 12 meses	
1.1.23.	Deve ser capaz de gerenciar, via funcionalidade de controladora wireless, ao menos 512 Pontos de Acesso sem fio	

1.1.24.	Deve estar licenciado para permitir número ilimitado de estações de rede e usuários	
1.1.25.	Incluir licença para a funcionalidade de VPN SSL	
1.1.26.	Incluir licença para atualização de vacina de antivírus/anti-spyware	
1.1.27.	Incluir licença de atualização para filtro de conteúdo web	
1.1.28.	Incluir licença de atualização do IPS e da lista de aplicações detectadas	
1.1.29.	Fornecer documentação técnica, bem como manual de utilização, em inglês ou português do Brasil	
1.1.30.	Possuir integração com Servidores de Autenticação RADIUS, LDAP e Microsoft Active Directory.	
1.1.31.	Possuir integração com tokens para autenticação de dois fatores	
1.1.32.	Suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS	
1.1.33.	Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet).	
1.1.34.	Possuir a funcionalidade de tradução de endereços estáticos – NAT *(Network Address Translation)*, um para um, N-para-um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT	
1.1.35.	Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana	
1.1.36.	Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br	
1.1.37.	Possuir a funcionalidade de fazer tradução de endereços dinâmicos,	

	muitos para um, PAT.	
1.1.38.	Suporte a roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4	
1.1.39.	Possuir funcionalidades de DHCP usuário, Servidor e Relay.	
1.1.40.	Suportar aplicações multimídia como: H.323, SIP.	
1.1.41.	Tecnologia de firewall do tipo Statefull	
1.1.42.	Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego	
1.1.43.	Deve suportar PBR - Policy Based Routing	
1.1.44.	Permitir a criação de VLANS no padrão IEEE 802.1q	
1.1.45.	Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando)	
1.1.46.	Permitir filtro de pacotes sem controle de estado “stateless” para verificação em camada 2.	
1.1.47.	Permitir forwarding de camada 2 para protocolos não IP.	
1.1.48.	Suportar forwarding multicast.	
1.1.49.	Suportar roteamento multicast PIM Sparse Mode e Dense Mode	
1.1.50.	Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP	
1.1.51.	Permitir o agrupamento de serviços	
1.1.52.	Permitir o filtro de pacotes sem a utilização de NAT	
1.1.53.	Permitir a abertura de novas portas por fluxo de dados para serviços	

	que requerem portas dinâmicas.	
1.1.54.	Possuir mecanismo de anti-spoofing	
1.1.55.	Permitir criação de regras definidas pelo usuário	
1.1.56.	Permitir o serviço de autenticação para tráfego HTTP e FTP	
1.1.57.	Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC gerando maior controle dos endereços internos e impedindo o IP spoofing	
1.1.58.	Possuir a funcionalidade de balanceamento e contingência de links	
1.1.59.	Suporte a sFlow	
1.1.60.	O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.	
1.1.61.	Deve ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como por exemplo tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows	
1.1.62.	Deve ter a capacidade de criar e aplicar políticas de reputação de CONTRATANTE para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades web em categorias de risco, proteção de aplicação, locais geográficos que os usuários estão tentando se comunicar	
1.1.63.	Permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS	

1.1.64.	Permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação	
1.1.65.	Suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP	
1.1.66.	Permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou vlan-tagged	
1.1.67.	Possuir interface USB que permita a adição de modem 3G/4G	
1.1.68.	Possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS	
1.1.69.	Suportar SIP/H.323/SCCP NAT Traversal	
1.1.70.	Permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras	
1.1.71.	Possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha	
1.2.	Funcionalidade de Traffic Shaping e Priorização	
1.2.1.	Capacidade de suportar configurações como: Max Bandwidth, Guaranteed Bandwidth, DSCP;	
1.2.2.	Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (*inbound/outbound*) através da classificação dos pacotes (*Shaping*), criação de filas de prioridade, gerência de congestionamento e QoS.	
1.2.3.	Permitir modificação de valores DSCP para o *DiffServ*	

1.2.4.	Permitir priorização de tráfego e suportar TOS	
1.2.5.	Limitar individualmente a banda utilizada por programas tais como peer-to-peer, streaming, chat, VoIP, web, etc.	
1.2.6.	Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados	
1.2.7.	Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP	
1.2.8.	Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP	
1.2.9.	Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação	
1.2.10.	Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino	
1.2.11.	Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino	
1.2.12.	Deve ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como por exemplo tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows	
1.3.	Funcionalidade de Antivírus	
1.3.1.	Possuir funções de Antivírus e Anti-spyware	
1.3.2.	Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, SMB e FTP	

1.3.3.	Possuir verificação de vírus para aplicativos de mensagens instantâneas (AIM, MSN, Yahoo Messenger, ICQ)	
1.3.4.	Permitir o bloqueio de malwares (adware, spyware, *hijackers*, *keyloggers*, etc.)	
1.3.5.	Possuir proteção contra conexões a servidores Botnet	
1.3.6.	Permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipo de arquivo.	
1.3.7.	Permitir o bloqueio de download de arquivos por tamanho	
1.3.8.	Possuir o modo “Inspection mode”: Flow-based e Proxy.	
1.3.9.	Possuir a tecnologia “detect virus”: Block e Monitor.	
1.3.10.	Possuir capacidade de enviar arquivos para “Sandbox Cloud” para inspeção de conteúdo.	
1.3.11.	Detect Connections to Botnet C&C Servers	
1.3.12.	Deve ter a capacidade de permitir a criação de perfis de antivírus específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como por exemplo tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows	
1.4.	Funcionalidade de Anti-spam	
1.4.1.	Possuir verificação na funcionalidade de anti-spam da verificação do cabeçalho SMTP do tipo *MIME*	
1.4.2.	Possuir filtragem de e-mail por palavras chaves	
1.4.3.	Permitir adicionar rótulo ao assunto da mensagem quando classificado como *SPAM*	
1.4.4.	Possuir para a funcionalidade de Anti-Spam o recurso de RBL	

1.4.5.	Permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico	
1.4.6.	Deve ter a capacidade de permitir a criação de perfis de antispam específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como por exemplo tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows	
1.5.	Funcionalidade de Filtro de conteúdo Web	
1.5.1.	Possuir solução de filtro de conteúdo web integrado a solução de segurança	
1.5.2.	Possuir pelo menos 70 categorias para classificação de sites web	
1.5.3.	Possuir base mínima contendo, 100 milhões de *sites* internet web já registrados e classificados	
1.5.4.	Possuir a funcionalidade de cota de tempo de utilização por categoria	
1.5.5.	Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como: Proxy Anônimo Webmail Instituições de Saúde Notícias Abuso Infantil Abuso de Droga Evitação de Procuração	

	Grupos Extremistas Hacking Ilegal ou não-ético Plágio Racismo e Ódio Violência Explícita Armas (vendas) Crenças Alternativas Educação Sexual Esporte de Caça e Jogos de Guerra Jogo Lingerie e Traje de Banho Maconha Namorar Nudez e Risque Organizações de Advocacia Outros Materiais para Adultos Pornografia Tabaco Álcool Compartilhamento de arquivos Peer-to-peer (P2P)	

	Downloads de Freeware e Software Mídia no formato de Streaming Rádio de Internet e TV Telefonia de Internet Spam URLs Spyware e Malware Phishing	
1.5.6.	Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários	
1.5.7.	Permitir a criação de pelo menos 5 (cinco) categorias personalizadas	
1.5.8.	Permitir a re-classificação de *sites* web, tanto por URL quanto por endereço IP	
1.5.9.	Prover termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado	
1.5.10.	Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.	
1.5.11.	Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory	
1.5.12.	Possuir integração com tokens para autenticação de dois fatores	
1.5.13.	Exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança	

1.5.14.	Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em *applets* Java, *cookies*, activeX através de: base de URL própria atualizável.	
1.5.15.	Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual	
1.5.16.	Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra	
1.5.17.	Deverá permitir o bloqueio de URLs inválidas cujo o campo CN do certificado SSL não contém um domínio válido	
1.5.18.	Filtro de conteúdo baseado em categorias em tempo real	
1.5.19.	Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web	
1.5.20.	Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP	
1.5.21.	Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem	
1.5.22.	Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem	
1.5.23.	Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP	
1.5.24.	Deverá permitir o bloqueio de redirecionamento HTTP	
1.5.25.	Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Vídeo e URLs originadas de Spam	

1.5.26.	Possuir Proxy Explícito e Transparente	
1.5.27.	Implementar roteamento WCCP e ICAP	
1.5.28.	Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra	
1.5.29.	Deve ter a capacidade de permitir a criação de perfis de filtragem web específicos para tipos de dispositivos identificados automáticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como por exemplo tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows	
1.5.30.	O Firewall Appliance UTM precisa possuir tecnologias como: Block Invalid URLs, Allow Websites When a Rating Error Occurs, Block HTTP Redirects by Rating, Restrict Google Account Usage to Specific Domains, Web resume Download Block, Provide Details for Blocked HTTP 4xx and 5xx Errors.	
1.5.31.	Inspection Mode: Proxy, Flow-base, DNS	
1.6.	Funcionalidade de Detecção de Intrusão	
1.6.1.	Permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.	
1.6.2.	Possui base de assinaturas de IPS com pelo menos 3500 ameaças conhecidas.	
1.6.3.	O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes.	
1.6.4.	Deverá permitir funcionar em modo transparente, sniffer e router	
1.6.5.	Possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente	

1.6.6.	Deverá permitir a criação de padrões de ataque manualmente	
1.6.7.	O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança.	
1.6.8.	Possuir capacidade de remontagem de pacotes para identificação de ataques	
1.6.9.	Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;	
1.6.10.	Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;	
1.6.11.	Deve ter a capacidade de permitir a criação de perfis de inspeção específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como por exemplo tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.	
1.6.12.	Mecanismos de detecção/proteção de ataques	
1.6.13.	Reconhecimento de padrões	
1.6.14.	Análise de protocolos	
1.6.15.	Detecção de anomalias	
1.6.16.	Detecção de ataques de RPC (Remote procedure call)	
1.6.17.	Proteção contra ataques de Windows ou NetBios	
1.6.18.	Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol)	

1.6.19.	Proteção contra ataques DNS (Domain Name System)	
1.6.20.	Proteção contra ataques a FTP, SSH , Telnet e rlogin	
1.6.21.	Proteção contra ataques de ICMP (Internet Control Message Protocol).	
1.6.22.	Métodos de notificação de detecção de ataques	
1.6.23.	Alarmes na console de administração.	
1.6.24.	Alertas via correio eletrônico.	
1.6.25.	Monitoração do comportamento do appliance mediante SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.	
1.6.26.	Capacidade de resposta/logs ativa a ataques	
1.6.27.	Terminação de sessões via TCP resets.	
1.6.28.	Armazenamento de logs de sessões	
1.6.29.	Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos	
1.6.30.	O Sistema de detecção de Intrusos deverá mitigar os efeitos dos ataques de negação de serviços.	
1.6.31.	Deverá permitir a criação de assinaturas personalizadas.	
1.6.32.	Possuir filtros de ataques por anomalias	
1.6.33.	Permitir filtros de anomalias de tráfego estatístico de: *flooding*, *scan*, source e *destinationsessionlimit*	
1.6.34.	Permitir filtros de anomalias de protocolos	
1.6.35.	Suportar reconhecimento de ataques de DoS, *reconnaissance*,	

	exploits e *evasion*	
1.6.36.	Suportar verificação de ataque nas camada de aplicação	
1.6.37.	Suportar verificação de tráfego em tempo real, via aceleração de hardware	
1.6.38.	Possuir as seguintes estratégias de bloqueio: *pass*, *drop*, *reset*,	
1.7.	Funcionalidade de VPN	
1.7.1.	Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES.	
1.7.2.	Suporte a certificados PKI X.509 para construção de VPNs	
1.7.3.	Possuir suporte a VPNs IPSeC site-to-site, VPNs IPSec client-to-site.	
1.7.4.	Possuir suporte a VPN SSL.	
1.7.5.	Possuir capacidade de realizar SSL VPNs utilizando certificados digitais	
1.7.6.	A VPN SSL deve possibilitar o acesso a toda infra-estrutura de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java.	
1.7.7.	Possuir hardware acelerador criptográfico para incrementar o desempenho da VPN.	
1.7.8.	A VPN SSL deverá suportar CONTRATANTE para plataforma Windows, Linux e Mac OS X	
1.7.9.	Deve permitir a arquitetura de *vpn hub and spoke*	
1.7.10.	Suporte a VPN do tipo PPTP, L2TP	
1.7.11.	Suporte a inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) e mediante	

	arquivos.	
1.8.	Funcionalidade de Controle de Aplicações	
1.8.1.	Deverá reconhecer no mínimo 2000 aplicações;	
1.8.2.	Deverá possuir pelo menos 10 categorias para classificação de aplicações;	
1.8.3.	Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como: Botnet Business Cloud.IT Collaboration Email Game General.Interest Network.Service P2P Proxy Remote.Access Social.Media Storage.Backup Update Video/Audio	

	VoIP Industrial Web.Others	
1.8.4.	Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários	
1.8.5.	Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-a apenas pelo comportamento de tráfego da mesma	
1.8.6.	Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;	
1.8.7.	Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;	
1.8.8.	Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;	
1.8.9.	Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;	
1.8.10.	Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;	
1.8.11.	Possuir integração com tokens para autenticação de dois fatores	
1.8.12.	Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;	
1.8.13.	Deverá permitir a inspeção/bloqueio de códigos maliciosos para no mínimo as seguintes categorias: Instant Messaging; Transferência de arquivos	

1.8.14.	Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações	
1.8.15.	Deverá permitir criação de padrões de aplicação manualmente	
1.8.16.	Deve ter a capacidade de permitir a criação de perfis de controle de aplicações específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como por exemplo tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows	
1.8.17.	Deep Inspection of Cloud Applications	
1.8.18.	Replacement Messages for HTTP-based Applications	
1.9.	Funcionalidade de Cache e Otimização WAN	
1.9.1.	Deverá implementar otimização do tráfego entre dois equipamentos	
1.9.2.	Deverá possuir capacidade de armazenamento local	
1.9.3.	Deverá implementar, no mínimo, as seguintes técnicas de otimização: Otimização de protocolos; Byte caching; Web caching.	
1.9.4.	Deverá otimizar no mínimo os seguintes protocolos: CIFS, FTP, HTTP, MAPI e TCP.	
1.9.5.	Deverá permitir criptografar a comunicação entre os appliances envolvidos na otimização do tráfego através de protocolos IPSEC ou SSH	
1.9.6.	Deverá implementar alta disponibilidade no mínimo ativo-passivo	

1.9.7.	Deverá possuir Cache de páginas web (HTTP)	
1.9.8.	Deverá apresentar gráfico ou relatório que indique a quantidade de tráfego que está sendo otimizada, em porcentagem ou bytes	
1.10.	Funcionalidade de DLP (Data Leak Prevention)	
1.10.1.	O sistema de DLP (Proteção contra Vazamento de Informações) de gateway deve funcionar de maneira que consiga parar que dados sensíveis saiam da rede e também deve funcionar de modo que previna que dados não requisitados entrem na sua rede.	
1.10.2.	O sistema de DLP deverá inspecionar no mínimo os tráfegos de Email, HTTP, NNTP e de Mensageiros Instantâneos.	
1.10.3.	Sobre o tráfego de email, deverá inspecionar no mínimo os protocolos SMTP, POP3 e IMAP;	
1.10.4.	Sobre o tráfego de Mensageiros instantâneos, deverá inspecionar no mínimo os protocolos AIM, ICQ, MSN e Yahoo!.	
1.10.5.	Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;	
1.10.6.	Deverá fazer a varredura no conteúdo de um Cookie HTTP buscando por determinado texto.	
1.10.7.	Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário.	
1.10.8.	Deverá verificar para aplicações do tipo email, se o anexo das mensagens de correio entrantes/saintes possuí um tamanho máximo especificado pelo administrador.	
1.10.9.	Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos.	
1.10.10.	Deverá tomar minimamente as ações de bloquear, banir usuário e quarentenar a interface sobre as regras que coincidirem com o tráfego esperado pela regra.	
1.10.11.	Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de Email, HTTP e Mensageiros Instantâneos.	
1.10.12.	Deverá permitir a composição de múltiplas regras de DLP formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.	
1.11.	Funcionalidade de Balanceamento de Carga	

1.11.1.	Permitir a criação de endereços IPs virtuais	
1.11.2.	Permitir balanceamento de carga entre pelo menos 4 servidores reais	
1.11.3.	Suportar balanceamento ao menos para os seguintes serviços: HTTP, HTTPS, TCP e UDP	
1.11.4.	Permitir balanceamento ao menos com os seguintes métodos: hash do endereço IP de origem, Round Robin, Weighted, First alive e HTTP host	
1.11.5.	Permitir persistência de sessão por cookie HTTP ou SSL session ID	
1.11.6.	Permitir que seja mantido o IP de origem	
1.11.7.	Suportar SSL offloading	
1.11.8.	Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam.	
1.11.9.	Permitir que o health check seja feito ao menos via icmp, TCP em porta configurável e HTTP em URL configurável	
1.12.	Funcionalidade de Virtualização	
1.12.1.	Deve suportar a criação de ao menos 10 instâncias virtuais no mesmo hardware	
1.12.2.	Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais	
1.12.3.	Deve permitir a criação de um administrador global que tenha acesso à todas as configurações das instâncias virtuais criadas	
1.13.	Funcionalidade de Controle de Endpoint	
1.13.1.	Deve possuir software endpoint para instalação em máquinas de usuários e que sejam gerenciados de forma centralizada	
1.13.2.	Deve possuir antivírus no endpoint com capacidade de analisar arquivos locais e copiados da rede	
1.13.3.	Deve possuir filtro de conteúdo web no endpoint capaz de controlar o acesso a sites na web baseado nas mesmas categorias existentes no filtro de conteúdo da rede	

1.13.4.	Deve possuir usuários de VPN IPSec no endpoint	
1.13.5.	Deve possuir capacidade de identificar aplicações instaladas nas máquinas dos usuários	
1.13.6.	O endpoint deve enviar os logs de bloqueio ocorridos à plataforma de gerência	
1.13.7.	Deve permitir integração com o firewall de rede de forma que seja possível bloquear o acesso aos endpoints que não estejam atualizados	
1.13.8.	Deve permitir integração com o firewall de rede de forma que seja possível bloquear o acesso aos usuários que não possuam endpoints instalados	
1.13.9.	Deve permitir integração com o firewall de rede de forma que seja possível bloquear o acesso aos usuários que possuam determinadas aplicações instaladas tais como usuários P2P, proxies anônimos, malwares, entre outros.	
1.14.	Funcionalidade de Controladora Wireless e WiFi	
1.14.1.	Ser capaz de gerenciar centralizadamente outros Pontos de Acesso do mesmo fabricante	
1.14.2.	Suporte ao serviço de servidor DHCP por SSID para prover endereçamento IP automático para os usuários wireless	
1.14.3.	Suporte a monitoração e supressão de Ponto de Acesso indevido	
1.14.4.	Prover autenticação para a rede wireless através de bases externas como LDAP, RADIUS ou TACACS+	
1.14.5.	Deverá permitir a visualização dos usuários conectados	
1.14.6.	Deverá prover suporte a Fast Roaming	
1.14.7.	Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF	
1.14.8.	Possuir Captive Portal por SSID	
1.14.9.	Permitir configurar o bloqueio de tráfego entre SSIDs	
1.14.10.	Deverá suportar Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de AES e/ou TKIP.	
1.14.11.	Deve suportar os seguintes métodos de autenticação EAP:	

	EAP-TLS, LEAP, EAP-TTLS/MSCHAPv2, PEAPv0/MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST, EAP-TTLS	
1.14.12.	Deverá suportar 802.1x através de RADIUS	
1.14.13.	Deverá suportar filtro baseado em endereço MAC por SSID	
1.14.14.	Permitir configurar parâmetros de rádio como: banda e canal	
1.14.15.	Possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast	
1.14.16.	Possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs e usuários ofensores	
1.14.17.	Possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);	
1.14.18.	Possuir WIDS com ao menos os seguintes perfis: - Unauthorized Device Detection - Rogue/Interfering AP Detection - Ad-hoc Network Detection and Containment - Wireless Bridge Detection - Misconfigured AP Detection - Weak WEP Detection - Multi Tenancy Protection - MAC OUI Checking	

1.14.19.	Permitir o uso de voz e dados sobre um mesmo SSID;	
1.14.20.	A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário	
1.14.21.	Possuir controle baseado em política de firewall para acesso entre as Wlans	
1.14.22.	Deverá permitir a criação de políticas de traffic shaping	
1.14.23.	Deverá permitir a criação de políticas de firewall baseadas em horário	
1.14.24.	Deverá permitir NAT nas políticas de firewall	
1.14.25.	Possibilitar definir número de usuários por SSID	
1.14.26.	Permitir e/ou bloquear o tráfego entre SSIDs	
1.14.27.	Possuir mecanismo de criação automática de usuários visitantes e senhas auto-geradas e/ou manual, que possam ser enviadas por email ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha	
1.14.28.	A comunicação entre o Access Point e a controladora wireless deve poder ser efetuada de forma criptografada	
1.14.29.	Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois access points gerenciados	
1.14.30.	Possuir mecanismo de balanceamento de tráfego/usuários entre Access Points	
1.14.31.	Possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou radios	
1.14.32.	Toda a configuração do Ponto de Acesso deve ser executada através da Controladora Wireless	

1.14.33.	Deve permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica	
1.14.34.	Possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que radio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído	
1.14.35.	A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a controladora	
1.14.36.	Possuir controle baseado em política de firewall para acesso entre as Wlans cujo tráfego seja tunelado até a controladora	
1.14.37.	Deverá permitir a criação de políticas de firewall baseadas em horário	
1.14.38.	Deverá permitir NAT nas políticas de firewall	
1.14.39.	Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a controladora	
1.14.40.	Deve permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a controladora	
1.14.41.	Deve permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a controladora	
1.14.42.	Deve permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a controladora	
1.14.43.	Deve permitir aplicar políticas controle antispam para todas as redes cujo tráfego seja tunelado até a controladora	

1.14.44.	Deve permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, Streaming de áudio e vídeo, Jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado à controladora.	
1.14.45.	Possuir certificação WiFi Alliance	
1.15.	Certificações necessárias	
1.15.1.	Certificação ICSA para Firewall	
1.15.2.	Certificação ICSA para Antivírus	
1.15.3.	Certificação ICSA para VPN SSL	
1.15.4.	Certificação ICSA para VPN IPSec	
1.15.5.	Certificação ICSA para IPS	
1.15.6.	O equipamento de firewall e/ou IPS deve ter sido aprovado nos testes da NSS Labs e deve estar na lista de recomendados.	
1.16.	Outras funcionalidades gerais	
1.16.1.	Capacidade de suportar token virtual (Instalado em smartphone ou tablete) ou token físico.	
1.16.2.	Visualizador em tempo real com no mínimo: Visualização das origens de acesso, aplicações acessadas, destinos e sessões ativas.	
1.16.3.	Monitor de política de firewall	
1.16.4.	Monitor de controle de banda “Traffic Shaper”	