MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DE LAVRAS

DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

COORDENADORIA DE AQUISIÇÕES DE TECNOLOGIA DA INFORMAÇÃO

DIRETORIA DE LICITAÇÕES, CONTRATOS E CONVÊNIOS

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

Processo Administrativo nº 23090.003445/2022-07

Atualização da Solução de Firewall

Lavras, agosto de 2022

Histórico de Revisões

Data	Versão	Descrição	Autor
28/06/2022	1.0	Finalização da primeira versão do documento	Plínio Torres
02/08/2022	1.1	Finalização da segunda versão do documento, após revisão	Equipe de Planejamento da Contratação

Sumário

TERMO DE REFERÊNCIA

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1 – OBJETO DA CONTRATAÇÃO

1.1 Contratação de empresa especializada no fornecimento de soluções de segurança da informação para atualização do Firewall SonicWall Supermassive 9600 para o modelo NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade, por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses, e aquisição da licença SonicWall Analytics Software, pelo período de 24 meses.

2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1 Bens e serviços que compõem a solução

Id.	Descrição do Bem ou Serviço	Código CATMAT / CATSER	Quantidade	Métrica ou Unidade
1	Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade, por 24 meses, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	484747	1	Unidade
2	Aquisição da licença SonicWall Analytics Software, pelo período de 24 meses.	27502	1	Unidade

2.1.1. A descrição da solução de TIC encontra-se pormenorizada nos Estudos Técnicos Preliminares (ETP), apêndice deste Termo de Referência.

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. A contratação visa maior proteção de acessos à rede LAN (interna) e WAN (externa), no intuito de garantir a confidencialidade, integridade e disponibilidade dos dados transmitidos ou armazenados na infraestrutura de rede da Universidade Federal de Lavras - UFLA, bem como gerenciar os riscos e ameaças aos ativos de tecnologia da informação dessa instituição.

3.1.2. A solução de firewall não é uma opção de segurança da informação, mas uma necessidade obrigatória para proteger os ativos de tecnologia da informação contra ataques cibernéticos e viabilizar a continuidade dos processos de negócios institucionais que usam ativos de tecnologia da informação. Dessa forma, a solução de firewall busca garantir uma infraestrutura física apropriada para as atividades acadêmicas e administrativas na UFLA, bem como salvaguardar os ativos de tecnologia da informação e segurança da informação.

3.1.3 Além disso, é necessário aprimorar os conhecimentos técnicos da equipe de segurança computacional e segurança da informação em relação à administração da solução de firewall contratada, pois é necessário atualizar os profissionais de tecnologia da informação da DGTI sobre as novas técnicas de administração da solução de firewall contratada, para uso racional do recurso e resposta rápida a incidentes de segurança da informação.

3.1.4. A justificativa e a contextualização da contratação encontram-se pormenorizadas nos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
Objetivo 1.3.4 do PDI 2021 - 2025 da UFLA	Manter a excelência no nível de Governança e Gestão de TI da UFLA
Objetivo 1.6.3 do PDI 2021 - 2025 da UFLA	Gerir a Segurança da Informação e Privacidade de Dados em conformidade com a legislação e boas práticas
Objetivo 11 da EGD 2020-2022	Garantia da segurança das plataformas de governo digital e de missão crítica
Objetivo 16 da EGD 2020-2022	Otimização das infraestruturas de tecnologia da informação

ALINHAMENTO AO PDTIC 2021-2025			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A.5.1	Conduzir estudo técnico sobre a aquisição da solução Planejar treinamento da tecnologia na organização	**M.5.1**	Conduzir processo de aquisição de Firewall

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
5869	Firewall

3.2.1. Entende-se que o objeto em questão não se trata de oferta digital de serviços públicos, sendo assim, não é necessário integração à Plataforma de Cidadania Digital, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016.

3.3. Estimativa da demanda

3.3.1. A Universidade Federal de Lavras disponibiliza uma infraestrutura de TI para cerca de 20.000 (vinte mil) usuários da comunidade acadêmica, sendo composta por alunos, professores e técnicos administrativos em educação.

3.3.2. Atualmente, possui a solução da SonicWall Supermassive 9600, que permite um nível de segurança na filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e transporte do modelo OSI, Filtro de Botnet, Gateway (Antivírus, Anti-Spyware, Prevenção de Intrusão) filtro de conteúdo, possibilidade de atualização de software e firmware, alta disponibilidade, gerenciamento centralizado das configurações, alertas e logs.

3.3.3. Outro fator que deve ser ressaltado é a ausência de mecanismos que permitam o monitoramento do tráfego. Nesse contexto, os gestores da rede não conseguem obter uma visão mais detalhada do tráfego a nível das aplicações que estão trafegando dados, qual o nível de risco do tráfego e se ele pode trazer ameaças para a rede. Esse tipo de informação é muito importante para prover uma rápida análise caso ocorra algum incidente e para a geração de relatórios sobre uso da banda, o que auxilia a diagnosticar de forma rápida e eficiente as causas de possíveis ataques cibernéticos ou lentidão na rede.

3.3.4.Para que isso não ocorra, faz-se necessária a renovação das licenças dos softwares internos do firewall nos seguintes quantitativos:

Descrição	Quantidade	Tempo da licença
Contratação de solução de Firewall, implantação, garantia e suporte técnico.	1	2 anos
Contratação de software de gerência de Logs e relatórios centralizados, implantação, garantia e suporte técnico.	1	2 anos

3.3.5. Todavia, com o crescimento, na UFLA, da infraestrutura computacional e as novas demandas surgindo devido às novas tecnologias emergentes, o atual firewall está quase atingindo sua capacidade máxima de gerir as informações na rede da UFLA.

3.4. Parcelamento da Solução de TIC

3.4.1. Devido à interdependência e acoplamento técnico entre os itens 1 e 2 da solução de firewall, não é possível o parcelamento da solução, devendo ser licitada de forma agrupada.

3.4.2. Esse agrupamento se justifica devido à necessidade de serem fornecidos pelo mesmo licitante, uma vez que os itens 1 e 2 são interdependentes, de forma que o item 2, para seu correto funcionamento e operação, necessita de informações contidas no item 1.

3.4.3. Assim, segregar em itens poderia implicar em interrupção do correto funcionamento da solução de firewall, trazendo prejuízos à segurança da informação e aos ativos de tecnologia da informação na UFLA.

3.5. Resultados e Benefícios a Serem Alcançados

3.5.1. Aumentar a disponibilidade dos sistemas institucionais por meio de uma melhor e mais segura infraestrutura de redes, melhorando a continuidade dos processos de negócio.

3.5.2. Aumentar a velocidade de acesso à Internet, para usuários institucionais, aproveitando toda a largura de banda disponibilizada para a Universidade.

3.5.3. Melhorar a capacidade de bloqueio de ataques e conexões estranhas aos serviços de tecnologia da informação da UFLA, tendo uma maior e mais precisa visibilidade do tráfego que passa pelo firewall, podendo analisar melhor possíveis ameaças, identificando problemas na rede e salvaguardando seus ativos de tecnologia da informação, criando um isolamento seguro dos serviços de tecnologia.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. O firewall institucional deverá:

4.1.1.1. Regular o tráfego de dados entre rede UFLA e a Internet, bem como impedir a transmissão e recepção de informações a partir de acessos indevidos.

4.1.1.2. Atuar como ferramenta de prevenção contra possíveis ataques que venham explorar vulnerabilidades da rede e dos servidores.

4.1.2. Partindo-se de tais pressupostos, deverá garantir:

4.1.2.1. Alta disponibilidade da rede, através da proteção anti-malware, anti-spyware, antivírus, anti-bot, filtro de conteúdo e filtro de URL.

4.1.2.2. Controle de aplicações.

4.1.2.3. Inspeção de pacotes, relatórios, inspeção SSL, VPNs, QoS, autenticação de usuários e anti-DoS.

4.1.2.4. Segurança da rede de dados institucional, possibilitando a continuidade de atividades fundamentais para a Instituição.

4.2. Requisitos de Capacitação

4.2.1. A CONTRATADA deverá ter capacidade técnica para prestar serviços de consultoria para a CONTRATANTE, durante toda a vigência do contrato.

4.2.2. No momento da implantação e migração do SonicWall Supermassive 9600 para o NSA 5700, a equipe local da CONTRATADA deverá ser capacitada para operar, configurar, administrar e resolver problemas usuais, englobando tanto os componentes de hardware, quanto de software.

4.2.3. Deverá ser ofertado curso de capacitação do Firewall com conteúdo completo, pela CONTRATADA, com o mínimo de 20 horas de duração.

4.2.3.1 O conteúdo deve ser composto de, no mínimo, os seguintes tópicos: introdução, fundamentos do sistema operacional, dashboards, escalabilidade e confiabilidade, acesso seguro e controle de conteúdo, gerenciamento unificado de ameaças, configuração de regras de segurança, relatórios e solução de problemas.

4.2.4. O curso de capacitação deverá ser ministrado em um ambiente idêntico ao da administração do Firewall.

4.2.5. A disponibilização do curso de capacitação deverá ser remota, para até 8 pessoas indicadas pela CONTRATANTE.

4.2.6. Todas as informações ministradas no curso de capacitação deverão estar no material didático a ser entregue para a CONTRATANTE, em formato digital, onde deverá estar descrito de forma detalhada e procedural sobre como configurar os recursos da solução.

4.2.7. Os dias e horários do curso serão definidos em reunião a ser realizada entre a CONTRATANTE e a CONTRATADA, após a assinatura do contrato.

4.2.8. O curso de capacitação e as eventuais consultorias durante a vigência do contrato não terão custo adicional para a UFLA, estando seus valores incluídos na proposta apresentada pela licitante na sessão pública.

4.3. Requisitos Legais

4.3.1. A contratação de pessoa jurídica para fornecimento do objeto deste Termo de Referência tem amparo legal na Instrução Normativa nº 1, de 4 de abril de 2019 e alterações, na Lei nº 10.520, de 17 de julho de 2002, no Decreto nº 10.024, de 20 de setembro de 2019, no Decreto nº 7.746, de 5 de junho 2012, no Decreto nº 7.174, de 12 de maio de 2010, na Instrução Normativa nº 1, de 19 de janeiro de 2010, na Instrução Normativa nº 73, de 5 de agosto de 2020, na Lei Complementar nº 123, de 14 de dezembro de 2006, no Decreto nº 8.538, de 6 de outubro de 2015, aplicando-se, subsidiariamente, a Lei 8.666, de 21 de junho de 1993, bem como nas demais legislações específicas e pertinentes.

4.3.2. Os equipamentos devem possuir homologação da Anatel.

4.4. Requisitos de Manutenção

4.4.1. Garantia técnica evolutiva: fornecimento de novas versões e/ou releases corretivos de softwares, lançadas durante a vigência do contrato, mesmo em caso de mudança de designação do nome.

4.4.1.1. A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

4.4.1.1.1. Deverá, também, no que couber, implementar novas funcionalidades relativas aos equipamentos.

4.4.2. Garantia técnica corretiva: série de procedimentos executados para recolocar a solução em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários.

4.4.2.1. Durante a vigência do contrato, a CONTRATADA deverá prestar garantia técnica corretiva sempre que acionada pela CONTRATANTE.

4.4.2.2. O prazo para a CONTRATADA realizar o atendimento dos chamados de garantia técnica corretiva será de 12 horas úteis, após encaminhados pela CONTRATANTE.

4.4.3. Garantia técnica assistencial: atividades que incluem, mas não se limitam à execução e

provimento de informação; assistência e orientação para: instalação, desinstalação, configuração, substituição e atualização de programas (software) e dispositivos físicos (hardware); aplicação de correções (patches) e atualizações de software; diagnósticos, avaliações e resolução de problemas; ajustes finos e customização da solução; esclarecimento acerca das características dos produtos e demais atividades.

4.4.3.1. Durante a vigência do contrato, a CONTRATADA deverá prestar garantia técnica assistencial sempre que acionada pela CONTRATANTE.

4.4.3.2. O prazo para a CONTRATADA realizar o atendimento dos chamados de garantia técnica assistencial será de 12 horas úteis, após encaminhados pela CONTRATANTE.

4.5. Requisitos Temporais

4.5.1. O prazo de entrega do equipamento deverá ser de até 60 (sessenta) dias, contados a partir do recebimento da Ordem de Fornecimento de Bens (OFB) pela CONTRATADA.

4.5.2. Após o recebimento do equipamento, o serviço de implantação, com a migração das regras e configurações para a nova solução, deverá ocorrer em até 30 (trinta) dias.

4.5.2.1. O serviço de instalação, configuração e migração será realizado de forma presencial e as diretrizes para sua realização serão definidas na reunião inicial, que ocorrerá em data a ser definida entre a CONTRATADA e a CONTRATANTE.

4.5.4. O serviço de suporte técnico (Service Desk) terá prazo iniciado apenas a partir da conclusão da implantação do serviço, ou seja, o prazo de 12 (doze) meses do serviço de suporte técnico iniciará apenas após a conclusão do serviço de implantação, da migração das regras e configurações para o pleno funcionamento da nova solução.

4.6. Requisitos de Segurança e Privacidade

4.6.1. A CONTRATADA deverá submeter-se aos procedimentos de segurança existentes da CONTRATANTE, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da CONTRATANTE.

4.6.2. A CONTRATADA deverá manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros, de que tomar conhecimento, em razão da execução do objeto, devendo orientar seus empregados nesse sentido também - conforme termo de compromisso e termo de ciência, previstos no item 6.4. deste Termo de Referência.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês.

4.7.2. Todos os contatos relativos à garantia ou para o gerenciamento de chamados e suporte técnico deverão ser realizados no idioma Português (Brasil).

4.7.2.1. A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob forma eletrônica, evitando-se a impressão de papel.

4.7.3. Em conformidade com a IN SLTI/MPOG nº 01/2010, a CONTRATADA deverá cumprir com os seguintes requisitos de sustentabilidade ambiental: o equipamento e seus componentes devem, sempre que possível, ser acondicionados em embalagem individual adequada, com o menor tamanho possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

4.7.4. O equipamento ofertado deve cumprir todos os critérios legais vigentes em relação à segurança, compatibilidade eletromagnética e eficiência energética.

4.7.5. O equipamento não poderá conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil polibromados (PBDEs).

4.8. Requisitos de Arquitetura Tecnológica

4.8.1. Requisitos Mínimos:

4.8.1.1. Deve apresentar desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 15 Gbps ou superior.

4.8.1.2. Deve apresentar desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 7 Gbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

4.8.1.3. Deve apresentar desempenho mínimo de 17 Gbps de IPS.

4.8.1.4. Deve possuir suporte mínimo de 5.000.000 conexões simultâneas/concorrentes no modo SPI.

4.8.1.5. Deve possuir suporte mínimo de 228.000 novas conexões por segundo.

4.8.1.6. Deve possuir armazenamento interno de no mínimo 128 GB e suportar expansão de armazenamento interno para até 256 Gb.

4.8.1.7. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

4.8.1.8. Deve possuir no mínimo 24 interfaces 1 GbE padrão RJ-45.

4.8.1.9. Deve possuir no minimo 6 interfaces 10 GbE SFP+.

4.8.1.10. Deve possuir 1 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

4.8.1.11. Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

4.8.1.12. Deve possuir no mínimo 2 interfaces 10G/5G/2.5G/1G - Cu Ports.

4.8.1.13. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 2.000 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 4.000 usuários simultâneos, com aquisição de licença complementar.

4.8.1.14. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1.500 usuários simultâneos, com aquisição de licença complementar.

4.8.1.15. Deve suportar 6.000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

4.8.1.16. Deve suportar, no mínimo, 15 Gbps de desempenho de VPN IPSEC.

4.8.1.17. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante.

4.8.1.18. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

4.8.1.19. O fornecimento dos produtos e seus licenciamentos devem ser entregues por meio de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado por meio do site do fabricante ou por meio de carta de reconhecimento ou documento similar assinado pelo representante legal do fabricante no Brasil.

4.8.1.20. O equipamento deverá ser homologado pela ANATEL.

4.8.1.21. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 24 (vinte e quatro) meses.

4.8.1.22. A garantia do hardware (item 1) deverá ser de 24 (vinte e quatro) meses.

4.8.2. Requisitos e Características Gerais:

4.8.2.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente FIREWALL.

4.8.2.1.1.Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques dia zero, filtro de URL, identificação de usuários e controle granular de permissões.

4.8.2.1.2.Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço.

4.8.2.2. Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

4.8.2.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

4.8.2.4. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

4.8.3. Requisitos e Características Diversos:

4.8.3.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P, entre outros, baseados nos endereços de origem e destino.

4.8.3.2. Deve implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.

4.8.3.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

4.8.3.5. Deve possuir proteção anti-spoofing.

4.8.3.6. Deve suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP.

4.8.3.7. Deve suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

4.8.3.8. Deve possuir suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

4.8.3.9. A solução deverá implementar tecnologia de SD-WAN (Software Defined WAN).

4.8.3.10. Deve possuir capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

4.8.3.10.1. O equipamento deve permitir escolhas de caminhos baseado em:

4.8.3.10.1.1. Latência.

4.8.3.10.1.2. Jitter.

4.8.3.10.1.3. Perda de pacotes.

4.8.3.11. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego, simultaneamente, por todos os links pertencentes a esse canal lógico.

4.8.3.12. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática, baseada nas políticas previamente aplicadas.

4.8.3.13. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

4.8.3.14. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

4.8.3.15. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

4.8.3.16. Deve implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

4.8.3.17. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

4.8.3.18. Deve suportar DHCP relay.

4.8.3.19. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

4.8.3.20. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, VLAN ou zona de segurança.

4.8.3.21. Possuir capacidade de inspecionar e bloquear, em tempo real, aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, Telegram, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

4.8.3.22. Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

4.8.3.23. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS, devidamente licenciados.

4.8.3.24. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

4.8.3.25. Detectar e bloquear a origem de portscans.

4.8.3.26. Deve permitir o bloqueio de ataques.

4.8.3.27. Deve permitir o bloqueio de exploits conhecidos.

4.8.3.28. O gateway Anti-Vírus deve suportar a análise de, pelo menos, os protocolos HTTP, FTP, IMAP, e SMTP.

4.8.3.29. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverão ser decriptografados de forma transparente à aplicação.

4.8.3.30. Deve implementar DSCP (Differentiated Services Code Points).

4.8.3.31. Deve possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

4.8.3.32. Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

4.8.3.33. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

4.8.3.34. Possuir suporte ao protocolo SNMP versões 2 e 3.

4.8.3.35. Possuir suporte a log via syslog.

4.8.3.36. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

4.8.3.37. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente desse certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

4.8.3.38. Visando estabelecer confiabilidade e qualidades da solução de firewall de nova geração o fabricante da solução deverá ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2020 ou mais recentes.

4.8.3.39. Deve reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

4.8.3.40. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

4.8.3.41. Deve permitir controle, inspeção e de-criptografia de SSL/TLS por política para

tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a, no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.

4.8.4. Requisitos de VPN:

4.8.4.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

4.8.4.2. Suportar algoritmos de criptografia 3DES, AES 128 e AES 256.

4.8.4.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

4.8.4.4. Suportar Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits).

4.8.4.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

4.8.4.6. Deve permitir autenticação via túneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

4.8.4.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

4.8.4.8. A solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e/ou dinâmico.

4.8.4.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

4.8.4.10. A solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IPs públicos dinâmicos.

4.8.4.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

4.8.4.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora desse tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

4.8.4.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar por meio da Internet.

4.8.4.14. Deve permitir implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pre-Shared Key, certificados digitais e XAUTH client authentication.

4.8.4.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

4.8.4.16. Deve possuir interoperabilidade, no mínimo, com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

4.8.5. Requisitos de Alta Disponibilidade:

4.8.5.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

4.8.5.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover.

4.8.5.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

4.8.5.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

4.8.5.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

4.8.5.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

4.8.5.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

4.8.5.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

4.8.6. Requisitos de Controle de Ameaças:

4.8.6.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

4.8.6.2. A solução de Anti-Vírus integrada deve ter capacidade de analisar arquivos maiores que 1Gb.

4.8.6.3. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliances por meio de assinaturas.

4.8.6.4. Deve permitir implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

4.8.6.5. Deve permitir implementar funcionalidade de detecção e bloqueio de “call-backs”.

4.8.6.6. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

4.8.6.7. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de

endereço IP.

4.8.6.8. Deve permitir implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

4.8.6.9. Deve permitir implementar interface CLI segura por meio do protocolo SSH.

4.8.6.10. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

4.8.6.11. A solução deve permitir criar regras de exceção de acordo com a proteção.

4.8.6.12. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

4.8.6.13. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

4.8.6.14. A solução deve ser capaz de proteger contra ataques a DNS.

4.8.6.15. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

4.8.6.16. A solução deve ser capaz de prevenir acesso a websites maliciosos.

4.8.6.17. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

4.8.6.18. A solução deverá receber atualizações de um serviço baseado em cloud.

4.8.6.19. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

4.8.6.20. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

4.8.6.21 A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para essa mesma finalidade

4.8.6.22 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas.

4.8.6.23 A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações.

4.8.6.24 A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho.

4.8.6.25 A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitado neste Termo de Referência.

4.8.6.26 Possuir capacidade de remontagem de pacotes para identificação de ataques.

4.8.6.27 O mecanismo de inspeção deve receber e implementar em tempo real atualizações

para os ataques emergentes sem a necessidade de reiniciar o appliance.

4.8.6.28 Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante.

4.8.6.29 A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada.

4.8.6.30 As regras de exceção devem possuir: origem, destino e serviço.

4.8.6.31 A solução deve ser capaz de inspecionar tráfego HTTPS.

4.8.6.32 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.

4.8.6.33 Deve permitir detecção de anomalias.

4.8.6.34 A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção).

4.8.6.35 O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS.

4.8.6.36 O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas, sem a necessidade de reiniciar o appliance.

4.8.6.37 Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino.

4.8.6.38 A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP.

4.8.6.39 Deve incluir proteção contra worms.

4.8.6.40 Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao longo do tempo, dispondo o sumário quantitativo das ameaças analisadas.

4.8.6.41 A solução deve possuir esquema de atualização de assinaturas através de um click.

4.8.6.42 Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução.

4.8.6.43 A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS).

4.8.6.44 A solução deverá ser capaz de inspecionar e proteger apenas hosts internos.

4.8.6.45 A solução deverá possuir proteções para sistemas SCADA.

4.8.6.46 A solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

4.8.7. Requisitos de Proteção contra Ataques Avançados :

4.8.7.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

4.8.7.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

4.8.7.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

4.8.7.4. Deve identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

4.8.7.5. Deve implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

4.8.7.6. Deve implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

4.8.7.7. Deve implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

4.8.7.8. Deve conter ameaças de dia-zero, permitindo ao usuário final o recebimento dos arquivos livres de malware.

4.8.7.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

4.8.7.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliances por meio de assinaturas.

4.8.7.11. Deve implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

4.8.7.12. Deve implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego.

4.8.7.13. Deve conter ameaças avançadas de dia zero.

4.8.7.14. Toda análise deverá ser realizada de forma automatizada, sem a necessidade de criação de regras específicas e/ou interação de um operador.

4.8.7.15. Deve implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.

4.8.7.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

4.8.7.17. Deve suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

4.8.7.18. Deve implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

4.8.7.19. Deve possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP , IMAP e CIFS.

4.8.7.20. Deve mitigar ameaças de dia zero de forma transparente para o usuário final.

4.8.7.21. Deve mitigar ameaças de dia zero por meio de tecnologias de emulação e código de registro.

4.8.7.22. Deve implementar mecanismo de pesquisa por diferentes intervalos de tempo.

4.8.7.23. Deve mitigar ameaças de dia zero via tráfego de internet.

4.8.7.24. Deve permitir a contenção de ameaças de dia-zero sem a alteração da infra-estrutura de segurança.

4.8.7.25. Deve mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

4.8.7.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

4.8.7.27. Deve mitigar ameaças de dia-zero antes da execução e evasão de qualquer código malicioso.

4.8.7.28. Deve conter e mitigar exploits avançados.

4.8.7.29. A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus 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).

4.8.7.30. Deve possuir suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

4.8.8. Requisitos de Filtro de Conteúdo Web:

4.8.8.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.

4.8.8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local.

4.8.8.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real por meio da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período

de vigência da garantia e do contrato de manutenção e suporte técnico.

4.8.8.4. Permitir a customização de página de bloqueio.

4.8.8.5. Deve permitir controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

4.8.8.6. Deve permitir submissão de novos sites para categorização.

4.8.8.7. Permitir a classificação dinâmica de sites web, URLs e domínios.

4.8.8.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

4.8.8.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

4.8.8.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

4.8.9. Requisitos e Características de Autenticação:

4.8.9.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

4.8.9.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

4.8.9.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

4.8.9.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

4.8.9.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

4.8.9.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que, antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW.

4.8.9.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

4.8.9.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

4.8.9.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar por meio da Internet.

4.8.10. Requisitos e Características de Administração:

4.8.10.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

4.8.10.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

4.8.10.3. Possuir mecanismo para realizar remotamente, por meio de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

4.8.10.4. Possuir mecanismo para agendamento e realização das cópias de segurança (backups) de configuração.

4.8.10.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

4.8.10.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo, com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

4.8.10.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma dessas sessões ou conexões.

4.8.10.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

4.8.10.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

4.8.10.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.

4.8.10.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando esses recursos, informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

4.8.10.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real, estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

4.8.10.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão desse relatório em formato PDF.

4.8.10.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

4.8.10.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

4.8.10.16. Possibilitar a geração de, pelo menos, os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

4.8.10.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

4.8.10.18. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

4.8.10.19. A solução deve possuir mecanismo de gerenciamento por meio de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

4.8.10.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

4.8.10.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

4.8.10.22. O aplicativo móvel deve permitir a visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

4.8.10.23. O aplicativo móvel deve permitir a visualização dos últimos logs gerados no NGFW.

4.8.10.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

4.8.10.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

4.9. Requisitos de Projeto e de Implementação

4.9.1. Serviço de Implementação deverá contemplar o seguinte escopo:

4.9.1.1. Reunião entre CONTRATADA e CONTRATANTE para detalhamento de todos os parâmetros de rede e modo de operação da rede.

4.9.1.2. Definição do plano de testes, em conjunto com o corpo responsável da UFLA, de cada etapa para migração de todas as regras e serviços.

4.9.1.3. Definição de cronograma de implementação do projeto com o planejamento de migração, para não afetar a operação da rede atual.

4.9.1.4. Atualização com o firmware mais recente disponível pelo fabricante.

4.9.1.5. Configuração do equipamento sobre os seguintes aspectos:

4.9.1.5.1 Definição das regras de firewall e opções de segurança;

4.9.1.5.2. Conectividades com todos os switches de distribuição;

4.9.1.5.3. Definição de parâmetros de segurança da informação;

4.9.1.5.4. Definição das regras de filtro de conteúdo;

4.9.1.5.5. Definição das regras NAT;

4.9.1.5.6. Configuração de regras de roteamento;

4.9.1.5.7. Definição de todas as Interfaces e VLANs a serem usadas na rede;

4.9.1.5.8. Definição do LAG (Link aggregation) com o equipamento core da rede legada;

4.9.1.5.9. Execução do plano de testes para validação da operação de implementação e migração;

4.9.1.5.10. Relatórios sobre o progresso de cada etapa;

4.9.1.5.11. Passagem de conhecimento do processo implementado;

4.9.1.5.12. Documentação do projeto “as-is”;

4.9.2. O Serviço de Implementação deverá ser executado por profissionais devidamente capacitados, com certificação do fabricante, a ser comprovada com certificados do mesmo, em Sonicwall.

4.10. Requisitos de Implantação

4.10.1. A implantação não deverá interferir na rede em funcionamento na UFLA.

4.10.2. Toda a operação deverá ser feita de modo que a rede legada não sofra interrupções.

4.10.2.1. Em caso de necessidade de interrupções justificadas, as mesmas deverão ser autorizadas e programadas em horários a serem definidos com a Diretoria de Gestão de Tecnologia da Informação (DGTI)/UFLA.

4.10.3. A configuração e implantação dos equipamentos deverá acontecer de forma presencial nas dependências da Diretoria de Gestão de Tecnologia da Informação (DGTI)/UFLA.

4.11. Requisitos de Garantia e Manutenção

4.11.1. A garantia dos equipamentos deverá possuir o período mínimo de 24 meses.

4.11.2. O suporte técnico, por parte do fabricante da solução, deverá ser 24/7, por meio de plataforma eletrônica, e-mail, telefax, mensageiro instantâneo ou chamado telefônico à central de atendimento, a ser informada pela CONTRATADA, onde poderá ser possível abrir tickets de manutenção, pelo período mínimo de 24 meses.

4.11.3. A garantia dos serviços deverá possuir o período mínimo de 12 meses.

4.11.4. O suporte técnico por parte da CONTRATADA da solução deverá ser 8/5, por meio de plataforma eletrônica, e-mail, telefax, mensageiro instantâneo ou chamado telefônico à central de atendimento, a ser informada pela CONTRATADA, onde poderá ser possível abrir tickets de manutenção, pelo período mínimo de 12 meses.

4.11.5 Entende-se por suporte da CONTRATADA toda dúvida, necessidade de configuração, resolução de problemas, análise de pacotes, incidentes em segurança da informação, afinação e calibração de configurações, melhores práticas de configuração, análise em relatórios do Analytics, entre outros;

4.11.6. O suporte por parte da CONTRATADA poderá ser prestado à distância, desde que as pendências solicitadas sejam resolvidas de forma plena.

4.11.7. Em caso de impossibilidade no atendimento da demanda de forma remota, a CONTRATADA deverá comparecer presencialmente para solucionar a demanda, às suas expensas.

4.11.8. Nos casos de troca de equipamentos defeituosos, os mesmos deverão ser enviados pela CONTRATADA no próximo dia útil subsequente à abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais para a CONTRATANTE, inclusive frete.

4.12. Requisitos de Experiência Profissional

4.12.1. A CONTRATADA deverá possuir, no momento da execução, certificação Sonicwall SNSA (SonicWall Network Security Administrator).

4.12.2. A CONTRATADA deverá possuir, no momento da execução, profissional com contrato de prestação de serviço ou profissional pertencente ao quadro permanente que deverá possuir certificação emitida pelo desenvolvedor/fabricante do appliance, que comprove a capacidade técnica para execução do serviço de integração entre a nova solução de firewall com a solução legada Supermassive 9600.

4.12.3. A CONTRATADA deverá possuir, no momento da execução, a certificação ISO 27001 (gestão da segurança da informação). A norma tem, como princípio geral, a adoção pela organização de um conjunto de requisitos, processos e controles com o objetivo de mitigar e gerir adequadamente o risco da organização.

4.13. Requisitos de Formação da Equipe

4.13.1. A CONTRATADA deverá apresentar, no momento da execução, a comprovação, por meio de apresentação da Carteira de Trabalho ou Ficha de Registro de Empregado ou

Contrato de Prestação de Serviços devidamente registrado em cartório, que possui em seu quadro de funcionários no mínimo 1 (um) profissional treinado e certificado pelas especificações do item 4.12 - Requisitos de Experiência Profissional.

4.13.2. É permitido à CONTRATADA apresentar diferentes profissionais treinados, de modo a contemplar todo o escopo das certificações solicitadas no item 4.12 - Requisitos de Experiência Profissional. Nesse caso, todos os profissionais treinados deverão estar presentes para a realização das atividades referentes às suas capacitações.

4.13.3. A qualificação desse(s) funcionário(s) deverá conter, no mínimo:

PERFIL – Integrador	
Responsável por realizar todas as atividades relacionadas à integração do novo appliance firewall com a rede legada da UFLA, conforme as normas, padrões e diretrizes da CONTRATANTE, implementando as regras e os casos de uso, integrando os componentes e módulos do sistema, além de gerar e manter as rotinas de implantação.	
Experiência/Qualificação	**Modo de Comprovação**
Experiência mínima de 01 (um) ano em prestação de serviços na appliance de firewall SONICWALL.	Registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
Formação	**Modo de Comprovação**
Curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação.	Diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou mestrado ou doutorado, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.

4.14. Requisitos de Metodologia de Trabalho

4.14.1. Após a entrega dos equipamentos, a CONTRATADA deverá entrar em contato com a UFLA para agendar a reunião para definição das diretrizes de instalação/configuração e cronograma de implantação, desde que observadas as condições de prazos estabelecidos neste Termo de Referência.

4.14.2. Deverá ocorrer uma reunião inicial, que poderá ser por meio de conferência, contemplando os planos e objetivos definidos, de forma clara, da implantação e migração da solução.

4.14.3. O contato com a UFLA para agendamento da reunião inicial será por meio do e-mail

dgti@ufla.br.

4.15. Requisitos de Segurança da Informação e Privacidade

4.15.1. A solução CONTRATADA deverá respeitar a adequação à legislação vigente sobre segurança da informação e privacidade, tais como:

4.15.1.1. LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

4.15.1.2. Marco Civil da Internet (Lei nº 12.965/2014).

4.15.1.3. Norma Brasileira ABNT NBR ISO/IEC 27002.

4.15.2. A CONTRATADA deverá manter a integridade da rede de dados e das informações da UFLA durante a prestação dos serviços.

4.15.3. A CONTRATADA deverá respeitar a Política de Segurança da Informação e Comunicações da Universidade Federal de Lavras, bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.

4.15.1.5. A CONTRATADA deverá guardar sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

4.15.1.6. A CONTRATADA deverá assinar o Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança da informação vigentes, a ser assinado pelo representante legal da mesma, juntamente com o Termo de Ciência, conforme item 6.4 do presente Termo de Referência.

4.16. Outros Requisitos Aplicáveis

4.16.1. Deverá ser apresentada a documentação técnica do fabricante do equipamento, comprovando o atendimento a todos os requisitos contidos neste Termo de Referência, com o atendimento das seguintes condições:
4.16.1.1. Não serão aceitas referências a futuras atualizações ou versões de produtos para comprovar a existência ou aderência a qualquer quesito deste Termo de Referência.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos.

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico.

5.1.3. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.

5.1.4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável.

5.1.5. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato.

5.1.6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável.

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.1.9. Verificar, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e, posterior, recebimento definitivo.

5.2. Deveres e responsabilidades da CONTRATADA

5.2.1. Indicar formalmente e por escrito, no prazo máximo de 05 (cinco) dias úteis após a assinatura do contrato, junto à CONTRATANTE, um preposto idôneo com poderes de decisão para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato.

5.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

5.2.3. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por

culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE.

5.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão.

5.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação.

5.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC.

5.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato.

5.2.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração.

5.2.9. Executar o objeto do certame em estreita observância dos ditames estabelecidos pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

5.2.10. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da CONTRATANTE.

5.2.11. Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do contrato em questão.

5.2.12. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade, no que couber.

5.2.13. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos, preferencialmente nas dependências da UFLA.

5.2.14. Caso os produtos apresentem qualquer defeito durante o período em garantia, quaisquer ônus com materiais, peças ou componentes substituídos, supervisão técnica e/ou operacional, transporte, diárias e demais despesas decorrentes da prestação do serviço correrão por conta da CONTRATADA.

5.2.15. Caso necessário, a CONTRATADA se responsabilizará pelo envio e acompanhamento dos produtos junto aos respectivos fabricantes, sendo que, quaisquer ônus com transporte, diárias e demais despesas decorrentes da prestação do serviço correrão por conta da CONTRATADA.

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. O prazo de entrega dos bens é de até 60 (sessenta) dias, contados da data de recebimento da Ordem de Fornecimento de Bens (OFB), na Diretoria de Materiais e Patrimônio, localizada no *Campus* Universitário, que poderá solicitar o encaminhamento dos mesmos para outros locais da Universidade, com todas as despesas pagas pelo licitante vencedor.

6.1.2. A CONTRATADA deverá comunicar à CONTRATANTE, por meio da Diretoria de Materiais e Patrimônio, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

6.1.3. Os equipamentos da Solução deverão ser instalados no DataCenter da UFLA. A reunião inicial deverá ser marcada pela CONTRATADA após assinatura do contrato. As reuniões deverão sempre ser agendadas por meio de e-mail fornecido pela CONTRATANTE, em momento oportuno.

6.1.4. Para minimizar o impacto (downtime dos serviços) na integração das soluções, esse serviço deverá ser realizado presencialmente, no horário e dia proposto pela CONTRATANTE, podendo ser em finais de semana e após o horário comercial.

6.1.5. As identificações e certificações dos funcionários que irão executar o serviço devem ser fornecidas na primeira reunião.

6.2. Quantidade mínima de bens ou serviços para comparação e controle

6.2.1. Não há quantidade mínima de equipamentos a serem entregues. A quantidade deverá obedecer ao contrato assinado.

6.3. Mecanismos formais de comunicação

6.3.1. Após a assinatura do contrato, a CONTRATADA deverá agendar a reunião inicial com a CONTRATANTE por meio de e-mail.

6.3.2. O mecanismo formal de comunicação a ser utilizado para troca de informações entre a CONTRATADA e a CONTRATANTE será o e-mail (dgti@ufla.br). Poderá ser utilizada outra forma de comunicação (telefone, telefax, sms, app de mensagens, entre outros), porém, toda demanda deverá ser formalizada via e-mail.

6.4. Manutenção de Sigilo e Normas de Segurança

6.4.1 A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

6.4.2. O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA, e **Termo de Ciência**, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se nos ANEXOS II e III do Edital.

7 – MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.1.1. Os bens serão recebidos provisoriamente pela Diretoria de Materiais e Patrimônio, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.1.2. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de até 10 (dez) dias úteis, a contar da notificação do licitante vencedor, às suas custas, sem prejuízo da aplicação das penalidades.

7.1.3. Caso a substituição não ocorra no prazo definido no item anterior, estará o licitante vencedor incorrendo em atraso na entrega, sujeito à aplicação das sanções previstas neste Termo de Referência.

7.1.4. Os bens serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

7.1.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

7.2. Procedimentos de Teste e Inspeção

7.2.1 Os procedimentos de teste, verificação e inspeção serão realizados conforme descrição estabelecida no item 4 deste Termo de Referência.

7.3. Níveis Mínimos de Serviço Exigidos

IAE – INDICADOR DE ATRASO DE ENTREGA A PARTIR DO RECEBIMENTO DA ORDEM DE FORNECIMENTO DE BENS (OFB)	
Tópico	**Descrição**
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na OFB.
Meta a cumprir	**60 dias**
Instrumento de medição	Inicial: Recebimento da OFB. Final: Termo de recebimento provisório pelo setor competente da UFLA.
Forma de acompanhamento	O acompanhamento será realizado, com base no instrumento de medição, por membro designado pela Diretoria de Gestão de Tecnologia da Informação (DGTI/UFLA). A DGTI/UFLA notificará o descumprimento do prazo.
Periodicidade	Única
Mecanismo de Cálculo (métrica)	**IAE = <u>TEX – TEST</u>** **TEST** Onde: **IAE** – Indicador de Atraso de Entrega; **TEX** – Tempo de Execução – corresponde ao período de execução da entrega, da sua data de início (recebimento da OFB) até a data de entrega dos produtos (recebimento atestado pela DGTI) . **TEST** – Tempo Estimado para a Entrega conforme estipulado no Termo de Referência.
Observações	Obs1: Serão utilizados dias corridos na medição.

	Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante.
Início de Vigência	A partir do recebimento da OFB.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IAE**: De 0 a 0,10 – Pagamento integral; De 0,11 a 0,20 – Glosa de 1%; De 0,21 a 0,30 – Glosa de 2%; De 0,31 a 0,50 – Glosa de 5%; De 0,51 a 1,00 – Glosa de 7%; Acima de 1 – Será aplicada Glosa de 10% e multa de 10% sobre o valor do contrato.

IAI – INDICADOR DE ATRASO NA IMPLANTAÇÃO DA SOLUÇÃO		
Tópico	**Descrição**	
Finalidade	Medir o tempo de atraso na implantação e instalação do Firewall e licenciamento constantes no contrato.	
Meta a cumprir	**30 dias**	
Instrumento de medição	Inicial: Termo de recebimento provisório pelo setor competente da UFLA. Final: Ateste por parte da UFLA quanto ao pleno funcionamento dos equipamentos e dos softwares contratados.	
Forma de acompanhamento	O acompanhamento será realizado, com base no instrumento de medição, por membro designado pela Diretoria de Gestão de Tecnologia da Informação (DGTI/UFLA).	

	A DGTI/UFLA notificará o descumprimento do prazo.
Periodicidade	Única
Mecanismo de Cálculo (métrica)	**IAI = <u>TEX – TEST</u>** **TEST** Onde: **IAI** – Indicador de Atraso na Implantação da Solução; **TEX** – Tempo de Execução – corresponde ao período de execução da implantação da solução, da sua data de início (data do Termo de Recebimento Provisório) até a data de ateste quanto ao pleno funcionamento dos equipamentos e dos softwares contratados (atestado pela DGTI) . **TEST** – Tempo Estimado para a implantação da solução conforme estipulado no Termo de Referência.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante.
Início de Vigência	A partir da data do Termo de Recebimento Provisório.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IAI**: De 0 a 0,10 – Pagamento integral; De 0,11 a 0,20 – Glosa de 1%; De 0,21 a 0,30 – Glosa de 2%; De 0,31 a 0,50 – Glosa de 5%; De 0,51 a 1,00 – Glosa de 7%; Acima de 1 – Será aplicada Glosa de 10% e multa de 10% sobre o valor do

	contrato.

7.4. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.4.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

7.4.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

7.4.1.2. ensejar o retardamento da execução do objeto;

7.4.1.3. falhar ou fraudar na execução do contrato;

7.4.1.4. comportar-se de modo inidôneo;

7.4.1.5. cometer fraude fiscal.

7.4.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

7.4.2.1. advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CONTRATANTE;

7.4.2.2. multa moratória de 0,1% (zero vírgula um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

7.4.2.3. multa compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

7.4.2.4. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

7.4.2.5. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

7.4.2.6. impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

7.4.2.6.1. a sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 7.1 deste Termo de Referência;

7.4.2.7. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre

que a CONTRATADA ressarcir a CONTRATANTE pelos prejuízos causados.

7.4.3. As sanções previstas nos subitens 7.4.2.1., 7.4.2.5., 7.4.2.6. e 7.4.2.7. acima poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

7.4.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

7.4.4.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

7.4.4.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

7.4.4.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

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

7.4.6. As multas devidas e/ou prejuízos causados à CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

7.4.6.1. Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.4.7. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

7.4.8. 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 à Administração, observado o princípio da proporcionalidade.

7.4.9. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

7.4.10. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

7.4.11. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

7.4.12. As penalidades serão obrigatoriamente registradas no SICAF.

7.4.13. As glosas porventura aplicadas, conforme previstas no item 7.3 deste Termo de Referência, serão descontadas dos pagamentos devidos pela UFLA ou cobradas diretamente da CONTRATADA penalizada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas.

7.4.14. Serão considerados injustificados os atrasos não comunicados tempestivamente e indevidamente fundamentados e a aceitação da justificativa ficará a critério da UFLA, que examinará a legalidade da conduta da CONTRATADA.

7.4.15. Comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela UFLA, conforme procedimento esboçado no subitem anterior, a CONTRATADA ficará isenta das glosas mencionadas.

7.5. Do Pagamento

7.5.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.5.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

7.5.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão CONTRATANTE atestar a execução do objeto do contrato.

7.5.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

7.5.3.1. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

7.5.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

7.5.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.5.6. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

7.5.7. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize

sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

7.5.8. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

7.5.9. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.5.10. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

7.5.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

7.5.11.1. Será rescindido o contrato em execução com a CONTRATADA inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da CONTRATANTE.

7.5.12. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.5.12.1. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

7.5.13. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$EM = I \times N \times VP, \text{ sendo:}$$

EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)

I = (6 / 100) / 365

I = 0,00016438

TX = Percentual da taxa anual = 6%

8 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Id.	Descrição do Bem ou Serviço	Qtde.	Unidade de Medida	Valor Unitário Máximo Aceitável	Valor Total Máximo Aceitável
1	Atualização do Firewall SonicWall Supermassive 9600 para o NSA 5700 e aquisição da licença Essential Protection Service Suite para NSA 5700 em Par de Alta Disponibilidade por 24 meses, com migração do Supermassive 9600 para a nova solução, com serviço mensal de Service Desk prestado pelo fornecedor em regime de 8/5, pelo período de 12 meses.	01	Unidade	R$ 452.484,47	R$ 452.484,47
2	Aquisição da licença SonicWall Analytics Software pelo período de 24 meses.	01	Unidade	R$ 9.022,19	R$ 9.022,19
Total Estimado Geral				R$ 461.506,66	

9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. Para a contratação foi informada a seguinte adequação orçamentária:

NATUREZA DE DESPESA: 449052 e 339040

PROGRAMAS:

12.364.5013.20RK.0031	FONTE:	8100000000	TESOURO
12.364.5013.20RK.0031	FONTE:	8150262630	RENDAS PRÓPRIAS
12.364.5013.8282.0031	FONTE:	8100000000	REUNI

9.2. Não se aplica ao objeto da contratação um cronograma de execução física e financeira.

10 – DA VIGÊNCIA DO CONTRATO

10.1. O contrato vigorará por 24 (vinte e quatro) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a 48 (quarenta e oito) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso IV, Art. 57, da Lei nº 8.666, de 1993.

10.2. A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada da realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

10.3. A licença Essential Protection Service Suite para NSA 5700 em par de Alta Disponibilidade, contida no Item 1 e imprescindível ao correto funcionamento da solução, é qualificada como serviço contínuo, conforme disposto na Portaria MEC nº 14.787/2014, que dispõe sobre quais são os serviços considerados continuados em seu âmbito. Assim, nos incisos XV, XXXIII e LXXIV da referida portaria tem-se: XV - contratação de serviço de suporte técnico à plataforma de produtos software; XXXIII - licença de uso de software e LXXIV - sustentação a serviços de Tecnologia da Informação.

10.4. Da mesma forma, a licença SonicWall Analytics Software, contida no item 2, também se classifica como serviço contínuo, conforme disposto na Portaria MEC nº 14.787/2014, que dispõe sobre quais são os serviços considerados continuados em seu âmbito. Assim, nos incisos XV, XXXIII e LXXIV da referida portaria tem-se: XV - contratação de serviço de suporte técnico à plataforma de produtos software; XXXIII - licença de uso de software e LXXIV - sustentação a serviços de Tecnologia da Informação.

10.5. Isto posto, a possibilidade de renovação prevista no item 10.1 se aplica ao disposto nos itens 10.3 e 10.4 deste Termo de Referência, ou seja, o fornecimento do equipamento se dará uma única vez, mas os serviços associados são passíveis de prorrogação contratual.

11 – DO REAJUSTE DE PREÇOS

11.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de 24 (vinte e quatro) meses contados da assinatura do contrato.

11.2. Após o interregno de 24 (vinte e quatro) meses, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do ICTI (Índice de Custos de Tecnologia da Informação) mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

11.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

11.4. 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.

11.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

11.6. Caso o índice estabelecido para reajustamento 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.

11.7. 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.

11.8. O reajuste será realizado por apostilamento.

12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

12.1.1. Será utilizada a modalidade do Pregão, na forma Eletrônica, onde o objeto enquadra-se na classificação de bens e serviços comuns, nos termos do parágrafo único do art. 1° da Lei nº 10.520/2002 e do inciso II do art. 3º do Decreto nº 10.024/2019.

12.1.2. O objeto da licitação será adjudicado por grupo, mediante critério de menor preço.

12.2 Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

12.2.1. O Decreto nº 7.174/2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, em seu artigo 5º, traz a seguinte redação:

“Art. 5º. Será assegurada preferência na contratação, nos termos do disposto no art. 3º da Lei nº 8.248, de 1991, para fornecedores de bens e serviços, observada a seguinte ordem:

I - bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

II - bens e serviços com tecnologia desenvolvida no País; e

III - bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal.

Parágrafo único. As microempresas e empresas de pequeno porte que atendam ao disposto nos incisos do caput terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo inciso.”

12.2.2. Isto posto, em relação ao Decreto 7.174/2010, será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8°.

12.2.3. A Lei Complementar nº 123/2006 - Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte: aplicável. A referida Lei, traz em seu artigo 48:

“Art. 48. Para o cumprimento do disposto no art. 47 desta Lei Complementar, a administração pública:

I - deverá realizar processo licitatório destinado exclusivamente à participação de microempresas e empresas de pequeno porte nos itens de contratação cujo valor seja de até R$ 80.000,00 (oitenta mil reais);

(...)

III - deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte.”

12.2.4. A aplicação do disposto no item 12.2.3 geraria benefícios diferentes para cada item. Considerando a necessidade de agrupamento dos itens para adequação da solução e a natureza majoritária do item 1 (bem não divisível com valor estimado superior a R$ 80.000,00) na composição do grupo, não é possível a destinação da disputa da licitação exclusiva para ME/EPP, bem como a criação de cotas exclusivas. Dessa forma, o grupo composto pelos dois itens deste Termo de Referência será destinado à ampla concorrência, o que justifica-se com respaldo no art. 49, inciso III da Lei Complementar nº 123/2006:

“Art. 49. Não se aplica o disposto nos arts. 47 e 48 desta Lei Complementar quando:

(...)

III - o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado”

12.3 Critérios de Qualificação Técnica para a Habilitação

12.3.1. A CONTRATADA deve possuir, no momento da execução, a certificação SNSA (SonicWall Network Security Administrator).

12.3.2. A CONTRATADA deverá possuir, no momento da execução, profissional com contrato de prestação de serviço ou profissional pertencente ao quadro permanente que deverá possuir certificação emitida pelo desenvolvedor/fabricante do appliance, que comprove a capacidade técnica para execução do serviço de integração entre a nova Solução de firewall com a solução Legada Supermassive 9600.

12.3.3. A CONTRATADA deve possuir, no momento da execução, a certificação ISO 27001 (gestão da Segurança da informação). A norma tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controles com o objetivo de mitigar e gerir adequadamente o risco da organização.

12.4. Visita Técnica Facultativa

12.4.1. De forma a ter maior conhecimento do Datacenter, do Firewall legado e das circunstâncias locais, para correto dimensionamento e elaboração de sua proposta, é facultado aos licitantes a realização de vistoria.

12.4.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

12.4.3. A visita técnica deverá ser agendada junto à Diretoria de Gestão de Tecnologia da Informação, por meio dos telefones (35)3829-1521 ou do e-mail cic.dgti@ufla.br, de segunda-feira a sexta-feira nos horários de 08h00 às 12h00 e das 14h00 às 17h00.

12.4.4. Por ocasião da visita técnica, o licitante deverá trazer a Declaração de Vistoria, elaborada de acordo com o Anexo IV do Edital, devidamente impressa e preenchida, em duas vias, que serão visadas pelo servidor responsável da UFLA e constituirá documento de habilitação do certame.

12.4.4.1. A visita técnica só poderá ser realizada pelo licitante que conste no contrato social ou no Sicaf ou por seu representante legal, devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua designação para a realização da vistoria, como procuração.

12.4.5. A visita técnica é facultativa, no entanto, caso se opte por não vistoriar, a Declaração de Vistoria deverá ser substituída pela Declaração de Não Vistoria, elaborada e devidamente preenchida de acordo com o Anexo V do Edital. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais de execução do objeto, devendo a licitante vencedora assumir os ônus decorrentes.

12.4.5.1. A Declaração de Não Vistoria, caso seja essa a opção, constituirá documento de habilitação do certame.

12.4.6. Em virtude da pandemia pelo coronavírus, o licitante deverá, durante toda a visita técnica, fazer uso de máscara, álcool gel e cumprir o protocolo de biossegurança vigente na UFLA, respeitando o distanciamento.

12.4.6.1. A máscara, o álcool gel e qualquer outro equipamento de proteção individual

entendido como necessário não serão fornecidos pela UFLA, sendo de exclusiva responsabilidade do licitante.

12.4.6.2. A UFLA se reserva no direito de cancelar a visita técnica do licitante que não cumpra o disposto nos itens 12.4.6 e 12.4.6.1.

13 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

A Equipe de Planejamento da Contratação foi instituída pela Portaria SGV/Reitoria nº 09, de 08 de março de 2022, reconduzida pela Portaria SGV/Reitoria nº 19, de 13 de maio de 2022.

Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

_____ **Integrante Requisitante** Plínio Márcio Braga Torres	_____ **Integrante Técnico** Jairo Antônio Resende Paviani	_____ **Integrante Administrativo** Lísias André de Vieira e Silva

Autoridade Máxima da Área de TIC
_____ Erasmo Evangelista de Oliveira