TERMO DE REFERÊNCIA

PE

Processo Administrativo nº

23081.125728/2022-18

Aquisição de Next Generation Firewall para a Universidade Federal de Santa Maria

Santa Maria, 25 de outubro de 2022.

Sumário

TERMO DE REFERÊNCIA OU PROJETO BÁSICO

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

1 - OBJETO DA CONTRATAÇÃO

Esta licitação tem por objeto o Registro de Preços para contratação de solução de Firewall de Próxima Geração (NGFW) para segurança da informação de perímetro que possibilite a visibilidade aplicações em camada 7 e controle de todo tráfego, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN, controle granular de banda de rede e controle de todo tráfego, independentemente da origem ou destino, compreendendo o fornecimento de equipamentos e licenças integrados em forma de appliance conforme quantidades e exigências estabelecidas neste Termo de Referência.

2 - DESCRIÇÃO DA SOLUÇÃO DE TIC

Conforme visto no Estudo Técnico Preliminar (ETP), com ênfase na análise comparativa entre as possíveis soluções e observando seus benefícios, desvantagens e custos, a melhor e mais viável solução para a universidade é a Aquisição de equipamentos do mesmo fabricante, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela equipe de segurança da informação e necessidades da UFSM.

Essa solução prevê a aquisição de novos equipamentos e licenças do mesmo fabricante da solução de NGFW adquirida em 2020. Nesse caso, os novos equipamentos seriam adicionados ao cluster de firewalls já existente e ao gerenciamento centralizado realizado por meio do software Panorama, que possibilita o gerenciamento de até 25 (vinte e cinco) dispositivos com uma única licença (a qual a UFSM já possui).

As demais características relacionadas à solução estão descritas no item 4.8 Requisitos de Arquitetura Tecnológica - especificação técnica.

2.1. Bens e serviços que compõem a solução

Id.	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade
1	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS	2	Peça
2	AQUISIÇÃO DE LICENÇAS: THREAT PREVENTION, DNS SECURITY, WILDFIRE, URL FILTERING	2	Licença
3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	2	Serviço

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

A Universidade Federal de Santa Maria (UFSM) disponibiliza uma infraestrutura de tecnologia da Informação (TI) para cerca de 20.000 (vinte mil) usuários da comunidade acadêmica, sendo composta por alunos, professores e técnicos administrativos em educação. A equipe de Segurança da Informação, parte da Divisão de Suporte, é composta por dois analistas que são responsáveis por planejar, executar e manter políticas e medidas que garantam a segurança e proteção da rede e dos sistemas computacionais na Universidade. Dessa forma, essa equipe atua diretamente na implementação e manutenção dos sistemas de proteção, como por exemplo, no firewall.

A infraestrutura de segurança da informação na UFSM apresentou algumas evoluções nos últimos anos. Até o final do ano 2020, a UFSM utilizava uma solução de firewall baseada em software livre, denominada PFSense. Esse firewall oferecia um nível básico de proteção, diante da dimensão e grande fluxo de informações trafegadas na rede da Universidade. A proteção da rede implementada no PFSense era baseada na filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e transporte do modelo OSI. Dessa forma, ele atuava apenas com base nos cabeçalhos dos pacotes da camada de rede (IPv4, IPv6 e ICMP) e da camada de transporte (UDP e TCP). Assim, era possível criar regras apenas com base nos endereços IP (origem e/ou destino), portas (origem e/ou destino) e protocolos citados anteriormente.

Em 2020, foi realizado o processo de licitação para a aquisição de uma solução de Firewall de Próxima Geração, ou, Next Generation Firewall (NGFW). Conforme o Estudo Técnico Preliminar (ETP) realizado nesse processo de licitação, verificou-se que a UFSM necessitaria adquirir 4 (quatro) equipamentos físicos para operar em alta disponibilidade, atendendo os dois segmentos da rede de comunicação: borda (entrada/saída da Internet) e rede interna (entre dispositivos/servidores).

Devido a disponibilidade de recursos financeiros no momento da aquisição para adquirir apenas dois equipamentos e a falta de novos recursos, a ata gerada no processo de licitação teve sua validade vencida, visto que sua validade era até 2021, ou seja, um ano de validade. Os equipamentos adquiridos são produzidos pelo fabricante Palo Alto, modelo PA-3260 e possuem as seguintes licenças: Threat Prevention, DNS Security, WildFire e URL Filtering.

Dessa forma, atualmente, a UFSM possui um cluster de firewalls, com dois equipamentos NGFW operando em alta disponibilidade, ou seja, um equipamento ativo e outro redundante, provendo alta disponibilidade da solução, instalado entre a rede interna da Universidade e a Internet, realização a proteção contra ameaças externas e inspecionando o tráfego que tem como origem ou destino a Internet.

Esses equipamentos são gerenciados de forma centralizada por meio de um software de gerenciamento centralizado denominado Panorama, o qual foi adquirido junto aos equipamentos em 2020. Além de permitir o gerenciamento centralizado, esse software possibilita o armazenamento de logs.

A solução de NGFW adquirida em 2020 está atendendo plenamente, provendo a

segurança necessária contra ameaças oriundas da Internet, tendo sido devidamente dimensionada para atender a este cenário.

Nesses termos, a grande maioria dos serviços e operações fundamentais para o funcionamento da UFSM são fortemente dependentes da disponibilidade da sua rede de computadores e de seu datacenter, de forma que se faz necessário garantir a disponibilidade e, principalmente, a segurança dos dados e aplicações minimizando o risco de paralisações nos serviços prestados e evitando um impacto negativo no desempenho institucional da UFSM.

Neste contexto, a segurança do ambiente de tecnologia, que sustenta a operação desta universidade, torna-se um elemento crucial. Segurança é um processo contínuo. Com o avanço constante da tecnologia novas formas de ataques cibernéticos são descobertas diariamente, o que faz com que os processos referentes à segurança da informação tenham que ser revistos constantemente e novas abordagens de segurança precisam ser incorporadas à infraestrutura de TI.

Conforme apresentado no ETP elaborado em 2020 e visando evoluir a infraestrutura de segurança da informação, o conceito de Zero Trust Network Access (ZTNA) deve ser destacado e observado. Nessa abordagem, todo o tipo de tráfego é inspecionado, sem exceção, independentemente da origem e do destino do tráfego, podendo este tráfego ter sido originado de um computador da rede interna da universidade, o qual, na teoria, seria uma origem confiável, e tendo como destino o data center da universidade, por exemplo, outro destino confiável.

Em uma abordagem de segurança tradicional onde só é realizada inspeção do tráfego oriundo da internet, sendo a internet uma rede não confiável, para a rede interna, sendo a rede interna um ambiente confiável e vice-versa, um tráfego que teria como origem e destino objetos pertencentes a rede interna não seria passível de inspeção. Nesse cenário, quando um dispositivo participante da rede interna acessa um determinado serviço, como por exemplo, portais web ou site da Universidade, não é realizada nenhuma filtragem de pacotes ou inspeção de comunicação.

Para garantir que todos os hosts e serviços da Universidade estejam devidamente protegidos e seguros, é necessário aplicar o conceito Zero Trust Network Access, onde todos os usuários e acessos são considerados, inicialmente, como não confiáveis. Dessa forma, todas as comunicações devem passar pelo firewall, independente de sua origem ou destino. Nesse cenário, os servidores que disponibilizam os serviços e aplicações podem ser incluídos em uma DMZ.

Após o entendimento do conceito de ZTNA e sua importância na evolução da infraestrutura de segurança, é importante destacar que a implementação dessa nova abordagem na UFSM é essencial. Conforme descrito anteriormente, a UFSM possui cluster de firewalls Palo Alto PA-3260, provendo alta disponibilidade da solução. Para a implementação do ZTNA no cenário atual deve ser observado o impacto do aumento do tráfego a ser inspecionado pelo firewall. Atualmente, o firewall realiza a inspeção de um tráfego superior a 2 Gbps em determinados horários.

Em um cenário onde todo o tráfego deve ser inspecionado, independentemente da origem ou destino, esses valores tendem a crescer de forma significativa, o que pode ocasionar impactos significativos em relação a desempenho e performance. Isso se deve ao fato de que o firewall além de realizar os procedimentos relacionados a inspeção de

pacotes, necessita o roteamento de pacotes também. Ou seja, o firewall opera com suas interfaces em layer 3 do modelo OSI, realizando o roteamento por meio da funcionalidade de roteador virtual. Essa funcionalidade é necessária para realizar o encaminhamento dos pacotes após realizadas as devidas inspeções e verificações de concordância com as políticas de segurança estabelecidas.

Nesse contexto, observando os conceitos de ZTNA e as melhores práticas utilizadas no mercado de segurança da informação, uma abordagem interessante é realizar a segmentação da rede em perímetros menores, como por exemplo: separar o tráfego da Internet (origem ou destino) do tráfego existente entre apenas dispositivos/servidores da rede interna. Nesse caso, a alta disponibilidade também deve ser observada.

Com a aquisição de novos equipamentos será possível avançar a proteção a níveis recomendados nas melhores práticas citadas na literatura e já adotadas em instituições que visam proteger suas redes, ativos e informações.

A solução de firewall que a Universidade já possui, se mostrou eficiente e confiável desde a sua implementação, atendendendo aos requisitos técnicos de performance, tendo em vista o alto volume de tráfego da universidade, considerando ainda todos os requisitos de proteção contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises específica.

Ao expandir essa solução, através da aquisição de novos equipamentos e licenças, será possível planejar e implementar avanços significativos em termos de proteção e performance, observando e seguindo as melhores e mais modernas práticas citadas na literatura e utilizadas em instituições de diversos portes que prezam por garantir a segurança das informações e do ambiente computacional.

Outro aspecto importante para escolha dessa solução é os benefícios que a padronização de equipamentos apresenta. Por meio dela, os processos relacionados a gerenciamento, monitoramento e implementação de novas funcionalidades são facilitados, devido ao conhecimento já existente sobre a metodologia e funcionalidades da solução.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos (2016-2026) do Plano de Desenvolvimento Institucional**
PR-D5-01	Otimizar as rotinas administrativas e os sistemas de informação, primando pela agilidade, desburocratização, transparência e qualidade das informações e da gestão.

AI-D2-03	Oferecer uma infraestrutura de apoio qualificada e de acordo com as necessidades de cada área de conhecimento.
AI-D5-03	Modernizar a infraestrutura de TI para suportar as necessidades acadêmicas e administrativas.
PR-D2-01	Fortalecer aprendizado extraclasse, oportunizando atividades de extensão, inserção na sociedade, empreendedorismo, pesquisa e inovação.

ALINHAMENTO AO PDTI 2021-2024			
ID	**Ação do PDTI**	**ID**	**Meta do PDTI associada**
A3.6	Aquisição de Soluções de Segurança da Informação	**M03**	Promover a segurança da informação no âmbito da instituição
A3.2	Evoluir estrutura e proteção da rede com Next Generation Firewall - NGFW	**M03**	Promover a segurança da informação no âmbito da instituição

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
DFD 481/2021	Servidor para segurança em redes

3.3. Estimativa da demanda

Devido a necessidade em adquirir uma solução de Firewall de Próxima Geração, as quantidades abaixo foram estimadas durante a realização do Estudo Técnico Preliminar para compor o projeto em sua totalidade:

GRUPO	Item	Descrição	QTD
1	1	FIREWALL COM SUPORTE E GARANTIA DE 03 ANOS	2
	2	AQUISIÇÃO DE LICENÇAS: THREAT PREVENTION, DNS SECURITY, WILDFIRE, URL FILTERING	2
	3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	2

3.4. Parcelamento da Solução de TIC

Os equipamentos, licenças e serviços que constituem a solução aqui proposta se interagem entre si de forma a convergir para um sistema unificado, de modo que o fornecimento parcelado inviabilizaria a implantação de tecnologia capaz de atender as necessidades deste órgão. Assim, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, deverão ser do mesmo fabricante dos equipamentos deste grupo/lote.

3.5. Resultados e Benefícios a Serem Alcançados

- Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Proteção de todos os segmentos da rede de comunicação de dados;
- Implementação dos mais modernos mecanismos de segurança, amplamente discutidos e homologados pela literatura e instituições de diversos portes;
- Garantia que qualquer comunicação, independentemente da sua origem ou destino, será inspecionado pelo firewall;
- Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
- Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
- Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
- Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
- Criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados através do fechamento de portas não utilizadas, controlando a

banda de internet a fim de evitar abusos em sua utilização;

- Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
- Melhor filtro de conteúdo URL, sancionando acesso a sites indesejados de conteúdo ilícito.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

- Autenticação e rastreabilidade das informações de acesso dos usuários, sejam eles docentes, discentes e técnicos administrativos em educação desta Universidade pelo período mínimo de 01 ano de acordo com o Marco Civil da Internet Lei nº 12.965/2014;
- Preservação da integridade e da confidencialidade dos dados dos usuários, sejam eles docentes, discentes e técnicos administrativos em educação desta Universidade para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- Melhorar o nível de qualidade e segurança dos serviços das aplicações internas da Universidade;
- Proteção da infraestrutura de TI desta Universidade de modo a impedir que a mesma seja utilizada para outros fins (por exemplo: processamento no Datacenter utilizado para mineração de bitcoins, links de Internet utilizados para download de conteúdo ilícito ou ataques de negação de serviço - DDoS).

4.2. Requisitos de Capacitação

- Considerando que se trata da aquisição de uma solução para a qual a equipe da UFSM já possui conhecimento técnico suficiente para manter a solução funcionando corretamente e aplicando as melhores práticas sugeridas na literatura e adotadas por instituições de diversos portes, não existe necessidade de adquirir treinamentos específicos.

4.3. Requisitos Legais

- Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa n° 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão — SLTI/MPOG e no Decreto n° 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

Deverão ser cumpridas, no que couber, as exigências:

- Do inciso XI, art. 7º da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos — PNRS;

- Do art. 6º da Instrução Normativa MPOG n° 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.
- Da Portaria N° 170, de 10 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia — INMETRO.

4.4. Requisitos de Manutenção

- Os itens adquiridos nesse processo deverão possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 3 anos, contados a partir do recebimento definitivo da solução.
- Manutenção preventiva:
    - Durante o prazo de garantia, deverá ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correções.
    - Durante o prazo de garantia, deverá ser possível realizar a atualização das assinaturas de proteção da solução.
- Manutenção corretiva:
    - Durante o prazo de garantia, deverá estar prevista a reposição de peças e equipamentos. Essa reposição deverá abranger todos os itens que compõem a solução, incluindo módulos ou outros equipamentos fornecidos pela Contratada para atendimento do edital;
    - Em caso de defeitos de fabricação ou a necessidade de substituição hardware, a garantia deverá incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital. O envio da peça ou equipamento de reposição deverá ser realizado, no máximo, até o fim do próximo dia útil após a detecção da falha.
- Suporte e comunicação
    - Durante o prazo de garantia, os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website ou e-mail. O suporte deverá estar disponível na modalidade de 24x7 (24 horas por dia, 7 dias por semana).
    - O suporte deverá respeitar os seguintes tempos de resposta para os níveis de severidade abaixo:
        - a. Crítica: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deverá ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);
        - b. Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deverá ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
        - c. Média: Redução de performance do equipamento ou aplicação de

solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

- d. Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial.

- Poderão ser realizadas consultas técnicas ou questionamentos da equipe técnica da Contratante para sanar dúvidas, repassar conhecimentos, ou ainda obter melhores práticas. Estas consultas deverão ser realizadas através de e-mail, chat, ou outro meio acordado com a Contratante.

4.5. Requisitos Temporais

- A entrega de todos os produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.
- A entrega deverá ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.
- A implantação completa da solução deverá ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.

4.6. Requisitos de Segurança

A Contratada deverá submeter-se aos procedimentos de segurança existentes, 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.

4.7. Requisitos Sociais, Ambientais e Culturais

A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

Em conformidade com a IN SLTI/MPOG n. 01/2010, a Contratada deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:

- Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.
- Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.
- Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

- Que os bens não contenham 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 - especificação técnica

4.8.1. Item 1: Firewall com suporte e garantia de 03 anos

Aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta.

1. Requisitos técnicos gerais

1.1. A solução deverá consistir em appliance físico de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) do fabricante Palo Alto;

1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

1.3. A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7;

1.4. Deverá permitir autenticação centralizada, tanto da rede cabeada como da rede sem fio, utilizando-se da base LDAP existente;

1.5. O hardware e software que executem a funcionalidade de proteção de rede deverá ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.6. Todos os equipamentos fornecidos deverão ser próprios para montagem em rack 19 polegadas, incluindo kit tipo trilho para adaptação se necessário e todos acessórios (como cabo de energia, conectores, etc.) necessários para sua instalação;

1.7. Deverá possuir um throughput mínimo de 4 Gbps com as seguintes funcionalidades habilitadas simultaneamente (para todas as assinaturas que a plataforma de segurança possuir, devidamente ativadas e atuantes): controle de aplicações, IPS, Anti Malware, Antivírus e Antispyware;

1.8. Os throughputs deverão ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em amostra, assim como o atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei;

1.9. Os documentos públicos deverão comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego

real (real-word traffic blend);

1.10. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até a camada 4.
1.11. Suporte a, no mínimo, 1.000.000 de conexões simultâneas;
1.12. Suporte a, no mínimo, 10.000 novas conexões por segundo;
1.13. Possuir fonte 120/240 AC ou DC, redundante e hot-swappable;
1.14. Deverá possuir Disco Solid State Drive (SSD), com no mínimo, 240 GB;
1.15. Deverá possuir, no mínimo, 04 interfaces de rede 10 Gbps SFP+;
1.16. Deverá possuir, no mínimo, 05 interfaces de rede RJ-45 10/100/1000 Mbps, estando incluída uma interface para gerenciamento;
1.17. Deverá possuir, no mínimo, duas interfaces dedicadas para alta disponibilidade. Caso não possua, deverá possuir mais, no mínimo, duas interfaces RJ-45 10/100/1000 Mbps que possam ser utilizadas para esse fim (além das interfaces citadas no item 1.18, ou seja, um total de, no mínimo, 7 (sete) interfaces RJ-45 10/100/1000 Mbps;
1.18. Deverá possuir, no mínimo, 1 (uma) interface do tipo console ou similar;
1.19. Deverá ser incluído 8 (oito) módulos transceivers 10 GE SFP+;
1.20. Deverá suportar, no mínimo, 60 (sessenta) zonas de segurança**;**
1.21. Deverá estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) clientes de VPN SSL simultâneos;
1.22. Deverá estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) túneis de VPN IPSEC simultâneos;
1.23. Deverá suportar, no mínimo, 1 (um) sistema virtual lógico (Contexto) no firewall Físico;
1.24. Os contextos virtuais deverão suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Antispyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
1.25. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale ou qualquer outra forma de lista de descontinuidade;
1.26. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, deverão ser do mesmo fabricante dos equipamentos deste grupo/lote;
1.27. A solução deverá possuir pelo menos as seguintes funcionalidades:
    1.27.1. Suportar sub-interfaces ethernet lógicas;
    1.27.2. Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de firewall;
    1.27.3. O firewall deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deverá estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deverá ter a capacidade de usar rota

alternativa para estabelecer a comunicação;

1.28. Deverá suportar os seguintes tipos de NAT:
  1.28.1. Nat dinâmico (Many-to-1);
  1.28.2. Nat dinâmico (Many-to-Many);
  1.28.3. Nat estático (1-to-1);
  1.28.4. NAT estático (Many-to-Many);
  1.28.5. Nat estático bidirecional 1-to-1;
  1.28.6. Tradução de porta (PAT);
  1.28.7. NAT de Origem;
  1.28.8. NAT de Destino;
  1.28.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
1.29. A solução deverá possuir as seguintes funcionalidades:
  1.29.1. Suporte a 4094 VLAN Tags 802.1q;
  1.29.2. Agregação de links 802.3ad e LACP;
  1.29.3. Policy based routing ou policy-based forwarding;
  1.29.4. DHCP Relay;
  1.29.5. DHCP Server;
  1.29.6. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
1.30. Deverá implementar balanceamento de link através de políticas por usuário e/ou grupos de usuários do LDAP/AD;
1.31. Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino;
1.32. Deverá implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance deverão ser acessíveis via SNMP;
1.33. Deverá os registros de logs para sistemas de monitoração externos, simultaneamente. Deverá haver a opção de enviar logs via protocolo TCP e SSL;
1.34. Deverá permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
1.35. Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
1.36. Deverá implementar Proteção contra anti-spoofing;
1.37. Deverá permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
1.38. Deverá permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
1.39. Deverá suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64 ou Dual stack IPv4/IPv6, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras

de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

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

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

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

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

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

1.41. Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

1.41.1. Em modo transparente;

1.41.2. Em layer 3;

1.42. A configuração em alta disponibilidade deverá sincronizar:

1.42.1. Sessões;

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

1.42.3. Certificados decriptografados;

1.42.4. Associações de Segurança das VPNs;

1.42.5. Tabelas FIB;

1.42.6. O HA (modo de Alta-Disponibilidade) deverá possibilitar a monitoração de falha de link.

1.43. As funcionalidades de firewall, IDS/IPS, identificação de usuários, controle de aplicações, VPN IPSec e SSL, QOS, decriptografia SSL e SSH, DHCP server, DHCP relay, NAT, suporte a VLAN e protocolos de roteamento dinâmico deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

2. Controle por política de Firewall

2.1. Deverá suportar controles e criação de políticas por zona de segurança, porta/protocolo e aplicações, categorias de aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações usuários, grupos de usuários, endereço IP e redes;

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

2.3. Deverá permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
2.4. Deverá permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
2.5. Deverá permitir controle, inspeção e decriptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
2.6. Deverá permitir offload de certificado em inspeção de conexões SSL de entrada (Inbound);
2.7. Deverá permitir decriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
2.8. Deverá permitir decriptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
2.9. Deverá permitir Controle de inspeção e de-criptografia de SSH por política;
2.10. A decriptografia de SSH deverá possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado como técnica evasiva para burlar os controles de segurança;
2.11. Deverá permitir espelhamento de tráfego decriptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
2.12. Deverá permitir bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;
2.13. Deverá suportar objetos e regras IPV6;
2.14. Deverá suportar objetos e regras multicast;
2.15. Deverá permitir no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
2.16. Deverá suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

3. Controle de aplicações

3.1. A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

3.1.1. Deverá permitir a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
3.1.2. Deverá permitir a inspeção do payload do pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deverá determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
3.1.3. Deverá aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
3.1.4. Deverá identificar o uso de táticas evasivas, ou seja, deverá ter a

capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

3.1.5. Para tráfego criptografado SSL, deverá decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

3.1.6. Deverá permitir decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deverá identificar funcionalidades específicas dentro de uma aplicação, além de detectar arquivos e outros conteúdos que deverão ser inspecionados de acordo as regras de segurança implementadas;

3.1.7. Deverá permitir identificar o uso de táticas evasivas via comunicações criptografadas;

3.1.8. Deverá atualizar a base de assinaturas de aplicações automaticamente;

3.1.9. Deverá reconhecer aplicações em IPv6;

3.1.10. Deverá permitir limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem;

3.1.11. Deverá permitir adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

3.1.12. Deverá permitir múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

3.1.13. Deverá permitir o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

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

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

3.1.16. O fabricante deverá permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

3.1.17. Deverá permitir alertar o usuário quando uma aplicação for bloqueada;

3.1.18. Deverá permitir que o controle de portas seja aplicado para todas as aplicações;

3.1.19. Deverá permitir criar filtro na tabela de regras de segurança para exibir somente:

3.1.19.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada a aplicação

por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra. Caso essa informação não possa ser exibida através da criação de filtro, tais informações deverão ser exibidas em tabelas ou gráficos em dashboards e/ou monitores do console de gerenciamento;

3.1.19.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra. Caso não seja possível criar filtro, deverá ser possível visualizar a sessões associadas a uma determinada regra, através do campo "hit count";

3.1.19.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias. Caso não seja possível criar esse filtro, deverá ser possível visualizar a data e horário da última vez que houve associação de tráfego a uma regra;

3.1.19.4. Deverá possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

3.1.20. Deverá permitir a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

3.1.20.1. Tecnologia utilizada na aplicação (Client-Server, Browser Based, Network Protocol, etc).

3.1.20.2. Nível de risco da aplicação.

3.1.20.3. Categoria e subcategoria de aplicações.

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

4. Identificação de usuários

4.1. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, E-directory e base de dados local;

4.2. Deverá permitir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.3. Deverá permitir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

4.4. Deverá permitir que a autenticação da rede com fio seja realizada através de captive portal;

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

(Captive Portal);

4.6. Deverá permitir a autenticação via Kerberos;

4.7. Deverá permitir identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

4.8. Deverá permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;

4.9. Deverá permitir a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP;

4.10. Deverá permitir a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

5. QOS

5.1. Deverá permitir controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda;

5.2. Deverá permitir a criação de políticas de QoS por:

5.2.1. Endereço de origem;

5.2.2. Endereço de destino;

5.2.3. Por usuário e grupo do LDAP/AD;

5.2.4. Por aplicações;

5.2.5. Por porta;

5.3. O QoS deverá possibilitar a definição de classes por:

5.3.1. Banda Garantida;

5.3.2. Banda Máxima;

5.3.3. Fila de Prioridade;

5.4. Deverá permitir marcação de pacotes Diffserv, inclusive por aplicação;

5.5. Deverá disponibilizar estatísticas RealTime para classes de QoS;

5.6. Deverá permitir QOS (traffic-shapping), em interface agregadas;

5.7. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes e sessões.

6. VPN

6.1. Deverá permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Universidade remotamente;

6.2. Deverá suportar VPN Site-to-Site e Client-To-Site;

6.3. Deverá suportar IPSec VPN;

6.4. Deverá suportar SSL VPN;

6.5. A VPN IPSEc deverá suportar:

6.5.1. 3DES;

6.5.2. Autenticação MD5 e SHA-1;

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

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

6.5.5. AES 128, 192 e 256 (Advanced Encryption Standard)
6.5.6. Autenticação via certificado IKE PKI.

6.6. Deverá possuir interoperabilidade com os seguintes fabricantes:
6.6.1. Cisco;
6.6.2. Checkpoint;
6.6.3. Juniper;
6.6.4. Palo Alto Networks;
6.6.5. Fortinet;
6.6.6. Sonic Wall;

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

6.8. A VPN SSL deverá possuir os seguintes requisitos:
6.8.1. Deverá permitir ao usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
6.8.2. A funcionalidades de VPN SSL deverão ser atendidas com ou sem o uso de agente;
6.8.3. Deverá permitir atribuição de endereço IP nos clientes remotos de VPN SSL;
6.8.4. Deverá permitir a atribuição de IP fixos nos usuários remotos de VPN SSL;
6.8.5. Deverá permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário LDAP e grupo de usuário LDAP;
6.8.6. Deverá permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
6.8.7. Deverá permitir a atribuição de DNS nos clientes remotos de VPN;
6.8.8. A solução de VPN deverá verificar se o cliente que está realizando a conexão é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deverá ser bloqueado caso o dispositivo não seja o correto;
6.8.9. Deverá permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
6.8.10. A VPN SSL deverá suportar proxy arp e uso de interfaces PPPOE;
6.8.11. Deverá permitir autenticação via Radius, LDAP, OTP (One Time Password), certificado e base de usuários local;
6.8.12. Deverá permitir a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada;
6.8.13. Deverá permitir estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
6.8.14. Deverá permitir leitura e verificação de CRL (certificate revocation list);
6.8.15. Deverá permitir a aplicação de políticas de segurança e visibilidade para

as aplicações que circulam dentro dos túneis SSL;

6.8.16. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

6.8.16.1. Deverá permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

6.8.16.2. Antes do usuário autenticar na estação;

6.8.16.3. Após autenticação do usuário na estação;

6.8.16.4. Sob demanda do usuário;

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

6.9. O agente de VPN SSL client-to-site deverá ser compatível com pelo menos: Windows 7, Windows 8 e Mac OS;

6.10. Deverá haver a opção de o cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

4.8.2. Item 2: Aquisição de Licenças: Threat Prevention, DNS Security, WildFire, URL Filtering

1. Prevenção de ameaças

1.1. Para proteção do ambiente contra ataques, a solução deverá possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;

1.2. Deverá ser capaz de identificar e bloquear as seguintes ameaças: vírus, trojans, spywares, ransomwares e demais tipos de malwares;

1.3. Deverá permitir a inclusão de assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

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

1.5. Deverá permitir sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/passivo;

1.6. Deverá permitir os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

1.7. Deverá permitir detectar e prevenir ameaças em tráfegos HTTP/2;

1.8. Deverá permitir ativar ou desativar as assinaturas, ou ainda habilitá-las apenas em modo de monitoração;

1.9. Deverá permitir exceções por IP de origem ou de destino deverão ser possíveis nas regras, de forma geral e assinatura a assinatura;

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

1.11. Deverá permitir o bloqueio de vulnerabilidades;

1.12. Deverá permitir o bloqueio de exploits conhecidos;
1.13. Deverá incluir proteção contra ataques de negação de serviços (DoS);
1.14. Deverá permitir a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;
1.15. Deverá possuir os seguintes mecanismos de inspeção de IPS:
  1.15.1. Análise de padrões de estado de conexões;
  1.15.2. Análise de decodificação de protocolo;
  1.15.3. Análise para detecção de anomalias de protocolo;
  1.15.4. Análise heurística;
  1.15.5. IP Defragmentation;
  1.15.6. Remontagem de pacotes de TCP;
  1.15.7. Bloqueio de pacotes malformados;
1.16. Deverá ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
1.17. Deverá detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
1.18. Deverá bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
1.19. Deverá suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
1.20. Deverá possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
1.21. Deverá possuir assinaturas para bloqueio de ataques de buffer overflow;
1.22. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
1.23. Deverá permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
1.24. Deverá permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
1.25. Deverá suportar bloqueio de arquivos por tipo;
1.26. Deverá identificar e bloquear comunicação com botnets;
1.27. Deverá suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
1.28. Deverá suportar referência cruzada com CVE;
1.29. Deverá registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
1.30. Deverá suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;

1.31. Deverá permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deverá permitir selecionar, no mínimo, 50 pacotes;
1.32. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
1.33. Deverá permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
1.34. Deverá incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
1.35. Deverá incluir proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos;
1.36. Deverá incluir rastreamento de vírus em PDF;
1.37. Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
1.38. Deverá ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
1.39. Deverá possuir a capacidade de detectar e bloquear tentativas de resolução de domínios gerados de forma automática através de algoritmos (Domain generation algorithm - DGA);
1.40. Deverá mostrar nos logs as seguintes informações sobre domínios DGA:
    1.40.1. Domínio suspeito identificado;
    1.40.2. ID de assinatura de detecção;
    1.40.3. Usuário logado na estação/servidor que originou o tráfego;
    1.40.4. Aplicação;
    1.40.5. Porta de destino;
    1.40.6. IP de origem;
    1.40.7. IP de destino;
    1.40.8. Horário;
    1.40.9. Ação do firewall;
    1.40.10. Severidade;
1.41. Deverá possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle
1.42. A análise automática deverá incluir, no mínimo, as seguintes características:
    1.42.1. Padrões de consulta;
    1.42.2. Entropia;
    1.42.3. Análise de frequência n-gram de domínios;
    1.42.4. Taxa de consultas.

2. Análise de malwares modernos

2.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deverá possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta;

2.2. Deverá aplicar o conceito de Sandbox, que funciona como um ambiente isolado para análise de ameaças desconhecidas e que não estejam nas assinaturas do fabricante;

2.3. Deverá ser capaz de enviar arquivos trafegados de forma automática para análise, onde o arquivo será executado e simulado em ambiente controlado;

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

2.5. Deverá possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixam o sistema operacional lento, que alteram parâmetros do sistema, etc.;

2.6. Deverá suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistemas operacionais Windows;

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

2.8. A análise de links em sandbox deverá ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

2.9. Deverá permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

2.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas deverão ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

2.11. Deverá suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

2.12. Deverá suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

2.13. Deverá permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API;

2.14. Deverá permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução.

3. Filtro de URL

3.1. A solução deverá possuir as seguintes funcionalidades de filtro de URL:

3.1.1. Deverá permitir especificar política por tempo, ou seja, a definição de

regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

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

3.1.3. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.1.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

3.1.5. Deverá permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

3.1.6. Deverá permitir bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deverá ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

3.1.7. Deverá suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

3.1.8. Deverá permitir classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

3.1.9. Deverá permitir classificar sites em mais de uma categoria, de acordo com a necessidade;

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

3.1.11. Deverá permitir a criação categorias de URLs customizadas;

3.1.12. Deverá permitir a exclusão de URLs do bloqueio, por categoria;

3.1.13. Deverá permitir a customização de página de bloqueio;

3.1.14. Deverá permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

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

3.1.16. Deverá permitir a inclusão nos logs do produto de informações das atividades dos usuários;

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

4. Filtro de dados

4.1. Deverá permitir a criação de filtros para arquivos e dados pré-definidos;

4.2. Os arquivos deverão ser identificados por extensão e assinaturas;

4.3. Deverá permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre;

4.4. Deverá permitir a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.5. Deverá permitir listar o número de aplicações suportadas para controle de dados;
4.6. Deverá permitir listar o número de tipos de arquivos suportados para controle de dados.

4.8.3. Item 3: Serviços de instalação de firewall

1. Requisitos técnicos

A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

1.1. Reuniões de alinhamento para criação do escopo do projeto previamente à instalação;
1.2. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos, no local determinado pela equipe responsável pelo projeto por parte da contratante (DTI). Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
1.3. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;
1.4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
1.5. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
1.6. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;
1.7. Toda configuração de sistema (políticas gerais, objetos, itens de administração) deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada;
1.8. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;
1.9. Durante a implantação da solução, a equipe da Contratada deverá repassar as informações para a equipe da UFSM apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
1.10. O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
1.11. Os serviços de instalação e configuração deverão ser realizados por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante.
1.12. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da contratante.

4.9. Requisitos de Projeto e de Implementação

A Contratada deverá apresentar, antes de iniciar a fase de implantação da solução, projeto de instalação que deverá ser aprovado pela Contratante. O projeto deverá incluir uma proposta de cronograma.

4.10. Requisitos de Implantação

- A implantação da solução deverá ser realizada por profissionais especializados da contratada, que possuam certificação do fabricante da solução adquirida, ou pelo próprio fabricante.
- A implantação da solução deverá ocorrer com participação direta dos técnicos da UFSM que atuarão na solução.
- A implantação deverá abranger:
    - Integração da solução com a infraestrutura atual da UFSM;
    - Configuração das funcionalidades suportadas pela solução e descritas no presente Termo de Referência;
    - Demais requisitos apresentados no item 4.8 no referente ao serviço de instalação de firewall.
- As informações referentes à implantação deverão estar presentes no projeto de instalação.
- A Contratada deverá fornecer documentação completa da solução, incluindo especificação do equipamento, características, funcionalidades, comentários e configurações executadas.
- O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.
- A instalação/configuração deverá ser realizada de tal forma que as interrupções no ambiente de produção da UFSM sejam as mínimas possíveis e estritamente necessárias.

4.11. Requisitos de Garantia

- Os itens adquiridos nesse processo deverão possuir garantia do fabricante ou autorizada no Brasil, para hardware e licenças de software, com validade mínima de 3 anos contados a partir do recebimento definitivo da solução.
- Como comprovação de autorizada, deverá ser apresentado documento com informações da empresa prestadora da assistência técnica com sua identificação, endereço, CNPJ, responsável técnico e região de atuação.
- A garantia deverá respeitar os requisitos de manutenção e suporte descritos no item 4.4. Requisitos de Manutenção.

4.12. Requisitos de Experiência Profissional

Os profissionais componentes da equipe de implantação da solução por parte da Contratada deverão ser devidamente qualificados pelo fabricante da solução ou pela Contratada.

A comprovação deverá ser feita através da apresentação de certificados de capacitação emitidos em nome do profissional.

4.13. Requisitos de Formação da Equipe

A Equipe da UFSM que trabalhará com a solução deverá ser composta por Analistas e Técnicos de TI. Considerando que se trata da aquisição de uma solução para a qual a equipe da UFSM já possui conhecimento técnico suficiente para manter em operação, não existe necessidade de aquisição de treinamentos específicos.

4.14. Requisitos de Metodologia de Trabalho

A Contratante será a responsável pela verificação da aderência aos padrões de qualidade exigidos dos produtos entregues. A Contratada será responsável pelo fornecimento do software e gestão dos recursos humanos e materiais necessários para a prestação do suporte técnico.

A metodologia de trabalho relacionada aos serviços prestados deverá observar os preceitos do ITIL V4 quando aplicável.

4.15. Requisitos de Segurança da Informação

- A solução contratada deverá respeitar a adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).
- A solução contratada deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.
- A Contratada deverá manter a integridade da rede de dados e das informações da UFSM durante a prestação dos serviços.
- A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações (POSIC) da Universidade Federal de Santa Maria bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.
- 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 pelo Contratante a tais documentos.
- O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, deverá ser assinado por um representante da Contratada e encontra-se no ANEXO I. A Contratada deverá providenciar a assinatura do Termo de Ciência, disponível no ANEXO II, por todos os seus colaboradores que estejam relacionados com a execução do projeto. O Termo de Compromisso e o Termo de Ciência deverão ser entregues assinados durante a reunião inicial.

- Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse do Contratante mesmo após o uso, após dano à unidade ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deverá ser realizada no prédio do CPD/UFSM e imediatamente entregue a Contratante.
- Caso haja necessidade de manutenção fora das dependências do CPD/UFSM as unidades de armazenamento deverão ser removidas dentro das dependências do CPD/UFSM e deverão ficar sob responsabilidade da Contratante enquanto perdurar o conserto.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

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

b) 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;

c) Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d) Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

e) Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

f) Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável; e

h) Prever que 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, pertençam à Administração.

5.2. Deveres e responsabilidades da CONTRATADA

a) Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

b) Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

c) A contratada e seus prepostos, que participarem da execução desta relação

contratual, se obrigam a guardar sigilo dos dados e das informações postas à sua disposição, no grau em que tenham sido previamente qualificados pela parte que os forneceu, não podendo cedê-los a terceiros ou divulgá-los de qualquer forma sem anuência expressa da contratante, devendo assinar o Termo de Manutenção de Sigilo e providenciar que os seus funcionários assinem o Termo de Ciência;

d) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

e) Prestar todos os esclarecimentos que forem solicitados pela fiscalização da CONTRATANTE acerca da situação dos serviços contratados;

f) 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;

g) 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, sempre que considerar a medida necessária;

h) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

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

j) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e

k) 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, os modelos de dados e as bases de dados à Administração.

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

a) Efetuar o registro do licitante fornecedor;

b) Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

c) Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

d) Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a

capacidade mínima de fornecimento e for requerida pela contratada; e

3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

- Realização da Reunião Inicial
    - Após a assinatura do Contrato, o Gestor do contrato deverá convocar a reunião inicial com todos os envolvidos na contratação. A reunião inicial poderá ser realizada de forma presencial ou de forma remota. Na reunião inicial:
        - O representante legal da contratada deverá entregar o Termo de Compromisso e o Termo de Ciência, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade;
        - O representante legal da contratada deverá apresentar o cronograma de execução do projeto;
        - Serão feitos esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.
- Prazos, horários de fornecimento de bens ou prestação dos serviços
    - A entrega de todos os produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.
    - A implantação completa da solução deverá ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.
    - Os equipamentos deverão ser entregues e instalados no Centro de Processamento de Dados da Universidade de Santa Maria (Avenida Roraima, 1000, Prédio 48 - Camobi, RS, 97105-900). A entrega e instalação deverá ser realizada em dias úteis no horário das 08:00 às 12:00 e das 14:00 às 18:00.
    - A entrega deverá ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.
    - O suporte técnico deverá ser de, no mínimo, 3 anos.
- Documentação mínima exigida
    - A Contratada deverá fornecer:
        - Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;
        - Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações

executadas.

- Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

- Formas de transferência de conhecimento
  - A fim de promover a transferência de conhecimento, a implantação da solução deverá ocorrer com participação direta dos técnicos da UFSM que atuarão na solução. Durante a implantação da solução a equipe da Contratada deverá repassar as informações para a equipe da UFSM apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados.

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

Não se aplica.

6.3. Mecanismos formais de comunicação

As questões administrativas formais ocorridas durante a execução do contrato serão tratadas através de ofício. Questões administrativas ou operacionais cotidianas durante a execução do contrato poderão ser tratadas através de mensagem eletrônica (e-mail), telefone, aplicativo de mensagens ou outro meio informatizado que armazene o histórico da tramitação das solicitações e respostas.

6.4. Manutenção de Sigilo e Normas de Segurança

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.

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 I e II.

7 – MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

- **Para Item 1 - FIREWALL COM SUPORTE E GARANTIA DE 03 ANOS:**
  - Serão realizadas consultas diretamente no site do fabricante do equipamento, inclusive em manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste Termo de Referência. Em caso de dúvidas ou divergência na comprovação da especificação técnica, a UFSM poderá solicitar uma amostra do equipamento

ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para configuração e comprovação dos itens pendentes, nas dependências do CPD/UFSM.

- Os produtos serão inspecionados no ato da entrega, no CPD/UFSM, para verificar a conformidade, quantidade e realizar a inspeção visual da solução. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos usados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas.
- A existência de inspeção não isenta a contratada da responsabilidade pela qualidade do material fornecido.
- A solução será recebida provisoriamente por uma equipe designada pelo Diretor do Centro de Processamento de Dados acompanhada dos fiscais do contrato a fim de permitir a realização dos testes e inspeção descritos no item 7.2.
- O aceite do bem e recebimento definitivo somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presentes neste Termo de Referência e após aprovação no teste descrito no item 7.2.
- O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

- **Para Item 2 - AQUISIÇÃO DE LICENÇAS: THREAT PREVENTION, DNS SECURITY, WILDFIRE, URL FILTERING:**
  - O aceite do serviço somente será dado após a ativação e validação das licenças e suas respectivas funcionalidades.
- **Para Item 3 - SERVIÇOS DE INSTALAÇÃO DE FIREWALL:**
  - O aceite do serviço somente será dado após comprovação da instalação e o efetivo cumprimento de todas as configurações necessárias para funcionamento do equipamento dentro da estrutura da UFSM, como, por exemplo, a migração das regras de firewall existentes.

7.2. Procedimentos de Teste e Inspeção

- Previamente ao recebimento definitivo da solução serão realizados a verificação, testes e inspeção do atendimento integral às especificações técnicas exigidas. Estas ações serão realizadas por equipe designada pelo Diretor do Centro de Processamento de Dados acompanhados dos fiscais do contrato.
- Inicialmente deverá ser realizada a verificação das especificações exigidas através da inspeção física dos equipamentos, análise dos manuais técnicos enviados juntamente com os equipamentos ou disponibilizados de alguma forma e da análise

de informações disponibilizadas no site da fabricante. Para esta etapa deve-se observar a seguinte lista de verificação:

- Verificar se a caixa do equipamento foi entregue lacrada, em embalagem original e apresentando identificações de marca e modelo de acordo a descrição da proposta da CONTRATADA;
- Verificar se o equipamento está novo e sem uso;
- Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;
- Verificar se o equipamento foi entregue acompanhado de todos os acessórios previstos nas especificações técnicas (como cabo de energia, conectores, etc.) e descritos na documentação apresentada junto com a proposta da CONTRATADA;
- Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);
- Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);
- Verificar se os equipamentos foram recebidos de forma que funcionem na tensão elétrica 220 V.

Após, deverá ser conduzida a inspeção através da verificação da conformidade da execução dos serviços em relação aos requisitos exigidos nas especificações técnicas. Para avaliação, serão considerados relatórios das ferramentas, verificação das configurações, testes de uso das funcionalidades, documentações de projeto, manuais das soluções e quaisquer outros documentos pertinentes.

- Para esta etapa deve-se observar a seguinte lista de verificação:
  - Conectar cabos de alimentação e verificar funcionamento dos equipamentos;
  - Conectar cabos UTP e fibra óptica, e verificar funcionamentos das portas dos equipamentos;
  - Realizar configurações relacionadas à rede (configuração de interfaces, endereços IP, roteamento, resolução de nomes (DNS);
  - Realizar a criação de objetos, de políticas de segurança e regras de firewall;
  - Realizar a configuração do serviço DHCP;
  - Configurar modo de alta disponibilidade, com um firewall em modo ativo e outro em modo passivo;
  - Verificar a sincronização entre equipamentos (firewall ativo e passivo);
  - Verificar o funcionamento do modo de alta disponibilidade, através da simulação de falta de conexão no firewall configurado em modo ativo;
  - Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Universidade para monitoramento de ativos de rede;
  - Realizar a configuração do software de gerenciamento centralizado e armazenamento de logs, e verificar a integração e sincronismo entre os o firewall e o software;

- Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;
- Testar as seguintes funcionalidades no firewall:
  - Detecção de intrusão (Intrusion Prevention System - IPS) de tráfego malicioso;
  - Decriptografar tráfego SSL para inspeção de conteúdo;
  - Permitir inspeção em camada 7 (nível de aplicação);
  - Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos e desconhecidos;
  - Permitir a distribuição de endereços IPv4 e IPv6 para clientes, através do serviço DHCP;
  - Realizar a tradução de endereços IP: NAT (Network Address Translation);
  - Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Universidade remotamente;
  - Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base LDAP existente;
  - Permitir que a autenticação da rede sem fio seja integrada (single sign on) com a solução de WIFI existente, marca Cisco, controladora modelo 5508;
  - Deverá ser analisada a performance da solução na infraestrutura da UFSM, verificando principalmente possíveis perdas de pacotes durante o uso da solução com todas as funcionalidades de inspeção e IPS/IDS ativas simultaneamente;
  - Realizar testes de performance, com ênfase no throughput, utilizando ferramentas capazes de gerar relatórios relacionados a largura de banda;
  - Também deverá ser realizado um método comparativo de verificação entre os requisitos da solução e os prospectos do fabricante.

- A Metodologia de Avaliação da Qualidade será realizada pela Contratante, de acordo com a avaliação das seguintes condições que deverão ser cumpridas pela Contratada:
  - O cumprimento dos prazos e outras obrigações assumidas pela contratada;
  - Entrega da documentação exigida;
  - Atendimento dos critérios de aceitação;
  - Execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados no suporte técnico e;
  - A Metodologia de Avaliação da Qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico especializado junto com as solicitações de garantia;
  - Durante a vigência do suporte técnico, A fiscalização técnica dos contratos avaliará constantemente a prestação do serviço e usará como indicador a tabela disponível no item 7.3. Níveis Mínimos de Serviço Exigidos;

- A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las de maneira presencial ou através de documentação, em qualquer momento da contratação.

7.3. Níveis Mínimos de Serviço Exigidos

- Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website ou e-mail. O suporte deverá estar disponível na modalidade de 24x7 (24 horas por dia, 7 dias por semana).
    - O suporte deverá respeitar os seguintes tempos de resposta para os níveis de severidade abaixo:
        - a. Crítica: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deverá ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);
        - b. Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deverá ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
        - c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
        - d. Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial.

7.4. Sanções Administrativas

Id	Ocorrência	Glosa / Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 1% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato,	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo

	comportar-se de modo inidôneo ou cometer fraude fiscal.	das demais cominações legais, e multa de 10% do estimado da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar que não possui idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual. Aplicação de multa de 10% sobre o valor do contrato.
5	Não executar total ou parcialmente os serviços/materiais previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual. Aplicação de multa de 10% sobre o valor do contrato.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 10% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	A Contratada será declarada impedida de licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual. Aplicação de multa de 5% sobre o valor do contrato.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 8 (oito) horas úteis.	Multa de 0,1% (um décimo por cento) sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela CONTRATANTE, até o limite de 7 dias úteis.
		Após o limite de 7 dias úteis, aplicar-se-á multa de 1% (cinco por cento) do valor total do Contrato.

9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc.).	A Contratada será declarada impedida de licitar ou contratar com a Administração Pública pelo prazo de 12 (doze) meses, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada impedida de licitar ou contratar com a Administração Pública pelo prazo de 12 (doze) meses, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será declarada impedida de licitar ou contratar com a Administração Pública pelo prazo de 12 (doze) meses, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
13	Atraso na resolução de chamados de suporte técnico	Chamados de suporte técnico com severidade Baixa: Advertência.
		Chamados de suporte técnico com severidade Média: Multa de 0,11% do valor total do Contrato.
		Chamados de suporte técnico com severidade Alta: Multa de 0,30% do valor total do Contrato.
		Chamados de suporte técnico com severidade Crítica: Multa de 1% do valor

		total do Contrato.
14	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 10% do valor total do Contrato.

7.5. Do Pagamento

O pagamento será efetuado mediante a apresentação da Nota Fiscal, devidamente certificada, acusando o recebimento, por parte do responsável pelo órgão solicitante/UFSM. O prazo para pagamento será de no máximo 30 (trinta) dias a partir da data de sua entrega na UFSM, desde que não haja impedimento legal.

8 – Modelo de proposta

Id.	Descrição do Bem ou Serviço	Quantidade	Unidade de medida	Valor unitário	Valor total
1	FIREWALL COM SUPORTE, GARANTIA DE 03 ANOS	2	Peça		
2	AQUISIÇÃO DE LICENÇAS: THREAT PREVENTION, DNS SECURITY, WILDFIRE, URL FILTERING	2	Licença		
3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	2	Serviço		

9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

Trata-se de Sistema de Registro de Preços e a fonte de recursos deverá ser informada no momento da contratação.

10 – DA VIGÊNCIA DO CONTRATO

O contrato vigorará por 48 (quarenta e oito) meses, contados a partir da data da sua assinatura.

11 – DO REAJUSTE DE PREÇOS

Em caso de reajuste, será utilizado o IPCA-E.

12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

O certame será realizado na forma de licitação para REGISTRO DE PREÇOS, na modalidade PREGÃO, do tipo MENOR PREÇO GLOBAL.

12.2. Critérios de Julgamento das Propostas

- Durante a apresentação da proposta, a licitante deverá demonstrar que o produto ofertado atende às exigências solicitadas nesta especificação. Para esta comprovação, serão aceitos catálogos, datasheets, manuais, sites ou outra documentação oficial onde se possa identificar de maneira inequívoca o modelo de equipamento proposto.
- Em caso de dúvidas na comprovação da especificação, poderão ser solicitados por meio de diligência, esclarecimentos sobre a especificação dos produtos cotados pela licitante.
- A licitante deverá apresentar declaração de que o produto atende a todas especificações exigidas.

12.3 Critérios de Qualificação Técnica para a Habilitação

- Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação da seguinte documentação complementar:
    - Atestado de Capacidade Técnica demonstrando que a proponente forneceu equipamentos, para pessoa física ou jurídica de direito público ou privado, e realizou a instalação de solução de firewall de próxima geração compatível com o objeto deste termo de referência;
    - O atestado acima referido deverá conter identificação do emitente, características e localização da prestação do serviço, local, data da expedição e declaração do emitente do atestado de que o serviço foi realizado a contento.
    - O atestado deverá ser em nome da LICITANTE, e elaborados em papel

timbrado da empresa emitente, contendo os seguintes dados mínimos e obrigatórios:

- a) Razão Social, CNPJ e endereço completo da empresa emitente;
- b) Razão Social da LICITANTE;
- c) Vigência: de __/__ /__ a __/__ /__;
- d) Objeto do contrato;
- e) Descrição do objeto do contrato: (descrição detalhada dos serviços prestados);
- f) Local e Data de emissão do Atestado;
- g) Nome, assinatura do signatário, telefone e e-mail de contato da empresa emitente.

13 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

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** Jéssica Lasch de Moura Analista de TI Matrícula/SIAPE: 2355540	_____ **Integrante Requisitante** Lucimara Dalla Porta Menezes Friedrich Técnico de TI Matrícula/SIAPE: 2265885	_____ **Integrante Requisitante** Eduardo Schwanck Saraiva Administrador Matrícula/SIAPE: 1831047
Santa Maria, 25 de outubro de *2022*.		

_____	_____

Integrante Técnico	**Integrante Administrativo**
Alexandre Silva Rodrigues Analista de TI Matrícula/SIAPE: 2997477	Alessandra Daniela Bavaresco Técnico em Contabilidade Matrícula/SIAPE: 1089281
Santa Maria, 25 de outubro de *2022*.	

Autoridade Máxima da Área de TIC
_____ *Fábio André Barcelos* *Diretor Substituto do Centro de Processamento de Dados* Matrícula/SIAPE: 1345246
Santa Maria, 25 de outubro de *2022*.

Aprovo,

Autoridade Competente
_____ Alessandra Daniela Bavaresco Diretor de Departamento Executivo Matrícula/SIAPE: 1089281
Santa Maria, 25 de outubro de *2022*.

ANEXO I

Termo de Compromisso e Manutenção de Sigilo

A _____, CNPJ _____, por intermédio de seu representante legal abaixo assinado, _____,CPF_____, doravante designados simplesmente CONTRATADA e RESPONSÁVEL, se comprometem, por intermédio do presente TERMO DE COMPROMISSO, a não divulgar sem autorização, quaisquer Informações Confidenciais (conforme definido abaixo) em relação ao Projeto de "Aquisição de Next Generation Firewall para a Universidade Federal de Santa Maria" e de propriedade da Universidade Federal de Santa Maria, CNPJ 95.591.764/0001-05, doravante designada UFSM, em conformidade com as seguintes cláusulas e condições:

1. Por este instrumento, a Contratada declara estar apta a aceitar e receber INFORMAÇÕES com respeito ao parque tecnológico da UFSM, se comprometendo a manter absoluta confidencialidade destas INFORMAÇÕES, independente de solicitação expressa neste sentido pela UFSM ou quaisquer de seus representantes;
2. As INFORMAÇÕES abrangidas por este termo são de natureza técnica, operacional, comercial, jurídica e financeira expressas de forma escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, ficando expressamente vedada sua divulgação a terceiros, a qualquer título;
3. As partes deverão restringir a divulgação das INFORMAÇÕES para o pessoal que estiverem diretamente envolvidos na sua utilização em razão do fornecimento das INFORMAÇÕES e da elaboração do serviço a ser fornecido, ficando vedado o intercâmbio destas INFORMAÇÕES com terceiros que não estejam diretamente envolvidos com a prestação dos serviços;
4. A CONTRATADA obriga-se a informar imediatamente a UFSM qualquer violação das regras de sigilo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço;
1. A CONTRATADA deverá prestar obediência às políticas de segurança da informação vigentes na Universidade Federal de Santa Maria ou que poderão ser instituídas durante a vigência do contrato;
5. A não observância de qualquer das disposições estabelecidas neste instrumento sujeitará a CONTRATADA aos procedimentos judiciais cabíveis relativos a perdas e danos que possam advir ao UFSM e aos seus usuários;
6. O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal de acordo com as leis aplicáveis dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Gestor do Contrato da UFSM:

_____

Representante da Contratada:

_____

Local, UF, _____ de _____ de _____.

ANEXO II

Termo de Ciência

IDENTIFICAÇÃO DO CONTRATO

Contrato n°:

Objeto: “Aquisição de Next Generation Firewall para a Universidade Federal de Santa Maria”

Contratada:

CNPJ:

Representante da Contratada:

CPF:

Pelo presente instrumento, o(s) funcionário(s) abaixo qualificado(s) e assinado(s) declara(m):

2. Ter plena ciência e conhecimento do Termo de Compromisso e Manutenção de Sigilo firmado pela CONTRATADA;
3. Ter conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deverá ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo;
4. Comprometer-se a guardar sigilo necessário sobre todas as informações que eventualmente venha(m) a tomar conhecimento;
5. Comprometer-se a prestar obediência às políticas de segurança da informação vigentes na Universidade Federal de Santa Maria ou que poderão ser instituídas durante a vigência do contrato.

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome:

CPF:

Função/Cargo:

_____

Assinatura

Nome:

CPF:

Função/Cargo:

_____

Assinatura

Local, UF, _____ de _____ de _____.