

# **TERMO DE REFERÊNCIA**

## **PE 158/2020**

**Processo Administrativo nº 23081.038263/2020-96**

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

Santa Maria, 09 de novembro de 2020.

## Sumário

1 - OBJETO DA CONTRATAÇÃO	4
2 - DESCRIÇÃO DA SOLUÇÃO DE TIC	4
2.1. Bens e serviços que compõem a solução	4
3 – JUSTIFICATIVA PARA A CONTRATAÇÃO	5
3.1. Contextualização e Justificativa da Contratação	5
3.2. Alinhamento aos Instrumentos de Planejamento Institucionais	7
3.3. Estimativa da demanda	8
3.4. Parcelamento da Solução de TIC	8
3.5. Resultados e Benefícios a Serem Alcançados	8
4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO	9
4.1. Requisitos de Negócio	9
4.2. Requisitos de Capacitação	9
4.3. Requisitos Legais	9
4.4. Requisitos de Manutenção	10
4.5. Requisitos Temporais	11
4.6. Requisitos de Segurança	11
4.7. Requisitos Sociais, Ambientais e Culturais	11
4.8. Requisitos de Arquitetura Tecnológica - especificação técnica	12
4.8.1. Item 1: Firewall com suporte, garantia e licenças de proteção com vigência de 03 anos	12
1. Requisitos técnicos gerais	12
2. Controle por política de Firewall	15
3. Controle de aplicações	16
4. Prevenção de ameaças	17
5. Análise de malwares modernos	20
6. Filtro de URL	20
7. Identificação de usuários	21
8. QOS	22
9. Filtro de dados	22
10. VPN	22
11. CONSOLE DE GERÊNCIA E MONITORAÇÃO	24
Item 2: Software de gestão centralizada e armazenamento de logs com suporte e garantia de 03 anos	27
1. Requisitos técnicos	27

4.8.3. Item 3: Serviços de instalação de firewall	28
1. Requisitos técnicos	28
4.8.4. Item 4: Treinamento oficial de firewall	28
1. Requisitos técnicos	28
4.9. Requisitos de Projeto e de Implementação	29
4.10. Requisitos de Implantação	29
4.11. Requisitos de Garantia	30
4.12. Requisitos de Experiência Profissional	30
4.13. Requisitos de Formação da Equipe	30
4.14. Requisitos de Metodologia de Trabalho	30
4.15. Requisitos de Segurança da Informação	30
5 – RESPONSABILIDADES	31
5.1. Deveres e responsabilidades da CONTRATANTE	31
5.2. Deveres e responsabilidades da CONTRATADA	32
5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços	32
6 – MODELO DE EXECUÇÃO DO CONTRATO	33
6.1. Rotinas de Execução	33
6.2. Quantidade mínima de bens ou serviços para comparação e controle	34
6.3. Mecanismos formais de comunicação	34
6.4. Manutenção de Sigilo e Normas de Segurança	34
7 – MODELO DE GESTÃO DO CONTRATO	34
7.1. Critérios de Aceitação	34
7.2. Procedimentos de Teste e Inspeção	35
7.3. Níveis Mínimos de Serviço Exigidos	37
7.4. Sanções Administrativas	38
7.5. Do Pagamento	40
8 – Modelo de proposta	40
9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO	41
10 – DA VIGÊNCIA DO CONTRATO	41
11 – DO REAJUSTE DE PREÇOS	41
12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR	41
12.1. Regime, Tipo e Modalidade da Licitação	41
12.2. Critérios de Julgamento das Propostas	42
12.3 Critérios de Qualificação Técnica para a Habilitação	42
ANEXO I	43
ANEXO II	44

## 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 para segurança da informação de perímetro que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance conforme quantidades e exigências estabelecidas neste Termo de Referência.

### 2 - DESCRIÇÃO DA SOLUÇÃO DE TIC

Como visto no Estudo Técnico Preliminar, a melhor e mais viável solução para a Universidade é um **Firewall de Próxima Geração (NGFW)**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela equipe segurança da informação e necessidades da UFSM. Além disso, realizou-se uma pesquisa junto a algumas universidades federais que possuem uma infraestrutura de TI semelhante a infraestrutura da UFSM. Entre as universidades consultadas, todas elas já possuem esse tipo de solução implementada e apresentaram relatos positivos sobre os resultados obtidos após suas implementações, tendo em vista os níveis de segurança proporcionados a suas infraestruturas e facilidade de gerenciamento. Vale ressaltar que uma dessas universidades relatou que utilizava uma solução semelhante a que a UFSM utiliza, com diversos servidores PFSense e tinha os mesmos problemas de performance e gerenciamento, e conseguiu resolver tais problemas através da aquisição de um NGFW. Cabe ainda citar que as soluções de Firewall de Próxima Geração possuem recursos de funcionamento em cluster, que permite contratar solução com capacidade para atender a demanda existente, e no futuro adicionar outros equipamentos no mesmo cluster, aumentando a capacidade de processamento e throughput, preservando o investimento já realizado. Por esta razão, serão registrados 4 equipamentos na modalidade de Registro de Preços, prevendo um possível crescimento neste período de 36 meses.

Dessa forma, pode ser realizada a contratação de 2 equipamentos, capazes de atender a demanda de 5 Gbps com redundância. Essa demanda se justifica pelo link atual que a Universidade possui (3 Gbps) somado ao tráfego que não é filtrado pelo firewall (entre hosts da rede interna). No caso de o link ser expandido futuramente, uma nova contratação poderá ser realizada, e os novos equipamentos poderão operar em cluster, junto aos equipamentos já existentes (primeira contratação).

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	4	Peça

	LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS		
2	SOFTWARE DE GESTÃO CENTRALIZADA E ARMAZENAMENTO DE LOGS COM SUPORTE E GARANTIA DE 03 ANOS	1	Licença
3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	4	Serviço
4	TREINAMENTO OFICIAL DE FIREWALL	5	Serviço

### 3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

#### 3.1. Contextualização e Justificativa da Contratação

Atualmente, a Universidade Federal de Santa Maria disponibiliza uma infraestrutura de TI para cerca de 20.000 (vinte mil) usuários da comunidade acadêmica, sendo composta por alunos, professores e técnicos administrativos em educação. A equipe de Segurança da Informação, parte da Divisão de Suporte, é composta por três 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.

No momento, a UFSM conta com uma solução de firewall baseada em software livre, denominada PFSense. Esse firewall oferece 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 é baseada na filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e transporte do modelo OSI. Dessa forma, ele atua apenas com base nos cabeçalhos dos pacotes da camada de rede (IPv4, IPv6 e ICMP) e da camada de transporte (UDP e TCP). Assim, é possível criar regras apenas com base nos endereços IP (origem e/ou destino), portas (origem e/ou destino) e protocolos citados anteriormente.

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

Além disso, com base na maior utilização de dispositivos e sistemas computacionais, é importante observar o aumento da demanda de uso da banda de Internet existente na UFSM. Isso se deve ao fato de que, com o passar dos anos, a infraestrutura de TI desta Universidade cresceu muito com a disseminação da Internet móvel, permitindo a proliferação dos dispositivos pessoais dentro desta Infraestrutura, e considerando a evolução das aplicações e métodos de criptografia SSL utilizados na maioria das conexões existentes acarretou em extrema complexidade para a gestão da segurança da Informação. Em virtude desse maior consumo da banda, a solução de firewall atual sofre problemas de performance. Esse aspecto torna-se mais importante em um cenário de expansão de link. Assim, cabe mencionar que existe uma negociação de ampliação dos links, através de Rede Nacional de Pesquisas (RNP) para 5 Gbps e posteriormente, 10 Gbps. Embora sem uma expectativa de prazo, espera-se que aconteça dentro dos próximos 3 anos.

Conforme demonstrado no Estudo Técnico Preliminar, a solução de firewall atual não suportaria um aumento na banda disponível ou a implementação de novos mecanismos de segurança, pois, atualmente a solução em questão já trabalha com o máximo da sua capacidade. Nesse caso, isso ocasionaria frequentes perdas e necessidade de retransmissão de pacotes, o que reflete em atrasos no tráfego de dados, ou seja, uma lentidão na rede, a qual pode ser percebida pelos usuários em momentos de maior utilização.

Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração, possibilita a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso seria possível ter uma visualização detalhada da utilização da rede e das aplicações utilizadas. Com isso, o processo de identificação de ameaças é facilitado e permite a aplicação de políticas de segurança mais eficientes. Outra funcionalidade importante que pode ser implementada é a identificação de usuários que utilizam a rede e o registro de conexões. Essas informações são extremamente importantes, seja para realizar a adequação ao Marco Civil da Internet ou para realizar o tratamento de incidentes de segurança notificados pelo CAIS (Centro de Atendimento a Incidentes de Segurança). No cenário atual, essas informações muitas vezes são ineficientes, visto que a arquitetura implementada não possibilita armazenar tais informações. Nesse contexto, é importante destacar o gerenciamento e armazenamento dessas informações. Um firewall de próximo geração oferece isso de forma interessante, sendo possível gerar relatórios de forma rápida e detalhada sobre tudo o que acontece na rede. Além disso, é importante que o firewall possa ser integrado a solução de rede Wireless já implementada na Universidade através da autenticação Single Sign On. Assim, o firewall teria informações sobre os usuários conectados à rede sem fio.

Neste ano, a Lei Geral de Proteção de Dados nº 13.709, de 14 de agosto de 2018, entrou em vigência, ampliando as exigências do Marco Civil da Internet e reforçando a utilização de melhores práticas de mercado no que tange aspectos da Segurança da Informação. Tal Lei, a partir de 2021 passa a aplicar sanções administrativas pesadas para entidades privadas e públicas de até R\$ 50.000.000,00 (cinquenta milhões de reais) por infração. A exemplificar, no caso de vazamento de informações de algum banco de dados de usuários desta Instituição, caracterizaria infração e aplicação de sanção.

Ao contar apenas com três analistas na equipe de segurança da informação, por motivos de férias, recesso ou licença é comum a equipe em trabalho manter uma rotina reduzida de pessoal. Soluções de software livre carecem de padronização e permitem muitas customizações com patches e add-ons o que dificulta a administração em equipe. Como as regras e configurações são manuais, cada administrador pode interagir de forma diferente com a ferramenta, a exemplificar, no caso de criação/modificação de funcionalidades por um administrador que entrou de férias, o outro pode assumir conduta de configuração totalmente diferente e ainda não conseguir entender exatamente o que o administrador anterior realizou. Ainda a exemplificar num pior cenário, onde apenas um administrador da equipe detém de conhecimento avançado das modificações realizadas ao longo dos anos, caso ele venha a deixar a instituição, a equipe ficaria sem amparo para manter a solução. Outro motivador desta contratação é o simples fato de que a solução atual não possui qualquer suporte ou garantia de funcionamento. Soluções baseadas em software livre dependem do trabalho não remunerado da comunidade de desenvolvedores, portanto, não é possível manter central de atendimento ao usuário com prazos de SLA, ou sequer garantir que o sistema esteja livre de vulnerabilidades ou falhas. Neste aspecto, esta Universidade vem enfrentando ao longo destes anos dificuldades para identificar e corrigir problemas quando estes acontecem no firewall, sendo que alguns até hoje ainda não foram sanados. Portanto, pode-se destacar que aquisição de um firewall de próxima geração é um investimento que apresentará grandes benefícios para toda a comunidade acadêmica. Isso evidencia-se por ele trazer um maior nível de segurança a todos usuários da rede e a todos

equipamentos ativos na rede sistemas computacionais disponibilizados pela UFSM, além de garantir mais eficiência e qualidade para utilizar a Internet.

### 3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

<b>ALINHAMENTO AOS PLANOS ESTRATÉGICOS</b>	
<b>ID</b>	<b>Objetivos Estratégicos (2016-2026) do Plano de Desenvolvimento Institucional</b>
<b>PR-D5-01</b>	Otimizar as rotinas administrativas e os sistemas de informação, primando pela agilidade, desburocratização, transparência e qualidade das informações e da gestão.
<b>AI-D2-03</b>	Oferecer uma infraestrutura de apoio qualificada e de acordo com as necessidades de cada área de conhecimento.
<b>AI-D5-03</b>	Modernizar a infraestrutura de TI para suportar as necessidades acadêmicas e administrativas.
<b>PR-D2-01</b>	Fortalecer aprendizado extraclasse, oportunizando atividades de extensão, inserção na sociedade, empreendedorismo, pesquisa e inovação.

<b>ALINHAMENTO AO PDTIC</b>
O Plano Diretor de Tecnologia da Informação 2020 ainda não foi aprovado na UFSM. O PDTI está em fase de construção e está sendo elaborado de acordo com as diretrizes do Plano de Desenvolvimento Institucional.

<b>ALINHAMENTO AO PAC 2020</b>	
<b>Item</b>	<b>Descrição</b>

<b>1933</b>	<p>FIREWALL</p> <p>Código do item: 150100</p> <p>Tipo de item: Soluções de TIC</p> <p>Subitem: MATERIAIS DE TIC</p>
-------------	---

### **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:

<b>GRUPO</b>	<b>Item</b>	<b>Descrição</b>	<b>QTD</b>
1	1	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS	4
	2	SOFTWARE DE GESTÃO CENTRALIZADA E ARMAZENAMENTO DE LOGS COM SUPORTE E GARANTIA DE 03 ANOS	1
	3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	4
	4	TREINAMENTO OFICIAL DE FIREWALL	5

### **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);

- 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 pode não ter conhecimento técnico suficiente para manter em operação, deverão fazer parte da aquisição treinamentos específicos que deverão ser conduzidos pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.
- O treinamento deverá ser ministrado em Língua Portuguesa/Brasil e seus principais requisitos estão descritos no item 4.8. Requisitos de Arquitetura Tecnológica - especificação técnica do presente Termo de Referência.

### **4.3. Requisitos Legais**

- Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade

ambiental contidos no Art. 5º da Instrução Normativa nº 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 nº 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 nº 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.
- Da Portaria Nº 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:
  - o Durante o prazo de garantia, deverá ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correções.
  - o Durante o prazo de garantia, deverá ser possível realizar a atualização das assinaturas de proteção da solução.
- Manutenção corretiva:
  - o 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;
  - o 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
  - o 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 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.
- o 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 poder 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, garantia e licenças de proteção com vigência 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), e console de gerência e monitoração;
- 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. O hardware e software que executem as funcionalidades console de gerência e monitoração, deverão ser do tipo appliance físico ou virtual;
- 1.7. 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;
- 1.8. O software do appliance deverá ser fornecido em sua versão mais atualizada;
- 1.9. Deverá possuir um throughput mínimo de 5 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, Antimalware, Antivírus e Antispyware;
- 1.10. 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 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;
- 1.11. 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);
- 1.12. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.
- 1.13. Suporte a, no mínimo, 1.000.000 de conexões simultâneas;
- 1.14. Suporte a, no mínimo, 10.000 novas conexões por segundo;

- 1.15. Possuir fonte 120/240 AC ou DC, redundante e hot-swappable;
- 1.16. Deverá possuir Disco Solid State Drive (SSD), com no mínimo, 240 GB;
- 1.17. Deverá possuir, no mínimo, 04 interfaces de rede 10 Gbps SFP+;
- 1.18. Deverá possuir, no mínimo, 05 interfaces de rede RJ-45 10/100/1000 Mbps, estando incluída uma interface para gerenciamento;
- 1.19. 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;
- 1.20. Deverá possuir, no mínimo, 1 (uma) interface do tipo console ou similar;
- 1.21. Deverá ser incluído 8 (oito) módulos transceivers 10 GE SFP+;
  - 1.21.1. Deverá ser do tipo bidirecional (transmissão e recepção utilizando apenas uma fibra óptica);
  - 1.21.2. Deverá ser do tipo short range;
  - 1.21.3. Os módulos transceivers devem ser compatíveis com switches dos seguintes fabricantes: Cisco, HP, Huawei e Extreme;
- 1.22. Deverá suportar, no mínimo, 60 (sessenta) zonas de segurança;
- 1.23. Deverá estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) clientes de VPN SSL simultâneos;
- 1.24. Deverá estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) túneis de VPN IPSEC simultâneos;
- 1.25. Deverá suportar, no mínimo, 1 (um) sistema virtual lógico (Contexto) no firewall Físico;
- 1.26. Os contextos virtuais deverão suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
- 1.27. 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;
- 1.28. 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;
- 1.29. A solução deverá possuir pelo menos as seguintes funcionalidades:
  - 1.29.1. Suportar sub-interfaces ethernet lógicas;
  - 1.29.2. Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de firewall;
  - 1.29.3. 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;
- 1.30. Deverá suportar os seguintes tipos de NAT:
  - 1.30.1. Nat dinâmico (Many-to-1);
  - 1.30.2. Nat dinâmico (Many-to-Many);
  - 1.30.3. Nat estático (1-to-1);
  - 1.30.4. NAT estático (Many-to-Many);
  - 1.30.5. Nat estático bidirecional 1-to-1;

- 1.30.6. Tradução de porta (PAT);
- 1.30.7. NAT de Origem;
- 1.30.8. NAT de Destino;
- 1.30.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
- 1.31. A solução deverá possuir as seguintes funcionalidades:
  - 1.31.1. Suporte a 4094 VLAN Tags 802.1q;
  - 1.31.2. Agregação de links 802.3ad e LACP;
  - 1.31.3. Policy based routing ou policy-based forwarding;
  - 1.31.4. DHCP Relay;
  - 1.31.5. DHCP Server;
  - 1.31.6. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
- 1.32. Deverá implementar balanceamento de link através de políticas por usuário e/ou grupos de usuários do LDAP/AD;
- 1.33. Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino;
- 1.34. 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;
- 1.35. Deverá os registros de logs para sistemas de monitoração externos, simultaneamente. Deverá haver a opção de enviar logs via protocolo TCP e SSL;
- 1.36. Deverá permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
- 1.37. 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;
- 1.38. Deverá implementar Proteção contra anti-spoofing;
- 1.39. Deverá permitir bloquear sessões TCP que usarem variações do 3-way handshake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
- 1.40. Deverá permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
- 1.41. 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;
- 1.42. 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 (I2) e camada 3 (I3);
  - 1.42.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
  - 1.42.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
  - 1.42.3. 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;
- 1.42.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 1.43. Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
  - 1.43.1. Em modo transparente;
  - 1.43.2. Em layer 3;
- 1.44. A configuração em alta disponibilidade deverá sincronizar:
  - 1.44.1. Sessões;
  - 1.44.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
  - 1.44.3. Certificados decryptografados;
  - 1.44.4. Associações de Segurança das VPNs;
  - 1.44.5. Tabelas FIB;
  - 1.44.6. O HA (modo de Alta-Disponibilidade) deverá possibilitar monitoração de falha de link.
- 1.45. As funcionalidades de firewall, IDS/IPS, identificação de usuários, controle de aplicações, VPN IPsec e SSL, QOS, criptografia 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 criptografia 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 decryptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- 2.8. Deverá permitir decryptografar 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 decryptografia 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 decryptografado (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 as 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 decifrar 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. Prevenção de ameaças**

- 4.1. Para proteção do ambiente contra ataques, a solução deverá possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 4.2. Deverá ser capaz de identificar e bloquear as seguintes ameaças: vírus, trojans, spywares, ransomwares e demais tipos de malwares;

- 4.3. Deverá permitir a inclusão de assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 4.4. As funcionalidades de IPS, Antivírus e Anti-Spyware deverão operar em carácter 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;
- 4.5. Deverá permitir sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/passivo;
- 4.6. 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;
- 4.7. Deverá permitir detectar e prevenir ameaças em tráfegos HTTP/2;
- 4.8. Deverá permitir ativar ou desativar as assinaturas, ou ainda habilitá-las apenas em modo de monitoração;
- 4.9. Deverá permitir exceções por IP de origem ou de destino deverão ser possíveis nas regras, de forma geral e assinatura a assinatura;
- 4.10. 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;
- 4.11. Deverá permitir o bloqueio de vulnerabilidades;
- 4.12. Deverá permitir o bloqueio de exploits conhecidos;
- 4.13. Deverá incluir proteção contra ataques de negação de serviços (DoS);
- 4.14. Deverá permitir a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;
- 4.15. Deverá possuir os seguintes mecanismos de inspeção de IPS:
  - 4.15.1. Análise de padrões de estado de conexões;
  - 4.15.2. Análise de decodificação de protocolo;
  - 4.15.3. Análise para detecção de anomalias de protocolo;
  - 4.15.4. Análise heurística;
  - 4.15.5. IP Defragmentation;
  - 4.15.6. Remontagem de pacotes de TCP;
  - 4.15.7. Bloqueio de pacotes malformados;
- 4.16. Deverá ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;
- 4.17. Deverá detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
- 4.18. Deverá bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 4.19. 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;
- 4.20. Deverá possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 4.21. Deverá possuir assinaturas para bloqueio de ataques de buffer overflow;
- 4.22. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 4.23. 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;
- 4.24. Deverá permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
  - 4.25. Deverá suportar bloqueio de arquivos por tipo;
  - 4.26. Deverá identificar e bloquear comunicação com botnets;
  - 4.27. Deverá suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
  - 4.28. Deverá suportar referência cruzada com CVE;
  - 4.29. 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;
  - 4.30. Deverá suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;
  - 4.31. 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;
  - 4.32. 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;
  - 4.33. Deverá permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
  - 4.34. Deverá incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
  - 4.35. Deverá incluir proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos;
  - 4.36. Deverá incluir rastreamento de vírus em PDF;
  - 4.37. Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
  - 4.38. 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.
  - 4.39. Deverá possuir a capacidade de detectar e bloquear tentativas de resolução de domínios gerados de forma automática através de algoritmos (Domain generation algorithm - DGA);
  - 4.40. Deverá mostrar nos logs as seguintes informações sobre domínios DGA:
    - 4.40.1. Domínio suspeito identificado;
    - 4.40.2. ID de assinatura de detecção;
    - 4.40.3. Usuário logado na estação/servidor que originou o tráfego;
    - 4.40.4. Aplicação;
    - 4.40.5. Porta de destino;
    - 4.40.6. IP de origem;
    - 4.40.7. IP de destino;
    - 4.40.8. Horário;
    - 4.40.9. Ação do firewall;
    - 4.40.10. Severidade;
  - 4.41. 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

- 4.42. A análise automática deverá incluir, no mínimo, as seguintes características:
  - 4.42.1. Padrões de consulta;
  - 4.42.2. Entropia;
  - 4.42.3. Análise de frequência n-gram de domínios;
  - 4.42.4. Taxa de consultas.

## **5. Análise de malwares modernos**

- 5.1. 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;
- 5.2. 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;
- 5.3. Deverá ser capaz de enviar arquivos trafegados de forma automática para análise, onde o arquivo será executado e simulado em ambiente controlado;
- 5.4. 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;
- 5.5. 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.;
- 5.6. Deverá suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistemas operacionais Windows;
- 5.7. 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;
- 5.8. 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;
- 5.9. Deverá permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
- 5.10. 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;
- 5.11. Deverá suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 5.12. 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;
- 5.13. Deverá permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API;
- 5.14. Deverá permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução.

## **6. Filtro de URL**

- 6.1. A solução deverá possuir as seguintes funcionalidades de filtro de URL:
  - 6.1.1. 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);
- 6.1.2. Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;
- 6.1.3. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
- 6.1.4. 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;
- 6.1.5. Deverá permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
- 6.1.6. 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;
- 6.1.7. Deverá suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
- 6.1.8. Deverá permitir classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
- 6.1.9. Deverá permitir classificar sites em mais de uma categoria, de acordo com a necessidade;
- 6.1.10. A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;
- 6.1.11. Deverá permitir a criação categorias de URLs customizadas;
- 6.1.12. Deverá permitir a exclusão de URLs do bloqueio, por categoria;
- 6.1.13. Deverá permitir a customização de página de bloqueio;
- 6.1.14. 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;
- 6.1.15. 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);
- 6.1.16. Deverá permitir a inclusão nos logs do produto de informações das atividades dos usuários;
- 6.1.17. Deverá salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

## **7. Identificação de usuários**

- 7.1. 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;
- 7.2. Deverá permitir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 7.3. Deverá permitir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 7.4. Deverá permitir que a autenticação da rede com fio seja realizada através de captive portal;

- 7.5. 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);
- 7.6. Deverá permitir a autenticação via Kerberos;
- 7.7. 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;
- 7.8. 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;
- 7.9. Deverá permitir a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP;
- 7.10. Deverá permitir a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

## **8. QOS**

- 8.1. Deverá permitir controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda;
- 8.2. Deverá permitir a criação de políticas de QoS por:
  - 8.2.1. Endereço de origem;
  - 8.2.2. Endereço de destino;
  - 8.2.3. Por usuário e grupo do LDAP/AD;
  - 8.2.4. Por aplicações;
  - 8.2.5. Por porta;
- 8.3. O QoS deverá possibilitar a definição de classes por:
  - 8.3.1. Banda Garantida;
  - 8.3.2. Banda Máxima;
  - 8.3.3. Fila de Prioridade;
- 8.4. Deverá permitir marcação de pacotes Diffserv, inclusive por aplicação;
- 8.5. Deverá disponibilizar estatísticas RealTime para classes de QoS;
- 8.6. Deverá permitir QOS (traffic-shapping), em interface agregadas;
- 8.7. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes e sessões.

## **9. Filtro de dados**

- 9.1. Deverá permitir a criação de filtros para arquivos e dados pré-definidos;
- 9.2. Os arquivos deverão ser identificados por extensão e assinaturas;
- 9.3. Deverá permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre;
- 9.4. Deverá permitir a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 9.5. Deverá permitir listar o número de aplicações suportadas para controle de dados;
- 9.6. Deverá permitir listar o número de tipos de arquivos suportados para controle de dados.

## **10. VPN**

- 10.1. 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;

- 10.2. Deverá suportar VPN Site-to-Site e Client-To-Site;
- 10.3. Deverá suportar IPSec VPN;
- 10.4. Deverá suportar SSL VPN;
- 10.5. A VPN IPSEc deverá suportar:
  - 10.5.1. 3DES;
  - 10.5.2. Autenticação MD5 e SHA-1;
  - 10.5.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
  - 10.5.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
  - 10.5.5. AES 128, 192 e 256 (Advanced Encryption Standard)
  - 10.5.6. Autenticação via certificado IKE PKI.
- 10.6. Deverá possuir interoperabilidade com os seguintes fabricantes:
  - 10.6.1. Cisco;
  - 10.6.2. Checkpoint;
  - 10.6.3. Juniper;
  - 10.6.4. Palo Alto Networks;
  - 10.6.5. Fortinet;
  - 10.6.6. Sonic Wall;
- 10.7. 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 troubleshooting;
- 10.8. A VPN SSL deverá possuir os seguintes requisitos:
  - 10.8.1. Deverá permitir ao usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
  - 10.8.2. A funcionalidades de VPN SSL deverão ser atendidas com ou sem o uso de agente;
  - 10.8.3. Deverá permitir atribuição de endereço IP nos clientes remotos de VPN SSL;
  - 10.8.4. Deverá permitir a atribuição de IP fixos nos usuários remotos de VPN SSL;
  - 10.8.5. 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;
  - 10.8.6. 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;
  - 10.8.7. Deverá permitir a atribuição de DNS nos clientes remotos de VPN;
  - 10.8.8. 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;
  - 10.8.9. Deverá permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
  - 10.8.10. A VPN SSL deverá suportar proxy arp e uso de interfaces PPPOE;
  - 10.8.11. Deverá permitir autenticação via Radius, LDAP, OTP (One Time Password), certificado e base de usuários local;
  - 10.8.12. Deverá permitir a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada;
  - 10.8.13. 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;
  - 10.8.14. Deverá permitir leitura e verificação de CRL (certificate revocation list);

- 10.8.15. Deverá permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 10.8.16. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;
  - 10.8.16.1. Deverá permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
  - 10.8.16.2. Antes do usuário autenticar na estação;
  - 10.8.16.3. Após autenticação do usuário na estação;
  - 10.8.16.4. Sob demanda do usuário;
- 10.8.17. Deverá manter uma conexão segura com o portal durante a sessão.
- 10.9. O agente de VPN SSL client-to-site deverá ser compatível com pelo menos: Windows 7, Windows 8 e Mac OS;
- 10.10. 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;

## **11. CONSOLE DE GERÊNCIA E MONITORAÇÃO**

- 11.1. Deverá permitir centralizar a administração de regras e políticas, inclusive quando configurado em um cluster, usando uma única interface de gerenciamento;
- 11.2. O gerenciamento da solução deverá suportar acesso via SSH, cliente ou WEB (HTTPS);
- 11.3. Deverá permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall, com a possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
- 11.4. Caso haja a necessidade de instalação de cliente para administração da solução, o mesmo deve ser compatível com sistemas operacionais Windows e/ou Linux;
- 11.5. O gerenciamento deverá permitir/possuir:
  - 11.5.1. Criação e administração de políticas de firewall e controle de aplicação;
  - 11.5.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
  - 11.5.3. Criação e administração de políticas de Filtro de URL;
  - 11.5.4. Monitoração de logs;
  - 11.5.5. Ferramentas de investigação de logs;
  - 11.5.6. Debugging;
  - 11.5.7. Captura de pacotes;
- 11.6. Deverá permitir acesso concorrente de administradores;
- 11.7. Deverá permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
- 11.8. Deverá mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos;
- 11.9. Deverá permitir busca global na solução onde possa se consultar por: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo;
- 11.10. Deverá permitir busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- 11.11. Deverá permitir usar palavras chaves e/ou cores para facilitar identificação de regras;

- 11.12. Deverá permitir monitorar via SNMP falhas de hardware (por exemplo: fonte e discos), uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN client-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas. Caso alguma dessas informações não possam ser monitoradas via SNMP, elas deverão ser monitoradas e/ou exibidas via dashboard na interface gráfica (web e/ou cliente);
- 11.13. Deverá permitir bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- 11.14. Deverá permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 11.15. Deverá permitir autenticação integrada ao servidor Radius;
- 11.16. Deverá permitir a localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- 11.17. Deverá definir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
- 11.18. Deverá permitir a criação de regras que fiquem ativas em horário definido;
- 11.19. Deverá permitir a criação de regras com data de expiração;
- 11.20. Deverá permitir backup das configurações e rollback de configuração para a última configuração salva;
- 11.21. Deverá permitir Rollback de Sistema Operacional para a última versão local;
- 11.22. Deverá permitir upgrade via SCP, TFTP e interface de gerenciamento;
- 11.23. Deverá permitir validação de regras antes da aplicação;
- 11.24. Deverá permitir validação de configurações antes da aplicação das mesmas permitindo identificar erros;
- 11.25. Deverá permitir análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos;
- 11.26. Deverá permitir a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.
- 11.27. Deverá permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação à versão anterior;
- 11.28. Deverá permitir a integração com outras soluções de SIEM de mercado;
- 11.29. Deverá permitir geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- 11.30. Deverá permitir gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
- 11.31. Deverá permitir geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- 11.32. Deverá prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
- 11.33. Deverá permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas

- pele IPS, Antivírus, Anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;
- 11.34. Deverá permitir a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
  - 11.35. Deverá permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, Antivírus, Anti-spyware, Filtro de URL e filtro de arquivos;
  - 11.36. Deverá permitir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;
  - 11.37. Deverá permitir visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware) e URLs que passaram pela solução;
  - 11.38. Deverá permitir "Drill-Down" para navegação nos relatórios em RealTime. Nas opções de "Drill-Down", deverá ser possível identificar o usuário que fez determinado acesso;
  - 11.39. Deverá ser possível acessar o equipamento e aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
  - 11.40. Deverá permitir fazer o envio de logs para soluções externas;
  - 11.41. Deverá permitir a exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua):
    - 11.41.1. Situação do dispositivo e do cluster;
    - 11.41.2. Principais aplicações;
    - 11.41.3. Principais aplicações por risco;
    - 11.41.4. Administradores autenticados na gerência da plataforma de segurança;
    - 11.41.5. Número de sessões simultâneas;
    - 11.41.6. Status das interfaces;
    - 11.41.7. Uso de CPU;
  - 11.42. Deverá permitir a geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
    - 11.42.1. Resumo gráfico de aplicações utilizadas;
    - 11.42.2. Principais aplicações por utilização de largura de banda de entrada e saída;
    - 11.42.3. Principais aplicações por taxa de transferência de bytes;
    - 11.42.4. Principais hosts por número de ameaças identificadas;
  - 11.43. Deverá permitir a criação de relatórios personalizados;
  - 11.44. Deverá permitir gerar alertas automáticos via:
    - 11.44.1. Email;
    - 11.44.2. SNMP;
    - 11.44.3. Syslog;
  - 11.45. A plataforma de segurança deve permitir através de API (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em tempo real com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como por exemplo Perl, PHP ou outras.
  - 11.46. Caso alguma das funcionalidades citadas nessa seção (11. Console de gerência e monitoração) não seja atendida, ela deverá ser atendida pelo software de gestão centralizada, o qual está descrito no item 2 (Software de gestão centralizada e armazenamento de logs com suporte e garantia de 03 anos).

## **Item 2: Software de gestão centralizada e armazenamento de logs com suporte e garantia de 03 anos**

### **1. Requisitos técnicos**

- 1.1. Poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deverá ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deverá ser compatível com o hypervisor KVM;
- 1.2. Os softwares de gestão centralizada e armazenamento de logs poderão ser entregues em appliances separados, caso não seja possível entregar em um mesmo appliance;
- 1.3. O software deverá ser fornecido em sua versão mais atualizada;
- 1.4. Deverá possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
- 1.5. O gerenciamento da solução deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
- 1.6. O Software de Gestão Centralizada deverá ser homologado e totalmente compatível com o item "FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS" especificado neste Termo de Referência para permitir o gerenciamento dos equipamentos e o armazenamento de logs gerados pelos mesmos;
- 1.7. Deverá permitir o armazenamento de logs sem limite de tempo para retenção e, em caso de esgotamento do espaço em disco disponibilizado para armazenamento dos logs, deverá ser realizado o log-rotation, conservando os dados mais recentes e excluindo os dados mais antigos;
- 1.8. Deverá permitir o armazenamento de logs sem limite de tempo e permitir alocar um no mínimo 20 TB de discos;
- 1.9. Deverá permitir armazenar no mínimo 1,6 TB de logs por mês;
- 1.10. Deverá permitir armazenar no mínimo 50 GB de logs por dia;
- 1.11. Deverá permitir a exportação dos logs para outros sistemas;
- 1.12. Deverá permitir controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;
- 1.13. Deverá permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;
- 1.14. Deverá permitir organizar os dispositivos administrados em grupos: os sistemas virtuais deverão ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
- 1.15. Deverá permitir implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
- 1.16. Deverá permitir a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
- 1.17. Deverá permitir a criação de objetos e políticas compartilhadas;
- 1.18. Deverá consolidar logs e relatórios de todos os dispositivos administrados;
- 1.19. Deverá permitir exportar backup de configuração automaticamente via agendamento;
- 1.20. Deverá permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;
- 1.21. Deverá exibir os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

### **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 a 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. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;
- 1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
- 1.7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Anti-vírus e Anti-malware de acordo com as exigências levantadas;
- 1.8. 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. O fabricante da solução ofertada deverá disponibilizar ferramenta gratuita (ou incluir nos custos de serviço) para acompanhamento da evolução da parametrização de proteção dos firewalls a fim de garantir a melhor eficiência da solução durante o período de vigência das licenças;
- 1.9. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;
- 1.10. 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;
- 1.11. 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;
- 1.12. Os serviços de instalação e configuração deverão ser realizados por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante.
- 1.13. 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.

### **4.8.4. Item 4: Treinamento oficial de firewall**

#### **1. Requisitos técnicos**

- 1.1. A contratada deverá disponibilizar vouchers para treinamento oficial do fabricante;
- 1.2. O treinamento deverá ser ministrado abrangendo teoria e prática de implantação,

configuração, administração e solução de problemas no ambiente deste órgão, bem como assuntos teóricos relacionados;

1.3. Deverá conter no mínimo a seguinte ementa:

- 1.3.1. Arquitetura e Plataforma;
- 1.3.2. Configuração Inicial;
- 1.3.3. Configuração de Interface;
- 1.3.4. Políticas de Segurança e NAT;
- 1.3.5. Identificação de Aplicações;
- 1.3.6. Identificação de Conteúdo Básico;
- 1.3.7. Filtro URL;
- 1.3.8. Criptografia;
- 1.3.9. Sandboxing de ameaças avançadas;
- 1.3.10. Identificação de Usuários;
- 1.3.11. VPN;
- 1.3.12. Monitoramento e Relatórios;
- 1.3.13. Configuração de Alta Disponibilidade (redundância);
- 1.3.14. Demais assuntos pertinentes a solução;

1.4. O treinamento terá duração de, no mínimo, 5 (cinco) dias e ministrado em horário comercial e deverá ser realizado pelo fabricante ou parceiro certificado e autorizado pelo fabricante a ministrar treinamentos, preferencialmente de forma presencial nas instalações do fabricante ou do parceiro autorizado e deverá oferecer material didático e certificado de conclusão. As despesas de deslocamento, hospedagem e alimentação serão de responsabilidade 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;
  - Migração das regras de firewall existentes;
  - 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 de a 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 pode não ter conhecimento técnico suficiente para manter em operação, deverão fazer parte da aquisição treinamentos específicos que deverão ser conduzidos pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.

#### **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 relacionado 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 de 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.
  - O(s) equipamento(s) 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 14:0 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, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA 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, afim de 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 acompanhados 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 3 - SERVIÇOS DE INSTALAÇÃO DE FIREWALL:**
    - 1.1. 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.
  - **Para Item 4 - TREINAMENTO OFICIAL DE FIREWALL:**
    - O aceite do serviço somente será dado após a apresentação de todos os conteúdos esperados e da resolução de possíveis dúvidas da equipe em treinamento.
  - Caso seja verificada alguma inconformidade na aceitação inicial do objeto, a Contratante informará à Contratada os motivos da não aceitação, devolvendo o(s) bem(ns) para correção.
  - Caberá à Contratada sanar as irregularidades identificadas na entrega dos bens, inclusive, substituí-los no prazo de 15 (quinze) dias da notificação, às suas expensas, quando fornecidos com problemas, apresentados fora das especificações técnicas estabelecidas, sob pena de incorrer nas sanções legais cabíveis.

## **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:

- o 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;
- o Verificar se o equipamento está novo e sem uso;
- o Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;
- o 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;
- o Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);
- o Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);
- o 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:
  - o Conectar cabos de alimentação e verificar funcionamento dos equipamentos;
  - o Conectar cabos UTP e fibra óptica, e verificar funcionamentos das portas dos equipamentos;
  - o Realizar configurações relacionadas à rede (configuração de interfaces, endereços IP, roteamento, resolução de nomes (DNS));
  - o Realizar a criação de objetos, de políticas de segurança e regras de firewall;
  - o Realizar a configuração do serviço DHCP;
  - o Configurar modo de alta disponibilidade, com um firewall em modo ativo e outro em modo passivo;
  - o Verificar a sincronização entre equipamentos (firewall ativo e passivo);
  - o Verificar o funcionamento do modo de alta disponibilidade, através da simulação de falta de conexão no firewall configurado em modo ativo;
  - o Caso o software de gerenciamento seja entregue em appliance virtual, verificar a compatibilidade com o hypervisor KVM, criar máquina virtual e realizar as configurações necessárias;
  - o Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Universidade para monitoramento de ativos de rede;
  - o 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;
  - o Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;
  - o 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 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, comportar-se de modo inidôneo ou cometer fraude fiscal.	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 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 não possuir 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.	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**

<b>Id.</b>	<b>Descrição do Bem ou Serviço</b>	<b>Quantidade</b>	<b>Unidade de medida</b>	<b>Valor unitário</b>	<b>Valor total</b>
1	FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS	4	Peça		
2	SOFTWARE DE GESTÃO CENTRALIZADA E ARMAZENAMENTO DE LOGS COM SUPORTE E GARANTIA DE 03 ANOS	1	Licença		
3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	4	Serviço		
4	TREINAMENTO OFICIAL DE FIREWALL	5	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 se realizará na forma 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:
  - o 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 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 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.

## 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 \_\_\_\_\_.