

## EDITAL DE LICITAÇÃO

### PREGÃO PRESENCIAL Nº 006/2019

#### TIPO: MENOR PREÇO

O Serviço Nacional de Aprendizagem do Cooperativismo do Estado de Minas Gerais – Sescoop/MG, sediado na Rua Ceará, nº 771, Bairro Funcionários, Cidade Belo Horizonte/MG, registrado no CNPJ sob o número 07.064.534/0001-20, por intermédio de seu Pregoeiro e membros da equipe de apoio, torna público para conhecimento dos interessados que na data, horário e local abaixo indicados fará realizar Licitação na modalidade de PREGÃO PRESENCIAL, do TIPO MENOR PREÇO, para **Contratação de empresa especializada em fornecimento de solução de firewall, baseado em tecnologia (UTM) do inglês Unified Threat Management (Gerenciamento Unificado de Ameaças) com alta disponibilidade em formato appliance (dispositivo de hardware separado e discreto, selado, com software integrado e do mesmo fabricante do hardware), com implantação, suporte e garantia com o intuito de disponibilizar proteção digital à rede lógica do SESCOOP/MG**, conforme Termo de Referência – ANEXO I e demais condições que se estabelecem:

Os itens abaixo discriminados integram este documento convocatório, dele fazendo parte como se transcritos em seu corpo:

	Página
1) Sumário	01
2) Especificação do Edital	03
3) Anexo I – Termo de Referência	17
4) Anexo II – Modelo de Carta Proposta	36
5) Anexo III – Modelo de Procuração	38
6) Anexo IV – Modelo de Declaração de Pleno Atendimento à Habilitação	39
7) Anexo V – Modelo de Atestado de Capacidade Técnica	40
8) Anexo VI – Modelo de Declarações – Exigências Legais	41
9) Anexo VII – Minuta Contratual	42

### SUMÁRIO

- Serviço Nacional de Aprendizagem do Cooperativismo de Minas Gerais – **Sescoop/MG**.
- Modalidade: **Pregão Presencial**
- Tipo de Licitação: **Menor Preço**

#### Justificativa:

A solução proposta visa atender a necessidade de segurança com o consequente controle e bloqueio de permissões, seja indesejado ou não, que permita a mitigação de riscos, para a manutenção da disponibilidade e integridade das informações disponíveis na rede local de forma a estar aderente à Norma de Procedimento Interna de Segurança da Informação do SESCOOP/MG.

Consideramos que as corporações que fazem uso ou oferecem serviços por meio da Internet, redes parceiras ou por qualquer outro tipo de conexão, que interajam seus ambientes internos aos externos, devem ter extrema preocupação com esses canais de comunicação, pois além do benefício de permitir conectividade, também representam, em contrapartida, risco potencial para acessos não autorizados e maliciosos.

Para que seja possível manter o adequado nível de segurança em seus ambientes e, assim preservar os ativos corporativos (hardware, software e dados), de modo a garantir a integridade, confidencialidade e segurança das informações institucionais, torna-se imprescindível a adoção de soluções estratégicas que minimizem os riscos e evitem ocorrências de prejuízos técnicos e financeiros e não afetem a credibilidade institucional.

Nesse sentido, o emprego de soluções de Firewall possibilita que o tráfego de dados seja monitorado e controlado, a ponto de permitir o estabelecimento de um único canal de entrada e saída entre esses ambientes e permita a proteção preventiva da rede local. A arquitetura da solução proposta está focada nas melhores práticas de segurança e melhores ferramentas disponíveis no mercado para a segurança de ambientes corporativos, além dos benefícios inerentes aos novos equipamentos.

#### **Da Legalidade:**

Esta Licitação é regida pelo Regulamento de Licitação e Contratos do Serviço Nacional de Aprendizagem do Cooperativismo – SESCOOP, aprovado pela Resolução nº 850/2012 do Conselho Nacional (publicada no D.O.U. de 26/03/2012).

Neste aspecto, visando dar maior abrangência e publicidade à licitação em epígrafe, bem como dar maior celeridade ao processo de licitação, buscando ainda o cumprimento do princípio da economicidade em suas contratações, vislumbramos a utilização de processo de licitação na modalidade de Pregão Presencial, compreendendo que esta forma de licitação cumpre com satisfação o seu papel para obtenção de melhores preços e mais vantajosos para o SESCOOP/MG.

Entrega dos Envelopes: **até as 14h do dia 01/07/2019.**

- Local de entrega dos Envelopes: À Comissão Permanente de Licitação, localizada na Rua Ceará, nº 771, Bairro Funcionários, CEP 30150-311, Belo Horizonte, Minas Gerais.
- Data e hora do início e local de abertura dos envelopes contendo a documentação de proposta de preço com posterior início dos lances verbais: **14h do dia 01/07/2019**, na sala de treinamento do **Sescoop/MG**, localizada na Rua Ceará, nº 771, Bairro Funcionários, CEP 30150-311, Belo Horizonte, Minas Gerais.

**“Apenas com a violação do primeiro envelope de proposta de preços, a sessão será declarada aberta, não sendo mais admitidos novos proponentes”**

## ESPECIFICAÇÃO DO EDITAL

### ÍNDICE – PREÂMBULO

ITENS	DISCRIMINAÇÃO	PÁGINA
01	Do Local e horário para exame e aquisição do Edital	03
02	Do Objeto	03
03	Do Credenciamento	03
04	Das Condições para participação na licitação	04
05	Da Impugnação e esclarecimentos sobre o edital	05
06	Da Entrega da documentação para habilitação e proposta	05
07	Da Sessão pública do pregão	06
08	Da Proposta de preço (ENVELOPE Nº 01)	08
09	Do Julgamento	09
10	Da Habilitação (ENVELOPE Nº 02)	10
11	Dos Recursos administrativos	12
12	Das Sanções para o caso de inadimplemento	12
13	Da Homologação e adjudicação	13
14	Do Contrato	13
15	Do Prazo de vigência e execução dos serviços	13
16	Do Faturamento e forma de pagamento	14
17	Da Fonte de recursos e estimativa de preços	14
18	Das Disposições gerais	15

### 1 – DO LOCAL E HORÁRIO PARA EXAME E AQUISIÇÃO DO EDITAL

1.1 – O Edital contendo todas as normas, orientações, procedimentos, especificações, formulários, relação de documentos a serem apresentados, e demais informações indispensáveis à participação dos interessados na licitação, poderá ser obtido a partir das **09h** do dia **19/06/2019** até as **17h** do dia **28/06/2019**, através da Comissão Permanente de Licitação do **Sescoop/MG**, localizada na Rua Ceará, nº 771, Bairro Funcionários, CEP 30150-311, Belo Horizonte, Minas Gerais. Telefone: (31) 3025-7059. E-mail: [administrativa@minasgerais.coop.br](mailto:administrativa@minasgerais.coop.br)

### 2 – DO OBJETO

2.1 – A presente licitação tem como objeto a **Contratação de empresa especializada em fornecimento de solução de firewall, baseado em tecnologia (UTM) do inglês Unified Threat Management (Gerenciamento Unificado de Ameaças) com alta disponibilidade em formato appliance (dispositivo de hardware separado e discreto, selado, com software integrado e do mesmo fabricante do hardware), com implantação, suporte e garantia com o intuito de disponibilizar proteção digital à rede lógica do SESCOOP/MG**, conforme Termo de Referência – ANEXO I e demais termos e condições estabelecidos neste Edital.

### 3 – DO CREDENCIAMENTO

3.1 – No dia, hora e local designados neste Edital, será realizada Sessão Pública para recebimento das Propostas e da Documentação de Habilitação, devendo o Interessado ou seu Representante Legal proceder ao respectivo Credenciamento, comprovando, se

for o caso, possuir os necessários poderes para formulação de Propostas e para a prática de todos os demais atos inerentes ao certame, conforme modelo **ANEXO III** do Edital.

3.2 – Para o credenciamento deverão ser apresentados os seguintes documentos:

- a) Tratando-se de Representante Legal, cópia do Estatuto Social, Contrato Social ou outro instrumento de Registro Comercial, registrado na Junta Comercial ou, tratando-se de Sociedade Civil, o Ato Constitutivo registrado no Cartório de Registro Civil de Pessoas Jurídicas, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura;
- b) Tratando-se de Procurador, a procuração por instrumento público ou particular **com firma reconhecida (Modelo ANEXO III do Edital)**, da qual constem poderes específicos para formular lances, negociar preço, interpor recursos e desistir de sua interposição e praticar todos os demais atos pertinentes ao certame, acompanhada do correspondente documento, dentre os indicados no Subitem 3.2.1 supra, que comprove os poderes do mandante para a outorga.

3.3 – O Representante Legal ou Procurador deverá identificar-se exibindo documento oficial que contenha foto recente.

3.4 – Será admitido apenas 1 (um) representante ou procurador para cada licitante credenciado, sendo que cada um deles poderá representar apenas uma Empresa credenciada.

3.5 – No caso de o representante ser Sócio ou Diretor da Empresa licitante, o mesmo deverá anexar cópia do Contrato Social para comprovação que tem poderes para tomar e assinar decisões pela a mesma.

3.6 – O credenciamento deverá ser entregue à Comissão Permanente de Licitação na reunião de abertura dos trabalhos, **apartada do(s) envelope(s)**, ficando retido para instrução do processo.

3.7 – O não credenciamento do representante impedirá qualquer pessoa presente de se manifestar e responder pela licitante, sem prejuízo do direito de oferecimento dos documentos de habilitação e proposta, respeitado o disposto no item “3.8” subsequente.

3.8 – Outro representante não credenciado junto ao **Sescoop/MG** poderá participar da licitação, **somente como ouvinte**, não lhe sendo permitido rubricar ou assinar documentos, oferecer lances verbais ou fazer qualquer observação.

3.9 – Fica assegurado às licitantes, a qualquer tempo, mediante juntada dos documentos previstos nos itens antecedentes, a indicação ou substituição do seu representante junto à Comissão.

#### **4 – DAS CONDIÇÕES PARA PARTICIPAÇÃO NA LICITAÇÃO**

4.1 – Poderão apresentar propostas as empresas que estiverem legalmente estabelecidas que satisfaçam às condições deste Edital e de seus anexos.

4.2 – Poderão participar deste Pregão os interessados do ramo pertinente ao objeto da presente contratação, que atendam a linha de fornecimento e a todas as demais exigências constantes neste Edital e seus Anexos.

4.3 – Não poderão participar desta licitação:

- a) Empresas que deixarem de entregar no local e data, nas condições definidas neste Edital, os envelopes nº 01 (Proposta de Preço) e nº 02 (Documentação para Habilitação);
- b) Empresas que se apresentarem sob a forma de consórcio, qualquer que seja sua forma de constituição;
- c) Empresas suspensas de licitar e contratar com o **Sescoop/MG**.

## **5 – DA IMPUGNAÇÃO E ESCLARECIMENTOS SOBRE O EDITAL**

5.1 – O ato convocatório poderá ser impugnado, no todo ou em parte, até 02 (dois) dias úteis antes da data fixada para o recebimento das propostas. Não impugnado o ato convocatório, preclui toda matéria nele constante. **A impugnação deverá ser protocolada pessoalmente no endereço sede do Sescoop/MG, não sendo possível seu protocolo por e-mail.**

5.1.1 – A impugnação deverá ser protocolada no prazo estipulado no item 5.1 acima, considerando para tal o horário de funcionamento da entidade, a saber, 08h30 as 17h30 horas de segunda a sexta feira, exceto feriados legais.

5.2 – Os interessados que necessitarem de quaisquer esclarecimentos sobre o Edital, documentos e outros procedimentos da licitação, poderão solicitá-los ao Sescoop/MG, por escrito, até 02 (dois) dias úteis antes da data fixada para o recebimento das propostas, impreterivelmente, através do e-mail [administrativa@minasgerais.coop.br](mailto:administrativa@minasgerais.coop.br), no número e no endereço indicado no subitem 1.1 deste instrumento, mediante requerimento com identificação.

## **6 – DA ENTREGA DA DOCUMENTAÇÃO PARA HABILITAÇÃO E PROPOSTA**

6.1 – Aberta a Sessão, os interessados ou seus representantes legais deverão apresentar a **Declaração que cumprem plenamente os Requisitos de Habilitação**, conforme o modelo **ANEXO IV** do edital, entregando também ao Pregoeiro os envelopes, procedendo-se à sua imediata abertura e à verificação da conformidade das Propostas com os requisitos estabelecidos neste Edital.

6.2 – As licitantes deverão entregar ao Pregoeiro e equipe de apoio, no endereço mencionado no item 1.1 do edital, até as **14h do dia 01/07/2019**, os envelopes numerados externamente, contendo a proposta de preço (Envelope Nº 01) e documentos de Habilitação (Envelope Nº 02).

6.3 – Os envelopes deverão conter externamente as seguintes informações:

### **ENVELOPE Nº 01 - PROPOSTA DE PREÇO**

Ao Serviço Nacional de Aprendizagem do Cooperativismo de Minas Gerais/SESCOOP

Razão Social do Proponente:

Pregão Presencial nº 006/2019

**"ATENÇÃO: NÃO ABRIR-LICITAÇÃO"**

### **ENVELOPE Nº 02 – HABILITAÇÃO**

Ao Serviço Nacional de Aprendizagem do Cooperativismo de Minas Gerais/SESCOOP

Razão Social do Proponente:

Pregão Presencial nº 006/2019

**"ATENÇÃO: NÃO ABRIR-LICITAÇÃO"**

6.4 – A Declaração falsa relativa ao Pleno Atendimento aos Requisitos de Habilitação e Proposta sujeitará os licitantes às sanções previstas no item 12 do Edital e também dos artigos 31 e 32 do Regulamento de Licitação e Contratos do SESCOOP.

6.4.1 – A Declaração de pleno atendimento aos Requisitos de Habilitação deverá ser **apresentada fora dos envelopes** nº 1 e nº 2, conforme modelo **ANEXO IV** do edital.

6.5 – A empresa que não apresentar Declaração de Pleno Atendimento aos Requisitos de Habilitação, poderá elaborar o documento durante a sessão, antes da abertura dos envelopes nº 1 “Proposta de Preços”. Somente se o representante da licitante estiver devidamente credenciado, conforme item 3 do edital.

6.6 – A Proposta deverá ser elaborada em papel timbrado da empresa e redigida em língua portuguesa, salvo quanto às expressões técnicas de uso corrente, sem rasuras, emendas, borrões ou entrelinhas e ser datada e assinada pelo Representante Legal do licitante ou pelo procurador.

6.7 – Quando os Envelopes forem enviados pelo correio ou outro meio que não seja o seu Representante Legal, deverão estar de posse do Pregoeiro no local, data e horário estabelecidos neste Edital, para abertura da licitação, sob pena de não participar desta licitação.

6.8 – A Sessão será declarada aberta com a abertura do 1º (primeiro) envelope. Declarada aberta a Sessão Pública pelo Pregoeiro, não mais serão admitidos novos proponentes, dando-se início aos trabalhos do Pregão.

6.9 – Primeiramente serão abertos os Envelopes nº 01 contendo as Propostas de Preços, sendo verificada sua conformidade e posterior rubrica.

6.10 – Após apresentação da Proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro.

## **7 – DA SESSÃO PÚBLICA DO PREGÃO**

7.1 – Os **Documentos** referentes ao **Credenciamento**, **Declaração de pleno atendimento aos requisitos de habilitação** e os **Envelopes** contendo as propostas comerciais e os documentos de habilitação das empresas interessadas deverão ser entregues diretamente ao pregoeiro no momento da abertura da Sessão Pública de

Pregão, que está prevista para as **14h do dia 01/07/2019**, na Rua Ceará, nº 771, Bairro Funcionários, CEP 30150-311, Belo Horizonte, Minas Gerais ou enviados por correio em conformidade ao item 6.7 deste Edital.

7.2 – Na hora e local indicado no subitem 7.1, serão observados os seguintes procedimentos pertinentes a este PREGÃO:

- a) Credenciamento dos representantes legais das empresas interessadas em participar do certame, mediante apresentação, fora dos envelopes 01 e 02, conforme previsto no item 3 do presente edital;
- b) Apresentação da Declaração de pleno atendimento aos requisitos de habilitação – **ANEXO IV, fora dos envelopes 01 e 02;**
- c) Após o credenciamento e análise da Declaração de pleno atendimento aos requisitos de habilitação passa-se à fase do recebimento dos envelopes “proposta” e “documentação”, e abertura dos envelopes de proposta escrita **sendo vedada, a partir deste momento a admissão de novos participantes na licitação.**

7.3 – Abertura e análise dos envelopes nº 1 “PROPOSTA DE PREÇO”.

7.4 – Desclassificação das propostas que não atenderem às exigências deste edital e classificação provisória das demais em ordem crescente de preços, considerando o Menor Preço Global.

7.5 – Abertura de oportunidade de oferecimento de lances verbais, aos representantes das empresas, cujas propostas estejam classificadas, no intervalo compreendido entre o menor preço e o preço superior àquele em até 15% (quinze por cento).

7.6 – Não havendo pelo menos três ofertas poderão as empresas autoras das melhores propostas, até o máximo de três, oferecer novos lances verbais e sucessivos.

7.7 – Condução de rodadas de lances verbais, pelo valor global, sempre a partir do representante da empresa com proposta de maior preço, em ordem decrescente de valor, respeitadas as sucessivas ordens de classificação provisória, até o momento em que não haja novos lances de preços menores aos já ofertados.

7.7.1 – Caso duas ou mais propostas iniciais apresentem preços iguais, será realizado sorteio para a determinação da ordem de oferta dos Lances;

7.7.2 – A desistência do licitante em apresentar lance verbal, quando convocado pelo Pregoeiro, implicará a exclusão do mesmo da etapa de lances verbais e na manutenção do último preço por ele apresentado, para efeito de ordenação das propostas;

7.7.3 – Caso não se realizem lances verbais, será verificada a conformidade entre a proposta escrita de menor preço e o valor estimado para a contratação;

7.7.4 – A etapa de lances será considerada encerrada quando todos os participantes declinarem da formulação de lances;

7.7.5 – O Pregoeiro poderá negociar com o autor da oferta de menor valor com vistas à redução do preço.

7.8 – Na fase de lances verbais, não serão aceitos lances de valor igual ou maior ao do último e os sucessivos lances deverão ser feitos em valores decrescentes com intervalos de, no mínimo, **R\$ 200,00 (duzentos reais)**.

7.8.1 – A fim de promover o aumento da disputa de lances verbais durante a sessão pública e buscando os melhores preços para o Sescop/MG, o Sr. Pregoeiro terá a prerrogativa de abrir mão do lance mínimo estipulado no item 7.8.

7.9 – Não poderá haver desistência de lances ofertados, sujeitando-se o desistente às penalidades previstas neste edital.

7.10 – Declarada encerrada a etapa competitiva, o pregoeiro procederá à classificação definitiva das propostas, consignando-a em ata.

7.11 – Classificação definitiva das propostas em ordem crescente de **MENOR PREÇO GLOBAL**.

7.12 – Abertura do(s) envelope(s) nº 2 “HABILITAÇÃO” apenas da empresa, cuja proposta tenha sido classificada em primeiro lugar.

7.13 – Sendo inabilitada a proponente cuja proposta tenha sido classificada em primeiro lugar, prosseguindo o pregoeiro com a abertura do envelope de documentação da proponente classificada em segundo lugar, e assim sucessivamente, se for o caso, até a habilitação de uma das licitantes.

7.14 – Proclamação da empresa vencedora do certame pelo critério de Menor Preço Global.

7.15 – Declarada a vencedora, qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, conforme previsto no item 11 do edital.

7.16 – Encaminhamento dos autos do processo à autoridade competente para adjudicação e homologação do certame, conforme previsto no item 13 do edital.

7.17 – É facultado ao Sescop/MG, quando a adjudicatária não assinar o contrato no prazo e condições estabelecidos, convocar as demais licitantes, na ordem de classificação, para fazê-lo em igual prazo e, preferencialmente, nas mesmas condições ofertadas pela adjudicatária.

7.18 – Os envelopes contendo a documentação relativa à habilitação das licitantes desclassificadas e das classificadas não declaradas vencedoras permanecerão sob custódia do Sescop/MG, até a efetiva formalização da contratação.

## **8 – DA PROPOSTA DE PREÇO (ENVELOPE Nº 01)**

8.1 – A Proposta poderá ser apresentada conforme Modelo **ANEXO II** do edital, sem rasuras e emendas, entrelinhas ou ressalvas, **com nome e endereço completo**,

telefone, CNPJ, nº da agência, nº da conta corrente e nome do banco, datada e assinada pelo responsável legal.

8.2 – A Proposta deverá estar acompanhada dos seguintes elementos:

**QUANTIDADE, VALORES UNITÁRIOS E TOTAIS. PREÇOS OFERTADOS PARA OS APPLIANCES DE SEGURANÇA, LICENÇAS, SOFTWARE DE GERENCIAMENTO CENTRALIZADO E VALOR (VERBA) REFERENTE A MÃO DE OBRA PARA INSTALAÇÃO DA SOLUÇÃO.** Todos os valores ofertado(s) em Real (R\$) e em duas casas decimais, devendo estar incluso(s) todos os custos inerentes a prestação dos serviços, tais como, mão de obra, encargos sociais, transportes, equipamentos, entrega e montagem, embalagens, ferramentas, instalações, impostos, taxas e todo ônus direto e indireto, necessário para cumprimento da obrigação, conforme Modelo **ANEXO II** do edital;

- a) **CARTA PROPOSTA** digitada em 01 (uma) via da qual deverá constar o preço unitário p/ pessoa e valor global, conforme Modelo **ANEXO II** do edital;

8.3 – Apenas para efeito de ordenamento de valores das propostas, ocorrendo discordância entre os preços unitários e totais, prevalecerão os primeiros, e entre os valores expressos em algarismos e por extenso, serão considerados estes últimos.

8.4 – Decorrido 60 (sessenta) dias da data do encerramento da fase de lances deste Pregão, sem convocação para a contratação, fica o licitante vencedor liberado do compromisso assumido.

## 9 – DO JULGAMENTO

9.1 – Para julgamento das propostas, o Pregoeiro levará em consideração o **MENOR PREÇO GLOBAL** apresentado (Valor total do item 01 + Valor total do item 02+ Valor total do item 3), desde que atendidas as especificações constantes deste edital e seus anexos, sendo desclassificadas a(s) Proposta(s) que estiver(em) em desacordo com as especificações – **ANEXO I** deste Edital.

9.1.1 – Para identificação do Menor Preço Global, para fins de julgamento e identificação da licitante vencedora, a licitante deverá ofertar “obrigatoriamente” o valor unitário mensal e o valor (verba) referente aos serviços de montagem / configuração / instalação / ativação do link, conforme Modelo de Carta Proposta – **ANEXO II**.

Ex.: Ex: Valor total do item 01 + Valor total do item 02 + Valor do item 03

9.2 – Serão desclassificadas as propostas que:

- a) Não atendam as condições contidas neste edital;
- b) Apresentem preço global, com valor nulo ou zero, simbólicos, inexequíveis, irrisórios ou incompatíveis com os preços praticados no mercado;
- c) Apresentem cotação parcial, deixando de apresentar preço para o serviço e/ou vantagens baseadas nas ofertas dos demais licitantes;

- d) Não sejam feitas em moeda nacional;
- e) Apresentem diferentes opções de preço para o mesmo serviço ou item;
- f) Deixem de atender às solicitações da Comissão ou da área técnica competente, quando da realização de diligência.
- g) Ofertem preço superior a 15% em relação ao menor preço dentre as propostas escritas e classificadas.

9.3 – Em nenhuma hipótese poderá ser alterado o conteúdo da proposta apresentada, ressalvadas apenas aquelas destinadas a sanar evidentes erros materiais, a juízo exclusivo do Pregoeiro, puder ser sanável, sem a quebra de igualdade de tratamento oferecida a todos os licitantes.

9.4 – Encerrada a etapa competitiva de lances e ordenadas às ofertas de acordo com o menor preço apresentado, o Pregoeiro verificará a aceitabilidade do melhor preço ofertado e avaliará a aceitabilidade da proposta classificada em primeiro lugar quanto ao objeto e valor decidindo motivadamente a respeito.

9.5 – Se a oferta não for aceitável ou se a proponente não atender às exigências do edital, o Pregoeiro examinará as ofertas subsequentes, na ordem de classificação, até a apuração de uma proposta em conformidade com este Edital.

9.5.1 – Sendo o proponente remanescente na ordem de classificação declarado classificado e habilitado a ele será adjudicado o objeto, desde que não tenha havido manifestação pela interposição de recurso, submetendo os autos à homologação do Superintendente e Presidente do SESCOOP/MG.

9.6 – Da sessão lavrar-se-á ata circunstanciada que será assinada pelo Pregoeiro, pela equipe de apoio e pelos licitantes presentes.

9.7 – Tendo sido declarada a empresa vencedora, esta deverá apresentar no primeiro dia subsequente e útil à data da sessão, nova proposta indicando o novo valor ofertado.

9.7.1 – O percentual de desconto concedido pela empresa vencedora, após a rodada de lances verbais, deverá ser aplicado proporcionalmente ao preço mensal, anual e serviço (verba) para instalação.

## **10 – DA HABILITAÇÃO (ENVELOPE Nº 02)**

10.1 – A comprovação da Habilitação do licitante com melhor Proposta será verificada pelo Pregoeiro, após a etapa de lances com a abertura do Envelope nº 02 e estão relacionados nos subitens Habilitação Jurídica, Regularidade Fiscal e Qualificação Técnica.

10.1.1 – Os documentos deverão ser fornecidos, em 01 (uma) via de cada, em plena validade, em original ou extraídos da Internet ou cópia autenticada (verso e anverso, absolutamente legíveis) com todas as folhas rubricadas pelo

representante legal do licitante, **NÃO** podendo ser substituídos por qualquer tipo de protocolo;

10.1.2 – Se junto à documentação for(em) inserida(s) cópia(s) sem autenticação(ões), o(s) original(is) desta(s) deverá(ão) ser obrigatoriamente exibido(s) ao pregoeiro, **no ato da abertura do respectivo envelope**, para que a(s) referida(s) cópia(s) seja(m) devidamente conferida(s). **O(s) documento(s) deverá(ão) estar dentro de seu(s) prazo(s) de validade;**

10.1.3 – Não serão aceitas fotocópias efetuadas em aparelho “fac-símile”;

10.1.4 – Nenhuma alteração ou complementação da documentação de habilitação ou das propostas comerciais será aceita após seu recebimento, ressalvados eventuais esclarecimentos que venham a ser solicitados, a qualquer tempo, pelo **Sescoop/MG**;

10.1.5 – Uma vez incluído no processo, nenhum documento será devolvido exceto os originais, se substituídos por cópias autenticadas.

## 10.2 – HABILITAÇÃO JURÍDICA:

10.2.1 – Ato Constitutivo ou Estatuto ou Contrato Social ou Cadastro de Empresário Individual ou Inscrição de Empresário (Art. 967 da Lei 10.406/02), todos em vigor e obrigatoriamente acompanhados de suas respectivas alterações, caso ocorridas, bem como devidamente registrados em se tratando de Sociedades Comerciais e, no caso de Sociedades por ações, acompanhados de documentos da eleição de seus atuais administradores;

10.2.2 – Nos casos em que o ato constitutivo, estatuto ou contrato social tenham sido consolidados, deverão ser apresentadas a consolidação e alterações posteriores, caso ocorridas;

10.2.3 – Não será aceito Extrato do Contrato Social (Certidão de breve relato ou simplificada).

## 10.3 – REGULARIDADE FISCAL:

10.3.1 – Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

10.3.2 – Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.3.3 – Prova de regularidade (Certidão Negativa de Débito ou Certidão Positiva com efeitos de Negativa) para com as Fazendas Municipal (Certidão de Quitação Plena Pessoa Jurídica) e Estadual (Certidão de Débitos Tributários – Somente relativos a Dívida Ativa) ambos do domicílio ou sede do licitante, expedida pelo órgão competente, na forma da lei;

10.3.4 – Certificado de Regularidade do FGTS – CRF (Certidão Negativa de Débito ou Certidão Positiva com efeitos de Negativa), expedido pela Caixa Econômica

Federal, com a finalidade de comprovar a inexistência de débitos junto ao Fundo de Garantia por Tempo de Serviço – FGTS;

10.3.5 – Certidão Conjunta de débitos (Certidão Negativa de Débito ou Certidão Positiva com efeitos de Negativa) relativos a Tributos Federais perante a Receita Federal do Brasil – RFB, a Dívida Ativa da União perante a Procuradoria Geral da Fazenda Nacional – PGFN e ao Instituto Nacional do Seguro Social – INSS, que abrange a regularidade das contribuições previdenciárias e de terceiros.

10.3.6 – Prova de inexistência de débitos inadimplentes perante a Justiça do Trabalho, mediante a apresentação de certidão negativa (Certidão Negativa de Débitos Trabalhistas – CNDT).

#### 10.4 – QUALIFICAÇÃO TÉCNICA:

10.4.1 – Deverá ser apresentado NO MÍNIMO 01 (hum) ATESTADO DE CAPACIDADE TÉCNICA, conforme Modelo **ANEXO V** do edital, expedido por pessoa jurídica de direito público ou privado, que comprove ter o licitante prestado, com qualidade satisfatória, serviços da mesma natureza objeto da licitação;

### 11 – DOS RECURSOS ADMINISTRATIVOS

11.1 – Declarado o vencedor, qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, quando lhe será concedido o prazo de 02 (dois) dias para apresentação das razões do recurso, cujo documento original deverá ser **obrigatoriamente protocolado** na Rua Ceará, nº 771, 3º andar, Bairro Funcionários, Belo Horizonte/MG, ficando os demais licitantes desde logo intimados para apresentar contrarrazões em igual período, que começarão a correr do término do prazo do recorrente.

11.1.1 – O(s) recurso(s) deverão ser protocolado(s) pessoalmente no prazo estipulado no item 11.1 acima, considerando para tal o horário de funcionamento da entidade, a saber, 08h30 as 17h30, de segunda a sexta feira, exceto feriados legais.

11.2 – O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

11.3 – A ausência de manifestação imediata e motivada da licitante implicará a decadência do direito de recurso e a adjudicação do objeto da licitação à vencedora.

### 12 – DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

12.1 – A prática de atos ilícitos, em quaisquer das fases do procedimento licitatório, o descumprimento de prazos e condições do Edital, implicarão na aplicação das penalidades previstas nos artigos 31 e 32 do Regulamento de Licitações e Contratos do SESCOOP, sem prejuízo das demais sanções previstas em Lei, garantida a defesa prévia.

12.2 – A inexecução total ou parcial injustificada, a execução deficiente, irregular ou inadequada do objeto licitatório, pela licitante vencedora, assim como o descumprimento

dos prazos e condições estipulados e, sem prejuízo das mesmas, implicarão nas penalidades abaixo mencionadas:

- a) Multa de 10% (dez por cento) do valor total do contrato de prestação de serviços;
- b) Advertência;
- c) Cancelamento do contrato do fornecedor;
- d) Suspensão temporária do direito de participar em licitação e impedimento de contratar com o **SESCOOP**, por prazo de até 02 (dois) anos.

12.3 – Ocorrendo aplicação de multa, esta será descontada sobre o valor da nota fiscal/fatura ou dos créditos a que a licitante vencedora fizer “jus”, no ato do pagamento, ou recolhidas diretamente à tesouraria do SESCOOP/MG, ou ainda, quando for o caso, cobrada judicialmente.

12.4 – O prestador dos serviços terá o seu contrato cancelado, caso o mesmo deixe de atender as condições deste edital ou deixe de atender o pedido de fornecimento enviado.

12.5 – Para aplicação das penalidades aqui previstas, a licitante vencedora será notificada para apresentação de defesa prévia, no prazo de 05 (cinco) dias, contados da notificação.

12.6 – As penalidades previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis, tal como a rescisão contratual.

### **13 – DA HOMOLOGAÇÃO E ADJUDICAÇÃO**

13.1 – Após comunicação do resultado final, não houver sido interposto recurso ou se já decididos os porventura interpostos, o pregoeiro remeterá o processo à Superintendência do SESCOOP/MG para homologação e autorização de adjudicação do objeto à licitante vencedora.

13.2 – A Superintendência do SESCOOP/MG poderá cancelar a presente licitação, antes de emitido o(s) Contrato(s), por motivo justificado, conforme previsto no Artigo 40, do Regulamento de Licitações e Contratos do SESCOOP.

### **14 – DO CONTRATO**

14.1 – Tão logo seja homologada a decisão, a Comissão notificará a licitante vencedora para que compareça na Rua Ceará, nº 771, Bairro Funcionários, Belo Horizonte/MG, para a assinatura do Contrato, que deverá ser atendido em todos os seus termos pelo proponente.

14.2 – O contrato será único, sendo, **60 dias** para o fornecimento, instalação e configuração realizada pela empresa licitante vencedora, de **90 dias** após o término da implantação da solução para prestar suporte direto, utilizando força própria, visando atender o período de adaptação onde surgirão dúvidas e necessidades de ajustes e de **05 anos** para garantia dos equipamentos, licenciamento e suporte por parte do fabricante.

### **15 – DO PRAZO DE VIGÊNCIA E EXECUÇÃO DOS SERVIÇOS**

15.1 – O prazo de vigência, garantia e de suporte do fabricante será de 60 meses, no entanto, a garantia da implantação e configuração dos serviços, será de 03 meses, iniciando-se na data de sua assinatura, podendo ser prorrogado sucessivamente, se do interesse das partes, mediante termo aditivo, também até o limite de 60 (sessenta) meses.

15.2 – O prazo de fornecimento e implantação completa do ambiente deverá ser de até 60 (sessenta) dias, já inclusos neste, o prazo de 10 dias para criação e aprovação de um cronograma físico de atividades.

## 16 – DO FATURAMENTO E FORMA DE PAGAMENTO

16.1– O faturamento poderá ocorrer imediatamente após o fornecimento, sendo que o pagamento será efetuado mediante apresentação da Nota Fiscal / Fatura, devidamente aprovada pela Gerência Administrativa do **Sescoop/MG**, conforme tabela abaixo:

<b>Data de entrega do Recibo</b>	<b>Data de pagamento</b>
Do dia 1º ao dia 10 do mês	Até o dia 20 do mês
Do dia 11 ao dia 20 do mês	Até o dia 30 do mês
Do dia 21 ao dia 30/31 do mês	Até o dia 10 do mês subsequente

16.1.1 – Para processar-se o pagamento, a licitante vencedora deverá submeter ao Sescoop/MG à(s) competente(s) nota(s) fiscal(is)/fatura(s);

16.1.2 – O pagamento de taxas, impostos, licenças, emolumentos, demais tributos e encargos sociais que incidam sobre os serviços contratados serão de exclusiva responsabilidade da licitante vencedora;

16.1.3– No caso de incorreção na(s) Nota(s) Fiscal(is), esta(s) será(ão) restituída(s) à licitante vencedora para as correções solicitadas. O prazo de pagamento será contado a partir da data da regularização do serviço ou do documento fiscal, não respondendo o Sescoop/MG por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes;

16.1.4 – Nenhum pagamento será feito à licitante vencedora enquanto perdurar qualquer pendência contratual;

16.1.5 – No caso de emissão de Nota(s) Fiscal(is) na forma “eletrônica”, a licitante fica obrigada a enviar juntamente com o documento o arquivo eletrônico denominado “XML” para fins de conferência e fechamento junto a receita estadual. A(s) Nota(s) Fiscal(is) ficará(ão) retida(s) para pagamento, até o envio do presente arquivo;

16.1.6 – A emissão e envio das notas fiscais deverão ocorrer até o dia 25 de cada mês. Após esta data, a mesma deverá ser emitida no 1º dia do mês subsequente à prestação do serviço. Este procedimento se faz necessário em virtude do prazo para recolhimento dos impostos. A emissão das notas fiscais no 1º dia do mês subsequente ao da prestação dos serviços realizados entre os dias 25 e 30/31, não sofrerão alteração na sua programação de pagamento, prevista para o dia 10, conforme tabela no item 16.1;

## 17 – DA FONTE DE RECURSOS E ESTIMATIVA E PREÇOS

17.1 – As despesas inerentes à execução do objeto da presente licitação correrão por conta de recursos próprios do SESCOOP/MG, consignados também em seu orçamento.

Centro de Responsabilidade: 23.0.10.30.001 – Manutenção do Funcionamento GETIN.

17.2 – A estimativa da licitação parte da fase interna do processo licitatório, sendo a média obtida através de pesquisa de mercado realizada pelo SESCOOP/MG, devendo ser utilização para verificação e aceitabilidade das propostas apresentadas.

17.2.1 – As propostas com preços manifestamente inexequíveis ou excessivamente altos, assim considerados aqueles que não venham a ter demonstrada sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os preços praticados no mercado, serão desclassificadas após avaliação da comissão de licitação.

## **18 – DAS DISPOSIÇÕES GERAIS**

18.1 – Fica assegurado ao SESCOOP/MG o direito de alterar as condições deste Edital de acordo com seu interesse, desde que seja feita divulgação pela mesma forma que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar, substancialmente, a formulação das propostas.

18.2 – Na contagem dos prazos estabelecidos no Regulamento de Licitações e Contratos do SESCOOP, excluir-se-á o dia do início e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário. Para fins deste item, esclarecemos que os prazos somente se iniciam e vencem em dia funcionamento do SESCOOP/MG.

18.3 – As licitantes são responsáveis, em qualquer época, pela fidelidade e veracidade das informações dos documentos apresentados.

18.4 – Os casos omissos desta licitação serão resolvidos pelo Pregoeiro e equipe de apoio do SESCOOP/MG, com aplicação do Regulamento de Licitações e Contratos do SESCOOP.

18.5 – O SESCOOP/MG poderá introduzir acréscimos ou supressões que se fizerem necessários, em até 25% (vinte e cinco por cento) do valor inicial do contrato, conforme lhe faculta o artigo 30 do Regulamento de Licitações e Contratos do SESCOOP.

18.6 – O SESCOOP/MG poderá revogar a licitação por razões de interesse público decorrente de fato superveniente devidamente comprovado, devendo anulá-la por ilegalidade, de ofício ou por provocação de terceiros.

18.7 – Este Edital poderá ser retirado gratuitamente na Secretaria da Comissão Permanente de Licitação do SESCOOP/MG, localizada na Rua Ceará, nº 771, 3º andar, Bairro Funcionários, Belo Horizonte, Minas Gerais ou solicitado e enviado através de e-mail eletrônico.

18.8 – O Foro da Comarca de Belo Horizonte, Minas Gerais, será o competente para dirimir as questões oriundas desta licitação e da relação jurídica dela decorrente.

Belo Horizonte, 17 de junho de 2019.

Robert Martins Santos  
PREGOEIRO - Sescop/MG

## **ANEXO I**

### **TERMO DE REFERÊNCIA ESPECIFICAÇÕES DOS SERVIÇOS**

#### **OBJETO:**

Contratação de empresa especializada em fornecimento de solução de firewall, baseado em tecnologia (UTM) do inglês Unified Threat Management (Gerenciamento Unificado de Ameaças) com alta disponibilidade em formato appliance (dispositivo de hardware separado e discreto, selado, com software integrado e do mesmo fabricante do hardware), com implantação, suporte e garantia com o intuito de disponibilizar proteção digital à rede lógica do SESCOOP/MG

#### **JUSTIFICATIVA**

A solução proposta visa atender a necessidade de segurança com o consequente controle e bloqueio de permissões, seja indesejado ou não, que permita a mitigação de riscos, para a manutenção da disponibilidade e integridade das informações disponíveis na rede local de forma a estar aderente à Norma de Procedimento Interna de Segurança da Informação do SESCOOP/MG.

Consideramos que as corporações que fazem uso ou oferecem serviços por meio da Internet, redes parceiras ou por qualquer outro tipo de conexão, que interajam seus ambientes internos aos externos, devem ter extrema preocupação com esses canais de comunicação, pois além do benefício de permitir conectividade, também representam, em contrapartida, risco potencial para acessos não autorizados e maliciosos.

Para que seja possível manter o adequado nível de segurança em seus ambientes e, assim preservar os ativos corporativos (hardware, software e dados), de modo a garantir a integridade, confidencialidade e segurança das informações institucionais, torna-se imprescindível a adoção de soluções estratégicas que minimizem os riscos e evitem ocorrências de prejuízos técnicos e financeiros e não afetem a credibilidade institucional.

Nesse sentido, o emprego de soluções de Firewall possibilita que o tráfego de dados seja monitorado e controlado, a ponto de permitir o estabelecimento de um único canal de entrada e saída entre esses ambientes e permita a proteção preventiva da rede local. A arquitetura da solução proposta está focada nas melhores práticas de segurança e melhores ferramentas disponíveis no mercado para a segurança de ambientes corporativos, além dos benefícios inerentes aos novos equipamentos.

## ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

Lote	Item	Descrição	Quantidade
Lote Único	Item 1	Appliances de Segurança Incluindo Licenças de Segurança e alta disponibilidade do appliance completo.	2
	Item 2	Software de gerenciamento centralizado	1
	Item 3	Mão de obra para instalação da solução	1

### **1 Item 1 - Appliances de Segurança Incluindo Licenças de Segurança e alta disponibilidade do appliance completo.**

#### 1.1 Especificações de Performance e hardware

- 1.1.1 Performance de Firewall Stateful Packet Inspection igual ou superior a 3 (três) Gbps;
- 1.1.2 Performance de todos os serviços ativos UTM (Proteção Anti-Malware e Antivírus, IDS, IPS e Controle de Aplicação) deverá ser de 600 (seiscentos) Mbps ou superior. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA).
- 1.1.3 Performance de Inspeção (descriptografia e criptografia) de tráfego criptografado (SSL) de no mínimo 250 (duzentos e cinquenta) Mbps, os throughputs devem ser comprovados por documento de domínio público do fabricante. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA). Não serão aceitos declarações ou cartas de fabricantes para atendimento a este item;
- 1.1.4 Performance de IPS de 1400 (mil e quatrocentos) Mbps ou superior;
- 1.1.5 Suporte a, no mínimo, 1.000.000 (um milhão) de conexões do tipo SPI simultâneas
- 1.1.6 Suporte a, no mínimo, 500 (quinhentos mil) conexões do tipo DPI simultâneas;
- 1.1.7 Suporte a, no mínimo, 14.000 (quatorze mil) novas conexões por segundo;
- 1.1.8 Disco de armazenamento de no mínimo 16 Gb;
- 1.1.9 Deve ser fornecido com fonte de alimentação redundante com chaveamento automático de 100-240 VAC
- 1.1.10 Deverá possuir pelo menos 12(doze) interfaces de rede 10/100/1000 base-TX. Todas as interfaces devem possuir mecanismo de autosense e seleção de modo half/full duplex. A seleção da velocidade e duplex deve ser realizada obrigatoriamente através da interface gráfica de gerenciamento. As interfaces devem suportar as seguintes atribuições:

- 1.1.10.1 Segmento WAN , ou externo.
- 1.1.10.2 Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador.
- 1.1.10.3 Segmento LAN ou rede interna.
- 1.1.10.4 Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)
- 1.1.10.5 Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade
- 1.1.10.6 Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.
- 1.1.11 01 (uma) interface do tipo console ou similar;
- 1.1.12 01 (uma) interface de rede dedicada para gerenciamento;
- 1.1.13 A VPN SSL deve ser licenciada para, no mínimo, 2(dois) usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 300 (trezentos) usuários simultâneos, com aquisição de licença futura;
- 1.1.14 Suportar 1000 (mil) túneis de VPN IPSEC simultâneos;
- 1.1.15 Suportar, no mínimo, 1500 (mil e quinhentos) Mbps de throughput de VPN IPSEC;
- 1.1.16 O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovada através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.
- 1.1.17 Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de performance solicitados;
- 1.1.18 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e/ou end-of-sale ou situação semelhante.

## 1.2 CARACTERÍSTICAS GERAIS

- 1.2.1 Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;
- 1.2.2 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 1.2.3 O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 1.2.4 O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;
- 1.2.5 Não serão permitidas soluções baseadas em sistemas operacionais abertos(OpenSource) como Free BSD, Debian ou mesmo Linux;
- 1.2.6 Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;
- 1.2.7 Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

- 1.2.8 A solução deverá suportar monitoramento através de SNMP v2 e v3;
- 1.2.9 Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicializada de backups da configuração em determinado dia e hora;
- 1.2.10 Suporte à definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;
- 1.2.11 A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput;
- 1.2.12 A solução deve suportar configuração de port-redundancy de interfaces para a alta disponibilidade de interfaces;
- 1.2.13 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:
  - 1.2.13.1 Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
  - 1.2.13.2 Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
  - 1.2.13.3 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
  - 1.2.13.4 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;
  - 1.2.13.5 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
- 1.2.14 Possuir DHCP Server interno;
- 1.2.15 Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como DHCP Relay, suportando os protocolos e portas:
  - 1.2.15.1 Time service—UDP porta 37
  - 1.2.15.2 DNS—UDP porta 53
  - 1.2.15.3 DHCP—UDP portas 67 e 68
  - 1.2.15.4 Net-Bios DNS—UDP porta 137
  - 1.2.15.5 Net-Bios Datagram—UDP porta 138
  - 1.2.15.6 Wake On LAN—UDP porta 7 e 9
  - 1.2.15.7 mDNS—UDP porta 5353
  - 1.2.15.8 Suporte a Jumbo Frames;
  - 1.2.15.9 Implementar sub-interfaces ethernet lógicas;
  - 1.2.15.10 Deve suportar os seguintes tipos de NAT:
    - 1.2.15.11 Nat dinâmico (Many-to-1);
    - 1.2.15.12 Nat dinâmico (Many-to-Many);
    - 1.2.15.13 Nat estático (1-to-1);

- 1.2.15.14 NAT estático (Many-to-Many);
- 1.2.15.15 Nat estático bidirecional 1-to-1;
- 1.2.15.16 Tradução de porta (PAT);
- 1.2.15.17 NAT de origem;
- 1.2.15.18 NAT de destino;
- 1.2.16 Suportar NAT de origem e NAT de destino simultaneamente.
- 1.2.17 Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) ;
- 1.2.18 Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;
- 1.2.19 Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida.
- 1.2.20 Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);
- 1.2.21 Permitir remarcação de pacotes utilizando TOS e/ou DSCP;
- 1.2.22 Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas.
- 1.2.23 Suporte ao protocolo de roteamento multicast (PIM-SM);
- 1.2.24 Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;
- 1.2.25 Suportar Equal Cost Multi-Path (ECMP) ;
- 1.2.26 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 1.2.27 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3, RIPng);
- 1.2.28 A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6;
- 1.2.29 Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão de endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de endereço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques to tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e antivírus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;
- 1.2.30 Possui suporte a log via syslog;
- 1.2.31 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- 1.2.32 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall.
- 1.2.33 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 1.2.34 Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real.

### 1.3 Alta Disponibilidade

- 1.3.1 A solução deverá ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover;
- 1.3.2 Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;
- 1.3.3 O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge;
- 1.3.4 A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;
- 1.3.5 A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, para verificar a existência de problemas lógicos na rede e possibilitar failover;
- 1.3.6 A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;
- 1.3.7 A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster, incluindo, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;
- 1.3.8 A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os pares do cluster, status de sincronização das configurações, status atual equipamento backup.

### 1.4 VPN

- 1.4.1 Criptografia 3DES, AES 128 e AES 256;
- 1.4.2 Autenticação com MD5, SHA-1, SHA-256 e SHA-384;
- 1.4.3 Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits);
- 1.4.4 Algoritmo Internet Key Exchange (IKE);
- 1.4.5 Autenticação via certificado IKE PKI;
- 1.4.6 Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC`s;
- 1.4.7 A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;
- 1.4.8 Solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico;
- 1.4.9 Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;
- 1.4.10 Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;
- 1.4.11 Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

- 1.4.12 Permitir que seja criada políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;
- 1.4.13 Suportar a criação de túneis IP sobre IP (IPSEC Túnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

## 1.5 Autenticação

- 1.5.1 Permitir a utilização de LDAP, AD e RADIUS;
- 1.5.2 Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerência remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;
- 1.5.3 Suporte a uma rede com múltiplos domínios, possibilitando a integração em um ambiente onde existam domínios diferentes e totalmente segregados.
- 1.5.4 Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
- 1.5.5 Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7 , Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
- 1.5.6 Permitir a restrição de atribuição de perfil de acesso a um usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.
- 1.5.7 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;

## 1.6 IPS

- 1.6.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;
- 1.6.2 A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;
- 1.6.3 A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

- 1.6.4 A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;
- 1.6.5 Possuir capacidade de remontagem de pacotes para identificação de ataques;
- 1.6.6 O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;
- 1.6.7 Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante.
- 1.6.8 A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;
- 1.6.9 As regras de exceção devem possuir: origem, destino e serviço;
- 1.6.10 A solução deve ser capaz de inspecionar tráfego HTTPS.
- 1.6.11 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 1.6.12 Detecção de anomalias;
- 1.6.13 A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);
- 1.6.14 O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;
- 1.6.15 O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;
- 1.6.16 Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;
- 1.6.17 A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;
- 1.6.18 Deve incluir proteção contra worms;
- 1.6.19 Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao longo do tempo dispondo o sumário quantitativo das ameaças analisadas.
- 1.6.20 A solução deve possuir esquema de atualização de assinaturas através de um click;
- 1.6.21 Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;
- 1.6.22 A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);
- 1.6.23 A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;
- 1.6.24 A solução deverá possuir proteções para sistemas SCADA;
- 1.6.25 Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.
- 1.6.26 Possibilitar operação em modo de detecção baseado em base de assinaturas SNORT.

## 1.7 Controle de Aplicações

- 1.7.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades abaixo:
  - 1.7.1.1 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.
  - 1.7.1.2 Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers
  - 1.7.1.3 Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, WhatsApp, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.
  - 1.7.1.4 Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate, etc.
- 1.7.2 Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
- 1.7.3 Atualizar a base de assinaturas de aplicações automaticamente;
- 1.7.4 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- 1.7.5 A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;
- 1.7.6 Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;
- 1.7.7 Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, Email e extensão de arquivos.
- 1.7.8 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;
- 1.7.9 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 1.7.10 Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 1.7.11 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;
- 1.7.12 Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;
- 1.7.13 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
  - 1.7.13.1 Nível de risco da aplicação.
  - 1.7.13.2 Categoria de aplicações.

## 1.8 Filtro de URL

- 1.8.1 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;
- 1.8.2 Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;
- 1.8.3 Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;
- 1.8.4 A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL:
- 1.8.5 Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);
- 1.8.6 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);
- 1.8.7 Deve ser possível à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;
- 1.8.8 O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);
- 1.8.9 Deverá permitir criar política de confirmação de acesso ;
- 1.8.10 Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-in-the-middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;
- 1.8.11 O administrador poderá adicionar filtros por palavra-chave de modo específico;
- 1.8.12 Deverá permitir o bloqueio Web através de senha pré-configurada pelo administrador
- 1.8.13 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);
- 1.8.14 A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
- 1.8.15 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.
- 1.8.16 Suportar a criação de políticas baseadas no controle por URL e categoria de URL;
- 1.8.17 Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de máquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE, evitando delay de comunicação/validação das URLs;
- 1.8.18 Possuir pelo menos 50 categorias de URLs;
- 1.8.19 Suporta a criação de categorias de URLs customizadas;
- 1.8.20 Suporta a exclusão de URLs do bloqueio, por categoria;
- 1.8.21 Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;
- 1.8.22 A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

1.8.23 Permite a customização de página de bloqueio.

## 1.9 Proteção Contra Vírus e Bot-Nets

- 1.9.1 Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
- 1.9.2 Deve possuir módulo de antivírus e antibot integrado no próprio appliance de segurança;
- 1.9.3 A solução deve possuir nuvem de inteligência proprietária do fabricante sendo esta responsável em atualizar toda a base de segurança dos appliances através de assinaturas.
- 1.9.4 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 1.9.5 Implementar funcionalidade de detecção e bloqueio de callbacks;
- 1.9.6 A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;
- 1.9.7 A solução Antibot deve possuir mecanismo de detecção que inclui, reputação de endereço IP;
- 1.9.8 Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;
- 1.9.9 Implementar interface CLI segura através do protocolo SSH;
- 1.9.10 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;
- 1.9.11 A solução deve permitir criar regras de exceção de acordo com a proteção;
- 1.9.12 Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;
- 1.9.13 Permitir o bloqueio de malwares (vírus, worms, spyware e etc);
- 1.9.14 A solução deve ser capaz de proteger contra ataques para DNS;
- 1.9.15 A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;
- 1.9.16 A solução deve ser capaz de prevenir acesso a websites maliciosos;
- 1.9.17 A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH;
- 1.9.18 A solução deverá receber atualizações de um serviço baseado em cloud;
- 1.9.19 A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;
- 1.9.20 A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;
- 1.9.21 A solução deve suportar funcionalidade de GeolIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

## 1.10 Proteção Contra-Ataques Avançados

- 1.10.1 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;
- 1.10.2 Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;
- 1.10.3 A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH;
- 1.10.4 Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;
- 1.10.5 Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;
- 1.10.6 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;
- 1.10.7 Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, MacOS, Android, Linux;
- 1.10.8 Conter ameaças de dia zero permitindo ao usuário final o recebimento de arquivos livres de malware;
- 1.10.9 A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;
- 1.10.10 A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança do appliance através de assinaturas.
- 1.10.11 Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;
- 1.10.12 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 1.10.13 Conter ameaças avançadas de dia zero;
- 1.10.14 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;
- 1.10.15 Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;
- 1.10.16 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;
- 1.10.17 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;
- 1.10.18 Implementar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

- 1.10.19 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;
- 1.10.20 Conter ameaças de dia zero de forma transparente para o usuário final;
- 1.10.21 Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;
- 1.10.22 Implementar mecanismo de pesquisa por diferentes intervalos de tempo;
- 1.10.23 Conter ameaças de dia zero via tráfego de internet;
- 1.10.24 Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;
- 1.10.25 Conter ameaças de dia zero que possam burlar o sistema operacional emulado;
- 1.10.26 A solução deve permitir a criação de White list baseado no MD5 do arquivo;
- 1.10.27 Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;
- 1.10.28 Conter exploits avançados;
- 1.10.29 A análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);
- 1.10.30 Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

## 1.11 Administração

- 1.11.1 Suportar no mínimo 20.000 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Esta comprovação poderá ser exigida em testes sobre o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens.
- 1.11.2 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
- 1.11.3 Fornecer gerência remota, com interface gráfica nativa;
- 1.11.4 A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;
- 1.11.5 Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;
- 1.11.6 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

- 1.11.7 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- 1.11.8 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 1.11.9 Permitir a visualização de estatísticas do uso de CPU do firewall e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
- 1.11.10 Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.
- 1.11.11 Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 1.11.12 Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.
- 1.11.13 Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;
- 1.11.14 Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;
- 1.11.15 Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

## 1.12 Relatórios

- 1.12.1 Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;
- 1.12.2 Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);
- 1.12.3 Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em

caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;

- 1.12.4 Permitir o envio dos relatórios, através de email para usuários pré-definidos;
- 1.12.5 Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;
- 1.12.6 Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática
- 1.12.7 Disponibilizar download dos relatórios gerados.

### 1.13 Garantia Suporte e Licenciamento

- 1.13.1 O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 60(sessenta) meses.
- 1.13.2 A garantia deverá ser de 60(sessenta) meses.
- 1.13.3 Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:
  - 1.13.3.1 O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando no regime 8x5 com atendimento em língua portuguesa. Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente;
  - 1.13.3.2 Deve permitir o acesso à base de conhecimento da solução.

### 1.14 Conformidade

- 1.14.1 Deve ser comprovado que o fabricante da solução tem participação no MAPP da Microsoft;
- 1.14.2 A tecnologia da solução deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivírus;
- 1.14.3 O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 95 % (noventa por cento) da avaliação de segurança efetiva;
- 1.14.4 No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;
- 1.14.5 Deve ser homologado pela ANATEL.

## **2 Lote 1 – Item 2 – Solução de Gerenciamento Centralizado**

### 2.1 Características Gerais

- 2.1.1 Poderá ser composto de appliance ou máquina virtual únicos ou composição de appliances ou máquinas virtuais ou solução em nuvem, de forma a atender a todos os requisitos solicitados sem perda de funcionalidade. Em caso de appliance o hardware deve ser do mesmo fabricante do equipamento de firewall;
- 2.1.2 Além das opções de appliance e máquina virtual, a solução de gerenciamento centralizado também deverá suportar ser instalada em equipamentos com sistema operacional Windows 2012 Server ou superior;
- 2.1.3 Caso a solução entregue utilize virtualização deverá ser compatível com Hyper-V, VMware vSphere 5 ou superior;
- 2.1.4 Caso a solução seja fornecida em appliance, o armazenamento total em disco (SAS) deverá ser de no mínimo 2.25 TB de pelo menos 10000 RPM em operando em modo RAID 5. Estes discos poderão ainda ser substituídos pela contratante / contratada sem a paralisação parcial ou total do sistema;
- 2.1.5 Caso seja fornecida em appliance, deve possuir no mínimo 16 GB de memória RAM;
- 2.1.6 Caso seja fornecida em appliance, deve possuir no mínimo uma interface de rede 10/100/1000 Mbps;
- 2.1.7 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
- 2.1.8 Fornecer gerência remota, com interface gráfica nativa;
- 2.1.9 Registrar em log de auditoria as ações dos usuários administradores, registrando todas as alterações realizadas em uma política de segurança, permitindo a identificação do responsável pela mudança, o horário e a origem;
- 2.1.10 Permitir a criação de janela de mudança podendo executar regras imediatamente ou criar um agendamento;
- 2.1.11 A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos firewalls sem a necessidade de se executar várias interfaces;
- 2.1.12 A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPNs, NAT, perfis de acesso e regras de filtragem;
- 2.1.13 Facilidade de busca com, no mínimo, opção de consulta por: endereços IP específicos ou parte deles, usuário de rede, eventos duplicados, eventos não utilizados e associação de eventos com regras;
- 2.1.14 Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;
- 2.1.15 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

- 2.1.16 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- 2.1.17 A solução deve incluir uma opção de busca para poder consultar facilmente qualquer objeto de rede configurado;
- 2.1.18 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 2.1.19 Permitir a visualização para cada firewall gerenciado de estatísticas do uso de CPU, memória e tráfego de rede em todas as interfaces através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
- 2.1.20 Permitir a conexão simultânea de vários administradores no modo de visualização;
- 2.1.21 Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML e PDF: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;
- 2.1.22 Suportar a distribuição automática de relatórios por e-mail;
- 2.1.23 Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);
- 2.1.24 Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática em pelo menos três servidores web diferentes, através do protocolo FTP;
- 2.1.25 Prover mecanismo de visualização de eventos em tempo real das funções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações:
  - 2.1.25.1 Aplicações mais utilizadas;
  - 2.1.25.2 Usuários com maior atividade;
  - 2.1.25.3 Estatísticas de uso;
  - 2.1.25.4 Ataques e eventos do IPS correlacionados com o Common Vulnerabilities and Exposures (CVE);
  - 2.1.25.5 Principais aplicações por taxa de transferência de bytes;
  - 2.1.25.6 Principais hosts por número de ameaças identificadas;
- 2.1.26 Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
- 2.1.27 Deve permitir a criação de relatórios personalizados;
- 2.1.28 Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 2.1.29 Prover mecanismo de consulta às informações registradas integrado à interface de administração;
- 2.1.30 Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado;

2.1.31 A interface gráfica de visualização de logs deve possuir ferramenta de pesquisa que permita criar um filtro através de operadores lógicos (AND e OR) e coringas (\* e ?), facilitando assim a busca da informação.

## 2.2 Licenciaanexmento

2.2.1 A solução de gerenciamento centralizado deve estar licenciada para no mínimo poder gerenciar os appliances de segurança referentes ao item 1 do Lote 1 deste termo.

2.2.2 O período de licenciamento será de 05 (cinco) anos, onde a CONTRATANTE deverá receber os direitos de atualização da solução contratada.

## 2.3 Suporte Técnico

2.3.1 A solução de gerenciamento centralizado deverá ser fornecida com suporte técnico 7x24 diretamente pelo fabricante pelo período de 5 anos, mesmo estando vigente o suporte técnico da LICITANTE.

# 3 Lote 1 – Item 3 – Mão de obra para implantação da Solução

## 3.1 Serviços de Implantação

3.1.1 Deverão ser fornecidos todos os serviços necessários a implantação completa da solução incluindo documentação, treinamento hands-on e acompanhamento de entrada em produção;

3.1.2 Os serviços, incluem, mas não se limitam a:

3.1.2.1 Instalação física dos appliances de segurança;

3.1.2.2 Configuração da solução de gerenciamento centralizado;

3.1.2.3 Atualização de firmware dos appliances;

3.1.2.4 Aplicação de licenças;

3.1.2.5 Configuração das portas do appliance e sua interligação a rede;

3.1.2.6 Registro dos appliances na solução de gerenciamento centralizado;

3.1.2.7 Configuração do appliance para utilizar os links wan disponíveis, incluindo balanceamento de carga se necessário;

3.1.2.8 Configuração do cluster de alta disponibilidade em cada site;

3.1.2.9 Integração da solução ao Active Directory do contratante;

3.1.2.10 Configuração de segurança avançadas: IPS, filtro de conteúdo, antivírus, filtro de aplicações e demais funções de segurança da solução;

3.1.2.11 Configuração de VPN IPSEC entre sites;

3.1.2.12 Configuração de autenticação de convidados externos para utilização de acesso à Internet (via wifi e/ou rede cabeada) com armazenamento de logs de conexão e de acesso.

3.1.2.13 Configuração de DMZ para servidores web;

3.1.2.14 Quaisquer outras configurações dos appliances fornecidos caso necessárias a integração ao ambiente do CONTRATANTE;

- 3.1.2.15 Testes de funcionamento;
- 3.1.2.16 Configuração de relatórios e agendamento de envio por email;
- 3.1.2.17 Acompanhamento de entrada em produção;
- 3.1.2.18 Criação de documentação detalhada das configurações efetuadas;
- 3.1.2.19 Treinamento hands-on com entrega de manual das principais funções da solução;
- 3.1.3 Após o término da implantação da solução e aceite pelo CONTRATANTE a LICITANTE vencedora deverá prestar suporte direto, utilizando força própria, por um período mínimo de 90(noveenta) dias, visando atender o período de adaptação a solução onde surgirão dúvidas e necessidades de ajustes por parte do CONTRATANTE;
- 3.1.4 A solução deverá ser implantada por analista certificado pelo fabricante da solução ofertada. Deverá ser comprovado o vínculo empregatício deste profissional com a LICITANTE visando a garantia de qualidade de serviço de implantação e suporte durante o período de adaptação;
- 3.1.5 Os serviços que puderem gerar algum tipo de impacto ao ambiente do CONTRATANTE deverão obrigatoriamente ser executados em horários não comerciais e de acordo com agendamento prévio;
- 3.1.6 Em até 10 dias após a assinatura do contrato deverá ser criado cronograma prévio de todas as ações macro que serão efetuadas durante o processo de implantação para aprovação do CONTRATANTE;
- 3.1.7 Após recebimento dos equipamentos e licenças todos os serviços de implantação deverão ser concluídos num período máximo de 30 (trinta) dias corridos, iniciando a contagem assim que a CONTRATANTE der o aval para início do processo de implementação;

## **4 Local de Instalação dos Appliances**

- 4.1 Rua Ceará, 771 – Funcionários – Belo Horizonte / MG
- 4.2 Rua Carandaí, 335 – Funcionários – Belo Horizonte / MG

## ANEXO II

### MODELO DE CARTA PROPOSTA

Local e data

À Comissão Permanente de Licitação

**REF.: PROCESSO LICITATÓRIO – PREGÃO PRESENCIAL Nº 006/2019 – Contratação de empresa especializada em fornecimento de solução de firewall, baseado em tecnologia (UTM) do inglês Unified Threat Management (Gerenciamento Unificado de Ameaças) com alta disponibilidade em formato appliance (dispositivo de hardware separado e discreto, selado, com software integrado e do mesmo fabricante do hardware), com implantação, suporte e garantia com o intuito de disponibilizar proteção digital à rede lógica do SESCOOP/MG.**

A (razão social da empresa), inscrita no CNPJ sob o número \_\_\_\_\_, sediada (ou domiciliada) na (endereço completo), aqui representada pelo sr.(a) \_\_\_\_\_, carteira de identidade nº \_\_\_\_\_, CPF nº \_\_\_\_\_, tendo tomado conhecimento da licitação **PREGÃO PRESENCIAL Nº 006/2019**, manifesta seu interesse em apresentar proposta e o faz nas seguintes condições:

Item	Descrição	Qtde	Valor Unitário	Valor Total
01	Appliances de Segurança Incluindo Licenças de Segurança e alta disponibilidade do appliance completo. (licença de suporte e garantia 5 anos)	02		

Item	Descrição	Qtde	Valor Unitário	Valor Total
02	Software de gerenciamento centralizado (licença de uso 5 anos)	01		

Item	Descrição	Qtde	Valor Unitário	Valor Total
03	Mão de obra para instalação da solução	01		

**VALOR TOTAL GLOBAL PARA JULGAMENTO E LANCES VERBAIS: R\$ \_\_\_\_\_ (item 01 + item 02 + item 03)**

### DECLARAÇÃO

- Que o preço por nos ofertado é completo e já estão inclusas todas as despesas necessárias para cumprimento das obrigações, inclusive entrega, mão de obra e etc, conforme edital e Termo de Referência – ANEXO I;

- Nossa empresa se compromete a exercer suas atividades dentro dos preceitos legais, cumprir as convenções legais, ambientais e trabalhistas, não contratar mão de obra infantil, não adotar práticas discriminatórias e zelar pela ética nas suas relações.

- Informamos que tomamos conhecimento de todos os termos e condições do edital, bem como de seus anexos e não restando quaisquer dúvidas de nossa parte.

Informamos ainda que o Sr(a). \_\_\_\_\_, já qualificado (a) no preâmbulo, tem plenos poderes para representar este proponente no processo **PREGÃO PRESENCIAL Nº 006/2019**, estando apto para desistir do prazo recursal, agindo em nome desse proponente para todos os efeitos legais.

---

(Assinatura do representante legal da empresa)

### ANEXO III

#### MODELO DE PROCURAÇÃO

Obs.: O Licitante deverá apresentar no ato do Credenciamento documentação que comprove totais poderes para participar do **Pregão Presencial nº 006/2019** do Sescop/MG.

Por este Instrumento particular de Procuração, à (RAZÃO SOCIAL DA EMPRESA), com sede (ENDEREÇO COMPLETO DA MATRIZ) inscrita no CNPJ/MF sob nº 00.000.000/0000-00 e Inscrição Estadual sob nº 0000000000, representada neste ato por seu (QUALIFICAÇÃO DO OUTORGANTE) Sr(a) XXXXXXXXXXXX, portador(a) da Cédula de Identidade RG nº 0000000 SSP-XX e CPF nº 000.000.000-00, nomeia e constitui seu bastante Procurador o(a) Sr(a) XXXXXXXXXXXX, portador(a) da Cédula de Identidade RG nº 0000000 SSP-XX e CPF nº 000.000.000-00, a quem confere amplos poderes para representar a (RAZÃO SOCIAL DA EMPRESA) perante ao Serviço Nacional de Aprendizagem do Cooperativismo e Minas Gerais – Sescop/MG, com poderes para tomar qualquer decisão durante a Licitação, inclusive apresentar Proposta e Declaração de Atendimento dos Requisitos de Habilitação em nome da Outorgante, formular verbalmente novas Propostas de Preços na Etapa de Lances, desistir expressamente da Intenção de Interpor Recurso Administrativo, manifestar-se imediata e motivadamente a Intenção de Interpor Recurso Administrativo ao final da Sessão, Interpor Recurso Administrativo, assinar a Ata da Sessão, prestar todos os esclarecimentos solicitados pelo Pregoeiro, enfim, praticar todos os demais Atos pertinentes ao Certame em nome da Outorgante, inclusive assinar Contratos de Execução do Serviço e demais compromissos. A presente procuração é válida até o dia XX de XXXXXXXXXXXX de 20XX. Por ser verdade, firmamos a presente declaração para que se produza os efeitos legais.

#### (PROCURAÇÃO COM ASSINATURA COM FIRMA RECONHECIDA EM CARTÓRIO)

Local de data

---

(Assinatura do outorgante com poderes para este fim conforme  
Contrato Social da empresa carimbo da Empresa)

#### Observação:

1. A Procuração deverá vir acompanhada da documentação necessária para comprovação da validade da mesma, ou seja, contrato social ou estatuto

## ANEXO IV

### MODELO DE DECLARAÇÃO DE PLENO ATENDIMENTO À HABILITAÇÃO

Ao  
Sescoop/MG

Prezados Senhores:

Pelo presente, declaramos para efeito do cumprimento ao estabelecido neste edital, sob as penalidades cabíveis, que cumprimos plenamente aos requisitos da Proposta e dos documentos de Habilitação, exigidos no Edital do Pregão Presencial nº 006/2019.

Local e data

---

(Nome e assinatura do Representante Legal  
Carimbo da Empresa)

#### Observações:

1. Este atestado (ou declaração) deverá ser emitido em papel que identifique o órgão (ou empresa) emissor;
2. **Este documento deverá ser entregue ao pregoeiro no início da sessão, antes da abertura dos envelopes**

## ANEXO V

### MODELO DE ATESTADO DE CAPACIDADE TÉCNICA

Atestamos (ou declaramos) que a empresa \_\_\_\_\_, inscrita no CNPJ (MF) nº \_\_\_\_\_, inscrição estadual nº \_\_\_\_\_, estabelecida no (a) \_\_\_\_\_ prestou os serviços relativos a \_\_\_\_\_

Atestamos (ou declaramos), ainda, que os compromissos assumidos pela empresa foram cumpridos satisfatoriamente, nada constando em nossos arquivos que a desabone comercial ou tecnicamente.

Local e data

\_\_\_\_\_  
(Assinatura e carimbo do emissor)

#### Observações:

1. Este atestado (ou declaração) deverá ser emitido em papel que identifique o órgão (ou empresa) emissor;
2. O atestado deverá estar visado pelo respectivo órgão fiscalizador.

## ANEVO VI

### MODELO DE DECLARAÇÕES – EXIGÊNCIAS LEGAIS

Empresa ....., inscrita no CNPJ nº....., por intermédio de seu representante legal o(a) sr.(a)....., portador(a) da Carteira de Identidade nº..... e do CPF nº ....., **DECLARA sob as penas da Lei:**

- a) **ATENDIMENTO AO ART. 27, INCISO V da LEI 8666/93**, acrescido pela Lei 9.854/99, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos;
- b) **DE INEXISTÊNCIA DE FATO IMPEDITIVO PARA A HABILITAÇÃO:** que, até a presente data inexistem fato(s) impeditivo(s) para a sua habilitação, estando ciente da obrigatoriedade de declarar ocorrências posteriores;
- c) **DE CONHECIMENTO DO EDITAL:** ter recebido todos os documentos e informações, conhecer e acatar as condições para o cumprimento das obrigações objeto da licitação;
- d) **DE INEXISTÊNCIA DE IMPEDIMENTO PARA A PARTICIPAÇÃO:** que não incorre em nenhum dos casos relacionados no item 4 do edital;
- e) **DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA:** que a proposta apresentada foi elaborada de maneira independente, que não tentou influir na decisão de qualquer outro potencial participante desta licitação, e que com estes ou com outras pessoas não discutiu nem recebeu informações.

Local e data

\_\_\_\_\_  
(Assinatura do representante legal da empresa)  
CARIMBO/CNPJ

## ANEXO VII (MINUTA DO CONTRATO)

TIPO: CPS
Nº: XX/2019

**CONTRATO** que entre si celebram o **Serviço Nacional de Aprendizagem do Cooperativismo de Minas Gerais– SESCOOP/MG** e a **XXXXXXXXXXXXXX**

### CLAUSULA PRIMEIRA: DAS PARTES

1.1. **O SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS, SESCOOP/MG**, denominado **CONTRATANTE**, com sede em Belo Horizonte/MG, na Rua Ceará, nº 771, Bairro Funcionários, CEP 30150-311, inscrito no CNPJ sob o nº 07.064.534/0001-20, neste ato representado por seu Presidente RONALDO SCUCATO, CPF nº XXXXX, C.I. M-XXXXX e por seu superintendente ALEXANDRE GATTI LAGES, portador do CPF nº XXXXX e C.I. nº M XXXX, SSP/MG e

1.2. **XXXXXXXXXXXXXXXXXXXX** doravante denominada **CONTRATANTE**, com sede na Avenida XXXXXX, nº XXX, Bairro XXXXX, CEP: XXXXXX, no Município de Belo Horizonte, no Estado de Minas Gerais, inscrito no CNPJ nº XXXXXXXX, Inscrição Estadual nº XXXXXXXXXXXX, representado por XXXXXXXXXXXXXXXXXXXX, portador do CPF nº XXXXXXXXXXXXXXXX e C.I. nº XXXXXXXXXXXX.

### CLAUSULA SEGUNDA: DA DOCUMENTAÇÃO

As partes acordam que passa a fazer parte deste **CONTRATO**, os seguintes documentos:

- 2.1 Edital Pregão Presencial nº 006/2019 do SESCOOP/MG;
- 2.2 Proposta da **CONTRATADA** datada de XX/06/2019; e
- 2.3 Termo de Homologação e de Adjudicação, datado de XX/XX/2019.

### CLÁUSULA TERCEIRA: DO OBJETO

Constitui objeto deste **CONTRATO**, a prestação, pela **CONTRATADA** em fornecimento de solução de firewall, baseado em tecnologia (UTM) do inglês *Unified Threat Management* (Gerenciamento Unificado de Ameaças) com alta disponibilidade em formato *appliance* (dispositivo de hardware separado e discreto, selado, com software integrado e do mesmo fabricante do hardware), com implantação, suporte e garantia com o intuito de disponibilizar proteção digital à rede lógica do SESCOOP/MG.

### CLAUSULA QUARTA: DAS OBRIGAÇÕES DAS PARTES

#### 4.1. DO CONTRATANTE:

- 4.1.1. Acompanhar e supervisionar a execução do objeto deste **CONTRATO**, bem como questionar eventualidades que desvirtuem o caráter intrínseco dos mesmos.
- 4.1.2. Prestar as informações e os esclarecimentos que forem solicitados pela **CONTRATADA** durante o prazo de vigência do Contrato.
- 4.1.3. Colaborar no que lhe couber e for possível para o bom desempenho do objeto deste **CONTRATO**.
- 4.1.4. Efetuar os pagamentos conforme Clausula 5ª do presente contrato.
- 4.1.5. Rejeitar, no todo ou em parte, serviços ou fornecimentos executados em desacordo com o **CONTRATO**.

#### 4.2. DA CONTRATADA:

4.2.1. Executar o objeto do presente **CONTRATO**, nas condições exigidas no Edital Pregão Presencial nº 006/2019, inclusive o que consta nos anexos desta. Mantendo as condições de habilitação e qualificação técnica exigida no Edital Pregão Presencial nº 006/2019 e observar as diretrizes constantes neste **CONTRATO**.

4.2.2. Prestar serviços dentro dos parâmetros e rotinas estabelecidos, com observância às recomendações aceitas pela boa técnica de procedimentos, das normas e legislação que regulamentam o objeto.

4.2.3. Manter os valores ofertados no Pregão Presencial nº 006/2019.

ou 4.2.4. Manter absoluto sigilo sobre quaisquer informações de que venha a tomar conhecimento ter acesso quando da execução do objeto do presente instrumento.

4.2.5. Atender, as solicitações do SESCOOP-MG, adotando todas as providências necessárias à regularização de faltas e irregularidades verificadas.

4.2.6. Os serviços de implantação deverão ser fornecidos com todos os serviços necessários a implantação completa da solução incluindo documentação, treinamento hands-on e acompanhamento de entrada em produção.

4.2.7. Os serviços, incluem, mas não se limitam a:

- Instalação física dos appliances de segurança;
- Configuração da solução de gerenciamento centralizado;
- Atualização de firmware dos appliances;
- Aplicação de licenças;
- Configuração das portas do appliance e sua interligação a rede;
- Registro dos appliances na solução de gerenciamento centralizado;
- Configuração do appliance para utilizar os links wan disponíveis, incluindo balanceamento de carga se necessário;
- Configuração do cluster de alta disponibilidade em cada site;
- Integração da solução ao Active Directory do contratante;
- Configuração de segurança avançadas: IPS, filtro de conteúdo, antivírus, filtro de aplicações e demais funções de segurança da solução;
- Configuração de VPN IPSEC entre sites;
- Configuração de autenticação de convidados externos para utilização de acesso à Internet (via wifi e/ou rede cabeada) com armazenamento de logs de conexão e de acesso.
- Configuração de DMZ para servidores web;
- Quaisquer outras configurações dos appliances fornecidos caso necessárias a integração ao ambiente do CONTRATANTE;
- Testes de funcionamento;
- Configuração de relatórios e agendamento de envio por email;
- Acompanhamento de entrada em produção;
- Criação de documentação detalhada das configurações efetuadas;
- Treinamento hands-on com entrega de manual das principais funções da solução;

4.2.8. A solução deverá ser implantada por analista certificado pelo fabricante da solução ofertada. Deverá ser comprovado o vínculo empregatício deste profissional com a CONTRATADA visando a garantia de qualidade de serviço de implantação e suporte durante o período de adaptação;

4.2.9. Os serviços que puderem gerar algum tipo de impacto ao ambiente do CONTRATANTE deverão obrigatoriamente ser executados em horários não comerciais e de acordo com agendamento prévio;

4.2.10. Em até 10 dias após a assinatura do contrato deverá ser criado cronograma prévio de todas as ações macro que serão efetuadas durante o processo de implantação para aprovação do CONTRATANTE. Este prazo de 10 dias deverá estar incluso no período máximo de 60 dias previstos para fornecimento e implantação completa do ambiente;

4.2.11. Após recebimento dos equipamentos e licenças todos os serviços de implantação deverão ser concluídos num período máximo de 30 (trinta) dias corridos, iniciando a contagem assim que a CONTRATANTE der o aval para início do processo de implementação;

#### **CLAUSULA QUINTA: DO VALOR E DA FORMA DE PAGAMENTO**

5.1. O valor global do contrato é de R\$ XXX,00 (XXXXX reais), considerando para tal o valor de R\$ XXXX, referente a Appliances de Segurança Incluindo Licenças de Segurança e alta disponibilidade do appliance completo, o valor de R\$XXX referente ao Software de gerenciamento centralizado e o valor de R\$XXX referente a mão de obra para instalação da solução; conforme Termo de Homologação e de Adjudicação datado de XX/XX/2019 e proposta da CONTRATADA de XX/XX/2019;

5.2. O faturamento poderá ocorrer imediatamente após o fornecimento, sendo que o pagamento será efetuado mediante apresentação da Nota Fiscal / Fatura, devidamente aprovada pela Gerência Administrativa do SESCOOP/MG, conforme tabela abaixo:

<b>Data de entrega do Recibo</b>	<b>Data de pagamento</b>
Do dia 1º ao dia 10 do mês	Até o dia 20 do mês
Do dia 11 ao dia 20 do mês	Até o dia 30 do mês
Do dia 21 ao dia 30/31 do mês	Até o dia 10 do mês subsequente

5.3. Para processar-se o pagamento, a licitante vencedora deverá submeter ao SESCOOP/MG à(s) competente(s) nota(s) fiscal(is)/fatura(s);

5.4. Nenhum pagamento será feito à **CONTRATADA** enquanto perdurar qualquer pendência contratual.

5.5. No caso de incorreção na(s) Nota(s) Fiscal(is), esta(s) será(ão) restituída(s) à Contratada para as correções solicitadas. O prazo de pagamento será contado a partir da data da regularização do serviço ou do documento fiscal, não respondendo o SESCOOP/MG por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes;

5.6. No caso de emissão de Nota(s) Fiscal(is) na forma “eletrônica”, a licitante fica obrigada a enviar juntamente com o documento o arquivo eletrônico denominado “XML” para fins de conferência e fechamento junto a receita estadual. A(s) Nota(s) Fiscal(is) ficará(ão) retida(s) para pagamento, até o envio do presente arquivo;

5.7. A emissão e envio das notas fiscais deverão ocorrer até o dia 25 de cada mês. Após esta data, a mesma deverá ser emitida no 1º dia do mês subsequente à prestação do serviço. Este procedimento se faz necessário em virtude do prazo para recolhimento dos impostos. A emissão das notas fiscais no 1º dia do mês subsequente ao da prestação dos serviços realizados entre os dias 25 e 30/31, não sofrerão alteração na sua programação de pagamento, prevista para o dia 10.

5.8. O pagamento de taxas, impostos, licenças, emolumentos, demais tributos e encargos sociais que incidam sobre os serviços contratados serão de exclusiva responsabilidade da CONTRATADA;

#### **CLÁUSULA SEXTA: DA VIGÊNCIA E EXECUÇÃO DOS SERVIÇOS**

6.1. O prazo de fornecimento e implantação completa do ambiente deverá ser de até 60 (sessenta) dias, já inclusos neste prazo o período previsto no item 4.2.10.

6.2. Após o término da implantação da solução e aceite pelo CONTRATANTE a CONTRATADA deverá prestar suporte direto, utilizando força própria, por um período mínimo de 90 (noventa) dias, iniciando-se na data de sua assinatura, podendo ser prorrogado sucessivamente, se do interesse das partes, mediante termo aditivo, visando atender o período de adaptação a solução onde surgirão dúvidas e necessidades de ajustes por parte do CONTRATANTE.

6.3. O prazo de vigência, garantia e de suporte do fabricante será de 60 (sessenta) meses.

#### **CLÁUSULA SÉTIMA: DO PESSOAL, RESPONSABILIDADE E ÔNUS FISCAIS**

7.1. A **CONTRATADA** será a única responsável pelos seus empregados ou contratados para o desempenho do objeto do presente, bem como por todas as exigências da legislação trabalhista e de previdência social, não existindo entre seus empregados, contratados e/ou cooperados e o **CONTRATANTE** nenhum vínculo empregatício ou de qualquer outra natureza.

#### **CLÁUSULA OITAVA: DAS PENALIDADES**

8.1. A inexecução total ou parcial injustificada, a execução deficiente, irregular ou inadequada do objeto do presente contrato, assim como o descumprimento dos prazos e condições estipulados e, sem prejuízo das mesmas, implicarão nas penalidades abaixo mencionadas:

8.1.1. Advertência;

8.1.2. Cancelamento do contrato;

8.1.3. Multa por atraso de entrega dos serviços, no percentual de 0,5% (meio por cento) ao dia referente a etapa em atraso, limitada a 10% (dez por cento) do valor total do **CONTRATO**;

8.1.4. Suspensão temporária do direito de participar em licitação e impedimento de contratar com o **Sescoop/MG**, por prazo de até 02 (dois) anos.

8.2. Ocorrendo a aplicação de multa, esta será descontada sobre o valor da nota fiscal/fatura ou dos créditos a que a empresa licitante vencedora fizer "jus", no ato do pagamento, ou recolhidas diretamente à tesouraria do **CONTRATANTE**, ou ainda, quando for o caso, cobrada judicialmente;

8.3. Para aplicação das penalidades aqui previstas, a **CONTRATADA** será notificada para apresentação de defesa prévia, no prazo de 05 (cinco) dias, contados da notificação.

8.4. As penalidades previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis, tal como a rescisão contratual.

#### **CLÁUSULA NONA: DA RESCISÃO**

9.1. O não cumprimento pelas partes, das obrigações assumidas por este instrumento, importará em sua rescisão de pleno direito, independentemente de interpelação judicial.

9.2. O **CONTRATANTE**, a qualquer tempo, por questões administrativas/financeiras, mediante aviso por escrito com 30 (trinta) dias de antecedência, poderá rescindir o presente **CONTRATO**, desde que efetue todos os pagamentos à **CONTRATADA**, pelo fornecimento executado até aquela data.

#### **CLÁUSULA DÉCIMA: DA TOLERÂNCIA QUANTO ÀS DISPOSIÇÕES CONTRATUAIS E REMÉDIOS JURÍDICOS**

10.1. Nenhuma omissão ou demora por parte do **SESCOOP/MG** em exercer qualquer direito ou remédio jurídico estabelecido neste **CONTRATO** ou previsto em Lei, deverá operar ou se constituir em renúncia do mesmo; e

10.2. Nenhum dispositivo ou direito contratual será tido como renunciado pela **SESCOOP/MG**, a menos que essa renúncia seja feita por escrito.

#### **CLAUSULA DÉCIMA PRIMEIRA – DO ACOMPANHAMENTO**

11.1. Ao **SESCOOP/MG** ficará assegurado o direito de acompanhar a execução dos trabalhos desenvolvidos pela **CONTRATADA**, assim como questionar quaisquer eventualidades que desvirtuem o caráter intrínseco do mesmo.

11.2. Os serviços da **CONTRATADA** serão acompanhados pelo funcionário **XXXXXX**, CPF: XXXXX, ou na falta desta, por quem o **SESCOOP/MG** indicar para cumprir a função.

## **CLÁUSULA DÉCIMA SEGUNDA: DA ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO**

<b>Lote</b>	<b>Item</b>	<b>Descrição</b>	<b>Quantidade</b>
Lote Único	Item 1	Appliances de Segurança Incluindo Licenças de Segurança e alta disponibilidade do appliance completo.	2
	Item 2	Software de gerenciamento centralizado	1
	Item 3	Mão de obra para instalação da solução	1

### **12.1 Da Appliances de Segurança Incluindo Licenças de Segurança e alta disponibilidade do appliance completo.**

#### **12.1.1. Especificações de Performance e hardware:**

- 12.1.1.1. Performance de Firewall Stateful Packet Inspection igual ou superior a 3 (três) Gbps;
- 12.1.1.2. Performance de todos os serviços ativos UTM (Proteção Anti-Malware e Antivírus, IDS, e Controle de Aplicação) deverá ser de 600 (seiscentos) Mbps ou superior. Caso o fornecedor possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA).
- 12.1.1.3. Performance de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL) no mínimo 250 (duzentos e cinquenta) Mbps, os throughputs devem ser comprovados por documento de domínio público do fabricante. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA). Não serão aceitos declarações ou cartas de fabricantes para atendimento a este item;
- 12.1.1.4. Performance de IPS de 1400 (mil e quatrocentos) Mbps ou superior;
- 12.1.1.5. Suporte a, no mínimo, 1.000.000 (um milhão) de conexões do tipo SPI simultâneas;
- 12.1.1.6. Suporte a, no mínimo, 500 (quinhentos mil) conexões do tipo DPI simultâneas;
- 12.1.1.7. Suporte a, no mínimo, 14.000 (quatorze mil) novas conexões por segundo;
- 12.1.1.8. Disco de armazenamento de no mínimo 16 Gb;
- 12.1.1.9. Deve ser fornecido com fonte de alimentação redundante com chaveamento automático de 100-240 VAC;
- 12.1.1.10. Deverá possuir pelo menos 12(doze) interfaces de rede 10/100/1000 base-TX. Todas as interfaces devem possuir mecanismo de autosense e seleção de modo half/full duplex. A seleção da velocidade e duplex deve ser realizada obrigatoriamente através da interface gráfica de gerenciamento. As interfaces devem suportar as seguintes atribuições:
- 12.1.1.10.1. Segmento WAN , ou externo.
- 12.1.1.10.2. Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador.
- 12.1.1.10.3. Segmento LAN ou rede interna.
- 12.1.1.10.4. Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)
- 12.1.1.10.5. Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade
- 12.1.1.10.6. Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.
- 12.1.1.11. 01 (uma) interface do tipo console ou similar;

12.1.1.12. 01 (uma) interface de rede dedicada para gerenciamento;  
12.1.1.13. A VPN SSL deve ser licenciada para, no mínimo, 2(dois) usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 300 (trezentos) usuários simultâneos, com aquisição de licença futura;  
12.1.1.14. Suportar 1000 (mil) túneis de VPN IPSEC simultâneos;  
12.1.1.15. Suportar, no mínimo, 1500 (mil e quinhentos) Mbps de throughput de VPN IPSEC;  
12.1.1.16. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovada através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.  
12.1.1.17. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de performance solicitados;

## 12.1.2 CARACTERÍSTICAS GERAIS

12.1.2.1. Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;  
12.1.2.2. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;  
12.1.2.3. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;  
12.1.2.4. O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;  
12.1.2.5. Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux;  
12.1.2.6. Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;  
12.1.2.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;  
12.1.2.8. A solução deverá suportar monitoramento através de SNMP v2 e v3;  
12.1.2.9. Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicializada de backups da configuração em determinado dia e hora;  
12.1.2.10. Suporte à definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;  
12.1.2.11. A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput;  
12.1.2.12. A solução deve suportar configuração de port-redundancy de interfaces para a alta disponibilidade de interfaces;  
12.1.2.13. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:  
12.1.2.13.1. Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);  
12.1.2.13.2. Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;  
12.1.2.13.3. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;  
12.1.2.13.4. 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;  
12.1.2.13.5. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.  
12.1.2.14. Possuir DHCP Server interno;

12.1.2.15. Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como DHCP Relay, suportando os protocolos e portas:

- 12.1.2.15.1. Time service—UDP porta 37
- 12.1.2.15.2. DNS—UDP porta 53
- 12.1.2.15.3. DHCP—UDP portas 67 e 68
- 12.1.2.15.4. Net-Bios DNS—UDP porta 137
- 12.1.2.15.5. Net-Bios Datagram—UDP porta 138
- 12.1.2.15.6. Wake On LAN—UDP porta 7 e 9
- 12.1.2.15.7. mDNS—UDP porta 5353
- 12.1.2.15.8. Suporte a Jumbo Frames;
- 12.1.2.15.9. Implementar sub-interfaces ethernet lógicas;
- 12.1.2.15.10. Deve suportar os seguintes tipos de NAT:
- 12.1.2.15.11. Nat dinâmico (Many-to-1);
- 12.1.2.15.12. Nat dinâmico (Many-to-Many);
- 12.1.2.15.13. Nat estático (1-to-1);
- 12.1.2.15.14. NAT estático (Many-to-Many);
- 12.1.2.15.15. Nat estático bidirecional 1-to-1;
- 12.1.2.15.16. Tradução de porta (PAT);
- 12.1.2.15.17. NAT de origem;
- 12.1.2.15.18. NAT de destino;

12. 1.2.16. Suportar NAT de origem e NAT de destino simultaneamente.

12.1.2.17. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);

tanto 12.1.2.18. Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

12.1.2.19. Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida.

(Differentiated Services Code Points); 12.1.2.20. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP

12.1.2.21. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

de 12.1.2.22. Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas.

12.1.2.23. Suporte ao protocolo de roteamento multicast (PIM-SM);

12.1.2.24. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

12.1.2.25. Suportar Equal Cost Multi-Path (ECMP) ;

12.1.2.26. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

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

com 12.1.2.28. A solução deve suportar integralmente o padrão IPv6, assim como criação de regras objetos que utilizem endereços IPv4 e IPv6;

de 12.1.2.29. Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de endereço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques to tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e antivírus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;

12.1.2.30. Possui suporte a log via syslog;

12.1.2.31. Possui mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

se 12.1.2.32. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que encontrem ativas através do firewall.

utilizados 12.1.2.33. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

12.1.2.34. Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real.

### **12.1.3. Alta Disponibilidade**

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

12.1.3.2. Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;

12.1.3.3. O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge;

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

12.1.3.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, para verificar a existência de problemas lógicos na rede e possibilitar failover;

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

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

12.1.3.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os pares do cluster, status de sincronização das configurações, status atual equipamento backup.

### **12.1.4 VPN**

12.1.4.1. Criptografia 3DES, AES 128 e AES 256;

12.1.4.2. Autenticação com MD5, SHA-1, SHA-256 e SHA-384;

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

12.1.4.4. Algoritmo Internet Key Exchange (IKE);

12.1.4.5. Autenticação via certificado IKE PKI;

12.1.4.6. Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC's;

12.1.4.7. A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;

12.1.4.8. Solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico;

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

12.1.4.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

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

12.1.4.12. Permitir que seja criadas políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;

12.1.4.13. Suportar a criação de túneis IP sobre IP (IPSEC Túnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

### **12.1.5. Autenticação**

12.1.5.1. Permitir a utilização de LDAP, AD e RADIUS;

12.1.5.2. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerência remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;

12.1.5.3. Suporte a uma rede com múltiplos domínios, possibilitando a integração em um ambiente onde existam domínios diferentes e totalmente segregados.

12.1.5.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;

12.1.5.5. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;

12.1.5.6. Permitir a restrição de atribuição de perfil de acesso a um usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.

12.1.5.7. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;

#### **12.1.6. IPS**

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

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

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

12.1.6.4. A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada; 12.1.6.5. Possuir capacidade de remontagem de pacotes para identificação de ataques;

12.1.6.6. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

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

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

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

12.1.6.10. A solução deve ser capaz de inspecionar tráfego HTTPS.

12.1.6.11. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

12.1.6.12. Detecção de anomalias;

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

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

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

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

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

12.1.6.18. Deve incluir proteção contra worms;

- 12.1.6.19. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao longo do tempo dispondo o sumário quantitativo das ameaças analisadas.
- 12.1.6.20. A solução deve possuir esquema de atualização de assinaturas através de um click;
- 12.1.6.21. Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;
- 12.1.6.22. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);
- 12.1.6.23. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;
- 12.1.6.24. A solução deverá possuir proteções para sistemas SCADA;
- 12.1.6.25. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.
- 12.1.6.26. Possibilitar operação em modo de detecção baseado em base de assinaturas SNORT.

### **12.1.7. Controle de Aplicações**

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

12.1.7.1.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.

12.1.7.1.2. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers

12.1.7.1.3. Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, WhatsApp, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.

12.1.7.1.4. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate, etc.

12.1.7.2. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

12.1.7.3. Atualizar a base de assinaturas de aplicações automaticamente;

12.1.7.4. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

12.1.7.5. A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;

12.1.7.6. Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;

12.1.7.7. Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, Email e extensão de arquivos.

12.1.7.8. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

12.1.7.9. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

12.1.7.10. Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;

12.1.7.11. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;

12.1.7.12. Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;

12.1.7.13. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

12.1.7.13.1. Nível de risco da aplicação.

12.1.7.13.2. Categoria de aplicações.

### **12.1.8. Filtro de URL**

12.1.8.1. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;

12.1.8.2. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

12.1.8.3. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;

12.1.8.4. A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL:

12.1.8.5. Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);

12.1.8.6. 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);

12.1.8.7. Deve ser possível à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;

12.1.8.8. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);

12.1.8.9. Deverá permitir criar política de confirmação de acesso ;

12.1.8.10. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-in-the-middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;

12.1.8.11. O administrador poderá adicionar filtros por palavra-chave de modo específico;

12.1.8.12. Deverá permitir o bloqueio Web através de senha pré-configurada pelo administrador

12.1.8.13. 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);

12.1.8.14. A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

12.1.8.15. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.

12.1.8.16. Suportar a criação de políticas baseadas no controle por URL e categoria de URL;

12.1.8.17. Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de máquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE, evitando delay de comunicação/validação das URLs;

12.1.8.18. Possuir pelo menos 50 categorias de URLs;

12.1.8.19. Suporta a criação de categorias de URLs customizadas;

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

12.1.8.21. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

12.1.8.22. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;

12.1.8.23. Permite a customização de página de bloqueio.

### **12.1.9. Proteção Contra Vírus e Bot-Nets**

- 12.1.9.1. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
- 12.1.9.2. Deve possuir módulo de antivírus e antibot integrado no próprio appliance de segurança;
- 12.1.9.3. A solução deve possuir nuvem de inteligência proprietária do fabricante sendo esta responsável em atualizar toda a base de segurança dos appliances através de assinaturas.
- 12.1.9.4. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 12.1.9.5. Implementar funcionalidade de detecção e bloqueio de callbacks;
- 12.1.9.6. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;
- 12.1.9.7. A solução Antibot deve possuir mecanismo de detecção que inclui, reputação de endereço IP;
- 12.1.9.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;
- 12.1.9.9. Implementar interface CLI segura através do protocolo SSH;
- 12.1.9.10. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;
- 12.1.9.11. A solução deve permitir criar regras de exceção de acordo com a proteção;
- 12.1.9.12. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;
- 12.1.9.13. Permitir o bloqueio de malwares (vírus, worms, spyware e etc);
- 12.1.9.14. A solução deve ser capaz de proteger contra ataques para DNS;
- 12.1.9.15. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;
- 12.1.9.16. A solução deve ser capaz de prevenir acesso a websites maliciosos;
- 12.1.9.17. A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH;
- 12.1.9.18. A solução deverá receber atualizações de um serviço baseado em cloud;
- 12.1.9.19. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;
- 12.1.9.20. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;
- 12.1.9.21. A solução deve suportar funcionalidade de GeolIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

#### **12.1.10. Proteção Contra-Ataques Avançados**

- 12.1.10.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;
- 12.1.10.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;
- 12.1.10.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH;
- 12.1.10.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;
- 12.1.10.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;
- 12.1.10.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;
- 12.1.10.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, MacOS, Android, Linux;
- 12.1.10.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento de arquivos livres de malware;

- 12.1.10.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;
- 12.1.10.10. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança do appliance através de assinaturas.
- 12.1.10.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;
- 12.1.10.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 12.1.10.13. Conter ameaças avançadas de dia zero;
- 12.1.10.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;
- 12.1.10.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;
- 12.1.10.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;
- 12.1.10.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;
- 12.1.10.18. Implementar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 12.1.10.19. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;
- 12.1.10.20. Conter ameaças de dia zero de forma transparente para o usuário final;
- 12.1.10.21. Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;
- 12.1.10.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;
- 12.1.10.23. Conter ameaças de dia zero via tráfego de internet;
- 12.1.10.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;
- 12.1.10.25. Conter ameaças de dia zero que possam burlar o sistema operacional emulado;
- 12.1.10.26. A solução deve permitir a criação de White list baseado no MD5 do arquivo;
- 12.1.10.27. Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;
- 12.1.10.28. Conter exploits avançados;
- 12.1.10.29. A análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede);
- 12.1.10.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

#### **12.1.11. Administração**

- 12.1.11.1. Suportar no mínimo 20.000 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Esta comprovação poderá ser exigida em testes sobre o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens.
- 12.1.11.2. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
- 12.1.11.3. Fornecer gerência remota, com interface gráfica nativa;

- 12.1.11.4. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;
- 12.1.11.5. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;
- 12.1.11.6. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- 12.1.11.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- 12.1.11.8. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 12.1.11.9. Permitir a visualização de estatísticas do uso de CPU do firewall e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
- 12.1.11.10. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.
- 12.1.11.11. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 12.1.11.12. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.
- 12.1.11.13. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;
- 12.1.11.14. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;
- 12.1.11.15. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

#### **12.1.12. Relatórios**

- 12.1.12.1. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;
- 12.1.12.2. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);
- 12.1.12.3. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;
- 12.1.12.4. Permitir o envio dos relatórios, através de email para usuários pré-definidos;
- 12.1.12.5. Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;
- 12.1.12.6. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática
- 12.1.12.7. Disponibilizar download dos relatórios gerados.

### **12.1.13. Garantia Suporte e Licenciamento**

12.1.13.1. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 60(sessenta) meses.

12.1.13.2. A garantia deverá ser de 60(sessenta) meses.

12.1.13.3. Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:

12.1.13.3.1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando no regime 8x5 com atendimento em língua portuguesa. Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente;

12.1.13.3.2. Deve permitir o acesso à base de conhecimento da solução.

### **12.1.14. Conformidade**

12.1.14.1. Deve ser comprovado que o fabricante da solução tem participação no MAPP da Microsoft;

12.1.14.2. A tecnologia da solução deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivírus;

12.1.14.3. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 95 % (noventa por cento) da avaliação de segurança efetiva;

12.1.14.4. No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;

12.1.14.5. Deve ser homologado pela ANATEL.

## **12.2. Solução de Gerenciamento Centralizado**

### **12.2.1. Características Gerais**

12.2.1.1. Poderá ser composto de appliance ou máquina virtual únicos ou composição de appliances ou máquinas virtuais ou solução em nuvem, de forma a atender a todos os requisitos solicitados sem perda de funcionalidade. Em caso de appliance o hardware deve ser do mesmo fabricante do equipamento de firewall;

12.2.1.2. Além das opções de appliance e máquina virtual, a solução de gerenciamento centralizado também deverá suportar ser instalada em equipamentos com sistema operacional Windows 2012 Server ou superior;

12.2.1.3. Caso a solução entregue utilize virtualização deverá ser compatível com Hyper-V, VMware vSphere 5 ou superior;

12.2.1.4. Caso a solução seja fornecida em appliance, o armazenamento total em disco (SAS) deverá ser de no mínimo 2.25 TB de pelo menos 10000 RPM em operando em modo RAID 5. Estes discos poderão ainda ser substituídos pela contratante / contratada sem a paralisação parcial ou total do sistema;

12.2.1.5. Caso seja fornecida em appliance, deve possuir no mínimo 16 GB de memória RAM;

12.2.1.6. Caso seja fornecida em appliance, deve possuir no mínimo uma interface de rede 10/100/1000 Mbps;

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

12.2.1.8. Fornecer gerência remota, com interface gráfica nativa;

- 12.2.1.9. Registrar em log de auditoria as ações dos usuários administradores, registrando todas as alterações realizadas em uma política de segurança, permitindo a identificação do responsável pela mudança, o horário e a origem;
- 12.2.1.10. Permitir a criação de janela de mudança podendo executar regras imediatamente ou criar um agendamento;
- 12.2.1.11. A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos firewalls sem a necessidade de se executar várias interfaces;
- 12.2.1.12. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPNs, NAT, perfis de acesso e regras de filtragem;
- 12.2.1.13. Facilidade de busca com, no mínimo, opção de consulta por: endereços IP específicos ou parte deles, usuário de rede, eventos duplicados, eventos não utilizados e associação de eventos com regras;
- 12.2.1.14. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;
- 12.2.1.15. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- 12.2.1.16. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- 12.2.1.17. A solução deve incluir uma opção de busca para poder consultar facilmente qualquer objeto de rede configurado;
- 12.2.1.18. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 12.2.1.19. Permitir a visualização para cada firewall gerenciado de estatísticas do uso de CPU, memória e tráfego de rede em todas as interfaces através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
- 12.2.1.20. Permitir a conexão simultânea de vários administradores no modo de visualização;
- 12.2.1.21. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML e PDF: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;
- 12.2.1.22. Suportar a distribuição automática de relatórios por e-mail;
- 12.2.1.23. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);
- 12.2.1.24. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática em pelo menos três servidores web diferentes, através do protocolo FTP;
- 12.2.1.25. Prover mecanismo de visualização de eventos em tempo real das funções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações:
- 12.2.1.25.1. Aplicações mais utilizadas;
  - 12.2.1.25.2. Usuários com maior atividade;
  - 12.2.1.25.3. Estatísticas de uso;
  - 12.2.1.25.4. Ataques e eventos do IPS correlacionados com o Common Vulnerabilities and Exposures (CVE);
  - 12.2.1.25.5. Principais aplicações por taxa de transferência de bytes;
  - 12.2.1.25.6. Principais hosts por número de ameaças identificadas;
- 12.2.1.26. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
- 12.2.1.27. Deve permitir a criação de relatórios personalizados;
- 12.2.1.28. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

12.2.1.29. Prover mecanismo de consulta às informações registradas integrado à interface de administração;

12.2.1.30. Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado;

12.2.1.31. A interface gráfica de visualização de logs deve possuir ferramenta de pesquisa que permita criar um filtro através de operadores lógicos (AND e OR) e coringas (\* e ?), facilitando assim a busca da informação.

### **12.2.2. Licenciamento**

12.2.2.1. A solução de gerenciamento centralizado deve estar licenciada para no mínimo poder gerenciar os appliances de segurança referentes ao item 1 do Lote 1 deste termo.

12.2.2.2. O período de licenciamento será de 05 (cinco) anos, onde a CONTRATANTE deverá receber os direitos de atualização da solução contratada.

### **12.2.3. Suporte Técnico**

7x24 12.2.3.1. A solução de gerenciamento centralizado deverá ser fornecida com suporte técnico diretamente pelo fabricante pelo período de 5 anos, mesmo estando vigente o suporte técnico da CONTRATADA.

## **CLÁUSULA DÉCIMA TERCEIRA: DA CONFIDENCIALIDADE:**

13.1. As PARTES reconhecem que todas as informações, de qualquer natureza, eventualmente reveladas pela CONTRATANTE à CONTRATADA, sejam feitas em meio físico, magnético ou oralmente, durante a vigência do presente CONTRATO, incluídas, mas não se limitando à base de dados técnicos, planos comerciais ou estratégicos, informações financeiras e projeções, dados ou informações sobre o mercado, clientes, parceiros, fornecedores ou equipamentos, documentos, projetos, ou até mesmo correspondências classificadas como informações confidenciais e sobre as mesmas deverá ser guardado sigilo absoluto, para todos os efeitos.

13.2. A obrigação de confidencialidade de que trata o presente CONTRATO visa proteger os direitos e interesses de todo gênero da CONTRATANTE, buscando impedir a revelação e a utilização indevida das Informações Confidenciais, motivo pelo qual a CONTRATADA obriga-se, de forma perene, em caráter irrevogável e irretratável, a manter sob sigilo absoluto todas as Informações Confidenciais a que vier a ter acesso, tratando-as como segredo industrial e de negócios.

13.3. É vedado à CONTRATADA divulgar informação, dado ou modelo que tenha sido desenvolvido a partir de qualquer Informação Confidencial, bem como desenvolver produtos, métodos ou serviços com base tanto nas Informações Confidenciais, como nas demais informações e conhecimentos obtidos no desenvolvimento do propósito deste CONTRATO, sem qualquer exceção.

## **CLÁUSULA DÉCIMA QUARTA: DAS DISPOSIÇÕES GERAIS**

14.1. Casos omissos e modificações serão resolvidos entre as partes através de termos aditivos, que farão parte integrante deste **CONTRATO**;

14.2. Os casos fortuitos ou de força maior serão excludentes de responsabilidade das partes, na forma do Código Civil Brasileiro;

14.3. O CONTRATANTE poderá introduzir acréscimos ou supressões que se fizerem necessários, em até 25% (vinte e cinco por cento) do valor inicial do contrato, conforme lhe faculta o artigo 30 do Regulamento de Licitações e Contratos do SESCOOP.

14.4. Fica eleito o Foro da Comarca de Belo Horizonte, Estado de Minas Gerais, que será o competente para dirimir dúvidas decorrentes da execução deste **CONTRATO**, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

Por estarem assim justas e acordadas, as partes assinam o presente contrato, em duas vias de igual teor, juntamente com as testemunhas abaixo.

Belo Horizonte, XX de julho de 2019.

**SESCOOP/MG:**

\_\_\_\_\_  
**RONALDO SCUCATO**  
**PRESIDENTE**

\_\_\_\_\_  
**ALEXANDRE GATTI LAGES**  
**SUPERINTENDENTE**

XXXXXXXXXXXXXXXXXXXXX:

\_\_\_\_\_  
XXXXXXXXXXXXXXXXXXXXX

**TESTEMUNHAS:**

\_\_\_\_\_  
**ROBERT MARTINS DOS SANTOS**

\_\_\_\_\_  
**MOACIR ROSA**