EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 013/2016

TIPO: MENOR PREÇO POR LOTE

OBJETO: CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE APPLIANCE DEDICADO COM SUBSISTEMAS DE FIREWALL STATEFUL, VPN, FILTRO DE URL, FILTRO DE MALWARE, GARANTIA, SUPORTE TÉCNICO E SERVIÇOS DE ASSINATURA, DE ACORDO COM AS DESCRIÇÕES CONTIDAS NO ANEXO I – TERMO DE REFERÊNCIA, PARTE INTEGRANTE DESTE EDITAL.

ABERTURA: 05/08/2016 às 09:00 horas
Obs.: Horário de Brasília

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 013/2016

A Agência Goiana de Habitação S/A – AGEHAB, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 040/2016, de 01/03/2016, torna público que fará realizar licitação na modalidade **Pregão (eletrônico),** tipo **Menor Preço por Lote**, destinada à CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE APPLIANCE DEDICADO COM SUBSISTEMAS DE FIREWALL STATEFUL, VPN, FILTRO DE URL, FILTRO DE MALWARE, GARANTIA, SUPORTE TÉCNICO E SERVIÇOS DE ASSINATURA, DE ACORDO COM AS DESCRIÇÕES CONTIDAS NO ANEXO I – TERMO DE REFERÊNCIA, PARTE INTEGRANTE DESTE EDITAL, relativo ao Processo Administrativo nº **0775/2016**, SEPNET nº **201600031000103**, nos termos da Lei Federal nº 10.520, de 17 de julho de 2002, Decreto Estadual nº 7.466/2011, Decreto Estadual nº 7.468, de 20 de outubro de 2011 e Lei nº 8.666, de 21 de junho de 1993, Lei Complementar nº 123/2006 e 147/2014, e demais normas regulamentares aplicáveis à espécie. O edital alterado e seus anexos encontram-se disponíveis no endereço: Rua 18-A, nº 541, 2º andar, coordenação de licitações, Setor Aeroporto, Goiânia – Goiás, fone (62) 3096-5041 ou nos sites www.comprasnet.go.gov.br e www.agehab.go.gov.br. A licitação será realizada em sessão pública, com **recursos do Convênio 003/2015 celebrado entre a AGEHAB e a Secretaria de Estado de Meio Ambiente, Recursos Hídricos, Infraestrutura, Cidades e Assuntos Metropolitanos – SECIMA, conforme plano de trabalho constante do mesmo, ação 2, atividade C,** através do Sistema Eletrônico de Gestão de Compras – COMPRASNET.GO, por meio do *site* **www.comprasnet.go.gov.br** no dia **05/08/2016 a partir das 09h00min (horário de Brasília-DF)**.

Aquilino Alves de Macedo
Pregoeiro

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 013/2016

PROCESSO Nº 0775/2016

SEPNET nº 201600031000103

1 - PREÂMBULO

A Agência Goiana de Habitação S/A – AGEHAB, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 040/2016, de 01/03/2016, torna público que se encontra aberta, nesta unidade, licitação na modalidade **Pregão Eletrônico**, tipo **Menor Preço por Lote,** através do Sistema Eletrônico de Gestão de Compras – COMPRASNET.GO, por meio do *site* www.comprasnet.go.gov.br, conforme as disposições da Lei nº 10.520, de 17 de julho de 2002, Decreto Estadual nº 7.466, de 18 de outubro de 2011, Decreto Estadual nº 7.468, de 20 de outubro de 2011, Lei nº 8.666, de 21 de junho de 1993, Lei Complementar nº 123/2006 e 147/2014, e demais normas regulamentares aplicáveis à espécie, bem como as condições estabelecidas neste Edital e seus anexos.

2 – DO OBJETO

2.1. Constituem objeto da presente licitação a CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE APPLIANCE DEDICADO COM SUBSISTEMAS DE FIREWALL STATEFUL, VPN, FILTRO DE URL, FILTRO DE MALWARE, GARANTIA, SUPORTE TÉCNICO E SERVIÇOS DE ASSINATURA, DE ACORDO COM AS DESCRIÇÕES CONTIDAS NO ANEXO I – TERMO DE REFERÊNCIA, PARTE INTEGRANTE DESTE EDITAL.

3 – DO LOCAL, DATA E HORA

3.1. O Pregão Eletrônico será realizado em sessão pública, através do site www.comprasnet.go.gov.br no dia **05/08/2016** a partir das **09h00min**, mediante condições de segurança, criptografia e autenticação, em todas as suas fases.

3.2. As Propostas Comerciais deverão ser encaminhadas, através do site www.comprasnet.go.gov.br no período compreendido entre as **09h00min e 10h00min horas** do dia **05 de agosto de 2016.**

3.3. A fase competitiva (lances) terá início previsto às **10h10min do dia 05/08/2016.**

3.4. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, independentemente de nova comunicação, desde que não haja comunicação do Pregoeiro em contrário.

3.5. Todas as referências de tempo contidas neste Edital, no Aviso e durante a Sessão Pública observarão, obrigatoriamente, o horário de Brasília – DF e, dessa forma, serão

registradas no sistema eletrônico e na documentação relativa ao certame.

4 – DAS CONDIÇÕES DE PARTICIPAÇÃO E DA EXCLUSIVIDADE DE CONTRATAÇÃO DE MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

4.1. Poderão participar deste Pregão as empresas:

a) do ramo pertinente ao seu objeto, legalmente constituídos;

b) que atendam as condições estabelecidas neste Edital e seus anexos;

c) que possuam cadastro obrigatório (certificado de registro cadastral – CRC emitido pelo CADFOR ou certificado de registro cadastral que atenda aos requisitos previstos na legislação geral). O certificado de registro cadastral deverá estar homologado e válido na data de realização do Pregão. Caso o certificado de registro cadastral apresente *"status irregular"*, será assegurado à licitante o direito de apresentar, via fax ou e-mail, a documentação atualizada e regular na própria sessão. O licitante vencedor que se valer de outros cadastros para participar de pregão por meio eletrônico deverá providenciar sua inscrição junto ao CADFOR, como condição obrigatória para a sua contratação;

d) que, previamente, realizem o credenciamento junto ao ComprasNet.GO.

4.2. A participação neste pregão eletrônico dar-se-á por meio da digitação de senha privativa do licitante e subseqüente encaminhamento da Proposta Comercial em data e horário previstos neste Edital, exclusivamente por meio eletrônico.

4.3. Como requisito para participação neste Pregão, a licitante deverá manifestar em campo próprio do sistema eletrônico www.comprasnet.go.gov.br, o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital.

4.4. É vedada a participação de empresa:

4.4.1. Em recuperação judicial ou em processo de falência, sob concurso de credores, em dissolução ou em liquidação.

4.4.2. Que tenha sido declarada inidônea pela Administração Pública e, caso participe do processo licitatório, estará sujeita às penalidades previstas no Art. 97, parágrafo único da Lei Federal nº 8.666/93.

4.4.3. Que esteja suspensa de licitar junto ao Cadastro Unificado de Fornecedores do Estado – CADFOR.

4.4.4. Cujos dirigentes pertençam, simultaneamente, a mais de uma firma licitante.

4.4.5. Empresas cujos sócios tenham vínculos de parentesco com servidores ou dirigentes da AGEHAB, em observância ao disposto no art. 9º, inciso III, da Lei nº 8.666/93;

4.5. As licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas, sendo que a AGEHAB não será, em nenhum caso, responsável por esses custos, independentemente da condição ou do resultado do processo licitatório.

4.6. Não poderão se beneficiar do regime diferenciado e favorecido em licitações concedido às microempresas e empresas de pequeno porte pela Lei Complementar nº

123/2006, licitantes que se enquadrem em qualquer das exclusões relacionadas no artigo terceiro da referida Lei.

4.7. Conforme estabelecido no Decreto Estadual nº 7.466/2011, será assegurada preferência de contratação para as microempresas e empresas de pequeno porte.

4.7.1. Para usufruir dos benefícios estabelecidos no Decreto Estadual nº 7.466/2011, a licitante que se enquadrar como microempresa ou empresa de pequeno porte, deverá declarar-se como tal, devendo apresentar certidão que ateste o enquadramento expedida pela Junta Comercial ou, alternativamente, documento gerado pela Receita Federal, por intermédio de consulta realizada no sítio www.receita.fazenda.gov.br/simplesnacional, podendo ser confrontado com as peças contábeis apresentadas ao certame licitatório.

4.7.2. O próprio sistema disponibilizará à licitante a opção de declarar-se como microempresa ou empresa de pequeno porte. A não manifestação de enquadramento, quando indagado pelo sistema eletrônico, implicará no decaimento do direito de reclamar, posteriormente, essa condição, no intuito de usufruir dos benefícios estabelecidos na Lei supramencionada.

4.7.3. Será assegurado, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte.

4.7.3.1. Entende-se por empate aquelas situações em que as ofertas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores ao menor preço registrado para o lote ofertado.

4.7.3.2. O critério de desempate, preferência de contratação, aqui disposto somente se aplicará quando a melhor oferta válida não tiver sido apresentada por microempresa, empresa de pequeno porte ou equiparada.

4.7.3.3. A preferência aqui tratada será concedida da seguinte forma:

I – ocorrendo empate, a microempresa, empresa de pequeno porte ou equiparada melhor classificada poderá apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que será adjudicado o objeto licitado em seu favor;

II – o direito de preferência previsto no inciso I será exercido, sob pena de preclusão, após o encerramento da rodada de lances, devendo ser apresentada nova proposta no prazo máximo de cinco minutos para o lote em situação de empate;

III – no caso de igualdade dos valores apresentados pelas microempresas e empresa de pequeno porte que se encontrem em situação de empate, será realizado sorteio entre elas para que se identifique aquela que poderá exercer o direito de preferência previsto no inciso I;

IV – na hipótese da não contratação da microempresa, empresa de pequeno porte ou equiparada com base no inciso I, serão convocadas as remanescentes que porventura se enquadrem em situação de empate, na ordem classificatória, para o exercício do mesmo direito.

4.7.3.4. Na hipótese da não-contratação nos termos previstos no item **4.7.3.3**, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do

certame.

5 – DO CREDENCIAMENTO

5.1. O acesso ao credenciamento se dará somente às licitantes com cadastro homologado pelo Cadastro Unificado de Fornecedores do Estado – CADFOR da Superintendência de Suprimentos e Logística da SEGPLAN ou àquelas que atendam às condições do item 5.1.5. abaixo.

5.1.1. Para cadastramento, renovação cadastral e regularização, o interessado deverá atender a todas as exigências do cadastro Unificado de Fornecedores do Estado – CADFOR da Superintendência de Suprimentos e Logística da SEGPLAN até o 5º (quinto) dia útil anterior à data de registro das propostas. A relação de documentos para cadastramento está disponível no site www.comprasnet.go.gov.br.

5.1.2. Não havendo pendências documentais será emitido o CRC – Certificado de Registro Cadastral pelo CADFOR, no prazo de 04 (quatro) dias úteis contados do recebimento da documentação.

5.1.3. A simples inscrição do pré-cadastro no sistema Comprasnet.go, não dará direito à licitante de credenciar-se para participar deste Pregão, em razão do bloqueio inicial da sua senha.

5.1.4. O desbloqueio do login e da senha do fornecedor será realizado após a homologação do cadastro da licitante.

5.1.5. Conforme Instrução Normativa nº 004/2011 – SEGPLAN, em caso do licitante pretender utilizar-se de outros cadastros que atendam a legislação pertinente para participar do pregão eletrônico, efetuará seu credenciamento de forma simplificada junto ao CADFOR, caso em que ficará dispensado de apresentar toda a documentação abrangida pelo referido cadastro, mediante a apresentação do mesmo ao CADFOR e terá registrado apenas a condição de "credenciado".

5.2. Os interessados que estiverem com o cadastro homologado ou "credenciados" (conforme item 5.1.5.), deverão credenciar-se pelo *site* *www.comprasnet.go.gov.br*, opção "login do FORNECEDOR", conforme instruções nele contidas.

5.3. O credenciamento dar-se-á de forma eletrônica por meio da atribuição de chave de identificação ou senha individual.

5.4. O credenciamento do usuário será pessoal e intransferível para acesso ao sistema, sendo o mesmo responsável por todos os atos praticados nos limites de suas atribuições e competências.

5.5. O credenciamento do usuário implica sua responsabilidade legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

5.6. O uso da senha de acesso pelo licitante é de sua exclusiva responsabilidade, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou a AGEHAB, promotora da licitação, responsabilidade por

eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

5.7. As informações complementares para cadastro e credenciamento poderão ser obtidas pelo telefone (62) 3096-5041, e para operação no sistema Comprasnet.go pelo telefone (62) 3201-6515 e 3201-6516.

6 – DAS PROPOSTAS COMERCIAIS

6.1. Concluída a fase de credenciamento, as licitantes registrarão suas propostas. Só será aceita uma proposta por item para cada licitante e, ao término do prazo estipulado para a fase de registro de propostas, o sistema automaticamente bloqueará o envio de novas propostas.

6.2. As propostas comerciais deverão ser enviadas através do site www.comprasnet.go.gov.br na data e hora estabelecidas neste edital, após o preenchimento do formulário eletrônico, com manifestação em campo próprio do sistema de que tem pleno conhecimento e que atende às exigências de habilitação e demais condições da proposta comercial previstas no edital e seus anexos.

6.3. A proposta comercial deverá ser formulada e enviada, exclusivamente por meio do Sistema Eletrônico, **indicando o valor unitário do item,** e o ônus de comprovação de sua exequibilidade caberá exclusivamente à licitante, caso solicitado pelo pregoeiro.

6.3.1. O sistema Comprasnet.go possibilita à licitante a exclusão/alteração da proposta dentro do prazo estipulado no edital para registro de propostas. Ao término desse prazo, definido no item 3.2, não haverá possibilidade de exclusão/alteração das propostas, as quais serão analisadas conforme definido no edital.

6.4. A licitante se responsabilizará por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos durante a sessão pública.

6.5. O licitante é responsável pelo ônus da perda de negócios resultante da inobservância de quaisquer mensagens emitidas pelo Pregoeiro ou pelo sistema, ainda que ocorra sua desconexão.

6.6. As propostas deverão atender as especificações contidas no Termo de Referência, Anexo I deste Edital.

6.7. Todas as empresas deverão cotar seus preços com todos os tributos cabíveis inclusos, bem como todos os demais custos diretos e indiretos necessários ao atendimento das exigências do Edital e seus anexos.

6.8. Quaisquer tributos, custos e despesas diretas ou indiretas omitidos na proposta ou incorretamente cotados, serão considerados como inclusos nos preços, não sendo aceitos pleitos de acréscimos, a esse ou qualquer outro título.

6.9. A licitante detentora da melhor oferta, após a fase de lances, deverá enviar Proposta Comercial, por fax ou e-mail, devendo a mesma conter, obrigatoriamente, ainda:

a) Nome da Empresa, CNPJ, endereço, fone/fax, nº da conta corrente, Banco, nº da agência, nome do responsável;
b) Nº do Pregão;
c) Preço em Real, unitário e total com no máximo duas casas decimais, onde deverá estar inclusas todas as despesas que influam nos custos, tais como: encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, impostos, taxas, assim como outros de qualquer natureza que se fizerem indispensáveis ao cumprimento integral do objeto do presente edital;
d) Objeto ofertado, consoante exigências editalícias e com a quantidade licitada;
e) Prazo de validade da proposta de **60 (sessenta) dias,** a contar da data da sessão deste Pregão Eletrônico. Caso não apresente prazo de validade será este considerado;
f) Data e assinatura do responsável.

6.10. – Critério de Julgamento e estimativa de preços:

6.10.1. O critério de julgamento e seleção da proposta mais vantajosa para a **AGEHAB** será a que oferecer o menor preço do lote.

6.10.2. O valor estimado é de **R$ 96.789,86 (noventa e seis mil, setecentos e oitenta e nove reais e oitenta e seis centavos),** para um período de 12 (doze) meses.

7 – DA SESSÃO DO PREGÃO ELETRÔNICO

7.1. A partir das **09h00min, do dia 05 de agosto de 2016,** data e horário previstos neste Edital, terá início à sessão pública do **Pregão Eletrônico nº 013/2016**, com a divulgação das Propostas de Preços recebidas.

7.2. Após a abertura da sessão pública deste Pregão Eletrônico não serão permitidos quaisquer adendos, complementações, acréscimos ou retificações às Propostas de Preços apresentadas.

7.3. Após a abertura da sessão pública deste Pregão Eletrônico não caberá desistência da Proposta de Preços apresentada, salvo por motivo justo, decorrente de fato superveniente e aceito pelo Pregoeiro.

7.4. O Pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estiverem em conformidade com os requisitos estabelecidos no Edital, em decisão fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.5. O sistema ordenará automaticamente as propostas classificadas pelo Pregoeiro, sendo que somente estas participarão da fase de lances.

7.6. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os Licitantes, permitindo que durante o transcurso da sessão pública eletrônica, haja a divulgação, em tempo real, de todas as mensagens trocadas no *chat* do sistema, inclusive valor e horário do menor lance registrado e apresentado pelas Licitantes, vedada a identificação do fornecedor.

8 – DOS LANCES

8.1. Após a análise e classificação das propostas, o Pregoeiro dará início à fase competitiva, quando então as Licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, observado o horário estabelecido e as regras de aceitação dos mesmos, sendo imediatamente informados do seu recebimento e respectivo horário de registro e valor.

8.2. Os licitantes poderão oferecer lances sucessivos, **MENOR PREÇO,** sempre inferior ao último por ele ofertado e registrado pelo sistema, obedecendo, quando o Pregoeiro fixar, ao percentual ou valor mínimo exigido entre os lances.

8.2.1. O sistema eletrônico rejeitará automaticamente os lances em valores superiores aos anteriormente apresentados pelo mesmo licitante.

8.3. Não serão aceitos dois ou mais lances iguais, **para a mesma proposta,** prevalecendo aquele que for recebido e registrado no sistema em primeiro lugar.

8.4. Caso a licitante não realize lances, permanecerá o valor inicial de sua proposta eletrônica, que será incluída na classificação final.

8.5. Durante o transcurso da sessão pública eletrônica, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes, vedada a identificação do detentor do lance.

8.6. A fase de lances terá duas etapas: a primeira, com tempo de duração de **15 minutos,** após a abertura da fase de lances e será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema às Licitantes. A segunda transcorrerá com abertura de prazo de até 30 (trinta) minutos, aleatoriamente determinado também pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

8.7. Após o encerramento da etapa de lances da sessão pública, o Pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes das previstas no edital.

8.8. A negociação será realizada por meio do sistema eletrônico, podendo ser acompanhada pelas demais licitantes.

8.9. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do pregão, se o sistema eletrônico permanecer acessível às licitantes para a recepção dos lances, estes continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.10. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa e reiniciada somente após comunicação aos participantes, no endereço eletrônico utilizado para divulgação.

9 – DO JULGAMENTO DAS PROPOSTAS DE PREÇOS

9.1. O julgamento das propostas será objetivo, tendo seu critério baseado no ***MENOR***

PREÇO DO LOTE**,** não se admitindo, sob pena de responsabilidade, reformulação dos critérios de julgamento previstos no ato convocatório.

9.2. Considerar-se-á **vencedora do certame** aquela proposta que, tendo sido aceita, estiver de acordo com os termos deste Edital e seus Anexos, ofertar o menor preço, após a fase de lances e for devidamente habilitada após apreciação da documentação.

9.2.1. Na análise da Proposta de Preços, fica facultado ao Pregoeiro, se necessário, solicitar parecer técnico para subsidiar sua análise, podendo suspender temporariamente a sessão pública do pregão, informando através do *chat* de comunicação o horário de reabertura dos trabalhos.

9.3. Havendo apenas uma proposta de preços, desde que atenda a todas as condições do edital e estando o seu valor compatível com os praticados no mercado, poderá ser aceita, devendo o Pregoeiro negociar, visando a obter melhor preço.

9.4. Encerrada a etapa de lances da sessão pública ou, quando for o caso, após a negociação e decisão acerca da aceitação do lance de menor valor, a proposta de preços que, em consequência com as especificações contidas no Termo de Referência, tenha apresentado menor valor, o sistema informará a Licitante detentora da melhor oferta, e esta deverá encaminhar de imediato, nova proposta com valores (unitários e total) readequados ao valor ofertado e registrado como de menor lance, bem como a documentação de habilitação para as exigências não contempladas no CRC e todos os documentos exigidos neste Edital e seus Anexos. Esta comprovação se dará mediante encaminhamento da documentação *via fax: (62) 3096-5041 ou e-mail: cpl@agehab.go.gov.br*.

9.4.1. Posteriormente deverá ser encaminhada, no prazo máximo de 05 (cinco) dias úteis contados da data de encerramento do Pregão Eletrônico, via correio ou por representante, a proposta de preços em original, assinada e atualizada com os valores, unitários e global, informando todas as características do objeto e demais exigências descritas neste Edital e seus Anexos. Deverão ser enviadas, no mesmo prazo, as demais documentações exigidas para habilitação, estas em original ou por cópia autenticada, sendo inclusive condição indispensável para a contratação.

9.4.2. O pregoeiro verificará a regularidade cadastral da Licitante que apresentou a melhor oferta junto ao CADFOR, e em caso de irregularidade, será assegurado o direito de apresentar a documentação atualizada, ao final da sessão em até 02 (duas) horas, via fax ou pelo e-mail: *cpl@agehab.go.gov.br*, devendo a documentação original ou cópia autenticada ser encaminhada no prazo máximo de 05 (cinco) dias úteis contados da data de encerramento do Pregão Eletrônico.

9.4.3. O CRC, emitido pelo CADFOR, poderá ser impresso pelo Pregoeiro para averiguação da sua conformidade com as exigências do Edital e apresentando *"status irregular",* será assegurada à Licitante o direito de apresentar a documentação atualizada e regular na própria sessão.

9.4.4. Para fins de habilitação a verificação, pela Equipe de Apoio do certame, nos sítios oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

9.5. Constatado, que a Licitante que apresentou proposta de menor preço final atende às

exigências editalícias, será ela declarada vencedora.

9.6. Na hipótese da Licitante detentora da melhor oferta desatender às exigências habilitatórias, o Pregoeiro deverá restabelecer a etapa competitiva de lances entre os licitantes. **(Lei Estadual nº 18.989, 27/08/2015).**

9.7. Da sessão pública do Pregão Eletrônico, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes, que estará disponível para consulta no site www.comprasnet.go.gov.br.

9.8. O resultado final será disponibilizado no site: www.comprasnet.go.gov.br.

10 – DOS DOCUMENTOS DE HABILITAÇÃO

O licitante vencedor deverá enviar no endereço e nas conformidades exigidas neste certame a seguinte documentação:

10.1. CRC – Certificado de Registro Cadastral expedido pelo CADFOR da Superintendência de Suprimento e Logística – SUPRILOG, atualizado, em vigência e com o *status* REGULAR ou IRREGULAR.

10.1.1. Na data da abertura do procedimento de licitação, os documentos dos itens 10.2, 10.3 e 10.4 (**conforme art. 4º da Instrução Normativa 004/2011-GS**), que comprovarem suas regularidades e/ou que estiverem com suas datas em vigor no CADFOR da SUPRILOG, estarão dispensados de apresentação pelos licitantes.

10.1.2. A licitante deverá apresentar os seguintes:

a) Um ou mais testados de capacidade técnica com firma reconhecida, fornecidos por pessoa jurídica de direito público ou privado que comprove o fornecimento, nos termos do Termo de Referência, dos produtos e serviços compatíveis com o objeto desta licitação;
b) Um ou mais atestados de capacidade técnica com firma reconhecida, fornecidos por pessoa jurídica de direito público ou privado que comprove a realização de treinamento com no mínimo 20 horas (50% do TR) em appliance firewall com profissional certificado pelo fabricante da solução;
c) Apresentar portifólio do produto ofertado.
d) A licitante deverá apresentar todos os Part Number (P/N) e Fabricante da solução ofertada, juntamente com a proposta devidamente assinada.

10.1.3. Certidão que ateste o enquadramento expedida pela Junta Comercial ou, alternativamente, documento gerado pela Receita Federal, por intermédio de consulta realizada no sítio www.receita.fazenda.gov.br/simplesnacional, podendo ser confrontado com as peças contábeis apresentadas ao certame licitatório, se for o caso.

10.2. Regularidade Jurídica

a) Cédula de identidade.
b) Registro comercial, no caso de empresa individual.

c) Ato constitutivo, estatuto ou contrato social em vigor, e suas respectivas alterações (endereço, razão social, etc..) devidamente registrados, em se tratando de sociedades comerciais, e no caso de sociedade de ações, acompanhadas de documentos de eleição de seus administradores.

d) Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício.

e) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo Órgão competente, quando a atividade assim o exigir.

10.3. Regularidade Fiscal e Trabalhista

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ.

b) 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.

c) Certificado de Regularidade para com o FGTS, expedido pela Caixa Econômica Federal.

d) Certidão Negativa de Débito para com o INSS, ou prova equivalente que comprove regularidade de situação para com a Seguridade Social, ou ainda prova de garantia em juízo de valor suficiente para pagamento do débito, quando em litígio.

e) Prova de regularidade para com a Fazenda Federal.

f) Prova de regularidade para com a Fazenda Estadual do domicílio ou sede do licitante, **se sediado/domiciliado em outra unidade da federação, e do Estado de Goiás.**

g) Prova de regularidade para com a Fazenda Municipal do domicílio ou sede do licitante.

h) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa.

10.4. Qualificação Econômico-Financeira

a) Certidão negativa de Falência e Concordata, expedido pelo cartório distribuidor da comarca da sede da pessoa jurídica ou de execução de pessoa física.

b) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis a apresentação na forma da lei, que comprovem a boa situação financeira da empresa, vedada a substituição por balancetes ou balanços provisórios, podendo ser atualizados, através de índices oficiais, quando encerrado há mais de três meses da data de apresentação da proposta;

b.1. Comprovação de boa situação financeira da empresa através de no mínimo um dos seguintes índices contábeis, o qual deverá ser maior ou igual a 1:

- ILC – Índice de Liquidez Corrente ou,

- ILG – Índice de Liquidez Geral ou,

- GS – Grau de Solvência

ILC =	$\frac{AC}{PC}$	=	$\frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$
ILG =	$\frac{AC + RLP}{PC + ELP}$	=	$\frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Exigível a Longo Prazo}}$
GS =	$\frac{AT}{PC + ELP}$	=	$\frac{\text{Ativo Total}}{\text{Passivo Circulante + Exigível a Longo Prazo}}$

10.5. Das Declarações:

a) Declaração de Inexistência de Fato Superveniente (**modelo Anexo IV**);

b) Declaração de Inexistência de menor Trabalhador (**modelo Anexo V**);

c) Declaração de pleno atendimento aos requisitos de habilitação (**modelo Anexo III**);

d) Declaração de Enquadramento na Lei Complementar nº 123/2006 (**modelo Anexo VIII**);

e) Declaração de inexistência de sócios comuns, endereços coincidentes e/ou indícios de parentesco (**modelo Anexo IX**).

10.6. Se o licitante que apresentou a melhor oferta tenha optado, quando do seu credenciamento, por exibir outro certificado de registro cadastral que atenda aos requisitos previstos na legislação geral, para comprovação de sua regularidade documental deverá apresentar junto ao Cadastro de Fornecedores – CADFOR documentos que comprovem sua habilitação jurídica, regularidade fiscal e trabalhista, qualificação econômico-financeira, qualificação técnica e declaração de que atende plenamente ao que dispõe o inciso XXXIII do art. 7º da Constituição Federal, no prazo de até 05 (cinco) dias úteis do encerramento do presente Pregão Eletrônico.

10.7. Havendo alguma restrição na comprovação da regularidade fiscal das microempresas e empresas de pequeno porte, será assegurado o prazo de até 5 (cinco) dias úteis para a regularização da documentação, contados do momento em que o proponente for declarado o vencedor do certame, observando-se, quanto ao mais, as demais disposições contidas no art. 5º da Lei Estadual nº 17.928/2012.

10.7.1. A não regularização da documentação, no prazo previsto acima, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81, da Lei Federal nº 8.666/93, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a

licitação.

10.7.2. As microempresas e empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

10.8. Todos os documentos deverão estar com prazo vigente, e para as certidões que não mencionarem prazo de validade, considerará o prazo de **60 (sessenta) dias**, contados da data de sua expedição.

10.9. Os documentos exigidos para habilitação, não contemplados pelo CRC, juntamente com a Proposta Comercial deverão estar atualizados na data da Sessão Pública, devendo ser encaminhados pela licitante detentora da melhor oferta por fax e/ou e-mail (cpl@agehab.go.gov.br) no prazo máximo de 01 (um) dia útil, após finalização da fase de lances. Posteriormente os mesmos deverão ser encaminhados no prazo máximo de até 05 (cinco) dias úteis após a data do encerramento do Pregão. Caso ocorra pedido de documentação técnica e/ou amostra (laudos, manuais e etc) a licitante terá o prazo de 05 (cinco) dias úteis para envio após o encerramento da sessão pública. O endereço para envio da documentação é o seguinte: Coordenadoria de Licitações e Contratos da AGEHAB, na Rua 18-A nº 541, Setor Aeroporto, Goiânia – Goiás, Fone: (62) 3096-5041 ou 3096-5003, e estarem separados, em 02 envelopes fechados e indevassáveis, contendo em sua parte externa, além da identificação com nome, endereço, CNPJ da proponente, os seguintes dizeres:

Envelope nº 01 – PROPOSTA
Pregão Eletrônico nº 013/2016
Processo nº 201600031000103

Envelope nº 02 – DOCUMENTAÇÃO
Pregão Eletrônico nº 013/2016
Processo nº 201600031000103

10.9.1. Os prazos de envio deverão ser respeitados, sob pena de desclassificação e inabilitação da empresa vencedora, sendo, inclusive, condição indispensável para a contratação.

11. DOS PEDIDOS DE ESCLARECIMENTO, PROVIDÊNCIAS E IMPUGNAÇÃO DO ATO CONVOCATÓRIO

11.1. Até 2 (dois) dias úteis antes da data fixada para a abertura da sessão pública, qualquer cidadão ou licitante poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório deste Pregão Eletrônico.

11.2. Os pedidos de esclarecimentos, providências ou impugnação do edital e seus anexos deverão ser encaminhados por escrito ao Pregoeiro na Rua 18-A nº 541, Setor Aeroporto, Goiânia – Goiás, Fone/ Fax: (62) 3096-5041, e-mail: cpl@agehab.go.gov.br.

11.2.1. Nos pedidos de esclarecimentos, providências ou impugnação do edital, remetidos ao Pregoeiro, deverá constar, obrigatoriamente, o e-mail do peticionante.

11.2.2. Caberá ao Pregoeiro decidir sobre os pedidos no prazo de 24 (vinte e quatro) horas e encaminhar a resposta ao peticionante por e-mail.

11.3. Acolhida a impugnação do ato convocatório, o Pregoeiro procederá à retificação do edital, e republicação, com devolução dos prazos quando a alteração afetar a formulação das propostas.

12. DOS RECURSOS

12.1. Declarado o vencedor, ao final da sessão, qualquer licitante poderá manifestar, no prazo de até 10 (dez) minutos, a intenção motivada de recorrer da decisão do Pregoeiro, com o registro da síntese de suas razões no campo próprio definido no sistema eletrônico, sendo que a falta de manifestação no prazo concedido importará na decadência do direito de recurso e, consequentemente, na adjudicação do objeto da licitação ao licitante vencedor.

12.2. A intenção motivada de recorrer é aquela que identifica, objetivamente, os fatos e o direito que a licitante pretende que sejam revistos pelo Pregoeiro.

12.3. Ao licitante que manifestar intenção de interpor recurso será concedido o prazo de 03 (três) dias, contados de sua manifestação, para apresentação das razões do recurso, através de formulário próprio do Sistema Eletrônico, ficando as demais licitantes desde logo intimados para apresentar, através de formulário próprio do sistema eletrônico, contrarrazões em igual prazo, que terá inicio no primeiro dia útil subsequente ao do término do prazo do recorrente.

12.4. Somente serão conhecidos os recursos, suas razões e, consequentemente, as contrarrazões, quando interpostos tempestivamente e encaminhados através do sistema eletrônico.

12.5. Caberá ao pregoeiro receber, examinar, instruir e decidir sobre os recursos e, quando mantida a sua decisão, encaminhar os autos ao Presidente da AGEHAB para deliberação.

12.5.1. O exame, a instrução e, em caso de manutenção de sua decisão, o encaminhamento dos recursos ao Presidente da AGEHAB, autoridade competente, para nesse caso, apreciá-los, serão realizados pelo Pregoeiro no prazo de até 3 (três) dias úteis, podendo este prazo ser dilatado até o dobro, por motivo justo.

12.6. O Presidente da AGEHAB terá prazo de 3 (três) dias úteis para decidir sobre os recursos interpostos, podendo este prazo ser dilatado até o dobro, por motivo justo, devidamente comprovado.

12.7. O acolhimento do recurso pelo Pregoeiro ou pela autoridade competente importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

12.8. A decisão em grau de recurso será definitiva e dela dar-se-á conhecimento às interessadas, através de comunicação por escrito via fax e divulgação nos "sites" pertinentes.

13. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

13.1. Inexistindo manifestação recursal, o Pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pelo Presidente da AGEHAB.

13.2. Havendo manifestação recursal, após decididos os recursos, o Presidente da AGEHAB adjudicará o objeto ao licitante vencedor e homologará a licitação.

14. DAS CONDIÇÕES DE ASSINATURA, VIGÊNCIA, ALTERAÇÃO E RESCISÃO DO CONTRATO

14.1. Findo o processo licitatório, o licitante vencedor será convocado a assinar o contrato relativo ao objeto do Pregão Eletrônico.

14.2. O não comparecimento do licitante vencedor, injustificadamente, dentro do prazo de 10 (dez) dias após regularmente convocado para assinatura do termo contratual, ensejará, garantido o direito prévio ao contraditório e à ampla defesa.

14.2.1. O impedimento de licitar e contratar com a Administração e descredenciamento junto ao Cadastro de Fornecedores – CADFOR, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

14.2.2. A aplicação de multa de até 10% (dez por cento) sobre o valor do contrato.

14.3. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração.

14.4. Se o licitante vencedor não apresentar situação regular no ato da assinatura do contrato, ou recursar-se a assiná-lo, o Pregoeiro convocará os licitantes remanescentes, na ordem de classificação, para negociar diretamente com a proponente melhor classificada e, respeitados os procedimentos já definidos neste edital, será declarada a nova adjudicatária do objeto deste Pregão Eletrônico.

14.5. Até a efetiva assinatura do contrato, a proposta do licitante vencedor poderá ser desclassificada caso da AGEHAB venha ter conhecimento de fato que desabone sua habilitação, conhecido após o julgamento.

14.6. O contrato terá vigência de 12 (doze) meses, a contar da data de sua assinatura.

14.7. O contrato poderá ser rescindido a qualquer tempo, com base nos motivos previstos no art. 77 e 78, na forma dos arts. 79 e 80, da Lei Federal nº 8.666/93, assegurado à **CONTRATADA** o direito ao contraditório e à ampla defesa.

14.8. O contrato poderá ser alterado, com as devidas justificativas, nos casos previstos no art. 65 da Lei Federal nº 8.666/93, sempre por meio de termos aditivos.

14.9. A **CONTRATADA** é obrigada a aceitar nas mesmas condições da licitação, os

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

acréscimos ou supressões que se fizerem no objeto licitado, de até 25% (vinte e cinco por cento) sobre o valor inicial atualizado do contrato, nos termos do § 1º, do art. 65, da Lei Federal nº 8.666/93.

15. DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

15.1. Todos os itens deverão seguir os padrões de prazo, local de entrega e forma de recebimento descritos abaixo.

15.1.1. Os equipamentos deverão ser entregues até 60 (sessenta) dias a contar da assinatura do contrato ou instrumento equivalente, à cede da Agência Goiana de Habitação S/A Rua 18 A nº 541, Setor Aeroporto, Goiânia-GO, CEP 74070-060;

15.1.2. A CONTRATANTE determinará o local para entrega e verificará todas as condições e especificações, em conformidade com este Termo de Referência;

15.1.3. Entende-se por entrega as seguintes atividades: o transporte dos produtos embalados para o local determinado pela CONTRATANTE, a entrega dos volumes, a desembalagem, a verificação visual do produto e sua reembalagem se for o caso;

15.1.4. Os equipamentos deverão ser novos e sem uso e deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

15.1.5. No ato da entrega, a gerência responsável emitirá TERMO DE RECEBIMENTO PROVISÓRIO relacionando todos os produtos recebidos, nos termos da Nota Fiscal;

15.1.6. Os produtos serão objeto de inspeção, que será realizada por pessoa designada pela gerência responsável, conforme procedimentos a seguir:

15.1.6.1. Abertura das embalagens;

15.1.6.2. Comprovação de que o produto atende às especificações mínimas exigidas e/ou aquelas superiores oferecidas pela CONTRATADA;

15.1.6.3. Colocação do produto em funcionamento, se for o caso;

15.1.6.4. Teste dos componentes se for o caso;

15.1.6.5. O período de inspeção será de até 10 (dez) dias úteis;

15.1.7. Nos casos de sinais externos de avaria de transporte ou de mau funcionamento do produto, verificados na inspeção do mesmo, este deverá ser substituído por outro com as mesmas características, no prazo de até 30 (trinta) dias corridos, a contar da data de realização da inspeção;

15.1.8. Findo o prazo de inspeção e comprovada a conformidade dos produtos com as especificações técnicas exigidas no Edital e aquelas oferecidas pela CONTRATADA, a gerência responsável emitirá o TERMO DE RECEBIMENTO DEFINITIVO;

15.1.9. Nos casos de substituição do produto, iniciar-se-ão os prazos e procedimentos estabelecidos nestas CONDIÇÕES DE RECEBIMENTO

15.1.10. Correrão por conta da CONTRATADA as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos.

16. DOS RECURSOS FINANCEIROS

16.1. As despesas decorrentes da presente licitação correrá à conta de **Recursos do Convênio 003/2015, firmado entre a AGEHAB e a Secretaria de Estado de Meio Ambiente, Recursos Hídricos, Infraestrutura, Cidades e Assuntos Metropolitanos - SECIMA, conforme Plano de Trabalho, Ação 2, Atividade "C" do Plano de Trabalho.**

17. DAS SANÇÕES ADMINISTRATIVAS

17.1. O licitante que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, garantido o direito prévio da ampla defesa, ficará impedido de licitar e contratar com a Administração e será descredenciado junto ao CADFOR, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste edital e demais cominações legais inclusive advertência.

17.2. A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará a **CONTRATADA,** além das cominações legais cabíveis, à multa de mora, graduada de acordo com a gravidade de infração obedecidos os seguintes limites máximos:

17.2.1. 10% (dez por cento) sobre o valor do contrato, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatório em firmar o contrato ou retirar a nota de empenho, dentro de 10 (dez) dias contados da data de sua convocação;

17.2.2. 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;

17.2.3. 0,7% (sete décimos por cento) sobre o valor da parte do fornecimento não realizado, por cada dia subsequente ao trigésimo;

17.2.4. O valor da multa será descontado quando dos próximos pagamentos devidos pela AGEHAB em razão da execução do contrato, ou, ainda, quando for o caso, cobrada judicialmente.

17.7. Antes da aplicação de qualquer penalidade, será garantido à **CONTRATADA** a ampla defesa e o contraditório.

18. DAS DISPOSIÇÕES FINAIS

18.1. Este Edital deverá ser lido e interpretado na integra. Após o registro da proposta no sistema, não serão aceitas alegações de desconhecimento.

18.2. A AGEHAB poderá revogar a licitação em face de razões de interesse público, derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de oficio ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

18.2.1. Da decisão que anular ou revogar a licitação caberá recurso, no prazo de 05 (cinco) dias úteis contados da intimação do ato ou lavratura da ata garantindo aos licitantes o contraditório e a ampla defesa.

18.2.2. A anulação do procedimento licitatório induz à do contrato.

18.2.3. Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratado de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do contrato.

18.3. É facultado ao Pregoeiro ou ao Senhor Presidente da AGEHAB, ou autoridade por ele delegada, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da Sessão Pública.

18.4. Os licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

18.5. É vedada a subcontratação, cessão ou transferência no todo ou em parte do objeto ora licitado.

18.6. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local anteriormente estabelecido, desde que não haja comunicação do Pregoeiro em contrário.

18.7. Na contagem dos prazos estabelecidos neste Edital e seus anexos, excluir-se-á o dia do inicio e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dia de expediente regular e integral na AGEHAB.

18.8. O desatendimento de exigências formais não essenciais não importará no afastamento do Licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

18.8.1. Exigências formais não essenciais são aquelas cujo descumprimento não acarretam irregularidades no procedimento, bem como não importam em vantagens a um ou mais Licitantes em detrimento dos demais.

18.9. As normas que disciplinam este Pregão Eletrônico serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança do futuro contrato ou instrumento equivalente.

18.10. Havendo divergência entre a descrição do objeto constante no Edital e seus anexos e a descrição do objeto constante nos sites www.comprasnet.go.gov.br e www.agehab.go.gov.br, **prevalecerá, sempre, a descrição deste Edital e seus anexos**.

18.11. É de responsabilidade do licitante o acompanhamento do processo pelos sites www.comprasnet.go.gov.br ou www.agehab.go.gov.br até a data da realização da sessão pública.

19. DO FORO

19.1. O foro para solucionar os litígios decorrentes do presente edital é o da Comarca de Goiânia, Capital do Estado de Goiás, excluído qualquer outro.

20. DOS ANEXOS

ANEXO I - Termo de Referência
ANEXO II – Modelo de Carta Proposta
ANEXO III – Modelo de Declaração de Inexistência de Fato Superveniente
ANEXO IV – Declaração de Inexistência de Menor Trabalhador
ANEXO V – Declaração I de pleno atendimento aos requisitos de habilitação
ANEXO VI – Declaração II de pleno atendimento aos requisitos de habilitação
ANEXO VII - GLOSSÁRIO
ANEXO VIII – Minuta do Contrato
ANEXO IX - Declaração de inexistência de sócios comuns.

Goiânia, 19 de julho de 2016.

Aquilino Alves de Macêdo
Pregoeiro

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Aquisição de appliance dedicado com subsistemas de firewall stateful, VPN, filtro de URL, filtro de malware, garantia, suporte técnico e serviço de assinatura, conforme descrição contida no Termo de Referência.

1.2. O objeto da licitação deverá ser adjudicado para o menor valor GLOBAL.

1.2.1. Todos os itens são dependentes para o funcionamento do equipamento por isso a AGEHAB descarta o fracionamento dos itens.

2. CARACTERIZAÇÃO DO OBJETO

2.1. Todos os equipamentos deverão ser entregues no endereço da CONTRATANTE, situado na Rua 18 A nº 541 Setor Aeroporto, Goiânia, Goiás, CEP: 74.070-060, A/C do Gestor do Contrato, em mídia CD-ROM ou DVD-ROM, acompanhado da respectiva Nota Fiscal.

3. JUSTIFICATIVA

3.1. Firewall é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. "Parede de fogo", a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa. A sua missão, por assim dizer, consiste basicamente em bloquear tráfego de dados indesejado e liberar acessos bem-vindos.

3.2. O firewall pode ajudar a impedir que hackers ou softwares mal-intencionados (como worms) obtenham acesso ao seu computador através de uma rede ou da Internet. Um firewall também pode ajudar a impedir o computador de enviar software mal-intencionado para outros computadores.

3.3. Cada vez mais os hackers encontram novas formas de invadir redes privadas e roubar arquivos e dados das pessoas. Os criminosos virtuais atingiram tal ponto de ousadia que chegam a manter estes arquivos reféns até que a empresa pague um resgate pela devolução deles.

3.4. Hoje em dia, as empresas estão completamente dependentes de computadores para organizar as suas informações. São Banco de dados, apresentações, documentos, fotos e outros tipos de arquivos importantes.

3.5. O quão grave seriam as consequências caso eles fossem perdidos em uma invasão via internet? Um firewall assegura a integridade e a segurança dos documentos corporativos, sem que o usuário tenha a sua produtividade impactada.

3.6. A AGEHAB possui firewall por software que foi descontinuado pela fabricante e suporte findado em dezembro de 2015.

3.7. A feature de web protection services foi descontinuada em 31 de dezembro de 2015. A partir de 01 de Janeiro de 2016, os serviços de URL Filtering, Malware Inspection e Network Inspection continuarão funcionando, mas, sem atualização.

3.8. Conforme notícia publica no em 09 de 2015 no portal g1.globo.com "Hackers invadem e bloqueiam sistema interno da Prefeitura de Pratânia. Ciber pediu 'resgate' de três mil dólares para liberar senhas. Segundo o prefeito, pagamento de servidores está prejudicado."

3.9. Os prejuízos no caso de vazamentos ou invasão na rede da AGEHAB são imensuráveis, podendo ocorrer toda paralização da empresa.

4. DA QUALIFICAÇÃO TÉCNICA

4.1. O licitante deverá apresentar um ou mais atestados de capacidade técnica com firma reconhecida, fornecidos por pessoa jurídica de direito público ou privado que comprovem o fornecimento, nos termos do Termo de Referência, dos produtos e serviços compatíveis com o objeto desta licitação.

4.2. O licitante deverá apresentar um ou mais atestados de capacidade técnica com firma reconhecida, fornecidos por pessoa jurídica de direito público ou privado que comprovem a realização de treinamento com no mínimo 20 Horas (50% do TR) em appliance firewall com profissional certificado pelo fabricante da solução.

4.3. A licitante deverá apresentar portifólio do produto ofertado.

4.4. A licitante deverá apresentar todos os Part Number (P/N) e Fabricante da solução ofertada, juntamente com a proposta devidamente assinada.

5. DO APPLIANCE FIREWALL – ITEM 1

As características descritas nesse item será os requisitos mínimos para o produto ofertada;

5.1. Deve suportar a definição de VLAN trunking conforme padrão IEEE 802.1q, a criação de interfaces lógicas associadas às VLANs e o estabelecimento de regras de filtragem (Stateful Firewall) entre elas;

5.2. Deve suportar agregação de portas, com a criação de grupos de pelo menos 08 (oito) portas. Deve ser suportado o padrão LACP (Link Aggregation Control Protocol);

5.3. Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de sequência dos pacotes TCP, status dos flags “ACK”, “SYN” e “FIN”;

5.4. Deve permitir a “randomização” do número de sequência TCP, ou seja, funcionar como um “proxy” de número de sequência TCP de modo a garantir que um host situado em uma interface considerada “externa” (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;

5.5. Deve possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;

5.6. Deve suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos: hosts, redes IP, serviços. Deve ser possível verificar a utilização

("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos.

5.7. Deve possuir a funcionalidade de "proxy" de autenticação ("authentication proxy"), permitindo a criação de políticas de segurança de forma dinâmica, com autenticação e autorização do acesso aos serviços de rede sendo efetuadas por usuário. Deve ser possível obter as informações de usuário/senha por meio de pelo menos os seguintes protocolos: HTTP, HTTPS e Telnet. Deve ser possível ao Firewall exigir autenticação inclusive para uso de protocolos que não possuam nativamente recursos de autenticação;

5.8. Deve suportar autenticação usando base local de usuários (interna ao equipamento);

5.9. Deve permitir a integração do Firewall com a solução Microsoft Active Directory (MS-AD), permitindo a criação de políticas de filtragem baseados em usuários e grupos de usuários existentes na base MS AD;

5.10. Deve implementar listas de controle de acesso com no mínimo os seguintes campos: IP de Origem, Nome do Usuário/Grupo do AD, IP de Destino, Serviço de origem, Serviço de destino e Ação (permit/deny). O "nome de usuário" deverá ser identificado de forma automática e transparente para o usuário final através de consultas à base MS-AD;

5.11. Deve implementar políticas de controle de acesso baseadas em informações de horário ("time-based access control");

5.12. Deve implementar remontagem virtual de fragmentos ("Virtual Fragment Reassembly") em conjunto com o processo de inspeção stateful. Deve ser possível estabelecer o número máximo de fragmentos por pacotes e timeouts de remontagem;

5.13. Deve possuir suporte a inspeção "stateful" para pelo menos os seguintes protocolos de aplicação: Oracle SQL*Net Access, Remote Shell, FTP, HTTP, SMTP, ILS (Internet Locator Service), LDAP, ESMTP, TFTP;

5.14. Deve suportar a tradução do endereço IP carregado em uma mensagem DNS Reply (NAT na camada de aplicação) juntamente com a tradução do endereço IP presente no cabeçalho L3;

5.15. Deve possuir suporte a inspeção stateful dos protocolos de sinalização de telefonia H.323(v1, v2, v3, v4), SIP (Session Initiation Protocol), MGCP e SCCP. A partir da inspeção dos protocolo de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos;

5.16. Deve ser suportada a inspeção do protocolo SIP (SIP over TLS) em ambientes com voz criptografada. A partir da inspeção do protocolo de sinalização, devem ser criadas as conexões pertinentes para o tráfego SRTP (Secure RTP);

5.17. Deve possuir capacidade de limitar o número de conexões TCP simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);

5.18. Deve possuir capacidade de limitar o número de conexões TCP incompletas (‘half-open’) simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);

5.19. Deve possuir capacidade de limitar o número de conexões TCP simultâneas para um endereço de destino especificado;

5.20. Deve possuir capacidade de limitar o número de conexões TCP incompletas (‘half-open’) simultâneas para um endereço de destino especificado;

5.21. Deve permitir simultaneamente com a implementação “Network Address Translation” a filtragem “stateful” de pelo menos as seguintes aplicações:

5.21.1. H.323 (v1,v2, v3,v4) , Real Time Streaming Protocol (RTSP), SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol)

5.21.2. Microsoft Networking client and server communication (NetBIOS over IP)

5.21.3. Oracle SQL*Net client and server communication;

5.21.4. Domain Name System (DNS)

5.21.5. SUN Remote Procedure Call (RPC);

5.21.6. File Transfer Protocol (FTP) – modos “standard” e “passive”

5.22. VIRTUALIZAÇÃO

5.22.1. Deve possuir suporte a tecnologia de Firewall Virtual, com instâncias totalmente isoladas entre si. Dentro de cada instância de Firewall deve ser possível definir regras independentes de filtragem, regras de NAT, rotas e VLANs alocadas;

5.22.2. Dentro de cada instância de Firewall deve ser possível alocar no mínimo os seguintes tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC;

5.22.3. Dentro de cada instância de Firewall deve ser possível limitar (promover “rate limiting”) os seguintes recursos: taxa de estabelecimento de novas conexões, taxa de inspeção de aplicações, taxa de transmissão de mensagens Syslog;

5.22.4. A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter influência sobre a operação das demais instâncias;

5.22.5. Deve ser possível selecionar o modo de operação de cada instância de Firewall (seleção, por instância, de modo transparente ou roteado);

5.22.6. Deve ser suportada qualquer combinação de contextos em modo transparente e roteado, dentro do limite de instâncias solicitado.

5.23. SUBSISTEMA VPN

5.23.1. Deve suportar versões do cliente IPSEC VPN fornecido com a appliance para, no mínimo, os seguintes sistemas operacionais: Windows XP, Windows Vista, Windows 7, Linux (Intel) e MacOS;

5.23.2. Deve suportar a terminação túneis IPSEC do tipo “site-to-site” (LAN-to-LAN);

5.23.3. Deve suportar a terminação simultânea de conexões IPSEC VPN;

5.23.4. Deve suporte à criação de VPNs IPSEC com criptografia 168-bit 3DES, 128-bit AES e 256-bit AES;

5.23.5. Deve suportar alta disponibilidade das conexões IPSEC VPN, permitindo a utilização de uma segunda unidade em "standby". Em caso de falha de uma das unidades, não deverá haver perda das conexões ativas (stateful failover) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final;

5.23.6. Deve suportar negociação de túneis VPN IPSEC utilizando o protocolo IKE (Internet Key Exchange) nas versões 1 e 2, para garantir a geração segura das chaves de criptografia simétrica;

5.23.7. Deve suporte à integração com servidores RADIUS, LDAP, Microsoft AD e Kerberos, para tarefas de autenticação, autorização e accounting (AAA) dos usuários VPN;

5.23.8. Deve ser capaz de passar pelo menos os seguintes parâmetros para o cliente: endereço IP do cliente VPN, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name. A configuração do cliente VPN deve ser completamente automatizada, sendo exigida do usuário apenas a instalação do cliente VPN em seu PC;

5.23.9. Deve ser capaz de configurar nos VPN clients uma lista de acesso de "split tunneling", de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta (sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo "all tunneling", em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida;

5.23.10. Deve permitir a criação de "banners" personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN e, em caso de sucesso, mensagens de natureza administrativa;

5.23.11. Deve suportar o uso de certificados digitais emitidos pela autoridade certificadora ICP Brasil para autenticação das VPNs IPSec;

5.23.12. Deve permitir a criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança de forma interna ao equipamento;

5.23.13. Deve permitir a criação de pools de endereços IP de VPN (endereços privados) internamente ao equipamento;

5.23.14. Deve suportar a integração com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes;

5.23.15. Deve permitir que os endereços IP de VPN (endereços privados) sejam obtidos a partir de um servidor DHCP especificado pelo administrador do sistema;

5.23.16. Deve ser possível a associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN;

5.23.17. Deve permitir a definição dos horários do dia e dos dias das semana em que um dado usuário pode requisitar uma conexão VPN;

5.23.18. Deve suportar NAT (Network Address Translation;

5.23.19. Deve suportar operação no modo transparente a NAT ("NAT-transparent mode"), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation);

5.23.20. Deve permitir a terminação de conexões no modo IPSEC over TCP;

5.23.21. Deve permitir a terminação de conexões no modo IPSEC over UDP;

5.23.22. Deve ser possível visualizar no concentrador o número de conexões VPN estabelecidas em um dado instante e os respectivos usuários que estão fazendo uso destas;

5.23.23. Deve ser possível visualizar no cliente VPN o endereço privado adquirido durante a negociação da conexão IPSEC;

5.23.24. Deve ser possível definir vários templates de conexão no cliente VPN antes que seja enviado para instalação no computador do usuário final. Estes templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2 (IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES,AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5 e 7) e tempo de duração ("lifetime") da conexão. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN cliente;

5.23.25. 3.25. Deve suportar a utilização de certificados digitais padrão X.509 para a própria appliance VPN, possuindo integração com pelo menos as seguintes Certificate Authorities (CAs): Baltimore, Entrust, Verisign, Microsoft e RSA. Os clientes VPNs devem ter o mesmo suporte a certificados digitais. Deve ser suportado o protocolo SCEP para "enrollment" automático na autoridade certificadora (tanto para o concentrador como para os clientes IPSEC);

5.23.26. 3.26. Deve suportar protocolo Syslog para geração de logs de sistema;

5.23.27. 3.27. Deve implementar protocolo DTLS (TLS over UDP) de acordo com a RFC 4748;

5.23.28. 3.28. Deve permitir o mapeamento de atributos LDAP e RADIUS para parâmetros existentes na configuração local de grupos do concentrador. Deve ser possível escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS.

5.24. GERENCIAMENTO E CONECTIVIDADE

5.24.1. Deve implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;

5.24.2. Deve ser gerenciável via SNMP, v2c e v3;

5.24.3. Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS;

5.24.4. Deve ser fornecido com pelo menos uma interface 10/100/1000 dedicada a gerenciamento (out-of-band). Esta interface não deverá ser contabilizada para o atendimento daquelas originalmente especificadas para a appliance firewall;

5.24.5. Deve possuir mecanismo interno de captura de pacotes. Deve ser possível selecionar através de guias de configuração ("wizards") quais os pacotes (IP de origem e destino, portas TCP/UDP de origem e destino e interfaces de entrada devem ser capturados);

5.24.6. Deve permitir o armazenamento de pacotes capturados em formato tcpdump;

5.24.7. Deve possuir memória flash para armazenamento de imagem do sistema operacional e arquivos de configuração do equipamento;

5.24.8. Deve implementar completamente a porção cliente do protocolo TACACS+ para controle de acesso administrativo ao equipamento. Deve ser possível especificar conjuntos de comandos acessíveis a cada grupo de usuários administrativos e cada comando deve ser autorizado individualmente no servidor TACACS+. Todos os comandos executados bem como todas as tentativas não autorizadas de execução de comandos devem ser enviadas ao servidor TACACS+;

5.24.9. Deve vir acompanhado de interface gráfica para gerenciamento das funcionalidades de VPN e Stateful Firewall relativas ao dispositivo;

5.24.10. Deve implementar, por interface, as funções de DHCP Server, Client e Relay.

5.25. ROTEAMENTO

5.25.1. Deve suportar a criação de rotas estáticas e pelo menos os seguintes protocolos de roteamento dinâmicos: RIP, RIPv2, OSPF, OSPFv3 e BGPv4. Deve suportar a utilização de pelo menos dois processos de roteamento simultâneos e independentes.

5.25.2. Deve implementar o protocolo PIM (Protocol Independent Multicast) em Sparse Mode;

5.25.3. Deve suportar a operação como IGMP Proxy Agent.

5.26. IPv6

5.26.1. Deve suportar inspeção stateful de tráfego IPv6;

5.26.2. Deve suportar simultaneamente a criação de regras IPv4 e IPv6;

5.26.3. Deve suportar roteamento estático;

5.26.4. Deve implementar randomização do número de sequência TCP para conexões TCP que trafegam sobre IPv6;

5.26.5. Deve suportar anti-spoofing (sem uso de ACLs) para endereços IPv6;

5.26.6. Deve suportar gerenciamento sobre IPv6. Devem ser suportados pelo menos os seguintes protocolos de gerência: Telnet, SSH e HTTPS;

5.26.7. Deve suportar stateful failover de conexões IPv6;

5.26.8. Deve suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos.

5.27. ALTA-DISPONIBILIDADE

5.27.1. A solução deverá suportar alta disponibilidade em modo ativo-standby com todas as funcionalidades habilitadas;

5.27.2. Deverá suportar alta disponibilidade em modo cluster, com todas as unidades ativas simultaneamente. O modo cluster deve ser suportado com pelo menos as funcionalidades Stateful Firewall, VPN site-to-site e Next-Generation Firewall/IPS ativas simultaneamente;

5.28. SUBSISTEMA DE FILTRAGEM DE APLICAÇÃO

5.28.1. Deve suportar a identificação e controle de aplicações através de inspeção profunda de pacotes (Deep Packet Inspection), independentemente das portas usadas pela aplicação;

5.28.2. As aplicações devem ser classificadas de acordo com categoria, tipo e nível de risco;

5.28.3. Deve permitir criar regras para monitoramento e controle das aplicações e serviços, sendo capaz de executar no mínimo as seguintes ações:

5.28.4. Permitir o uso irrestrito de uma ou mais aplicações;

5.28.5. Permitir o uso irrestrito de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

5.28.6. Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

5.28.7. Negar totalmente o uso de uma ou mais aplicações independentes do usuário;

5.28.8. Deve suportar o controle de aplicações Web 2.0, definindo quais são as operações permitidas para cada uma destas aplicações (deve ser possível, no mínimo, restringir operações de “Post”, bloquear transferência de arquivos, bloquear uso de “games”);

5.28.9. Deve ser possível controlar as micro-applicações que podem ser utilizadas por cada uma destas aplicações Web 2.0 (esse tipo de controle deve estar disponível, no mínimo, para as aplicações Facebook, Google+, Twitter e Skype);

5.28.10. Deve permitir a customização de regras de detecção de novas aplicações.

5.29. SUBSISTEMA DE FILTRAGEM DE URL

5.29.1. Deve permitir a criação de regras de controle de acesso com base em informação de reputação dos sites. Essa base deve ser atualizada dinamicamente;

5.29.2. Deve permitir criar políticas de acesso baseadas em filtro de categorias de URL;

5.29.3. Deve ser incluído módulo de filtro de URL integrado na própria ferramenta de Firewall;

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

5.29.5. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, MS Active Directory;

5.29.6. Deverá possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e Grupos de usuários;

5.29.7. Deverá possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.29.8. Deverá incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

5.29.9. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação;

5.29.10. Deve possibilitar base de URLs local no appliance, evitando delay de comunicação/validação da URLs;

5.29.11. Deverá possuir pelo menos 50 (cinquenta) categorias de URLs;

5.29.12. Deverá possibilitar a criação categorias de URLs customizadas;

5.29.13. Deverá possibilitar a exclusão de URLs do bloqueio por categoria;

5.29.14. Deve possibilitar a customização de página de bloqueio;

5.29.15. Deve possibilitar o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site por um tempo);

5.29.16. Os logs do produto devem incluir informações das atividades dos usuários;

5.29.17. A atualização da base de dados deve ser automática com a opção de ser feita manualmente.

5.30. SUBSISTEMA IPS

5.30.1. Deve permitir a configuração de regras de exceção de inspeção de tráfego por endereço IP origem/destino ou VLAN, por segmento, realizando apenas a comutação do tráfego sem executar inspeção;

5.30.2. Deve realizar a monitoração de segmentos de rede em modo transparente sem endereço IP associado às interfaces de monitoração;

5.30.3. Deve possuir suporte a Jumbo Frame;

5.30.4. Deve monitorar VLANs padrão 802.1q;

5.30.5. Deve suportar o protocolo SNTP ou NTP;

5.30.6. Deve permitir nativamente o uso do SNMP versão 3;

5.30.7. Deve ser capaz de realizar auditoria das atividades de cada usuário;

5.30.8. Deve ser capaz de visualizar no mínimo as seguintes informações:

5.30.8.1. Incidentes de Intrusão;

5.30.8.2. Políticas aplicadas;

5.30.8.3. Atualizações instaladas;

5.30.8.4. Login e logout na interface web de gerencia;

5.30.8.5. Requisições de aumento de privilégio;

5.30.8.6. Inclusões e remoções de regras;

5.30.8.7. Registro de sensores na console de gerenciamento.

5.30.9. Configurações relacionadas ao envio de informações detectada pelos sensores de prevenção contra invasão, para dispositivo de armazenamento externo a solução de gerenciamento;

5.30.10. Deve permitir enviar os logs de auditoria das atividades de cada usuário, para um servidor de Syslogs;

5.30.11. Deve permitir armazenamento dos arquivos de configuração diretamente no appliance;

5.30.12. Deve permitir temporariamente, o armazenamento dos dados coletados e inspecionados em banco de dados local armazenado no sensor de IPS;

5.30.13. Deve permitir inspeção em IP versão 6 incluindo tunelamento IP versão 4 em IP versão 6, IP versão 6 em IP versão 4, IP versão 6 em IP versão 6, IP versão 6 com VLAN e label MPLS;

5.30.14. Deve permitir a inspeção em túneis GRE;

5.30.15. Deve permitir identificar/ restringir o acesso de hosts externos ao perímetro monitorado baseando-se em informações de reputação de domínios de e ranges de endereço IP;

5.30.16. Deve possuir capacidade de criar regras independentes para cada segmento monitorado;

5.30.17. Deve ser capaz de reconstruir e inspecionar fluxos de dados na camada de aplicação;

5.30.18. Deve possuir capacidade de remontagem de fluxo TCP e IP desfragmentation;

5.30.19. Deve possuir capacidade a resistência às ferramentas de evasão;

5.30.20. Deve possuir a capacidade de identificação de protocolos que utilizam portas aleatórias;

5.30.21. Deve detectar e bloquear ataques independente do sistema operacional alvo;

5.30.22. Deve permitir monitoração de sessões de pacotes na rede, atuando em modo “stateful inspection” (análise pacote a pacote e todo o seu estado), sendo capaz de bloquear ataques e tráfego não autorizado ou suspeito;

5.30.23. Deve possuir filtros de “PortScan”, protegendo a rede contra ataques do tipo “scan”;

5.30.24. Deve possuir filtros de proteção a equipamentos de rede, protegendo contra ataques a vulnerabilidades de equipamentos de rede (ex.: roteadores, switches, etc.);

5.30.25. Deve realizar análise e decodificação de fluxos de pacotes nas camadas 2 à 7 com no mínimo suporte aos seguintes protocolos e aplicações: IP, DNS, H.323, TCP, RPC, MPLS, SIP, ICMP, HTTP, FTP, P2P, ARP, Telnet, SMTP, IM, UDP, IMAP, SMB;

5.30.26. Deve possuir filtros de vulnerabilidades específicos dos protocolos de VoIP que bloqueiem: anomalias de protocolos, ataques de negação de serviço, vulnerabilidades específicas conhecidas, ferramentas de ataque e geradores de tráfego que causem degradação ou indisponibilidade de serviços;

5.30.27. Deve possuir no mínimo as seguintes proteções contra ataques a aplicações Web:

5.30.27.1. Web Protection;

5.30.27.2. Cross-Site Scripting;

5.30.27.3. SQL Injection;

5.30.27.4. Client-side attacks;

5.30.27.5. Injection Attacks;

5.30.27.6. Malicious Files Execution;

5.30.27.7. Information Disclosure;

5.30.27.8. Path Traversal;

5.30.27.9. Authentication;

5.30.27.10. Buffer Overflow;

5.30.27.11. Brute Force;

5.30.27.12. Directory Indexing.

5.30.28. Deve permitir criar regras para filtro com base em endereços de origem/destino, protocolo e VLAN ID;

5.30.29. Deve implementar proteção contra ataques DDoS através dos seguintes métodos:

5.30.29.1. Controle (limite de quantidade) de conexões por origem;

5.30.29.2. Controle (limite de quantidade) de conexões por destino;

5.30.29.3. Controle (limite de quantidade) de requisições “SYN” por origem;

5.30.29.4. Controle (limite de quantidade) de requisições “SYN” por destino;

5.30.29.5. Controle (limite de quantidade) de conexões (origem e Destino) e Controle (limite de quantidade) de requisições “SYN”(Origem e Destino).

5.30.30. Deve possibilitar que os pacotes sejam capturados para análise;

5.30.31. Deve ser capaz de identificar e bloquear ataques baseados em análises de anomalias de tráfego, anomalias de protocolo (RFC Compliance, Protocol Decoders, Normalização), assinaturas e vulnerabilidades;

5.30.32. Deve ser fornecido com uma configuração de filtros recomendados pré-configurados;

5.30.33. Deve permitir a inclusão de informações de vulnerabilidades oriundas de ferramentas de varredura externa (ex.: Nessus, Qualys, Foundstone, etc);

5.30.34. Deve permitir a identificação de anomalia de rede observando o tráfego ou informações do flow de ativos da rede de forma nativa;

5.30.35. Deve permitir a análise do comportamento da rede, com o intuito de detectar ameaças com origem/destino a segmentos monitorados pelo IPS. Isto inclui a capacidade de estabelecer padrões "normais" de tráfego através de técnicas de análise de fluxo (por exemplo, IPfix) e a capacidade de detectar desvios dos padrões considerados normais;

5.30.36. Deve permitir a análise do comportamento da rede fornecendo visibilidade do uso do segmento monitorado para auxiliar na solução de falhas de rede ou degradação de desempenho, no mínimo as seguintes informações devem ser disponibilizadas:

5.30.36.1. Fluxos de sessão dos hosts;

5.30.36.2. Hora de início/fim;

5.30.36.3. Quantidade de dados trafegados.

5.30.37. Deve permitir coletar, armazenar e correlacionar as informações adquiridas passivamente, sobre hosts que trafegam pelos segmentos monitorados pelo(s) IPS. No mínimo as seguintes informações devem ser correlacionadas e armazenadas:

5.30.37.1. Sistema operacional do Host;

5.30.37.2. Serviços existentes no Host;

5.30.37.3. Portas em uso no Host;

5.30.37.4. Aplicações em uso no Host;

5.30.37.5. Vulnerabilidades existentes no Host;

5.30.37.6. Smart phones e tablets;

5.30.37.7. Network flow;

5.30.37.8. Anomalias de redes;

5.30.37.9. Identidades de usuários;

5.30.37.10. Tipo de arquivo e protocolo;

5.30.37.11. Conexões maliciosas.

5.30.38. Deve permitir criar uma lista com o ”ambiente ideal esperado” e a cada mudança nesse ambiente, o sensor deverá no mínimo alertar a console de gerencia sobre a mudança identificada. Entendemos como “ambiente ideal esperado” o conjunto de informações pré-configuradas na gerencia dos sensores de IPS a respeito dos atributos dos hosts participantes desse segmento, deve ser configurado no mínimo os seguintes atributos:

5.30.38.1. Sistema Operacional;

5.30.38.2. Serviços vigentes nos hosts;

5.30.38.3. Aplicações autorizadas a serem executadas nos hosts;

5.30.38.4. Aplicações não autorizadas a serem executadas nos hosts.

5.30.39. Deve permitir criar ou importar regras no padrão OpenSource , essas regras, devem poder ser habilitadas para simples monitoramento ou para bloqueio de tráfego, não deve haver limite da quantidade de regras a serem criadas ou importadas e não deve haver limite de funcionalidade nas regras criadas ou a serem importadas;

5.30.40. Deve permitir criar regras para monitoramento e controle das aplicações e serviços nos segmentos monitorados, os sensores de IPS devem ser capazes de executar no mínimo as seguintes ações:

5.30.40.1. Permitir o uso irrestrito de uma ou mais aplicações;

5.30.40.2. Permitir o uso irrestrito de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

5.30.40.3. Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

5.30.40.4. Negar totalmente o uso de uma ou mais aplicações independentes do usuário;

5.30.41. Deve possuir capacidade de criar assinaturas definidas pelo usuário com uso de expresses regulares;

5.30.42. Deve possuir capacidade de modificar e alterar as assinaturas existente, podendo a critério do administrador, alterar o modificar o conteúdo da assinatura

5.30.43. Deve ter a capacidade de identificar o tipo de arquivo trafegado e permitir a criação de políticas de detecção e bloqueio de eventos baseados no tipo de arquivo;

5.30.44. A solução deverá detectar e bloquear as seguintes categorias de ataques e ameaças:

5.30.44.1. Malwares;

5.30.44.2. Port Scans;

5.30.44.3. VoIP attacks;

5.30.44.4. IPv6 attacks;

5.30.44.5. DoS attacks;

5.30.44.6. Buffer overflows;

5.30.44.7. P2P attacks;

5.30.44.8. Anomalias em protocolos e aplicações;

5.30.44.9. Ameaças Zero-day;

5.30.44.10. Pacotes malformados;

5.30.44.11. Segmentação TCP e fragmentação IP.

5.30.45. Deve ser fornecido com serviço de atualização permanente de filtros de ataques e vulnerabilidades por 03 anos;

5.30.46. Os equipamentos deverão ser fornecidos com seu software com licença irrestrita, em sua versão mais atual e completa. O fornecimento deverá incluir todas as licenças de software necessárias para a implementação de todas as funcionalidades disponibilizadas pelo fabricante para os equipamentos fornecido.

5.31. SUBSISTEMA CONTRA MALWARE

5.31.1. Deve prover as funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de command & control, resolução e call-backs;

5.31.2. Deve possui capacidade para monitoração em tempo real;

5.31.3. Deve permitir diariamente, semanalmente ou mensalmente informações a respeito das tendências de ataque e riscos do ambiente;

5.31.4. Deve permitir identificar tráfego de rede gerado por dispositivos conectados no segmento monitorado, incluindo tráfego malware e ataques associados;

5.31.5. Deve oferecer capacidade nativa e sem necessidade de equipamentos tipo SIEM de correlacionar informações de alertas malwares com ataques detectados e condições de tráfego, para assim definir um tipo de alerta personalizado em tempo tempo real;

5.31.6. Deve permitir o controle em tempo real de arquivos;

5.31.7. Deve permitir o bloqueio em tempo real de malwares;

5.31.8. Deve permitir em tempo real o controle e bloqueio de aplicações (protocolos, clientes e web);

5.31.9. Deve permitir o controle de acesso;

5.31.10. Deve permitir o controle de URL’s;

5.31.11. Deve suportar em tempo real a detecção e prevenção (bloqueio imediato) de arquivos malwares e ataques para os protocolos HTTP (Inbound e Outbound), SMTP (Inbound e Outbound), FTP (Inbound e Outbound), POP3 (Inbound e Outbound), IMAP (Inbound e Outbound), NETBIOS-SSN (SMB, Inbound e Outbound) e adicionalmente permite em tempo real a detecção (Inbound ou outbound) e prevenção (bloqueio imediato, Inbound ou outbound) de ataques e tráfego malware do tipo: comunicações de comando e controle, identificação de backdoors, propagação de infecção, presença e uso de ferramentas malware, ataques de negação de serviço, comunicação e presença de keyloggers (troca de informações), identificar redirecionamentos, identificar a exploração de overflows;

5.31.12. Deve implementar e identifica existência de Malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Command and Control;

5.31.13. Deve implementar mecanismos de detecção e bloqueio de vazamento de informações sensíveis no ambiente, ao permitir a identificação de dados em: arquivos Microsoft Word (não criptografados) sendo enviados ou recebidos via protocolos FTP e HTTP, números de cartões de crédito para até 8 tipos de protocolos diferentes, endereços e-mail para até 8 tipos de protocolos diferentes e dados customizados pelo administrador para até 8 tipos de protocolos diferentes;

5.31.14. Deve possuir capacidade de Implementar detecção de ataques e malwares que utilizem mecanismo de exploit em arquivos PDF;

5.31.15. Deve implementar capacidade paara detecção de explorações diretas, uso suspeito ou malicioso das seguintes aplicações;

5.31.16. Deve permitir que arquivos executáveis (MSEXE) identificados pelo sensor sejam automaticamente enviados para análise utilizando tecnologia de virtualização em nuvem;

5.31.17. Deve manter um histórico dos resultados de avaliações prévias e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite;

5.31.18. Deve permitir virtualização para análise sobre sistemas operacional Windows;

5.31.19. Deve implementar rede de inteligência global en tiempo real proprietária para cobrir ataques originados de qualquer localidade global, novas origens e destinos de comunicações e distribuição de malwares;

5.31.20. Deve permitir modo de configuração in-line (em linha) totalmente transparente que permita em tempo real a detecção (inbound e/ou outbound) e a prevenção através de bloqueio (inbound e/ou outbound) de ataques malwares sejam estes no formato de arquivos maliciosos, comunicações ou explorações diretas, caso seja necessário a solução suporta a utilização de configurações de proxies;

5.31.21. Deve possuir capacidade de automatica e periódicam para download e instalar atualizações de dados de reputação IP para identificação de tráfego

associado a origens e destinos de malware, comando e controle, spam, bots, proxies abertos, relays abertos, phishing e TOR (the onion router);

5.31.22. Deve implementar 02 (dois) modos de operação: detecção passiva e inline sendo que no último a solução deve permitir implementar bloqueios em tempo real e inclusive especificar a terminação das conexões de ataques utilizando pacotes "tcp reset" ao detectar a transferência de arquivos maliciosos, atividade de comunicação, infecção e proliferação de malwares assim como outras categorias de explorações remotas e motivadores de ataques através da rede monitorada pela solução;

5.31.23. Deve implementar funcionalidade de bloqueio em tempo real de arquivos maliciosos (detectados como malwares) e comunicações malwares conhecidas no modo inline;

5.31.24. Deve possuir um recurso de análise tipo "sandbox", para no mínimo arquivos executáveis (MSEXE) de modo a permitir a análise completa do comportamento do Malware ou código malicioso;

5.31.25. Deve possuir recursos que permitem o envio de informações de eventos de ataques e malwares para ferramentas de SIEM de fabricantes terceiros;

5.31.26. Deve possuir recursos que permitem o envio de informações de eventos de ataques e malwares para servidores Syslog;

5.31.27. Deve implementar suporte a protocolo SNMP v1, v2 e v3 para atividades de gerenciamento;

5.31.28. Deve implementar atualização da base de dados da Rede de Inteligência de forma automático, permitindo o agendamento mínimo de 2 hora de intervalo;

5.31.29. Deve implementar via interface de gráfica de gerenciamento todas as opções de análise e tratamento eventos de ataques de rede, Malware, detecção de tráfego e notificação de eventos em tempo real, adicionalmente implementa automáticamente a capacidade de traçar uma visão cronológica de eventos de forma gráfica permitindo identificar em tempo-real a trajetória de acesso ou propagação de ameaças malware de forma lateral no ambiente, identificando o nome do arquivo, tipo e categoria do arquivo, nível de ameaça quando disponível, sha-256, tipo de evento, protocolo de aplicação utilizado, aplicação cliente utilizada para transferência, quantidade de visualizações, dia e hora, origem e destino do tráfego;

5.31.30. Deve realizar toda detecção e bloqueio de ataques de rede e malwares em tempo real, não sendo uma solução que necessita de ou é exclusivamente dependentes de tecnologia de virtualização tipo "sandboxing" para detecção de arquivos maliciosos e presenção de malware na rede monitorada;

5.31.31.

5.31.32. Os processos de detecção e determinação de malwares, ataques e tráfego assim como os bloqueios preventivos inclusive para os arquivos sendo transferidos pela rede pelos protocolos suportados são realizados de forma automatizada e em tempo real;

5.31.33. O recurso de execução em ambiente de virtualização disponibilizado (sandbox), permite a automatização do envio de arquivos suportados pela solução de rede para este tipo de solicitação de análise dinâmica;

5.31.34. A solução Implementa múltiplos motores (engines) para verificação de Malware e/ou códigos maliciosos, não dependendo somente da utilização de recursos de análise virtualizada (sandbox) como método de identificação de malwares em arquivos;

5.31.35. Deve permitir Implementar mecanismo de definição de exceções do tipo whitelist de arquivos, endereços IP, aplicações;

5.31.36. Deve permitir criação de regras de detecção e permitir a criação de detecções de arquivos maliciosos utilizando amostra de arquivo, hash SHA-256 único e lista de hash SHA-256;

5.31.37. Deve permitir Implementar mecanismo de whitelist e detecções customizadas de arquivos, permitindo definição de regras por VLAN, subrede, endereço IP para utilização das listas;

5.31.38. Deve implementar a identificação e capacidade de controle de acesso em tempo real para os seguintes tipos de arquivo:

5.31.38.1. MSEXE,9XHIVE,DMG,DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG_PICT,MAYA,PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN,BINARY_DATA,BINHEX, EICAR, ELF,ISHIELD_MSI, MACHO, RPM, TORRENT, AMR,FFMPEG,FLAC,FLIC,FLV,IVR,MIDI,MKV,MOV,MPEG,OGG,PLS,R1M,REC,RIFF,RIFX,RMF,S3M,SAMI,SMIL,SWF,WAV,WEBM,7Z,ARJ,BZ,CPIO_CRC,CPIO_NEWC,CPIO_ODC,,JAR,LHA,MSCAB, MSSZDD,OLD_TAR,POSIX_TAR,RAR,SIS,SIT,ZIP,ZIP_ENC,ACCDB,HLP,MAIL,MDB,MDI,MNY,MSCHM,MSOLE2,MSWORD_MAC5, MWL,NEW_OFFICE,ONE,PST,RTF,TNEF,WAB,WP,WRI,XLW,XPS.

5.31.39. Deve implementar em tempo real a inspeção, detecção e bloqueio autónomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos:

5.31.39.1. 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC.

5.31.40. A solução ofertada deve ser totalmente do mesmo fabricante

5.31.41. Deve ser fornecido com serviço de atualização permanente por 03 anos;

5.32. ARQUITETURA

5.32.1. Deve ser montável em rack de 19 polegadas (devem ser fornecidos os kits de fixação necessários). O equipamento fornecido deve ocupar no máximo 02 (duas) unidades de rack (02U);

5.32.2. Deve ser fornecido com fonte internas ao equipamento;

5.32.3. Deve ser fornecido com pelo menos 8 (Oito) interfaces 1 Gigabit Ethernet .

5.33. DESEMPENHO

5.33.1. Deve suportar pelo menos 250.000 (Duzentas e cinquenta mil) conexões simultâneas em sua tabela de estados de Stateful Firewall;

5.33.2. Deve suportar a criação de pelo menos 20.000 (Vinte mil) novas conexões TCP por segundo para a funcionalidade de Stateful Firewall;

5.33.3. Deve suportar taxa de encaminhamento de Stateful Firewall de pelo menos 750.000 pps (Setecentos e cinquenta mil pacotes por segundo);

5.33.4. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 1.8 Gbps (Um Gbps e Oitocentos Mbps) para pacotes UDP;

5.33.5. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 900 Mbps (Novecentos Mbps) para pacotes TCP multiprotocolo;

5.33.6. Deve suportar um throughput de, no mínino, 850 Mbps (Oitocentos e Cinquenta Mbps por segundo) com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;

5.33.7. Deve suportar a terminação de pelo menos 50 (Cinquenta) túneis IPSEC VPN simultaneamente. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;

5.33.8. Deve suportar a terminação simultânea de túneis IPSEC, de modo que se suporte um total de pelo menos 300 (Trezentos) usuários VPN, independentemente do tipo de sessão. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;

5.33.9. Deve possuir desempenho de, no mínimo, 250 Mbps (Duzentos e Cinquenta Megabits por segundo) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;

5.33.10. Não deve haver restrição de número de usuários simultâneos através do equipamento para a licença de software fornecida para a funcionalidade de Stateful Firewall;

5.33.11. Deve ser possível criar pelo menos 100 (Cem) interfaces lógicas associadas a VLANs;

5.33.12. Devem ser suportadas, através de licenças adicionais, instâncias virtuais de Firewall, sendo entregue com pelo menos 5(Cinco) instâncias virtuais;

5.33.13. Deve reconhecer mais de 1000 (mil) aplicações com atualizações automáticas;

5.33.14. Deve suportar pelo menos 80 categorias de URL;

5.34. SUBSISTEMA DE GERÊNCIA CENTRALIZADA

5.34.1. Deve ser fornecido na forma de appliance dedicado ou appliance virtual compatível com VMWARE, com licenças e capacidade suficientes para gerenciar a quantidade de dispositivos solicitada;

5.34.2. Deve permitir a instalação, monitoramento, configuração e atualização de múltiplos equipamentos, simultaneamente, estejam estes instalados localmente ou remotamente;

5.34.3. Deverá ser capaz de monitorar, configurar, diagnosticar problemas e gerar relatórios de múltiplos equipamentos;

5.34.4. Deve possuir no mínimo as seguintes opções de resposta automática às ameaças detectadas:

5.34.4.1. Alertas automáticos;

5.34.4.2. Remediações em firewall;

5.34.4.3. Remediações em roteador;

5.34.4.4. Scans de rede;

5.34.5. Deve permitir configurar o perfil de inspeção de tráfego independentemente do segmento associado (físico ou lógico) bem como a direção de inspeção dentro do segmento (somente de entrada, somente de saída ou ambos os sentidos);

5.34.6. Deve permitir aplicar um ou mais perfis de inspeção de tráfego a um segmento ou a um grupo de segmentos;

5.34.7. Deve suportar a aplicação de diversos perfis de inspeção de tráfego, trabalhando de maneira simultânea em diferentes segmentos físicos ou lógicos;

5.34.8. Deve permitir criar políticas de inspeção baseada em grupos, usando os seguintes parâmetros para montagem dos grupos:

5.34.8.1. Sensores;

5.34.8.2. Conjunto de Interfaces de um único equipamento;

5.34.8.3. Conjunto de Interfaces de equipamentos distintos;

5.34.9.

5.34.10. Deve permitir que toda alteração de política e definições na console de gerenciamento seja registrada;

5.34.11. Deve permitir a criação e aplicação de respostas a eventos;

5.34.12. Deve categorizar os eventos de acordo com a severidade;

5.34.13. Deve permitir configurar diferentes perfis de usuários com níveis de privilégios hierárquicos;

5.34.14. Deve possuir capacidade de atualização manual e automática das assinaturas dos subsistemas IPS gerenciados;

5.34.15. Deve permitir a atualização do firmware dos IPSs gerenciados;

5.34.16. Deve coletar passivamente informações de identidade do usuário, para correlacionar o endereçamento IP com o nome de usuário, e tornar esta informação disponível para efeitos de gestão/correlação de eventos;

5.34.17. Deve permitir identificar usuários da rede interna, através de diretório padrão LDAP e correlacioná-los com os eventos de rede, tanto de

conformidade com a política de segurança como de intrusão, sem necessidade de solução externa;

5.34.18. A análise de comportamento de rede deve permitir correlacionar os nomes de usuários com eventos de segurança suspeitos;

5.34.19. Deve permitir monitorar as condições de "saúde" dos subsistemas IPS monitorados, apresentando informações em sua console gráfica de no mínimo seguintes informações:

5.34.19.1.

5.34.19.2. Heartbeat dos subsistemas IPS, permitindo monitorar se os equipamentos gerenciados estão operantes;

5.34.19.3. Uso da CPU- Deve permitir monitorar o uso da CPU, deve ser possível definir no dois tipos diferentes de alertas, para diferentes níveis de uso da CPU;

5.34.19.4. Reset da interfaces - Deve permitir monitorar o reset nas interfaces de inspeção dos subsistemas IPS;

5.34.19.5. Uso de Disco- Deve permitir monitorar o uso do Disco, deve ser possível definir nos dois tipos diferentes de alertas, para diferentes níveis de uso do Disco;

5.34.19.6. Taxa de eventos de IPS- Deve permitir monitorar a taxa de eventos de IPS recebida por segundo, deve ser possível definir nos dois tipos diferentes de alertas, para diferentes níveis de eventos de IPS recebidos por segundo;

5.34.19.7. Uso de Memória - Deve permitir monitorar o uso da memória do appliance, deve ser possível definir nos dois tipos diferentes de alertas, para diferentes níveis de uso de memória;

5.34.19.8. Sincronização de tempo – Monitoramento da diferença de tempo de dispositivos gerenciados;

5.34.19.9. Traffic Status - Deve permitir monitorar se as interfaces de inspeção dos sensores de IPS estão recebendo tráfego.

5.34.20. Deve gerar gráficos em tempo real das estatísticas do tráfego, ataques filtrados, hosts de rede e serviços;

5.34.21. Deve ser gerenciado através de interface WEB segura (HTTPS) e toda a comunicação entre dispositivo de gerencia e sensor de IPS deve ser criptografada;

5.34.22. Deve possuir recurso de geolocalização. Localização geográfica da máquina do atacante;

5.34.23. Deve permitir criar no mínimo os relatórios descritos abaixo:

5.34.23.1. Relatórios dos 10 ataques mais comuns;

5.34.23.2. IP de Origem;

5.34.23.3. IP de Destino;

5.34.23.4. Ataques por severidade;

5.34.23.5. Ataques por ação, por porta, por segmento, por protocol;

5.34.23.6. Ataques por endereço IP de Destino, endereço IP de Origem.

5.34.24. Deve permitir gerar relatórios gráficos, permitindo a geração de relatórios periódicos de forma automática. A solução deverá permitir também o envio automático dos relatórios para e-mail escolhido pelo administrador da solução;

5.34.25. Deve exportar relatórios para no mínimo os seguintes formatos: HTML, PDF e CSV;

5.34.26. Deve possuir ferramenta interna de manutenção do banco de dados, capaz de realizar no mínimo as seguintes funções:

5.34.26.1. Backup Manual dos dados e das configurações do sistema de gerenciamento;

5.34.26.2. Backup agendado dos dados e das configurações do sistema de gerenciamento;

5.34.26.3. Armazenar no disco local do sistema de gerenciamento o backup dos sensores e sistema de gerenciamento.

5.34.26.4. Assim que o backup for concluído o sistema de gerenciamento deve ser capaz de copiar através de protocolo de comunicação criptografado (nativo do equipamento) e sem intervenção humana o Backup realizado para um host diferente;

5.34.27. Deve possuir banco de dados interno para armazenamento dos logs, permitindo ao administrador da solução que redirecione o armazenamento dessa base de dados em um volume de disco remoto;

5.34.28. Deve manter os logs de ataques e de alarmes enviados pelos subsistemas IPS;

5.34.29. Deve permitir enviar as informações para um Syslog remoto;

5.34.30. Deve ser gerenciável via linha de comando através de acesso seguro utilizando o protocolo SSH;

5.34.31. Deve implementar nativamente (sem uso de ferramentas de terceiros) SNMPv3;

5.34.32. Deve permitir envio de eventos SNMP relativos ao desempenho e funcionamento do equipamento;

5.34.33. Deve implementar NTP ou SNTP.

6. DO TREINAMENTO

6.1. O treinamento será Hands-on (mão na massa), treinamento feito durante a própria implantação do sistema/ appliance, ou seja, o Sistema/ appliance está sendo instalado, os técnicos da AGEHAB acompanham a implantação e são treinados ao mesmo tempo. Essa atividade resume-se em transferir as rotinas e conhecimentos necessários para a equipe técnica da CONTRATANTE.

6.2. O treinamento deverá ser de responsabilidade da CONTRATADA com carga horária suficiente para capacitar, de forma adequada, os 02 (dois) técnicos da CONTRATANTE.

6.3. A CONTRATADA deve disponibilizar profissional certificado pelo fabricante da solução ofertada para realizar o treinamento junto a CONTRATANTE.

6.4. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento, hospedagem, alimentação, o fornecimento do material didático em língua portuguesa.

6.5. O treinamento Hands-on deverá ser marcado com a Gerência de Tecnologia da Informação com antecedência mínima de 03 (três) dias antes da data do treinamento.

6.6. Para efeito de cálculo e orientação da CGU (Controladoria Geral da União) será utilizada a unidade UST (Unidade de Serviço Técnico) que equivale a uma hora de trabalho.

7. DA GARANTIA, SUPORTE E SERVIÇOS DE ASSINATURA

7.1. Todos os itens deveram seguir os padrões abaixo. Os serviços de garantia, suporte técnico e serviços de assinaturas deverão ser fornecidos pelo fabricante do equipamento.

7.1.1. O serviço de suporte técnico durante o período de garantia de 36 (trinta e seis) meses atendendo as seguintes exigências:

7.1.1.1. O serviço de suporte técnico deverá ser 24x7x4 (vinte e quatro horas por dia, sete dias por semana, quatro horas de tempo de resposta), no local onde a solução se encontrar instalada (on-site), por técnicos devidamente habilitados e credenciados pelo fabricante, e sem qualquer ônus adicional;

7.1.1.2. O fabricante deverá disponibilizar canal de atendimento para abertura de chamados técnicos 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante número 0800 ou número local em Brasília;

7.1.1.3. Para cada chamado técnico, deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas;

7.1.1.4. Todos os serviços baseados em assinaturas devem estar disponíveis por, no mínimo, 36 (trinta e seis) meses.

8. DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

8.1. Todos os itens deveram seguir os padrões de prazo, local de entrega e forma de recebimento descritos abaixo.

8.1.1. Os equipamentos deverão ser entregues até 60 (sessenta) dias a contar da assinatura do contrato ou instrumento equivalente, na cede da Agência Goiana

de Habitação S/A Rua 18 A nº 541, Setor Aeroporto, Goiânia-GO, CEP 74070-060;

8.1.2. A CONTRATANTE determinará o local para entrega e verificará todas as condições e especificações, em conformidade com o Termo de Referência;

8.1.3. Entende-se por entrega as seguintes atividades: o transporte dos produtos embalados para o local determinado pela CONTRATANTE, a entrega dos volumes, a desembalagem, a verificação visual do produto e sua reembalagem se for o caso;

8.1.4. Os equipamentos deverão ser novos e sem uso e deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

8.1.5. No ato da entrega, a gerência responsável emitirá TERMO DE RECEBIMENTO PROVISÓRIO relacionando todos os produtos recebidos, nos termos da Nota Fiscal;

8.1.6. Os produtos serão objeto de inspeção, que será realizada por pessoa designada pela gerência responsável, conforme procedimentos a seguir:

8.1.6.1. Abertura das embalagens;

8.1.6.2. Comprovação de que o produto atende às especificações mínimas exigidas e/ou aquelas superiores oferecidas pela CONTRATADA;

8.1.6.3. Colocação do produto em funcionamento, se for o caso;

8.1.6.4. Teste dos componentes se for o caso;

8.1.6.5. O período de inspeção será de até 10 (dez) dias úteis;

8.1.7. Nos casos de sinais externos de avaria de transporte ou de mau funcionamento do produto, verificados na inspeção do mesmo, este deverá ser substituído por outro com as mesmas características, no prazo de até 30 (trinta) dias corridos, a contar da data de realização da inspeção;

8.1.8. Findo o prazo de inspeção e comprovada a conformidade dos produtos com as especificações técnicas exigidas no Edital e aquelas oferecidas pela CONTRATADA, a gerência responsável emitirá o TERMO DE RECEBIMENTO DEFINITIVO;

8.1.9. Nos casos de substituição do produto, iniciar-se-ão os prazos e procedimentos estabelecidos nestas CONDIÇÕES DE RECEBIMENTO

8.1.10. Correrão por conta da CONTRATADA as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos.

9. DAS OBRIGAÇÕES DA CONTRATADA

9.1. Além das resultantes da Lei 8.666/93 a adjudicatária se obriga, nos termos deste Termo de Referência, a:

9.1.1. Prestar todos os esclarecimentos que forem solicitados pela fiscalização da contratante;

9.1.2. Manter durante toda a execução do termo respectivo, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;

9.2. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

9.3. Manter atualizados, durante a vigência do contrato, para fins de pagamento, a Certidão Negativa de Débito – CND de Débito Trabalhista-CNDT, o Certificado de Regularidade - CRF do FGTS e certidão de regularidade junto à Fazenda Federal e municipal;

9.4. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado no Termo de Referência.

9.5. Efetuar treinamento para operacionalização e implantação do appliance de firewall e seus subsistemas, para equipe técnica da AGEHAB;

9.6. **São expressamente vedadas à CONTRATADA**:

9.6.1. A ceder, sob qualquer forma, os créditos oriundos deste contrato a terceiros;

10. DAS OBRIGAÇÕES DA CONTRATANTE

10.1. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da contratada ou por seu preposto;

10.2. Fornecer de toda a infraestrutura necessária para instalação e funcionamento dos equipamentos, como local físico, tomadas elétricas, pontos de acesso à rede, etc.

10.3. Efetuar o pagamento conforme execução dos serviços, desde que cumpridas todas as formalidades e exigências do contrato;

10.4. Exercer a fiscalização do contrato;

10.5. Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato;

10.6. Convocar reunião inicial, quando necessário, com todos os envolvidos na contratação; e acompanhar e monitorar toda a execução dos serviços.

11. DO LOCAL DE ENTREGA

11.1. Todos produtos licitados serão entregues na sede da Agência Goiana de Habitação S/A - AGEHAB, situadas na Rua 18 A nº 541 – Setor Aeroporto – Goiânia – GO – CEP 74070-060.

11.2. A proposta comercial deverá considerar todos os custos relativos a logística e entrega dos equipamentos na cidade de Goiânia – GO.

12. DA VIGÊNCIA

12.1. O contrato terá um prazo de 12 (doze meses) meses.

12.2. Na hipótese da adjudicatária não comparecer para assinar o Contrato no prazo estipulado, sem prejuízo das sanções previstas neste Edital, será convocada licitante remanescente, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições da sua proposta.

13. DO PAGAMENTO

13.1. O pagamento do itens licitados será procedido mediante a apresentação da Nota Fiscal/Fatura, após o fechamento do mês e a quitação até o décimo dia útil do mês seguinte.

13.2. As nota(s) fiscal (is)/faturas deverão conter no mínimo os seguintes dados:

13.3. Data de emissão

13.4. Estar endereçada a Agência Goiana de Habitação - AGEHAB, situada a Rua 18-A nº 541, Setor Aeroporto - Goiânia/GO, CNPJ nº 01.274.240/0001-47;

13.5. Preços unitários;

13.6. O pagamento será efetuado após ateste da autoridade competente assim como das respectivas requisições da AGEHAB, desde que a Certidão Negativa de Débito – CND, o Certificado de Regularidade do FGTS – CRF, a prova de regularidade para com a Fazenda Federal e municipal

13.7. Na ocorrência da rejeição de nota fiscal/fatura, motivada por erro ou incorreções, o prazo estipulado no subitem 14.1 passará a ser contado a partir da data da sua reapresentação, examinadas as causas da recusa;

14. DA ESTIMATIVA DE PREÇOS

14.1. Valor estimado para o objeto licitado.

Item	Descrição	Unidade	Quantidade	Preço unitário (R$)	Preço Total (R$)
1	Appliance de Firewall	Un.	01	R$ 76.656,66	R$ 76.656,66
2	Treinamento Hands-on	UST	40	R$ 503,33	R$ 20.133,20
				VALOR ESTIMADO TOTAL	R$ 96.789,86

Saulo de Tarso G. Vitoy
Gerente de Tecnologia da Informação

ANEXO II

MODELO DE CARTA PROPOSTA

Dados da empresa:
Razão Social:
CNPJ:
Endereço completo:
Fone/Fax:
E-mail:

Proposta que faz a empresa _____, CNPJ nº_____, aquisição dos produtos conforme as especificações contidas no edital nº 013/2016.

Lote 01:

Item	Descrição	Unidade	Quantidade	Preço unitário (R$)	Preço Total (R$)
1	Appliance de Firewall	Un.	01		
2	Treinamento Hands-on	UST	40		
VALOR TOTAL DA PROPOSTA					

Condições gerais da Proposta:
Validade da Proposta:
Prazo e Local de entrega: Rua 18-A n541 Setor Aeroporto – Goiânia-GO CEP 74.070-060
Condições de pagamento:

Das Declarações:
→ Declaração expressa, de que seus empregados são regidos pela legislação trabalhista vigente (consolidação das Leis de Trabalho - CLT), em cumprimento ao Termo de Conciliação Judicial;
→ Declaração expressa de estarem incluídos nos preços propostos todos os impostos e encargos devidos, bem como, quaisquer outras despesas, diretas e indiretas, incidentes no fornecimento do material/serviço.

....., ... de ..... 2016.

_____
assinatura e carimbo
(Representante Legal)

ANEXO III

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATO SUPERVENIENTE

À
COMISSÃO PERMANENTE DE LICITAÇÃO DA
AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB
REFERENTE: PREGÃO ELETRÔNICO Nº 013/2016

_____, CNPJ _____(Nome e CNPJ da empresa), sediada na _____**(endereço completo)** declara, sob as penas da lei, que até a presente data inexistam fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

_____, _____ de _____ de 2016.

_____
(Nome completo do declarante)
(Nº da CI do declarante)

ANEXO IV

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE MENOR TRABALHADOR

À
COMISSÃO PERMANENTE DE LICITAÇÃO DA
AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB
REFERENTE: PREGÃO ELETRÔNICO Nº 013/2016

(Nome da Empresa) _____, (CNPJ da empresa) _____, sediada na _____ (endereço completo) por intermédio de seu representante legal o (a) Sr(a) _____ portador(a) da carteira de identidade nº _____ e do CPF nº _____, DECLARA, para fins do disposto no inciso V do art. 27 da Lei nº 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854/99, regulamentada pelo Decreto nº 4.358/202, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos.

Ressalva: emprega menor, a partir de 14 (quatorze) anos na condição de aprendiz:
SIM ( ) NÃO ( )

_____, _____ de _____ de 2016.

_____
(Nome e nº da Identidade do declarante)

ANEXO V

DECLARAÇÃO DE PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO

A
AGÊNCIA GOIANA DE HABITAÇÃO S/A
Rua 18-A nº 541, Setor Aeroporto
Goiânia - GO

Declaramos, sob as penas da Lei, conhecer e aceitar as condições constantes do Pregão Eletrônico nº 013/2016 e seus anexos e que atendemos plenamente aos requisitos necessários para a habilitação.

....., ... de ..... 2016.

_____

Nome / Assinatura do Representante Legal

Cargo:

PREENCHIDA EM PAPEL TIMBRADO DA EMPRESA E ASSINADA POR SEUS REPRESENTANTES LEGAIS OU PROCURADOR (es) DEVIDAMENTE HABILITADO (s)

ANEXO VI

DECLARAÇÃO DE PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO

Ref: (Identificação da Licitação)

.....,inscrito no CNPJ n.º....., por intermédio de seu representante legal o(a) Sr. (a)....., portador da Carteira de Identidade n.º ..... DECLARA, sob as penas da lei, em especial o art. 299 do código penal brasileiro, que é fornecedora de bens e serviço de informática.

Declara, ainda, que apresentará os documentos comprobatórios do disposto acima na etapa de habilitação da empresa.

_____

(Data)

_____

(Representante Legal)

ANEXO VII

GLOSSÁRIO

Unidade de Serviço Técnico (UST)	Unidade de Serviço Técnico (UST), é uma unidade de mensuração de esforço para a execução de um serviço que envolva prioritariamente esforço humano não mensurável previamente com precisão ou de difícil mensuramento por outras técnicas (qualquer técnica com precisão de mensuração inferior a 90% é candidata a ser substituída pela UST. É bastante utilizada em contratos de prestação de serviços que envolvam diversos tipos de serviços com variada complexidade. O uso de UST na prestação de serviços da área de Engenharia de Software. De acordo com a CGU - Controladoria Geral da União uma UST equivale a uma hora de trabalho.
Firewall	Um firewall (em português: parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, proxy de aplicações, etc. Os firewalls são geralmente associados a redes TCP/IP. Este dispositivo de segurança existe na forma de software e de hardware, a combinação de ambos é chamado tecnicamente de "appliance" . A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.
Filtros de Pacotes	Estes sistemas analisam individualmente os pacotes à medida que estes são transmitidos, verificando apenas o cabeçalho das camadas de rede (camada 3 do modelo ISO/OSI) e de transporte (camada 4 do modelo ISO/OSI).
Proxy Firewall ou Gateways de Aplicação	Os conceitos de gateways de aplicação (application-level gateways) e "bastion hosts" foram introduzidos por Marcus Ranum em 1995. Trabalhando como uma espécie de eclusa, o firewall de proxy trabalha recebendo o fluxo de conexão, tratando as requisições como se fossem uma aplicação e originando um novo pedido sob a responsabilidade do mesmo firewall (non-transparent proxy) para o servidor de destino. A resposta para o pedido é recebida pelo firewall e analisada antes de ser entregue para o solicitante original. Os gateways de aplicações conectam as redes corporativas à Internet através de estações seguras (chamadas de bastion hosts) rodando aplicativos especializados para tratar e filtrar os dados (os proxy firewalls). Estes gateways, ao receberem as requisições de acesso dos usuários e realizarem uma segunda conexão externa para receber estes dados, acabam por esconder a identidade dos usuários nestas requisições externas, oferecendo uma proteção adicional contra a ação dos crackers
Stateful Firewall (ou Firewall de	Com a tecnologia SMLI/Deep Packet Inspection, o firewall utiliza mecanismos otimizados de verificação de tráfego para analisá-los

Estado de Sessão)	sob a perspectiva da tabela de estado de conexões legítimas. Simultaneamente, os pacotes também vão sendo comparados a padrões legítimos de tráfego para identificar possíveis ataques ou anomalias. A combinação permite que novos padrões de tráfegos sejam entendidos como serviços e possam ser adicionados às regras válidas em poucos minutos. Supostamente a manutenção e instalação são mais eficientes (em termos de custo e tempo de execução), pois a solução se concentra no modelo conceitual do TCP/IP. Porém, com o avançar da tecnologia e dos padrões de tráfego da Internet, projetos complexos de firewall para grandes redes de serviço podem ser tão custosos e demorados quanto uma implementação tradicional.
VLANs	Virtual LAN. Uma rede local virtual, normalmente denominada de VLAN, é uma rede logicamente independente. Várias VLANs podem co-existir em um mesmo comutador (switch), de forma a dividir uma rede local (física) em mais de uma rede (virtual), criando domínios de broadcast separados.
Malwares	O que é malware, adware, cavalo de Troia e spyware. O termo malware é proveniente do termo em inglês MALicious software. Trata-se de um software destinado a se infiltrar em um computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não).4 de mai de 2013
Hacker	Hackers são necessariamente programadores habilidosos (mas não necessariamente disciplinados). Muitos são jovens, especialmente estudantes (desde nível médio a pós-graduação). Por dedicarem muito tempo a pesquisa e experimentação, hackers tendem a ter reduzida atividade social e se encaixar no estereótipo do nerd. Suas motivações são muito variadas, incluindo curiosidade, necessidade profissional, vaidade, espírito competitivo, patriotismo, ativismo ou mesmo crime. Hackers que usam seu conhecimento para fins imorais, ilegais ou prejudiciais são chamados crackers.
OpenSource	Open source é um termo em inglês que significa código aberto. Isso diz respeito ao código-fonte de um software, que pode ser adaptado para diferentes fins. O termo foi criado pela OSI (Open Source Initiative) que o utiliza sob um ponto de vista essencialmente técnico.
Hands-on	Expressão comum usada em empresas. Significa primariamente pronta disposição do funcionário para qualquer necessidade da empresa, ou, em outras palavras, pró-atividade. "Hands-on" refere-se, também, à expressão "mão na massa" ou "aprender fazendo". Significa também a passagem de um cargo para outra pessoa. Essa atividade resume-se em transferir as rotinas e conhecimentos necessários para o novo funcionário assumir as tarefas sem causar grandes impactos em processos desenvolvidos e em desenvolvimento. A boa Administração leva a esta prática. É um termo também utilizado em informática para treinamentos que são feitos durante a própria implantação de sistemas, ou seja, o Sistema está sendo instalado os usuários acompanham a implantação e são

	treinados ao mesmo tempo.
TI	Tecnologia da Informação.
Proposta Comercial	Documento apresentado pela LICITANTE contendo todas as informações preliminares a respeito do fornecimento do objeto licitado, incluindo informações técnicas atinentes ao sistema ofertado, preço com, no mínimo, o nível de detalhamento exigido, cronogramas financeiro, prazo de validade, Garantias, Suporte Técnico e Manutenção Evolutiva, e outras informações que a LICITANTE julgar necessário desde que não confrontem o Termo de Referência.
LICITANTE	Empresa participante da Licitação.
Termo de Aceite	Documento emitido pela AGEHAB relatando a aceitação de determinado serviço ou artefato produzido pela empresa CONTRATADA.

ANEXO VIII

MINUTA DO CONTRATO

CONTRATO DE FORNECIMENTO QUE ENTRE SI FAZEM, DE UM LADO, COMO CONTRATANTE, A AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB, E DE OUTRO LADO, COMO CONTRATADA, A EMPRESA …....., EM CONFORMIDADE COM O PROCESSO N° 775/2016 - 201600031000103.

Por este instrumento particular, as partes abaixo mencionadas e qualificadas, acordam entre si firmar o presente Contrato de fornecimento, conforme as cláusulas e condições a seguir elencadas:

1 – Qualificação das Partes
AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB**, sociedade de economia mista, portadora do CNPJ nº 01.274.240/0001-47, com sede na Rua 18-A nº 541, Setor Aeroporto, Goiânia – GO, neste ato representada por seu Presidente **Luiz Antonio Stival Milhomens,** brasileiro, casado, contador, portador da Carteira de Identidade nº 3.358.373 2ª Via SSP/GO e CPF nº 839.954.471-04, residente e domiciliado na cidade de Nova Veneza – Goiás, por seu Diretor Administrativo **Fernando Jorge de Oliveira**, brasileiro, casado, tecnólogo em contabilidade, portador da Carteira de Identidade nº 1792760 SSP-GO e do CPF nº 375.685.581-34, residente e domiciliado nesta Capital e por seu Diretor Financeiro **Hyulley Aquino Machado,** brasileiro, casado, advogado, portador da Carteira de Identidade nº 18481 OAB/GO e do CPF nº 789.352.881-87, residente e domiciliado na cidade de Anápolis – Goiás, doravante designada simplesmente **CONTRATANTE.

*_____, pessoa jurídica de direito privado, situada na _____, _____, inscrita no CNPJ sob o nº _____, neste ato representada por seu representante legal o(a) Sr.(a) _____, brasileiro(a),_____, _____, residente e domiciliado em _____, doravante designada simplesmente **CONTRATADA**.*

DO FUNDAMENTO LEGAL

Este contrato decorre da licitação realizada na modalidade Pregão Eletrônico nº 013/2016, de acordo com a Lei Federal nº 10.520/2002, Lei Federal nº 8.666/1993 e suas alterações posteriores, Lei Estadual nº 17.928/2012, Decreto Estadual nº 7.468/2011, Lei Complementar nº 123, de 14 de dezembro de 2006, e demais normas regulamentares aplicáveis à espécie, conforme termo de Homologação e processo administrativo nº 0775/2016, regendo-o no que for omisso.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por finalidade o fornecimento de APPLIANCE dedicado com subsistemas de FIREWALL STATEFUL, VPN, filtro de URL, FILTRO DE MALWARE, garantia, suporte técnico e serviços de assinatura, conforme descrições contidas no Termo de Referência - ANEXO I e Proposta da Contratada, conforme quadro abaixo:

LOTE 01:

Item	Descrição	Unidade	Quantidade	Preço unitário (R$)	Preço Total (R$)
1	Appliance de Firewall	Un.	01		
2	Treinamento Hands-on	UST.	40		
VALOR TOTAL DA PROPOSTA					

DAS CARACTERÍSTICAS DO APPLIANCE FIREWALL

1.2. As características descritas nesse item será os requisitos mínimos para o produto ofertada;

1.2.1. Deve suportar a definição de VLAN trunking conforme padrão IEEE 802.1q, a criação de interfaces lógicas associadas às VLANs e o estabelecimento de regras de filtragem (Stateful Firewall) entre elas;

1.2.2. Deve suportar agregação de portas, com a criação de grupos de pelo menos 08 (oito) portas. Deve ser suportado o padrão LACP (Link Aggregation Control Protocol);

1.2.3. Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de sequência dos pacotes TCP, status dos flags “ACK”, “SYN” e “FIN”;

1.2.4. Deve permitir a “randomização” do número de sequência TCP, ou seja, funcionar como um “proxy” de número de sequência TCP de modo a garantir que um host situado em uma interface considerada “externa” (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;

1.2.5. Deve possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;

1.2.6. Deve suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos: hosts, redes IP, serviços. Deve ser possível verificar a utilização (“hit counts”) de cada regra de filtragem (“Access Control Entry”) individualmente,

independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos.

1.2.7. Deve possuir a funcionalidade de "proxy" de autenticação ("authentication proxy"), permitindo a criação de políticas de segurança de forma dinâmica, com autenticação e autorização do acesso aos serviços de rede sendo efetuadas por usuário. Deve ser possível obter as informações de usuário/senha por meio de pelo menos os seguintes protocolos: HTTP, HTTPS e Telnet. Deve ser possível ao Firewall exigir autenticação inclusive para uso de protocolos que não possuam nativamente recursos de autenticação;

1.2.8. Deve suportar autenticação usando base local de usuários (interna ao equipamento);

1.2.9. Deve permitir a integração do Firewall com a solução Microsoft Active Directory (MS-AD), permitindo a criação de políticas de filtragem baseados em usuários e grupos de usuários existentes na base MS AD;

1.2.10. Deve implementar listas de controle de acesso com no mínimo os seguintes campos: IP de Origem, Nome do Usuário/Grupo do AD, IP de Destino, Serviço de origem, Serviço de destino e Ação (permit/deny). O "nome de usuário" deverá ser identificado de forma automática e transparente para o usuário final através de consultas à base MS-AD;

1.2.11. Deve implementar políticas de controle de acesso baseadas em informações de horário ("time-based access control");

1.2.12. Deve implementar remontagem virtual de fragmentos ("Virtual Fragment Reassembly") em conjunto com o processo de inspeção stateful. Deve ser possível estabelecer o número máximo de fragmentos por pacotes e timeouts de remontagem;

1.2.13. Deve possuir suporte a inspeção "stateful" para pelo menos os seguintes protocolos de aplicação: Oracle SQL*Net Access, Remote Shell, FTP, HTTP, SMTP, ILS (Internet Locator Service), LDAP, ESMTP, TFTP;

1.2.14. Deve suportar a tradução do endereço IP carregado em uma mensagem DNS Reply (NAT na camada de aplicação) juntamente com a tradução do endereço IP presente no cabeçalho L3;

1.2.15. Deve possuir suporte a inspeção stateful dos protocolos de sinalização de telefonia H.323(v1, v2, v3, v4), SIP (Session Initiation Protocol), MGCP e SCCP. A partir da inspeção dos protocolo de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos;

1.2.16. Deve ser suportada a inspeção do protocolo SIP (SIP over TLS) em ambientes com voz criptografada. A partir da inspeção do protocolo de sinalização, devem ser criadas as conexões pertinentes para o tráfego SRTP (Secure RTP);

1.2.17. Deve possuir capacidade de limitar o número de conexões TCP simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);

1.2.18. Deve possuir capacidade de limitar o número de conexões TCP incompletas ('half-open') simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);

1.2.19. Deve possuir capacidade de limitar o número de conexões TCP simultâneas para um endereço de destino especificado;

1.2.20. Deve possuir capacidade de limitar o número de conexões TCP incompletas ('half-open') simultâneas para um endereço de destino especificado;

1.2.21. Deve permitir simultaneamente com a implementação "Network Address Translation" a filtragem "stateful" de pelo menos as seguintes aplicações:

1.2.21.1. H.323 (v1,v2, v3,v4) , Real Time Streaming Protocol (RTSP), SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol)

1.2.21.2. Microsoft Networking client and server communication (NetBIOS over IP)

1.2.21.3. Oracle SQL*Net client and server communication;

1.2.21.4. Domain Name System (DNS)

1.2.21.5. SUN Remote Procedure Call (RPC);

1.2.21.6. File Transfer Protocol (FTP) – modos "standard" e "passive"

1.3. VIRTUALIZAÇÃO

1.3.1. Deve possuir suporte a tecnologia de Firewall Virtual, com instâncias totalmente isoladas entre si. Dentro de cada instância de Firewall deve ser possível definir regras independentes de filtragem, regras de NAT, rotas e VLANs alocadas;

1.3.2. Dentro de cada instância de Firewall deve ser possível alocar no mínimo os seguintes tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC;

1.3.3. Dentro de cada instância de Firewall deve ser possível limitar (promover "rate limiting") os seguintes recursos: taxa de estabelecimento de novas conexões, taxa de inspeção de aplicações, taxa de transmissão de mensagens Syslog;

1.3.4. A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter influência sobre a operação das demais instâncias;

1.3.5. Deve ser possível selecionar o modo de operação de cada instância de Firewall (seleção, por instância, de modo transparente ou roteado);

1.3.6. Deve ser suportada qualquer combinação de contextos em modo transparente e roteado, dentro do limite de instâncias solicitado.

1.4. SUBSISTEMA VPN

1.4.1. Deve suportar versões do cliente IPSEC VPN fornecido com a appliance para, no mínimo, os seguintes sistemas operacionais: Windows XP, Windows Vista, Windows 7, Linux (Intel) e MacOS;

1.4.2. Deve suportar a terminação túneis IPSEC do tipo "site-to-site" (LAN-to-LAN);

1.4.3. Deve suportar a terminação simultânea de conexões IPSEC VPN;

1.4.4. Deve suporte à criação de VPNs IPSEC com criptografia 168-bit 3DES, 128-bit AES e 256-bit AES;

1.4.5. Deve suportar alta disponibilidade das conexões IPSEC VPN, permitindo a utilização de uma segunda unidade em "standby". Em caso de falha de uma das unidades, não deverá haver perda das conexões ativas (stateful failover) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final;

1.4.6. Deve suportar negociação de túneis VPN IPSEC utilizando o protocolo IKE (Internet Key Exchange) nas versões 1 e 2, para garantir a geração segura das chaves de criptografia simétrica;

1.4.7. Deve suporte à integração com servidores RADIUS, LDAP, Microsoft AD e Kerberos, para tarefas de autenticação, autorização e accounting (AAA) dos usuários VPN;

1.4.8. Deve ser capaz de passar pelo menos os seguintes parâmetros para o cliente: endereço IP do cliente VPN, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name. A configuração do cliente VPN deve ser completamente automatizada, sendo exigida do usuário apenas a instalação do cliente VPN em seu PC;

1.4.9. Deve ser capaz de configurar nos VPN clients uma lista de acesso de "split tunneling", de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta (sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo "all tunneling", em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida;

1.4.10. Deve permitir a criação de "banners" personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN e, em caso de sucesso, mensagens de natureza administrativa;

1.4.11. Deve suportar o uso de certificados digitais emitidos pela autoridade certificadora ICP Brasil para autenticação das VPNs IPSec;

1.4.12. Deve permitir a criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança de forma interna ao equipamento;

1.4.13. Deve permitir a criação de pools de endereços IP de VPN (endereços privados) internamente ao equipamento;

1.4.14. Deve suportar a integração com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes;

1.4.15. Deve permitir que os endereços IP de VPN (endereços privados) sejam obtidos a partir de um servidor DHCP especificado pelo administrador do sistema;

1.4.16. Deve ser possível a associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN;

1.4.17. Deve permitir a definição dos horários do dia e dos dias das semana em que um dado usuário pode requisitar uma conexão VPN;

1.4.18. Deve suportar NAT (Network Address Translation;

1.4.19. Deve suportar operação no modo transparente a NAT ("NAT-transparent mode"), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation);

1.4.20. Deve permitir a terminação de conexões no modo IPSEC over TCP;

1.4.21. Deve permitir a terminação de conexões no modo IPSEC over UDP;

1.4.22. Deve ser possível visualizar no concentrador o número de conexões VPN estabelecidas em um dado instante e os respectivos usuários que estão fazendo uso destas;

1.4.23. Deve ser possível visualizar no cliente VPN o endereço privado adquirido durante a negociação da conexão IPSEC;

1.4.24. Deve ser possível definir vários templates de conexão no cliente VPN antes que seja enviado para instalação no computador do usuário final. Estes templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2 (IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES,AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5 e 7) e tempo de duração ("lifetime") da conexão. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN cliente;

1.4.25. Deve suportar a utilização de certificados digitais padrão X.509 para a própria appliance VPN, possuindo integração com pelo menos as seguintes Certificate Authorities (CAs): Baltimore, Entrust, Verisign, Microsoft e RSA. Os clientes VPNs devem ter o mesmo suporte a certificados digitais. Deve ser suportado o protocolo SCEP para "enrollment" automático na autoridade certificadora (tanto para o concentrador como para os clientes IPSEC);

1.4.26. Deve suportar protocolo Syslog para geração de logs de sistema;

1.4.27. Deve implementar protocolo DTLS (TLS over UDP) de acordo com a RFC 4748;

1.4.28. Deve permitir o mapeamento de atributos LDAP e RADIUS para parâmetros existentes na configuração local de grupos do concentrador. Deve ser possível escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS.

1.5. GERENCIAMENTO E CONECTIVIDADE

1.5.1. Deve implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;

1.5.2. Deve ser gerenciável via SNMP, v2c e v3;

1.5.3. Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS;

1.5.4. Deve ser fornecido com pelo menos uma interface 10/100/1000 dedicada a gerenciamento (out-of-band). Esta interface não deverá ser contabilizada para o atendimento daquelas originalmente especificadas para a appliance firewall;

1.5.5. Deve possuir mecanismo interno de captura de pacotes. Deve ser possível selecionar através de guias de configuração ("wizards") quais os pacotes (IP de origem e destino, portas TCP/UDP de origem e destino e interfaces de entrada devem ser capturados);

1.5.6. Deve permitir o armazenamento de pacotes capturados em formato tcpdump;

1.5.7. Deve possuir memória flash para armazenamento de imagem do sistema operacional e arquivos de configuração do equipamento;

1.5.8. Deve implementar completamente a porção cliente do protocolo TACACS+ para controle de acesso administrativo ao equipamento. Deve ser possível especificar

conjuntos de comandos acessíveis a cada grupo de usuários administrativos e cada comando deve ser autorizado individualmente no servidor TACACS+. Todos os comandos executados bem como todas as tentativas não autorizadas de execução de comandos devem ser enviadas ao servidor TACACS+;

1.5.9. Deve vir acompanhado de interface gráfica para gerenciamento das funcionalidades de VPN e Stateful Firewall relativas ao dispositivo;

1.5.10. Deve implementar, por interface, as funções de DHCP Server, Client e Relay.

1.6. ROTEAMENTO

1.6.1. Deve suportar a criação de rotas estáticas e pelo menos os seguintes protocolos de roteamento dinâmicos: RIP, RIPv2, OSPF, OSPFv3 e BGPv4. Deve suportar a utilização de pelo menos dois processos de roteamento simultâneos e independentes.

1.6.2. Deve implementar o protocolo PIM (Protocol Independent Multicast) em Sparse Mode;

1.6.3. Deve suportar a operação como IGMP Proxy Agent.

1.7. IPv6

1.7.1. Deve suportar inspeção stateful de tráfego IPv6;

1.7.2. Deve suportar simultaneamente a criação de regras IPv4 e IPv6;

1.7.3. Deve suportar roteamento estático;

1.7.4. Deve implementar randomização do número de sequência TCP para conexões TCP que trafegam sobre IPv6;

1.7.5. Deve suportar anti-spoofing (sem uso de ACLs) para endereços IPv6;

1.7.6. Deve suportar gerenciamento sobre IPv6. Devem ser suportados pelo menos os seguintes protocolos de gerência: Telnet, SSH e HTTPS;

1.7.7. Deve suportar stateful failover de conexões IPv6;

1.7.8. Deve suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos.

1.8. ALTA-DISPONIBILIDADE

1.8.1. A solução deverá suportar alta disponibilidade em modo ativo-standby com todas as funcionalidades habilitadas;

1.8.2. Deverá suportar alta disponibilidade em modo cluster, com todas as unidades ativas simultaneamente. O modo cluster deve ser suportado com pelo menos as funcionalidades Stateful Firewall, VPN site-to-site e Next-Generation Firewall/IPS ativas simultaneamente;

1.9. SUBSISTEMA DE FILTRAGEM DE APLICAÇÃO

1.9.1. Deve suportar a identificação e controle de aplicações através de inspeção profunda de pacotes (Deep Packet Inspection), independentemente das portas usadas pela aplicação;

1.9.2. As aplicações devem ser classificadas de acordo com categoria, tipo e nível de risco;

1.9.3. Deve permitir criar regras para monitoramento e controle das aplicações e serviços, sendo capaz de executar no mínimo as seguintes ações:

1.9.4. Permitir o uso irrestrito de uma ou mais aplicações;

1.9.5. Permitir o uso irrestrito de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

1.9.6. Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

1.9.7. Negar totalmente o uso de uma ou mais aplicações independentes do usuário;

1.9.8. Deve suportar o controle de aplicações Web 2.0, definindo quais são as operações permitidas para cada uma destas aplicações (deve ser possível, no mínimo, restringir operações de "Post", bloquear transferência de arquivos, bloquear uso de "games");

1.9.9. Deve ser possível controlar as micro-applicações que podem ser utilizadas por cada uma destas aplicações Web 2.0 (esse tipo de controle deve estar disponível, no mínimo, para as aplicações Facebook, Google+, Twitter e Skype);

1.9.10. Deve permitir a customização de regras de detecção de novas aplicações.

1.10. SUBSISTEMA DE FILTRAGEM DE URL

1.10.1. Deve permitir a criação de regras de controle de acesso com base em informação de reputação dos sites. Essa base deve ser atualizada dinamicamente;

1.10.2. Deve permitir criar políticas de acesso baseadas em filtro de categorias de URL;

1.10.3. Deve ser incluído módulo de filtro de URL integrado na própria ferramenta de Firewall;

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

1.10.5. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, MS Active Directory;

1.10.6. Deverá possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e Grupos de usuários;

1.10.7. Deverá possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.10.8. Deverá incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.10.9. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação;

1.10.10. Deve possibilitar base de URLs local no appliance, evitando delay de comunicação/validação da URLs;

1.10.11. Deverá possuir pelo menos 50 (cinquenta) categorias de URLs;

1.10.12. Deverá possibilitar a criação categorias de URLs customizadas;

1.10.13. Deverá possibilitar a exclusão de URLs do bloqueio por categoria;

1.10.14. Deve possibilitar a customização de página de bloqueio;

1.10.15. Deve possibilitar o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site por um tempo);

1.10.16. Os logs do produto devem incluir informações das atividades dos usuários;

1.10.17. A atualização da base de dados deve ser automática com a opção de ser feita manualmente.

1.11. SUBSISTEMA IPS

1.11.1. Deve permitir a configuração de regras de exceção de inspeção de tráfego por endereço IP origem/destino ou VLAN, por segmento, realizando apenas a comutação do tráfego sem executar inspeção;

1.11.2. Deve realizar a monitoração de segmentos de rede em modo transparente sem endereço IP associado às interfaces de monitoração;

1.11.3. Deve possuir suporte a Jumbo Frame;

1.11.4. Deve monitorar VLANs padrão 802.1q;

1.11.5. Deve suportar o protocolo SNTP ou NTP;

1.11.6. Deve permitir nativamente o uso do SNMP versão 3;

1.11.7. Deve ser capaz de realizar auditoria das atividades de cada usuário;

1.11.8. Deve ser capaz de visualizar no mínimo as seguintes informações:

1.11.8.1. Incidentes de Intrusão;

1.11.8.2. Políticas aplicadas;

1.11.8.3. Atualizações instaladas;

1.11.8.4. Login e logout na interface web de gerencia;

1.11.8.5. Requisições de aumento de privilégio;

1.11.8.6. Inclusões e remoções de regras;

1.11.8.7. Registro de sensores na console de gerenciamento.

1.11.9. Configurações relacionadas ao envio de informações detectada pelos sensores de prevenção contra invasão, para dispositivo de armazenamento externo a solução de gerenciamento;

1.11.10. Deve permitir enviar os logs de auditoria das atividades de cada usuário, para um servidor de Syslogs;

1.11.11. Deve permitir armazenamento dos arquivos de configuração diretamente no appliance;

1.11.12. Deve permitir temporariamente, o armazenamento dos dados coletados e inspecionados em banco de dados local armazenado no sensor de IPS;

1.11.13. Deve permitir inspeção em IP versão 6 incluindo tunelamento IP versão 4 em IP versão 6, IP versão 6 em IP versão 4, IP versão 6 em IP versão 6, IP versão 6 com VLAN e label MPLS;

1.11.14. Deve permitir a inspeção em túneis GRE;

1.11.15. Deve permitir identificar/ restringir o acesso de hosts externos ao perímetro monitorado baseando-se em informações de reputação de domínios de e ranges de endereço IP;

1.11.16. Deve possuir capacidade de criar regras independentes para cada segmento monitorado;

1.11.17. Deve ser capaz de reconstruir e inspecionar fluxos de dados na camada de aplicação;

1.11.18. Deve possuir capacidade de remontagem de fluxo TCP e IP desfragmentation;

1.11.19. Deve possuir capacidade a resistência às ferramentas de evasão;

1.11.20. Deve possuir a capacidade de identificação de protocolos que utilizam portas aleatórias;

1.11.21. Deve detectar e bloquear ataques independente do sistema operacional alvo;

1.11.22. Deve permitir monitoração de sessões de pacotes na rede, atuando em modo "stateful inspection" (análise pacote a pacote e todo o seu estado), sendo capaz de bloquear ataques e tráfego não autorizado ou suspeito;

1.11.23. Deve possuir filtros de "PortScan", protegendo a rede contra ataques do tipo "scan";

1.11.24. Deve possuir filtros de proteção a equipamentos de rede, protegendo contra ataques a vulnerabilidades de equipamentos de rede (ex.: roteadores, switches, etc.);

1.11.25. Deve realizar análise e decodificação de fluxos de pacotes nas camadas 2 à 7 com no mínimo suporte aos seguintes protocolos e aplicações: IP, DNS, H.323, TCP, RPC, MPLS, SIP, ICMP, HTTP, FTP, P2P, ARP, Telnet, SMTP, IM, UDP, IMAP, SMB;

1.11.26. Deve possuir filtros de vulnerabilidades específicos dos protocolos de VoIP que bloqueiem: anomalias de protocolos, ataques de negação de serviço, vulnerabilidades específicas conhecidas, ferramentas de ataque e geradores de tráfego que causem degradação ou indisponibilidade de serviços;

1.11.27. Deve possuir no mínimo as seguintes proteções contra ataques a aplicações Web:

1.11.27.1. Web Protection;

1.11.27.2. Cross-Site Scripting;

1.11.27.3. SQL Injection;

1.11.27.4. Client-side attacks;

1.11.27.5. Injection Attacks;

1.11.27.6. Malicious Files Execution;

1.11.27.7. Information Disclosure;

1.11.27.8. Path Traversal;

1.11.27.9. Authentication;

1.11.27.10. Buffer Overflow;

1.11.27.11. Brute Force;

1.11.27.12. Directory Indexing.

1.11.28. Deve permitir criar regras para filtro com base em endereços de origem/destino, protocolo e VLAN ID;

1.11.29. Deve implementar proteção contra ataques DDoS através dos seguintes métodos:

1.11.29.1. Controle (limite de quantidade) de conexões por origem;

1.11.29.2. Controle (limite de quantidade) de conexões por destino;

1.11.29.3. Controle (limite de quantidade) de requisições “SYN” por origem;

1.11.29.4. Controle (limite de quantidade) de requisições “SYN” por destino;

1.11.29.5. Controle (limite de quantidade) de conexões (origem e Destino) e Controle (limite de quantidade) de requisições “SYN”(Origem e Destino).

1.11.30. Deve possibilitar que os pacotes sejam capturados para análise;

1.11.31. Deve ser capaz de identificar e bloquear ataques baseados em análises de anomalias de tráfego, anomalias de protocolo (RFC Compliance, Protocol Decoders, Normalização), assinaturas e vulnerabilidades;

1.11.32. Deve ser fornecido com uma configuração de filtros recomendados pré-configurados;

1.11.33. Deve permitir a inclusão de informações de vulnerabilidades oriundas de ferramentas de varredura externa (ex.: Nessus, Qualys, Foundstone, etc);

1.11.34. Deve permitir a identificação de anomalia de rede observando o tráfego ou informações do flow de ativos da rede de forma nativa;

1.11.35. Deve permitir a análise do comportamento da rede, com o intuito de detectar ameaças com origem/destino a segmentos monitorados pelo IPS. Isto inclui a capacidade de estabelecer padrões "normais" de tráfego através de técnicas de análise de fluxo (por exemplo, IPfix) e a capacidade de detectar desvios dos padrões considerados normais;

1.11.36. Deve permitir a análise do comportamento da rede fornecendo visibilidade do uso do segmento monitorado para auxiliar na solução de falhas de rede ou degradação de desempenho, no mínimo as seguintes informações devem ser disponibilizadas:

1.11.36.1. Fluxos de sessão dos hosts;

1.11.36.2. Hora de início/fim;

1.11.36.3. Quantidade de dados trafegados.

1.11.37. Deve permitir coletar, armazenar e correlacionar as informações adquiridas passivamente, sobre hosts que trafegam pelos segmentos monitorados pelo(s) IPS. No mínimo as seguintes informações devem ser correlacionadas e armazenadas:

1.11.37.1. Sistema operacional do Host;

1.11.37.2. Serviços existentes no Host;

1.11.37.3. Portas em uso no Host;

1.11.37.4. Aplicações em uso no Host;

1.11.37.5. Vulnerabilidades existentes no Host;

1.11.37.6. Smart phones e tablets;

1.11.37.7. Network flow;

1.11.37.8. Anomalias de redes;

1.11.37.9. Identidades de usuários;

1.11.37.10. Tipo de arquivo e protocolo;

1.11.37.11. Conexões maliciosas.

1.11.38. Deve permitir criar uma lista com o ”ambiente ideal esperado” e a cada mudança nesse ambiente, o sensor deverá no mínimo alertar a console de gerencia sobre a mudança identificada. Entendemos como “ambiente ideal esperado” o conjunto de informações pré-configuradas na gerencia dos sensores de IPS a respeito dos atributos dos hosts participantes desse segmento, deve ser configurado no mínimo os seguintes atributos:

1.11.38.1. Sistema Operacional;

1.11.38.2. Serviços vigentes nos hosts;

1.11.38.3. Aplicações autorizadas a serem executadas nos hosts;

1.11.38.4. Aplicações não autorizadas a serem executadas nos hosts.

1.11.39. Deve permitir criar ou importar regras no padrão OpenSource , essas regras, devem poder ser habilitadas para simples monitoramento ou para bloqueio de tráfego, não deve haver limite da quantidade de regras a serem criadas ou

importadas e não deve haver limite de funcionalidade nas regras criadas ou a serem importadas;

1.11.40. Deve permitir criar regras para monitoramento e controle das aplicações e serviços nos segmentos monitorados, os sensores de IPS devem ser capazes de executar no mínimo as seguintes ações:

1.11.40.1. Permitir o uso irrestrito de uma ou mais aplicações;

1.11.40.2. Permitir o uso irrestrito de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

1.11.40.3. Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

1.11.40.4. Negar totalmente o uso de uma ou mais aplicações independentes do usuário;

1.11.41. Deve possuir capacidade de criar assinaturas definidas pelo usuário com uso de expresses regulares;

1.11.42. Deve possuir capacidade de modificar e alterar as assinaturas existente, podendo a critério do administrador, alterar o modificar o conteúdo da assinatura

1.11.43. Deve ter a capacidade de identificar o tipo de arquivo trafegado e permitir a criação de políticas de detecção e bloqueio de eventos baseados no tipo de arquivo;

1.11.44. A solução deverá detectar e bloquear as seguintes categorias de ataques e ameaças:

1.11.44.1. Malwares;

1.11.44.2. Port Scans;

1.11.44.3. VoIP attacks;

1.11.44.4. IPv6 attacks;

1.11.44.5. DoS attacks;

1.11.44.6. Buffer overflows;

1.11.44.7. P2P attacks;

1.11.44.8. Anomalias em protocolos e aplicações;

1.11.44.9. Ameaças Zero-day;

1.11.44.10. Pacotes malformados;

1.11.44.11. Segmentação TCP e fragmentação IP.

1.11.45. Deve ser fornecido com serviço de atualização permanente de filtros de ataques e vulnerabilidades por 03 anos;

1.11.46. Os equipamentos deverão ser fornecidos com seu software com licença irrestrita, em sua versão mais atual e completa. O fornecimento deverá incluir todas

as licenças de software necessárias para a implementação de todas as funcionalidades disponibilizadas pelo fabricante para os equipamentos fornecido.

1.12. SUBSISTEMA CONTRA MALWARE

1.12.1. Deve prover as funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de command & control, resolução e call-backs;

1.12.2. Deve possui capacidade para monitoração em tempo real;

1.12.3. Deve permitir diariamente, semanalmente ou mensalmente informações a respeito das tendências de ataque e riscos do ambiente;

1.12.4. Deve permitir identificar tráfego de rede gerado por dispositivos conectados no segmento monitorado, incluindo tráfego malware e ataques associados;

1.12.5. Deve oferecer capacidade nativa e sem necessidade de equipamentos tipo SIEM de correlacionar informações de alertas malwares com ataques detectados e condições de tráfego, para assim definir um tipo de alerta personalizado em tempo tempo real;

1.12.6. Deve permitir o controle em tempo real de arquivos;

1.12.7. Deve permitir o bloqueio em tempo real de malwares;

1.12.8. Deve permitir em tempo real o controle e bloqueio de aplicações (protocolos, clientes e web);

1.12.9. Deve permitir o controle de acesso;

1.12.10. Deve permitir o controle de URL's;

1.12.11. Deve suportar em tempo real a detecção e prevenção (bloqueio imediato) de arquivos malwares e ataques para os protocolos HTTP (Inbound e Outbound), SMTP (Inbound e Outbound), FTP (Inbound e Outbound), POP3 (Inbound e Outbound), IMAP (Inbound e Outbound), NETBIOS-SSN (SMB, Inbound e Outbound) e adicionalmente permite em tempo real a detecção (Inbound ou outbound) e prevenção (bloqueio imediato, Inbound ou outbound) de ataques e tráfego malware do tipo: comunicações de comando e controle, identificação de backdoors, propagação de infecção, presença e uso de ferramentas malware, ataques de negação de serviço, comunicação e presença de keyloggers (troca de informações), identificar redirecionamentos, identificar a exploração de overflows;

1.12.12. Deve implementar e identifica existência de Malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Command and Control;

1.12.13. Deve implementar mecanismos de detecção e bloqueio de vazamento de informações sensíveis no ambiente, ao permitir a identificação de dados em: arquivos Microsoft Word (não criptografados) sendo enviados ou recebidos via protocolos FTP e HTTP, números de cartões de crédito para até 8 tipos de protocolos diferentes, endereços e-mail para até 8 tipos de protocolos diferentes e dados customizados pelo administrador para até 8 tipos de protocolos diferentes;

1.12.14. Deve possuir capacidade de Implementar detecção de ataques e malwares que utilizem mecanismo de exploit em arquivos PDF;

1.12.15. Deve implementar capacidade paara detecção de explorações diretas, uso suspeito ou malicioso das seguintes aplicações;

1.12.16. Deve permitir que arquivos executáveis (MSEXE) identificados pelo sensor sejam automaticamente enviados para análise utilizando tecnologia de virtualização em nuvem;

1.12.17. Deve manter um histórico dos resultados de avaliações prévias e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite;

1.12.18. Deve permitir virtualização para análise sobre sistemas operacional Windows;

1.12.19. Deve implementar rede de inteligência global en tiempo real proprietária para cobrir ataques originados de qualquer localidade global, novas origens e destinos de comunicações e distribuição de malwares;

1.12.20. Deve permitir modo de configuração in-line (em linha) totalmente transparente que permita em tempo real a detecção (inbound e/ou outbound) e a prevenção através de bloqueio (inbound e/ou outbound) de ataques malwares sejam estes no formato de arquivos maliciosos, comunicações ou explorações diretas, caso seja necessário a solução suporta a utilização de configurações de proxies;

1.12.21. Deve possuir capacidade de automatica e periódicam para download e instalar atualizações de dados de reputação IP para identificação de tráfego associado a origens e destinos de malware, comando e controle, spam, bots, proxies abertos, relays abertos, phishing e TOR (the onion router);

1.12.22. Deve implementar 02 (dois) modos de operação: detecção passiva e inline sendo que no último a solução deve permitir implementar bloqueios em tempo real e inclusive especificar a terminação das conexões de ataques utilizando pacotes “tcp reset” ao detectar a transferência de arquivos maliciosos, atividade de comunicação, infecção e proliferação de malwares assim como outras categorias de explorações remotas e motivadores de ataques através da rede monitorada pela solução;

1.12.23. Deve implementar funcionalidade de bloqueio em tempo real de arquivos maliciosos (detectados como malwares) e comunicações malwares conhecidas no modo inline;

1.12.24. Deve possuir um recurso de análise tipo “sandbox”, para no mínimo arquivos executáveis (MSEXE) de modo a permitir a análise completa do comportamento do Malware ou código malicioso;

1.12.25. Deve possuir recursos que permitem o envio de informações de eventos de ataques e malwares para ferramentas de SIEM de fabricantes terceiros;

1.12.26. Deve possuir recursos que permitem o envio de informações de eventos de ataques e malwares para servidores Syslog;

1.12.27. Deve implementar suporte a protocolo SNMP v1, v2 e v3 para atividades de gerenciamento;

1.12.28. Deve implementar atualização da base de dados da Rede de Inteligência de forma automático, permitindo o agendamento mínimo de 2 hora de intervalo;

1.12.29. Deve implementar via interface de gráfica de gerenciamento todas as opções de análise e tratamento eventos de ataques de rede, Malware, detecção de tráfego e notificação de eventos em tempo real, adicionalmente implementa automáticamente a capacidade de traçar uma visão cronológica de eventos de forma gráfica permitindo identificar em tempo-real a trajetória de acesso ou propagação de ameaças malware de forma lateral no ambiente, identificando o nome do arquivo, tipo e categoria do arquivo, nível de ameaça quando disponível, sha-256, tipo de evento, protocolo de aplicação utilizado, aplicação cliente utilizada para transferência, quantidade de visualizações, dia e hora, origem e destino do tráfego;

1.12.30. Deve realizar toda detecção e bloqueio de ataques de rede e malwares em tempo real, não sendo uma solução que necessita de ou é exclusivamente dependentes de tecnologia de virtualização tipo "sandboxing" para detecção de arquivos maliciosos e presenção de malware na rede monitorada;

1.12.31. Os processos de detecção e determinação de malwares, ataques e tráfego assim como os bloqueios preventivos inclusive para os arquivos sendo transferidos pela rede pelos protocolos suportados são realizados de forma automatizada e em tempo real;

1.12.32. O recurso de execução em ambiente de virtualização disponibilizado (sandbox), permite a automatização do envio de arquivos suportados pela solução de rede para este tipo de solicitação de análise dinâmica;

1.12.33. A solução Implementa múltiplos motores (engines) para verificação de Malware e/ou códigos maliciosos, não dependendo somente da utilização de recursos de análise virtualizada (sandbox) como método de identificação de malwares em arquivos;

1.12.34. Deve permitir Implementar mecanismo de definição de exceções do tipo whitelist de arquivos, endereços IP, aplicações;

1.12.35. Deve permitir criação de regras de detecção e permitir a criação de detecções de arquivos maliciosos utilizando amostra de arquivo, hash SHA-256 único e lista de hash SHA-256;

1.12.36. Deve permitir Implementar mecanismo de whitelist e detecções customizadas de arquivos, permitindo definição de regras por VLAN, subrede, endereço IP para utilização das listas;

1.12.37. Deve implementar a identificação e capacidade de controle de acesso em tempo real para os seguintes tipos de arquivo:

1.12.37.1. MSEXE,9XHIVE,DMG,DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG_PICT,MAYA,PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN,BINARY_DATA,BINHEX, EICAR, ELF,ISHIELD_MSI, MACHO, RPM, TORRENT, AMR,FFMPEG,FLAC,FLIC,FLV,IVR,MIDI,MKV,MOV,MPEG,OGG,PLS,R1M,REC,RIFF,RIFX,RMF,S3M,SAMI,SMIL,SWF,WAV,WEBM,7Z,ARJ,BZ,CPIO_CRC,CPIO_NEWC,CPIO_ODC,,JAR,LHA,MSCAB,MSSZDD,OLD_TAR,POSIX_TAR,RAR,SIS,SIT,ZIP,ZIP_ENC,ACCDB,HLP,MAIL,MDB,MDI,MNY,MSCHM, MSOLE2,MSWORD_MAC5,MWL,NEW_OFFICE,ONE,PST,RTF,TNEF,WAB,WP,WRI,XLW,XPS.

1.12.38. Deve implementar em tempo real a inspeção, detecção e bloqueio autónomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos:

1.12.38.1. 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC.

1.12.39. A solução ofertada deve ser totalmente do mesmo fabricante

1.12.40. Deve ser fornecido com serviço de atualização permanente por 03 anos;

1.13. ARQUITETURA

1.13.1. Deve ser montável em rack de 19 polegadas (devem ser fornecidos os kits de fixação necessários). O equipamento fornecido deve ocupar no máximo 02 (duas) unidades de rack (02U);

1.13.2. Deve ser fornecido com fonte internas ao equipamento;

1.13.3. Deve ser fornecido com pelo menos 8 (Oito) interfaces 1 Gigabit Ethernet .

1.14. DESEMPENHO

1.14.1. Deve suportar pelo menos 250.000 (Duzentas e cinquenta mil) conexões simultâneas em sua tabela de estados de Stateful Firewall;

1.14.2. Deve suportar a criação de pelo menos 20.000 (Vinte mil) novas conexões TCP por segundo para a funcionalidade de Stateful Firewall;

1.14.3. Deve suportar taxa de encaminhamento de Stateful Firewall de pelo menos 750.000 pps (Setecentos e cinquenta mil pacotes por segundo);

1.14.4. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 1.8 Gbps (Um Gbps e Oitocentos Mbps) para pacotes UDP;

1.14.5. Deve suportar funcionalidade de Stateful Firewall com desempenho mínimo de 900 Mbps (Novecentos Mbps) para pacotes TCP multiprotocolo;

1.14.6. Deve suportar um throughput de, no mínino, 850 Mbps (Oitocentos e Cinquenta Mbps por segundo) com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;

1.14.7. Deve suportar a terminação de pelo menos 50 (Cinquenta) túneis IPSEC VPN simultaneamente. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;

1.14.8. Deve suportar a terminação simultânea de túneis IPSEC, de modo que se suporte um total de pelo menos 300 (Trezentos) usuários VPN, independentemente do tipo de sessão. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;

1.14.9. Deve possuir desempenho de, no mínimo, 250 Mbps (Duzentos e Cinquenta Megabits por segundo) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;

1.14.10. Não deve haver restrição de número de usuários simultâneos através do equipamento para a licença de software fornecida para a funcionalidade de Stateful Firewall;

1.14.11. Deve ser possível criar pelo menos 100 (Cem) interfaces lógicas associadas a VLANs;

1.14.12. Devem ser suportadas, através de licenças adicionais, instâncias virtuais de Firewall, sendo entregue com pelo menos 5(Cinco) instâncias virtuais;

1.14.13. Deve reconhecer mais de 1000 (mil) aplicações com atualizações automáticas;

1.14.14. Deve suportar pelo menos 80 categorias de URL;

1.15. SUBSISTEMA DE GERÊNCIA CENTRALIZADA

1.15.1. Deve ser fornecido na forma de appliance dedicado ou appliance virtual compatível com VMWARE, com licenças e capacidade suficientes para gerenciar a quantidade de dispositivos solicitada;

1.15.2. Deve permitir a instalação, monitoramento, configuração e atualização de múltiplos equipamentos, simultaneamente, estejam estes instalados localmente ou remotamente;

1.15.3. Deverá ser capaz de monitorar, configurar, diagnosticar problemas e gerar relatórios de múltiplos equipamentos;

1.15.4. Deve possuir no mínimo as seguintes opções de resposta automática às ameaças detectadas:

1.15.4.1. Alertas automáticos;

1.15.4.2. Remediações em firewall;

1.15.4.3. Remediações em roteador;

1.15.4.4. Scans de rede;

1.15.5. Deve permitir configurar o perfil de inspeção de tráfego independentemente do segmento associado (físico ou lógico) bem como a direção de inspeção dentro do segmento (somente de entrada, somente de saída ou ambos os sentidos);

1.15.6. Deve permitir aplicar um ou mais perfis de inspeção de tráfego a um segmento ou a um grupo de segmentos;

1.15.7. Deve suportar a aplicação de diversos perfis de inspeção de tráfego, trabalhando de maneira simultânea em diferentes segmentos físicos ou lógicos;

1.15.8. Deve permitir criar políticas de inspeção baseada em grupos, usando os seguintes parâmetros para montagem dos grupos:

1.15.8.1. Sensores;

1.15.8.2. Conjunto de Interfaces de um único equipamento;

1.15.8.3. Conjunto de Interfaces de equipamentos distintos;

1.15.9.

1.15.10. Deve permitir que toda alteração de política e definições na console de gerenciamento seja registrada;

1.15.11. Deve permitir a criação e aplicação de respostas a eventos;

1.15.12. Deve categorizar os eventos de acordo com a severidade;

1.15.13. Deve permitir configurar diferentes perfis de usuários com níveis de privilégios hierárquicos;

1.15.14. Deve possuir capacidade de atualização manual e automática das assinaturas dos subsistemas IPS gerenciados;

1.15.15. Deve permitir a atualização do firmware dos IPSs gerenciados;

1.15.16. Deve coletar passivamente informações de identidade do usuário, para correlacionar o endereçamento IP com o nome de usuário, e tornar esta informação disponível para efeitos de gestão/correlação de eventos;

1.15.17. Deve permitir identificar usuários da rede interna, através de diretório padrão LDAP e correlacioná-los com os eventos de rede, tanto de conformidade com a política de segurança como de intrusão, sem necessidade de solução externa;

1.15.18. A análise de comportamento de rede deve permitir correlacionar os nomes de usuários com eventos de segurança suspeitos;

1.15.19. Deve permitir monitorar as condições de "saúde" dos subsistemas IPS monitorados, apresentando informações em sua console gráfica de no mínimo seguintes informações:

1.15.19.1.

1.15.19.2. Heartbeat dos subsistemas IPS, permitindo monitorar se os equipamentos gerenciados estão operantes;

1.15.19.3. Uso da CPU- Deve permitir monitorar o uso da CPU, deve ser possível definir no dois tipos diferentes de alertas, para diferentes níveis de uso da CPU;

1.15.19.4. Reset da interfaces - Deve permitir monitorar o reset nas interfaces de inspeção dos subsistemas IPS;

1.15.19.5. Uso de Disco- Deve permitir monitorar o uso do Disco, deve ser possível definir nos dois tipos diferentes de alertas, para diferentes níveis de uso do Disco;

1.15.19.6. Taxa de eventos de IPS- Deve permitir monitorar a taxa de eventos de IPS recebida por segundo, deve ser possível definir nos dois tipos diferentes de alertas, para diferentes níveis de eventos de IPS recebidos por segundo;

1.15.19.7. Uso de Memória - Deve permitir monitorar o uso da memória do appliance, deve ser possível definir nos dois tipos diferentes de alertas, para diferentes níveis de uso de memória;

1.15.19.8. Sincronização de tempo – Monitoramento da diferença de tempo de dispositivos gerenciados;

1.15.19.9. Traffic Status - Deve permitir monitorar se as interfaces de inspeção dos sensores de IPS estão recebendo tráfego.

1.15.20. Deve gerar gráficos em tempo real das estatísticas do tráfego, ataques filtrados, hosts de rede e serviços;

1.15.21. Deve ser gerenciado através de interface WEB segura (HTTPS) e toda a comunicação entre dispositivo de gerencia e sensor de IPS deve ser criptografada;

1.15.22. Deve possuir recurso de geolocalização. Localização geográfica da máquina do atacante;

1.15.23. Deve permitir criar no mínimo os relatórios descritos abaixo:

1.15.23.1. Relatórios dos 10 ataques mais comuns;

1.15.23.2. IP de Origem;

1.15.23.3. IP de Destino;

1.15.23.4. Ataques por severidade;

1.15.23.5. Ataques por ação, por porta, por segmento, por protocol;

1.15.23.6. Ataques por endereço IP de Destino, endereço IP de Origem.

1.15.24. Deve permitir gerar relatórios gráficos, permitindo a geração de relatórios periódicos de forma automática. A solução deverá permitir também o envio automático dos relatórios para e-mail escolhido pelo administrador da solução;

1.15.25. Deve exportar relatórios para no mínimo os seguintes formatos: HTML, PDF e CSV;

1.15.26. Deve possuir ferramenta interna de manutenção do banco de dados, capaz de realizar no mínimo as seguintes funções:

1.15.26.1. Backup Manual dos dados e das configurações do sistema de gerenciamento;

1.15.26.2. Backup agendado dos dados e das configurações do sistema de gerenciamento;

1.15.26.3. Armazenar no disco local do sistema de gerenciamento o backup dos sensores e sistema de gerenciamento.

1.15.26.4. Assim que o backup for concluído o sistema de gerenciamento deve ser capaz de copiar através de protocolo de comunicação criptografado (nativo do equipamento) e sem intervenção humana o Backup realizado para um host diferente;

1.15.27. Deve possuir banco de dados interno para armazenamento dos logs, permitindo ao administrador da solução que redirecione o armazenamento dessa base de dados em um volume de disco remoto;

1.15.28. Deve manter os logs de ataques e de alarmes enviados pelos subsistemas IPS;

1.15.29. Deve permitir enviar as informações para um Syslog remoto;

1.15.30. Deve ser gerenciável via linha de comando através de acesso seguro utilizando o protocolo SSH;

1.15.31. Deve implementar nativamente (sem uso de ferramentas de terceiros) SNMPv3;

1.15.32. Deve permitir envio de eventos SNMP relativos ao desempenho e funcionamento do equipamento;

1.15.33. Deve implementar NTP ou SNTP.

CLÁUSULA SEGUNDA - DO TREINAMENTO

2.1. O treinamento será Hands-on (mão na massa), treinamento feito durante a própria implantação do sistema/ appliance, ou seja, o Sistema/ appliance está sendo instalado, os técnicos da AGEHAB acompanham a implantação e são treinados ao mesmo tempo. Essa atividade resume-se em transferir as rotinas e conhecimentos necessários para a equipe técnica da CONTRATANTE.

2.2. O treinamento deverá ser de responsabilidade da CONTRATADA com carga horária suficiente para capacitar, de forma adequada, os 02 (dois) técnicos da CONTRATANTE.

2.3. A CONTRATADA deve disponibilizar profissional certificado pelo fabricante da solução ofertada para realizar o treinamento junto a CONTRATANTE.

2.4. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento, hospedagem, alimentação, o fornecimento do material didático em língua portuguesa.

2.5. O treinamento Hands-on deverá ser marcado com a Gerência de Tecnologia da Informação com antecedência mínima de 03 (três) dias antes da data do treinamento.

2.6. Para efeito de cálculo e orientação da CGU (Controladoria Geral da União) será utilizada a unidade UST (Unidade de Serviço Técnico) que equivale a uma hora de trabalho.

CLÁUSULA TERCEIRA – DA GARANTIA, SUPORTE E SERVIÇOS DE ASSINATURA

3.1. Todos os itens deveram seguir os padrões abaixo. Os serviços de garantia, suporte técnico e serviços de assinaturas deverão ser fornecidos pelo fabricante do equipamento.

3.2. O serviço de suporte técnico durante o período de garantia de 36 (trinta e seis) meses atendendo as seguintes exigências:

3.2.1. O serviço de suporte técnico deverá ser 24x7x4 (vinte e quatro horas por dia, sete dias por semana, quatro horas de tempo de resposta), no local onde a solução se encontrar instalada (on-site), por técnicos devidamente habilitados e credenciados pelo fabricante, e sem qualquer ônus adicional;

3.2.2. O fabricante deverá disponibilizar canal de atendimento para abertura de chamados técnicos 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante número 0800 ou número local em Brasília;

3.2.3. Para cada chamado técnico, deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas;

3.2.4. Todos os serviços baseados em assinaturas devem estar disponíveis por, no mínimo, 36 (trinta e seis) meses.

CLÁUSULA QUARTA – DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

4.1. Todos os itens deverão seguir os padrões de prazo, local de entrega e forma de recebimento descritos abaixo:

4.1.1. Os equipamentos deverão ser entregues até 60 (sessenta) dias a contar da assinatura do contrato ou instrumento equivalente, na sede da Agência Goiana de Habitação S/A Rua 18 A nº 541, Setor Aeroporto, Goiânia-GO, CEP 74070-060;

4.1.2. A CONTRATANTE determinará o local para entrega e verificará todas as condições e especificações, em conformidade com o Termo de Referência;

4.1.3. Entende-se por entrega as seguintes atividades: o transporte dos produtos embalados para o local determinado pela CONTRATANTE, a entrega dos volumes, a desembalagem, a verificação visual do produto e sua reembalagem se for o caso;

4.1.4. Os equipamentos deverão ser novos e sem uso e deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

4.1.5. No ato da entrega, a gerência responsável emitirá TERMO DE RECEBIMENTO PROVISÓRIO relacionando todos os produtos recebidos, nos termos da Nota Fiscal;

4.1.6. Os produtos serão objeto de inspeção, que será realizada por pessoa designada pela gerência responsável, conforme procedimentos a seguir:

4.1.6.1. Abertura das embalagens;

4.1.6.2. Comprovação de que o produto atende às especificações mínimas exigidas e/ou aquelas superiores oferecidas pela CONTRATADA;

4.1.6.3. Colocação do produto em funcionamento, se for o caso;

4.1.6.4. Teste dos componentes se for o caso;

4.1.6.5. O período de inspeção será de até 10 (dez) dias úteis;

4.1.7. Nos casos de sinais externos de avaria de transporte ou de mau funcionamento do produto, verificados na inspeção do mesmo, este deverá ser substituído por outro com as mesmas características, no prazo de até 30 (trinta) dias corridos, a contar da data de realização da inspeção;

4.1.8. Findo o prazo de inspeção e comprovada a conformidade dos produtos com as especificações técnicas exigidas no Edital e aquelas oferecidas pela CONTRATADA, a gerência responsável emitirá o TERMO DE RECEBIMENTO DEFINITIVO;

4.1.9. Nos casos de substituição do produto, iniciar-se-ão os prazos e procedimentos estabelecidos nestas CONDIÇÕES DE RECEBIMENTO

4.1.10. Correrão por conta da CONTRATADA as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos.

CLÁUSULA QUINTA – DA FISCALIZAÇÃO DO CONTRATO

5.1. Será gestor deste contrato o empregado Sr/Srª _____, conforme portaria nº _____. Este ficará responsável pelo acompanhamento da execução bem como pela fiscalização do presente instrumento, por meio de relatórios, inspeções, visitas, atestado da satisfatória realização do objeto e outros procedimentos que julgar

necessário.

CLÁUSULA SEXTA – DO VALOR E DA FORMA DE PAGAMENTO

6.1. O valor global do presente contrato é de R$ _____(_____).

6.2. O pagamento será procedido mediante a apresentação da Nota Fiscal/Fatura, que deverá ser eletrônica em original ou a primeira via e original atestada, com a data e contendo a identificação do gestor que a atestou, após o fechamento do mês e a sua quitação será até o décimo dia útil do mês seguinte.

6.3. As notas(s) fiscal(is)/faturas deverão conter no mínimo os seguintes dados:
a) Data de emissão;
b) Estar endereçada a Agência Goiana de Habitação – AGEHAB, situada a Rua 18-nº 541, Setor Aeroporto, Goiânia/GO, CNPJ nº01. 274.240/0001-47;
c) Preços unitários.

6.4. O pagamento será efetuado após ateste da autoridade competente assim como das respectivas requisições da AGEHAB, desde que a Certidão Negativa de Débito – CND, o Certificado de Regularidade do FGTS – CRF, a prova de regularidade para com a Fazenda Federal e Municipal.

6.5. Na ocorrência da rejeição de nota fiscal/fatura, motivada por erro ou incorreções, o prazo estipulado no subitem 6.2. passará a ser contado a partir da data da sua reapresentação, examinadas as causas da recusa.

6.6. No caso de serviços de prestação de mão de obra na sede da AGEHAB, apresentar nas solicitações de pagamentos mensais os seguintes documentos:
a) Cópias autenticadas, legíveis e pagas das guias de recolhimento ao INSS e ao FGTS, juntamente com a relação da SEFIP dos funcionários que estiveram prestando serviços para a contratante, referente ao mês anterior ao do pagamento;
b) Cópia autenticada, legível da Folha de pagamento ou dos contracheques devidamente quitados pela contratada e assinados pelos empregados dela, executores dos serviços na AGEHAB, referente ao mês anterior ao do pagamento.

CLÁUSULA SÉTIMA – DO PRAZO DE VIGÊNCIA

7.1. O contrato terá um prazo de 12 (doze meses) meses.

CLÁUSULA OITAVA– DOS RECURSOS FINANCEIROS

8.1. As despesas decorrentes do presente contrato correrão à conta de **Recursos do Convênio 003/2015, firmado entre a AGEHAB e a Secretaria de Estado de Meio Ambiente, Recursos Hídricos, Infraestrutura, Cidades e Assuntos Metropolitanos - SECIMA, conforme Plano de Trabalho, Ação 2, Atividade "C".**

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA

9.1. Além das resultantes da Lei 8.666/93 a adjudicatária se obriga, nos termos do Termo de Referência, a:

9.1.1. Prestar todos os esclarecimentos que forem solicitados pela fiscalização da contratante;

9.1.2. Manter durante toda a execução do termo respectivo, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;

9.2. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

9.3. Manter atualizados, durante a vigência do contrato, para fins de pagamento, a Certidão Negativa de Débito – CND de Débito Trabalhista-CNDT, o Certificado de Regularidade - CRF do FGTS e certidão de regularidade junto à Fazenda Federal e municipal;

9.4. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado no Termo de Referência.

9.5. Efetuar treinamento para operacionalização e implantação do appliance de firewall e seus subsistemas, para equipe técnica da AGEHAB;

9.6. **São expressamente vedadas à CONTRATADA**:

9.6.1. A ceder, sob qualquer forma, os créditos oriundos deste contrato a terceiros;

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE

10.1. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da contratada ou por seu preposto;

10.2. Fornecer de toda a infraestrutura necessária para instalação e funcionamento dos equipamentos, como local físico, tomadas elétricas, pontos de acesso à rede, etc.

10.3. Efetuar o pagamento conforme execução dos serviços, desde que cumpridas todas as formalidades e exigências do contrato;

10.4. Exercer a fiscalização do contrato;

10.5. Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato;

10.6. Convocar reunião inicial, quando necessário, com todos os envolvidos na contratação; e acompanhar e monitorar toda a execução dos serviços.

CLÁUSULA DECIMA PRIMEIRA – DAS PENALIDADES E MULTAS

11.1. Pela inexecução contratual, atraso injustificado na execução do contrato, sujeitará a Contratada, além das cominações legais cabíveis, à multa de mora, graduada de acordo com a gravidade da infração, obedecida os seguintes limites máximos:

1) 10% (dez por cento) sobre o valor do contrato em caso de descumprimento total da obrigação;

a) Multa de até 0,1% (um décimo por cento) por semana de atraso, calculado sobre a respectiva etapa do serviço de implantação;

b) No caso de atraso superior a 90 (noventa) dias, será aplicada penalidade adicional de até (um por cento) sobre a respectiva etapa do serviço de implantação, por mês, até o limite de 10 (dez) meses;

c) No caso do não cumprimento ou cumprimento irregular dos serviços de Manutenção e Evolução Tecnológica dos Softwares ERPI; Suporte Técnico das Soluções Implementadas ERP; Treinamento nos softwares ERP será aplicada multa de até 0,2% (dois décimos por cento) sobre o valor total do Contrato, por dia de atraso, até o limite de 5% (cinco por cento);

2) 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;

3) 0,7% (sete décimos por cento) sobre o valor do fornecimento não realizado, por cada dia subseqüente ao trigésimo.

4) suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração Pública, por prazo não superior a 05 (cinco) anos;

5) declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

11.2. A multa será descontada dos pagamentos eventualmente devidos, ou ainda, quando for o caso, cobrada judicialmente.

11.3. Qualquer das penalidades aqui previstas e aplicadas será registrada junto ao CADFOR.

CLÁUSULA DECIMA SEGUNDA – DA RESCISÃO

12.1. A rescisão do presente contrato poderá ser:

12.1.1. Determinada por ato motivado da Administração, após processo regular, assegurado o contraditório e a ampla defesa, nos casos do artigo 78, incisos I a XII, XVII e parágrafo único e inciso XVIII, da Lei Federal n° 8.666 de 21/06/1993.

12.1.2. Amigável, por acordo entre as partes, reduzida a termo, desde que haja conveniência para a Contratante.

12.1.3. Judicial, nos termos da legislação.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES GERAIS

13.1. O presente contrato reger-se-á pelas suas cláusulas e normas consubstanciadas na Lei Federal n° 8.666/93.

13.2. Fica declarado competente o foro da Comarca de Goiânia, para dirimir quaisquer dúvidas referentes a este contrato.

13.3. Os casos omissos serão resolvidos de acordo com a Lei nº 8.666/93, e demais normas aplicáveis.

E por estarem justos e contratados, os representantes das partes assinam o presente instrumento, na presença de testemunhas conforme abaixo, em 03(três) vias de igual teor e forma, para um só efeito.

Goiânia,_____ de _____ de 2016.

LUIZ ANTONIO STIVAL MILHOMENS
Presidente

FERNANDO JORGE DE OLIVEIRA
Diretor Administrativo

HYULLEY AQUINO MACHADO
Diretor Financeiro

_____
Representante Legal
Contratada

Testemunhas:

1 - _____
CPF:_____

2 - _____
CPF: _____

ANEXO IX

Declaração de Inexistência de Sócios comuns, endereços coincidentes e/ou indícios de parentesco

À CPL/AGEHAB

Ref.: **Pregão Eletrônico nº 013/2016**

_____(RAZÃO SOCIAL DA LICITANTE), _____(CNPJ Nº), sediada no (a)_____ (ENDEREÇO COMPLETO), **DECLARA**, sob as penas da lei, que cumpre, plenamente, os requisitos exigidos no procedimento licitatório referenciado.

Igualmente, **DECLARA** sob as penas da lei, em especial para atender à orientação do TCU – Acórdão 2136/2006/TCU/1ª Câmara, de 01/08/2006, ata nº 27/2006, que nossa Empresa não possui sócios em comum, endereços idênticos e/ou indícios de parentesco, com as demais licitantes presentes, ou das que se fazem representar no momento do credenciamento.

Finalizando, declaramos que temos pleno conhecimento de todos os aspectos relativos à licitação em causa e nossa plena concordância com as condições estabelecidas no Edital da licitação e seus anexos.

Local e Data

Atenciosamente,

_____

FIRMA LICITANTE/CNPJ

ASSINATURA DO REPRESENTANTE LEGAL