EDITAL DE PREGÃO ELETRÔNICO OBJETIVANDO A PRESTAÇÃO DE SERVIÇOS CONTÍNUOS CONTRATADOS SOB O REGIME DE EMPREITADA POR PREÇO GLOBAL.

PREÂMBULO

EDITAL DE PREGÃO ELETRÔNICO n° 19/16

PROCESSO n° FP 462/16

OFERTA DE COMPRA nº 171101170462016OC00170

ENDEREÇO ELETRÔNICO: www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br

DATA DO INÍCIO DO PRAZO PARA ENVIO DA PROPOSTA ELETRÔNICA: 16/11/2016

DATA E HORA DA ABERTURA DA SESSÃO PÚBLICA: 28/11/2016 – 9:00 HS

O Sr. **MARCELLO GONELLA DE ANDRADE**, Diretor Adjunto de Administração e Finanças, usando a competência delegada pelos artigos 3° e 7°, inciso I, do Decreto estadual nº 47.297, de 06 de novembro de 2002, c.c. artigo 8°, do Decreto estadual nº 49.722, de 24 de junho de 2005, torna público que se acha aberta, nesta unidade, licitação na modalidade PREGÃO, a ser realizada por intermédio do sistema eletrônico de contratações denominado "Bolsa Eletrônica de Compras do Governo do Estado de São Paulo – Sistema BEC/SP", com utilização de recursos de tecnologia da informação, denominada **PREGÃO ELETRÔNICO, do tipo MENOR PREÇO** – Processo FP 462/16 objetivando a **EXECUÇÃO DE SERVIÇOS de CONTROLE E ACESSO DE REDE - FIREWALL**, sob o regime de empreitada por preço global, que será regida pela Lei federal nº. 10.520, de 17 de julho de 2002, pelo Decreto n° 49.722, de 24 de junho de 2005, pelo regulamento anexo à Resolução n° CC27, de 25/05/2006, aplicando-se, subsidiariamente, no que couberem, as disposições da Lei federal nº 8.666, de 21 de junho de 1993, da Lei estadual nº 6.544, de 22 de novembro de 1989, do Decreto estadual n° 47.297, de 06 de novembro de 2002, da Resolução CEGP-10, de 19 de novembro de 2002, e demais normas regulamentares aplicáveis à espécie.

As propostas deverão obedecer às especificações deste instrumento convocatório e seus anexos e serão encaminhadas por meio eletrônico, após o registro dos interessados em participar do certame e o credenciamento de seus representantes no Cadastro Unificado de Fornecedores do Estado de São Paulo – CAUFESP.

A sessão pública de processamento do Pregão Eletrônico será realizada no endereço eletrônico www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br, no dia e hora mencionados no preâmbulo deste Edital e será conduzida pelo pregoeiro com o auxílio da equipe de apoio, designados nos autos do processo em epígrafe e indicados no sistema pela autoridade competente.

I. DO OBJETO

1. A presente licitação tem por objeto a contratação de serviços de **CONTROLE E ACESSO DE REDE – FIREWALL,** conforme especificações constantes do **MEMORIAL DESCRITIVO** que integra este edital como Anexo I.

II. DA PARTICIPAÇÃO

1. Poderão participar do certame todos os interessados em contratar com a Administração Estadual que estiverem registrados no CAUFESP, em atividade econômica compatível com o seu objeto, sejam detentores de senha para participar de procedimentos eletrônicos e tenham credenciado os seus representantes, na forma estabelecida no regulamento que disciplina a inscrição no referido Cadastro.

1.1. O registro no CAUFESP, o credenciamento dos representantes que atuarão em nome da licitante no sistema de pregão eletrônico e a senha de acesso, deverão ser obtidos anteriormente à abertura da sessão pública e autorizam a participação em qualquer pregão eletrônico realizado por intermédio do Sistema BEC/SP.

1.2. As informações a respeito das condições exigidas e dos procedimentos a serem cumpridos, para o registro no CAUFESP, para o credenciamento de representantes e para a obtenção de senha de acesso, estão disponíveis no endereço eletrônico www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br.

2. A participação no certame está condicionada, ainda, a que o interessado ao acessar, inicialmente, o ambiente eletrônico de contratações do Sistema BEC/SP, declare, mediante assinalação nos campos próprios, que inexiste qualquer fato impeditivo de sua participação no certame ou de sua contratação, que conhece e aceita os regulamentos do Sistema BEC/SP, relativos à Dispensa de Licitação, Convite e Pregão Eletrônico.

3. A licitante responde integralmente por todos os atos praticados no pregão eletrônico, por seus representantes devidamente credenciados, assim como pela utilização da senha de acesso ao sistema, ainda que indevidamente, inclusive por pessoa não credenciada como sua representante.

4. Cada representante credenciado poderá representar apenas uma licitante, em cada pregão eletrônico.

5. O envio da proposta vinculará a licitante ao cumprimento de todas as condições e obrigações inerentes ao certame.

6. Para o exercício do direito de preferência de que trata o subitem 6, bem como para a fruição do benefício da habilitação com irregularidade fiscal previsto na alínea “f”, do subitem 9, ambos do item V deste edital, a condição de microempresa ou de empresa de pequeno porte, ou de cooperativa que preencha as condições estabelecidas no artigo 34, da Lei federal nº 11.488, de 15/06/2007, deverá constar do registro da licitante junto ao CAUFESP.

III - DAS PROPOSTAS

1. As propostas deverão ser enviadas por meio eletrônico disponível no endereço www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br na opção PREGAO–ENTREGAR PROPOSTA, desde a divulgação da íntegra do edital no referido endereço eletrônico, até o dia e horário previstos no preâmbulo para a abertura da sessão pública, devendo a licitante, para

formulá-las, assinalar a declaração de que cumpre integralmente os requisitos de habilitação constantes do edital.

2. Os preços unitário e total para a prestação dos serviços serão ofertados no formulário eletrônico próprio, em moeda corrente nacional, em algarismos, apurados nos termos do subitem 4 deste item III, sem inclusão de qualquer encargo financeiro ou previsão inflacionária. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas e custos, como por exemplo: transportes, tributos de qualquer natureza e todas as despesas, diretas ou indiretas, relacionadas com a prestação de serviços objeto da presente licitação.

2.1. Proposta apresentada por cooperativa de trabalho deverá ser com posta pelo valor do serviço + valor dos insumos.

3. O prazo de validade da proposta será de 60 (sessenta) dias.

4. A proposta de preço deverá ser orçada em valores vigentes à data de sua apresentação, que será considerada a data de referência de preços.

IV- DA HABILITAÇÃO

1. O julgamento da habilitação se processará na forma prevista no subitem 9, do item V, deste Edital, mediante o exame dos documentos a seguir relacionados, os quais dizem respeito a:

1.1. HABILITAÇÃO JURÍDICA

a) Registro empresarial na Junta Comercial, no caso de empresário individual (ou *cédula de identidade em se tratando de pessoa física não empresária*);

b) **Ato constitutivo, estatuto ou contrato social atualizado e registrado na Junta Comercial**, em se tratando de sociedade empresária ou cooperativa;

c) Documentos de eleição ou designação dos atuais administradores, tratando-se de sociedades empresárias ou cooperativas;

d) Ato constitutivo atualizado e registrado no Registro Civil de Pessoas Jurídicas tratando-se de sociedade não empresária, acompanhado de prova da diretoria em exercício;

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

1.2 - REGULARIDADE FISCAL E TRABALHISTA

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ) ou no Cadastro de Pessoas Físicas (CPF);

b) Prova de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, relativo à sede ou ao domicílio da licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

c) Certidão de regularidade de débito com as Fazendas Estadual e Municipal, da sede ou do domicílio da licitante;

d) Certidão de regularidade de débito para com o Sistema de Seguridade Social (INSS) e o Fundo de Garantia por Tempo de Serviço (FGTS);

e) Certidão Conjunta Negativa de Débitos ou Positiva com efeitos de Negativa, relativa a tributos federais e dívida ativa da União.

1.3 - QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão negativa de falência, concordata, recuperação judicial e extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida pelo distribuidor do domicílio da pessoa física;

a.1) Se a licitante for cooperativa, a certidão mencionada na alínea “a”, deste subitem 1.3, deverá ser substituída por certidão negativa de ações de insolvência civil.

1.4 - QUALIFICAÇÃO TÉCNICA

a) Atestado de Capacidade Técnica, em nome da LICITANTE, expedido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de equipamentos similares aos ofertados serviços de instalação, configuração e suporte técnico, devendo estar explicita a marca, modelos e as quantidades fornecidas, devidamente registrados nas entidades profissionais competentes.

b) Declaração do Fabricante informando que a LICITANTE está autorizada a comercializar, instalar, configurar e prestar suporte técnico na solução ofertada – A SER FORNECIDA APENAS PELO LICITANTE VENCEDOR NO MOMENTO DA ASSINATURA DO CONTRATO.

1.5 - OUTRAS COMPROVAÇÕES

1.5.1 - Declarações subscritas por representante legal da licitante, elaboradas em papel timbrado, atestando que:

a) se encontra em situação regular perante o Ministério do Trabalho, conforme modelo anexo ao Decreto estadual nº 42.911, de 06/03/1998;

b) inexiste impedimento legal para licitar ou contratar com a Administração, inclusive em virtude das disposições da Lei estadual n° 10.218, de 12 de fevereiro de 1999;

c) atende às normas relativas à saúde e segurança do trabalho (parágrafo único, art. 117, Constituição do Estado).

d) informando que o produto que oferta atende a todas as características e funcionalidades exigidas e contidas neste edital e que possui técnicos certificados pelo Fabricante da solução para comprovar qualificação para execução do serviço.

e) Certidão expedida pela entidade estadual da organização das Cooperativas Brasileiras para as sociedades cooperativas nos termos do artigo 107 da Lei Federal 5764/71.

2 – DISPOSIÇÕES GERAIS

2.1. Na hipótese de não constar prazo de validade nas certidões apresentadas, a Administração aceitará como válidas as expedidas até 180 (cento e oitenta) dias imediatamente anteriores à data de apresentação das propostas.

V – DA SESSÃO PÚBLICA E DO JULGAMENTO

1. No dia e horário previstos neste edital, o Pregoeiro dará início à sessão pública do pregão eletrônico, com a abertura automática das propostas e a sua divulgação, pelo sistema, na forma de grade ordenatória, em ordem crescente de preços.

2. A análise das propostas pelo Pregoeiro visará ao atendimento das condições estabelecidas neste Edital e seus anexos.

2.1. Serão desclassificadas as propostas:

a) cujo objeto não atenda as especificações, prazos e condições fixados no Edital;

b) que apresentem preço baseado exclusivamente em proposta das demais licitantes.

c) que por ação da licitante ofertante contenham elementos que permitam a sua identificação.

2.1.1. A desclassificação se dará por decisão motivada do Pregoeiro.

2.2. Serão desconsideradas ofertas ou vantagens baseadas nas propostas das demais licitantes.

2.3. O eventual desempate de propostas do mesmo valor será promovido pelo sistema, com observância dos critérios legais estabelecidos para tanto.

3. Nova grade ordenatória será divulgada pelo sistema, contendo a relação das propostas classificadas e das desclassificadas.

4. Será iniciada a etapa de lances, com a participação de todas as licitantes detentoras de propostas classificadas.

4.1. A formulação de lances será efetuada, exclusivamente, por meio do sistema eletrônico.

4.1.1. Os lances deverão ser formulados em valores distintos e decrescentes, inferiores à proposta de menor preço, ou em valores distintos e decrescentes inferiores ao do último valor apresentado pela própria licitante ofertante, observada, em ambos os casos, a redução mínima entre eles de R$ 200,00 (duzentos reais), aplicável, inclusive, em relação ao primeiro formulado, prevalecendo o primeiro lance recebido, quando ocorrerem 2 (dois) ou mais lances do mesmo valor.

4.1.1.1. **A aplicação do valor de redução mínima entre os lances incidirá sobre o preço TOTAL (2 UNIDADES DE FIREWALL + INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA + ATUALIZAÇÕES E SUPORTE + TREINAMENTO/4 PESSOAS)**

4.2. A etapa de lances terá a duração de 15 (quinze) minutos.

4.2.1. A duração da etapa de lances será prorrogada automaticamente pelo sistema, visando à continuidade da disputa, quando houver lance admissível ofertado nos últimos 3 (três) minutos do período de que trata o subitem 4.2 ou nos sucessivos períodos de prorrogação automática.

4.2.1.1. Não havendo novos lances ofertados nas condições estabelecidas no subitem 4.2.1, a duração da prorrogação encerrar-se-á, automaticamente, quando atingido o terceiro minuto contado a partir do registro no sistema, do último lance que ensejar prorrogação.

4.3. No decorrer da etapa de lances, as licitantes serão informadas pelo sistema eletrônico:

a) dos lances admitidos e dos inválidos, horários de seus registros no sistema e respectivos valores;

b) do tempo restante para o encerramento da etapa de lances.

4.4. A etapa de lances será considerada encerrada findos os períodos de duração indicados no subitem 4.2.

5. Encerrada a etapa de lances, o sistema divulgará a nova grade ordenatória, contendo a classificação final, em ordem crescente de valores.

5.1. Para essa classificação será considerado o último preço admitido de cada licitante.

6. Com base na classificação a que alude o subitem 5 deste item, será assegurada às licitantes microempresas, empresas de pequeno porte e cooperativas que preencham as condições estabelecidas no artigo 34, da Lei federal nº 11.488, de 15/06/2007, preferência à contratação, observadas as seguintes regras:

6.1. - A microempresa, empresa de pequeno porte, ou cooperativa que preencha as condições estabelecidas no artigo 34, da Lei federal nº 11.488, de 15/06/2007, detentora da proposta de menor valor, dentre aquelas cujos valores sejam iguais ou superiores até 5% (cinco por cento) ao valor da proposta melhor classificada, será convocada pelo pregoeiro, para que apresente preço inferior ao da melhor classificada, no prazo de 5 (cinco) minutos, sob pena de preclusão do direito de preferência.

6.1.1 - A convocação recairá sobre a licitante vencedora de sorteio, no caso de haver propostas empatadas, nas condições do subitem 6.1.

6.2. - Não havendo a apresentação de novo preço, inferior ao preço da proposta melhor classificada, serão convocadas para o exercício do direito de preferência, respeitada a ordem de classificação, as demais microempresas, empresas de pequeno porte, e cooperativas que preencham as condições estabelecidas no artigo 34, da Lei federal nº 11.488, de 15/06/2007, cujos valores das propostas se enquadrem nas condições indicadas no subitem 6.1.

6.3. - Caso a detentora da melhor oferta, de acordo com a classificação de que trata o subitem 5, seja microempresa, empresa de pequeno porte, ou cooperativas que preencham as condições estabelecidas no artigo 34, da Lei federal nº 11.488, de 15/06/2007, não será assegurado o direito de preferência, passando-se, desde logo, à negociação do preço.

7. O Pregoeiro poderá negociar com o autor da oferta de menor valor, obtida com base nas disposições dos subitens 6.1 e 6.2, ou, na falta desta, com base na classificação de que trata o subitem 5, mediante troca de mensagens abertas no sistema, com vistas à redução do preço.

8. Após a negociação, se houver, o Pregoeiro examinará a aceitabilidade do menor preço, decidindo, motivadamente, a respeito.

8.1. - O critério de aceitabilidade dos preços ofertados será o de compatibilidade com os preços dos insumos e salários praticados no mercado, coerentes com a execução do objeto ora licitado, acrescidos dos respectivos encargos sociais e benefícios e despesas indiretas (BDI).

8.2. - O Pregoeiro poderá a qualquer momento solicitar às licitantes a composição de preços unitários de serviços e/ou de materiais/equipamentos, bem como os demais esclarecimentos que julgar necessário.

9. Considerada aceitável a oferta de menor preço, passará o Pregoeiro ao julgamento da habilitação, observando as seguintes diretrizes:

a) Verificação dos dados e informações do autor da oferta aceita, constantes do CAUFESP e extraídos dos documentos indicados no item IV deste edital;

b) Caso os dados e informações constantes no CAUFESP não atendam aos requisitos estabelecidos no item IV deste Edital, o Pregoeiro verificará a possibilidade de suprir ou sanear eventuais omissões ou falhas, mediante consultas efetuadas por outros meios eletrônicos hábeis de informações;

b.1) Essa verificação será certificada pelo Pregoeiro na ata da sessão pública, devendo ser anexados aos autos, os documentos passíveis de obtenção por meio eletrônico, salvo impossibilidade devidamente certificada e justificada;

c) A licitante poderá, ainda, suprir ou sanear eventuais omissões ou falhas, relativas ao cumprimento dos requisitos e condições de habilitação estabelecidos no Edital, mediante a apresentação de documentos, desde que os envie no curso da própria sessão pública do pregão e até a decisão sobre a habilitação, por correio eletrônico para o endereço compras@procon.sp.gov.br;

c.1) Sem prejuízo do disposto nas alíneas “a”, “b”, “c”, “d” e “e”, deste subitem 9, serão apresentados, obrigatoriamente, por fax ou por correio eletrônico, as declarações a que se refere o subitem 1.5.1, do item IV, deste edital.

d) A Administração não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos hábeis de informações, no momento da verificação a que se refere a línea “b”, ou dos meios para a transmissão de cópias de documentos a que se refere a alínea “c”, ambas deste subitem 9, ressalvada a indisponibilidade de seus próprios meios. Na hipótese de ocorrerem essas indisponibilidades e/ou não sendo supridas ou saneadas as eventuais omissões ou falhas, na forma prevista nas alíneas “b” e “c”, a licitante será inabilitada, mediante decisão motivada;

e) Os originais ou cópias autenticadas por tabelião de notas, dos documentos enviados na forma constante da alínea “c”, deverão ser apresentados no Núcleo de Licitações, Compras e Contratos da Fundação PROCON/SP, à Rua Barra Funda 930 - 3º andar – sala 303 – Barra Funda – São Paulo/SP – CEP 01152-000, em até 02 (dois) dias após o encerramento da sessão pública, sob pena de invalidade do respectivo ato de habilitação e a aplicação das penalidades cabíveis;

f) Para habilitação de microempresas, empresas de pequeno porte, ou cooperativas que preencham as condições estabelecidas no artigo 34, da Lei federal nº 11.488, de 15/06/2007, não será exigida comprovação de regularidade fiscal, mas será obrigatória a apresentação dos documentos indicados no subitem 1.2, alíneas “a” a “e” do item IV deste Edital, ainda que os mesmos veiculem restrições impeditivas à referida comprovação;

g) Constatado o cumprimento dos requisitos e condições estabelecidos no Edital, a licitante será habilitada e declarada vencedora do certame;

h) Por meio de aviso lançado no sistema, o Pregoeiro informará às demais licitantes que poderão consultar as informações cadastrais da licitante vencedora utilizando opção disponibilizada no próprio sistema para tanto. Deverá, ainda, informar o teor dos documentos recebidos por fac-símile ou outro meio eletrônico.

10. A licitante habilitada nas condições da alínea “f”, do subitem 9 deste item V, deverá comprovar sua regularidade fiscal, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis.

11. A comprovação de que trata o subitem 10 deste item V deverá ser efetuada mediante a apresentação das competentes certidões negativas de débitos, ou positivas com efeitos de negativas, no prazo de 5 (cinco) dias úteis, contado a partir do momento em que a licitante for declarada vencedora do certame, prorrogável por igual período, a critério da Administração.

12. Ocorrendo a habilitação na forma indicada na alínea “f”, do subitem 9, a sessão pública será suspensa pelo Pregoeiro, observados os prazos previstos no subitem 11, para que a licitante vencedora possa comprovar a regularidade fiscal de que tratam os subitens 10 e 11 deste item V.

13. Por ocasião da retomada da sessão, o Pregoeiro decidirá motivadamente sobre a comprovação ou não da regularidade fiscal de que tratam os subitens 10 e 11 deste item V, ou sobre a prorrogação de prazo para a mesma comprovação, observado o disposto no mesmo subitem 11.

14. Se a oferta não for aceitável, se a licitante desatender às exigências para a habilitação, ou não sendo saneada a irregularidade fiscal, nos moldes dos subitens 10 a 13, deste item V, o Pregoeiro, respeitada a ordem de classificação de que trata o subitem 5 do mesmo item V, examinará a oferta subseqüente de menor preço, negociará com o seu autor, decidirá sobre a sua aceitabilidade e, em caso positivo, verificará as condições de habilitação e assim sucessivamente, até a apuração de uma oferta aceitável cujo autor atenda aos requisitos de habilitação, caso em que será declarado vencedor.

VI. DO RECURSO, DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO.

1. Divulgado o vencedor ou, se for o caso, saneada a irregularidade fiscal nos moldes dos subitens 10 a 13 do item V, o Pregoeiro informará às licitantes, por meio de mensagem lançada no sistema, que poderão interpor recurso, imediata e motivadamente, por meio eletrônico, utilizando para tanto, exclusivamente, campo próprio disponibilizado no sistema.

2. Havendo interposição de recurso, na forma indicada no subitem “1” deste item, o Pregoeiro, por mensagem lançada no sistema, informará aos recorrentes que poderão apresentar memoriais contendo as razões de recurso, no prazo de 3 (três) dias após o encerramento da sessão pública, e às demais licitantes que poderão apresentar contra razões, em igual número de dias, os quais começarão a correr do término do prazo para apresentação de memoriais, sendo-lhes assegurada vista imediata dos autos, no endereço da unidade promotora da licitação, ou seja, Núcleo de Licitações, Compras e Contratos da Fundação PROCON/SP, à Rua Barra Funda 930 - 3º andar – sala 303 – Barra Funda – São Paulo/SP – CEP 01152-000.

2.1. Os memoriais de recurso e as contra razões serão oferecidas por meio eletrônico, no sítio www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br ,opção RECURSO, e a apresentação de documentos relativos às peças antes indicadas, se houver, será efetuada mediante protocolo, no Núcleo de Licitações, Compras e Contratos da Fundação PROCON/SP, à Rua Barra Funda 930 - 3º andar – sala 303 – Barra Funda – São Paulo/SP – CEP 01152-000, observados os prazos estabelecidos no subitem 2, deste item.

3. A falta de interposição na forma prevista no subitem “1” deste item importará a decadência do direito de recurso e o pregoeiro adjudicará o objeto do certame ao vencedor, na própria sessão, propondo à autoridade competente a homologação do procedimento licitatório.

4. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto da licitação à licitante vencedora e homologará o procedimento licitatório.

5. O recurso terá efeito suspensivo e o seu acolhimento importará a invalidação dos atos insuscetíveis de aproveitamento.

6. A adjudicação será feita considerando a totalidade do objeto.

7. Se a vencedora da licitação for cooperativa de trabalho, deverá apresentar no prazo de 02 (dois) dias úteis contado da data de adjudicação do objeto, os novos preços mensal e total para a contratação, a partir do valor total final obtido no certame.

VII – DA DESCONEXÃO COM O SISTEMA ELETRÔNICO

1. À licitante caberá acompanhar as operações no sistema eletrônico, durante a sessão pública, respondendo pelos ônus decorrentes de sua desconexão ou da inobservância de quaisquer mensagens emitidas pelo sistema.

2. A desconexão do sistema eletrônico com o Pregoeiro, durante a sessão pública, implicará:

a) fora da etapa de lances, a sua suspensão e o seu reinício, desde o ponto em que foi interrompida. Neste caso, se a desconexão persistir por tempo superior a 15 (quinze) minutos, a sessão pública deverá ser suspensa e reiniciada somente após comunicação expressa às licitantes de nova data e horário para a sua continuidade;

b) durante a etapa de lances, a continuidade da apresentação de lances pelas licitantes, até o término do período estabelecido no edital.

3. A desconexão do sistema eletrônico com qualquer licitante não prejudicará a conclusão válida da sessão pública ou do certame.

VIII- DO LOCAL E DAS CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

1 - O objeto desta licitação deverá ser executado na Fundação PROCON/SP, à Rua Barra Funda, 930 – Barra Funda – São Paulo/SP, em conformidade com o estabelecido no Anexo I deste Edital, correndo por conta da Contratada as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto do contrato.

IX - DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

1 - O objeto da presente licitação, em cada uma de suas etapas, será recebido provisoriamente, em até 03 (três) dias úteis, contados da data de recepção pela Administração do relatório de execução dos serviços do mês acompanhado da nota fiscal/fatura representativa da prestação dos serviços, de acordo com o estabelecido no subitem 1 do item X deste Edital.

2 Havendo rejeição dos serviços, no todo ou em parte, a contratada deverá refazê-los no prazo estabelecido pela Administração, observando as condições estabelecidas para a prestação.

2.1 - Na impossibilidade de serem refeitos os serviços rejeitados, ou na hipótese de não serem os mesmos executados, o valor respectivo será descontado da importância mensal devida à contratada, sem prejuízo da aplicação das sanções cabíveis.

3 - O recebimento do objeto dar-se-á definitivamente no prazo de 15 (quinze) dias úteis após o recebimento provisório, ou da data de conclusão das correções efetuadas com base no disposto no subitem 2.1 do item IX deste Edital, uma vez verificada a execução satisfatória dos serviços, mediante termo de recebimento definitivo, ou recibo, firmado pelo servidor responsável.

X - DOS PAGAMENTOS E DO REAJUSTE DE PREÇOS

1 - Para efeito de pagamento, a contratada encaminhará a Assessoria de Informática da Fundação PROCON/SP, à Rua Barra Funda 930 - 4º andar – Barra Funda – São Paulo/SP – CEP 01152-000, após a conclusão, a respectiva nota fiscal/fatura, acompanhada do relatório dos serviços prestados no período a que o pagamento se referir.

1.1 - A discriminação dos valores dos insumos, especialmente os dos serviços, exigida no subitem 2.1 do item III deste Edital, deverá ser reproduzida na nota fiscal/fatura apresentada para efeito de pagamento.

2 - Os pagamentos serão efetuados no prazo de 30 (trinta) dias. *(art. 2º do Decreto nº 32.117, de 10/08/1990, com redação dada pelo Decreto nº 43.914, de 26/03/1999)*, contado da data de entrada da nota fiscal/fatura no protocolo do órgão indicado no subitem 1 deste item X supra e à vista do termo de recebimento definitivo ou recibo, de que trata o subitem 3 do item IX deste edital.

3 - As notas fiscais/faturas que apresentarem incorreções serão devolvidas à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem 2 deste item X começará a fluir a partir da data de apresentação da nota fiscal/fatura, sem incorreções.

4 - Constitui condição para a realização dos pagamentos a inexistência de registros em nome da Contratada no “Cadastro Informativo dos Créditos não Quitados de Órgãos e

Entidades Estaduais do Estado de São Paulo – CADIN ESTADUAL", o qual deverá ser consultado por ocasião da realização de cada pagamento.

5 - O pagamento será feito mediante crédito aberto em conta corrente em nome da Contratada no Banco do Brasil S/A.

6 Havendo atraso nos pagamentos, sobre o valor devido incidirá correção monetária nos termos do artigo 74 da Lei estadual nº 6.544/1989, bem como juros moratórios, à razão de 0,5% (meio por cento) ao mês, calculados "pro rata tempore" em relação ao atraso verificado.

7 O valor é fixo e não poderá ser reajustado.

XI - DA CONTRATAÇÃO

1 - A contratação decorrente desta licitação será formalizada mediante celebração de termo de contrato, cuja minuta integra este edital como Anexo II.

1.1 - Se, por ocasião da formalização do contrato, as certidões de regularidade de débito da adjudicatária perante o Sistema de Seguridade Social (INSS), o Fundo de Garantia por Tempo de Serviço (FGTS) e a Fazenda Nacional (Certidão Conjunta Negativa de Débitos relativa a tributos federais e dívida ativa da União) estiverem com os prazos de validade vencidos, o órgão licitante verificará a situação por meio eletrônico hábil de informações, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios, salvo impossibilidade devidamente justificada.

1.2 - Se não for possível atualizá-las por meio eletrônico hábil de informações, a Adjudicatária será notificada para, no prazo de 05 (cinco) dias úteis, comprovar a sua situação de regularidade de que trata o subitem 1.1 deste item XI, mediante a apresentação das certidões respectivas com prazos de validade em vigência, sob pena de a contratação não se realizar.

1.3 Constitui condição para a celebração da contratação a inexistência de registros em nome da adjudicatária no "Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais do Estado de São Paulo – CADIN ESTADUAL", o qual deverá ser consultado por ocasião da respectiva celebração.

1.4 Se o contrato for firmado com sociedade cooperativa, deverá a mesma indicar gestor encarregado de representá-la com exclusividade perante o contratante (artigo 1º do Decreto 55938/10 alterado pelo Decreto 51579/11).

2 - A adjudicatária deverá, no prazo de 5 (cinco) dias corridos contado da data da convocação, comparecer ao Núcleo de Licitações, Compras e Contratos da Fundação PROCON/SP, à Rua Barra Funda 930 - 3º andar – sala 303 – Barra Funda – São Paulo/SP – CEP 01152-000, para assinar o termo de contrato.

3 Quando a Adjudicatária deixar de comprovar a regularidade fiscal, nos moldes dos subitens 10 e 11, ou na hipótese de invalidação do ato de habilitação com base no disposto na alínea “e”, do subitem “9”, todos do item V ou, ainda, quando convocada dentro do prazo de validade de sua proposta, não apresentar a situação regular de que tratam os subitens 1.1 e 1.3, ambos deste item XI, ou se recusar a assinar o contrato, serão convocadas as demais licitantes classificadas, para participar de nova sessão pública do pregão, com vistas à celebração da contratação.

3.1 - Essa nova sessão será realizada em prazo, não inferior a 02 (dois) dias úteis, contado da divulgação do aviso.

3.2 - A divulgação do aviso ocorrerá por publicação no Diário Oficial do Estado de São Paulo - DOE e divulgação nos endereços eletrônicos www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br e www.imesp.com.br ,opção “e-negociospublicos”.

3.3 Na sessão, respeitada a ordem de classificação, observar-se-ão as disposições dos subitens 7 a 10 do item V e subitens 1, 2, 3, 4 e 6 do item VI, todos deste Edital.

4 - O contrato será celebrado com duração de 36 (trinta e seis) meses, contados da data de sua assinatura, contemplando o prazo para atualização e suporte.

5 - A execução dos serviços (entrega do firewall) deverá ter início em até 10 (dez) dias, a contar da data de assinatura do contrato e não poderá ultrapassar o presente exercício.

6 – A instalação, configuração e treinamento deverá corresponder ao que pede o Memorial Descritivo.

7 – O contrato será rescindido, se firmado com sociedade cooperativa, de forma imediata, na hipótese de caracterização superveniente de prestação de trabalho nas condições de não eventualidade por pessoas físicas, com relação de subordinação ou dependência, em face da contratante.

XII. DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

1. Ficará impedida de licitar e contratar com a Administração direta e indireta do Estado de São Paulo, pelo prazo de até 5 (cinco) anos, a pessoa física ou jurídica, que praticar quaisquer atos previstos no artigo 7º da Lei federal nº 10.520, de 17 de julho de 2002, c.c. o artigo 15 da Resolução CEGP-10 de 19 de novembro de 2002.

2. A sanção de que trata o subitem anterior poderá ser aplicada juntamente com as multas previstas na Resolução SJ 35/90, garantido o exercício de prévia e ampla defesa, e deverá ser registrada no CAUFESP e no sítio www.sancoes.sp.gov.br.

XIII - DA GARANTIA CONTRATUAL

1 - Não será exigida a prestação de garantia para a contratação resultante desta licitação.

XIV - DAS DISPOSIÇÕES FINAIS

1. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitada a igualdade de oportunidade entre as licitantes, desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

2. Das sessões públicas de processamento do Pregão serão lavradas atas circunstanciadas, observado o disposto no artigo 14, inciso IX, do regulamento anexo à Resolução CC-27/2006, a serem assinadas pelo Pregoeiro e pela equipe de apoio.

3. O sistema manterá sigilo quanto à identidade das licitantes, para o Pregoeiro até a etapa de negociação com o autor da melhor oferta e para os demais até a etapa de habilitação.

4. O resultado deste Pregão e os demais atos pertinentes a esta licitação, sujeitos à publicação, serão divulgados no Diário Oficial do Estado e nos sítios eletrônicos www.imesp.com.br, opção "enegociospublicos" e www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br, opção "pregao eletronico".

5. Até 2 (dois) dias úteis anteriores à data fixada para abertura da sessão pública, qualquer pessoa poderá, por meio do sistema eletrônico, solicitar esclarecimentos, informações ou impugnar o ato convocatório do Pregão Eletrônico.

5.1. A impugnação, assim como os pedidos de esclarecimentos e informações, será formulada em campo próprio do sistema, encontrado na opção EDITAL.

5.2. As impugnações serão respondidas pelo subscritor do Edital e os esclarecimentos e informações prestados pelo pregoeiro, no prazo de até 1 (um) dia útil, anterior à data fixada para abertura da sessão pública.

5.3. Acolhida a impugnação contra o ato convocatório, será designada nova data para realização da sessão pública.

6. Os casos omissos do presente Pregão serão solucionados pelo Pregoeiro, e as questões relativas ao sistema, pelo Departamento de Controle de Contratações Eletrônicas – DCC.

7. Integram o presente Edital:

Anexo I – Memorial Descritivo;
Anexo II – Minuta de Contrato;
Anexo III – Modelo de Declaração;
Anexo IV – Resolução SJ 35/90.

8. Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente o foro da Comarca da Capital do Estado de São Paulo.

Marcello Gonella de Andrade – Diretor Adjunto de Administração e Finanças
Rosana Agnes Guizi – Pregoeira e Subscritora do Edital

ANEXO I – MEMORIAL DESCRITIVO FIREWALL UTM

Processo FP 462/16 - Pregão 19/16

MEMORIAL DESCRITIVO FIREWALL UTM

1. DOS REQUISITOS COMUNS PARA TODOS OS ITENS

Os produtos que compõe a Solução de Segurança devem todos ser produzidos pelo mesmo fabricante;

A Licitante deve informar na proposta comercial e na tabela de formação de preços marca e modelo do(s) produto(s) ofertado(s);

A Licitante deverá realizar a instalação dos produtos de segurança contratados pelo presente certame;

A Licitante deverá apresentar carta do fabricante quanto ao fornecimento, garantia e funcionalidade dos produtos ofertados.

A Licitante deverá apresentar declaração emitida pelo fabricante específica para este certame comprovando que a empresa faz parte do programa de parcerias e que possui autorização para comercializar os seus produtos e serviços.

A Licitante deverá emitir declaração que cumpre todos os requisitos técnicos do edital, se responsabilizando por isso, sendo que os requisitos técnicos serão validados pela equipe técnica de homologação.

A mesma deve fornecer atestado comprovando a existência de equipe técnica com pessoas capacitadas pelo fabricante em todas as soluções adquiridas. O atestado/diploma deverá ser fornecido pelo fabricante;

2. OBJETO

Solução integrada de Firewall NEXT GENERATION com funcionalidade de operação em modo de alta disponibilidade (ativo/passivo) composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) entendendo-se como tais o conjunto de serviços e recursos de: Filtro de pacotes com controle de estado, Filtro de conteúdo web, Interceptação SSL, Filtro de aplicações, Controle da web 2.0, Inspeção com proteção contra ataques de malwares, vírus, worm, e aplicativos maliciosos, integrar soluções do tipo (IDS/IPS, ATP, QoS, Balanceamento de serviços, Redundância de links, VPN, DHCP e DNS). Com a capacidade de integrar todos os recursos em um único dispositivo.

Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 36 meses.

Os itens que são objeto desta licitação seguem a seguir

Código	Descrição	Quantidade
1	Firewall UTM de 8Gbps de capacidade de firewall	2 unidades
2	Instalação e Configuração do Firewall UTM	40 horas
3	Atualização e Suporte 12x5	36 meses
4	Treinamento Oficial da solução com duração mínima de 40 horas	4 pessoas

3. ESPECIFICAÇÕES MÍNIMAS E CARACTERISTICAS TÉCNICAS DOS MODELOS DE HARDWARE

3.1. APPLIANCE DE UTM DE 8000 MBPS DE CAPACIDADE DE FIREWALL COM GARANTIA E ATUALIZAÇÃO PARA 36 MESES.

3.1.1. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U’s do referido rack;

3.1.2. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;

3.1.3. Dispor de fonte de alimentação interna com tensão de entrada de 110V a 220V AC automática e frequência de 50-60 Hz;

3.1.4. Possuir throughput de no mínimo 8 Gbps para tráfego TCP;

3.1.5. Possuir throughput de no mínimo 15 Gbps para tráfego UDP;

3.1.6. Suportar no mínimo 2.000.000 (2 milhões) conexões simultâneas;

3.1.7. Suportar no mínimo 100.000 (cem mil) novas conexões por segundo;

3.1.8. Possuir throughput de no mínimo 3,6 Gbps para tráfego HTTP/ HTTPS via proxy;

3.1.9. Possuir throughput de no mínimo 800 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;

3.1.10. Possuir throughput de no mínimo 600 Mbps para tráfego HTTP/ HTTPS com inspeção SSL + Inspeção ATP via proxy;

3.1.11. Possuir throughput de no mínimo 2,5 Gbps para tráfego IPS;

3.1.12. Possuir throughput de no mínimo 2,0 Gbps para tráfego ATP;

3.1.13. Possuir throughput de no mínimo 3,0 Gbps para tráfego VPN IPSEC com criptografia (AES-128);
3.1.14. Possuir throughput de no mínimo 1,8 Gbps para tráfego VPN SSL com criptografia (AES-128);
3.1.15. Suportar no mínimo 400 conexões de usuários concorrentes para VPN SSL;
3.1.16. Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade;
3.1.17. Permitir expandir no mínimo 16 interfaces GbE RJ45 ou 4 LANs 10GbE SFP+
3.1.18. Possuir no mínimo de 3(três) devices de rede GbE By-pass;
3.1.19. Possuir no mínimo 16 GB de memória RAM;
3.1.20. Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;
3.1.21. Possuir mínimo de 1 (uma) porta console de conexão padrão RJ45 para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232/RJ-45;
3.1.22. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

4. ESPECIFICAÇOES GERAIS DE SOFTWARE DE FIREWALL NEXT GENERATION UTM

A Solução deve ser uma solução UTM “Unified Threat Management” Gerenciador Unificado de ameaças, integrada com os demais recursos e serviços, deve ser capaz de instalar todos os recursos e serviços em um mesmo hardware ou de forma distribuída.

4.1. RECURSOS E SERVIÇOS GERAIS:

4.1.1. Deve suportar tecnologia de Firewall Stateful Packet Inspection.
4.1.2. Possuir conexão entre a estação de gerência e Appliance no modo criptografado tanto em interface gráfica quanto em CLI (linha de comando). O Acesso a interface de administração deve ser via WEB sob o protocolo HTTPS com ergonomia voltada a usabilidade;
4.1.3. Gerenciamento do tráfego e estatísticas sumarizadas através de um painel de controle;
4.1.4. Possuir sistemas de alertas e notificações do sistema em tempo real na interface WEB e envios automáticos por e-mail;
4.1.5. Interface responsiva compatível com dispositivos móveis;
4.1.6. Interface em português e inglês;

4.1.7. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

4.1.8. Permitir a criação de perfis de administração baseado em ACL (Acess list), de forma a possibilitar a definição de diversos administradores para o dispositivo, cada um responsável por determinada tarefa da administração;

4.1.9. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

4.1.10. Permitir criar as definições de ACL (Acess List) completa por administrador, sendo possível especificar os direitos, como: somente Visualizar ou Editar ”Alterar, Excluir, Cadastrar”;

4.1.11. Permitir auditoria do sistema com log das ações dos administradores por tipo de recurso e período;

4.1.12. Possuir porta console (serial) para possíveis manutenções no produto.

4.1.13. Acesso via WEB a console shell para gerenciamento através de interface de linha de comando CLI (Command Line Interface). Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

4.1.14. A interface CLI deve suportar a configuração de roteamento dinâmico no mínimo para os protocolos BGP, OSPF, RIP1 e RIP2 com suporte a interface Vty;

4.1.15. Possuir um Certificado digital (CA – Certificado de Autoridade) padrão X.509, nativo com chaves de 2048 bits, para os processos de autenticação do usuário, utilização do proxy SSL e em todas as conexões de serviços com o Appliance.

4.1.16. A solução deve manter um canal de comunicação segura, com criptografia baseada em certificados entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

4.1.17. Permitir a integração com qualquer autoridade certificadora válida emissora de certificados X509 que seguir os padrões descritos na RFC 2459.

4.1.18. Capacidade para criação de objetos com a finalidade de facilitar a administração e configuração do sistema, deve atender no mínimo os seguintes tipos de objetos: endereço IP, endereço MAC, Portas de serviços e protocolos, atendendo no mínimo os seguintes protocolos (TCP, UDP, ICMP, IGMP, AH, EGP, ESP, GRE, RSVP, e SCTP), tabela de horário, período com especificação de data/hora inicial e final, tabela de palavras chaves com a possibilidade de especificar expressões regulares, Tipos de conteúdo de arquivos (content types);

4.1.19. Possuir um sistema de armazenamento remoto com suporte a conexões do tipo SMB, NFS e Disco (USB-HDD);

4.1.20. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

4.1.21. As cópias de segurança (backups) devem ser armazenadas em dispositivos remotos do tipo NFS (Network File System) ou Disco externo (USB-HDD);

4.1.22. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto, e executar a manutenção de período automaticamente.

4.1.23. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

4.1.24. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

4.1.25. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

4.1.26. Suporte e integração com servidores de Network Time Protocol (NTP) para atualização de data e hora do sistema, o que padroniza e evita problemas com o horário de verão;

4.1.27. Atualização automática do sistema para correções e releases. O sistema de atualização deve permitir agendamento para verificação diária da base de atualizações do fabricante.

4.1.28. As atualizações devem ser disponibilizadas no intervalo máximo de 15 dias. Não podendo ultrapassar este período;

4.1.29. Efetuar controle de tráfego e monitor por estado de conexão no mínimo para os seguintes protocolos (TCP, UDP , ICMP, IGMP, AH, EGP, ESP, GRE, RSVP, e SCTP) baseados nos endereços de origem, destino e porta;

4.1.30. Suportar o Internet Protocol Versões 4 (IPv4);

4.1.31. Suporte a Interfaces Ethernet;

4.1.32. Suportar o protocolo 802.1q, para uso e segmentação da rede com VLANs;

4.1.33. Suporte a interfaces do tipo MACVLAN;

4.1.34. Suportar o protocolo 802,1ax e 802.3ad (LACP), Link Aggregation Control Protocol;

4.1.35. Suporte a interfaces DSL;

4.1.36. Suporte a roteamento estático;

4.1.37. Suporte ao protocolo SNMP;

4.1.38. A solução deve suportar funcionamento com 2 (dois) equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

4.2. AUTENTICAÇÃO:

4.2.1. Suporte a múltiplos domínios de autenticação, mínimo 3(três) domínios;

4.2.2. Permitir o cadastro dos usuários e grupos em base de dados própria por meio da interface de administração WEB do dispositivo;

4.2.3. Suporte a sincronismo de usuários e grupos com servidores Windows AD® e Servidores LDAP;

4.2.4. Permitir a utilização de LDAP, LDAP/SSL para a autenticação de usuários;

4.2.5. Permitir o login de usuários de forma transparente ao efetuar logon na rede para plataformas Windows 2008 e 2012 Servers (sem a necessidade de o usuário digitar novamente a senha), para todos os serviços suportados, considerando assim a autenticação do usuário, como uma autenticação unificada entre a plataforma Windows e o Appliance Firewall NG UTM;

4.2.6. Permitir o controle de acesso por usuário, para todas as plataformas com browser através de autenticação via portal WEB para todos os serviços suportados, de forma que um determinado usuário tenha seu perfil de acesso automaticamente carregado;

4.2.7. Possuir suporte a um sistema de autenticação do tipo Captive Portal capaz de redirecionar de forma automática a autenticação, deve ser compatível com autenticação Windows AD, LDAP e LOCAL;

4.2.8. O Captive Portal deve suportar o protocolo HTTPS para a tela de autenticação do usuário e para administração dos serviços de Captive Portal para o usuário;

4.2.9. A solução deverá permitir em seu portal de autenticação, o cadastro de novos usuários, para o caso de usuários itinerantes (visitantes/ temporários) se não for possível consultar uma base de autenticação o Captive Portal deverá solicitar informações para cadastro e o sistema deverá efetuar o auto cadastro do usuário itinerante a um “grupo” de usuários se enquadrando automaticamente em um perfil de acesso;

4.2.10. O sistema de Captive portal deve ser capaz de aplicar uma política geral e gerenciar a sessão do usuário autenticado:

4.2.11. Controlar o número de sessões concorrentes por usuário;

4.2.12. Controlar o número de tentativas de autenticação não autorizada;

4.2.13. Bloquear o endereço IP de origem das tentativas de autenticação não autorizada;

4.2.14. Definir o tempo de bloqueio do endereço IP das tentativas de autenticação não autorizada;

4.2.15. Definir tempo de sessão por inatividade;

4.2.16. Identificar endereço IP;

4.2.17. Identificar endereço MAC;

4.2.18. Permitir o administrador efetuar logout de sessão de qualquer usuário através da interface de gerenciamento WEB da solução de firewall;

4.2.19. Deverá oferecer também um recurso de integração para acesso aos serviços e recursos de conexões do tipo VPN SSL para acesso as aplicações disponibilizados pelo Túnel VPN SSL sob autenticação do Captive Portal;

4.2.20. Os usuários devem ter acesso a alguns recursos tais como: alterar dados pessoais; alterar senha para os casos de usuário do tipo local; fazer o download do Certificado de Autoridade (CA), e acesso ao termo de uso;

4.3. SEGURANÇA:

4.3.1. Prover a condição de configuração de uma Política padrão por agrupamento de devices ou zonas de rede, determinando origem e destino por tipo de agrupamento;

4.3.2. Possibilitar exigir autenticação para a política padrão;

4.3.3. Capacidade para trabalhar com conversão de endereços e portas (NAT/NAPT) conforme RFC 3022; ser capaz de aplicar mascaramento de pacotes do tipo: SNAT (source nat) por endereço IP de origem; SNAT (masquerade) por device de origem; DNAT (dnat) mascaramento de destino por endereço IP/porta de destino e Nat-T em VPN IPSec;

4.3.4. Prover mecanismos de segurança configuráveis, que permita habilitar proteção contra ataques do tipo: “Denied of Service; Portscan; Pacotes inválidos; SYN Flood; ICMP Flood”;

4.3.5. Possuir mecanismo que permita habilitar e desabilitar recursos do tipo: “ICMP Echo/Request – ping; ICMP Redirect; ICMP Broadcast; Source Routing; Checksum; Log Inválidos; TCP be liberal”;

4.3.6. Possuir mecanismo de configuração para o controle de tipos de conexão possibilitando definir limites máximos para cada tipo de controle das conexões do protocolo TCP;

4.3.7. Possuir mecanismo de configuração para o controle de conexão possibilitando definir limites de timeout para as conexões genéricas;

4.3.8. Possuir mecanismo de configuração para o controle de conexão do protocolo ICMP possibilitando definir limites de timeout;

4.3.9. Possuir mecanismo de configuração para o controle de conexão do protocolo UDP possibilitando definir limites de timeout;

4.3.10. Detectar automaticamente e inserir regras de bloqueio temporárias para varreduras de portas efetuadas contra o dispositivo ou contra qualquer máquina protegida por esse, mesmo que realizados em períodos maiores que 1 (um) dia;

4.3.11. Possuir politicas padrões de entrada para os serviços nativos do firewall por agrupamento de device ou zonas de rede, podendo exigir ou não autenticação, com possibilidade de aplicar ações de bloqueio, permissão, inspeção IDS/IPS ou inspeção ATP;

4.3.12. Permitir definir as políticas de entrada para os serviços nativos do firewall, podendo aplicar filtros no acesso por: usuário, grupos, endereço IP de origem, endereço IP de destino e horário.

4.4. PROXY:

4.4.1. Possuir Proxy nativo para tráfego HTTP, HTTPS, versões 1.0 e 1.1, FTP;

4.4.2. Deve possibilitar a conexão de tráfego para outros serviços e que contemplem a conexão em proxies HTTP, tais como: XMPP, SIP, H323, SMTP, POP3, IMAP, RTSP, TELNET e outros;

4.4.3. Deve permitir a configuração para outras portas de serviços;

4.4.4. Deve permitir implementar proxy transparente para os protocolos HTTP e HTTPS, de forma a dispensar a configuração dos browsers dos dispositivos clientes para a utilização das características o serviço;

4.4.5. Deve permitir implementar proxy configurado para os protocolos HTTP, HTTPS, FTP e SOCKS;

4.4.6. Deve permitir o armazenamento em Cache de conteúdo trafegado pelo protocolo HTTP e HTTPS;

4.4.7. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

4.4.8. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

4.4.9. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

4.4.10. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

4.4.11. Possibilitar a integração com servidores de cache WEB externos;

4.4.12. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Update;

4.4.13. Deve ser capaz de armazenar cache dinâmicos de streaming no mínimo para endereços do Youtube e MSN vídeos;

4.4.14. Deverá ser capaz de armazenar em cache dinâmicos conteúdo do Facebook, Google Maps e Sourceforge Downloads;

4.4.15. Deve possuir a capacidade de excluir URLs especificas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

4.4.16. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

4.4.17. Deve ter suporte à integração antivírus HTTP através de hierarquia de proxy;

4.4.18. Possuir mecanismos de integração a interceptação SSL com suporte a conexões de proxy transparente ou proxy configurado;

4.5. SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS:

4.5.1. Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

4.5.2. O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.

4.5.3. Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o

descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

4.5.4. A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

4.5.5. A base de assinaturas deve possuir mínimo de 2(duas) modalidades de assinaturas, atendendo a identificação de ameaças e aplicativos;

4.5.6. Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;

4.5.7. O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

4.5.8. Deverá permitir a atualização automática das assinaturas por meio de agendamento diário;

4.5.9. Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;

4.5.10. Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

4.5.11. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.

4.5.12. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP OpenSIP, Bria, ClearSea e Nero SIP;

4.5.13. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;

4.5.14. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;

4.5.15. Possuir mecanismo de bloqueio para listas de reputação de endereço IP catalogadas no mínimo para 6(seis) categorias, capaz de permitir seleção por categorização, elas devem atender as seguintes classificações: spam, reputation, malware, attacks, anonymous e abuse;

4.5.16. Possuir mecanismo de bloqueio e proteção por localização GeoIP para uma lista mínima de 250 Países e Repúblicas;

4.5.17. Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar aplicações criptografadas incluindo todo o payload;

4.5.18. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

4.5.19. Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

4.5.20. Suportar exceção para base de reputação IP por endereço IP;

4.5.21. Suportar exceção para a base de localização GeoIp por endereço IP;

4.5.22. Ação de Bloqueio do pacote ou reset da conexão em tempo real;

4.5.23. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;

4.5.24. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;

4.5.25. Deve possuir mecanismo para gerar Log; registro das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;

4.5.26. Gerar registro do tipo Top level, dos 50(cinquenta) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

4.5.27. Todos os logs e registros devem permitir ser gerados por período: “diário ou mensal”;

4.5.28. Possuir mecanismos para inspecionar, identificar e detectar os aplicativos e sub aplicativos trafegados via proxy e classificá-lo de acordo a base de assinaturas;

4.5.29. Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o trafego via proxy, e classificá-lo de acordo a base de assinaturas;

4.5.30. Deve permitir o bloqueio em caso de detecção dos aplicativos e ou ameaças e atacantes, com base nas políticas de cada assinatura;

4.6. SISTEMA DE PREVENÇÃO CONTRA INTRUSÃO:

4.6.1. Possuir sistema de prevenção contra intrusão de atacantes (IDS/IPS) nativo;

4.6.2. O Sistema de IPS deve monitorar, analisar o trafego e proteger a rede contra ataques internos e externos e utilizar técnicas de varredura e identificação que filtrem e bloqueie os pacotes atacantes, e descarte o pacote com conteúdo de código malicioso

4.6.3. Deve ser baseado na identificação de assinaturas de tipos de ataques e aplicações com vulnerabilidades conhecidas. O IPS deve contemplar uma base de assinaturas capaz de identificar o método de ataque com base em modelos de comportamento, características dos protocolos de rede, sistemas operacionais, inclusive comandos executados e esse conjunto de informações deve permitir que o pacote malicioso seja identificado e bloqueado em tempo real pelo IPS.

4.6.4. Possuir pelo menos 18000 mil (dezoito mil) assinaturas;

4.6.5. O fabricante deve garantir o fornecimento de atualizações regulares dentro do período de assinatura contratado;

4.6.6. Deverá permitir a atualização automática das assinaturas por meio de agendamento diário;

4.6.7. A base de assinaturas deve contemplar um mínimo de 65(sessenta e cinco) categorias, atendendo a identificação de ameaças e atacantes;

4.6.8. A solução deve ser capaz de detectar e prevenir as seguintes ameaças: Exploits e vulnerabilidades específicas de clientes e servidores, mau uso de protocolos, comunicação outbound de malware, tentativas de tunneling, e ataques genéricos;

4.6.9. A solução deve prover mecanismos de proteção contra ataques dos serviços de rede e aplicações, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de, DNS, FTP, SNMP, Telnet, TFTP, serviços Windows (Microsoft Networking) e VoIP.

4.6.10. A solução deve prover mecanismos de proteção contra ataques as assinaturas relacionadas a web-server, IIS, Apache, MSSql, MySql para que seja usado para proteção específica de Servidores Web;

4.6.11. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS), Exploits, Attack Response;

4.6.12. Detecção de ataques de RPC (Remote procedure call);

4.6.13. Deve prover mecanismos de Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

4.6.14. Deve prover mecanismos de Proteção contra ataques de ICMP (Internet Control Message Protocol);

4.6.15. Deve possuir mecanismos de integração nas conexões via proxy, a partir da interceptação SSL. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI), conseguir inspecionar pacotes criptografados incluindo todo o payload;

4.6.16. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

4.6.17. Ação de Bloqueio do pacote ou reset da conexão em tempo real;

4.6.18. Deve possuir mecanismo para gerar Log; registro das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;

4.6.19. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “ataques detectados” e os “ataques bloqueados”;

4.6.20. Gerar registro do tipo Top level, dos 50(cinquenta) mais, inclusive da relação de eventos entre os tipos de ataques e usuários, os graus de impacto e usuários, ataques identificados e bloqueados;

4.6.21. Todos os logs e registros devem permitir ser gerados por período: “diário ou mensal”;

4.6.22. Possuir mecanismos para inspecionar, identificar e detectar as ameaças e ataques do tráfego geral, incluindo o trafego via proxy, e classificá-lo de acordo a base de assinaturas;

4.6.23. Deve permitir o bloqueio em caso de detecção de ameaças e atacantes, com base nas políticas de cada assinatura;

4.7. QOS:

4.7.1. Deve permitir especializar as redes de forma a melhorar sensivelmente a qualidade de conexão, tratando de forma diferenciada e especifica as transmissões que exijam maior e melhor qualidade da rede.

4.7.2. Deve possuir mecanismo que permita criar controles por fila de prioridade, mínima de 5(cinco) níveis;

4.7.3. Deve ser capaz de alterar a velocidade dos acessos por nível de prioridade;

4.7.4. Deve ser capaz de criar limites de banda máxima por fila de prioridade;

4.7.5. Deve ser capaz de criar garantia de banda mínima por fila de prioridade;

4.7.6. Deve permitir a habilitação do controle de velocidade permitindo especificar a largura de banda ou velocidade downstream e Upstream de cada barramento ou device;

4.7.7. Priorização de pacotes com suporte às tecnologias de tratamento ToS (Type of Service) e DSCP (DiffServ Code Point);

4.7.8. Permitir modificação de valores TOS para a priorização de roteamento dos pacotes;

4.7.9. Implementar no mínimo 5(cinco) níveis de roteamento e tipos de serviços, com configuração e marcação para códigos TOS através da interface gráfica;

4.7.10. Permitir modificação de valores DSCP dos pacotes para o DiffServ;

4.7.11. Implementar no mínimo 20(vinte) classes de serviço distintas, com configuração do mapeamento e marcação para códigos DSCP através da interface gráfica;

4.8. BALANCEAMENTO DE LINK:

4.8.1. Deve ser capaz de segmentar e priorizar o tráfego através das interfaces de rede;

4.8.2. Deve contemplar a função de roteamento por prioridade de links;

4.8.3. Deve ser “Tolerante a falhas”, ou seja, possuir recurso de FailOver;

4.8.4. Deve possuir mecanismos de controle de falhas de link, capaz de aplicar testes da disponibilidade em tempo real. Estes testes devem retornar para o sistema o status atual de cada link, e em caso de falhas do link principal, este recurso deve alterar o “gateway padrão” do sistema para o próximo link da lista de prioridades de links;

4.8.5. O serviço de FailOver de links deve possibilitar que os testes e monitoramento sejam realizados através do protocolo ICMP para endereços de hosts externos;

4.8.6. O monitoramento no protocolo ICMP deverá permitir inserir múltiplos endereços para verificação e o link principal somente será marcado como inativo se todos os hosts externos pararem de responder;

4.8.7. Deverá possuir as seguintes opções de configurações para o monitoramento do link que fazem parte do FailOver e Balanceamento de link:

4.8.7.1. Intervalo de monitoramento;

4.8.7.2. Quantidade tentativas de testes por host, ou número de falhas necessárias antes de marcar o link como inativo;

4.8.8. Permitir utilizar um link como principal e outro como secundário. O tráfego apenas será redirecionado (FailOver) quando o principal ficar indisponível, retornado ao estado anterior quando o principal ficar ativo novamente;

4.8.9. Deve suportar regras de roteamento dos serviços de saída do próprio dispositivo de firewall, podendo selecionar entre os links, inclusive definindo prioridade do tráfego;

4.8.10. Suportar o uso simultâneo de múltiplos links em um mesmo firewall, de provedores distintos ou não.

4.8.11. Permitir o balanceamento de links, inclusive com IPs dinâmicos para ADSL, ou outra tecnologia de banda larga que não utilize IP Fixo;

4.8.12. Deve contemplar o recurso de balanceamento de links por políticas de segurança; podendo ser aplicadas por: Origem, Destino, Conteúdo web, Horário ou Período de data e hora inicial e final, Controles de tipo de conteúdo, Tipo de pacote; Políticas de mascaramento; Políticas de Proxy; Usuário e grupos;

4.9. CONTROLE DE APLICATIVOS WEB:

4.9.1. O controle de aplicativos web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado por tipo de aplicativo e sub aplicativos em uso, deve ser baseado em decodificadores de assinaturas e protocolos.

4.9.2. O controle desses aplicativos devem permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamentos de devices podem utilizar ou não estes recursos, definindo inclusive dentro das suas características quais recursos de cada aplicativo poderão ser utilizados.

4.9.3. A base deve contemplar um número mínimo de 790 aplicativos e sub aplicativos diferentes, catalogados e classificados em categorias, mínima de 24 categorias;

4.9.4. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer os aplicativos independente de porta e protocolo, com as seguintes funcionalidades:

4.9.5. Possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a necessidade de especificar endereço de origem ou destino das aplicações, para as tomadas de ação;

4.9.6. Reconhecer no mínimo aplicações do tipo redes sociais, aplicativos peer to peer, acesso remoto, games, streamings, aplicativos de lojas on line, mensageiros instantâneos, colaboração e vídeo conferencia, e-mails, fóruns, bloggers, storage, proxy anônimos, antivírus entre outras;

4.9.7. Deve contemplar assinaturas que identifique pelo menos os aplicativos e sub aplicativos tais como: Youtube, Facebook, Twitter, Linkdin, Tumblr, Bittorrent, Gnutella, AIM, Baidu, Syflex, logmein, Join.me, DropBox, Onedrive, Apple iCloud, Amazon, Ebay, iTunnes, Blospot, Instagram, Flickr, Photoshop, Picasso, Myspace, Netflix, Justin TV, Megavideo, Skype, Viber, Whatsapp, Yahoo Messenger, Spotify, Wunderlist, Webex, Gismodo, Google news, Google Docs, Google Earth, Google translator, Google finance, Money Control, Morningstar, Playstation, Wii, Xbox live;

4.9.8. Ser capaz de identificar assinaturas de aplicações de uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações de proxies que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Vtunnel, Zenguard, Privax, Proxydotorg,;

4.9.9. O recurso deve de forma objetiva controlar aplicativos web 2.0 com a finalidade de melhorar o desempenho da rede e evitar improdutividade do grupo de usuários da rede;

4.10. FILTRO DE CONTEÚDO WEB:

4.10.1. O filtro de conteúdo web deve possuir mecanismos de detecção capaz de tomar medidas contra o tráfego de rede indesejado dependendo da URL ou categoria web, deve ser baseado em uma lista de urls classificadas por tipo de conteúdo.

4.10.2. O Filtro de conteúdo WEB deve permitir inspecionar, permitir ou bloquear estes acessos nas conexões HTTP e HTTPS através de proxy transparente ou proxy configurado, inclusive a definição de quais usuários, grupos de usuários, redes, devices ou agrupamento de devices, podem acessar ou não as diversas categorias identificadas;

4.10.3. O filtro de conteúdo web deve possuir base de dados catalogada com mínimo de 40 milhões de URLs e classificada no mínimo em 88 categorias;

4.10.4. A solução deve possuir mecanismos de criação de regras que possibilite definir políticas de segurança de maneira simplificada, sem a necessidade de

correlacionar endereços de origem e destino das urls ou categorias web para as tomadas de ação;

4.10.5. A solução de filtro de conteúdo deve suportar a ação de forçar a pesquisa segura independente da configuração do navegador (browser) da estação de trabalho do usuário. Esta funcionalidade não permitirá que os sites de busca retornem resultados considerados inapropriados. Esta funcionalidade deve ser suportada no mínimo para os buscadores “Google”, “Bing” e “Yahoo”;

4.10.6. A solução deve contemplar filtros de navegação por User Agent, o filtro de conteúdo deve conseguir identificar um mínimo de 450 (quatrocentos e cinquenta) navegadores diferentes, a base de identificação deve incluir navegadores padrões, navegadores para mobile, navegadores offline e outros;

4.10.7. Deve possuir mecanismos de filtragem de métodos HTTP a fim de otimizar e melhorar a eficiência do tráfego web, deve comtemplar filtros do tipo: put, get, checkout, connect, delete, head, link, post, search e trace;

4.10.8. Deve permitir criar base de categorias personalizadas a partir de listas de URLs com suporte a lista de palavras chaves e expressões regulares;

4.10.9. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

4.10.10. Permitir a criação de filtros para arquivos e dados pré-definidos;

4.10.11. Os arquivos devem ser identificados por extensão e assinaturas;

4.10.12. Suporte a identificação de arquivos compactados, executáveis, imagens, e multimídias a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.10.13. Deve oferecer a opção de bloquear controles ActiveX e Java Scripts que possam comprometer o acesso web dos usuários;

4.10.14. Deve oferecer a opção de cota de tempo em horas ou minutos de navegação web por dia;

4.10.15. Deve oferecer a opção de cota de tráfego em MB de navegação web por dia;

4.10.16. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs, etc) identificados sobre aplicações (HTTP, HTTPS e FTP) inclusive oferecendo a opção de controle de tamanho máximo de download por navegação;

4.10.17. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, Compactados, Executáveis, ISOs, etc) identificados

sobre aplicações (HTTP, HTTPS e FTP) inclusive oferecendo a opção de controle de tamanho máximo de upload por navegação;

4.10.18. Deve suportar mecanismos de filtro e controle de login no Google por domínio, permitindo ao administrador especificar os domínios permitidos;

4.10.19. O sistema de filtro de conteúdo poderá ser aplicado por definição de horário, ou período de validade do filtro; podendo ou não especificar usuários, grupos de usuários, rede ou agrupamento de device para todos os recursos de filtragem e controles estabelecidos;

4.11. POLITICAS DE SEGURANÇA DO FIREWALL

4.11.1. O sistema deve integrar os respectivos recursos e serviços de integração com o firewall: NAT, Serviços diversos, proxy; filtro de conteúdo web, filtro de aplicações web, QoS, FailOver e balanceamento de links, de acordo as especificações técnicas descritas a fim de propiciar um sistema capaz de tratar o tráfego da rede em camadas, garantindo a segurança dos dados;

4.11.2. Estes recursos integrados devem permitir o tratamento do tráfego em camadas, de modo granular com o suporte a interceptar o tráfego SSL, identificar malwares e ações mal-intencionadas que utilizam o protocolo HTTPS para burlar firewalls, o sistema deve interceptar estas conexões, analisar e enviar os pacotes para tomadas de ações;

4.11.3. Deve também permitir a inspeção destes pacotes, detectar e prevenir dos ataques de intrusos, operando em conjunto com o firewall, impedir que acessos externos e/ou remotos executem rotinas de invasão. Executando ação pró ativa de bloqueio dos ataques;

4.11.4. Deve permitir gerar políticas de segurança capaz de filtrar os pacotes, integrar aos recursos de tratamento de filtro de conteúdo, filtro de aplicações, gerenciamento e controle dos pacotes definindo controle de banda por níveis de velocidade e garantia de banda por prioridade.

4.11.5. Deve permitir o roteamento estático por device, por endereço IP, serviços, usuários, grupos de usuários, para cada link de internet podendo distribuir o balanceamento de carga entre múltiplos links de internet ou ainda definir um roteamento exclusivo sem a opção de redundância ou failover;

4.11.6. As políticas de segurança devem permitir integrar em uma mesma interface interativa a definição de uma única política que atenda todos os recursos integrados com o firewall citados (no item 8.11.1);

4.11.7. As políticas de segurança devem tomar ações do tipo: Permitir, Bloquear, e inspecionar para o tráfego IPS ou Inspecionar para o tráfego ATP;

4.11.8. As políticas de segurança devem atender as especificações por prioridade, se o conteúdo do tráfego se enquadrar as definições da política, a mesma deve ser aplicada ignorando as políticas de menor prioridade

4.11.9. Deve permitir reordenação sempre que necessário;

4.11.10. Deve suportar mecanismos de balanceamento de links por política, inclusive com devices do tipo VLAN ou MACVLAN (endereços virtuais);

4.11.11. Deve ser permitido desabilitar uma política de segurança sem que seja necessário remove-la da lista;

4.11.12. A definição das políticas de segurança ainda deve permitir o administrador criar uma “tag” ou marcação similar para filtrar as pesquisas das regras. Este recurso deve ter a finalidade inclusive de auxiliar na composição do agrupamento das políticas em uma pesquisa;

4.11.13. A interação da interface ainda deve prover um recurso ou mecanismo para expandir a política, ou seja, permitir a visualização com as informações de filtros e a ação que compõe a regra;

4.12. VPN IPSEC

4.12.1. A solução deve prover comunicação através de túneis VPN “Virtual Private Network” ou “Rede virtual privada”. Ter como principal finalidade utilizar os recursos da rede pública “internet” para conectar redes remotas.

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

4.12.3. Deve suporte a VPN IPSEC Túnel lan to lan ou site to site;

4.12.4. Deve suportar VPN IPSEC RAS - Acesso remoto IPSEC;

4.12.5. Deve suportar os protocolos padrões de VPN: IPSEC, ESP, IKE e IKE versão 2;

4.12.6. A solução de VPN deve operar o padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

4.12.7. O suporte aos protocolos e algoritmos de autenticação e integridade IKEv1 e IKEv2 de acordo as RFC 7296, de modo a estabelecer canais de autenticação e criptografia com outros produtos que suportem tal padrão;

4.12.8. Deve possuir suporte a algoritmos de criptografia IKE: 3DES, AES, Blowfish;

4.12.9. Deve possuir suporte a algoritmos de integridade IKE: md5, sha1, sha256, sha384 e sha512;

4.12.10. Deve possuir suporte a algoritmos de criptografia ESP: DES, AES, Blowfish e Camélia;

4.12.11. Deve possuir suporte a algoritmos de integridade ESP: md5, sha1, sha2567, sha384, sha512, aesxcbc e aescmac;

4.12.12. Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;

4.12.13. A solução deve atender a suporte IKEv2 com suporte a fragmentação, de acordo a RFC 7383;

4.12.14. Deve possuir funcionalidade que permita estabelecer tuneis de VPN com Appliances da mesma solução ou outras soluções de VPN implementadas atrás de firewalls, através de encapsulamento UDP, de acordo a RFC 3947;

4.12.15. Implementar os esquemas de troca de chaves manual, para os protocolos IKE e IKEv2 através de chave compartilhada (Pré-Shared Key);

4.12.16. Suportar Main Mode e Aggressive mode em IKE v1;

4.12.17. Possuir funcionalidade Dead Peer Detection (DPD), ou similar;

4.12.18. Suportar VPN Redundante (Failover) reestabelecimento automático da VPN IPSEC sobre um segundo enlace caso haja falha no enlace principal);

4.12.19. Suporte a conexão por FQDN “Full Quality Domain Name”;

4.12.20. Compatibilidade e suporte a DDNS “Dinamic DNS”;

4.12.21. Deve permitir habilitar, desabilitar os tuneis de VPN IPSEC

4.12.22. Possuir suporte à inicialização IKE nos modos route, start e add, a partir da interface gráfica da solução;

4.12.23. A solução deve prover recursos de controle de conexão no tratamento do protocolo IKE que possibilite definir parâmetros dos tempos de vida das conexões e retransmissão e da autenticação IKE;

4.12.24. Deve permitir habilitar, desabilitar os tuneis de VPN IPSEC, facilitando o processo de throubleshooting;

4.12.25. O sistema de VPN IPSEC RAS deve funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs não válidos, colocando-os, virtualmente, em uma rede local estendida;

4.12.26. No modo VPN IPSEC RAS deve ser possível configurar o endereço/range IP a ser atribuída a interface de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;

4.12.27. O modo VPN IPSEC RAS deve suportar autenticação integrada X-Auth ((Integração Windows AD, PAM LDAP, e base de autenticação local) para usuários do firewall;

4.12.28. Deve possuir mecanismos de autenticação com suporte a EAP (MSCHAP2) para clientes VPN IPSEC Windows;

4.12.29. Compatibilidade com clientes VPN nativos para os sistemas operacionais iOS 7 ou superior, Android 4.4.4 ou superior, MacOS X 10.6 ou superior, Linux 2.6.36 ou superior, Windows 7 ou superior;

4.13. VPN SSL

4.13.1. A solução deve prover comunicação através de VPN SSL que permita um usuário remoto devidamente autorizado a utilizar um navegador WEB moderno para acessar com segurança diversos serviços da rede privada;

4.13.2. A solução deve suportar acesso com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPNs através da Internet;

4.13.3. A VPN SSL deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

4.13.4. O acesso deve oferecer versatilidade, facilidade de uso, e controles específicos de grupos e usuários em cada modalidade de aplicação e deve estar disponível através de um portal WEB.

4.13.5. Deve prover acesso via túnel SSL utilizando um navegador sem a necessidade de um cliente instalado na estação remota, e ser compatível no mínimo com o navegador Mozilla Firefox versão 47;

4.13.6. Deve ser compatível com as plataformas operacionais: MS-Windows, Linux, MacOS;

4.13.7. Deve possuir mecanismos de tunelamento de aplicações através de um portal web, com suporte a desvio de porta (Port Forward) para as aplicações internas;

4.13.8. Permitir acesso interno e externo ao portal WEB;

4.13.9. Deve suportar as seguintes modalidades de aplicações: Aplicações Túnel do tipo cliente-servidor, Aplicações de acesso remoto tais como: VNC, SSH, Terminal Service, Aplicações web do tipo HTTP e HTTPS, Compartilhamento de rede do tipo SMB;

4.13.10. Deve possuir suporte a autenticação integrada X-Auth (Integração Windows AD, PAM LDAP, e base de autenticação local) para usuários do firewall;

4.14. SERVIÇOS DE REDE (DDNS, DNS E DHCP):

4.14.1. A solução de UTM integrada deve fornecer um serviço de DDNS (Dynamic DNS);

4.14.2. Possuir suporte a publicação de hosts dinâmicos para os provedores de serviços: noIP e Dyndns;

4.14.3. Deve contemplar um mecanismo de atualização automática do DDNS por agendamento (update);

4.14.4. O serviço de DDNS deve ser compatível com Interface DSL ou PPOE;

4.14.5. O sistema também deve prover um recurso de redirecionamento DNS para provedores de DNS recursivo a fim de disponibilizar acesso a serviços de resolução de nomes remotos; permitir a consulta recursiva a partir dos redirecionamentos de DNS;

4.14.6. Permitir a configuração de acesso e redirecionamento por device de rede;

4.14.7. Suporte a cache de DNS;

4.14.8. Possuir mecanismos de proteção capaz de identificar ataques que disponibilizem servidores DNS válidos com autoridades sobre domínios configurados para responder um TTL (Time to live) muito baixo, inibindo a ação de guardar cache, o sistema deve possibilitar a proteção contra ataques que alteram a resposta a pesquisa de DNS para um endereço IP dinâmico de servidores com códigos maliciosos;

4.14.9. O sistema de proteção a este tipo de resposta (pesquisa de domínios com TTL muito baixo) deve possuir a opção de exceção para endereços de hosts locais e por domínios possibilitando especificar hosts e domínios confiáveis que não queira guardar cache;

4.14.10. Deve permitir DNS Redirect por listas de hosts;

4.14.11. A solução de UTM integrada deve fornecer um serviço de DHCP (Dynamic Host Configuration Protocol) Server;

4.14.12. Deve possuir mecanismo de configuração e distribuição de pool de endereços IPs por device de rede, com suporte a interfaces do tipo ethernet, VLAN, inclusive interface MACVLAN (Virtuais);

4.14.13. Deve permitir a distribuição do pool de endereços IPs por filtro de grupo ou objeto de endereço MAC; permitir a distribuição de endereço IP fixado ao endereço MAC.

4.14.14. A distribuição dos dados de configurações de serviços de rede deve contemplar a distribuição de Gateway ou roteamento, a definição de um sufixo de DNS; lista de endereço de servidores de DNS e servidores Wins;

4.14.15. Deve permitir a definição do tempo de vida do DHCP para a renovação do endereço IP entregue;

4.15. CLUSTER:

4.15.1. A solução deve suportar funcionamento com 2 (dois) ou mais equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo);

4.15.2. Os dois dispositivos devem ser ligados em paralelo, com réplicas das configurações entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal ficar inoperante;

4.15.3. Deverão ser capazes de manter o sincronismo de todos os itens de configuração e serviços, exemplo: Políticas de segurança, Configurações de segurança do firewall, Certificado de autoridade, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmico, Perfis, bases de antivírus, filtros web, IPS e ATP;

4.16. RELATÓRIOS

4.16.1. A geração de relatórios deve ser centralizada e disponibilizada através da interface WEB da solução e disposta em um painel de controle de gerenciamento.

4.16.2. A geração dos relatórios detalhados deve ser opcional e configurável por tipo de relatório: proxy, ataques e ameaças, aplicativos e firewall;

4.16.3. A solução deve disponibilizar a geração de relatórios acessíveis, fáceis de usar e baseados na web que ofereça visão em tempo real, relatórios sumarizados, gráficos e históricos detalhados.

4.16.4. Os relatórios devem propiciar ao administrador base concreta de análise fornecendo uma visão profunda de como a rede e os computadores estão sendo utilizados, permitindo-se entender e reforçar quando necessário as regras de conformidade.

4.16.5. A solução também deve através da interface de administração WEB, permitir administradores visualizar os relatórios dos usuários.

4.16.6. Acesso centralizado e consistente a todos os logs sumarizados e eventos do sistema com a opção de verificação “Diária” e “Mensal” dos registros e ainda com a opção de extração no formato “PDF” e “CSV”.

4.16.7. Suporte à geração em PDF para os relatórios estatísticos;

4.16.8. Deve ser capaz de gerar e manter os relatórios detalhados no mínimo por 7(sete) dias;

4.16.9. Deve suportar s exportação dos relatórios detalhados no formato CSV;

4.16.10. Possuir um mecanismo de arquivamento dos relatórios gerados para download, o arquivamento deve ser mantido pelo período mínimo de 1(hum) mês;

4.16.11. Possuir um serviço de manutenção de limpeza dos registros de estatísticas, e relatórios extraídos nos formatos CSV e PDF, mantendo os registros por um período mínimo de 30(trinta) dias;

4.16.12. A manutenção dos relatórios detalhados deve ser rotacional, automático e deve manter um período mínimo de 7 dias;

4.16.13. O sistema deve possuir um mecanismo de LOG que permita enviar os arquivos de log para outro servidor do tipo SYSLOG, especificando IP e porta;

4.16.14. Deve ser capaz de gerar relatório Online com (B.I) Business Intelligence para filtro na busca de relatórios;

4.16.15. Deve contemplar relação de eventos entre os itens de relatórios do proxy;

4.16.16. Deve contemplar relação de eventos entre os itens de relatórios das ameaças e aplicativos;

4.16.17. Deve contemplar relação de eventos entre os itens de relatórios dos atacantes;

4.16.18. A empresa fabricante da solução deve garantir que todos os relatórios detalhados devem ser assinados através de uma chave de integridade (key) que garanta a confiabilidade dos dados, atendendo ao Marco Civil nº 12.965/2014.

4.17. REGISTROS E LOGS DO SISTEMA:

4.17.1. Deve atender os registros e logs do sistema das respectivas informações de gerenciamento por dispositivo: Relatórios e gráficos gerais do sistema;

4.17.2. Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico diário por hora em (KB/ MB/ GB/ TB);

4.17.3. Gerar gráfico estatístico do sistema contendo informações do total de tráfego WEB via Proxy e histórico diário por hora em (KB/ MB/ GB/ TB);

4.17.4. Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo sistema de proteção de ameaças persistentes, tipo ATP e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

4.17.5. Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo sistema de prevenção de intrusos, tipo IPS (Inspection Prevention System) e contemplar inclusive um histórico diário por hora em (KB/ MB/ GB/ TB);

4.17.6. Gerar gráfico estatístico do sistema contendo informações do total de tráfego de rede e histórico mensal por dia em (KB/ MB/ GB/ TB);

4.17.7. Gerar gráfico estatístico do sistema contendo informações do total de tráfego WEB via Proxy e histórico mensal por dia em (KB/ MB/ GB/ TB);

4.17.8. Gerar gráfico estatístico do sistema contendo informações do total de ameaças e aplicativos detectados pelo ATP (Advanced Threats Protection) e histórico mensal por dia em (KB/ MB/ GB/ TB);

4.17.9. Gerar gráfico estatístico do sistema contendo informações do total de ataques detectados pelo IPS (Inspection Prevention System) e histórico mensal por dia em (KB/ MB/ GB/ TB);

4.17.10. Gerar histórico dos top 10 (dez) com o total do tráfego de rede em (KB/ MB/ GB/ TB) por: Usuários, Grupos, Serviços/Protocolos; Regras de conformidade; Categorias WEB;

4.17.11. Gerar histórico dos top 10 (dez) alertas de segurança dos ataques detectados pelo Firewall com o total de hits;

4.17.12. Gerar histórico dos top 10 (dez) aplicativos WEB (ATP) com o total de hits;

4.17.13. Gerar histórico das top 10 (dez) ameaças APT (Advanced Persistent Threats) detectados pelo ATP com o total de hits e classificação do tipo de impacto na rede;

4.17.14. Gerar histórico dos top 10 (dez) ataques detectados pelo (IPS) com o total de hits e classificação do tipo de impacto na rede;

4.17.15. Gerar gráfico estatístico do sistema contendo informações de desempenho como: (%) percentual de uso de processamento (CPU), (%) percentual de entrada/saída (I/O), (%) percentual de carga média (LOAD), (%) percentual de utilização de disco e (%) percentual de consumo de memória (RAM);

4.17.16. Gráfico estatístico do consumo de banda, mínimo de 5 (cinco) níveis de prioridade, em (B/ KB/ MB/ GB/ TB/);

4.17.17. Gráfico estatístico em tempo real do tráfego total da rede (RX/ TX);

4.17.18. Gráfico estatístico do sistema contendo histórico sobre o tráfego dos devices de rede (RX/ TX) e um serviço de monitoração em tempo real para cada device de rede;

4.17.19. A solução deve possuir um sistema de monitoração de tráfego para as novas conexões, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, e serviços com a especificação de porta e protocolo. O serviço de monitoração deve retornar os dados especificados nos filtros e a respectiva regra de conformidade;

4.17.20. A solução deve possuir um sistema de monitoração de tráfego para as conexões estabelecidas, podendo aplicar filtros por: endereço IP de origem, endereço IP de destino, serviços com a especificação de porta e protocolo, inclusive limitando o quadro de respostas até 50 (cinquenta) conexões estabelecidas. O serviço de monitoração deve retornar os dados especificados nos filtros, o total de tráfego em (KB/ MB/ GB/ TB), a velocidade em (bps/ kbps/ Mbps/ Gbps/ Tbps) e o número de pacotes trafegados;

4.18. RELATÓRIOS E GRÁFICOS GERAIS DO TRÁFEGO WEB VIA PROXY:

4.18.1. Gerar gráficos estatísticos do tráfego WEB via Proxy contendo as seguintes informações: total das requisições, total das requisições bloqueadas;

4.18.2. Gerar gráfico histórico ou resumo diário da relação de eventos entre o total de trafego WEB via Proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;

4.18.3. Gerar gráfico histórico ou resumo mensal da relação de eventos entre o total de tráfego WEB via Proxy dos acessos permitidos e os acessos bloqueados no intervalo de tempo de 1 (uma) hora;

4.18.4. Gerar gráfico histórico ou resumo diário da relação de eventos entre o total de trafego WEB via Proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (uma) hora;

4.18.5. Gerar gráfico ou resumo mensal do total da relação de eventos entre o tráfego WEB via Proxy dos acessos direto e os acessos ao cache no intervalo de tempo de 1 (hum) dia;

4.18.6. Gerar histórico dos top level 50 (cinquenta) com o total do tráfego em (KB/ MB/ GB/ TB) e o total dos acessos, com a opção de ordenação por tráfego e por acessos, das regras de conformidade permitidas e tipos de conteúdo permitidos;

4.18.7. Gerar histórico dos top level 50 (cinquenta) com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), e total de acessos, com a opção de ordenação por tráfego, por tempo, e por acessos, das categorias permitidas e aplicativos permitidos;

4.18.8. Gerar histórico dos top level 50 (cinquenta) “usuários” com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

4.18.9. Gerar histórico dos top level dos 50 (cinquenta), inclusive a relação de eventos entre “usuários” e as “categorias WEB” com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

4.18.10. Gerar histórico dos top level 50 (cinquenta), inclusive a relação de eventos entre os “usuários” e os “aplicativos WEB” com o total do tráfego em (KB/ MB/ GB/ TB), tempo em (horas/ minutos), Velocidade em (bps, Kbps/ Mbps/ Gbps/ Tbps), total de acessos permitidos e total de acessos bloqueados, com a opção de ordenação por tráfego, por tempo, permitidos e bloqueados;

4.18.11. Gerar histórico dos top level 50 (cinquenta), dos “bloqueados” com o total das tentativas de acesso, das regras de conformidade bloqueadas, categorias bloqueadas, aplicativos web bloqueados e tipos de conteúdo bloqueados;

4.18.12. A solução deve possuir um sistema de monitoração da navegação WEB via Proxy em tempo real por filtro do tipo: Servidor, origem (endereço IP ou usuário), URL de destino e porta de serviço. O serviço de monitoração deve retornar o tempo de tráfego em (hora/ minuto/ segundo), a origem (endereço IP ou usuário), o total de tráfego em (B/ KB/ MB/ GB/ TB), a velocidade em (bps/ Kbps/ Mbps/ Gbps/ Tbps) e a URL de destino;

4.19. RELATÓRIOS E GRÁFICOS GERAIS DO TRÁFEGO ATP:

4.19.1. Gerar gráficos estatísticos do tráfego ATP contendo as seguintes informações: total de ameaças detectadas, total de ameaças bloqueadas, total de aplicativos detectados, total de aplicativos bloqueados;

4.19.2. Gerar gráfico histórico ou resumo diário da relação de eventos entre o total de trafego ATP das ameaças detectadas a as ameaças bloqueadas no intervalo de tempo de 1 (uma) hora;

4.19.3. Gerar gráfico histórico ou resumo diário da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (uma) hora;

4.19.4. Gerar gráfico histórico ou resumo mensal da relação de eventos entre o total de trafego ATP das ameaças detectadas e as ameaças bloqueadas no intervalo de tempo de 1 (hum) dia;

4.19.5. Gerar gráfico histórico ou resumo mensal da relação de eventos entre o total de trafego ATP dos aplicativos detectados e os aplicativos bloqueados no intervalo de tempo de 1 (hum) dia;

4.19.6. Gerar gráficos estatísticos do tráfego ATP contendo as informações do total de ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

4.19.7. Gerar históricos ou resumos diários do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

4.19.8. Gerar históricos ou resumos mensais do total de tráfego ATP das ameaças e aplicativos detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

4.19.9. Gerar histórico do top level 50 (cinquenta) “detectados”, com o total de detecções e o tipo de impacto das ameaças e aplicativos;

4.19.10. Gerar histórico dos top level 50 (cinquenta), inclusive a relação de eventos entre as “ameaças” e os “usuários” com o tipo de impacto, total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

4.19.11. Gerar histórico dos top level 50 (cinquenta), inclusive a relação de eventos entre os “aplicativos” e os “usuários” com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

4.19.12. Gerar histórico dos top level 50 (cinquenta) “bloqueados” com o total das detecções, das ameaças e aplicativos;

4.20. RELATÓRIOS E GRÁFICOS GERAIS DO TRÁFEGO IPS:

4.20.1. Gerar gráficos estatísticos do tráfego IPS contendo as seguintes informações: total de ataques detectados, total de ataques bloqueados;

4.20.2. Gerar gráfico histórico ou resumo diário do total de trafego IPS da relação de eventos entre os “ataques detectados” e os “ataques bloqueados” no intervalo de tempo de 1 (uma) hora;

4.20.3. Gerar gráfico histórico ou resumo mensal do total de trafego IPS da relação de eventos entre os “ataques detectados” e dos “ataques bloqueados” no intervalo de tempo de 1 (hum) dia;

4.20.4. Gerar gráficos estatísticos do tráfego IPS contendo as informações do total dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de risco ou impacto;

4.20.5. Gerar gráficos históricos ou resumos diários do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (uma) hora;

4.20.6. Gerar gráficos históricos ou resumos mensais do total de tráfego IPS dos ataques detectados por grau de risco e impacto na rede, mínimo de 3 (três) tipos de graus de impacto no intervalo de tempo de 1 (hum) dia;

4.20.7. Gerar histórico dos tops 50 (cinquenta) “ataques detectados”, com o total de detecções e o tipo de risco ou impacto na rede;

4.20.8. Gerar histórico dos top level 50 (cinquenta), inclusive a relação de eventos entre os “ataques” e os “endereços IP ou usuários” com o tipo de risco ou impacto na rede,

total de detecções e o total de bloqueados, com a opção de ordenação por detecções e bloqueados;

4.20.9. Gerar histórico dos top level 50 (cinquenta), inclusive a relação de eventos entre o "grau de risco" e os "endereços IP ou usuários" com o total de detecções e o total de bloqueados, com a opção de ordenação por detecção e bloqueados;

4.20.10. Gerar histórico dos tops level 50 (cinquenta), "categorias de ataques" com o total das detecções, e total de bloqueados, com a opção de detalhar a categoria e identificar os endereços IPs ou usuários atacantes;

5. INSTALAÇÃO

5.1. A instalação dos Applainces UTM 8Gbps deverá ser feita pela contratada por pessoal devidamente certificado pelo fabricante.

5.2. A configuração inicial do sistema e integração com softwares já existente no ambiente do Procon deverá ser feita pela CONTRATADA

5.3. A CONTRATADA deverá instalar os equipamentos no prazo de até 30 dias corridos após a entrega dos equipamentos.

6. SUPORTE TÉCNICO

6.1. Os serviços e atendimentos de suporte técnico somente poderão ser realizados por técnicos especializados;

6.2. Os atendimentos deverão ser realizados por e-mail, telefone, presencialmente ou por meio de acesso remoto, de segunda a sexta-feira, das 07h00min às 19h00min;

6.3. Os serviços de suporte contemplam o funcionamento adequado do produto, aplicação de patches de correção e apoio na atualização das versões;

6.4. Os serviços de suporte incluem atender solicitações de suporte técnico relacionado a problemas, erros apresentados, formas de utilização da solução e correções necessárias para o restabelecimento de suas funcionalidades;

6.5. Os serviços de suporte incluem informações e orientações necessárias à atualização e ao perfeito funcionamento da solução;

6.6. Fornecimento, durante a vigência do contrato, garantia de hardware para os equipamentos Firewall propriedade do CONTRATANTE;

6.7. Durante a vigência do contrato, é de inteira responsabilidade da contratada substituir, sem ônus para o CONTRATANTE, todas as partes ou peças defeituosas, salvo

quando o defeito for provocado por uso inadequado dos equipamentos, devidamente comprovado;

6.8. Na eventualidade do CONTRATANTE necessitar os serviços de garantia de hardware, a contratada deverá disponibilizar para seu uso, durante o período em que o equipamento estiver em manutenção, outro firewall de capacidade igual ou superior, evitando a interrupção dos serviços de rede do CONTRATANTE.

7. ATUALIZAÇÕES

A CONTRATADA deverá fornecer, durante a vigência do contrato, a garantia de upgrade de versões e garantia de hardware (com direito a substituição de peças) para o firewall com assinatura válida por 36 (trinta e seis) meses;

8. TREINAMENTO

8.1. A CONTRATADA deverá fornecer treinamento completo da solução para os funcionários da CONTRATANTE com duração mínima de 40 horas podendo ser dividida em no máximo 4 horas diárias a ser agendado após a instalação, conforme disponibilidade da equipe do Procon – SP.

8.2. O treinamento deve ser o oficial do fabricante.

8.3. O treinamento deve ser feito na sede do Procon-SP localizado à Rua Barra Funda

8.4. Ao final do treinamento deverá ser emitido um certificado de conclusão para os participantes.

9. HABILITAÇÃO

9.1. Atestado de Capacidade Técnica, em nome da LICITANTE, expedido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de equipamentos similares aos ofertados serviços de instalação, configuração e suporte técnico, devendo estar explicita a marca, modelos e as quantidades fornecidas;

9.2. Declaração do Fabricante informando que a LICITANTE está autorizada a comercializar, instalar, configurar e prestar suporte técnico na solução ofertada;

9.3. Declaração do Fabricante informando que seu produto atende a todas as características e funcionalidades exigidas e contidas neste edital;

9.4. A LICITANTE deverá possuir técnicos certificados pelo Fabricante da solução para comprovar qualificação para execução do serviço.

Charles Eduardo da Silva Rodrigues
Assessor de Informática

ANEXO II – Minuta de Contrato

PROC FP 462/16 PREGÃO 19/16

CONTRATO XX/16

TERMO DE CONTRATO QUE ENTRE SI CELEBRAM **A FUNDAÇÃO DE PROTEÇÃO E DEFESA DO CONSUMIDOR - PROCON/SP** E A EMPRESA **XXXXXXX,** PARA FORNECIMENTO **DE SERVIÇOS de CONTROLE E ACESSO DE REDE – COM FORNECIMENTO DE FIREWALL INCLUSOS**

Aos XX dias do mês de XXX do ano de 2016, nesta cidade de São Paulo, compareceram de um lado a Fundação PROCON/SP, com sede na Rua Barra Funda, 930 – 4º andar – sala 432, inscrita no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda sob o nº 57.659.583/0001-84, neste ato representado por seu Diretor Adjunta de Administração e Finanças, Sr. Marcello Gonella de Andrade RG nº 16.298.872-2 e CPF 125.891.698-33, doravante denominada CONTRATANTE e de outro lado a empresa **XXXXXX**, inscrita no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda sob o nº XX.XXX.XXX/0001-XX, neste ato representada por XXXXX portadora do RG XXXXX e CPF XXXXXXX, neste ato denominada CONTRATADA, e pelos mesmos foi dito na presença das testemunhas ao final consignadas, que em face da adjudicação efetuada na licitação Pregão Eletrônico nº 19/16, o Processo FP 462/16, pelo presente instrumento avençam um contrato de **FORNECIMENTO DE SERVIÇOS de CONTROLE E ACESSO DE REDE – COM FORNECIMENTO DE APARELHOS (02) FIREWALL INCLUSOS,** sob o regime de empreitada por preço global, que será regido pela Lei Federal Nº 10.520, de 17 de julho de 2002, pelo Decreto Nº 49.722, de 24 de junho de 2005, pelo regulamento anexo a Resolução Nº CC-27, de 25/05/2006, aplicando-se, subsidiariamente, no que couberem, as disposições da Lei Federal Nº 8.666, de 21 de junho de 1993, da Lei Estadual Nº 6.544, de 22 de novembro de 1989, do Decreto estadual nº 47.297, de 06 de novembro de 2002, da Resolução CEGP-10, de 19 de novembro de 2002, e demais normas regulamentares aplicáveis à espécie e as seguintes cláusulas e condições que reciprocamente outorgam e aceitam:

Cláusula I - Do objeto

A CONTRATADA, nos termos de sua proposta e do edital do Pregão Eletrônico 19/16 em epígrafe e em tudo que com a mesma não colidir, obriga-se a prestar serviços de **FORNECIMENTO SERVIÇOS DE CONTROLE E ACESSO DE REDE COM 02 APARELHOS FIREWALL INCLUSOS, INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA, ATUALIZAÇÕES E SUPORTE/TREINAMENTO PARA 04 (QUATRO) PESSOAS,** conforme especificações constantes no Memorial Descritivo do mesmo Pregão, incluso todo o material e ferramental a ser utilizado, embalagem e entrega dos mesmos.

Parágrafo Primeiro – O objeto contratual executado deverá atingir o fim a que se destina, com a eficácia e a qualidade requeridas.

Parágrafo Segundo – O regime de execução deste contrato é o de empreitada por preço global.

Cláusula II - Do preço

Pelo fornecimento de cada aparelho FIREWALL especificado no Memorial Descritivo, marca xxx, modelo xxxx, a Fundação PROCON/SP pagará à CONTRATADA, o valor unitário de R$ xxxxxx (xxxxxx reais), pelo INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA FIREWALL UTM

a Fundação PROCON/SP pagará à CONTRATADA, o valor total de R$ xxxxxx (xxxxxx reais), pela ATUALIZAÇÃO E SUPORTE PELO PERÍODO DE 36 (TRINTA E SEIS) MESES, a Fundação PROCON/SP pagará à CONTRATADA, o valor total de R$ xxxxxx (xxxxxx reais) e pelo TREINAMENTO OFICIAL DA SOLUÇÃO COM DURAÇÃO MÍNIMA DE 40 (QUARENTA) HORAS para 04 (quatro) pessoas, a Fundação PROCON/SP pagará à CONTRATADA, o valor total de R$ xxxxxx (xxxxxx reais), sem qualquer reajuste.

Cláusula III - Dos recursos
O valor total deste contrato é de R$ XXX,00 (XXX reais) deverá onerar os elementos econômico 339039 referente à prestação de serviços e 449052 referente ao fornecimento dos aparelhos, todos na unidade orçamentária 17046, do orçamento vigente.

Cláusula IV - Dos prazos
A execução dos serviços (entrega do firewall) deverá ter início em até 10 (dez) dias, a contar da data de assinatura do contrato e não poderá ultrapassar o presente exercício.

A CONTRATADA deverá instalar os equipamentos no prazo de até 30 dias corridos após a entrega dos equipamentos.

A CONTRATADA deverá fornecer treinamento completo da solução para os funcionários da CONTRATANTE com duração mínima de 40 horas podendo ser dividida em no máximo 4 horas diárias a ser agendado após a instalação, conforme disponibilidade da equipe do PROCON/SP

Cláusula V – Da Garantia dos Aparelhos e do Serviço.
Os aparelhos FIREWALL terão um prazo de garantia de 12 (doze) meses.

A CONTRATADA deverá fornecer, durante a vigência do contrato, a garantia de upgrade de versões e garantia de hardware (com direito a substituição de peças) para o firewall com assinatura válida por 36 (trinta e seis) meses.

Cláusula VI - Das condições de pagamento
O valor devido será pago em conformidade com o estabelecido nos itens IX e X do edital da licitação.

Parágrafo Único – Constitui condição para a realização dos pagamentos a inexistência de registros em nome da Contratada no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais do Estado de São Paulo – CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento.

Cláusula VII - Das Sanções para o Caso de Inadimplemento
1. Ficará impedida de licitar e contratar com a administração direta e indireta do Estado de São Paulo, pelo prazo de até 05 (cinco) anos, a pessoa física ou jurídica, que praticar quaisquer atos previstos no artigo 7º da Lei Federal 10.520/02, cc artigo 15 da Resolução CEGP-10 de 19/11/02.

2. A Sanção que trata o subitem anterior poderá ser aplicada juntamente com as multas previstas na Resolução SJ 35/90, garantindo o exercício de previa e ampla defesa , e deverá ser registrada no CAUFESP e no sítio www.sancoes.sp.gov.br
Parágrafo Primeiro – A Contratante reserva-se o direito de descontar das faturas os valores correspondentes as multas que eventualmente forem aplicadas.

Parágrafo Segundo – As multas são autônomas e a aplicação de uma não exclui a de outra.

Cláusula VII - Da rescisão e Reconhecimento dos Direitos da Contratante
O presente Contrato poderá ser rescindido, na forma, com as conseqüências e pelos motivos previstos nos artigos 75 a 82 da Lei Estadual 6544/89 e artigos 77 a 80, 86 e 87 da Lei Federal 8666/93.

Parágrafo Primeiro – A Contratada reconhece desde já os direitos da Contratante em caso de rescisão administrativa prevista no art. 79 da Lei n.º 8.666/93 e no 77 da Lei Estadual 6544/89.

Parágrafo Segundo – O contrato será rescindido se firmado com sociedade cooperativa, de forma imediata, na hipótese de caracterização superveniente de prestação de trabalho nas condições de não eventualidade por pessoas físicas, com relação de subordinação ou dependência, em face da contratante (art. 1º do Decreto 55.938/10 alterado pelo Decreto 57159/11).

Cláusula VIII – Da Vigência
O presente contrato será vigente por 36 (trinta e seis) meses contados à partir da data de sua assinatura.

Cláusula IX – Da Subcontratação, Cessão ou Transferência dos Direitos e Obrigações Contratuais
É proibido à Contratada a subcontratação total ou parcial do objeto deste contrato, bem como sua cessão ou transferência total ou parcial.

Cláusula X – Da Garantia Contratual.
Não será exigida a prestação de garantia da execução contratual.

Cláusula XI – Obrigações da Contratada
1. Manter durante toda a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

2. Comunicar incontinente, por escrito, qualquer irregularidade constatada durante a vigência deste Contrato;

3. Responsabilizar-se com exclusividade por todos os ônus e/ou obrigações decorrentes da legislação da seguridade social, trabalhista, tributária, fiscal, securitária, comercial, civil e criminal, no que se relacionem com os serviços ora contratados, inclusive no tocante aos atos de seus empregados, dirigentes e prepostos;

4. Responder, por si e por seus sucessores, integralmente em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados ao CONTRATANTE ou a terceiros, por seus empregados ou serviços.

Cláusula XII – Obrigações da Contratante
1. A CONTRATANTE deverá fornecer ao CONTRATADO todas as informações necessárias à realização do serviço, devendo especificar os detalhes necessários à perfeita consecução

do mesmo, e a forma de como ele deve ser executado.

2. A CONTRATANTE deverá efetuar o pagamento na forma e condições estabelecidas na neste contrato.

Cláusula XIII – Do Local da Prestação de Serviços
O objeto desta licitação deverá ser executado na Fundação PROCON/SP, à Rua Barra Funda, 930 – Barra Funda – São Paulo/SP, em conformidade com o estabelecido no Anexo I deste Edital, correndo por conta da Contratada as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto do contrato.

Cláusula XII – Das Condições para o Recebimento do Objeto
1. A entrega do Firewall, a instalação e configuração do sistema, as atualizações, o suporte e treinamento deverão obedecer as condições e prazos estabelecidos no Memorial Descritivo.

Cláusula XVI - Do foro
Para as questões que surgirem em virtude da presente contratação e que não forem resolvidas administrativamente, será competente o Foro da Cidade de São Paulo.

Cláusula XVII – Das Disposições Finais

Fica ajustado, ainda que:

I – Consideram-se partes integrantes do presente contrato, como se nele estivessem transcritos:

a) o Edital do Pregão Eletrônico 19/16 e seus anexos;
b) a PROPOSTA apresentada pela CONTRATADA;
c) a Resolução SJ 35/90

II – Aplicam-se às omissões deste contrato as disposições da Lei Estadual nº 10.520/02, Decreto 49.722/05, o Regulamento anexo à Resolução CC-27 de 25/05/2006, do Decreto Estadual 47.292/02, da Lei Federal nº 8.666/93, e as normas regulamentares.

E assim, por estarem às partes justas e contratadas, foi lavrado o presente instrumento em 02 (duas) vias de igual teor e forma que lido e achado conforme pelas PARTES, vai por elas assinado para que produza todos os efeitos de direito, na presença das testemunhas abaixo identificadas.

Fundação de Proteção e Defesa do Consumidor – PROCON/SP
MARCELLO GONELLA DE ANDRADE

FORNECEDOR

Testemunha 1 Testemunha 2

ANEXO III – MODELO DE DECLARAÇÃO (ÕES) PARA PREGÃO ELETRONICO

PAPEL TIMBRADO DA EMPRESA

À

Fundação Procon

Pregão Eletrônico 19/16

Processo FP 462/16

_____(nome da pessoa jurídica) por seu representante legal abaixo assinado declara que se encontra em situação regular perante o Ministério do Trabalho no que refere ao disposto no inciso XXXIII do artigo 7º da Constituição Federal; que inexiste Impedimento Legal para Licitar ou Contratar com a Administração, inclusive em virtude das disposições da Lei Estadual 10.218, de 12/02/1999; que atende às normas relativas à saúde e segurança do trabalho conforme parágrafo único, do art. 117 da Constituição do Estado; que o produto que oferta atende a todas as características e funcionalidades exigidas e contidas no edital de pregão eletrônico especificado e que possui técnicos certificados pelo Fabricante da solução para comprovar qualificação para execução do serviço.

Local, ____ de _____ de 2.016

_____
Nome e assinatura do representante
legal /carimbo da empresa

ANEXO IV – RESOLUÇÃO SJ 35/90

PREGÃO 19/16 - PROC FP 462/16

RESOLUÇÃO SJ 35 DE 11/09/1990

O Secretário da Justiça, resolve:

Artigo 1º - A aplicação das multas a que se refere os artigos 79, 80, parágrafo 2º e 81, inciso II da Lei 6.544/89, obedecerá, no âmbito da Pasta, às seguintes normas:
I – Pela recusa injustificada em assinar o contrato dentro do prazo estabelecido pela Administração, multa de 5%a 30% do valor do ajuste.
II – Pelo atraso injustificado na execução do contrato:
Em se tratando de compras e serviços:
1 – atraso até 30 dias, multa de 0,2% sobre o valor da obrigação por dia de atraso;
2 – atraso superior a 30 dias, multa de 0,4% sobre o valor da obrigação, por dia de atraso.
Em se tratando de obras e serviços a estas vinculadas, multa de 0,1% sobre o valor da obrigação, por dia de atraso.
III – O valor do ajuste a servir de base de cálculo para as multas referidas nos incisos I e II, será o valor original reajustado até a data de aplicação da penalidade.
IV – Pela inexecução total ou parcial do ajuste:
- Multa de 10% a 30%, calculada sobre o valor das mercadorias, serviços ou obras não entregues ou da obrigação não cumprida.
- Multa correspondente à diferença de preço resultante da nova licitação realizada para complementação ou realização da obrigação não cumprida.

Parágrafo 1º - Se a multa for superior ao valor da garantia prestada, alem da perda desta, responderá o contratado pela diferença que será descontada dos pagamentos eventualmente devidos pela Administração ou cobradas judicialmente.
Parágrafo 2º - As disposições anteriores aplicam-se, também, às aquisições, serviços ou obras que, nos termos da legislação, forem realizados com dispensa de licitação.
Parágrafo 3º - As penalidades mencionadas nas alíneas "a" e "b" do inciso IV são alternativas, devendo a Administração optar, a seu critério, por uma delas.
Parágrafo 4º - AS normas estabelecidas nesta resolução deverão constar, obrigatoriamente, em todos instrumentos convocatórios das licitações e nos contratos sobre fornecimento ou serviços.
Artigo 2º - As multas previstas nesta resolução serão corrigidas monetariamente, consoante o índice oficial, até a data de seu recolhimento.
Artigo 3º - Da aplicação das multas previstas na resolução, caberá recurso no prazo de cinco dias úteis, consoante o disposto no artigo 83, inciso I, alínea "e" e parágrafos 1º e 2º , da lei 6544/89.
Artigo 4º - As multas são autônomas e a aplicação de uma não exclui a da outra.
Artigo 5º - Esta Resolução entrará em vigor na data de sua publicação, ficando revogada a Resolução SJ 215 de 28/12/1978.

ANEXO V – MODELO DE PROPOSTA DE PREÇOS

PREGÃO 19/16 - PROC FP 462/16

Papel timbrado

Descrição	Qtdade	Valor UNITÁRIO	VALOR TOTAL SUBITEM
Firewall UTM de 8Gbps de capacidade de firewall marca xxxxxxxxxx – modelo xxxxxxxxxx	**2 unidades**	**R$ xx,00**	**R$ xx,00**
Instalação e Configuração do Firewall UTM	**40 horas**	**R$ xx,00**	**R$ xx,00**
Atualização e Suporte 12x5	**36 meses**	**R$ xx,00**	**R$ xx,00**
Treinamento Oficial da solução com duração mínima de 40 horas	**4 pessoas**	**R$ xx,00**	**R$ xx,00**

Especificar marca/modelo

OBS:

*** VALOR TOTAL = 2 UNIDADES DE FIREWALL + INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA + ATUALIZAÇÕES E SUPORTE + TREINAMENTO/4 PESSOAS =**
*** R$ XX,00 (valor total por extenso)**

O * VALOR TOTAL SERÁ UTILIZADO PARA NEGOCIAÇÃO NA SESSÃO PÚBLICA/PREGÃO ELETRÔNICO

ESTA PLANILHA DE PREÇOS SERÁ ENVIADA SOMENTE PELO LICITANTE VENCEDOR JUNTO COM OS DOCUMENTOS PARA HABILITAÇÃO.

O FORNECEDOR TERÁ QUE EMITIR, OBRIGATORIAMENTE, 02 (DUAS) NOTAS FISCAIS SENDO: 1 REFERENTE A EXECUÇÃO DOS SERVIÇOS E 1 REFERENTE AO FORNECIMENTO DOS PRODUTOS (FIREWALL)

Local, data, assinatura e carimbo do responsável