PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO

CONTRATO TRT 16ª REG. Nº 07/2012
PA Nº 4345/2012

CONTRATO QUE ENTRE SI CELEBRAM A UNIÃO POR INTERMÉDIO DO TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO E A EMPRESA DAMOVO DO BRASIL S/A PARA AQUISIÇÃO DE SOLUÇÃO DE CLUSTER DE FIREWALLS PARA CONEXÃO À REDE CORPORATIVA DA JUSTIÇA DO TRABALHO (PROCESSO TST nº 502.793/2011-5).

Pelo presente instrumento particular, a **UNIÃO** por intermédio do **TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO**, com sede na Avenida Senador Vitorino Freire, 2001, Areinha, nesta cidade, CNPJ nº 23.608.631/0001-93, doravante denominado **CONTRATANTE**, neste ato, representado pela Exma. Desembargadora Presidente, **ILKA ESDRA SILVA ARAÚJO** e, de outro lado, a empresa **DAMOVO DO BRASIL S/A**, CNPJ n.º 56.795.362/0001-70 com sede na Alameda Santos, nº 200, Bairro Cerqueira César, São Paulo - SP, neste ato, representada por **ANTENOR PAGLIONE JUNIOR,** brasileiro, casado, Diretor Comercial, RG 7802961-2 SSPSP, inscrito no CPF sob o nº 062.516.138-66 e por **EDSON ALVES MENINI**, brasileiro, casado, Diretor Financeiro, RG 7696371-8 SSPSP, inscrito no CFP sob o nº 044.109.308-69, e daqui por diante designada **CONTRATADA**, ajustam entre si este Contrato, de acordo com o constante no PA nº 4345/2012, mediante utilização, como participante, da Ata de Registro de Preços gerenciada pelo Tribunal Superior do Trabalho, vinculada ao Pregão Eletrônico n.º 026/2012, pelo Sistema de Registro de Preços, conforme Processo TST nº 502.793/2011-5, regida pelas disposições contidas na Lei Complementar nº 123 de 14/12/2006, na Lei n.º 10.520 de 17/07/2002 e Decretos n.^{os} 3.931/2001, 5.450/2005 e 6.204/2007, e, subsidiariamente, pela Lei n.º 8.666/93 e alterações posteriores, e sob as condições estabelecidas neste instrumento, o qual se regerá mediante as seguintes cláusulas e condições adiante discriminadas.

CLÁUSULA PRIMEIRA - DOS FUNDAMENTOS LEGAIS DO CONTRATO

Este contrato fundamenta-se:

I. no Pregão Eletrônico n.º 026/2012, conforme a Lei Complementar n.º 123/2006, a Lei n.º 10.520/2002 e os Decretos n.os 3.931/01, 5.450/2005 e 6.204/07;

II. nos termos propostos pela Contratada que, simultaneamente:

a) constem no Processo Administrativo TST n.º 502.793/2011-5;

b) não contrariem o interesse público.

III. nas determinações das Leis n.os 8.666/93, 8.078/90 e 9.784/99;

IV. nos preceitos de direito público;

V. supletivamente, nos princípios da teoria geral dos contratos e nas disposições do direito privado.

CLÁUSULA SEGUNDA - DO OBJETO

Este contrato tem por objeto a de solução de Cluster de Firewalls para conexão à Rede Corporativa da Justiça do Trabalho, conforme especificações na tabela abaixo, nos termos e condições constantes no edital e neste contrato e seus anexos.

Item	Especificação		Unidade	Quantidade	Valor Unitário (R$)	Valor Total (R$)
2	Cluster failover de firewalls com dois nós (descrição conforme Anexo I - tipo 2) Marca: Cisco Modelo: ASA 5585-X Chas w/SSP10, IPS SSP10	Hardware (material permanente)	Un	01	114.540,10	210.929,98
		Software (Licenças)	Un	01	2.220,88	
		Serviços (Garantia, Suporte Técnico e Treinamento)	Un	01	94.169,00	

CLÁUSULA TERCEIRA - DA GARANTIA DO OBJETO

O objeto deste contrato tem garantia contra defeitos de fabricação de 36 (trinta e seis) meses, contados a partir do recebimento definitivo do objeto pelo **CONTRATANTE**, conforme o Termo de Garantia anexo, que terá vigência independente do prazo da vigência do contrato.

CLÁUSULA QUARTA - DA VIGÊNCIA

A vigência deste contrato é da data de sua assinatura até 90 (noventa) dias após o recebimento definitivo do objeto.

Subcláusula única. O prazo acima referido terá início e vencimento em dia de expediente, excluído o primeiro e incluído o último, e terá validade e eficácia legal após a publicação do extrato deste contrato no Diário Oficial da União.

CLÁUSULA QUINTA - DO VALOR

O valor total deste contrato é de R$ 210.929,98 (duzentos e dez mil, novecentos e vinte e nove reais e noventa e oito centavos).

Subcláusula única. Já estão incluídas no preço total todas as despesas de frete, embalagens, impostos, transporte, mão-de-obra e demais encargos indispensáveis ao perfeito cumprimento das obrigações decorrentes deste contrato.

CLÁUSULA SEXTA - DO REAJUSTE

Os preços ofertados para os itens do objeto deste contrato serão fixos e irreajustáveis, nos termos da legislação em vigor.

CLÁUSULA SÉTIMA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas oriundas deste contrato correrão à conta dos recursos orçamentários consignados ao **CONTRATANTE** por descentralização de crédito do Conselho Superior da Justiça do Trabalho, conforme autorizado no Processo TST - 502.280/2012-0, Natureza das Despesas 4490.52, 4490.39 e 3390.39, Notas de Empenho 2012NE000881, 2012NE000882 e 2012NE000884, emitidas em 20/07/2012.

CLÁUSULA OITAVA - DOS PRAZOS

A **CONTRATADA** deverá cumprir prazo de entrega dos equipamentos e implantação de, no máximo, 45 (quarenta e cinco) dias, contados da assinatura deste contrato, bem como cumprir aos demais prazos especificados neste instrumento.

Subcláusula primeira. A **CONTRATADA** deverá concluir o treinamento no prazo de, no máximo, 30 (trinta) dias, contados a partir da implantação da solução no **CONTRATANTE**.

Subcláusula segunda. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no parágrafo 1º do artigo 57 da Lei n.º 8.666/93, e a solicitação dilatória, sempre por escrito, fundamentada e instruída com os documentos necessários à comprovação das alegações, deverá ser recebida contemporaneamente ao fato que a ensejar.

Subcláusula terceira. A solicitação de prorrogação deverá ser encaminhada com antecedência mínima de três dias do vencimento, anexando-se documento comprobatório do alegado pela Contratada.

CLÁUSULA NONA - DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

A execução das obrigações contratuais terá como gestor o servidor Ary Arruda Gomes de Sá Filho, Diretor de Informática, e como fiscal o servidor Fernando Augusto Pestana Júnior, que terão autoridade para exercer, como representantes do **CONTRATANTE**, toda e qualquer ação de orientação geral, acompanhamento e controle da execução contratual.

Subcláusula primeira. À Fiscalização compete, entre outras atribuições:

I. solicitar à **CONTRATADA** e seus prepostos, ou obter do **CONTRATANTE**, tempestivamente, todas as providências necessárias ao bom andamento deste contrato e anexar aos autos do processo correspondente

cópia dos documentos escritos que comprovem essas solicitações de providências;
II. manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica;
III. acompanhar e atestar a execução, bem assim indicar as ocorrências verificadas;
IV. encaminhar à Diretoria-Geral os documentos que relacionem às ocorrências que impliquem possíveis sanções punitivas a serem aplicadas à **CONTRATADA**.

Subcláusula segunda. A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

CLÁUSULA DEZ - DO RECEBIMENTO E DA ACEITAÇÃO DOS SERVIÇOS

O objeto do presente contrato será recebido das seguintes formas:
I. provisoriamente, mediante recibo, imediatamente após efetuada a entrega, instalação ou treinamento, para efeito de posterior verificação de sua conformidade;
II. definitivamente, mediante recibo, em até dez dias úteis após o recebimento provisório e a verificação da perfeita execução nos termos contratuais, quanto à adequação dos equipamentos e execução dos serviços de implantação ou treinamento, ocasião em que se fará constar o ateste da nota fiscal.

Subcláusula primeira. A execução do objeto em desconformidade com o especificado neste contrato, no instrumento convocatório ou no indicado na proposta será rejeitada parcial ou totalmente, conforme o caso, e a **CONTRATADA** será obrigada a refazê-la no prazo estipulado pela gestão/fiscalização, contado da data do recebimento de notificação escrita necessariamente acompanhada do Termo de Recusa, sob pena de incorrer em atraso quanto ao prazo de execução.

Subcláusula segunda. A notificação referida na subcláusula anterior suspende os prazos de recebimento e de pagamento até que a irregularidade seja sanada.

Subcláusula terceira. A **CONTRATADA** ficará obrigada a trocar, a suas expensas, os produtos que vierem a ser recusados.

Subcláusula quarta. Independentemente da aceitação, a **CONTRATADA** garantirá a qualidade de cada unidade do produto pelo prazo estabelecido na respectiva garantia pelo fabricante, e estará obrigada a substituir aquela que apresentar defeito no prazo estabelecido pelo **CONTRATANTE**.

CLÁUSULA ONZE - DO PAGAMENTO

Os pagamentos serão efetuados, em moeda corrente nacional, em até dez dias úteis após a apresentação das notas fiscais devidamente atestadas pela Gestão/Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável, da seguinte forma:
I. 30% (trinta por cento) após a entrega dos equipamentos;
II. 20% (vinte por cento) após a realização dos serviços de instalação e implantação;

III. 20% (vinte por cento) após a conclusão do treinamento;
IV. 30% (trinta por cento) após o recebimento definitivo.

Subcláusula primeira. As notas fiscais e os documentos exigidos no edital e neste contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Diretoria de Material e Patrimônio do **CONTRATANTE**.

Subcláusula segunda. A nota fiscal deve corresponder ao objeto recebido e a Gestão/Fiscalização, no caso de divergência, especialmente quando houver adimplemento parcial, deve notificar a **CONTRATADA** a substituí-la em até três dias úteis, com suspensão do prazo de pagamento.

Subcláusula terceira. A **CONTRATADA** deverá entregar todo o material solicitado por meio da nota de empenho, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento total da obrigação.

Subcláusula quarta. A retenção dos tributos não será efetuada caso a **CONTRATADA** apresente, junto com sua nota fiscal, a comprovação de que é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte - SIMPLES.

Subcláusula quinta. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação regular em relação à Fazenda Federal, ao INSS e ao FGTS, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

Subcláusula sexta. O **CONTRATANTE** pagará à **CONTRATADA** a atualização monetária sobre o valor devido entre a data do adimplemento das obrigações contratuais e a do efetivo pagamento, excluídos os períodos de carência para recebimento definitivo e liquidação das despesas previstos neste contrato, utilizando o índice publicado pela Fundação Getúlio Vargas que represente o menor valor acumulado no período, desde que a **CONTRATADA** não tenha sido responsável, no todo ou em parte, pelo atraso no pagamento.

CLÁUSULA DOZE - DAS OBRIGAÇÕES DA CONTRATADA

Na execução do objeto do presente contrato, obriga-se a **CONTRATADA** a envidar todo o empenho necessário ao fiel e adequado cumprimento dos encargos que lhe são confiados e, ainda, a:

I. entregar os produtos objeto contratual e executar os serviços nos prazos e demais condições estabelecidas neste contrato e seus anexos;
a) os bens deverão ser industrializados, novos e entregues, no prédio-sede do **CONTRATANTE**, acondicionados adequadamente em suas embalagens originais lacradas;
b) os equipamentos deverão ser fornecidos com todos os itens acessórios de hardware e software necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle, programas de configuração etc;
c) os equipamentos deverão estar acompanhados de sua documentação técnica completa e atualizada, contendo os manuais, guias de instalação e outros pertinentes, observado que a documentação deverá ser fornecida em sua forma original, não sendo aceitas cópias de qualquer tipo;

d) é necessária a entrega de documentação ao **CONTRATANTE**, contendo: as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente, etc...); acesso à área de suporte técnico através de endereço eletrônico (web site) do fabricante do equipamento; devendo observar que a documentação deverá ser entregue junto com os equipamentos.

II. cumprir todos os requisitos descritos neste instrumento, responsabilizando-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para o **CONTRATANTE**;

III. reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto deste contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços;

IV. respeitar o sistema de segurança do **CONTRATANTE** e fornecer todas as informações solicitadas por ele;

V. acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades;

VI. guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do **CONTRATANTE**, sendo vedada à **CONTRATADA**, sua cessão, locação ou venda a terceiros;

VII. utilizar padrões definidos em conjunto com o **CONTRATANTE** (nomenclaturas, metodologias, etc.);

VIII. indenizar crachás confeccionados pelo **CONTRATANTE**, quando em caso de perda/extravio;

IX. responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez inexistir, no caso, vínculo empregatício deles com o **CONTRATANTE**;

X. responder, integralmente, por perdas e danos que vier a causar diretamente ao **CONTRATANTE** ou a terceiros, em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

Subcláusula primeira. A **CONTRATADA** deverá efetuar, após a entrega do objeto, a instalação física da solução proposta no **CONTRATANTE**, bem como configurá-la de tal forma que mantenha o perfeito funcionamento da rede do **CONTRATANTE**, atendendo os requisitos deste contrato e seus anexos;

I. A implantação consistirá na substituição das atuais soluções de firewall pela que for contratada por meio deste contrato;

a) a **CONTRATADA** deverá efetuar a troca física da solução atual pela nova, inclusive cabeamentos elétricos e lógicos que se fizerem necessários;

b) os cabos elétricos, cabos UTP, plugues e conectores utilizados na nova solução que não puderem ser aproveitados da atual e que não estejam previstos nesta contratação, serão fornecidos pelo **CONTRATANTE**, sem prejuízo para a **CONTRATADA**;

c) caberá à **CONTRATADA** migração de todas as configurações das soluções em uso no **CONTRATANTE** para a nova solução;

d) o serviço de implantação só será considerado concluído após a entrada em operação no ambiente de produção do **CONTRATANTE**.

Subcláusula segunda. A **CONTRATADA** deverá oferecer programa de capacitação para o corpo técnico do **CONTRATANTE**, abordando os assuntos: instalação, configuração e gerenciamento da solução proposta.

I. A especificação detalhada do programa de capacitação consta descrita no anexo III.

Subcláusula terceira. A **CONTRATADA** deverá prestar assistência técnica durante o período de garantia de 36 (trinta e seis) meses, contados a partir do recebimento definitivo, nos prazos e forma a seguir:

I. a assistência técnica em garantia consistirá na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças e componentes que se apresentarem defeituosos, de acordo com os manuais e normas técnicas específicas para os equipamentos; acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) do fabricante do equipamento, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações ("update" e "upgrade") de todos os componentes de software do sistema;

II. garantir assistência técnica credenciada pelo fabricante dos equipamentos, capaz de atender nos locais de entrega dos equipamentos com, no mínimo, uma central de assistência técnica;

III. a assistência técnica utilizará apenas peças e componentes originais salvo nos casos fundamentados por escrito e aceitos pelo **CONTRATANTE**;

IV. a assistência técnica em garantia será prestada na modalidade "on-site";

V. a partir da comunicação do(s) defeito(s) pelo **CONTRATANTE**, conforme sistema de registro próprio do **CONTRATANTE**, o início do atendimento e término do reparo do(s) equipamento(s) serão de até 2 horas e 24 horas, respectivamente;

VI. a assistência técnica em garantia será realizada de segunda-feira a sexta-feira, no horário das 7:30h às 17:30h, a pedido do **CONTRATANTE**;

VII. a abertura de chamados será efetuada por correio eletrônico e por telefone, sendo que no caso de abertura através de telefone, o contato será efetuado por meio de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800) ou números locais no município de entrega dos equipamentos;

a) em ambos os casos, o atendimento deverá ser efetuado em língua portuguesa;

VIII. o acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível vinte e quatro horas por dia, sete dias por semana;

IX. o término do reparo do equipamento não poderá ultrapassar o prazo previsto, caso contrário deverá ser providenciado pela **CONTRATADA** a colocação de equipamento equivalente ou de superior configuração como backup, até que seja sanado o defeito do equipamento;

X. durante o período de garantia, os equipamentos que apresentarem inoperância, em duas ocasiões separadas por no máximo um período de sessenta dias corridos, devem ser substituídos;

XI. durante o período de garantia, os equipamentos que apresentaram funcionamento irregular, em desacordo com aquele especificado pelo fabricante, em duas ocasiões separadas por até sessenta dias corridos, devem ser substituídos.

Subcláusula quarta. A **CONTRATADA** não será responsável:

I. por qualquer perda ou dano resultante de caso fortuito ou força maior;

II. por quaisquer trabalhos, serviços ou responsabilidades não previstos neste instrumento.

Subcláusula quinta. O **CONTRATANTE** não aceitará, sob pretexto algum, a transferência de responsabilidade da **CONTRATADA** para outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

CLÁUSULA TREZE - DAS OBRIGAÇÕES DO CONTRATANTE

O **CONTRATANTE**, durante a vigência deste contrato, compromete-se a:
I. proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitir o acesso dos funcionários da **CONTRATADA** às dependências do **CONTRATANTE** relacionadas à execução dos serviços;
II. promover os pagamentos dentro do prazo estipulado neste contrato;
III. fornecer atestados de capacidade técnica quando solicitados, desde que atendidas às obrigações contratuais.

CLÁUSULA QUATORZE - DA GARANTIA DO CONTRATO

Para segurança do **CONTRATANTE** quanto ao cumprimento das obrigações contratuais, a **CONTRATADA** deverá optar, no montante de 5% (cinco por cento) do valor total do contrato, por uma das seguintes modalidades de garantia:

I. caução em dinheiro ou em títulos da dívida pública, devendo estes terem sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;
II. seguro-garantia;
III. fiança bancária.

Subcláusula primeira. A **CONTRATADA** deverá providenciar a garantia contratual impreterivelmente em 5 (cinco) dias úteis, contados do recebimento da convocação para assinatura do contrato, sob pena de ser-lhe imputada multa conforme Subcláusula quarta da Cláusula Quinze.

Subcláusula segunda. É de inteira responsabilidade da **CONTRATADA** a renovação da garantia prestada, quando couber, estando sua liberação condicionada ao término das obrigações contratuais, incluindo todo o período de prestação de serviços de assistência técnica em garantia.

CLÁUSULA QUINZE - DAS PENALIDADES SOBRE A CONTRATADA

No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com o **CONTRATANTE**, as sanções administrativas aplicadas à **CONTRATADA** serão:

I. advertência;
II. multa;
III. suspensão temporária de participar de licitações e impedimento de contratar com a Administração Pública;

IV. declaração de inidoneidade para licitar ou contratar com a Administração Pública.

Subcláusula primeira. O atraso injustificado na execução contratual implicará multa correspondente a 1% (um por cento) por dia de atraso, calculado sobre o valor do objeto em atraso, até o limite de 30% (trinta por cento) do respectivo valor total.

Subcláusula segunda. Nesta hipótese mencionada na Subcláusula anterior, o atraso injustificado por período superior a 30 dias caracterizará o descumprimento total da obrigação, punível com as sanções previstas nos incisos III e IV do caput desta Cláusula, como também a inexecução total do contrato.

Subcláusula terceira. O atraso injustificado no início do atendimento técnico no período de garantia implicará multa de 1% (um por cento) do valor do equipamento faturado na nota fiscal entregue ao **CONTRATANTE**, por hora de atraso, para cada equipamento em que houver atraso, até o limite de 20% do valor do contrato, punível com as sanções previstas nos incisos III e IV do caput desta Cláusula, como também a inexecução total do contrato.

Subcláusula quarta. No caso de atraso no cumprimento do prazo para apresentação da garantia contratual, assinalado na Subcláusula primeira da Cláusula quatorze deste contrato, será aplicada multa de 0,5% (cinco décimos por cento) ao dia sobre o valor adjudicado, até o limite de 15% (quinze por cento).

Subcláusula quinta. As multas porventura aplicadas serão descontadas dos pagamentos devidos pelo Contratante, da garantia contratual ou cobradas diretamente da empresa, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

Subcláusula sexta. Aquele que ensejar o retardamento da execução do objeto contratual, não mantiver a proposta, falhar ou fraudar sua execução, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, e será descredenciado do SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste contrato e no edital e das demais cominações legais, conforme disposto no artigo 28 do Decreto n.º 5.450/2005.

Subcláusula sétima. As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para a **CONTRATADA**, na forma da lei.

CLÁUSULA DEZESSEIS - DAS CONDIÇÕES DE HABILITAÇÃO DA CONTRATADA

A **CONTRATADA** declara, no ato de celebração deste contrato, estar plenamente habilitada à assunção dos encargos contratuais e assume o compromisso de manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação.

CLÁUSULA DEZESSETE - DA PUBLICAÇÃO

A publicação resumida deste contrato na Imprensa Oficial, que é condição indispensável para sua eficácia, será providenciada pelo Contratante, nos termos do parágrafo único do artigo 61 da Lei n.º 8.666/93.

CLÁUSULA DEZOITO - DAS ALTERAÇÕES DO CONTRATO

Competem a ambas as partes, de comum acordo, salvo nas situações tratadas neste instrumento, na Lei n.º 8.666/93 e em outras disposições legais pertinentes, realizar, via termo aditivo, as alterações contratuais que julgarem convenientes.

CLÁUSULA DEZENOVE - DA RESCISÃO

Constituem motivos incondicionais para rescisão do contrato as situações previstas nos artigos 77 e 78, na forma do artigo 79, inclusive com as conseqüências do artigo 80, da Lei n.º 8.666/93.

CLÁUSULA VINTE - DA UTILIZAÇÃO DO NOME DO CONTRATANTE

A **CONTRATADA** não poderá, salvo em curriculum vitae, utilizar o nome do **CONTRATANTE** ou sua qualidade de **CONTRATADA** em quaisquer atividades de divulgação profissional como, por exemplo, em cartões de visita, anúncios diversos, impressos etc., sob pena de imediata rescisão deste contrato.

Subcláusula única. A **CONTRATADA** não poderá, também, pronunciar-se em nome do **CONTRATANTE** à imprensa em geral sobre quaisquer assuntos relativos às atividades deste, bem como a sua atividade profissional, sob pena de imediata rescisão contratual e sem prejuízo das demais cominações cabíveis.

CLÁUSULA VINTE E UM - DOS CASOS FORTUITOS, DE FORÇA MAIOR OU OMISSOS

Tal como prescrito na lei, o **CONTRATANTE** e a **CONTRATADA** não serão responsabilizados por fatos comprovadamente decorrentes de casos fortuitos ou de força maior, ocorrências eventuais cuja solução se buscará mediante acordo entre as partes.

CLÁUSULA VINTE E DOIS - DAS DISPOSIÇÕES FINAIS

A Administração do **CONTRATANTE** analisará, julgará e decidirá, em cada caso, as questões alusivas a incidentes que se fundamentem em motivos de caso fortuito ou de força maior.

Subcláusula primeira. Para os casos previstos no caput desta cláusula, o **CONTRATANTE** poderá atribuir a uma comissão, por este designada, a responsabilidade de apurar os atos e fatos comissivos ou omissivos que se fundamentem naqueles motivos.

Subcláusula segunda. Os agentes públicos responderão, na forma da lei, por prejuízos que, em decorrência de ação ou omissão dolosa ou culposa, causarem à

Administração no exercício de atividades específicas do cumprimento deste contrato, inclusive nas análises ou autorizações excepcionais constantes nestas disposições finais.

Subcláusula terceira. As exceções aqui referenciadas serão sempre tratadas com máxima cautela, zelo profissional, senso de responsabilidade e ponderação, para que ato de mera e excepcional concessão do Contratante, cujo objetivo final é o de atender tão-somente ao interesse público, não seja interpretado como regra contratual.

Subcláusula quarta. Para assegurar rápida solução às questões geradas em face da perfeita execução deste contrato, a Contratada fica desde já compelida a avisar, por escrito e de imediato, qualquer alteração em seu endereço ou telefone.

Subcláusula quinta. No curso do contrato, é admitida a fusão, cisão ou incorporação da empresa, bem assim sua alteração social, modificação da finalidade ou da estrutura, desde que não prejudique a execução do contrato, cabendo à Administração decidir pelo prosseguimento ou rescisão do contrato.

Subcláusula sexta. Quaisquer tolerâncias entre as partes não importarão em novação de qualquer uma das cláusulas ou condições estatuídas neste contrato, as quais permanecerão íntegras.

CLÁUSULA VINTE E TRÊS - DO FORO

Fica eleito o foro da Justiça Federal, Seção Judiciária do Maranhão, com renúncia de qualquer outro, por mais privilegiado que seja, para dirimir as questões relacionadas com o presente contrato, que não puderem ser resolvidas pela via Administrativa.

E, por estarem de pleno acordo, depois de lido e achado conforme, foi o presente Contrato lavrado em 02 (duas) vias de igual teor e forma, assinado pelas partes juntamente com as testemunhas abaixo.

São Luís, de de 2012.

ILKA ESDRA SILVA ARAÚJO
Desembargadora Presidente
TRT-16ª região

ANTENOR PAGLIONE JÚNIOR
Representante legal
Empresa DAMOVO DO BRASIL S/A

Paulo Rogério Damovo do Brasil S/A Diretor Regional

EDSON ALVES MENINI
Representante legal
Empresa DAMOVO DO BRASIL S/A

TESTEMUNHAS:

Ana Celia F. Mendes
Nome:
CPF:

Luiza Maria O. de Sá
Nome:
CPF: 713.958.363-00

ANEXO I – ESPECIFICAÇÃO TÉCNICA

1. Solução de firewall em cluster composto por 2 nós mais a Solução de Gerência de cada cluster (Hardware, Software e Gerência) e a Solução de Emissão de Relatórios:

1.1. Todos os hardwares e softwares relativos a solução de cluster e os softwares de gerência, logs, monitoração e relatórios devem ser do mesmo fabricante do software de firewall;

1.2. O hardware utilizado para gerência, logs e monitoração pode ser do mesmo fabricante do software de firewall ou ser indicado pelo fabricante, em ambos os casos devem atender às especificações do item 2.1;

1.3. Devem ser licenciados para usuários e endereços IP ilimitados;

1.4. Poderão ser aceitos equipamentos adicionais para complementar as funcionalidades exigidas neste Anexo, contanto que os itens de performance, quantidade de portas e alta disponibilidade sejam cumpridas para cada conjunto de equipamentos e que os equipamentos sejam homologados pelo fabricante do software de firewall;

1.5. Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado;

1.6. Todas as funcionalidades de firewall, solução de relatórios, solução de gerência, IPS, VPN e QoS deverão ser fornecidas pelo mesmo fabricante de maneira integrada e em uma mesma arquitetura, devem, ainda, ter todas as licenças que compõem a solução ativas e válidas de forma perene, mesmo após o término do contrato, exceto para atualizações, correções e assinaturas de IPS;

1.7. Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;

1.8. Os backups devem ficar armazenados localmente e deve existir a funcionalidade de transferi-los a um servidor TFTP ou SCP;

1.9. A solução deverá ser compatível com SNMPv2 e SNMPv3;

1.10. A solução deverá ser compatível com OpenLDAP.

2. Gerência da solução

2.1. O hardware para gerência da solução de cada cluster deverá funcionar conjuntamente para gerência da solução, armazenamento de log e emissão de relatórios, deverá suportar toda a solução e deverá possuir as características:

2.1.1. Deve possuir, pelo menos, 3 interfaces 10/100/1000Mbps;

2.1.2. Deve possuir discos do tipo SAS com as capacidades:

2.1.2.1. Pelo menos 500 GB de espaço disponível (líquido) em unidades SAS, configurados em RAID 1 para o sistema operacional e os aplicativos;

2.1.2.2. Pelo menos 2 TB de espaço disponível (líquido) em unidades SAS de 10.000RPM, configurados em RAID 5 para base de dados, logs e arquivos temporários.

2.1.3. Deve possuir pelo menos 4 núcleos de processamento, cada um com velocidade de pelo menos 3,00 GHz;

2.1.4. Deve possuir o mínimo de 4GB de memória RAM;

2.1.5. Deve possuir leitor de DVD;

2.1.6. Fonte redundante interna, com entrada de tensão de 100-240V;

2.1.7. Deve ocupar, no máximo, 2 U em rack padrão 19 polegadas e possuir todo o material necessário para sua correta fixação no rack;

2.1.8. Todos os softwares, cabos e acessórios necessários para funcionar perfeitamente, inclusive sistema operacional e devidas licenças.

2.2. As funcionalidades de gerência da solução de cada cluster devem possuir as seguintes características:

2.2.1. Deve disponibilizar acesso por meio de browser para visualização de políticas, objetos e usuários a fim de prover acesso para gerentes e auditores sem a necessidade de utilizar a console completa;

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

2.2.3. Deve oferecer opção de autorizar e bloquear os acessos dos usuários à visualização pelo browser;

2.2.4. O acesso por meio browser deve ocorrer sobre SSL;

2.2.5. Deve suportar diferentes perfis de administração, disponibilizando, pelo menos, os seguintes: read/write, read only, gerenciamento de usuários e visualização de logs;

2.2.6. Deve incluir CA interna x.509 capaz de gerenciar certificados para gateways e usuários permitindo autenticação em VPNs;

2.2.7. Deve incluir a capacidade de confiar em CAs externas ilimitadas com a opção de verificar o certificado de cada gateway externo através de, no mínimo, DN e IP;

2.2.8. Deve permitir a criação de diversos perfis de IPS a serem aplicados a diferentes gateways;

2.2.9. Deve permitir incorporar automaticamente novas proteções de IPS baseadas, no mínimo, em severidade e nível de confiança da proteção;

2.2.10. Deve possuir a facilidade de busca com, no mínimo, as opções de consulta: quais objetos contem IPs específicos ou parte deles, busca por objetos duplicados, busca por objetos não utilizados e listar em quais regras um objeto é utilizado;

2.2.11. Deve possuir a opção de segmentar as regras de segurança através de rótulos com a finalidade de organizar as políticas;

2.2.12. Deve prover a opção de salvar automaticamente e manualmente versões de políticas;

2.2.13. Deve prover a funcionalidade de mover objetos e serviços entre as regras e de uma lista de objetos e serviços para uma regra;

2.2.14. A solução deverá gerenciar de forma centralizada as licenças dos gateways controlados por ela.

3. As funcionalidades da solução de armazenamento de logs deverão prover as seguintes características:

3.1. Deverá possibilitar a filtragem de eventos baseado em diversas categorias (IP fonte, porta fonte, IP destino, porta destino, interface, categoria de ataque, translated IP, translated port, entre outras) simultaneamente;

3.2. A solução deverá ser executada no mesmo servidor da solução de gerência;

3.3. Deve incluir um mecanismo automático de captura de pacotes para eventos de IPS com a finalidade facilitar análise forense;

3.4. A solução deverá diferenciar os logs para atividades comuns de usuário e logs relacionados à gerencia;

3.5. A solução deverá permitir configurar para cada tipo de regra ou evento pelo menos três das opções: log, alerta, enviar trap SNMP, envio de e-mail, execução de script definido pelo usuário;

3.6. A solução deverá incluir a opção de alterar uma regra ativa a partir da interface gráfica de visualização de logs;

3.7. A solução deve ser capaz de exportar os logs para uma base de dados ou repositório externo;

3.8. A solução deve suportar a troca automática de arquivo de log, regularmente ou através do tamanho do arquivo.

4. As funcionalidades da solução de emissão de relatórios deverão possuir as seguintes características:

4.1. Deve permitir a visualização simultânea de eventos de todos os recursos do gateway;

4.2. Deve permitir a criação de filtros com base em pelo menos as seguintes características do evento: endereço IP de origem e destino, serviço, tipo de evento, severidade do evento e nome do ataque;

4.3. O administrador deve ser capaz de atribuir esses filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes;

4.4. Deve permitir ao administrador o agrupamento de eventos baseado em qualquer uma das opções de filtragem, incluindo vários níveis de alinhamento;

4.5. Deve estar inclusa a opção de procura dentro da lista de eventos;

4.6. Deve estar inclusa na lista de eventos a opção de gerar gráficos ou tabelas com o evento, origem e destinos;

4.7. Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes;

4.8. Deve suportar a detecção de ataques de força bruta para quebra de credencial;

4.9. Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais Serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos;

4.10. A ferramenta de relatórios deve suportar pelo menos os seguintes filtros: endereço de origem, endereço de destino, usuário, nome do ataque e número da regra;

4.11. A ferramenta de relatórios deve permitir a personalização de relatórios pré-definidos;

4.12. Deve suportar, no mínimo, dois dos seguintes formatos de relatórios: MHT, HTML, PDF, Microsoft Excel, Microsoft Visio, ODF e CSV;

4.13. Deve suportar a distribuição automática de relatórios por e-mail;

4.14. A ferramenta de relatórios deve fornecer informações consolidadas sobre:

4.14.1. O volume de conexões que foram bloqueadas pela solução;

4.14.2. Principais fontes de conexões bloqueadas, seus destinos e serviços;

4.14.3. Principais regras usadas pela solução;

4.14.4. Principais ataques detectados pela solução e indicação das suas principais fontes e destinos;

4.14.5. Número de políticas instaladas e desinstaladas na solução;

4.14.6. Principais serviços de rede;

4.14.7. Indicação dos serviços que mais utilizaram tráfego criptografado;

4.14.8. Principais usuários VPN.

5. Cada solução de cluster de alta disponibilidade deverá:

5.1. Ser implementada por meio de 2 (dois) dispositivos de hardware dedicados idênticos entre si;

5.2. Permitir a aplicação de atualizações em cada nó, de forma transparente e de maneira imperceptível para os usuários finais;

5.3. Permitir o retorno para versão anterior, de forma transparente e de maneira imperceptível para os usuários finais;

5.4. A solução deverá implementar alta disponibilidade e redundância por meio de cluster em modo Ativo-Ativo com balanceamento de carga, de maneira que caso um dos nós do cluster fique indisponível, todas as conexões sejam direcionadas para o nó ativo de forma transparente para os usuários finais, sem perdas das conexões ativas em caso de falhas em uma das unidades;

5.5. A solução deverá replicar automaticamente definições e alterações de configuração em todos os nós do cluster;

5.6. Todas as licenças que compõem a solução deverão permitir a plena continuidade de utilização e operação mesmo após o término do contrato, de forma perpétua, exceto para atualizações, correções e assinaturas de IPS;

5.7. Possuir funcionalidades de firewall e IPS implementadas no mesmo chassis:

5.7.1. A comunicação entre eles deverá ser interna, sem a necessidade de uso de qualquer interface externa entre IPS e firewall;

5.7.2. O firewall deverá permitir a seleção do tipo de tráfego enviado ao IPS, ou a definição de exceções ao processamento de IPS.

6. Funcionalidades de firewall

6.1. A funcionalidade de firewall de todos os appliances ofertados deve ser a mesma e deve ser licenciada para funcionamento em cluster ativo-ativo;

6.2. O software de firewall deve ser do mesmo fabricante do software de gerência da solução e dos hardwares dos itens 10 e 11;

6.3. O software deve suportar configuração via linha de comando e interface GUI;

6.4. Deve suportar alta disponibilidade;

6.5. Deve funcionar como Stateful inspection baseado em análise granular do estado da comunicação e da aplicação para acompanhar e controlar o fluxo da comunicação que passa por ele abrindo portas de maneira dinâmica e segura;

6.6. Deve trabalhar com regras e agrupamento de regras baseadas em objetos e grupos de objetos;

6.7. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou sejam obrigatoriamente listadas;

6.8. Deve suportar pelo menos 1024 VLANs;

6.9. Deve suportar controle de acesso para pelo menos as aplicações/protocolos/serviços seguintes: HTTP, FTP (modos ativo e passivo), TFTP, DNS, SMTP, SQLNet e RPC;

6.10. Deve proteger aplicações de VoIP suportando H323, SIP, MGCP e SCCP;

6.11. A solução deverá suportar políticas de QoS, pelo menos classificação e priorização, com base no modelo DiffServ;

6.12. Deve incluir NAT dinâmico (N-1 ou Hide) e estático (1-1), com a possibilidade de converter os IPs de origem e destino e as portas no mesmo pacote com apenas uma regra;

6.13. Deve permitir a ativação/desativação de regras por intervalo de tempo;

6.14. As licenças não devem limitar a quantidade de regras de segurança e NAT;

6.15. O firewall deve suportar métodos de autenticação de usuário, cliente e sessão;

6.16. Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;

6.17. Os seguintes esquemas de autenticação devem ser suportadas pelos módulos de firewall e VPN: Tokens (como SecureID), TACACS, RADIUS, certificados digitais e dispositivos biométricos;

6.18. Deve incluir uma base de dados local que permita autenticação e autorização de usuários sem a necessidade de um dispositivo externo;

6.19. Deve suportar DHCP nos modos server e relay;

6.20. Deve ser capaz de trabalhar em Transparent mode (bridged mode);

6.21. Deve ter a funcionalidade de controlar o acesso a compartilhamentos de arquivo Microsoft usando CIFS;

6.22. Deve suportar alta disponibilidade de gateways e balanceamento de carga no modo Ativo-Ativo;

6.23. Possuir mecanismo que possibilita o tráfego de serviços específicos em horários específicos;

6.24. Possuir mecanismo de proteção contra ataque de negação de serviço (DoS); 6.25. Possuir mecanismo contra ataques de falsificação de endereços de origem (IP Spoofing).

7. Funcionalidades IPSec / VPN

7.1. A funcionalidade de IPSec / VPN de todos os appliances ofertados deve ser a mesma e deve ser licenciada para funcionamento em cluster ativo-ativo;

7.2. Deve ser fornecida para quantidade ilimitada de usuários;

7.3. Deve incluir suporte a IPSEC manual e IKE;

7.4. Deve suportar criptografia 3DES e AES-256 para IKE fases I e II;

7.5. Deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit) e Grupo 5 (1536 bit);

7.6. Deve suportar integridade de dados md5 e sha1;

7.7. Deve incluir suporte para VPN site-to-site nas seguintes topologias: Full Meshed (todos para todos), Estrela (escritórios remotos para site central), Hub e Spoke (site remoto através de site central para outro site remoto);

7.8. Deve incluir suporte a cliente-to-site baseado em IPSEC;

7.9. Deve suportar VPNs L2TP;

7.10. Caso necessite de agentes VPN, o cliente IPSEC VPN incluso deve suportar roaming (mudança de redes/interfaces e mudança de endereço IP sem perda da conexão VPN) e Auto-Connect (uma conexão é feita automaticamente quando o endpoint está fora da rede corporativa e uma aplicação necessita acesso a essa rede);

7.11. Deve incluir gerenciamento centralizado de VPNs, com a possibilidade de criar várias VPNs ao mesmo tempo;

7.12. Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN;

7.13. Deve suportar VPNs, usando pelo menos 2 (dois) dos seguintes protocolos: RIPv2, EIGRP, BGP ou OSPF;

7.14. Deve incluir um mecanismo para mitigar o impacto de um ataque DoS ao IKE, fazendo a distinção entre peers conhecidos e desconhecidos;

7.15. Clientes IPSec do mesmo fabricante devem estar disponíveis para pelo menos as seguintes plataformas: Windows XP, Windows Vista e Windows 7;

7.16. Deve incluir a funcionalidade para estabelecer VPNs com gateways com IPs públicos dinâmicos.

8. Funcionalidades de IPS

8.1. As funcionalidades de IPS e firewall podem ser implementadas em um mesmo chassi, sendo que a comunicação entre eles deverá ser interna, sem a necessidade de uso de quaisquer interfaces externas;

8.2. Deve incluir pelo menos os seguintes mecanismos de detecção:

8.2.1. Assinaturas de vulnerabilidades e exploits;

8.2.2. Assinaturas de ataque;

8.2.3. Validação de protocolo;

8.2.4. Detecção de anomalia;

8.2.5. Detecção baseada em comportamento;

8.2.6. Nível de confiança de detecção de ataque;

8.2.7. Correlação multi-elemento.

8.3. O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (inbound);

8.4. O IPS deve incluir pelo menos 2000 definições de ataques que protejam tanto clientes quanto servidores;

8.5. O IPS deve oferecer ao menos duas políticas pré-definidas que podem ser usadas imediatamente;

8.6. O IPS deve incluir a habilidade de interromper temporariamente as proteções para fins de troubleshooting;

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

8.8. O administrador deve ser capaz de ativar novas proteções baseado em parâmetros configuráveis (impacto na performance, severidade da ameaça, proteção dos clientes, proteção dos servidores);

8.9. 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, controle de aplicações, ataques genéricos sem assinaturas pré-definidas;

8.10. Deve oferecer a habilidade de seguir o uso de aplicações específicas como peer-topeer, com a opção de bloquear estas aplicações;

8.11. Para cada proteção, a descrição da vulnerabilidade e da ameaça, severidade da ameaça e nível de confiança de detecção de ataque devem estar inclusos;

8.12. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na fonte, destino, serviço ou qualquer combinação dos três;

8.13. A solução deve fazer captura de pacotes para proteções específicas;

8.14. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, serviços Windows (Microsoft Networking) e VoIP;

8.15. Deve incluir a habilidade de detectar e bloquear ataques conhecidos e desconhecidos, protegendo de, pelo menos, os seguintes ataques conhecidos: IP Spoofing, SYN Flooding, Ping of death, ICMP Flooding, Port Scanning, ataques de força bruta a IKE e man-in-the-middle com VPNs;

8.16. A solução deve detectar pelo menos os seguintes worms: Code Red, Nimda, Bugbear e Slammer;

8.17. A solução deve incluir proteção aos protocolos POP e SMTP;

8.18. A solução deve ser capaz de inspecionar/filtrar portas conhecidas (como http 80) a fim de buscar aplicações que possam comprometer a segurança do Contratante, como P2P (KaZaa, Gnutella, Morpheus, BitTorrent) e IMs (Yahoo!, MSN, ICQ), mesmo quando elas pareçam ser tráfego válido;

8.19. Deve oferecer proteção contra MSN Messenger via MSNMS e SIP;

8.20. O administrador deve ser capaz de permitir chat, mas bloquear vídeo no MSN Messenger;

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

8.22. O administrador deve ser capaz de configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

8.23. Deve oferecer a opção de bloquear controles ActiveX e applets Java que possam comprometer usuários web;

8.24. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades em diversas áreas de interesse do administrador e a evolução no tempo. As diferentes áreas de interesse devem ser definidas usando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades do mesmo, incluindo pelo menos: origem, destino, serviço, tipo e nome do alerta.

9. Funcionalidades de controle de aplicações

9.1. Possuir pelo menos as seguintes categorias para classificação das aplicações:

9.1.1. P2P;

9.1.2. Web;

9.1.3. VOIP.

9.2. Deve funcionar integrado ao serviço de diretório Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

9.3. Dever prover integração com o Microsoft Active Directory, para permitir acesso individual ou de grupo a aplicativos específicos, enquanto restringe outros;

9.4. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

9.5. Permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

9.6. Permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

9.7. Permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

9.8. Permitir acessos com base nos usuários e grupo de usuários do Active Directory;

9.9. Deverá monitorar e controlar o uso de aplicativos ou protocolos com base na identidade, usuário ou grupo;

9.10. Identificar, permitir, bloquear ou limitar o uso de aplicações independentemente das portas e protocolos onde estejam;

9.11. A solução deverá ser capaz de fazer log de todas as sessões. Os registros deverão conter:

9.11.1. Usuário ou máquina de origem;

9.11.2. Endereço IP de origem;

9.11.3. Endereço IP de destino;

9.11.4. Data e hora da mensagem;

9.11.5. Aplicação e/ou URL acessada.

9.12. Deve permitir filtrar as informações de monitoramento e tráfego das aplicações pelo menos dos seguintes modos:

9.12.1. Em tempo real na forma de gráficos e relatórios;

9.12.2. Baseado em histórico – logs armazenados, na forma de gráficos e relatórios.

10. Hardware de cada nó do tipo 2:

10.1. Deverá ser novo, de primeiro uso, entregue em perfeito estado de funcionamento;

10.2. O appliance do tipo 2 deverá possuir, no mínimo, 12 interfaces 10/100/1000;

10.2.1. Todas as interfaces fornecidas na solução devem estar licenciadas e habilitadas para uso imediato.

10.3. Deve ter suporte a interface serial para acesso gerencial local (console) ao equipamento;

10.4. O throughput de firewall deve ser de, no mínimo, 4Gbps por nó do cluster sem aceleração por hardware;

10.5. O throughput de firewall combinado com a finalidade de IPS ativada com tráfego misto deve ser de pelo menos 2Gbps;

10.6. Deve suportar pelo menos 1.000.000 sessões TCP concorrentes por nó do cluster;

10.7. Suportar pelo menos, 50.000 novas conexões TCP por segundo, por nó do cluster, até o limite de capacidade de conexões simultâneas;

10.8. Os valores de desempenho especificados nos itens 11.6 e 11.7 devem ser ofertados de forma centralizada, não serão aceitas soluções baseadas em combinação de módulos de firewalls em um chassi;

10.9. Suportar 1.000.000 de pacotes de 64 bytes por segundo através do firewall, por nó do cluster;

10.10. O appliance deve ser capaz de armazenar mais de uma imagem do sistema operacional e deve permitir ao administrador alternar entre elas;

10.11. Deve possuir throughput de pelo menos 1.000 Mbps para VPN utilizando 3DES e AES;

10.12. Possuir fontes internas de alimentação redundante 110/220V e capacidade para suportar toda a solução, sem perda de funcionalidade ou capacidade, no caso de falha nas fontes principais;

10.13. Cada nó da solução deve ocupar, no máximo, 3 U em rack padrão 19 polegadas e possuir todo o material necessário para sua correta fixação no rack.

ANEXO II – PROGRAMA DE CAPACITAÇÃO

O programa de capacitação deverá ser concluído em até 60 (sessenta) dias após a implantação da solução no **CONTRATANTE**.

O treinamento deverá abranger, no mínimo, os seguintes tópicos:

- Arquitetura da solução proposta;
- Configurações da política de segurança e suas propriedades;
- Configuração e autenticação de usuários/sessão;
- Network Address Translation (NAT);
- Backup e restauração;
- Upgrade;
- Licenciamento;
- Instalação e implementação;
- Tracking e alertas;
- Balanceamento de carga para servidores;
- Habilitando Voz sobre IP (VoIP);
- Segurança de conteúdo;
- Criptografia e VPN's;
- Autoridades Certificadoras (CAs);
- Configuração de VPNs (Client-to-Site e Site-to-Site);
- Opções avançadas de proteção da solução;
- Integração com LDAP e AD para o gerenciamento de usuários;
- Domínios de criptografia para VPNs sobrepostos;
- VPNs para múltiplos pontos de entrada (MEPs);
- Solução de alta disponibilidade (HA) e clustering;
- Log, reports e auditoria;
- IPS;
- Troubleshooting e debugging.

O treinamento deverá ser ministrado em Brasília, em instalações fornecidas pela **CONTRATADA**, para um número de 30 (trinta) participantes, em horário que será estabelecido pelo **Tribunal Superior do Trabalho**, com carga horária mínima de 40 horas.

As despesas com o ambiente de treinamento (sala, computadores, projetores, servidores, apostilas, CD_ROM, etc.) será de responsabilidade da **CONTRATADA**.

O material didático a ser utilizado deverá ser preparado pela **CONTRATADA** e entregue 02 (dois) dias antes do início do treinamento.

O instrutor deverá ser certificado pelo fabricante da solução proposta.

As despesas com o instrutor, inclusive as relativas a transporte, estadia e alimentação, serão de responsabilidade da **CONTRATADA**.

A **CONTRATADA** deverá fornecer certificados para os participantes que obtiverem aproveitamento satisfatório, no prazo máximo de 05 (cinco) dias após o encerramento do treinamento.

A ementa definitiva do curso deverá ser elaborada pela Secretaria de Tecnologia da Informação do TST, juntamente com a **CONTRATADA**, no prazo máximo de 10 (dez) dias após a assinatura deste contrato.

ANEXO III - TERMO DE GARANTIA DO OBJETO

1 - DA GARANTIA

1.1. A EMPRESA DAMOVO DO BRASIL S/A, doravante denominada Concedente, garante os equipamentos e serviços por ela fabricados, fornecidos e/ou prestados, incluindo assistência técnica e manutenção, pelo período de 36 meses, incluída a garantia legal, contados a partir do recebimento definitivo do objeto do contrato.

1.2. Os 3 (três) primeiros meses compreendem a garantia legal, e os outros 33 (trinta e três) meses, compõem a garantia contratual, que é complementar àquela.

1.3. Esta garantia abrange peças, materiais e serviços, desde que os produtos tenham sido utilizados conforme as orientações contidas em seu manual de instrução e/ou guia de instalação.

1.4. A garantia compreende a substituição de peças, mão-de-obra, atualização da solução, assistência técnica e no reparo de defeitos de fabricação.

1.5. Somente um técnico autorizado pela Concedente está habilitado a reparar defeitos cobertos pela garantia, mediante apresentação da nota fiscal pelo usuário do produto.

2 - DA ASSISTÊNCIA TÉCNICA

2.1. A Concedente deverá prestar assistência técnica durante o período de garantia nos prazos e forma especificados a seguir:

2.1.1. A assistência técnica da garantia consistirá na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças e componentes que se apresentarem defeituosos, de acordo com os manuais e normas técnicas específicas para os equipamentos; acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) do fabricante do equipamento, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações ("update" e "upgrade") de todos os componentes de software do sistema;

2.1.2. Garantir assistência técnica credenciada pelo fabricante dos equipamentos, capaz de atender nos locais de entrega dos equipamentos com, no mínimo, uma central de assistência técnica;

2.1.3. A assistência técnica utilizará apenas peças e componentes originais salvo nos casos fundamentados por escrito e aceitos pelo **CONTRATANTE**;

2.1.4. A assistência técnica em garantia será prestada na modalidade "on-site";

2.1.5. A partir da comunicação do(s) defeito(s) pelo **CONTRATANTE**, conforme sistema de registro próprio do **CONTRATANTE**, o início do atendimento e término do reparo do(s) equipamento(s) serão de até 2 horas e 24 horas, respectivamente;

2.1.6. A assistência técnica da garantia será realizada de segunda-feira a sexta-feira, no horário das 7:30h às 17:30h, a pedido do **CONTRATANTE**;

2.1.7. A abertura de chamados será efetuada por correio eletrônico e por telefone, sendo que no caso de abertura através de telefone, o contato será efetuado por meio de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800) ou números locais no município de entrega dos equipamentos;

2.1.7.1 Em ambos os casos, o atendimento deverá ser efetuado em língua portuguesa.

2.1.8. O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível vinte e quatro horas por dia, sete dias por semana;

2.1.9. O término do reparo do equipamento não poderá ultrapassar o prazo previsto, caso contrário deverá ser providenciado pela Concedente a colocação de equipamento equivalente ou de superior configuração como backup, até que seja sanado o defeito do equipamento;

2.1.10. Durante o período de garantia, os equipamentos que apresentarem inoperância, em duas ocasiões separadas por no máximo um período de sessenta dias corridos, devem ser substituídos;

2.1.11. Durante o período de garantia, os equipamentos que apresentaram funcionamento irregular, em desacordo com aquele especificado pelo fabricante, em duas ocasiões separadas por até sessenta dias corridos, devem ser substituídos.

2.2 Responsabilizar-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para o **CONTRATANTE**.

3 - AS GARANTIAS LEGAL E/OU CONTRATUAL NÃO COBREM:

3.1. Falhas no funcionamento do produto decorrentes de uso inadequado, ou seja, em desacordo com as instruções e/ou recomendações do manual de instrução do produto;

3.2. Produtos ou peças que tenham sido danificados em consequência de remoção ou manuseio por pessoas não autorizadas, quedas, ou de fatos decorrentes de forças da natureza, tais como raios, chuvas, inundações etc.;

3.3. Peças sujeitas ao desgaste natural, descartáveis ou consumíveis, peças móveis ou removíveis em uso normal, bem como a mão-de-obra utilizada na aplicação das peças e as consequências advindas dessas ocorrências.

4 - AS GARANTIAS LEGAL E/OU CONTRATUAL FICAM AUTOMATICAMENTE INVALIDADAS SE:

4.1. Na utilização do produto não forem observadas as especificações e recomendações do manual de instrução;

4.2. O produto tiver sofrido alterações ou modificações estéticas e/ou funcionais, bem como tiver sido realizado conserto por pessoas ou entidades não credenciadas pela Concedente;

4.3. Os defeitos forem provocados pela utilização de material ou peças fora das especificações.

5 - SANÇÃO POR DESCUMPRIMENTO DE OBRIGAÇÕES DE GARANTIA

5.1. O atraso injustificado no início do atendimento técnico no período de garantia implicará multa de 1% (um por cento) do valor do equipamento faturado na nota fiscal entregue ao **CONTRATANTE**, por hora de atraso, para cada equipamento em que houver atraso, até o limite de 20% do valor do contrato, punível com as sanções previstas nos subitens 20.1.3 e 20.1.4 do edital, como também a inexecução total do contrato.