TERMO DE REFERÊNCIA

1. DO OBJETO

Registro de preço para aquisição de solução de infraestrutura de rede para modernização da topologia de rede da JUSTIÇA FEDERAL NA PARAÍBA (Órgão gerenciador) e órgãos participantes, com a finalidade de proporcionar a melhoria e ampliação da infraestrutura de interconectividade de Tecnologia da Informação da Justiça Federal de primeiro grau e atendendo a Política de Nivelamento de Infraestrutura de Tecnologia da Informação da Justiça Federal, Resolução Nº CJF-RES-2018/00477 de 28 de fevereiro de 2018, conforme condições, quantidades, exigências estabelecidas neste instrumento:

Item	**ÓRGÃOS PARTICIPANTES**						**QTD Total**
	JFPB	**TRF5**	**JFRN**	**JFPE**	**JFCE**	**JFSE**	
Item 01 - Concentrador SECURE SD-WAN	2	2	2	2	2	2	**12**
Item 02 - Solução de Gerenciamento Centralizado	1	-	1	1	1	1	**5**
Item 03 - Solução de Gerenciamento de Logs e Relatórios	1	1	1	1	-	1	**5**
Item 04 - Licença de Atualizações de Segurança para Concentrador SECURE SD-WAN	2	2	2	2	-	2	**10**
Item 05 - Unidades de Serviços Técnicos (UST)	30	30	30	30	30	30	**180**

2. DA JUSTIFICATIVA

A contratação objetiva a modernização da topologia de conectividade da rede da JFPB, sendo essencial para o provimento e continuidade dos serviços e soluções de TI disponibilizados na instituição, permitindo a comunicação da rede interna com toda rede que compõe a Justiça Federal da 5ª Região, com utilização de link's dedicados de tecnologias diversas, garantindo alta disponibilidade dos sistemas internos (PJE, SEI, SARH, Videoconferência, etc). Atualmente a JFPB se comunica com a rede da JF 5ª Região através de links MPLS.

As Unidades da Justiça Federal da 5ª Região(aí inclusa a JFPB) e o Tribunal Regional Federal da 5ª Região – TRF5, possuindo tal solução tecnológica (intercomunicando-se), além de padronização, o que permitirá melhor disseminação de conhecimentos sobre a administração da solução e diálogo entre as equipes técnicas da JF da 5ª Região, terá ferramenta para a solução ágil de problemas, que porventura surjam no decorrer do uso da mesma; podem ter mais flexibilidade/economicidade, com a facilidade que a funcionalidade SDWAN pode oferecer, tornando ágil a mudança de links/operadoras, sem prejuízos operacionais que poderiam ocorrer com a falta de conexão entres os órgãos.

Consultando a Subsecretaria de Infraestrutura do TRF5, a JFPB obteve a informação que atualmente o mesmo utiliza a solução do fabricante FORTINET, também já utilizada pelas Seções Judiciárias de Pernambuco e Alagoas. Neste sentido para garantir 100% de interoperabilidade, padronização de ambientes, disseminação de conhecimento, possibilidade de gerenciamento regional centralizado; **a solução a ser adquirida deve possuir 100% de compatibilidade de funcionalidades com as atualmente instaladas e em uso pelo TRF5 e seções citadas acima e deve atender as especificações técnicas abaixo.**

A contratação é composta pela aquisição de material e serviços, de acordo com o descrito nas especificações técnicas.

Ingressam como participante deste pregão para registro de preços a Justiça Federal de 1ª Instância de Pernambuco – JFPE, Justiça Federal de 1ª Instância no Ceará – JFCE, Justiça Federal de 1ª Instância em Sergipe – JFSE, Justiça Federal de 1ª Instância no Rio Grande do Norte – JFRN e o Tribunal Regional Federal da 5ª Região (TRF5), conforme quantitativos informados neste Termo de Referência.

3. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

3.1. Será considerado vencedor o licitante que apresentar o menor lance para o lote, devendo observar o preço máximo estabelecido por item, e atenderem a todos os requisitos do Termo de Referência.

LOTE 01			
ITEM	**VALOR UNITÁRIO**	**QUANT**	**VALOR TOTAL**
Item 01 - Concentrador SECURE SD-WAN	R$ 101.692,36	**12**	R$ 1.220.308,32
Item 02 - Solução de Gerenciamento Centralizado	R$ 30.635,06	**5**	R$ 153.175,30
Item 03 - Solução de Gerenciamento de Logs e Relatórios	R$ 63.117,09	**5**	R$ 315.585,45
Item 04 - Licença de Atualizações de Segurança para Concentrador SECURE SD-WAN	R$ 193.814,02	**10**	R$ 1.938.140,20
Item 05 - Unidades de Serviços Técnicos (UST)	R$ 1.671,13	**180**	R$ 300.803,40
VALOR TOTAL			R$ 3.928.012,67

4. DA PROPOSTA TÉCNICA

4.1. As propostas deverão conter todos os itens do lote, sob pena de desclassificação;

4.2. **As empresas proponentes deverão informar fabricante / marca / modelo dos produtos ofertados em sua proposta eletrônica**. E, quando do encaminhamento da proposta ajustada, a empresa proponente vencedora deverá apresentar proposta técnica completa contendo:

4.2.1. lista de equipamentos, softwares e serviços ofertados, incluindo fabricante, modelo, part-number de cada item que compõe sua oferta;

4.2.2. comprovação através de documentos do fabricante de que os produtos ofertados atendem a especificação técnica exigida, indicando link para o documento (ou cópia do documento) e trecho do documento. A CONTRATANTE, através de sua equipe técnica, poderá exigir para no prazo de 2(duas) horas, a CONTRATADA faça a indicação do link do documento que indica o atendimento de itens isolados da especificação técnica contida neste TR, sob pena de desclassificação da proposta;

4.2.3. comprovação de que a garantia ofertada do fabricante atende as exigências do edital;

4.2.4. atestado(s) emitido(s) por empresas de direito público ou privado comprovando capacidade técnica e operacional para fornecimento e execução dos serviços semelhantes ao objeto deste edital;

5. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

5.1. A contratante poderá fazer pedidos de itens específicos e individualizados ou na sua totalidade de acordo com a necessidade de atendimento da demanda e da disponibilidade orçamentária;

5.2. Os equipamentos fornecidos deverão estar cobertos por garantia conforme especificado nos itens ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE GARANTIA e ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE TREINAMENTO do Anexo I., deste Termo de Referência.

5.3. A entrega dos materiais a assistência técnica deverão ocorrer de forma "on site" nas instalações **do Núcleo de Tecnologia da Informação - SEÇÃO JUDICIÁRIA DA PARAÍBA (Órgão gerenciador) - Rua João Teixeira de Carvalho, 480 - Brisamar – João Pessoa - PB - C.E.P.: 58031-900**, e nos endereços abaixo para os demais órgãos participantes, no horário das 09hs às 18hs, o qual deverá fazer avaliação criteriosa constatando se os materiais apresentados conferem com as especificações solicitadas neste Termo de Referência.

5.3.1. TRIBUNAL REGIONAL FEDERAL DA 5ª REGIÃO: Cais do Apolo, s/n - Edifício Ministro Djaci Falcão, Bairro do Recife - Recife – PE, CEP 50030-908.

5.3.2. JUSTIÇA FEDERAL DE 1º GRAU EM PERNAMBUCO: Av. Recife, 6250 - Fórum Ministro Artur Marinho Jiquiá - Recife – PE, CEP 50865-900.

5.3.3. JUSTIÇA FEDERAL DE 1º GRAU NO CEARÁ: Praça Murilo Borges,
Centro - Fortaleza – CE, CEP 60035-210.

5.3.4. JUSTIÇA FEDERAL DE 1º GRAU NO RIO GRANDE DO NORTE: Rua Dr. Lauro Pinto, 245, Lagoa Nova, Natal - RN CEP: 59064-250.

5.3.5. JUSTIÇA FEDERAL DE 1º GRAU EM SERGIPE: Forum Ministro Geraldo Barreto Sobral - Centro Administrativo Governador Augusto Franco, Av. Dr. Carlos Rodrigues da Cruz, 1500 - Bairro Capucho - Aracaju/Sergipe, CEP 49.081-015.

5.4. O prazo de entrega não será superior a 45 (quarenta e cinco) dias corridos, contados a partir do recebimento da nota de empenho.

5.5. Os bens serão recebidos provisoriamente, a partir da entrega, pela Seção de Infraestrutura, responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência.

5.6. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

5.7. Os bens serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

5.8. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

5.9. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

6. **DAS OBRIGAÇÕES DA CONTRATANTE**

6.1. Acompanhar e fiscalizar a execução do Contrato;

6.2. Inspecionar ou testar os equipamentos, conectores, transceivers, cabos e outros periféricos para confirmar se eles atendem aos requisitos de Contrato;

6.3. Emitir Termo de Recebimento Provisório e Definitivo;

6.4. Rejeitar os produtos que não atendam aos requisitos constantes das especificações do Termo de Referência;

6.5. Atestar as Notas Fiscais emitidas pelo Fornecedor;

6.6. Efetuar o pagamento até o 5º (quinto) dia útil seguinte ao do recebimento definitivo (atesto da nota fiscal) de cada fornecimento, que deverá ser feito pelo Supervisor do Setor de Suporte e Manutenção;

6.7. Abrir chamado de suporte técnico;

6.8. Notificar o Fornecedor, quando necessário;

6.9. Gerenciar o projeto de instalação e configuração.

7. **OBRIGAÇÕES DA CONTRATADA**

7.1. Fornecer os produtos cotados rigorosamente de acordo com as especificações e condições apresentadas na proposta comercial, quanto às suas características e condições;

7.2. Responsabilizar-se por quaisquer despesas que incidam direta ou indiretamente sobre os materiais;

7.3. Responder solidariamente com o fabricante e o distribuidor pelos materiais fornecidos;

7.4. Substituir, no mesmo prazo previsto para a entrega, contado a partir da data da comunicação, via contato telefônico ou e-mail, e sem qualquer ônus para a Justiça Federal de Primeiro Grau na Paraíba e demais órgãos participantes, os materiais que apresentarem defeitos de fabricação dentro do prazo de validade;

7.5. Arcar com qualquer prejuízo causado à Administração ou a terceiros por seus empregados durante a entrega dos bens, inclusive durante a entrega dos equipamentos feita por transportadoras;

7.6. Realizar transferência de tecnologia operacional dos equipamentos que fazem parte deste projeto, mediante treinamento de acordo com o especificado neste termo de referência;

7.7. Cumprir as exigências de Garantia, Suporte Técnico e Entrega;

7.8. Instalar e Configurar a solução de acordo com planejamento elaborado em conjunto com a equipe técnica da contratante;

7.9. Garantir a integração da solução ao ambiente da JFPB e demais órgãos participantes;

7.10. Emitir toda documentação de projeto solicitada;

7.11. Emitir Nota Fiscal para o pagamento pela Administração;

7.12. Fazer a coleta no mesmo local de entrega, dos equipamentos e periféricos substituídos.

8. DAS **CONDIÇÕES DE PAGAMENTO**

8.1. O pagamento efetuar-se-á por intermédio de depósito em conta bancária da CONTRATADA, no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal/fatura discriminada, em 2 (duas) vias, ressalvada a hipótese prevista no § 3º do art. 5º da Lei nº 8.666/1993;

8.2. Caberá à CONTRATADA apresentar, juntamente com a nota fiscal, os comprovantes atualizados de regularidade com o Instituto Nacional do Seguro Social (INSS) e com o Fundo de Garantia por Tempo de Serviço (FGTS) e da Certidão Negativa de Débitos Trabalhistas (CNDT);

8.3. Os pagamentos referentes aos equipamentos e softwares serão efetuados após a equipe técnica da JFPB e demais órgãos participantes emitir o Termo de Recebimento Definitivo;

8.4. O pagamento referente aos serviços de instalação serão efetuados após a equipe técnica da JFPB e demais órgãos participantes constatar que todos os equipamentos foram devidamente entregue e atestados pela equipe do NTI com consequnte emissão do Termo de Recebimento Definitivo;

8.5. As eventuais despesas bancárias decorrentes de transferência de valores para outras praças ou agências são de responsabilidade da CONTRATADA;

8.6. Havendo vício a reparar em relação à nota fiscal/fatura apresentada ou em caso de descumprimento pela CONTRATADA de obrigação contratual, o prazo constante do parágrafo segundo desta cláusula será suspenso até que haja reparação do vício ou adimplemento da obrigação.

9. **DAS SANÇÕES APLICÁVEIS**

9.1. Aplicam-se ao contratado do fornecimento dos bens previstos neste Termo de Referência as seguintes penalidades pela sua inexecução total ou parcial, assegurados o contraditório e a ampla defesa em regular processo administrativo:

1	Atraso na entrega do(s) item(ns) contratado(s) ou na sua substituição durante o período de verificação para fins de recebimento definitivo ou por defeito de fabricação durante a garantia, se o atraso for de até 5 (cinco) dias;	Advertência
2	Se o atraso do ID 1 for incidente a partir do sexto e até o décimo quinto dia, dobrável a partir do décimo sexto e até trigésimo dia de atraso, sem prejuízo da advertência de que trata o ID 1	Multa moratória diária de 0,25% (vinte e cinco centésimos por cento) sobre o valor total do(s) item(s) contratado(s) e não fornecido(s), por atraso no fornecimento do(s) item(ns), ou na sua substituição, total ou parcial, durante o período de observação para fins de recebimento definitivo, ou por defeito de fabricação durante a garantia

3	Se o atraso que trata o ID 1 for superior a 30 (trinta) dias	Multa compensatória, correspondente a 20% (vinte por cento) do(s) item(ns) contratado(s) e não fornecido(s), ou não substituído(s) durante o período de observação para fins de recebimento definitivo
4	Se qualquer dos atrasos for superior a 30 (trinta) dias	Impedimento de participar de licitações e de contratar com a JFPB, sem prejuízo da multa;
5	Se apresentar documentação falsa, fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal	Impedimento de participar de licitações e de contratar com a União, com o consequente descredenciamento no SICAF após a publicação da sanção pelo prazo de 1 (um) a 5 (cinco) anos, sem prejuízo da multa e das sanções penais e civis aplicáveis.

9.2. Das infrações e das sanções administrativas:

9.2.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

9.2.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

9.2.1.2. ensejar o retardamento da execução do objeto;

9.2.1.3. fraudar na execução do contrato;

9.2.1.4. comportar-se de modo inidôneo;

9.2.1.5. cometer fraude fiscal;

9.2.1.6. não mantiver a proposta.

9.2.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

9.2.3. advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

9.2.4. Multa moratória de 0,5% (cinco décimos por cento por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 20 (vinte) dias;

9.2.5. multa compensatória de 5% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

9.2.6. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

9.2.7. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

9.2.8. impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

9.2.9. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

9.2.10. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:

9.2.10.1. tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

9.2.10.2. tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

9.2.10.3. demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

9.2.11. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando- se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

9.2.12. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

9.2.13. As penalidades serão obrigatoriamente registradas no SICAF.

9.2.14. A multa compensatória absorverá a multa moratória.

9.2.15. Para fins de dosagem da sanção, serão avaliados a gravidade da infração e os antecedentes da licitante no âmbito da Administração Pública Federal.

9.2.16. Tratando-se de serviços a serem pagos, o valor correspondente à multa moratória descontado na ocasião do pagamento.

9.2.17. Não havendo possibilidade de dedução da multa, a mesma será cobrada por via administrativa, a ser quitada no prazo de 5 (cinco) dias úteis, e, não sendo efetuado o seu recolhimento, cópia dos autos do processo administrativo será encaminhada à Advocacia Geral da União para fins de ação de execução.

9.2.18. As penalidades previstas neste item não prejudicam as sanções a que se refira o edital, relativas a infrações cometidas pelo particular durante o certame licitatório.

ANEXO I

ESPECIFICAÇÕES TÉCNICAS

SOLUÇÃO DE REDE SD-WAN

LOTE 01		
Item	**Descrição**	**Quantidade**
01	Concentrador SECURE SD-WAN	**12**
02	Solução de Gerenciamento Centralizado	**5**
03	Solução de Gerenciamento de Logs e Relatórios	**5**
04	Licença de Atualizações de Segurança para Concentrador SECURE SD-WAN	**10**
05	Unidades de Serviços Técnicos (UST)	**180**

Os produtos oferecidos deverão atender plenamente as seguintes especificações:

1. **LOTE 01 - ITEM 01 - CONCENTRADOR SECURE SD-WAN**
   1.1. REQUISITOS ESPECÍFICOS
   1.1.1. Throughput de, no mínimo, 20 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
   1.1.2. Suporte a, no mínimo, 4 milhões conexões simultâneas;
   1.1.3. Suporte a, no mínimo, 250 mil novas conexões por segundo;
   1.1.4. Throughput de, no mínimo, 5 Gbps de VPN IPSec;
   1.1.5. Suporte a 2.000 túneis de VPN IPSEC Site-to-Site simultâneos
   1.1.6. Suporte a 50.000 túneis de VPN IPSEC Client-to-Site simultâneos
   1.1.7. Throughput de, no mínimo, 5 Gbps de VPN SSL;
   1.1.8. Suporte a, no mínimo, 10000 clientes de VPN SSL simultâneos;
   1.1.9. Suportar no mínimo 5 Gbps de throughput de IPS;
   1.1.10. Suportar no mínimo 5 Gbps de throughput de Inspeção SSL;
   1.1.11. Throughput de, no mínimo, 4 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de

segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

1.1.12. Possuir ao menos 8 interfaces 1Gbps com conectores RJ-45, habilitadas para uso;

1.1.13. Possuir ao menos 2 interfaces 1Gbps com conectores SFP habilitadas para uso;

1.1.14. Possuir ao menos 2 interfaces 10GbE com conectores SFP+ habilitadas para uso;

1.1.15. Possuir fonte de alimentação redundante interna ao equipamento;

1.1.16. Disco SSD de, no mínimo, 220 GBytes para armazenamento de informações locais;

1.1.17. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

1.2. REQUISITOS GERAIS

1.2.1. Deve ser do tipo appliance físico. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

1.2.2. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.2.3. Deve possuir capacidade de agregar e balancear, no mínimo, 4 circuitos de dados utilizando uma interface dedicada para cada circuito.

1.2.4. A solução Secure SD-WAN deve suportar recursos de segurança integrados de Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web licenciados no item 04.

1.2.5. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

1.2.6. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

1.2.7. Os dispositivos de proteção de rede devem possuir suporte a:

1.2.7.1. Policy based routing ou policy based forwarding;

1.2.7.2. roteamento multicast (PIM-SM e PIM-DM);

1.2.7.3. DHCP Relay;

1.2.7.4. DHCP Server;

1.2.7.5. Jumbo Frames;

1.2.7.6. sub-interfaces ethernet logicas;

1.2.7.7. NAT dinâmico Many-to-1 e Many-to-Many;

1.2.7.8. NAT estático 1-to-1, Many-to-Many, bidirecional 1-to-1;

1.2.7.9. Tradução de porta (PAT);

1.2.7.10. NAT de Origem e NAT de Destino simultaneamente;

1.2.7.11. poder combinar NAT de origem e NAT de destino na mesma política;
1.2.7.12. Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
1.2.7.13. NAT64 e NAT46;
1.2.7.14. protocolo ECMP;
1.2.7.15. balanceamento de link por hash do IP de origem e destino;
1.2.7.16. balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

1.2.8. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

1.2.9. Enviar log para sistemas de monitoração externos, simultaneamente;

1.2.10. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

1.2.11. Proteção anti-spoofing;

1.2.12. Implementar otimização do tráfego entre dois equipamentos;

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

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

1.2.15. Suportar OSPF graceful restart;

1.2.16. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

1.2.17. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

1.2.18. A configuração em alta disponibilidade deve possuir sincronização de configurações entre os dispositivos primário e secundário;

1.2.19. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

1.2.20. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

1.2.21. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

1.2.22. Deve possuir suporte a criação de, no mínimo, cinco sistemas virtuais no mesmo appliance;

1.2.23. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

1.2.24. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

1.3. SECURE SD-WAN

1.3.1. A solução Secure SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN

1.3.2. A solução Secure SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos

1.3.3. A solução Secure SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações

1.3.4. A configuração VPN IPSEC deverá oferecer suporte para versão IKE v2.0

1.3.5. A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15

1.3.6. A solução deve suportar aos seguintes requisitos:

1.3.6.1. IPv6

1.3.6.2. VRRP ou Equivalente

1.3.6.3. VRF

1.3.6.4. BGP

1.3.6.5. OSPF

1.3.6.6. RIPv2

1.3.6.7. Dynamic Multipath

1.3.6.8. Policy Based Routing

1.3.7. Reconhecimento em camada 7 totalmente segregado da camada 4

1.3.8. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino

1.3.9. O reconhecimento de aplicações, deve ser atualizado de forma dinâmica e totalmente transparente para no dispositivo

1.3.10. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

1.3.11. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc)

1.3.12. A solução, em sua modalidade física e/ou virtual, deve considerar os seguintes itens:

1.3.13. 802.1Q

1.3.14. BFD para BGP

1.3.15. A solução de SECURE SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6

1.3.16. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SECURE SD-WAN em condições onde a largura de banda é modificada

1.3.17. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde

seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SECURE SD-WAN

1.3.18. A solução deve ser capaz de medir o Status de Saúde com Suporte a múltiplos servidores.

1.3.19. A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links

1.3.20. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual

1.3.21. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema

1.3.22. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SECURE SD-WAN

1.3.23. A solução deve permitir a consulta via SNMPv2/v3

1.3.24. A solução deve possibilitar a distribuição de Peso em cada um dos links que compõe o SECURE SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:

1.3.24.1. Número de Sessões,

1.3.24.2. Volume de Tráfego,

1.3.24.3. IP de Origem e Destino e

1.3.24.4. Transbordo de Link (Spillover)

1.3.25. A Solução deve apresentar compatibilidade com modens USB (3G/4G), onde estes sejam capazes de funcionar em modo redundante.

1.3.26. Solução deve possuir capacidade de autenticar usuários para administração do Equipamento, através de base de dados:

1.3.26.1. Local

1.3.26.2. Integrada a servidor TACACS+

1.3.26.3. Integrada a servidor Ldap

1.3.27. A Alta Disponibilidade provida pela solução de SECURE SD-WAN, independente em suas modalidades físicas ou virtual, deverá obedecer os seguintes critérios:

1.3.27.1. Suportar Balanceamento Ativo – Ativo, Ativo – Passivo, Distribuído Geograficamente

1.3.28. A solução Secure SD-WAN deve oferecer Troubleshooting em console de linha de comando ou gráfica, onde seja possível:

1.3.28.1. Executar Packet sniffer do tráfego interessante, filtrando por: IP e Porta

1.3.28.2. Realizar debug detalhado das fases de negociação VPN

1.3.29. A Solução Secure SD-WAN deve oferecer visualização gráfica de:

1.3.29.1. Aplicações mais utilizadas com respectiva largura de banda

1.3.29.2. Shapping de Tráfego SECURE SD-WAN

1.3.29.3. IPs de Destino mais utilizados com respectivo número de Sessões e Largura de Banda associados

1.3.30. A solução SDWAN deve suportar marcação de pacotes DSCP nas definições e regras para tráfego SDWAN.

1.4. VPN

1.4.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.4.2. Suportar IPSec VPN;

1.4.3. Suportar SSL VPN;

1.4.4. A VPN IPSEc deve suportar 3DES;

1.4.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

1.4.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

1.4.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

1.4.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

1.4.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

1.4.10. Deve possuir interoperabilidade utilizando IPSec com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

1.4.11. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

1.4.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

1.4.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

1.4.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.4.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

1.4.16. Atribuição de DNS nos clientes remotos de VPN;

1.4.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

1.4.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

1.4.19. Suportar leitura e verificação de CRL (certificate revocation list);

1.4.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

1.4.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;

1.4.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;
1.4.23. Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;
1.4.24. Deverá manter uma conexão segura com o portal durante a sessão;
1.4.25. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

1.5. IDENTIFICAÇÃO DE USUÁRIOS

1.5.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
1.5.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;
1.5.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
1.5.4. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
1.5.5. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
1.5.6. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
1.5.7. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
1.5.8. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

1.6. QOS E TRAFFIC SHAPING

1.6.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
1.6.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
1.6.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
1.6.4. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
1.6.5. O QoS deve possibilitar a definição de tráfego com banda garantida;
1.6.6. O QoS deve possibilitar a definição de tráfego com banda máxima;
1.6.7. O QoS deve possibilitar a definição de fila de prioridade;
1.6.8. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
1.6.9. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

1.7. GEO LOCALIZAÇÃO

1.7.1. Suportar a criação de políticas por geo-localização, permitindo o tráfego de determinado Pais/Países sejam bloqueados;
1.7.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
1.7.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

1.8. GARANTIA, INSTALAÇÃO E TREINAMENTO

1.8.1. Conforme especificado nos itens ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE GARANTIA, ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE INSTALAÇÃO e ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE TREINAMENTO do Anexo I.

2. LOTE 01 - ITEM 02 – SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

2.1. REQUISITOS ESPECÍFICOS

2.1.1. Deve ser do mesmo fabricante do item 01 deste termo de referência;
2.1.2. Deve permitir o gerenciamento centralizado de, pelo menos, 10 dispositivos;
2.1.3. Deve possuir capacidade de armazenamento de, pelo menos, 100 GB;
2.1.4. Deve permitir o recebimento de, pelo menos, 1 GB de log dos dispositivos por dia;

2.1.5. Deve permitir o aumento da capacidade de gerenciamento de dispositivos, armazenamento e processamento de logs através do uso de licenças de expansão;
2.1.6. Deve ser fornecido em appliance virtual;
2.1.7. Deve ser compatível com os seguintes hypervisors: VMware ESX/ESXi 5.5/6.0/6.5;
2.1.8. Garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
2.1.9. Definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
2.1.10. Gerar alertas automáticos via e-mail e snmp;
2.1.11. Possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema prevenção a intrusão (IPS – intrusion prevention system), antivírus e de filtro de URL;
2.1.12. Permitir usar palavras chaves ou cores para facilitar identificação de regras;
2.1.13. Permitir localizar quais regras um objeto (ex. Computador, serviço, etc.) Está sendo utilizado;
2.1.14. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
2.1.15. Permitir criação de regras que fiquem ativas em horário definido;
2.1.16. Permitir criação de regras com data de expiração;
2.1.17. Realizar o backup das configurações para permitir o retorno (rollback) de uma configuração salva;
2.1.18. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso.
2.1.19. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
2.1.20. Garantir que todos os equipamentos seguros sejam controlados de forma centralizada, utilizando apenas um servidor de gerência;
2.1.21. Garantir que os dispositivos de segurança sejam visualizados na operação integrada da rede através de geolocalização, e integrados com uma aplicação de mapas online (google maps, bing maps ou outra equivalente);
2.1.22. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
2.1.23. Permitir ao administrador transferir os backups para um servidor SFTP;
2.1.24. Realizar a função de gerência em um equipamento exclusivo, não exercendo outras funções (como firewall);

2.1.25. Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota, de maneira centralizada;

2.1.26. Permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários locais, de bases externas LDAP e RADIUS.

2.1.27. Suportar e realizar a sincronização do relógio interno dos equipamentos da solução via protocolo NTP;

2.1.28. Gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

2.1.29. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;

2.1.30. Permitir criar os objetos que serão utilizados nas políticas, de forma centralizada;

2.1.31. Permitir bloqueio por países para qualquer IP, domínio ou aplicações.

2.2. GARANTIA E TREINAMENTO

2.2.1. Conforme especificado nos itens ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE GARANTIA e ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE TREINAMENTO do Anexo I.

3. LOTE 01 - ITEM 03 - SOLUÇÃO DE GERENCIAMENTO DE LOGS E RELATÓRIOS

3.1. REQUISITOS ESPECÍFICOS

3.1.1. Deve ser capaz de receber os logs de todos os controladores SECURE SD-WAN deste referido grupo;

3.1.2. Deve ser fornecido em appliance virtual compatível com os seguintes Hypervisor: VMware ESX/ESXi /5.0/5.1/5.5/6.5;

3.1.3. Possuir capacidade de receber ao menos 05 GBytes de logs diários;

3.1.4. Possuir ao menos 02 TB de espaço em disco;

3.1.5. Possibilitar acesso simultâneo de administradores, permitindo a criação de perfis para administração e monitoração;

3.1.6. Permitir a criação de administradores que acessem a todas as instâncias de virtualização da solução de relatórios;

3.1.7. Garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego;

3.1.8. Definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

3.1.9. Possuir mecanismo para que logs antigos sejam removidos automaticamente, após estarem consolidados na solução de guarda e análise de logs e relatoria;
3.1.10. Permitir a extração de relatórios;
3.1.11. Garantir a exportação dos logs no formato de arquivo do tipo csv;
3.1.12. Gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
3.1.13. Possuir relatórios pré-definidos;
3.1.14. Possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida;
3.1.15. Possuir a capacidade de personalização de capas para os relatórios,;
3.1.16. Possibilitar, de forma centralizada, a visualização dos logs recebidos por um ou vários dispositivos externos, incluindo a capacidade de uso de filtros nas pesquisas deste log;
3.1.17. Permitir a geração de relatórios de logs de tráfego de dados;
3.1.18. Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos;
3.1.19. Possuir a capacidade de personalização de gráficos como barra, linha, tabela e pizza, para inserção aos relatórios;
3.1.20. Deve possuir mecanismo para exibir de forma detalhada (drill-down) nos relatórios em tempo real (realtime);
3.1.21. Dever ser possível fazer download dos arquivos de logs recebidos;
3.1.22. Possibilitar o envio de maneira automática de relatórios por e-mail;
3.1.23. Deve permitir a escolha do e-mail a ser enviado para cada relatório escolhido;
3.1.24. Permitir programar a geração de relatórios, conforme calendário definido pela contratante;
3.1.25. Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da contratante, adaptando-o às suas necessidades;
3.1.26. Ter a capacidade de definir filtros nos relatórios;
3.1.27. Ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;
3.1.28. Gerar alertas automáticos via e-mail, snmp e syslog baseados em eventos de ocorrência como log, severidade de log, entre outros;
3.1.29. Permitir a criação de painéis (dashboards) customizados para visibilidades do tráfego de aplicativos, categorias de url, ameaças, serviços, países, origem e destino;
3.1.30. Garantir a capacidade de criar consultas sql ou semelhante para uso nos gráficos e tabelas de relatórios;
3.1.31. Garantir a visualização na interface gráfica de usuário (gui) da solução de relatórios de informações do sistema: total de logs diários recebidos, alertas gerados, entre outros;

3.2. GARANTIA E TREINAMENTO

3.2.1. Conforme especificado nos itens ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE GARANTIA e ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE TREINAMENTO do Anexo I.

4. LOTE 01 - ITEM 04 - LICENÇA DE ATUALIZAÇÕES DE SEGURANÇA PARA CONCENTRADOR SECURE SD-WAN

4.1. CONTROLE POR POLÍTICA

4.1.1. Deverá suportar controles por zona de segurança:

4.1.1.1. Controles de políticas por porta e protocolo;

4.1.1.2. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

4.1.1.3. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

4.1.1.4. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

4.1.1.5. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

4.1.1.6. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);

4.1.1.7. Deve suportar o protocolo padrão da indústria VXLAN;

4.2. CONTROLE DE APLICAÇÕES

4.2.1.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

4.2.1.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.2.1.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.2.1.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins,

msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

4.2.1.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

4.2.1.6. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

4.2.1.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

4.2.1.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.2.1.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

4.2.1.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

4.2.1.11. Atualizar a base de assinaturas de aplicações automaticamente;

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

4.2.1.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

4.2.1.14. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.2.1.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

4.2.1.16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

4.2.1.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

4.2.1.18. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os

seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

4.2.1.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

4.2.1.20. Deve alertar o usuário quando uma aplicação for bloqueada;

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

4.2.1.22. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

4.2.1.23. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

4.2.1.24. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

4.2.1.25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

4.2.1.26. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

4.2.1.27. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

4.3. **PREVENÇÃO DE AMEAÇAS**

4.3.1.1. Para proteção do ambiente contra ataques, as licenças devem incluir funções de IPS, Antivírus e Anti-Spyware;

4.3.1.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.3.1.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

4.3.1.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

4.3.1.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

4.3.1.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.3.1.7. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
4.3.1.8. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
4.3.1.9. Deve permitir o bloqueio de vulnerabilidades;
4.3.1.10. Deve permitir o bloqueio de exploits conhecidos;
4.3.1.11. Deve incluir proteção contra-ataques de negação de serviços;
4.3.1.12. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;
4.3.1.13. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;
4.3.1.14. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística;
4.3.1.15. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;
4.3.1.16. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;
4.3.1.17. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;
4.3.1.18. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
4.3.1.19. Detectar e bloquear a origem de portscans;
4.3.1.20. Bloquear ataques efetuados por worms conhecidos;
4.3.1.21. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
4.3.1.22. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.3.1.23. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
4.3.1.24. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
4.3.1.25. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
4.3.1.26. Identificar e bloquear comunicação com botnets;
4.3.1.27. Registrar as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
4.3.1.28. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
4.3.1.29. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

4.3.1.30. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
4.3.1.31. Os eventos devem identificar o país de onde partiu a ameaça;
4.3.1.32. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
4.3.1.33. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

4.4. FILTROS DE URL

4.4.1.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.4.1.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
4.4.1.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
4.4.1.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
4.4.1.5. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
4.4.1.6. Possuir pelo menos 60 categorias de URLs;
4.4.1.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
4.4.1.8. Permitir a customização de página de bloqueio;
4.4.1.9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
4.4.1.10. Além do Explicit Web Proxy, suportar proxy Web transparente;

4.5. FILTROS DE DADOS

4.5.1.1. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.5.1.2. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.5.1.3. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão

de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

5. **LOTE 01 - ITEM 05 – UNIDADE DE SERVIÇO TÉCNICO (UST) PARA IMPLEMENTAÇÃO CUSTOMIZADA E MELHORIAS**
   5.1. O contrato de prestação das unidades de serviço técnico terá duração de 12 (doze) meses, iniciando-se a partir de sua assinatura, podendo ser prorrogado por igual e sucessivo período, até o limite de sessenta meses, a critério do CONTRATANTE, nos termos do art. 57, II da Lei nº 8.666/93, e terá eficácia legal após a publicação do seu extrato no Diário Oficial da União;
   5.2. Os serviços técnicos para a solução de infraestrutura de rede SDWAN não demandarão alocação exclusiva de profissionais do Prestador de Serviços. Os serviços serão executados de forma intermitente sob demanda da JFPB;
   5.3. Cada Unidade de Serviço Técnicos (UST) corresponderá à 4h (quatro horas) de analista / arquiteto especializado na plataforma ofertada para realizar atividades de assessement; desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; tunning; hardening; otimização; troubleshooting; updates; upgrades; provas de conceito; ensaios de contingência; customização de consultas de relatórios; treinamentos “hands on”; análise de vulnerabilidades; criação e manutenção de regras de segurança e redes; participação em comitês de segurança para esclarecimentos; documentação “as built”; documentação para rollout.
   5.4. As atividades deverão ser prestadas na modalidade “on-site”, exceto quando expressamente autorizado por este órgão;
   5.5. Este modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos.
   5.6. A contratada deverá entregar voucher relativos à quantidade de UST contratadas e que serão consumidas ao longo do período de garantia dos equipamentos;
   5.7. As UST serão consumidas sob demanda, de acordo com a necessidade deste órgão. Este órgão consultará a empresa contratada a estimativa de UST para realizar a atividade pretendida e emitirá Ordem de Serviço para execução;
   5.8. O prazo máximo para início das atividades pela empresa contratada será de 05 (cinco) dias úteis;
   5.9. As contabilizações de UST serão feitas individualmente para cada projeto definido pela contratante;
   5.10. As UST executadas fora do horário de 8:00 as 18:00 por solicitação deste órgão, serão contabilizadas e pagas em dobro;

5.11. A liquidação das UST consumidas será efetuada após a apresentação da Nota Fiscal pela CONTRATADA, e o respectivo ateste da equipe de gestão.

ANEXO II

ESPECIFICAÇÕES PADRÃO DE GARANTIA, INSTALAÇÃO, TREINAMENTO E UNIDADES DE SERVIÇOS TÉCNICOS

1. **ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE GARANTIA**
   1.1. Os serviços de garantia, suporte e subscrições de bases de dados de segurança ofertados devem ser serviços do fabricante dos produtos;
   1.2. O Atendimento poderá ser efetuado por empresa contratada, devendo esta comprovar ter em seu quadro de funcionários, técnicos que sejam certificados pelo fabricante da plataforma ofertada como arquitetos e analistas para desenhar, implementar, analisar e configurar.
   1.3. Os serviços de garantia, suporte e subscrições de bases de dados de segurança deverão ter vigência de 60 (sessenta meses), a partir do recebimento dos produtos. A empresa contratada deverá entregar os certificados de garantia e subscrição do fabricante junto com os produtos;
   1.4. Os serviços de garantia, suporte e subscrições de bases de dados de segurança deverão permitir acesso direto do órgão à Central de Suporte Técnico do fabricante através de chamada telefônica gratuita em português e também chat pela web para abertura de chamados com o mesmo, além login de acesso ao Portal Web do fabricante para acesso a boletins técnicos, base de conhecimento técnico, fóruns de discussão, documentação, guias técnicos, download de firmwares, fixes e patches, além de abrir e monitorar os chamados técnicos. Esse serviço deverá estar disponível 24x7 (vinte e quatro horas por dia, sete dias da semana, incluindo finais de semana e feriados).
   1.5. O Serviço de garantia e suporte deve incluir sem custos adicionais para a contratante, a substituição avançada de módulos ou do equipamento completo quando diagnosticado defeito. Isso significa que quando for diagnosticado defeito do equipamento pelo fabricante, o fabricante e/ou a contratada devem remeter módulo ou equipamento completo para substituição, aplicar arquivo de configuração da contratante para que o mesmo esteja funcional e então, recolher o módulo ou equipamento defeituoso. Após conclusão do diagnóstico final da falha, todos os dados do equipamento devem ser apagados e o equipamento totalmente resetado. O módulo ou equipamento substituto de modelo equivalente ou superior ao defeituoso e deve ser enviado para contratante no prazo máximo de dois dias úteis após o diagnóstico, e o serviço “on site”, no prazo máximo de 24h após chegada da parte ou equipamento;
   1.6. O Serviço de garantia e suporte do fabricante deve incluir licenças de uso para atualização de firmware e softwares, bem como, quando contratada Licenças do item 04, a subscrição para atualização das bases de dados de Application Control,

Internet Service, Client ID, IP Geography, Malicious URL, URL Whitelist, Botnet domain, IP Reputation, Anti-virus, Mobile Anti-virus e IPS, e deve incluir também serviços remotos na nuvem do fabricante de Sandbox, Content Disarm & Reconstruct, Virus Outbreak Protection Query, Web Filtering Query, Secure DNS Query e Anti-Spam Query;

2. **ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE INSTALAÇÃO**
   - 2.1. O serviço de instalação e ativação dos equipamentos serão efetuados após aprovação de planejamento de Unidades de Serviços Técnicos, item 05 do lote 01 do TR, junto a empresa CONTRATADA;
   - 2.2. O serviço de instalação/ativação deverá contemplar desembalagem, conferência, montagem, e inicialização básica incluindo conexões elétricas/lógicas, ativação, atualização e testes de verificação;
   - 2.3. Para os itens que exigirem paradas ou risco de parada do equipamento em produção, a instalação deverá ser planejada e ocorrer fora do horário comercial;
   - 2.4. A empresa CONTRATADA deverá informar os requisitos físicos e lógicos para instalação em até 10 (dez) dias após a emissão das notas de empenho;
   - 2.5. O serviço de instalação deverá incluir ativação das licenças e subscrições, orientação sobre navegação no Portal do Fabricante para obter suporte, status da vigência da garantia e subscrições;
   - 2.6. Prazo máximo de execução será de 5 (cinco) dias após emissão da ordem de serviço por parte da CONTRATANTE.

3. **ESPECIFICAÇÃO PADRÃO DO SERVIÇO DE TREINAMENTO**
   - 3.1. O treinamento será efetuado após aprovação de planejamento de Unidades de Serviços Técnicos, item 05 do lote 01 do TR, deverá ser realizado no formato “hands on” / “workshop”, ou seja, 100% prático;
   - 3.2. O especialista deverá ser, preferencialmente, um dos profissionais participantes da implementação da solução, com conhecimento e habilidades para realizar esse tipo de treinamento;
   - 3.3. O treinamento deverá ser realizado nas instalações da CONTRATANTE e utilizar os equipamentos adquiridos neste edital ou laboratório virtual;
   - 3.4. O treinamento deverá contemplar os procedimentos para operação, monitoração e administração, para três profissionais do órgão;
   - 3.5. A carga horária mínima deverá ser de 8h (oito horas) em horário comercial, e deverá ser iniciado até a data da conclusão dos serviços de implementação.