ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO – AVC

AQSETIN2018003 – Firewall de Nova Geração

1. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

1.1. A Solução de Tecnologia da Informação proposta tem por finalidade, promover, através da consecução de novas tecnologias utilizadas em perímetro de segurança da informação, atender as demandas de segurança do Judiciário Cearense e deverá ser capaz de: filtrar pacotes de Internet, controle de aplicações (camada 7), administrar a largura de banda (QoS), proporcionar VPN IPSec e SSL entre as Comarcas e o TJCE, permitir a prevenção contra ameaças de vírus, spywares e malwares, filtrar endereços de Internet, controlar a transmissão de dados e acesso à Internet e o fluxo de dados entre o Data Center e a Internet do TJCE. Deverá ser uma plataforma de segurança integrada e de preferência possuir gerenciamento centralizado e com garantia provido de atualizações de segurança e suporte.

1.1.1. Os Softwares que venham a compor a solução deverão ser licenciados/ativados para funcionamento com as funcionalidades de Controle de Aplicações, Prevenção de Ameaças, Proteção IPS, Proteção Antivírus e Antispyware, Análise de Malwares Modernos, Filtro de URL, Controle de Transferência de Arquivos, Controle de Tráfego, De-criptografia SSL, Módulo VPN, Roteamento e NAT;

1.1.2. Garantia de 60 (sessenta) meses para toda a solução; e

1.1.3. Local para a entrega da solução e execução do Serviços:

1.1.3.1. TJCE – Av. General Afonso Albuquerque Lima, S/N. – Cambeba, CEP: 60822-325, prédio ANEXO – Centro de Documentação e Informática (CDI) – Secretaria de Tecnologia da Informação/Departamento de Infraestrutura de TI.

2. REQUISITOS DE NEGÓCIO DA ÁREA REQUISITANTE

2.1. Necessidades de Negócio

Necessidade	Funcionalidade	Envolvido
Estabelecer canais de	A proteção dos dados trafegados é	Gerência de

comunicação seguro, através de *Virtual Private Network* (VPN), das unidades judiciárias interligadas através das redes GigaFOR e CDC – Cinturão Digital do Ceará; Garantir confidencialidade, integridade e disponibilidade das informações;	provida através da aplicação dos protocolos de criptografia.	Infraestrutura de TI, Coordenadoria de Suporte Técnico e Serviço de Segurança da Informação.
Garantir a segurança de perímetro; Manter e controlar o tráfego de rede e conteúdo *web*; prevenir contra ameaças cibernéticas digitais; Garantir confidencialidade, integridade e disponibilidade das informações;	Aplicação de regras de bloqueios através de *hardware e software c*ompartilhando a conexão com a Internet; Melhorar o desempenho do acesso através de um cache de páginas; Bloquear acesso a determinadas páginas através de filtros (URL) *Uniform Resource Locator.*	

2.2. Demais Requisitos

Requisito	DESCRIÇÃO
Requisitos Legais	Não se aplica.
Requisito De Segurança	O direito de posse e propriedade de todos os artefatos e produtos elaborados pela empresa fornecedora da Solução de Tecnologia da Informação em decorrência do CONTRATO é do Tribunal de

	Justiça do Estado do Ceará, sendo vedada sua cessão, locação ou venda a terceiros; Todas as informações obtidas ou extraídas pela empresa fornecedora da Solução de Tecnologia da Informação quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a mesma zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados. A obrigação assumida de Confidencialidade permanecerá válida durante e também após o período de vigência contratual; As obrigações e conhecimentos sobre os requisitos de segurança serão ratificados pelo TJCE e a empresa fornecedora da solução de TI em documentos posteriores.

3. LEVANTAMENTO DAS ALTERNATIVAS

Solução 1	
Entidade	1. Ministério Público do Trabalho/Procuradoria Geral do Trabalho – Edital 50/2015 Ata de Registro de Preços n.º 75 2. Tribunal de Justiça do Estado de Santa Catarina/TJSC – Pregão Eletrônico n.º 7/2015 3. Companhia de Saneamento Ambiental do Distrito Federal/CAESB – Pregão Eletrônico n.º 3/2016 4. Tribunal de Justiça do Estado do Paraná/TJPR – Pregão Eletrônico n.º 62/2014
Descrição	Registro de preços para futura e eventual contratação de empresa especializada para o fornecimento de solução de segurança de perímetro com características de Next

	Generation Firewall, appliances VPN, bem como fornecimento de garantia pelo período de 60 (sessenta) meses.		
Fornecedor	1. Ntsec Soluções em Teleinformática Ltda – Me 2. Energy Telecom Comércio e Serviços Ltda 3. Blackbull Network 4. Lanlink Soluções	**Valor**	R$ 2.673.883,99

Solução 2			
Entidade	Empresa Municipal de Informática – Edital 004/2016, Ata de Registro de Preços nº 007/2016		
Descrição	Alocação de solução integrada de software e hardware com funcionalidades de firewall, filtro de conteúdo web, prevenção de instrução e Serviços de Monitoramento de Disponibilidade e Performance, Gestão de Eventos de Segurança e Gerenciamento de Segurança de Rede.		
Fornecedor	Energy Telecom Comércio e Serviços Ltda.	Valor	R$ 2.3676.000,00

4. ANÁLISE DAS ALTERNATIVAS EXISTENTES

Quadro-resumo da aplicabilidade dos requisitos elencados no art. 14, II, alíneas “a” a “f”, da Resolução N° 182 do CNJ, para cada uma das alternativas relacionadas no item 3.

Requisito	ID da Solução	Sim	Não	N/A
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	*1*	X	-	-
	2	-	X	-
A Solução está disponível no Portal do Software Público Brasileiro?	*1*		X	
	2		X	
A Solução é um software livre ou software público?	*1*		X	
	2		X	

A Solução é aderente às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário?	*1*			X
	2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	*1*			X
	2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)?	*1*			X
	2			X

5. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

5.1. Identificação

Contratação de empresa especializada para o fornecimento de solução de segurança de perímetro com características de Next Generation Firewall, instalação, configuração e migração, bem como fornecimento de licenças de sofrware e garantia e suporte técnico da solução a ser adquirida, pelo período mínimo de 60 (sessenta) meses.

5.2. Justificativa

Das soluções apresentadas e ofertadas no mercado, foi verificado que a solução poderia ser adquirida de duas formas: a oferta da aquisição dos equipamentos, licenciamento/ativação de software com garantia, incluindo instalação e treinamento na solução por uma ou mais empresas, bem como, a terceirização dos serviços em Segurança de perímetro na forma de o*utsorcing*, incluindo equipamentos, softwares e sua operacionalização, assim como, definição de regras, gestão dos serviços e processos envolvidos.

Após pesquisas na Internet através de sites buscadores, identificamos vários Editais (Pregão Eletrônico N. 7/2015 do TJSC, Pregão Eletrônico N. 101/2013 do BACEN, Pregão Eletrônico N. 62/2014 do TJPR, Pregão Eletrônico N. 3/2016 da CAESB), que tratam de soluções

de perímetros, observamos que a prática nos órgãos públicos têm sido a aquisição dos equipamentos com garantia, instalação e treinamento na solução por uma ou mais empresas. No arquivo publicado através do link: http://www.governoeletronico.gov.br/eixos-de-atuacao/governo/sistema-de-administracao-dos-recursos-de-tecnologia-da-informacao-sisp/ncti-nucleo-de-contratacoes-de-tecnologia-da-informacao/consulta-licitacoes-de-ti, com data base de dados do mês de junho de 2016, para ativos de rede, identificamos 64 itens relacionados a Aquisição de solução em segurança de perímetro, onde apenas uma foi sob a forma de *outsorcing.*

Uma possível desvantagem do *outsourcing* é justamente a falta de segurança. Apesar dos benefícios, não podemos ignorar o fato de que todos os dados do TJCE estarão abertos a outra corporação completamente independente da sua, e por isso não há garantias de que essas informações não serão utilizadas de forma inadequada.

Além disso, está tramitando neste Poder processo administrativo nº 8507856-18.2016.8.06.0000 que trata da Política de Segurança da Informação do TJCE e que esta diz que as informações geradas no âmbito do Poder Judiciário do Estado do Ceará são de sua propriedade e devem ser adequadamente protegidas e utilizadas. Ora, caso a contratação fosse sob a forma de *outsourcing* as informações poderiam ficar desprotegidas, pois a solução seria gerenciada por terceiros e poderia ocorrer vazamento de informações ou roubo de dados.

Do ponto de vista da Segurança da Informação, todas as informações que trafegam na rede do TJCE e necessitam transpor ao ambiente externo, passam por um ponto único e sob a gestão e operacionalização do TJCE, desta forma entendemos que devido as regras de segurança hoje implementadas nos firewall, bem como, as regras que pretendemos implementar para o bloqueio de sites, gerenciamento de aplicações, verificações de vulnerabilidades e a gestão do processo de perímetro de segurança da informação de forma centralizada, não é recomendado a contratação da solução de segurança de perímetro sob a forma de *outsourcing.* Desta forma, descartamos a solução 2 que trata o objeto como “Alocação de solução integrada de software e hardware”.

Optamos pela solução 1, onde hoje em dia é a mais utilizada por órgãos de todas as esferas do Brasil, sendo realizado pregão eletrônico pelo TJCE.

Para interligação das comarcas do interior e o TJCE através do Cinturão Digital é

preciso da infraestrutura de última milha de fibra que é de responsabilidade da ETICE (Empresa de Tecnologia do Ceará). Conforme o planejamento da ETICE, está previsto a entrega de 8 (oito) comarcas com infraestrutura de última milha de fibra até o final de 2016 e o restante ao longo do ano de 2017. Também temos que, por questões de falta de infraestrutura (conexões lógicas e elétricas) do data center do FCB para receber novos equipamentos concentradores de firewall, parte dos itens para atender a solução deverão ser adquiridos em 2016 e a outra parte em 2017, quando a infraestrutura estiver disponível. A realização de pregão eletrônico proporcionará ao TJCE adquirir os itens de forma parcelada de acordo com o planejado para os anos de 2016 e 2017.

5.3. Descrição

5.3.1. Compreende a solução de segurança de perímetro o fornecimento de:

5.3.1.1. Appliances Next Generation Firewall em Cluster, para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo, licenciado/ativado para funcionamento com as funcionalidades de Controle de Aplicações, Prevenção de Ameaças, Proteção IPS, Proteção Antivírus e Antispyware, Análise de Malwares Modernos, Filtro de URL, Controle de Transferência de Arquivos, Controle de Tráfego, De-criptografia SSL, Módulo VPN, Roteamento, NAT, Gerenciamento e com garantia durante 60 (sessenta) meses conforme descrito no **ANEXO I – ESPECIFICAÇÕES TÉCNICAS e ANEXO II – GARANTIA E SUPORTE TÉCNICO**.

5.3.1.2. Instalação, Configuração e Migração, conforme descrito no **ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO**.

5.4. Bens que Compõem a Solução

ITEM	DESCRIÇÃO	UNIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Plataforma de Segurança em cluster, no mínimo: 02 (dois) Firewalls de Próxima, para operar em alta disponibilidade em	UND	1		

	modo ativo-passivo ou ativo-ativo. Serviço de instalação e configuração devem estar incluídos.				
2	Garantia da Solução de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em Português por autorizada credenciada e com serviço de suporte técnico remoto por 12 meses a ser prestado pela CONTRATADA.	Mes	60		
3	Software com licenciamento de uso perpétuo para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução em cluster. Com no mínimo, 60 meses de suporte.	Licença	1		
4	Módulo de Interface 1000BASE-T	UND	2		
5	Módulo de interface 10GBASE-SR	UND	14		
6	Software para Gerenciamento da Solução de Segurança em cluster.	UND	1		
7	Garantia do Software para Gerenciamento da Solução	Mes	60		

	de Segurança em cluster com Suporte Oficial do fabricante, através da Contratada, 24x7 fornecido no Brasil em Português. Com no mínimo, 60 meses de suporte.				
VALOR GLOBAL					

5.5. Relação entre a demanda e a quantidade

Id	Demanda Prevista	Bem/Serviço	Unidade de Medida	Quantidade
1	Está previsto a aquisição de 01 Cluster com 02 *appliance*, Instalação, Configuração e Migração, bem como Software de Gerenciamento para e licenciamento para para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução. em cluster .	Solução de Plataforma de Segurança em cluster, no mínimo: 02 (dois) Firewalls de Próxima, para operar em alta disponibilidade em modo ativo passivo ou ativo Geração. Serviço de instalação e configuração devem estar incluídos.	UND	02
2		Garantia da Solução de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em Português por autorizada credenciada e com serviço de suporte técnico remoto por 12 meses a ser prestado pela CONTRATADA.	MES	60
3		Software com licenciamento de uso perpétuo para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução em cluster. Com no mínimo, 60 meses de suporte.	Licença	01

4		Módulo de Interface 1000BASE-T	UND	2
5		Módulo de interface 10GBASE-SR	UND	14
6		Software com licenciamento perpétuo para Gerenciamento da Solução de Segurança em cluster.	Licença	1
7		Garantia do Software para Gerenciamento da Solução de Segurança em cluster com Suporte Oficial do fabricante, através da Contratada, 24x7 fornecido no Brasil em Português. Com no mínimo, 60 meses de suporte.	MES	60

5.6. Benefícios Esperados

Benefícios/Descrição
Manutenção e controle do tráfego de rede; Filtrar conteúdo Web e de dados; Prevenir a rede interna contra ameaças cibernéticas digitais; Estabelecer canal de comunicação seguro através da VPN; Aumentar a proteção da rede interna contra possíveis tentativas de acesso indevido; Implementar mecanismos de proteção, prevenção de intrusão.

6. PESQUISA MERCADOLÓGICA

6.1. ANEXO II

7. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

Será necessário adequações em conectividade: como instalação de Switch 2960, confecção de cabos de fibra ótica e verificação quanto a pontos elétricos.

8. APROVAÇÕES

Alexys Ribeiro Negreiros – 8201
Integrante Técnico

Adarildo de Brito Figueiredo – 8025
Integrante Requisitante

Werley da Silva Almeida – 22722
Integrante Administrativo

Fortaleza, 09 de maio de 2017

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1 ESPECIFICAÇÕES MÍNIMAS

1.1 A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

1.1.1 Throughput de 10 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

1.1.2 Throughput de 5 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;

1.1.3 Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o

direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;

1.1.4 Não será aceito a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

1.1.5 Quando as funcionalidades de controle de aplicação, IPS, antivírus e antispyware tiverem habilitadas de forma simultânea o tráfego deverá ser inspecionado de modo bidirecional com inspeção em toda a sessão do pacote, sem qualquer utilização de recurso de by-pass. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.

1.1.6 Suporte a, no mínimo, 2.000.000 de conexões simultâneas;

1.1.7 Suporte a, no mínimo, 110.000 novas conexões por segundo;

1.1.8 Fonte 120/240 AC ou DC, redundante e hot-swappble;

1.1.9 Cooler hot-swappble;

1.1.10 Disco Solid State Drive (SSD) redundante de, no mínimo, 240 GB.

1.1.11 12 (doze) interfaces de rede 1/10 Gbps SFP;

1.1.12 2 (duas) Gbps interfaces dedicadas para alta disponibilidade;

1.1.13 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

1.1.14 1 (uma) interface do tipo console ou similar;

1.1.15 Suporte a, no mínimo, 100 (cem) roteadores virtuais;

1.1.16 Suporte a, no mínimo, 400 (quatrocentas) zonas de segurança;

1.1.17 Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;

1.1.18 Estar licenciada para ou suportar sem o uso de licença, 4.000 (quatro mil) túneis de VPN IPSEC simultâneos;

1.2 Deve suportar, no mínimo, 25 sistemas virtuais lógicos (Contextos) no firewall Físico;

1.3 Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;

1.4 Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

1.5 Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;

1.6 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

1.7 Deve estar coberto por garantia no Brasil do próprio fabricante dos equipamentos por 60 (sessenta) meses, compreendendo atualizações e correções de sistema

operacional, atualização da base de aplicações, IPS, Antivírus, Anti – Spyware e demais funcionalidades requeridas neste processo e que dependem de atualização.

2 CARACTERÍSTICAS GERAIS

2.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

2.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

2.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

2.4 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

2.5 O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

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

2.7 O software deverá ser fornecido em sua versão mais atualizada;

2.8 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

2.8.1 Suporte a 4094 VLAN Tags 802.1q;

2.8.2 Agregação de links 802.3ad e LACP;

2.8.3 Policy based routing ou policy based forwarding;

2.8.4 Roteamento multicast (PIM-SM);

2.8.5 DHCP Relay;

2.8.6 DHCP Server;

2.8.7 Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

2.8.8 Suportar sub-interfaces ethernet logicas.

2.8.9 Deve suportar os seguintes tipos de NAT:

2.8.9.1 Nat dinâmico (Many-to-1);

2.8.9.2 Nat dinâmico (Many-to-Many);

2.8.9.3 Nat estático (1-to-1);

2.8.9.4 NAT estático (Many-to-Many);

2.8.9.5 Nat estático bidirecional 1-to-1;

2.8.9.6 Tradução de porta (PAT);

2.8.9.7 NAT de Origem;

2.8.9.8 NAT de Destino;

2.8.9.9 Suportar NAT de Origem e NAT de Destino simultaneamente;

2.8.10 Deve implementar Network Prefix Translation (NPTv6), prevenindo

problemas de roteamento assimétrico;

2.8.11 Deve implementar o protocolo ECMP;

2.8.12 Deve implementar balanceamento de link por hash do IP de origem;

2.8.13 Deve implementar balanceamento de link por hash do IP de origem e destino;

2.8.14 Deve implementar balanceamento de link através do método round-robin;

2.8.15 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

2.8.16 Deve suportar o balanceamento de, no mínimo, quarto links;

2.8.17 Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

2.8.18 Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;

2.8.19 Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;

2.8.20 Enviar log para sistemas de monitoração externos, simultaneamente;

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

2.8.22 Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

2.8.23 Proteção contra anti-spoofing;

2.8.24 Deve permitir bloquear sessoes TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

2.8.25 Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

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

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

2.8.28 Suportar a OSPF graceful restart;

2.8.29 Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;

2.8.30 O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces

físicas nos seguintes modos:

2.8.30.1 Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);

2.8.30.2 Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

2.8.30.3 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

2.8.30.4 Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

2.8.30.5 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

2.8.31 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

2.8.31.1 Em modo transparente;

2.8.31.2 Em layer 3;

2.8.32 A configuração em alta disponibilidade deve sincronizar:

2.8.32.1 Sessões;

2.8.32.2 Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

2.8.32.3 Certificados de-criptografados;

2.8.32.4 Associações de Segurança das VPNs;

2.8.32.5 Tabelas FIB;

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

2.8.33 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH;

2.8.34 Decryption e protocolos de roteamento dinâmico 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.

3 CONTROLE POR POLÍTICA DE FIREWALL

3.1 Deverá suportar controles por zona de segurança.

3.2 Controles de políticas por porta e protocolo.

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

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

3.5 Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do

tráfego.

3.6 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

3.7 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

3.8 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

3.9 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

3.10 Controle de inspeção e de-criptografia de SSH por política;

3.11 A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

3.12 A plataforma de segurança deve implementar espelhamento de tráfego decriptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

3.13 É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.

3.14 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

3.15 Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

3.16 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

3.17 Suporte a objetos e regras IPV6.

3.18 Suporte a objetos e regras multicast.

3.19 Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall:

3.19.1 Drop sem notificação do bloqueio ao usuário;

3.19.2 Drop com opção de envio de ICMP;

3.19.3 Unreachable para máquina de origem do tráfego;

3.19.4 TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

3.20 Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4 CONTROLE DE APLICAÇÕES

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

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

4.1.2 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;

4.1.3 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, etc;

4.1.4 Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

4.1.5 Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

4.1.6 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 ataques mediante a porta 443;

4.1.7 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;

4.1.8 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. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

4.1.9 Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

4.1.10 Identificar o uso de táticas evasivas via comunicações criptografadas;

4.1.11 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.12 Reconhecer aplicações em IPv6;

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

4.1.14 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;

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

4.1.16 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

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

4.1.18 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, mantendo a confidencialidade das aplicações do órgão;

4.2 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:

4.2.1 HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

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

4.4 Deve alertar o usuário quando uma aplicação for bloqueada;

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

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

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

4.8 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

4.9 Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;

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

4.10.1 Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

4.10.2 Nível de risco da aplicação;

4.10.3 Categoria e sub-categoria de aplicações;

4.10.4 Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

5 PREVENÇÃO DE AMEAÇAS

5.1 Para proteção do ambiente contra ataques, os dispositivos de proteção devem

possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;

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

5.3 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;

5.4 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

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

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

5.7 Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

5.8 Deve suportar granularidade nas politicas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

5.9 Deve permitir o bloqueio de vulnerabilidades;

5.10 Deve permitir o bloqueio de exploits conhecidos;

5.11 Deve incluir proteção contra-ataques de negação de serviços;

5.12 Deverá possuir os seguintes mecanismos de inspeção de IPS:

- 5.12.1 Análise de padrões de estado de conexões;
- 5.12.2 Análise de decodificação de protocolo;
- 5.12.3 Análise para detecção de anomalias de protocolo;
- 5.12.4 Análise heurística;
- 5.12.5 IP Defragmentation;
- 5.12.6 Remontagem de pacotes de TCP;
- 5.12.7 Bloqueio de pacotes malformados.

5.13 Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

5.14 Detectar e bloquear a origem de portscans;

5.15 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

5.16 Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

5.17 Possuir assinaturas específicas para a mitigação de ataques DoS e DdoS;

5.18 Possuir assinaturas para bloqueio de ataques de buffer overflow;
5.19 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
5.20 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
5.21 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos:
 5.21.1 HTTP, FTP, SMB, SMTP e POP3;
5.22 É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;
5.23 Suportar bloqueio de arquivos por tipo;
5.24 Identificar e bloquear comunicação com botnets;
5.25 Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
5.26 Deve suportar referencia cruzada com CVE;
5.27 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
 5.27.1 O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
5.28 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;
5.29 Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;
5.30 Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
5.31 Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
5.32 Os eventos devem identificar o país de onde partiu a ameaça;
5.33 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
5.34 Proteção contra downloads involuntários usando HTTP de arquivos executáveis;
5.35 Rastreamento de vírus em pdf;
5.36 Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
5.37 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em politicas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada politica de firewall poderá ter uma configuração diferentes de IPS, sendo essas politicas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

6 ANÁLISE DE MALWARES MODERNOS

6.1 Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

6.2 O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

6.3 Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

6.4 Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

6.5 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

6.6 Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);

6.7 Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

6.8 A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

6.9 Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

6.10 O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

6.11 O sistema automático de analise "In Cloud" ou local deve emitir relatório com

identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

6.12 Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

6.13 Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

6.14 Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

6.15 Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência;

6.16 Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

6.17 Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

6.18 Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado.

7 FILTRO DE URL

7.1 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

7.1.1 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);

7.1.2 Deve ser possível a criação de politicas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

7.1.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

7.1.4 Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

7.1.5 Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

7.1.6 Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

7.1.7 Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

7.1.8 Possui pelo menos 60 categorias de URLs;

7.1.9 A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
7.1.10 Suporta a criação categorias de URLs customizadas;
7.1.11 Suporta a exclusão de URLs do bloqueio, por categoria;
7.1.12 Permite a customização de página de bloqueio;
7.1.13 Permite 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);
7.1.14 A funcionalidade de Filtro de URL deve operar em caráter permanente, para base ou cache instalado na solução até a data de vencimento da licença, 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;
7.1.15 Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
7.1.16 Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

8 IDENTIFICAÇÃO DE USUÁRIOS

8.1 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;
8.2 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;
8.3 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
8.4 Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
8.5 Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
8.6 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
8.7 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);

8.8 Suporte a autenticação Kerberos;

8.9 Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

8.10 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;

8.11 Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

8.12 Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;

8.13 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

8.14 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

9 QOS

9.1 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 máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

9.2 Suportar a criação de políticas de QoS por:

- 9.2.1 Endereço de origem;
- 9.2.2 Endereço de destino;
- 9.2.3 Por usuário e grupo do LDAP/AD;
- 9.2.4 Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 9.2.5 Por porta;

9.3 O QoS deve possibilitar a definição de classes por:

- 9.3.1 Banda Garantida;
- 9.3.2 Banda Máxima;
- 9.3.3 Fila de Prioridade.

9.4 Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

9.5 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

9.6 Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos

na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

9.7 Disponibilizar estatísticas RealTime para classes de QoS;

9.8 Deve suportar QOS (traffic-shapping), em interface agregadas;

9.9 Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

10 FILTRO DE DADOS

10.1 Permite a criação de filtros para arquivos e dados pré-definidos;

10.2 Os arquivos devem ser identificados por extensão e assinaturas;

10.3 Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

10.4 Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;

10.5 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;

10.6 Permitir listar o número de aplicações suportadas para controle de dados;

10.7 Permitir listar o número de tipos de arquivos suportados para controle de dados;

11 Geo-localização

11.1 Suportar a criação de politicas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.

11.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

11.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.

12 VPN

12.1 Suportar VPN Site-to-Site e Cliente-To-Site;

12.2 Suportar IPSec VPN;

12.3 Suportar SSL VPN;

12.4 A VPN IPSEc deve suportar:

12.4.1 DES e 3DES;

12.4.2 Autenticação MD5 e SHA-1;

12.4.3 Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

12.4.4 Algoritmo Internet Key Exchange (IKEv1 e v2);

12.4.5 AES 128, 192 e 256 (Advanced Encryption Standard)

12.4.6 Autenticação via certificado IKE PKI.

12.5 Deve possuir interoperabilidade com os seguintes fabricantes:

12.5.1 Cisco;
12.5.2 Checkpoint;
12.5.3 Juniper;
12.5.4 Palo Alto Networks;
12.5.5 Fortinet;
12.5.6 Sonic Wall;

12.6 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

12.7 A VPN SSL deve suportar:

12.7.1 O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
12.7.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
12.7.3 Atribuição de endereço IP nos clientes remotos de VPN SSL;
12.7.4 Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
12.7.5 Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
12.7.6 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;
12.7.7 Atribuição de DNS nos clientes remotos de VPN;
12.7.8 Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
12.7.9 A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
12.7.10 Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
12.7.11 Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
12.7.12 Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
12.7.13 Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
12.7.14 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN

SSL;

12.7.15 A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

12.7.16 Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

12.7.17 Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

12.7.18 Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;

12.7.19 Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

12.7.20 Suporta leitura e verificação de CRL (certificate revocation list);

12.7.21 Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

12.7.22 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

12.7.23 O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;

12.7.24 Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

12.7.24.1 Antes do usuário autenticar na estação;

12.7.24.2 Após autenticação do usuário na estação;

12.7.24.3 Sob demanda do usuário;

12.7.25 Deverá manter uma conexão segura com o portal durante a sessão.

12.7.26 O agente de VPN SSL client-to-site deve ser compatível com pelo menos:

12.7.26.1 Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;

12.7.27 O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;

12.7.28 Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

12.7.29 Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

13 CONSOLE DE GERÊNCIA E MONITORAÇÃO

13.1 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

13.2 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
13.3 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
13.4 O gerenciamento deve permitir/possuir:
- 13.4.1 Criação e administração de políticas de firewall e controle de aplicação;
- 13.4.2 Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 13.4.3 Criação e administração de políticas de Filtro de URL;
- 13.4.4 Monitoração de logs;
- 13.4.5 Ferramentas de investigação de logs;
- 13.4.6 Debugging;
- 13.4.7 Captura de pacotes.

13.5 Acesso concorrente de administradores;
13.6 Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.
13.7 Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
13.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
13.9 Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
13.10 Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;
13.11 Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
13.12 Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
13.13 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
13.14 Autenticação integrada ao Microsoft Active Directory e servidor Radius;
13.15 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
13.16 Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
13.17 Criação de regras que fiquem ativas em horário definido;
13.18 Criação de regras com data de expiração;
13.19 Backup das configurações e rollback de configuração para a última configuração salva;

13.20 Suportar Rollback de Sistema Operacional para a ultima versão local;
13.21 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
13.22 Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
13.23 Validação de regras antes da aplicação;
13.24 Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
13.24.1 É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
13.25 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
13.25.1 É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
13.26 Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
13.27 Deve possibilitar a integração com outras soluções de SIEM de mercado (thirdparty SIEM vendors).
13.28 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
13.29 Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
13.30 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
13.31 Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS,Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
13.32 Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;
13.33 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
13.34 Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.
13.35 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;
13.36 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS,

Antivírus e Anti-Spware), e URLs que passaram pela solução;

13.37 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

13.38 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

13.39 Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

13.40 Deve ser possível exportar os logs em CSV;

13.41 Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

13.42 Rotação do log;

13.43 Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

13.44 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

- 13.44.1 Situação do dispositivo e do cluster;
- 13.44.2 Principais aplicações;
- 13.44.3 Principais aplicações por risco;
- 13.44.4 Administradores autenticados na gerência da plataforma de segurança;
- 13.44.5 Número de sessões simultâneas;
- 13.44.6 Status das interfaces;
- 13.44.7 Uso de CPU.

13.45 Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

- 13.45.1 Resumo gráfico de aplicações utilizadas;
- 13.45.2 Principais aplicações por utilização de largura de banda de entrada e saída;
- 13.45.3 Principais aplicações por taxa de transferência de bytes;
- 13.45.4 Principais hosts por número de ameaças identificadas;
- 13.45.5 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;
- 13.45.6 Deve permitir a criação de relatórios personalizados;

13.46 Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP’s distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

13.47 Gerar alertas automáticos via:

- 13.47.1 Email;
- 13.47.2 SNMP;

13.47.3 Syslog.

13.48 A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

ANEXO II – GARANTIA E SUPORTE TÉCNICO

1 A solução fornecida deverá estar coberta por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção ou montagem, pelo período mínimo especificado individualmente em cada item, a contar da data de emissão da nota fiscal;

2 Durante o período de garantia, deve ser possível realizar a atualização de software (firmware) dos equipamentos para resolução de problemas de software (correção de bugs);

3 A garantia deve incluir envio de peças/equipamentos de reposição nos locais especificados contratualmente;

4 Os chamados serão abertos diretamente com a empresa fornecedora da solução através de ligação telefônica, website e/ou email. O suporte da empresa fornecedora da solução deverá operar de segunda a sexta-feira, das 8 às 18 horas. O atendimento inicial deverá ocorrer em até 4 horas

úteis;

5 A empresa fornecedora da solução deverá disponibilizar um portal web 24x7 com sistema de help-desk para abertura de chamados de suporte técnico. Mediante login e senha de acesso ao sistema, os membros da equipe técnica da contratante poderão abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico;

6 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

7 A empresa fornecedora da solução deverá prestar o suporte de primeiro nível e caso julgue necessário poderá escalar o suporte ao fabricante dos equipamentos, ficando a empresa fornecedora da solução responsável por gerenciar o chamado durante todo o tempo em que o mesmo permanecer aberto;

8 A empresa fornecedora da solução poderá recorrer ao suporte do fabricante quando se tratarem de correções especiais, defeitos nos programas (firmwares) ou defeitos em hardwares que necessitem de reparos especiais, correções de bugs ou substituições de peças e/ou equipamentos;

9 Detectada a necessidade de substituição de peças/equipamentos, o envio do substituto deverá ocorrer em até 30 (trinta) dias úteis ou conforme especificado individualmente em cada item (prevalecendo o de menor prazo menor). A empresa fornecedora da solução deverá arcar com os custos do deslocamento do envio da peça de substituição, ficando a contratante responsável pelo envio da peça defeituosa;

10 Deve ser possível o contato direto da contratante com o fabricante dos equipamentos em horários não compreendidos pelos suportes da empresa fornecedora da solução, ou quando a contratante julgar necessário. O suporte do fabricante dos equipamentos deve operar em regime 24x7 (24 horas por dia, 7 dias por semana), com atendimento através de ligação telefônica para atendimentos emergenciais;

11 Não serão aceitos suportes compartilhados para envio de peças de reposição (shared support);

12 A empresa deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos equipamentos ou diretamente com o fabricante dos equipamentos.

13 Os serviços de suporte técnico remoto deverá atender as seguintes premissas:

13.1 A empresa fornecedora da solução deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, website e e-mail;

13.2 As ligações deverão ser gratuitas, adotando-se o sistema 0800;

13.3 A empresa fornecedora da solução deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de chamados de suporte técnico;

13.4 A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;

13.5 Os chamados abertos por e-mail deverão ter sua abertura automática no portal web;

13.6 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

13.7 A empresa fornecedora da solução deverá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a empresa fornecedora da solução responsável pelo gerenciamento do chamado e prestação de informações à contratante;
13.8 A empresa fornecedora da solução deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico.
13.9 A empresa fornecedora da solução deverá alocar até 4 horas mensais, no máximo, durante o intervalo de garantia do equipamento, sem custo adicional, não cumulativo e vedada ultrapassar esse intervalo, para atendimento remoto de demandas de manutenção, conforme necessidade da Contratante. Chamados técnicos da garantia dos produtos não estão compreendidos neste intervalo mensal.
13.10 As horas de atendimento serão realizadas normalmente em horário comercial, no período compreendido entre 08:30 e 18:30h, em dias de semana (segunda à sexta);
13.11 Horas que porventura precisem ser realizadas fora do horário comercial serão contabilizadas de acordo com a tabela:

Horário de Trabalho	Contabilização de horas (fator de conversão)
Entre 08:30 e 18:30 (dias de semana, segunda à sexta)	Cada hora trabalhada equivale a 1h
Entre 18:31 e 08:29 (dias de semana, segunda à sexta)	Cada hora trabalhada equivale a 1,5h
Em finais de semana (sábados e domingos)	Cada hora trabalhada equivale a 2h
Em feriados nacionais, estaduais e municipais	Cada hora trabalhada equivale a 2h

14 Prestação de serviços que compreendem, entre outros, os seguintes procedimentos de serviços da Solução de Plataforma de Segurança:
14.1 Alteração de qualquer configuração de topologia que esta Corte julgue necessário;
14.2 Habilitar licenças que porventura sejam adquiridas;
14.3 Sanar dúvidas relacionadas ao funcionamento dos equipamentos;
14.4 Administração e configuração da Solução de Gerenciamento Centralizado de firewall;
14.5 Suporte em caso de indisponibilidade de links e interfaces do cluster de firewall;
14.6 Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários desta Corte que dependam do cluster de firewall;
14.7 Suporte à configuração e resolução de problemas de acessos remotos VPNs client-to-site;
14.8 Suporta à configuração e resolução de problemas de VPNs site-to-site entre o cluster de firewall e outros equipamentos quando solicitado;

14.9 Suporte quanto a problemas de identificação de usuários;
14.10 Suporte quanto a de problemas de desconexão de aplicações;
14.11 Auxilio quanto as atualizações de sistema operacional e assinaturas de aplicação, prevenção de ameaças e filtro de URL;
14.12 Configurações e resolução de problemas quanto a funcionalidades aplicação, prevenção de ameaças e filtro de URL;
14.13 Realizar alterações de regras de roteamento estático, roteamento dinâmico (OSPF e BGP), PBF (Policy Base Routing) e tipos de NAT quando solicitado;
14.14 Realizar liberações ou bloqueios de aplicações quando solicitado;
14.15 Auxílio na customização de relatórios disponíveis na solução;
14.16 Verificação de funcionamento de regras;
14.17 Suporte na configuração de de-criptografia HTTPs inbound e outbound;
14.18 Auxílio na configuração de contextos virtuais;
14.19 Realizar manutenções preventivas do cluster de firewall quando solicitado;
14.20 Suporte em demais configurações de segurança, redundância e gerência;
14.21 Realizar otimização de performance (“tunning”) da solução de firewall;
14.22 Apoio técnico em configurações de alta disponibilidade, redundância e gerência de controladoras e pontos de acesso;
14.23 Suporte, administração e monitoramento das políticas e tarefas de backup;
14.24 Apoio técnico para tarefas de auditoria e análise de logs;
14.25 Encaminhar incidentes ao fabricante da solução;
14.26 Suporte técnico para identificação e resolução de problemas em software e hardware.

ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO

1 A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência;
2 O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter o objetivo dos serviços, as atividades que serão realizadas, os prazos estimados para cada atividade, as diretrizes dos serviços que serão realizados, os locais de execução, as informações necessárias, os padrões que serão aplicados, o nome do(s) gerente(s) de projetos responsável e do(s) técnico(s) responsável(is) pela execução dos serviços. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

3 Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a empresa fornecedora da solução sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

4 Após a instalação deve ser monitorado pelo prazo mínimo de 24 horas corridas as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação;

5 Ao final da instalação, deverá ser realizado o repasse de informações hands-on, apresentando as configurações realizadas nos equipamentos, de no mínimo 2 (duas) horas, ou conforme disposto individualmente em cada item (prevalecendo o disposto em individualmente em cada item). A contratante disponibilizará o local adequado para a transferência do conhecimento e acesso aos equipamentos de produção;

6 Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a contratante poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

7 Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

8 Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da contratante.

ANEXO IV– PESQUISA MERCADOLÓGICA

EMPRESA A					
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Appliances Next Generation Firewall para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo, licenciado/ativado para funcionamento com as funcionalidades de Controle de Aplicações, Prevenção de Ameaças, Proteção IPS, Proteção Antivírus e Antispyware, Análise de Malwares Modernos, Filtro de URL, Controle de Transferência de Arquivos, Controle de Tráfego, De-criptografia SSL, Módulo VPN, Roteamento e NAT e	UND	02		

	conforme descrito no **ANEXO I – ESPECIFICAÇÕES TÉCNICAS e ANEXO II – GARANTIA E SUPORTE TÉCNICO**, com garantia durante 60 (sessenta) meses.				
	Software de Gerência. Conforme **ANEXO I – ESPECIFICAÇÕES TÉCNICAS**.		01		
	Instalação, Configuração e Migração. Conforme **ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO**.		01		
			TOTAL		

EMPRESA B					
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Appliances Next Generation Firewall para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo, licenciado/ativado para funcionamento com as funcionalidades de Controle de Aplicações, Prevenção de Ameaças, Proteção IPS, Proteção Antivírus e Antispyware, Análise de Malwares Modernos, Filtro de URL, Controle de Transferência de Arquivos, Controle de Tráfego, De-criptografia SSL, Módulo VPN, Roteamento e NAT e conforme descrito no **ANEXO I – ESPECIFICAÇÕES TÉCNICAS e ANEXO II – GARANTIA E SUPORTE TÉCNICO**, com garantia durante 60 (sessenta) meses.	UND	02		
	Software de Gerência. Conforme **ANEXO I – ESPECIFICAÇÕES TÉCNICAS**.		01		
	Instalação, Configuração e Migração. Conforme **ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO**.		01		
			TOTAL		

EMPRESA C					
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Appliances Next Generation Firewall para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo, licenciado/ativado para	UND	02		

	funcionamento com as funcionalidades de Controle de Aplicações, Prevenção de Ameaças, Proteção IPS, Proteção Antivírus e Antispyware, Análise de Malwares Modernos, Filtro de URL, Controle de Transferência de Arquivos, Controle de Tráfego, De-criptografia SSL, Módulo VPN, Roteamento e NAT e conforme descrito no **ANEXO I – ESPECIFICAÇÕES TÉCNICAS e ANEXO II – GARANTIA E SUPORTE TÉCNICO**, com garantia durante 60 (sessenta) meses.				
	Software de Gerência. Conforme **ANEXO I – ESPECIFICAÇÕES TÉCNICAS**.		01		
	Instalação, Configuração e Migração. Conforme **ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO**.		01		
			TOTAL		

VALORES MÉDIOS					
ITEM	**DESCRIÇÃO**	**UNIDADE**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Appliances Next Generation Firewall para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo, licenciado/ativado para funcionamento com as funcionalidades de Controle de Aplicações, Prevenção de Ameaças, Proteção IPS, Proteção Antivírus e Antispyware, Análise de Malwares Modernos, Filtro de URL, Controle de Transferência de Arquivos, Controle de Tráfego, De-criptografia SSL, Módulo VPN, Roteamento e NAT e conforme descrito no **ANEXO I – ESPECIFICAÇÕES TÉCNICAS e ANEXO II – GARANTIA E SUPORTE TÉCNICO**, com garantia durante 60 (sessenta) meses.	UND	02		
	Software de Gerência. Conforme **ANEXO I – ESPECIFICAÇÕES TÉCNICAS**.		01		
	Instalação, Configuração e Migração. Conforme **ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO**.		01		
			TOTAL		