SOLICITAÇÃO DE ABERTURA DE PROCESSO LICITATÓRIO

PRESTAÇÃO DE SERVIÇOS

SETOR REQUISITANTE:
CPD

1. SERVIÇO (EXEMPLO: SERVIÇOS PERTINENTES AO SETOR):
1.1 Contratação de pessoa jurídica prestadora de serviços de suporte, remoto, telefônico e on-site em soluções de infraestrutura e segurança da informação com comodato de solução de 01 firewall do tipo NGFW (Next-Generation Firewall), incluindo serviço de migração, instalação, configuração e treinamento para a Farmácia do IPAM.

2. JUSTIFICATIVA DA NECESSIDADE DE CONTRATAÇÃO:
2.1 Término do contrato ref. ao processo 05/2021 e Pregão Presencial 02/2021.

3. CARACTERÍSTICAS DO OBJETO E DA PRESTAÇÃO DOS SERVIÇOS

3.1 Instalação, configuração, suporte e manutenção dos seguintes serviços em ambientes:

3.1.1 Tecnologia LAMP(Linux, Apache, MySQL e PHP);

3.1.2 Integração LDAP/Active Directory.

3.2 Instalação, configuração, suporte e manutenção das Soluções:

3.2.1 Virtualização;

3.2.2 Suporte ao sistema de E-mail com no mínimo 50 (cinquenta) usuários;

3.2.3 Suporte ao NG-Firewall ofertado.

4. Características Técnicas da Solução

4.1 Firewall NGFW:

4.1.1 Firewall:

4.1.1.1 Permitir a criação de regras de firewall de forma a liberar ou bloquear acessos operando no formato stateful firewall;

4.1.1.2 Permitir vínculo das regras de firewall com objetos (zonas, endereços, portas, protocolos, aplicações, usuário e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo, de acordo com a granularidade que atenda às necessidades da Farmácia do IPAM;

4.1.1.3 Permitir vínculo das regras de firewall com país de origem e país de destino das conexões;

4.1.1.4 Permitir a criação de regras de firewall com período de validade de forma programada (data e horário iniciais e finais);

4.1.1.5 Permitir a tradução de endereços, de forma estática e dinâmica, por meio de NAT (Network Address Translation) nos formatos um-para-um e muitos-para-um, inclusive NAT64, NAT46 e NAT66;

4.1.1.6 Permitir a tradução de portas PAT (Port Address Translation) nos formatos um-para-um e muitos-para-um;

4.1.1.7 Permitir a configuração de DHCP Server e DHCP Relay para cada uma das zonas de firewall, nos protocolos IPv4 e IPv6, com características próprias em cada zona de firewall;

4.1.1.8 Permitir a configuração de roteamento estático e dinâmico utilizando RIP, BGP e OSPF para os protocolos IPv4 e Ipv6;

4.1.1.9 Permitir OSPF graceful restart;

4.1.1.10 Permitir Policy Based Routing ou Policy Based Forwarding;

4.1.1.11 Permitir roteamento multicast no protocolo PIM Sparse Mode;

4.1.1.12 Permitir a customização da página de bloqueio de forma a informar ao usuário que o acesso não foi autorizado, bem como o motivo pelo qual o bloqueio ocorreu.

4.1.2 Filtro Web e Controle de Aplicações:

4.1.2.1 Permitir a criação de regras de filtro web e controle de aplicações de forma a liberar, bloquear ou limitar acessos;

4.1.2.2 Permitir vínculo das regras de filtro web e controle de aplicações em qualquer das regras de firewall previamente cadastradas, com a granularidade que atenda às necessidades da Farmácia do IPAM;

4.1.2.3 Permitir vínculo das regras de filtro web com categorias de sites, dispostas em uma base de dados catalogada e mantida pelo fabricante da solução, distribuídas por conteúdo do site em categorias distintas;

4.1.2.3.1 As categorias de sites devem possuir, no mínimo, agrupamentos baseados nas seguintes características: Conexão Remota, Compartilhamento de Conteúdo, Mensagens

Instantâneas, Multimídia (áudio, vídeo, streaming), Comunicação (telefonia, videochamadas), Proxy, Phising, Spam, Hacking, Websites Maliciosos, Redes Sociais, Entretenimento, Games/Jogos, Pornografia/Pedofilia, Violência, Drogas, Sites Ilegais, Comércio Eletrônico, Finanças, Governo, Organizações Sociais, Propaganda;

4.1.2.4 Permitir a criação de categorias de sites específicas conforme necessidades da Farmácia do IPAM;

4.1.2.5 Permitir a criação de exceções para sites específicos conforme necessidades da Farmácia do IPAM;
4.1.2.6 Permitir a criação de regras de filtro web através de filtros específicos nos dados do conteúdo acessado por meio de busca textual;

4.1.2.7 Permitir a filtragem completa de todo o conteúdo de URLs conhecidas e consideradas como fonte de material impróprio, bem como de códigos maliciosos (cookies, scripts, binários, applets, javascripts, activeX e outros) através de base de dados catalogada e mantida pelo fabricante da solução;

4.1.2.8 Permitir vincular aplicações ou categorias de aplicações às regras de firewall, dispostas em uma base de dados catalogada e mantida pelo fabricante da solução, distribuídas por conteúdo de aplicação em categorias distintas;

4.1.2.8.1 As categorias de aplicações devem possuir, no mínimo, agrupamentos baseados nas seguintes características: Conexão Remota, Peer-to-Peer, Proxy, Compartilhamento (armazenamento/backup), Colaboração, Multimídia (áudio, vídeo, streaming), Comunicação (telefonia, videochamadas), Redes Sociais e Games/Jogos;

4.1.2.8.2 As categorias de aplicações devem identificar, no mínimo, as aplicações: TeamViewer, LogMeIn, GoToMeeting, Citrix, Webex, Microsoft Remote Desktop, VNC, SSH, OpenVPN, Telnet, Http-Proxy, Http-Tunnel, Gnutella, BitTorrent, Emule, Onedrive, 4Shared, Dropbox, Google Drive, Google Docs, Evernote, GMail, Office 365, iTunes, Youtube, SIP, WhatsApp, Skype, Facebook, Twitter, LinkedIn, Google+, Hangouts, Facebook Chat, AIM, HTTP, HTTPS, DNS, DHCP, WINS, NTP, FTP, RADIUS, Kerberos, Microsoft RPC, XML.RCP, RCP over HTTP, Microsoft Active Directory, LDAP, PostgreSQL, MySQL, Microsoft SQL Server, Oracle, DB2, SNMP, Whois, SMTP, POP3, IMAP e Rsync, bem como suas funcionalidades e recursos internos específicos;

4.1.2.9 Permitir a liberação e bloqueio de aplicações sem a necessidade de liberação adicional de portas e protocolos, efetuando apenas a liberação ou bloqueio da aplicação desejada na respectiva regra de controle de aplicações;

4.1.2.10 Permitir a criação de regras baseado nas características, comportamento e funcionalidades das aplicações, de forma que seja possível permitir e bloquear 3.1.2.10 funcionalidades específicas de uma aplicação. Exemplo: Permitir acesso ao Facebook, porém

impedir acesso ao recurso Like ou Permitir acesso ao Google Hangout via chat, porém impedir videochamadas;

4.1.2.11 Permitir a criação de exceções para aplicações específicas nas categorias de aplicações conforme necessidades da Farmácia do IPAM. Exemplo: Bloquear a categoria de aplicações Redes Sociais mais criar uma exceção liberando o Facebook que é uma aplicação pertencente à categoria Redes Sociais;

4.1.2.12 Permitir a criação de inspeções personalizadas capazes de reconhecer aplicações proprietárias sem necessidade de ação do fabricante, utilizando como critério expressões regulares, sessões e payload de pacotes TCP e UDP;

41.2.13 Permitir controle, inspeção e descriptografia de pacotes de conexões TLS/SSL estabelecidas, para fluxos de entrada e saída, efetuando o controle individual e isolado dos certificados (adição, remoção e utilização) em cada ambiente de firewall virtual, independente da aplicação.

4.1.2.14 Permitir o monitoramento do tráfego web e de aplicações em tempo real, podendo filtrar a utilização por objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo, sem bloquear o acesso dos usuários ao conteúdo acessado;

4.1.2.15 Permitir a customização da página de bloqueio de forma a informar ao usuário que o acesso não foi autorizado, bem como o motivo pelo qual o bloqueio ocorreu.

4.1.3 QOS:

4.1.3.1 Permitir a configuração da utilização de banda através da criação de classes, para download e upload,baseado em objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo;

4.1.3.1.1 Permitir a definição da banda máxima, banda garantida e fila de prioridade, sendo que a priorização do tráfego deve ocorrer em tempo real;

4.1.3.1.2 Permitir a priorização do tráfego baseado em ToS (Type of Services);

4.1.3.1.3 Permitir sFlow ou NetFlow;

4.1.3.2 Permitir o monitoramento da utilização de banda em tempo real podendo filtrar a utilização por objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo, sem bloquear o acesso dos usuários ao conteúdo acessado, de forma a identificar a utilização excessiva de banda.

4.1.4 Controle de ameaças:

4.1.4.1 Permitir a criação de regras de detecção e controle de ameaças capazes de realizar inspeção, detecção, proteção e bloqueio a ataques através dos recursos de IPS integrados internamente à solução fornecida;

4.1.4.2 Permitir vínculo das regras de controle de ameaças em qualquer das regras de firewall previamente cadastradas, com a granularidade que atenda às necessidades da Farmácia do IPAM;

4.1.4.3 Permitir a criação de regras por objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, incluindo regras de exceção conforme necessidades da Farmácia do IPAM;

4.1.4.4 Permitir proteção e bloqueio para requisições de resolução de nomes para domínios maliciosos de botnets conhecidas;

4.1.4.5 Permitir proteção e bloqueio para conexões com servidores e redes considerados botnets, C&C ou ataque a partir da execução de malwares;

4.1.4.6 Permitir proteção e bloqueio para download e upload de conteúdos considerados maliciosos (adwares, spywares, worms, hijackers, keyloggers, etc), inclusive injetados em HTML e javascript, bem como bloqueio de download de arquivos por nome, extensão e tipo (independente da extensão do arquivo);

4.1.4.7 Permitir proteção e bloqueio para ataques do tipo portscan, buffer overflow, syn flood, ICMP flood, UDP flood, bem como outras formas de exploração conhecidas e consideradas críticas;

4.1.4.8 Permitir a detecção e bloqueio de aplicações que se utilizem de mecanismos de conexão evasivos, criptografados ou através de túneis, com o objetivo de burlar os métodos de bloqueio e proteção;

4.1.4.9 Permitir proteção e bloqueio para ataques de negação de serviços;

4.1.4.10 Permitir a construção de novos padrões de ataque para proteção e bloqueio;

4.1.4.11 Permitir a definição de ações distintas para os casos de ataque detectados: Permitir, Bloquear; Resetar conexão;

4.1.4.12 Permitir detecção de ameaças baseada em assinaturas atualizáveis automaticamente;

4.1.4.13Permitir a ativação e desativação de assinaturas específicas;

4.1.4.14 Permitir o agrupamento de assinaturas conforme o tipo de protocolo e serviço a ser inspecionado;

4.1.4.15 Permitir o registro por meio de logs de todas as ameaças e ataques identificados, independente da ação definida, armazenando endereços e portas de origem e destino da conexão, horário, usuário (se existir), aplicação e identificação do ataque, bem como os pacotes necessários para utilização em investigação forense e identificação de falsos positivos. Deve ser possível identificar o momento exato em que se refere o registro, utilizando horário GMT ou o fuso horário da configuração do equipamento;

4.1.4.16 Permitir o cadastro de endereços de e-mail para recebimento de notificações das ameaças e ataques identificados, bem como parametrização do nível mínimo para envio dos alertas;

4.1.4.17 Possuir antivírus de gateway que opere de forma integrada à solução fornecida capaz de realizar inspeção, detecção, proteção e bloqueio ao conteúdo trafegado. Suportar operação, no mínimo, nos protocolos HTTP, FTP, SMTP, IMAP e POP3;

4.1.4.18 Permitir configuração de proteção anti-spoofing.

4.1.5 VPN:

4.1.5.1 Permitir a criação de túneis IPSec;

4.1.5.2 Permitir que as funcionalidades de túneis VPN sejam atendidas sem o uso de agente instalado no sistema operacional. Neste caso o túnel deve ser configurado em aplicações clientes nativas das plataformas utilizadas pelo usuário (Linux, Android, Microsoft Windows);

4.1.5.3 Permitir a criação de túneis nos formatos site-to-site e client-to-site;

4.1.5.4 Permitir autenticação por certificado ou por chave pré-compartilhada em túneis no formato site-to-site;

4.1.5.5 Permitir algoritmos de autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

4.1.5.6 Permitir a aplicação de regras de firewall, filtro web, controle de aplicações, QoS e controle de ameaças no tráfego que ocorre em um túnel VPN, de acordo com as necessidades da Farmácia do IPAM;

4.1.5.7 Permitir o registro de log de conexão e desconexão, bem como monitorar o tráfego utilizado para cada usuário de VPN;

4.1.5.8 Permitir definições de acesso às zonas de acordo com as políticas e configurações conforme critérios definidos pela Farmácia do IPAM.

4.1.6 Autenticação:

4.1.6.1 Permitir a configuração de Portal de Autenticação na própria solução fornecida (Captive Portal) de forma que possa ser liberado o acesso aos recursos de rede somente após identificação do usuário. Não deve ser necessária a instalação de qualquer software no dispositivo cliente para a identificação do referido usuário ou acesso ao Portal de Autenticação;

4.1.6.2 Permitir autenticação de usuários de forma integrada com serviços de diretório da Farmácia do IPAM (LDAP, Microsoft Active Directory e RADIUS) que fará a identificação de usuários e grupos e com usuários locais cadastrados na solução que poderão ser vinculados a grupos locais;

4.1.6.3 Permitir a criação de usuários e grupos de usuários no próprio firewall com os mesmos recursos e funcionalidades de usuários autenticados nos serviços de diretório da Farmácia do IPAM (LDAP, Microsoft Active Directory e RADIUS);

4.1.6.4 Permitir single-sign-on para usuários autenticados através de Microsoft Active Directory, independente da quantidade de usuários, sem necessidade de licenciamentos adicionais ou restrições de utilização, para todos os ambientes virtuais de firewall;

4.1.6.5 Permitir autenticação de usuários que estejam utilizando redes IPv4 e Ipv6.

4.1.7 Administração:

4.1.7.1 Possuir interface de administração no próprio equipamento;

4.1.7.1.1 Não deve ser necessária a instalação de qualquer software no dispositivo cliente para realizar o acesso ou a administração dos recursos do equipamento, bem como adição e utilização de servidores e/ou appliances;

4.1.7.1.2 Permitir acesso a todos os módulos do equipamento de forma integrada, através da mesma interface de administração, sem exigir a instalação de plugins, emuladores ou runtimes para sua utilização;

4.1.7.1.3 Permitir a utilização de todas as suas funcionalidades pela interface web, através do protocolo HTTPS, em qualquer um dos navegadores atuais, sempre nas versões mais recentes e suportando, no mínimo, Microsoft Edge, Mozilla Firefox e Google Chrome e outros que venham a ocupar posição relevante nos rankings globais dos navegadores mais utilizados;

4.1.7.1.4 Permitir acesso à interface de administração por interface CLI através do protocolo SSH;

4.1.7.2 Permitir a exportação do backup das configurações do equipamento fornecido em arquivo no formato textual de forma que seja possível sua edição manual por qualquer pessoa com conhecimento da estrutura e novamente importado no equipamento ou outro equipamento similar, independente da interface de administração;

4.1.7.3 Permitir cópia do backup gerado para recurso externo à solução por meio de FTP, TFTP, SFTP ou SCP;

4.1.7.4 Permitir a configuração de ambientes virtuais na mesma solução fornecida (firewalls virtuais), de forma que cada ambiente administre domínios de firewall de forma independente, não impondo restrições e limitações quanto à utilização de recursos e funcionalidades nos ambientes virtuais em relação ao ambiente físico;

4.1.7.5 Permitir a criação de administradores com possibilidade de autenticação local na própria solução fornecida ou autenticação em serviços de diretório da Farmácia do IPAM (LDAP, Microsoft Active Directory e RADIUS), possibilitando, inclusive, utilizar vários serviços de diretório distintos para cada ambiente virtual, inclusive com níveis de permissões distintos para cada administrador, com a granularidade que atenda às necessidades da Farmácia do IPAM, para todos os módulos e componentes, para cada ambiente virtual de firewall.

4.1.8 Logs:

4.1.8.1 Permitir a gravação de logs de todos os módulos existentes no equipamento de forma que seja possível identificar objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), para origem e destino da conexão, incluindo o timestamp (momento que ocorreu a identificação) e a ação tomada;

4.1.8.1.1 Permitir a gravação de logs de auditoria de configurações realizadas e alteradas, informando o timestamp (momento que ocorreu a identificação) e o administrador que realizou a operação;

4.1.8.1.2 Permitir o envio de logs para uma console de relatórios;

4.1.8.1.3 Permitir o envio de logs de forma simultânea para sistemas de monitoramento externos através de syslog ou rsyslog;

4.1.8.1.4 Permitir a customização de todas as configurações de logs de forma específica para cada ambiente virtual habilitado no equipamento.

4.1.9 Hardware, Licenciamento e Capacidades:

4.1.9.1 O equipamento deve ser baseado no formato de appliance físico, composta por hardware, software e sistema operacional do mesmo fabricante;

4.1.9.2 Permitir a operação dos equipamentos como uma instância única, com cluster configurado no formato ativo-ativo, com alta disponibilidade entre ambos, incluindo todas as configurações, administradores, permissões, regras, políticas, catálogos, objetos de rede, sessões, tabelas, associações de segurança de VPNs, ambientes virtuais e outras informações necessárias para que, em caso de falha em quaisquer dos equipamentos configurados, o outro equipamento assuma o completo funcionamento e a continuidade da solução sem perdas de configurações já aplicadas no ambiente;

4.1.9.2.1 Permitir que a administração possa ser realizada em qualquer dos equipamentos componentes do cluster, de forma que quaisquer alterações e configurações efetuadas sejam replicadas ao outro equipamento;

4.1.9.2.2 Permitir a sincronização de dados no cluster por meio de agregação de links, configuração de interfaces redundantes ou através de interfaces dedicadas para essa funcionalidade;

4.1.9.3 Dispor de pelo menos uma fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.1.9.4 Possuir painel ou LED indicador on/off e devices de rede;

4.1.9.5 Permitir monitoramento remoto através de SNMPv3 de forma a identificar falhas de hardware e utilização dos recursos (processador, memória, conexões, utilização das interfaces);

4.1.9.6 Permitir agregação de links conforme padrão IEEE 802.3ad e LACP, inclusive quando o equipamento estiver operando no modo cluster;

4.1.9.6.1 Permitir a configuração de várias agregações de links em cada equipamento, habilitando ou não tais agregações para cada ambiente virtual criado, conforme as necessidades da Farmácia da Farmácia do IPAM;

4.1.9.7 Permitir a criação de VLANs no padrão IEEE 802.1q, podendo vincular várias VLANs a uma porta física ou agregação de link no equipamento;

4.1.9.8 Permitir a utilização de Jumbo Frames;

4.1.9.9 Permitir operação, através das interfaces físicas de rede, de forma simultânea nas camadas 2 e 3 do modelo OSI, bem como no modo sniffer (espelhamento do tráfego das portas de rede);

4.1.9.10 O equipamento fornecido deve atender às seguintes capacidades:

4.1.9.10.1 Possuir pelo menos 10 portas 1GbE no padrão UTP (conexão RJ45);

4.1.9.10.2 Possuir porta de console para acesso aos recursos de administração com todos os adaptadores necessários para sua utilização na Farmácia da Farmácia do IPAM;

4.1.9.10.3 Permitir taxa de transferência de 1.3 Gbps estando habilitadas, de forma concomitante, as funcionalidades de firewall, controle de aplicação e controle de ameaças, conforme especificações dos itens (Firewall, Filtro Web e Controle de Aplicações, Controle de Ameaças e Logs), considerando os logs de eventos habilitados em todo o tráfego do equipamento;

4.1.9.10.3.1 A métrica utilizada para medição da taxa de transferência deve considerar ambiente empresarial de produção. Caso o fabricante divulgue múltiplos números de desempenho para as funcionalidades, serão considerados os valores aferidos em situações do mundo real e, na ausência destes, será considerado o menor valor, pois será o limitante para o uso de múltiplas funções da solução;

4.1.9.10.4 Permitir 1.400.000 de sessões simultâneas;

4.1.9.10.5 Permitir 100.000 novas sessões por segundo;

4.1.9.10.6 Permitir criação de 5.000 políticas de segurança, incluindo regras de firewall, controle de aplicação e controle de ameaças;

4.1.9.10.7 Possuir base de dados catalogada mínima de 4.000 aplicações web;

4.1.9.10.8 Possuir base de dados catalogada mínima de 8.000.000 assinaturas de ameaças conhecidas;

4.1.9.10.9 Permitir 500 clientes de VPN IPsec simultâneos;

4.1.9.10.10 Permitir a criação de 10 ambientes virtuais de firewall*;*

4.1.9.10.11 Permitir a identificação de 10 servidores LDAP distintos;

4.1.9.10.12 Permitir a identificação de 4 servidores RADIUS distintos;

4.1.9.10.13 Não deve haver limitação na quantidade de usuários e grupos identificados nos serviços de diretório da Farmácia do IPAM (LDAP, Microsoft Active Directory e RADIUS). Caso haja limitação o equipamento deve serentregue licenciado para a quantidade máxima;

4.1.9.10.14 Não deve haver limitação na quantidade de usuários ou dispositivos cliente que estiverem utilizando a solução concomitantemente. Caso haja limitação o equipamento deve ser entregue licenciado para a quantidade máxima;

4.1.9.10.15 Permitir a criação de usuários com autenticação local no equipamento;

4.1.9.10.16 Permitir a criação de perfis de gerenciamento distintos;

4.1.9.10.17 Permitir a criação de usuários de gerenciamento distintos;

4.1.9.10.18 Caso o equipamento seja composto de módulos de expansão de portas, todos os módulos devem ser idênticos;

4.1.9.10.19 As quantidades de portas requisitadas devem estar totalmente disponíveis, não sendo aceito sobreposição de portas (by pass);

4.1.9.11 O licenciamento do equipamento não deve estar atrelado a configurações de rede do equipamento, como endereço IP, domínio ou interface de rede;

4.1.9.12 Todas as portas e módulos de rede fornecidos com o equipamento devem estar licenciados para utilização de forma completa;

4.1.9.12.1 Todas as funcionalidades e recursos do equipamento devem estar licenciadas para operação nas quantidades solicitadas para cada funcionalidade enquanto estiver vigente o direito de atualizações do sistema operacional, software e firmware, exceto as funcionalidades e recursos atendidas pelos tópicos (Firewall, QOS, VPN, Autenticação, Administração), que devem estar licenciadas durante a vigência do contrato;

4.1.9.13 Os equipamentos, inclusive suas peças e componentes, devem ser novos, de primeiro uso, fazer parte do catálogo de equipamentos comercializados pelo fabricante e estar em linha de produção e comercialização na data de entrega, não sendo aceitos equipamentos que constem como end-of-sale, end-of-support, end-of-engineering-support ou end-of-life;

5.1. Para fins de qualificação técnica, o interessado deverá:

5.1.1 Apresentar, juntamente com a proposta, A QUAL DEVE SEGUIR A FORMA APRESENTADA NO ANEXO I DESTE TERMO DE REFERÊNCIA qual o FABRICANTE e o MODELO da solução de NG-Firewall (Next-Generation Firewall) ofertada em comodato para verificar se a solução proposta atende ao solicitado no objeto;

5.1.2 A empresa responsável pela execução dos serviços deve comprovar, para o fornecimento de suporte e atualizações para estrutura, possuir a seguinte certificação:

5.1.2.1 No mínimo 01 (um) técnico Specialist Network Security na solução de NG-Firewall ofertada;

5.1.2.2 Apresentar, pelo menos, 01 (um) atestado de capacidade técnica fornecido por órgão público ou empresa privada comprovando que desempenhou de forma satisfatória implantação de solução de NG-Firewall ofertada ou de modelo superior, implantação e suporte a sistema operacional Linux e solução de e-mails.

5.1.2.2.1 Fica permitido o somatório de atestados para comprovação da capacidade técnica.

5.1.2.3 Comprovar através de documentação do Fabricante, que é um canal autorizado e capacitado para o fornecimento dos produtos da marca de NG-Firewall ofertada.

5.1.2.4 Comprovar através de atestado de visita técnica, que visitou as dependências do Datacenter da Farmácia do IPAM, a fim de tomar conhecimento do local onde a solução será instalada e dirimir eventuais dúvidas sobre o ambiente físico da instalação. O atestado será fornecido pelo Setor de Tecnologia da Informação.

5.1.2.5 A Licitada será responsável por assegurar o pleno funcionamento, manutenção e atualização de todos os equipamentos utilizados na prestação dos serviços. Sempre que houver necessidade de atualização de software, firmware ou demais recursos necessários ao adequado funcionamento dos equipamentos, caberá à Licitada realizar os procedimentos pertinentes, sem prejuízo à continuidade dos serviços. Caso determinado equipamento deixe de receber atualizações, torne-se obsoleto ou tecnicamente incompatível com as necessidades dos serviços contratados, a Licitada deverá substituí-lo por equipamento de tecnologia igual ou superior, devidamente atualizado e com capacidade técnica compatível com a execução integral dos serviços objeto da contratação.

6. HORÁRIO EM QUE SERÃO PRESTADOS OS SERVIÇOS:
Das 7h às 20h de segundas a sábado e domingo das 8h às 19h.

7. FORMA DE EXECUÇÃO DOS SERVIÇOS:
Presencial e Remoto

8. PRAZO EM QUE DEVERÃO SER EXECUTADOS OS SERVIÇOS:
Tempo de resposta de até 6 horas e até 24 horas para tempo de solução. Em casos específicos, em comunicação e acordo entre ambas as partes, poderá haver alteração nesses tempos de resposta e solução.

9. PRAZO DE VIGÊNCIA CONTRATUAL
12 Meses – podendo ser renovado por igual período até o máximo de 60 meses.

ASSINATURA DA DIREÇÃO:	AUTORIZAÇÃO SETOR COMPETENTE
