ANEXO I - MEMORIAL DESCRITIVO
Processo Licitatório Pregão Eletrônico nº 21/2026

1. OBJETO

1.1. Aquisição de Solução integrada de Firewall Next-Generation Firewall (NGFW) com Gerenciamento Avançado de Logs, incluindo serviço técnico especializado de implantação, configuração, migração, suporte técnico especializado, atualização e treinamento, para a Fundação Hospitalar Santa Terezinha de Erechim, conforme condições e descrição técnica contidas neste edital e seus anexos.

2. COMPOSIÇÃO DA SOLUÇÃO

A solução é composta pela locação de alguns itens e prestação de serviço especializado pela Contratada, conforme se segue.

2.1. **Locação de itens da solução:** Se faz necessário a locação dos seguintes itens:

2.1.1. Duas unidades de Firewall NGFW, que atenda aos seguintes requisitos (cada unidade):

2.1.1.1. Atendimento integral conforme especificação constantes neste Memorial Descritivo e seus anexos.

2.1.1.2. Licenciamentos, Garantia, Suporte e Atualizações direto do Fabricante por 5 anos.

2.1.1.3. Acompanhar todo e qualquer cabeamento, periférico e acessório que se fizer necessário (incluindo régua de energia de rack de no mínimo de 8 posições, 20 amperes) para instalação em Datacenter da Contratante.

2.1.2. Console de Relatórios, atendendo aos seguintes requisitos:

2.1.2.1. Atendimento integral conforme especificação constantes neste Memorial Descritivo e seus anexos.

2.1.2.2. Licenciamentos, Garantia, Suporte e Atualizações direto do Fabricante por 5 anos.

2.2. Prestação de Serviço

2.2.1. Prestação de serviço especializado de implantação, configuração, migração, suporte, atualizações e treinamento na solução. Deverá contemplar:

2.2.1.1. Implantação presencial da solução, envolvendo instalação, configuração, migração e treinamento operacional completo.

2.2.1.2. Treinamento operacional completo da solução para funcionários de TI da Contratante (até 4 funcionários);

2.2.1.3. A instalação dos equipamentos pela contratada compreende, entre outras ações que se fizerem necessárias:

2.2.1.3.1. A montagem, afixação e cabeamento nos *racks* existentes, incluindo ligações elétricas e lógicas, conforme disposição física proposta pelo Hospital;

2.2.1.3.2. Atualização de *firmware*, *software* e sistema operacional dos componentes da solução, incluindo aplicação de *patches*, para a última versão disponível conforme matriz de compatibilidade do fabricante;

2.2.1.3.3. Habilitação do *cluster* de alta disponibilidade no formato ativo-ativo e/ou ativo-passivo;

2.2.1.3.4. Configurações físicas e lógicas nos equipamentos como placas de rede, links de agregação, ambientes virtuais, administradores, licenças, balanceamento de carga e demais configurações necessárias;

2.2.1.4. Acompanhamento presencial pós implantação. Deverão ser realizados 3 acompanhamentos presenciais após a implantação, livres de qualquer custo para a Contratante (sem consumir horas mensais contratadas, já incluso deslocamento e demais despesas). Deverão ter a duração mínima de 6 horas cada e ser realizados, preferencialmente, com um intervalo mínimo de uma semana, a combinar com a Contratante. Nesta modalidade serão realizados ajustes em configurações e otimizações que tenham se mostrado necessários após a implantação da solução, esclarecimento de dúvidas, construção e adequação de relatórios de monitoramento e controle baseado em dados reais do ambiente de produção.

2.2.1.5. Suporte técnico especializado, dispondo de 10 horas mensais para atendimento remoto ou presencial. As horas mensais são cumulativas no sentido exclusivo de estarem disponíveis para uso, nos meses subsequentes, enquanto perdurar vínculo contratual.

2.2.1.5.1. O uso das horas deverá ser previamente autorizado ou ocorrer naturalmente através de solicitações de suporte efetuadas por pessoal autorizado pelo Hospital.

2.2.1.5.2. A Contratada deverá enviar mensalmente para o Hospital relatório de uso mensal de horas, detalhando o consumo.

3. REQUISITOS GERAIS DA SOLUÇÃO

Os seguintes requisitos são obrigatórios na composição da solução:

3.1. É vedada a subcontratação dos produtos e serviços objetos deste certame.

3.2. Não será permitida a participação de empresas em consórcio.

3.3. O vínculo com a Contratada poderá ser firmado pelo período de 12 meses, podendo ser prorrogado por iguais e sucessivos períodos até o limite de 120 meses.

3.4. Garantia, Suporte, Atualizações e Licenciamentos de toda a solução, durante o período de contrato, cobrindo também fenômenos de ordem natural, como descargas elétrica, inundações, entre outros.

3.5. Todas as atividades a serem executadas, bem como os serviços de instalação, configuração, migração, suporte, atualização e treinamento devem ser realizados por profissional especializado na solução, devidamente certificado pelo fabricante e pertencente ao quadro de funcionários da Contratada.

3.6. O planejamento da implantação deverá ser proposto pela Contratada e aprovado pela Contratante, devendo contemplar o seguinte:

3.6.1. Configuração da solução em Alta Disponibilidade (formato ativo-ativo).

3.6.2. Configuração de Gravação de Logs, Geração de Relatórios, Backups e demais rotinas em geral.

3.6.3. Migração das políticas de acesso da Contratante, contemplando liberações de acesso a internet, sites permitidos e bloqueados, serviços de rede interna e externa, bem como outras características existentes no ambiente.

3.6.4. Configuração e Ajustes de políticas de acesso de acordo com definição da equipe de TI da Contratante. Deverá ter por base as políticas de acesso atuais da Contratante.

3.6.5. Configuração e Ajustes de demais funcionalidades disponíveis na solução, inclusive parametrizações de

identidades visuais institucionais em páginas de autenticação e demais localizações da solução, conforme definição da equipe de TI da Contratante.

3.6.6. Configurações e Ajustes necessários nos computadores e estações que farão uso da solução.

3.7. Durante a implantação poderão ser realizadas outras configurações e ajustes na solução, que se mostrarem necessários ou desejáveis, proposto ou autorizado pela TI da contratante.

3.8. Os serviços de instalação, configuração e migração deverão ser realizados de forma presencial, durante o expediente da Contratante, sem prejudicar o ambiente de trabalho.

3.9. Os serviços de instalação, configuração, migração e treinamento deverão ser executados em até 90 dias a contar da assinatura do Contrato, ou da comprovação de que a licitante vencedora teve conhecimento sobre a existência da nota de empenho, o que ocorrer primeiro.

5. DESCRIÇÃO TÉCNICA DA SOLUÇÃO

4.1. As condições técnicas da solução se encontram disponíveis no ANEXO I do presente memorial descritivo.

5. NÍVEL DE SERVIÇO DA CONTRATADA

A Contratada deverá:

5.1. Oferecer suporte 8x5. Em caso de emergência de parada de ambiente fora deste horário, a contratada deverá atender mediante pagamento adicional por hora.

5.2. Realizar suporte remoto ou presencial. A modalidade remota será utilizada preferencialmente, porém, sempre quando a contratante solicitar ou a contratada entender que é necessário, será realizado na modalidade presencial.

5.3. Disponibilizar canais para a abertura de atendimento por telefone ou por escrito através de sistema, e-mail, chat, whatsapp ou outro canal que efetue o registro, encaminhamento, proporcione o acompanhamento da evolução e da resolução e permita o retorno das demandas apresentadas.

5.4. Efetuar o atendimento em até 24 HORAS quando for um chamado NORMAL. O chamado normal é aquele em que a Contratante não sinaliza que é de prioridade ALTA ou URGENTE e que não se enquadra como tal. São situações de ajustes finos em configurações e serviços que estão operando dentro de uma normalidade, bem como ativação ou desativação de funcionalidades, necessidade de orientação, e todas as demais situações.

5.5. Efetuar o atendimento em até 4 HORAS quando o chamado tiver prioridade ALTA. O chamado é classificado como prioridade alta, quando a situação envolve algum ajuste em configurações e serviços que não estejam operando adequadamente, mas que não impacte em uma situação de urgência, ou quando a contratante classificar desta forma.

5.6. Efetuar o atendimento em até 1 HORA quando o chamado for URGENTE. O chamado é classificado como urgente quando a situação envolve falha em equipamentos, inoperância ou mal funcionamento em serviços.

5.7. Fornecer um número de telefone para Suporte Técnico de Emergência – 24 horas (inclusive fora do horário de expediente, finais de semana e feriados), para casos urgentes . Deverá ser resolutivo.

5.8. Em caso de necessidade de substituição de equipamento redundante, realizar no máximo em 30 dias.

5.9. Em caso de necessidade de substituição de equipamentos, decorrente de um cenário de parada ou mal

funcionamento dos serviços (em que a redundância não resolva ou esteja comprometida também), realizar a substituição em até 8 horas, mesmo utilizando equipamento provisório compatível, igual ou superior, afim de promover o restabelecimento dos serviços.

5.10. Efetuar a substituição dos equipamentos da solução em caso de defeito ou mal funcionamento, sem custo algum para a Contratante, se encarregando da logística do envio das peças e módulos a serem substituídos e a logística reversa das peças e módulos que apresentaram problema.

ANEXO I - DESCRIÇÃO TÉCNICA DA SOLUÇÃO
Memorial descritivo do Pregão Eletrônico nº 21/2026.

1. Características Técnicas da Solução

1.1. Firewall NGFW

1.1.1. Firewall

1.1.1.1. Permitir a criação de regras de *firewall* de forma a liberar ou bloquear acessos operando no formato *statefull firewall*.

1.1.1.2. 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 do Hospital.

1.1.1.3. Permitir vínculo das regras de *firewall* com país de origem e país de destino das conexões.

1.1.1.4. Permitir a criação de regras de *firewall* com período de validade de forma programada (data e horário iniciais e finais).

1.1.1.5. 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.

1.1.1.6. Permitir a tradução de portas PAT (*Port Address Translation*) nos formatos um- para-um e muitos-para-um.

1.1.1.7. 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*.

1.1.1.8. Permitir a configuração de roteamento estático e dinâmico utilizando RIP, BGP e OSPF para os protocolos IPv4 e IPv6.

1.1.1.9. Permitir OSPF *graceful restart*.

1.1.1.10. Permitir *Policy Based Routing* ou *Policy Based Forwarding*.

1.1.1.11. Permitir roteamento *multicast* no protocolo *PIM Sparse Mode*.

1.1.1.12. 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.

1.1.1.13. Filtro Web e Controle de Aplicações

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

1.1.1.15. 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 do Hospital.

1.1.1.16. 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.

1.1.1.16.1. As categorias de sites devem possuir, no mínimo, agrupamentos baseadas em características, como por exemplo Redes Sociais, Games, Pornografia, dentre outras.

1.1.1.17. Permitir a criação de categorias de sites específicas conforme necessidades do Hospital.

1.1.1.18. Permitir a criação de exceções para sites específicos conforme necessidades do Hospital.

1.1.1.19. Permitir a criação de regras de filtro web através de filtros específicos nos dados do conteúdo acessado por meio de busca textual.

1.1.1.20. 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.

1.1.1.21. 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.

1.1.1.21.1. As categorias de aplicações devem possuir, no mínimo, agrupamentos baseadas em características, como por exemplo Redes Sociais, Acesso Remoto, Torrent, Comunicadores instantâneos, dentre outras.

1.1.1.22. 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.

1.1.1.23. Permitir a criação de regras baseado nas características, comportamento e funcionalidades das aplicações, de forma que seja possível permitir e bloquear funcionalidades específicas de uma aplicação.

1.1.1.24. Permitir a criação de exceções para aplicações específicas nas categorias de aplicações conforme necessidades do Hospital. Exemplo: Bloquear a categoria de aplicações *Redes Sociais* mais criar uma exceção liberando o Instagram que é uma aplicação pertencente à categoria *Redes Sociais*.

1.1.1.25. 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.

1.1.1.26. 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*, independente da aplicação.

1.1.1.27. 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.

1.1.1.28. 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.

1.1.2. QOS

1.1.2.1. 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.

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

1.1.2.1.2. Permitir a priorização do tráfego baseado em ToS (*Type of Services*).

1.1.2.1.3. Permitir sFlow ou NetFlow.

1.1.2.2. 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.

1.1.3. Controle de Ameaças

1.1.3.1. 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.

1.1.3.2. Permitir vínculo das regras de controle de ameaças em qualquer das regras de *firewall* previamente cadastradas, com a granularidade que atenda às necessidades do Hospital.

1.1.3.3. 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 do Hospital.

1.1.3.4. Permitir proteção e bloqueio para requisições de resolução de nomes para domínios maliciosos de *botnets* conhecidas.

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

1.1.3.6. 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).

1.1.3.7. 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.

1.1.3.8. 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.

1.1.3.9. Permitir proteção e bloqueio para ataques de negação de serviços.

1.1.3.10. Permitir a construção de novos padrões de ataque para proteção e bloqueio.

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

1.1.3.12. Permitir detecção de ameaças baseada em assinaturas atualizáveis automaticamente.

1.1.3.13. Permitir a ativação e desativação de assinaturas específicas.

1.1.3.14. Permitir o agrupamento de assinaturas conforme o tipo de protocolo e serviço a ser inspecionado.

1.1.3.15. 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.

1.1.3.16. 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.

1.1.3.17. 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.

1.1.3.18. Permitir configuração de proteção *anti-spoofing*.

1.1.4. VPN

1.1.4.1. Permitir a criação de túneis VPN SSL e/ou IPSec.

1.1.4.2. Possuir agente de conexão para VPN a ser instalado no sistema operacional das estações de trabalho compatível com Microsoft Windows 10 e superiores, para arquitetura 64 bits.

1.1.4.3. Permitir que as funcionalidades de túneis VPN sejam atendidas com ou 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).

1.1.4.4. Permitir que a conexão VPN seja estabelecida antes da autenticação do usuário na estação de trabalho, após a autenticação do usuário na estação de trabalho e sob demanda do usuário.

1.1.4.5. Permitir autenticação de usuários de VPN de forma integrada com serviços de diretório do Hospital (LDAP, *Microsoft Active Directory* e RADIUS) que fará a identificação de usuários e com usuários locais cadastrados na própria solução fornecida.

1.1.4.6. Permitir algoritmos de criptografia simétricos DES, 3DES, AES128 e AES256.

1.1.4.7. Permitir a utilização de certificados PKI X.509.

1.1.4.8. Permitir a criação de túneis nos formatos *site-to-site* e *client-to-site*.

1.1.4.9. Permitir autenticação por certificado ou por chave pré-compartilhada em túneis no formato *site-to-site*.

1.1.4.10. Permitir algoritmos de autenticação MD5, SHA1, SHA256, SHA384 e SHA512.

1.1.4.11. Permitir a configuração de VPN em IPv6 e IPv4, bem como efetuar tráfego IPv4 por meio de túneis IPv6 e tráfego IPv6 por meio de túneis IPv4.

1.1.4.12. Permitir NAT-T.

1.1.4.13. 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 do Hospital.

1.1.4.14. Permitir a alocação de um endereço IP para cada estação remota conectada no túnel VPN, fornecendo um endereço de forma dinâmica ou endereço previamente fixado ao cliente, conforme as necessidades do Hospital.

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

1.1.4.16. Permitir definições de acesso às zonas de acordo com as políticas e configurações conforme

critérios definidos pelo Hospital.

1.1.4.17. Permitir configuração do redirecionamento de *gateway* para internet, para cada usuário de VPN, de forma que seja possível impedir ou liberar a comunicação com outras redes que não façam parte da estrutura configurada no servidor de VPN. Exemplo: possibilitar a configuração se um usuário, ao conectar no servidor de VPN, deve acessar a internet pela rede remota onde estiver conectado ou através do túnel VPN estabelecido.

1.1.5. Autenticação

1.1.5.1. 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.

1.1.5.2. Permitir autenticação de usuários de forma integrada com serviços de diretório do Hospital (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.

1.1.5.3. 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 do Hospital (LDAP, *Microsoft Active Directory* e RADIUS).

1.1.5.4. 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.

1.1.5.5. Permitir autenticação de usuários que estejam utilizando redes IPv4 e IPv6.

1.1.6. Administração

1.1.6.1. Possuir interface de administração no próprio equipamento.

1.1.6.1.1. 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*.

1.1.6.1.2. 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.

1.1.6.1.3. 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.

1.1.6.1.4. Permitir acesso à interface de administração por interface CLI através do protocolo SSH.

1.1.6.2. Permitir a exportação do backup das configurações do equipamento fornecido em arquivo.

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

1.1.6.4. 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.

1.1.6.5. Permitir a criação de administradores com possibilidade de autenticação local na própria solução fornecida ou autenticação em serviços de diretório do Hospital (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 do Hospital, para todos os módulos e componentes, para cada ambiente virtual de *firewall*.

1.1.7. Logs

1.1.7.1. 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.

1.1.7.1.1. 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.

1.1.7.1.2. Permitir o envio de *logs* para a console de relatórios que compõe a solução.

1.1.7.1.3. Permitir o envio de *logs* de forma simultânea para sistemas de monitoramento externos através de syslog ou rsyslog.

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

1.1.8. Hardware, Licenciamento e Capacidades

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

1.1.8.2. 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.

1.1.8.2.1. 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.

1.1.8.2.2. 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.

1.1.8.3. Possuir características para montagem e instalação em rack no Datacenter do Hospital, devendo ser acompanhado de trilhos, suportes, parafusos, conectores, bandejas e demais acessórios necessários a sua correta afixação.

1.1.8.4. Possuir indicação frontal, por meio de display LCD ou LEDs, do status operacional do equipamento: desligado, energizado, ligado, falha em dispositivo e configuração do *cluster*.

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

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

1.1.8.6.1. Permitir a configuração de várias agregações de links em cada equipamento, habilitando ou não tais agregações para cada ambiente virtual criado, conforme as necessidades do Hospital.

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

1.1.8.8. Permitir a utilização de *Jumbo Frames*.

1.1.8.9. 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).

1.1.8.10. Cada equipamento fornecido deve atender individualmente às seguintes capacidades:

1.1.8.10.1. Possuir pelo menos 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

1.1.8.10.2. Possuir no mínimo 2 portas 1GBE SFP;

1.1.8.10.3. Permitir taxa de transferência de no mínimo 1 Gbps estando habilitadas, de forma concomitante, as funcionalidades de *firewall*, controle de aplicação e controle de ameaças, considerando os *logs* de eventos habilitados em todo o tráfego do equipamento.

1.1.8.10.3.1. 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.

1.1.8.10.4. Permitir no mínimo 1.500.000 de sessões simultâneas.

1.1.8.10.5. Permitir no mínimo 45.000 novas sessões por segundo.

1.1.8.10.6. Permitir criação de no mínimo 5.000 políticas de segurança, incluindo regras de *firewall*, controle de aplicação e controle de ameaças.

1.1.8.10.7. Possuir base de dados catalogada mínima de 4.000 aplicações web.

1.1.8.10.8. Possuir base de dados catalogada mínima de 8.000.000 assinaturas de ameaças conhecidas.

1.1.8.10.9. Não deve haver limitação na quantidade de usuários e grupos identificados nos serviços de diretório do Hospital (LDAP, *Microsoft Active Directory* e RADIUS). Caso haja limitação o equipamento deve ser entregue licenciado para a quantidade máxima.

1.1.8.10.10. 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.

1.1.8.10.11. Permitir a criação de usuários com autenticação local no equipamento.

1.1.8.10.12. Permitir a criação de perfis de gerenciamento distintos.

1.1.8.10.13. Permitir a criação de usuários de gerenciamento distintos.

1.1.8.10.14. Caso o equipamento seja composto de módulos de expansão de portas, todos os módulos devem ser idênticos.

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

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

1.1.8.10.17. Todas as funcionalidades e recursos do equipamento devem estar licenciadas para operação nas quantidades solicitadas para cada funcionalidade enquanto estiver vigente o contrato.

1.2. Console de Relatórios

1.2.1. Logs

1.2.1.1. Os *logs* dos equipamentos que compõem a solução devem ser armazenados de forma consolidada e centralizada em uma console única, possibilitando que consultas na base de dados retornem registros de qualquer dos dispositivos componentes da solução, específicas para cada ambiente virtual.

1.2.1.1.1. Possuir recurso que permita identificar a quantidade de registros de *logs* armazenados, o equipamento que efetuou o registro, o espaço utilizado em disco e o espaço restante de armazenamento.

1.2.1.1.2. Possuir mecanismo que remova automaticamente os *logs* armazenados conforme regras definidas pelo administrador, para cada ambiente virtual: quantidade de tempo e quantidade de espaço ocupado.

1.2.1.1.3. Possuir recurso de exportação de *logs*, em formato textual, por período inicial e final, específico para cada ambiente virtual.

1.2.1.2. Permitir armazenamento diário mínimo de 5 GB de *logs* para funcionalidades de todos os módulos da solução.

1.2.1.3. Permitir armazenamento total de *logs* para funcionalidades de todos os módulos da solução e suportar expansão de armazenamento.

1.2.1.4. Permitir armazenamento dos logs de todos os dispositivos da solução, de forma irrestrita e perpétua, dentro dos parâmetros mencionados.

1.2.2. Relatórios

1.2.2.1. Permitir a geração de relatórios sob os *logs* armazenados.

1.2.2.1.1. Permitir a definição de filtros para cada um dos campos dos relatórios, podendo informar intervalos inicial e final para os parâmetros além de expressões do tipo caractere que possam abranger mais de um valor por parâmetro. Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios.

1.2.2.1.2. Permitir a customização dos dados exibidos pelos relatórios, selecionando os campos a serem exibidos na listagem, configurando o *layout* (página, cabeçalho,rodapé, alinhamento dos dados, fontes, cores, quebras de página, totalizadores e operadores de agregação), bem como aplicando opções de filtro por meio de expressões regulares ou utilizando recursos de linguagem de consulta de dados similar à linguagem SQL.

1.2.2.1.3. Permitir a geração de relatórios nos formatos planilha eletrônica (CSV, ODS, XLS ou XLSX)

e PDF, possibilitando visualização de forma tabular ou gráfica, conforme o contexto dos dados que compõem o relatório.

1.2.2.1.4. Permitir a identificação dos países de origem e destino nos *logs* de acesso e relatórios gerados.

1.2.2.1.5. Permitir a geração de relatórios de *logs* em tempo real e através de agendamentos, conforme definições do administrador.

1.2.2.1.6. Permitir o envio automático de cópia dos relatórios gerados para caixa de correio eletrônico, a ser configurada em cada relatório da solução, para cada ambiente virtual.

1.2.2.1.7. Permitir a customização de relatórios da ferramenta, de acordo com as necessidades do Hospital, de forma que as customizações geradas possam ser salvas para novas execuções dentro da ferramenta.

1.2.2.1.8. Permitir a criação de telas de monitoramento (*dashboards*) para análise e visibilidade do tráfego, customizados de acordo com as necessidades e particularidades do Hospital, podendo analisar, de formas independentes, *firewall*, filtro web, aplicações e ameaças.

1.2.2.2. A gravação, exportação, exclusão ou a geração de relatórios, independente do período considerado ou do volume de dados envolvidos, não deve onerar ou causar gargalos na operação das demais funcionalidades ou capacidades da console de relatórios.

1.2.3. Administração

1.2.3.1. Permitir acesso à console de relatórios por interface *web* através do protocolo HTTPS.

1.2.3.1.1. Permitir a utilização de todas as suas funcionalidades em qualquer um dos navegadores atuais sempre nas suas versões mais recentes 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.

1.2.3.1.2. Permitir acesso a todos os recursos da console de forma integrada, através da mesma interface, sem exigir a instalação de *plugins*, emuladores ou *runtimes* para sua utilização.

1.2.3.1.3. Permitir a exportação do backup das configurações da console de relatórios.

1.2.3.1.4. Permitir a criação de perfis de gerenciamento distintos.

1.2.3.1.5. Permitir a criação de usuários de administração distintos.

1.2.3.2. Permitir operação nos protocolos IPv4 e IPv6.

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

1.2.4. Permitir a identificação de hosts infectados nas diversas redes através de mecanismo de inspeção de logs, que avalie padrões apoiado em indicadores sólidos e base de conhecimento da solução, ampla e constantemente atualizada.

1.3. Detalhes Gerais da Solução

1.3.1. Os objetos especificados nos itens 1.1 e 1.2 (Firewall NGFW e Console de Relatórios) deste ANEXO devem atender às seguintes regras:

1.3.1.1. Os objetos classificados como zonas devem suportar o vínculo de todas as zonas de segurança do ambiente de configuração.

1.3.1.2. Os objetos classificados como endereços devem suportar o vínculo de IP específico, intervalo de endereços IP, blocos de endereços IP (endereço e máscara), nos protocolos IPv4 e IPv6, além de endereços no formato FQDN (*Full Qualified Domain Name*). Ex. w*ww.fhste.com.br*

1.3.1.3. Os objetos classificados como portas devem suportar o vínculo de portas e intervalo de portas.

1.3.1.4. Os objetos classificados como protocolos devem suportar o vínculo de protocolos, independente da porta de comunicação utilizada.

1.3.1.5. Os objetos classificados como usuários devem suportar o vínculo de usuários e grupos de usuários do serviço de diretório do Hospital (LDAP, *Microsoft Active Directory* e RADIUS) ou usuários locais criados na solução.

1.3.2. Os equipamentos fornecidos para compor a solução devem ser todos do mesmo fabricante.

1.3.3. 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*.

1.3.4. Todos os equipamentos fornecidos para compor a solução devem ser idênticos, conforme as características e especificações de cada modelo.