TERMO DE REFERÊNCIA

1. OBJETO:

1.1 Contratação de empresa especializada na prestação de serviços de internet, para o Hospital Municipal de Aparecida de Goiânia CNES 9680977, de acordo com a Resolução de Diretoria Colegiada – RDC nº 63, de 25 de novembro de 2011, do Ministério da Saúde – MS, dispõe sobre os Requisitos de Boas Práticas de Funcionamento para os Serviços de Saúde, e nos termos do Contrato de Gestão 1095/2018 firmado entre o CONTRATANTE e o Município de Aparecida de Goiânia e a Secretaria Municipal de Saúde / Fundo Municipal de Saúde.

1.2 O presente objeto refere-se a contratação de empresa especializada que promova solução em serviços de telecomunicações com capacidade para prover tráfego de dados das aplicações corporativas da unidade hospitalar HMAP, tráfego de voz e imagens, videoconferência e acesso à Internet. Esses serviços serão prestados para interligação de unidade com a rede mundial de computadores e segurança da informação como previsto na lei geral de proteção de dados a LGPD.-

2. JUSTIFICATIVA

2.1. Tendo em vista a necessidade de garantir a continuidade dos serviços da unidade hospitalar essa nova aquisição deve ser contratada junto a outra operadora para garantir a continuidade dos serviços prestados a comunidade.

2.2. Dado a expansão dos serviços prestados e a implantação do serviço de exames de imagens que iniciou nesta unidade faz-se necessário garantirmos a qualidade e continuidade do trafego com segurança.

3. Planilha de Formação de Preços

Item	Descrição e Especificações	Unidade de Medida	Quantidade	Preço Unitário (R$)	Preço Total (R$)
1	Serviço de instalação de enlace dedicado à Internet.	Instalação	1		
2	Fornecimento de link de acesso dedicado à Internet na velocidade de 200 Mbps.	Meses	12		
3	Prestação de serviços de gerenciamento proativo do(s) link(s).	Meses	12		
4	Serviço de proteção contra ataques volumétricos de negação de serviços do tipo DDoS.	Meses	12		
5	Serviço de instalação e configuração da solução de segurança.	Instalação	12		
6	Fornecimento de solução de segurança do tipo NGFW.	Meses	12		
Total					

4. FUNDAMENTAÇÃO LEGAL:

4.1. Melhoria da qualidade dos serviços prestados ao cidadão e redução nos tempos de atendimento ao usuário.

4.2. Essa contratação agregará o serviço de filtros de dados que nos garante uma maior segurança nos dados trafegados.

5. DEFINICÕES:

5.1. Backbone: infraestrutura de interligação de uma rede, constituída de roteadores de borda do provedor e roteadores de núcleo, bem como os circuitos que existam entre eles.

5.2. ANATEL: Agência Nacional de Telecomunicações.

5.3. CPE (de Customer Premises Equipment): é um termo técnico muito utilizado por operadoras de telecomunicações e fornecedores de serviços de comunicação. Se trata do equipamento instalado dentro das instalações do cliente para prestação do serviço pela Operadora.

5.4. DNS: de *Domain Name System*, ou "Sistema de Nomes de Domínios". Trata-se, de servidores que armazenam listagens de domínios e seus respectivos endereços IPs. são os responsáveis por localizar e traduzir para números IP os endereços dos sites utilizados nos navegadores.

5.5. HTTP: O *Hypertext Transfer Protocol*, é um protocolo de comunicação utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web. Hipertexto é o texto estruturado que utiliza ligações lógicas entre nós contendo texto.

5.6. IP (de Internet Protocol): é um protocolo de comunicação usado para encaminhamento dos dados entre equipamentos em rede, utilizando endereços alocados em cada um dos elementos da mesma (endereços IP).

5.7. Last Mile ou Última Milha: circuito dedicado entre o roteador de borda do provedor e o roteador ou switch existente nas dependências do cliente.

5.8. MTTR: de *Mean Time to Repair* é um indicador de desempenho usado na manutenção para indicar o Tempo Médio Para Reparo de algum equipamento, componente, máquina ou sistema.

5.9. Router ou Roteador: equipamento tipicamente utilizado para fazer a interface entre uma rede local e uma rede de telecomunicações. É usado também nos nós de uma rede para processar roteamento do tráfego IP.

5.10. SLA: *Service Level Agreement*, que é traduzido em português por ANS (Acordo de Nível de Serviço). Refere-se à especificação, em termos mensuráveis e claros, de todos os serviços que o contratante pode esperar do fornecedor na negociação.

5.11. SNMP (Simple Network Management Protocol): protocolo de gerenciamento usado normalmente em redes IP.

5.12. DDoS (Distributed Denial of Service): é um ataque distribuído, o qual pode estar vinculado à milhares de computadores com interesse malicioso.

5.13. NGFW (Next Generation Firewall): um sistema de segurança baseado em hardware ou software que está habilitado a detectar e bloquear ataques sofisticados por reforçar políticas de segurança na camada de aplicação, camada 7 no modelo OSI.

6. ESPECIFICAÇÕES TÉCNICAS DO OBJETO:

6.1. REQUISITOS GERAIS

6.1.1. Contratação de empresa especializada para o fornecimento de acesso à Rede Mundial de Internet com 100% de garantia de banda downstream e upstream, full-duplex, com conectividade em protocolos IPv4 e IPv6.

6.1.2. Toda a infraestrutura de rede, acesso e CPE da CONTRATADA deverão ser dimensionadas e preparadas para suportar a totalidade do serviço.

6.1.3. A CONTRATADA deverá reservar os canais de comunicação e as portas de acesso à sua infraestrutura para uso exclusivo da CONTRATANTE, não sendo admitido o compartilhamento desses recursos com outro de seus clientes ou usuários

6.1.4. O acesso referido no item anterior deverá ser provido por meio de backbone próprio da prestadora de serviço.

6.1.5. Os equipamentos da CONTRATADA utilizados em toda a solução deverão ser novos e compatíveis com ambientes corporativos ou institucionais modernos.

6.1.6. A CONTRATADA obriga-se e se responsabiliza a prestar o serviço objeto da licitação, por meio de mão de obra especializada e devidamente qualificada, necessário à completa e perfeita execução dos serviços, em conformidade com as especificações do Termo de Referência.

6.1.7. Será de responsabilidade da CONTRATANTE o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede elétrica e a climatização das dependências.

6.2. CARACTERÍSTICAS DO LINK INTERNET

6.2.1. Fornecer e instalar link de Internet na taxa de 200Mbps dedicado.

6.2.2. A CONTRATADA deverá disponibilizar 04 endereços IPV4 e 04 endereços IPv6 fixos e válidos para provimento da solução de Internet.

6.2.3. A conexão entre o CPE da CONTRATADA e o equipamento da CONTRATANTE deverá ser realizada através de interface Gigabit Ethernet 1000BASE-TX.

6.2.4. A CONTRATADA poderá utilizar acessos de terceiros como última milha, sendo de inteira responsabilidade da CONTRATADA o cumprimento dos SLAs especificados 99.5%.

6.2.5. A velocidade do link do serviço entregue à CONTRATANTE deverá ser correspondente a 100% da banda contratada.

6.2.6. O acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso.

6.2.7. O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de vinte quatro (24) horas.

6.2.8. Disponibilizar serviço de Domain Name Resolution (DNS) da CONTRATADA, capaz de resolver direta e reversamente endereços de Internet, para registro no servidor DNS primário.

6.2.9. Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço.

6.2.10. Disponibilizar informações sobre os serviços de acesso à Internet por meio de um portal de monitoramento, com acesso restrito, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso.

6.2.11. Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualize relatórios das informações de desempenho dos serviços contratados

6.2.12. A CONTRATADA não poderá:

a) Implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado à CONTRATANTE, a menos que tenha expressa concordância com esta.

b) Implementar nenhum tipo de cache transparente, a menos que tenha expressa concordância da CONTRATANTE.

6.3. CARACTERÍSTICAS DO ROTEADOR

6.3.1. O roteador a ser instalado no ambiente da CONTRATANTE deverá ter no mínimo as seguintes características técnicas:

a) O equipamento e seus módulos e softwares não deverão constar em nenhuma lista do fabricante com as situações de “End-of-Sale”, “End-of-Order”, “End-of-Life” ou

"End-of-Support".

b) Deve possuir no mínimo quatro (04) interfaces Gigabit Ethernet padrão 1000BASE-TX.

c) Possuir protocolo SNMP habilitado com acesso de leitura.

d) Deve implementar os protocolos de roteamento RIP, OSPFv2, OSPFv3 e BGP-4.

e) Deve possuir suporte nativo ao protocolo IPv6.

f) Deve possuir suporte ao protocolo Netflow v9 ou superior.

g) Deve possuir suporte ao protocolo 802.1q.

h) Deve possuir suporte aos protocolos Telnet e SSHv2.

i) Deve possuir gerenciamento local através de uma porta console, sendo que todos os cabos e adaptadores necessários para o gerenciamento através da porta console deverão ser fornecidos pela CONTRATADA de forma a propiciar o gerenciamento do roteador a partir de uma porta USB.

j) Deverá ser disponibilizado para a CONTRATANTE com o último release de software estável disponibilizado pelo fabricante, capaz de atender a todos os requisitos acima, incluindo o suporte à atualização do referido software durante o período de vigência do contrato.

k) Deve ser montável em rack padrão EIA-310 com largura padrão 19" ocupando no máximo 1U de altura.

6.4. CARACTERÍSTICAS DO SERVIÇO Anti DDoS

6.4.1. A CONTRATADA deverá prover, no âmbito do serviço de segurança do link de Internet, uma solução para identificação, tratamento e mitigação transparente de ataques volumétricos do tipo negação de serviço distribuído (DDoS – Distributed Denial of Service).

6.4.2. A CONTRATADA deve possuir infraestrutura de mitigação própria com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional. Deverá possuir pelo menos 2 (dois) centros de limpeza, cada um com capacidade de mitigação de 40 Gbps (quarenta gigabits por segundo).

6.4.3. A CONTRATADA deverá disponibilizar em seu backbone, proteção contra ataques volumétricos de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DDoS (Distributed Denial of Service).

6.4.4. A CONTRATADA deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e com quantidade ilimitada de eventos de ataque ao longo da vigência contratual.

6.4.5. O ataque deve ser mitigado separando o tráfego legítimo do tráfego malicioso, de

modo que os serviços de Internet providos pelo cliente continuem disponíveis.

6.4.6. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos.

6.4.7. Em casos de ataques não detectados pela solução, quando identificados pela CONTRATANTE, deverão ser mitigados imediatamente pelas CONTRATADA após a abertura de chamado através da Central de Atendimento sempre como um chamado com Prioridade Máxima, e deverá realizá-la, sem nenhum ônus ao CONTRATANTE.

6.4.8. O serviço deve prover suporte à mitigação automática de ataques, utilizando múltiplas técnicas incluindo, mas não se restringindo a: White Lists, Black Lists, limitação de taxa de tráfego, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP, NTP e DNS, bloqueio por localização geográfica de endereços IP.

6.4.9. A CONTRATADA deve realizar a detecção de ataques utilizando-se dos recursos mais atuais para detecção de ataques de negação de serviço, tais como análise estatística de tráfego, padrões predefinidos para bloqueios de ataques, correlacionamento com ataques que estejam ocorrendo simultaneamente em outras partes do mundo e atualização para detecção de ataques de negação de serviço desconhecidos.

6.4.10. O serviço deve prover também análise de tráfego baseado em reputação de endereços IP, possuindo base de informações própria, que pode ser gerada durante a filtragem de ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

a) O serviço deve prover mecanismos capazes de detectar e migar todos e quaisquer ataques de DDoS que façam o uso não autorizado de recursos de rede, tanto para Ipv4 Ataques de inundação (Bandwidth Flood), Floods de UDP, TCP e ICMP.

b) Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets.

c) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.

d) Ataques provenientes de Botnets, Worms e que utilizam falsificação de endereços IP origem (IP Spoofing).

e) Ataques à camada de aplicação, incluindo protocolos HTTP, DNS, NTP, dentre outros.

f) O serviço deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATADA.

g) O serviço deve permitir a configuração de níveis diferenciados de proteção por grupo

de hosts ou subnets.

h) O serviço deve ser capaz de bloquear tráfego baseado em assinaturas em até 15 minutos.

i) O serviço deve ser capaz de analisar e aprender o comportamento do tráfego para criar automaticamente parâmetros de bloqueio (Limite de conexão HTTP, TCP, UDP, ICMP, etc.).

j) O serviço deve ser capaz de detectar anomalias no tráfego, ataques ainda não conhecidos e criar bloqueios em tempo real sem intervenção manual do administrador.

6.4.11. como para Ipv6, incluindo, mas não se restringindo aos seguintes:

6.4.12. O Serviço deve ser capaz de mitigar ataques DDoS na nuvem de forma automatizada, configurando thresholds diferenciados para os níveis de proteção criados que, se atingidos, redirecionem o tráfego para o centro de limpeza da CONTRATADA, para posterior devolução do tráfego limpo à rede da CONTRATANTE.

6.4.13. A CONTRATADA deve realizar a mitigação de ataques e limpeza do tráfego ilegítimo sem prejudicar ou impedir o tráfego legítimo, seja ele originado de uma ou mais fontes.

6.4.14. A CONTRATADA deve atuar na detecção de Falsos-Positivos e promover medidas proativas para que bloqueios indevidos não ocorram e nem impacte no tráfego de negócio da CONTRATANTE, desde que as atividades relacionadas estejam devidamente autorizadas pela CONTRATANTE por e-mail ou mediante atendimento de chamado técnico.

6.5. CARACTERÍSTICAS DA SOLUÇÃO DE SEGURANÇA (NGFW)

6.5.1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO NGFW

i. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração.

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

iii. 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.

iv. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

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

vi. A gestão do equipamento deve ser compatível através da interface de gestão Web

no mesmo dispositivo de proteção da rede.

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

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

ix. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding.

x. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).

xi. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay.

xii. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server.

xiii. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.

xiv. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.

xv. Deve suportar NAT dinâmico (Many-to-1).

xvi. Deve suportar NAT dinâmico (Many-to-Many).

xvii. Deve suportar NAT estático (1-to-1).

xviii. Deve suportar NAT estático (Many-to-Many).

xix. Deve suportar NAT estático bidirecional 1-to-1.

xx. Deve suportar Tradução de porta (PAT).

xxi. Deve suportar NAT de Origem.

xxii. Deve suportar NAT de Destino.

xxiii. Deve suportar NAT de Origem e NAT de Destino simultaneamente.

xxiv. Deve poder combinar NAT de origem e NAT de destino na mesma política

xxv. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

xxvi. Deve suportar NAT64 e NAT46.

xxvii. Deve implementar o protocolo ECMP.

xxviii. Deve implementar balanceamento de link por hash do IP de origem.

xxix. Deve implementar balanceamento de link por hash do IP de origem e destino.

xxx. 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. Deve suportar o balanceamento de, no mínimo, três links.

xxxi. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

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

xxxiii. Enviar log para sistemas de monitoração externos, simultaneamente.

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

xxxv. Proteção anti-spoofing.

xxxvi. Implementar otimização do tráfego entre dois equipamentos.

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

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

xxxix. Suportar OSPF graceful restart.

xl. Os 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: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).

xli. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

xlii. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.

xliii. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.

xliv. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

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

xlvi. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3.

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

xlviii. A configuração em alta disponibilidade deve sincronizar: Sessões.

xlix. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.

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

li. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB.

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

liii. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.

liv. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos.

lv. Deve permitir a criação de administradores independentes, para cada um dos

sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas.

lvi. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

lvii. Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede.

lviii. O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede.

lix. Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW.

6.5.2. CONDIÇÕES DO FORNECIMENTO DOS APPIANCES

a) A CONTRATADA deverá comunicar à CONTRATANTE, antecipadamente, a data e o horário da entrega, não sendo aceitos os produtos que estiverem em desacordo com as especificações constantes deste instrumento.

b) A CONTRATADA deverá se responsabilizar por todos os ônus relativos ao fornecimento dos equipamentos inclusive frete, seguro, cargas e descargas desde a origem até sua entrega no local de instalação

6.5.3. MANUAIS E DOCUMENTAÇÃO

a) A CONTRATADA deverá indicar os sites dos fabricantes envolvidos nesta solução que devem obrigatoriamente oferecer download gratuito de todas as atualizações de drivers de dispositivos e firmwares para os equipamentos ofertados bem como dispor dos manuais técnicos com informações detalhadas e atualizadas sobre instalação, configuração, operação e administração dos equipamentos.

6.5.4. TRANSFERÊNCIA DE CONHECIMENTO

a) A CONTRATADA deverá fazer a transferência de conhecimento de no mínimo 40 (quarenta) horas para até 6 (seis) funcionários a ser definidos pela CONTRATANTE. O repasse de conhecimento visa um treinamento básico de startup das soluções e não um treinamento oficial.

b) A transferência de conhecimento será feita nas dependências da CONTRATANTE e não inclui nenhum tipo de material didático ou certificado.

6.5.5. TREINAMENTO OFICIAL

a) Deverão ser ofertadas 3 (três) vagas para treinamento oficial de configuração, administração e utilização de TODOS OS COMPONENTES DE HARDWARE E SOFTWARE desta solução. Todos os materiais didáticos, ou seja, cada um dos 3 (três) participantes deverão receber o seu material didático oficial do fabricante.

b) A CONTRATADA não será responsável pelos valores de logísticas, hospedagem e alimentação. Somente pelo fornecimento dos vouchers para o treinamento oficial, estes citados acima.

c) Os treinamentos deverão ser ministrados por instrutores especialistas nos respectivos componentes da solução e que detenha todas as condições técnicas (teóricas e práticas) necessárias para desempenhar tal função.

d) Na conclusão de cada treinamento, deverão ser entregues a cada um dos 3 (três) participantes um certificado de conclusão do treinamento.

6.5.6. CONSOLE DE GERÊNCIA E MONITORAMENTO

a) Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

b) O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

c) Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux.

d) O gerenciamento deve permitir/possuir:

1. Criação e administração de políticas de firewall e controle de aplicação.
2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware.
3. Criação e administração de políticas de Filtro de URL.
4. Monitoração de logs.
5. Ferramentas de investigação de logs.
6. Debugging.
7. Captura de pacotes.

e) Acesso concorrente de administradores.

f)Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

g) Deve permitir usar palavras chaves e cores para facilitar identificação de regras.

h) 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.

i) Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores.

j) Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.

k) Autenticação integrada ao Microsoft Active Directory e servidor Radius.

l) Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados.

m) Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QoS.

n) Criação de regras que fiquem ativas em horário definido.

o) Criação de regras com data de expiração.

p) Backup das configurações e rollback de configuração para a última configuração salva.

q) Suportar Rollback de Sistema Operacional para a última versão local.

r) Habilidade de upgrade via SCP, TFTP e interface de gerenciamento.

s) Validação de regras antes da aplicação.

1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

t) Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).

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).

u) Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

v) Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

w) Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

x) 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.

y) Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

z) 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.

aa) O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.

bb) Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc.

cc) Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução.

dd) Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime.

ee) Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.

ff) Deve ser possível exportar os logs em CSV.

gg) 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.

hh) Rotação do log.

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

1. Situação do dispositivo e do cluster.
2. Principais aplicações.
3. Principais aplicações por risco.
4. Administradores autenticados na gerência da plataforma de segurança.
5. Número de sessões simultâneas.
6. Status das interfaces.
7. Uso de CPU

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

1. Resumo gráfico de aplicações utilizadas.
2. Principais aplicações por utilização de largura de banda de entrada e saída.
3. Principais aplicações por taxa de transferência de bytes.
4. Principais hosts por número de ameaças identificadas.
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.
6. Deve permitir a criação de relatórios personalizados.

kk) 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.

ll) Gerar alertas automáticos via:

1. Email.
2. SNMP.
3. Syslog.

6.5.7. CAPACIDADE DO APPLIANCE

a) Hardware Specifications
b) GE RJ45 WAN Interfaces 2
c) GE RJ45 Management/HA Ports 2
d) GE RJ45 Ports 14
e) GE SFP Slots 4
f) USB port 1
g) Console (RJ45) 1
h) Local Storage — 1x 480 GB SSD
i) Included Transceivers 0
j) PS Throughput 2 2.2 Gbps
k) NGFW Throughput 2, 4 1.8 Gbps
l) Threat Protection Throughput 2, 5 1.2 Gbps
m) Firewall Throughput
n) (1518 / 512 / 64 byte UDP packets)
o) 20 / 20 / 9 Gbps
p) Firewall Latency (64 byte UDP packets) 3 µs
q) Firewall Throughput (Packets Per Second) 13.5 Mpps
r) Concurrent Sessions (TCP) 2 Million
s) New Sessions/Second (TCP) 135,000
t) Firewall Policies 10,000
u) IPsec VPN Throughput (512 byte) 1 7.2 Gbps
v) Gateway-to-Gateway IPsec VPN Tunnels 2,000
w) Client-to-Gateway IPsec VPN Tunnels 10,000
x) SSL-VPN Throughput 900 Mbps
y) Concurrent SSL-VPN Users
z) (Recommended Maximum, Tunnel Mode)
aa) 500
bb) SSL Inspection Throughput (IPS, avg. HTTPS) 3 820 Mbps
cc) SSL Inspection CPS (IPS, avg. HTTPS) 3 1,000
dd) SSL Inspection Concurrent Session
ee) (IPS, avg. HTTPS) 3
ff) 240,000
gg) Application Control Throughput (HTTP 64K) 2 3.5 Gbps
hh) CAPWAP Throughput (1444 byte, UDP) 1.5 Gbps
ii) Virtual Domains (Default / Maximum) 10 / 10
jj) Maximum Number of FortiSwitches Supported 24
kk) Maximum Number of FortiAPs
ll) (Total / Tunnel Mode)
mm) 128 / 64
nn) Maximum Number of FortiTokens 5,000
oo) Maximum Number of Registered FortiClients 600
pp) High Availability Configurations Active / Active, Active / Passive, Clustering
qq) Height x Width x Length (inches) 1.75 x 17.0 x 11.9
rr) Height x Width x Length (mm) 44.45 x 432 x 301
ss) Weight 11.9 lbs (5.4 kg) 12.12 lbs (5.5 kg)
tt) Form Factor Rack Mount, 1 RU
uu) Power 100–240V AC, 50–60 Hz
vv) Maximum Current 110 V / 3 A, 220 V / 0.42 A

ww) Power Consumption (Average / Maximum) 70.98 / 109.9 W
xx) Heat Dissipation 374.9 BTU/h
yy) Operating Temperature 32–104°F (0–40°C)
zz) Storage Temperature -31–158°F (-35–70°C)
aaa) Humidity 10–90% non-condensing
bbb) Noise Level 31.1 dBA
ccc) Operating Altitude Up to 7,400 ft (2,250 m)
ddd) Compliance FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL,
eee) CB, BSMI
fff) Certifications ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN;
ggg) IPv6

6.5.8. CONTROLE POR POLÍTICA DE FIREWALL

a) Deverá suportar controles por zona de segurança.

b) Controles de políticas por porta e protocolo.

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

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

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

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

g) Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise).

h) Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF).

i) Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supere a velocidade de upload.

j) Deve suportar o protocolo padrão da indústria VXLAN.

6.5.9. CONTROLE DE APLICAÇÕES

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

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

c) 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.

d) 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.

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

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

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

h) 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.

i) 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.

j) Identificar o uso de táticas evasivas via comunicações criptografadas.

k) Atualizar a base de assinaturas de aplicações automaticamente.

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

m) 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.

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

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

p) Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações

desconhecidas e não somente sobre aplicações conhecidas.

q) 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.

r) A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.

s) O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

t) Deve alertar o usuário quando uma aplicação for bloqueada.

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

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

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

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

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

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

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

6.5.10. PREVENÇÃO DE AMEAÇAS

a) 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.

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

c) 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.

d) Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando

implementado em alta disponibilidade.

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

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

g) Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.

h) Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.

i) Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

j) Deve permitir o bloqueio de vulnerabilidades.

k) Deve permitir o bloqueio de exploits conhecidos.

l) Deve incluir proteção contra ataques de negação de serviços.

m) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões.

n) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo.

o) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo.

p) Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística.

q) Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation.

r) Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP.

s) Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados.

t) Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

u) Detectar e bloquear a origem de portscans.

v) Bloquear ataques efetuados por worms conhecidos.

w) Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

x) Possuir assinaturas para bloqueio de ataques de buffer overflow.

y) Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

z) Deve permitir usar operadores de negação na criação de assinaturas customizadas

de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.

aa) Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

bb) Identificar e bloquear comunicação com botnets.

cc) Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

dd) Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

ee) Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

ff) Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.

gg) Os eventos devem identificar o país de onde partiu a ameaça.

hh) Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

ii) Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

jj) Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

kk) O Firewall deve permitir que se analise a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que podem ser usadas para melhorar a segurança e o desempenho geral da rede.

ll) Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis.

mm) Análise de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint.

nn) Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem).

6.5.11. FILTRO DE URL

a) 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).

b) Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.

c) Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.

d) Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

e) Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.

f) Possuir pelo menos 60 categorias de URLs.

g) Deve possuir a função de exclusão de URLs do bloqueio, por categoria.

h) Permitir a customização de página de bloqueio.

i) Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).

j) Além do Explicit Web Proxy, suportar proxy Web transparente.

6.5.12. IDENTIFICAÇÃO DE USUÁRIOS

a) 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.

b) Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

c) Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2.

d) Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não

limitado à, utilização de sistemas virtuais, segmentos de rede, etc.

e) Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

f) Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

g) 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).

h) 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.

i) Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

j) Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.

k) Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

6.5.13. QoS E TRAFFIC SHAPING

a) Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

b) Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.

c) Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.

d) Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.

e) Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.

f) Suportar a criação de políticas de QoS e Traffic Shaping por porta.

g) O QoS deve possibilitar a definição de tráfego com banda garantida.

h) O QoS deve possibilitar a definição de tráfego com banda máxima.

i) O QoS deve possibilitar a definição de fila de prioridade.

j) Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

k) Suportar marcação de pacotes Diffserv, inclusive por aplicação.

l) Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.

m) Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

6.5.14. FILTRO DE CONTEÚDO

a) Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).

b) Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

c) Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

d) 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.

6.5.15. GEOLOCALIZAÇÃO

a) Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado Pais/Países sejam bloqueados.

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

c) Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

6.5.16. 1VPN IPSec

a) Suportar VPN Site-to-Site e Cliente-To-Site.

b) Suportar IPSec VPN.

c) Suportar SSL VPN.

d) A VPN IPSEc deve suportar 3DES.

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

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

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

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

i) A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

j) Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

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

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

m) A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

n) 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.

o) Atribuição de DNS nos clientes remotos de VPN.

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

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

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

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

t) Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Antes do usuário autenticar na estação.

u) Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Após autenticação do usuário na estação.

v) Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Sob demanda do usuário.

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

x) O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

7. DOS LOCAIS DE PRESTAÇÃO DO SERVIÇO

Órgão deverá disponibilizar a relação dos endereços e velocidades que deverão ser entregues na solução.

8. DOS PRAZOS DE EXECUÇÃO DOS SERVIÇOS

8.1. ELABORAÇÃO DO PLANO DE IMPLANTAÇÃO

8.1.1. A CONTRATADA deverá apresentar um Plano de Implantação em no máximo 10 (dez) dias corridos a partir da assinatura do Contrato.

8.1.2. A execução do Plano de Implantação somente poderá ser iniciada após a sua aprovação pela CONTRATANTE.

8.1.3. O detalhamento do Plano de Implantação deverá conter no mínimo:

a) Cronograma com macro atividades a serem desenvolvidas para a implantação de todos os serviços previstos neste Termo de Referência. O cronograma deverá conter as seguintes informações:

- Identificação dos responsáveis das atividades.
- Duração das atividades.

- Sequenciamento das atividades.

b) Projeto com topologias (física e lógica) da rede, elementos envolvidos, localização dos POPs, faixas de endereçamento IP, detalhamento da gerência, bem como a arquitetura do serviço, incluindo a estratégia de roteamento.

8.2. DA INSTALAÇÃO DOS SERVIÇOS

8.2.1. A CONTRATADA terá até trinta (30) dias corridos após a assinatura do contrato para instalar os serviços especificados no Edital e Termo de Referência.

8.2.2. A instalação do circuito e CPE somente será considerada concluída após a aprovação, pelo Gestor do Contrato, que ocorrerá em até 5 (cinco) dias corridos após notificação da CONTRATADA.

8.2.3. Todos os equipamentos deverão suportar alimentação com tensão de 110/220 Volts (corrente alternada) bifásica com frequência de 60 Hz.

8.3. DO GERENCIAMENTO DA IMPLANTAÇÃO

8.3.1. Disponibilizar e alocar 1 (um) profissional que será responsável pelo gerenciamento das atividades do projeto de implantação, por parte da CONTRATADA.

8.3.2. Obter informações e esclarecimentos necessários para que possa elaborar o Plano de Implantação do Serviço. Serão abordados e discutidos os seguintes pontos:

a) Instalação dos circuitos.

b) Datas e horários de restrição para implantação.

c) Requisitos de infraestrutura necessários para a instalação dos equipamentos.

d) Requisitos para a elaboração e entrega do Plano de Implantação do Serviço.

e) Serviços que deverão ser configurados na implantação.

f) Demais assuntos de interesse correlatos à implantação dos serviços.

8.3.1. Apresentar ao Gestor do Contrato do CONTRANTE o(s) profissional(is) que atuará(ão) como preposto(s) da empresa para assuntos relativos à execução contratual, e informar ao CONTRANTE o nome completo e o CPF deste(s) preposto(s).

9. CENTRAL DE ATENDIMENTO E SUPORTE TÉCNICO

9.1. A fim de manter os serviços em funcionamento adequado aos parâmetros contratuais, a CONTRATADA deverá:

9.1.1. Possuir um Centro de Operações de Rede (Network Operations Center – NOC) disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por monitorar o funcionamento dos serviços e realizar as ações corretivas necessárias para restabelecer a normalidade dos serviços.

9.1.2. Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento,

detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.

9.1.3. A CONTATADA deverá disponibilizar à CONTRATANTE uma Central de Atendimento Técnico, acessível via chamada telefônica gratuita (0800), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por prestar suporte técnico, receber chamados de serviços e prestar informações acerca do andamento destes.

9.1.4. O limite de atuação da CONTRATADA para fins de manutenção, reparo e configuração será a porta LAN de seus roteadores ou switches, de forma a garantir os níveis de serviço contratados.

9.1.5. Enviar à CONTRATANTE, por e-mail, notificações de abertura, andamento e fechamento de chamados, realização de manutenção preventiva ou corretiva e fatos relevantes para a prestação e utilização dos serviços.

9.1.6. Enviar à CONTRATANTE, por e-mail, uma lista de recorrência (“escalation list”) contendo os nomes, números de telefone e endereços de e-mail das pessoas que devem ser acionadas em caso de problemas no atendimento técnico. A lista de recorrência deverá ser mantida atualizada e sua versão mais recente deverá ser enviada à CONTRATANTE sempre que houver alteração.

9.1.7. A CONTRATADA deverá iniciar o atendimento no prazo máximo de 1 (uma) hora, contada a partir da data e hora do chamado.

9.1.8. Todo acesso às instalações da CONTRATANTE por pessoal técnico da CONTRATADA, ou de seu preposto, deverá ser previamente agendado.

9.1.9. Manutenções e/ou intervenções programadas nos serviços, quando necessárias, mesmo no caso daquelas que não impliquem inoperância dos serviços contratados ou alteração nas suas características, que necessitem a presença do técnico da CONTRATADA, deverão ser autorizadas pela CONTRATANTE.

9.1.10. Qualquer manutenção e/ou intervenção de caráter emergencial para solução de falhas, inoperâncias e/ou indisponibilidades, verificadas na rede, deverá ser agendada e acordada previamente com a CONTRATANTE.

10. PORTAL DE GERENCIAMENTO E ACOMPANHAMENTO DOS SERVIÇOS

10.1. A CONTRATADA deverá disponibilizar um Portal WEB de gerência, possibilitando a visualização online dos serviços prestados, como também realizar o registro e acompanhamento dos chamados.

10.1.1. **Consulta e visualização online:** O Portal deverá apresentar informações relativas aos ativos de rede utilizados com as seguintes funcionalidades:

a) Alertas em caso de falhas e anormalidade dos circuitos.

b) Topologia da rede, incluindo roteadores e circuitos, com a visualização do status de todos os elementos.

c) Visualização da utilização de banda dos circuitos, de forma diária, semanal e mensal, com a opção de consulta de dados históricos de até 3 (três) meses.

d) Visualização do consumo de CPU e memória dos roteadores.

e) Indicação da taxa de perda de pacotes, latência e disponibilidade nos circuitos.

f) Inventario dos roteadores contendo a configuração física de cada equipamento (interfaces, memoria, cpu, etc). modelo e fabricante. endereços IPs e máscaras.

10.1.2. Registro e acompanhamento dos chamados:

Permitir o acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços, relativos à pelo menos aos últimos 90 (noventa) dias, incluindo as seguintes informações:

a) Identificação do registro (número de chamado).
b) Data e hora de abertura do chamado (registro).
c) Descrição do problema.
d) Identificação do reclamante (nome e telefone).
e) Data e hora de conclusão do atendimento (fechamento do chamado).
f) Ações realizadas para a solução do problema.

11. GERENCIAMENTO PROATIVO

11.1. A CONTRATADA deverá prover o gerenciamento proativo, com funcionamento 24 horas por dia, 7 (sete) dias na semana, incluindo sábados, domingos e feriados. Entende-se por gerenciamento proativo a capacidade da CONTRATADA de detectar falhas ocorridas nos circuitos (serviços e equipamentos) de forma autônoma e independentemente de notificação por parte da CONTRATANTE. Da mesma forma autônoma a CONTRATADA deve dar início aos procedimentos de correção de falhas e em seguida informar a CONTRATANTE sobre o evento. A CONTRATADA deverá notificar a CONTRATANTE através de telefones e e-mails definidos pela CONTRATANTE no prazo máximo de 25 minutos após a identificação do incidente.

11.2. Gerência exclusiva de relacionamento para acompanhamento, apresentação da evolução e gestão da rede, que fará mensalmente o agendamento e apresentação dos relatórios, através de videoconferência ou por e-mail.

11.3. Atividades realizadas pela equipe responsável pelo gerenciamento proativo:

a) Gerenciamento individualizado da rede.
b) Relatórios mensais sobre a performance da rede.
c) Relatório Gráfico de indisponibilidade.
d) Relatório de tráfego de qualidade.

e) Relatório de Consumo de Banda.

f) Relatório de Eventos ocorridos.

g) Relatório de Disponibilidade dos serviços.

h) Gerenciamento de desempenho proativo.

12. DISPONIBILIDADE

12.1. Índice de Disponibilidade**:**

12.1.1. Os circuitos de comunicação deverão estar disponíveis 24 horas por dia, todos os dias do ano.

12.1.2. A CONTRATADA deverá garantir disponibilidade mensal de no mínimo, 99,5% para cada circuito fornecido à CONTRATANTE, calculada da seguinte forma:

DMA = [(43200 - TTICM) / 43200] x 100

Onde:

TTICM: Tempo Total de Interrupção do Circuito (em minutos) no Mês.

DMA(%): Disponibilidade Mensal Atingida

12.1.3. Para efeito de cálculo de TTICM, será considerado o período em minutos entre o primeiro minuto do primeiro dia e o último minuto do último dia do calendário do mês a que se refere a fatura.

12.1.4. O serviço será considerado indisponível quando não for possível a conexão entre o equipamento da CONTRATANTE e o da CONTRATADA, a partir do registro do chamado técnico na Central de Atendimento da CONTRATADA, sendo considerado disponível após o fechamento do chamado técnico, com a devida anuência da CONTRATANTE, na Central de atendimento da CONTRATADA.

12.1.5. Entende-se como início do atendimento a primeira mensagem trocada pela CONTRATANTE com a CONTRATADA informando a ocorrência ou início da ligação efetuada a central de atendimento da CONTRATADA independentemente do atendimento do operador.

12.1.6. O prazo máximo de recuperação dos circuitos será 2 (duas) horas, todos os dias do mês, inclusive sábados, domingos e feriados.

12.1.7. As indisponibilidades informadas pela gerência e supervisão da CONTRATADA, bem como os registros na Central de Atendimento da CONTRATADA serão validadas pelos sistemas de gerência e supervisão da CONTRATANTE.

12.1.8. No caso de interrupção programada por necessidade da CONTRATANTE, a mesma não afetará o índice de disponibilidade da CONTRATADA.

12.1.9. As interrupções programadas solicitadas pela CONTRATANTE serão previamente combinadas com a CONTRATADA.

12.2. Desconto por interrupção**:**

12.2.1. Para cada interrupção do circuito que for comprovadamente de responsabilidade da CONTRATADA, será calculado um desconto referente ao tempo de interrupção desse circuito, cujo valor apurado será ressarcido à CONTRANTANTE na Nota Fiscal/Fatura dos serviços com vencimento no mês seguinte ao da apuração.

12.2.2. O valor do desconto será obtido a partir do seguinte cálculo:

VD = (VC / 43200) x n

Onde:

VD = Valor do Desconto

VC = Valor mensal pago pelo circuito ativo

n = Quantidade de minutos em que o serviço ficou interrompido.

13. NÍVEIS MÍNIMOS DE SERVIÇO

A CONTRATADA deverá fornecer o serviço com os seguintes níveis mínimos de disponibilidade, latência e taxa máxima de erro, os quais são utilizados para mensurar o desempenho e a qualidade dos circuitos:

Métrica	**Nível Mínimo de Serviço**
Disponibilidade do circuito IP	>= 99,5%
Latência	<= 1ms
Perda de pacotes	<=2%

14. DAS OBRIGAÇÕES

14.1. OBRIGAÇÕES DA CONTRATANTE

a) Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

b) Comunicar oficialmente à CONTRATADA sobre quaisquer falhas verificadas na fiscalização do cumprimento dos serviços prestados.

c) Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.

d) Efetuar o pagamento devido pela execução do(s) serviço(s) dentro do prazo estipulado, desde que cumpridas todas as formalidades e exigências contratuais.

e) Acompanhar as visitas, inspeções, reuniões solicitadas pela CONTRATADA.

f)Prestar, por meio do Gestor do Contrato, as informações e os esclarecimentos pertinentes ao(s) serviço(s) contratado(s) que venham a ser solicitados pela

CONTRATADA.

g) Registrar os incidentes e problemas ocorridos durante a execução do Contrato.

h) Proporcionar os recursos necessários, técnicos e logísticos, dentro dos locais de instalação dos equipamentos para que a CONTRATADA possa executar os serviços conforme as especificações estabelecidas no Termo de Referência.

i) Permitir acesso dos empregados da CONTRATADA, desde que devidamente credenciados, às suas dependências para a realização dos serviços.

j) Aplicar as sanções previstas, assegurando à CONTRATADA o contraditório e à ampla defesa.

14.2. OBRIGAÇÕES DA CONTRATADA

a) Prestar os esclarecimentos que forem solicitados pelo CONTRATANTE, bem como dar ciência ao mesmo, imediatamente e por escrito, de qualquer anormalidade que verificar.

b) Comunicar imediatamente ao CONTRATANTE qualquer alteração ocorrida na conta bancária, endereço e outras informações necessárias para recebimento de correspondências e pagamento.

c) Responsabilizar-se pelo exato cumprimento de todas as obrigações e exigências decorrentes da legislação trabalhista e previdenciária, ficando claro inexistir entre seus empregados e o CONTRATANTE vínculo empregatício ou de qualquer outra natureza, razão pela qual correrão por conta exclusiva da CONTRATADA todos os ônus decorrentes de rescisões de contratos de trabalho e atos de subordinação de seu pessoal.

d) Arcar com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução do serviço contratado, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista.

e) Manter, durante a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação exigidas em razão da natureza das atividades prestadas e do certame licitatório.

f) Fazer diagnóstico das falhas no serviço relatadas pelo CONTRATANTE dentro do prazo estipulado.

g) Providenciar a recuperação de falhas na prestação do serviço, comunicadas pelo CONTRATANTE mantendo-o informado sobre as ações efetivadas até a completa normalização da prestação do serviço.

h) Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele.

i) Credenciar junto ao CONTRATANTE um representante, para prestar esclarecimentos e atender às reclamações que porventura surgirem durante a execução do contrato.

j) O CONTRATANTE não aceitará a transferência de responsabilidade da CONTRATADA

para terceiros.

k) Prestar o serviço contratado conforme especificações, prazos e demais condições estabelecidas no Termo de Referência.

l) Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas neste Contrato e no Termo de Referência.

m) Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do(s) serviço(s)

n) Atender e prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da área de tecnologia da Informação do CONTRATANTE, referentes a qualquer problema detectado ou ao andamento de atividades previstas.

o) Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas neste instrumento, caso os prazos, indicadores e condições não sejam cumpridos.

p) Manter seus profissionais nas dependências do CONTRATANTE adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível.

q) Manter-se, durante toda a execução do contrato, em conformidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

15. DA VIGÊNCIA DO CONTRATO

15.1. O contrato terá período de vigência de 12 (doze) meses. Podendo ser prorrogado por meio de termo aditivo.

16. DISPOSIÇOES FINAIS

16.1. Não serão aceitas propostas que apresentem preço global ou unitário simbólicos, irrisórios ou de valor zerado, incompatíveis com os preços pelo mercado.

17. DA VISITA TÉCNICA

17.1. É facultado aos interessados a realização de visita técnica no Hospital Municipal de Aparecida de Goiânia, localizado na Avenida V5 e V7, – Cidade Vera Cruz – Aparecida de Goiânia/GO, para levantamento do perfil e especificações dos serviços.

18. DA CONTRATAÇÃO

18.1. O IBGH não tem a obrigação de contratar o serviço publicado, e podendo optar também, na contratação parcial destes.

18.2. As propostas terão validade de 90 (noventa) dias, após a apresentação da mesma.

Aparecida de Goiânia/Go, 11 de outubro de 2019.

_____

Jefferson Tadeu de Oliveira

Gerencia de Tecnologia da Informação