**Contratação de empresa de telecomunicações devidamente autorizada pela Agência Nacional de Telecomunicações – ANATEL, para prestar serviços de comunicação de dados, voz e imagem, mediante a implantação, configuração, administração, gerenciamento, monitoramento e manutenção de uma Rede WAN do Sebrae em Rondônia, através da tecnologia MPLS e um Link dedicado de acesso à Internet com recursos de segurança.**

|  |
| --- |
| 1. **JUSTIFICATIVA**   Considerando o crescimento da rede de dados do SEBRAE/RO, com o aumento no número de usuários dos recursos de TI da instituição, a implantação de novos serviços em nossa infraestrutura e a necessidade de evolução tecnológica com mais rapidez e segurança. Fica evidente a necessidade de uma nova contratação, contemplando equipamentos como roteadores mais modernos, equipamentos que possam garantir a segurança corporativa e links com mais velocidades que possam atender as demandas atuais.  A Unidade de Tecnologia da Informação e Comunicação – UTIC vem atuando de forma alinhada aos objetivos, proporcionando os meios mais adequados para garantir a fluidez da informação e garantindo a segurança da informação. É premissa que tudo seja proporcionado dentro de uma adequada ótica de custos.  Embora parte de nossos serviços seja via protocolo HTTP – totalmente acessível pela Internet, ainda necessitamos de uma conexão estável e segura para manter o mínimo de qualidade no tráfego de informações entre as unidades. Assim, não podemos descartar a utilização da tecnologia MPLS como meio para estabelecer a rede WAN do Sebrae/RO. Outrossim, devemos considerar que para garantir a segurança da informação, em caso de links Internet (não MPLS), devemos, além de adquirir ferramentas para VPN (Virtual Private Net – Rede Privada Virtual), ter mão de obra disponível para o gerenciamento desta VPN e eventuais ocorrências.  Com a contratação de comunicação com a tecnologia MPLS estamos mitigando o risco, através da transferência de responsabilidade, em caso de falhas tanto de segurança quanto de indisponibilidade.  Outrossim, vale destacar que a UTIC vem proporcionando um melhor aproveitamento desta conexão com os escritórios através de criação de novos serviços. Recentemente agregamos a utilização de ramais sobre IP, possibilitando que as ligações entre Sede-Escritórios e Escritórios-Escritórios sejam efetuadas como ramais, sem utilizar as operadoras de telefonia.  Alguns serviços apresentam melhor performance sobre a rede MPLS, como o ERP Corpore RM, serviços de diretório, acesso à arquivos e os serviços disponibilizados pelo Sebrae/NA, uma vez que nossa conexão com o Sebrae/NA é MPLS.  Além da rede MPLS interligando os escritórios e os pontos de atendimento, há a necessidade de um link Internet na Sede Administrativa para, dentre outros serviços, prover uma redundância de acesso aos serviços disponibilizados localmente e permitir o compartilhamento de acesso à Internet em treinamentos que demandam este recurso. Devido a necessidade de ter uma conta nos domínios Sebrae, fica inviável fornecer o acesso Internet pela rede existente. Seria necessário criar uma conta para cada cliente.  Todo acesso será liberado mediante cadastro, mantendo conformidade com a lei 12.965 de 23 de abril de 2014 (Marco Civil da Internet). |
| 1. **OBJETO**   Contratação de empresa de telecomunicações devidamente autorizada pela Agência Nacional de Telecomunicações – ANATEL, para prestar serviços de comunicação de dados, voz e imagem, mediante a implantação, configuração, administração, gerenciamento, monitoramento e manutenção de uma Rede WAN do Sebrae em Rondônia, através da tecnologia MPLS e um link dedicado de acesso à Internet com recursos de segurança. |
| 1. **LEGISLAÇÃO APLICÁVEL**   Todo o procedimento será processado e julgado em conformidade com o Regulamento de Licitações e de Contratos do Sistema SEBRAE, em sua versão atualizada em 18 de maio de 2011, aprovada pela Resolução CDN nº 213/2011 que altera e consolida a lei complementar nº 123, de 14 de dezembro de 2006, recepcionada no âmbito do SEBRAE, via Resolução CDN nº 166/2008, pelo edital e seus anexos. |
| 1. **DETALHAMENTO DO OBJETO**  |  |  |  |  | | --- | --- | --- | --- | | **LOTE 01** | ESPECIFICAÇÃO | **UNID. DE MEDIDA** | **QUANT.** | | 1.1. Link Urbano de 400 Mbps, com Solução de Segurança UTM/NGFW em HA - high availability (fisico), com Proteção contra ataques DDoS e Serviço de monitoração pró-ativo. | Mbps | 01 | | **LOTE 02** | **ESPECIFICAÇÃO** | **UNID. DE MEDIDA** | **QUANT. (PONTOS)** | | 2.1. Serviço de Transmissão de dados de 350 Mbps com Serviço de monitoração pró-ativo - CONCENTRADOR MPLS/L2L. | Mbps | 01 | | 2.2. Serviço de Transmissão de dados de 50 Mbps com Serviço de monitoração pró-ativo – Rede MPLS/L2L. | Mbps | 07 |  * 1. A Empresa CONTRATADA deverá fornecer Links Urbanos e Interurbanos para interligação da sede do Sebrae em Rondônia, utilizando tecnologia MPLS/L2L com disposições e características, com as especificações abaixo:      1. Links com acesso à Internet com banda igual ou superior a 400 Mbps (**LOTE 01**), com tecnologia ATM ou Ethernet/Metro Ethernet ou outras tecnologias, suportando o protocolo TCP/IP, com 98,5% de garantia de utilização de banda e obedecendo aos seguintes parâmetros:  |  |  |  | | --- | --- | --- | | **link dedicado de acesso à Internet com recursos de segurança** | | | | **LOTE 01** | | | | **DESCRIÇÃO DO LOTE** | **QTDE** | **CPE** | | 1.1 Link Urbano de 400 Mbps, com Solução de Segurança UTM/NGFW em HA - high availability (fisico), com Proteção contra ataques DDoS e Serviço de Monitoração Pró-ativo. | 01 | *TIPO 01* |  1. O Link referente ao **LOTE 01** deverá ser instalado no Prédio Sede, localizado Av. Campos Sales nº 3421 - Bairro Olaria, Porto Velho – RO CEP: 76801-281; 2. Link dedicado com estrutura exclusivamente em fibra óptica até seu ponto final; 3. Não serão aceitos links dedicados via enlace de rádio digital, ou par metálico, mesmo que devidamente licenciado e autorizado pela Anatel; 4. Fornecimento de conectividade IP – *Internet Protocol* – a 400 Mbps (megabytes por segundo), velocidade fixa, *full duplex*, síncrona, simétrica e permanente, que suporte aplicações TCP/IP e proveja o acesso à rede Internet; 5. O acesso deverá ser permanente (24 horas por dia e 07 dias por semana, a partir de sua ativação), dedicado, exclusivo, ou seja, serviço determinístico na rede de acesso e com total conectividade IP; 6. Todo o serviço de Internet deverá ser disponibilizado por meio de conexão direta e exclusiva da CONTRATANTE a um provedor de *backbone* Internet, não sendo necessária a contratação de provedor de acesso por parte da CONTRATANTE; 7. Fornecimento de, no mínimo, 16 (dezesseis) números IPs próprios e válidos na Internet, para o item do **LOTE 01;** 8. O índice de latência, perda de pacotes e disponibilidade do serviço deverão atender aos valores expressos abaixo:    * *Latência (milissegundos): consiste no tempo médio de trânsito (ida e volta – roundtrip) de um pacote de 64 bytes entre dois pontos de backbone. É usada a média do backbone considerando o centro de gerenciamento da rede e cada um dos centros de roteamento. Objetivo: 50 ms;*    * *Perda de Pacotes (%): consiste na taxa de falha na transmissão de pacotes IP entre dois pontos do backbone. É usada a média do backbone considerando o centro de gerenciamento da rede e cada um dos centros de roteamento. Objetivo: 2,0%;*    * *Disponibilidade (%): consiste no percentual de tempo no qual a rede está operacional em um período de tempo. É considerado o ROTEADOR DE ACESSO (do backbone) no qual está instalada a porta de conectividade IP do cliente. Objetivo: 99,35%.* 9. O equipamento ROTEADOR deverá ser fornecido pela empresa e acoplável a Rack de 19’’, atendendo às seguintes especificações:    * *Possuir, no mínimo, 04 (quatro) Gigabit Ethernet 10/100/1000 de detecção automática que sejam compatíveis com os padrões ISO 8802.3 e IEE 802.3;*    * *A interface física da porta LAN deverá ser fornecida no padrão RJ-45 (10baseT), para cabos UTP, CAT;*    * *Possuir opção de boot local via memória flash ou similar;*    * *Permitir ser alimentado de forma automática por tensões de 110/220 VAC, frequência 60 Hz com duas fontes redundantes;*    * *Deverá suportar e implementar serviços de DHCP Server;*    * *Deverá ser gerenciável via SNMP.*      1. Pontos de Interligação Interurbana, à sede do SEBRAE, Porto Velho - RO:  |  |  |  | | --- | --- | --- | | **linkS MPLS/l2L – INTERURBANO com monitoramento pró-ativo** | | | | **LOTE 02** | | | | **DESCRIÇÃO DO LOTE** | **QTDE** | **CPE** | | 2.1 Concentrador MPLS/L2L de 350Mpls | 1 | *TIPO 01* | | 2.2 Link MPLS/L2L de 50 Mbps | 7 | *TIPO 02* |  * 1. Inclui-se, na execução dos serviços a ser contratado, o fornecimento de equipamentos necessários ao funcionamento dos serviços objeto deste Termo de Referência, bem como a instalação, garantia de peças, suporte e assistência técnica permanente ao equipamento, objetivando atender nossa necessidade atual de comunicação, com manutenção e reposição de partes e peças desgastadas pelo uso normal do equipamento. A solução proposta deverá contemplar todos os equipamentos necessários, tais como: modems, roteadores, Sub-bastidor, fontes, softwares, numeração IP Privada e serviços necessários para implantação e manutenção dos mesmos. O valor, tanto de instalação, quanto mensal do Link de Internet, bem como roteador e equipamentos necessários, serviços de segurança, deverão estar previstos na formação de preço de todos os **LOTES;**   2. A CONTRATADA aplicará nos equipamentos, quando necessário, a substituição de partes e peças originais, adequadas, novas ou, quando não, que mantenham as especificações técnicas do fabricante, ficando desde logo, autorizada pelo Sebrae em Rondônia;   3. Os endereços das unidades do Sebrae em Rondônia previstas para serem interligadas, estão relacionados nos itens 5.1, 5.2 e 5.3 do Termo de Referência. Os endereços, bandas e classes constantes neste Termo foram levantados no momento da elaboração deste Termo de Referência, e podem ser alterados. No decorrer da vigência do contrato de prestação de serviço poderá eventualmente haver mudança de endereços, bandas e classes das unidades do Sebrae em Rondônia, assim como a adição de novas unidades no projeto. No caso de mudança de endereços e a adição de novas unidades, a CONTRATADA deverá arcar com os respectivos custos de alteração da rede, desde que não seja necessário o desenvolvimento de projetos especiais para atendimento, estimulado por estar fora da área de ATB, definido pela ANATEL, ou que não seja um concentrador instalado em Fibra Ótica;   4. Havendo a necessidade de desenvolvimento de projetos especiais para mudança de endereço e/ou adição de novas unidades, a CONTRATADA deverá apresentar uma planilha de valores referente à alteração/adição, para previa aprovação da CONTRATANTE;   5. **Requisitos Obrigatórios para o Link de Internet:**  |  |  | | --- | --- | | ***Requisitos Obrigatórios para o Link de INTERNET*** | ***REFERÊNCIA*** | | ***Tipo de Acesso*** – Especifica o tipo de conexão com a unidade remota do órgão. | Internet com acesso terrestre. | | ***Disponibilidade de Serviço*** – Relação entre o tempo de operação plena e prejudicada no período de 30 dias. | 99,35%. | | ***Tempo Máximo de Retardo Admissível*** – O tempo máximo de retardo na comunicação unilateral entre o ponto de conexão e o roteador de borda da Proponente para um pacote de 32 bytes. | Deverá ser igual ou inferior a 100 ms. | | ***Banda Mínima Garantida*** – Banda mínima disponível para acesso à Internet para cada um dos pontos contemplados. | 98,5% da largura da banda contratada. | | ***Ativação*** – Período entre a assinatura do contrato e ativação do serviço. | 30 (trinta dias). | | ***Prazo de Manutenção*** – Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento. | 12 (doze) horas. | | ***Prazo Mínimo de Notificação de Manutenção Preventiva ou Atualização de Recursos Técnicos*** – Período mínimo entre a notificação do cliente pela operadora até o início da interrupção programada. | 07 (sete) dias. | | ***Abertura de Chamado*** – Disponibilidade de atendimento para solicitação de reparos, Help Desk da Operadora Contratada e discagem sem cobrança (0800) em língua portuguesa. | 24 x 7  (00:00 às 24:00 de Segunda a Domingo). | | ***Horário de Reparo*** – Disponibilidade de atendimento técnico a partir da abertura do chamado. | | ***Quantidade de IPs Fixos Válidos*** – Disponibilização de endereços IPs fixos válidos. | 16 (dezesseis). | | ***Sistema WEB de Monitoramento do Link*** – Disponibilidade de acesso ao sistema WEB de monitoramento de disponibilidade, utilização e falha do Link. | Sim. | | ***Serviço de Segurança*** – Disponibilização de acesso à Internet com solução integrada de segurança da informação. |  * 1. **Requisitos Obrigatórios para os Links (Urbano e Interurbano):**  |  |  | | --- | --- | | ***Requisitos Obrigatórios para os Links MPLS/L2L*** | ***REFERÊNCIA*** | | ***Tipo de Acesso*** – Especifica o tipo de conexão com a unidade remota do órgão. | Acesso por Fibra Óptica, que garantam o funcionamento de todas as especificações deste Termo de Referência. | | ***Tempo Máximo de Retardo Admissível*** – O tempo máximo de retardo na comunicação unilateral entre o ponto de conexão e o roteador de borda da Proponente para um pacote de 32 bytes. | Fibra Óptica:  = ou < 50 MS | | Demais Conexões:  = ou < 400 MS | | ***Banda Mínima Garantida*** – Banda mínima disponível para acesso a Internet para cada um dos pontos contemplados. | Fibra Óptica:  98,5% da banda | | Demais Conexões:  98,5% da banda | | ***Ativação*** – Período entre a assinatura do contrato e ativação do serviço. | 60 (sessenta dias). | | ***Prazo de Manutenção*** – Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento. | 24 (vinte e quatro) horas | | ***Prazo Mínimo de Notificação de Manutenção Preventiva ou Atualização de Recursos Técnicos*** – Período mínimo entre a notificação do cliente pela operadora até o início da interrupção programada. | 07 (sete) dias. | | ***Abertura de Chamado*** – Disponibilidade de atendimento para solicitação de reparos, Help Desk da Operadora Contratada e discagem sem cobrança (0800) em língua portuguesa. | 24 x 7  (00:00 às 24:00 de Segunda a Domingo). | | ***Horário de Reparo*** – Disponibilidade de atendimento técnico a partir da abertura do chamado. | 06 (seis) horas |  SERVIÇO DE PROTEÇÃO NO BACKBONE CONTRA ATAQUES DDoS PARA O LOTE 01:  * + 1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*);     2. A CONTRATADA deve disponibilizar um Centro Operacional de Segurança (*ou SOC – Security Operations Center*) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 07 (sete) dias da semana, no período de vigência contratual;     3. O acesso à Internet (circuito de dados) não poderá ser subcontratado de terceiros, devendo a CONTRATADA fornecer ambos os serviços, solução ANTI-DDoS e circuito de dados;     4. A técnica ANTI-DDoS utilizada deverá ser por métrica de volumetria, assim a contratada deverá enviar junto com a proposta técnica, qual a estratégia utilizada para mitigação de ataques DDOS sobre o circuito de dados;     5. A solução ANTI-DDoS deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (*DDoS – Distributed Denial of Service*) ou não;     6. A CONTRATADA deve possuir e disponibilizar 01 (um) centro de limpeza nacional com capacidade de mitigação de no mínimo 40Gbps, sendo o mesmo responsável também por limpeza internacional;     7. A contratada deve apresentar certificado ou atestado da Ferramenta Anti-DDoS utilizada;     8. Não haverá taxa adicional para a por volume de mitigação de ataques (*DDoS – Distributed Denial of Service*) nos IP’s monitorados;     9. A alteração de capacidade de mitigação deverá ser implementada em um prazo máximo de 5 dias úteis, a contar da data de solicitação formal através de correio eletrônico encaminhado via chave oficial ou de autorizados pelo gestor do contrato;     10. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis;     11. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;     12. 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;     13. A CONTRATADA deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo;     14. Para a mitigação dos ataques o tráfego só deverá ser encaminhado para limpeza fora do território brasileiro nos casos em que os centros nacionais não suportarem a capacidade de mitigação e a demanda de ataques, no restante os ataques de origem nacional deverão ser tratados nos centros nacionais e os de origem internacional nos centros internacionais;     15. O envio de tráfego para mitigação em centros internacionais deverá ser justificado em relatório;     16. Nos períodos de ataque a latência do circuito deverá ser de no máximo 150 ms (milissegundos) quando a mitigação se originar dos centros de limpeza nacionais e de no máximo 250 ms (milissegundos) quando se originar do(s) centro(s) internacionais;     17. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;     18. A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da contratante para coleta dos dados a serem analisados;     19. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;     20. A solução 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 por um determinado cliente;     21. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP/HTTPS, DNS, VPN, FTP, NTP, UDP, ICMP, correio eletrônico, bloqueio por localização geográfica de endereços IP, dentre outras;     22. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4, incluindo, mas não se restringindo aos seguintes:     - Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;     - Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;     - Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;     - Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing).     1. Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de bordas da contratada;     2. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;     3. Realizar a comunicação da ocorrência do ataque à CONTRATANTE imediatamente após a detecção;     - A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;     - Outras configurações deverão ser possíveis, como exemplo monitoração de um cliente por sub-interface no PE;     1. A CONTRATADA deverá disponibilizar relatórios mensais de mitigação de ataques, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação, horário de sucesso da mitigação e horário de fim do ataque. Em conjunto com o relatório mensal relatórios dinâmicos deverão ser disponibilizados em até 48 horas após um ataque por solicitação da CONTRATANTE;     2. A CONTRATADA deverá apresentar relatório analítico, enviado mensalmente ao cliente;     3. A CONTRATADA terá no máximo 15 minutos para iniciar a mitigação de ataques de DoS e DDoS;     4. A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estar fornecendo serviço de limpeza contra ataques de DDoS (*Distributed Denial of Service*);     5. A interface digital a ser conectada no backbone do Sebrae em Rondônia deverá seguir o padrão Gigabit Ethernet;     6. Os serviços ofertados deverão operar no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);     7. O backbone IP do provedor deve ter saída com destino direto a outros provedores de backbone IP Nacionais de nível Tier 1, 2 e 3, com banda de 100 Gbps no mínimo no Total;     8. O Provedor deve estar conectado diretamente a no mínimo 02 PPT’s Nacionais (entende-se como PTT Pontos de troca de Tráfego).  INSTALAÇÃO, IMPLEMENTAÇÃO, SUPORTE TÉCNICO E MUDANÇA DE LINKS:  * + 1. **Da Instalação e Implementação:**   A Solução deve ser fornecida com os componentes necessários para sua completa instalação e o perfeito funcionamento da solução.   * + - 1. A CONTRATADA deverá disponibilizar os serviços para os links, no prazo de até 30 (trinta) dias corridos, contados da assinatura do contrato. * Em caso de necessidade de elaboração de projeto específico para viabilizar a infraestrutura necessária à prestação do serviço, o prazo de entrega do serviço poderá ser prorrogado por igual período mediante justificativa da contratada, a ser entregue antes de findar o prazo inicial.   1. **Do Suporte Técnico:**      1. O suporte técnico deverá ser prestado 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o período de vigência do contrato e o atendimento deverá ocorrer imediatamente após a abertura do chamado técnico, no qual deverá ser fornecido um número de registro de chamado técnico.   2. **Da Mudança de Links:**      1. Durante o período de vigência do contrato, caso haja mudança física e/ou de velocidade nas instalações do Sebrae em Rondônia, a Contratada deverá reinstalar e ativar os links;      2. As mudanças físicas e/ou de velocidade dos links cotados deverão ser solicitadas por escrito pela Contratante, num prazo mínimo de 30 (trinta) dias de antecedência;      3. A Contratada deverá se manifestar num prazo máximo de 10 (dez) dias, após recebimento do comunicado, através de relatório técnico da viabilidade ou não da mudança física e/ou de velocidade dos links. Caso a Contratada não se manifeste no prazo estipulado, serão consideradas como aceitas as mudanças solicitadas;      4. Caso a Contratada comprove no relatório técnico que não é possível fazer a mudança física dos links nas mesmas condições definidas neste Edital, a mesma deverá apresentar proposta para nova instalação;      5. A Contratada deverá comunicar por escrito, devidamente justificado, o aceite ou não da nova instalação física e/ou de velocidade dos links, bem como sua supressão ou não da fatura mensal;      6. Os roteadores instalados e configurados no Sebrae em Rondônia poderão ser substituídos por equipamentos fornecidos pelo mesmo, sendo o custo dos mesmos subtraídos da fatura mensal;      7. Quando da substituição dos equipamentos da Contratada, pelos fornecidos pelo Sebrae em Rondônia, a instalação e configuração dos mesmos deverão ser feitas obrigatoriamente em conjunto entre ambos, com emissão de relatórios assinado por ambas as partes de todas as configurações feitas.   3. **CARACTERÍSITICAS DOS SERVIÇOS – REDE SEBRAE EM RONDÔNIA:**      1. A Contratada deverá fornecer senha de acesso com direito a acesso (leitura) dos equipamentos, a fim de proporcionar ao Sebrae em Rondônia ferramentas de avaliação técnica dos mesmos, proporcionando adoção de ações preventivas ou corretivas;      2. Os equipamentos (roteadores), fornecidos pela Contratada deverão estar com SNMP, COMUNIDADE, RMON e TRAP habilitados para leitura, de sorte a proporcionar ao Sebrae em Rondônia ferramentas de avaliação técnica dos mesmos, proporcionando adoção de ações preventivas ou corretivas;      3. O Link Concentrador deverá ser entregue pela CONTRATADA em um único meio físico, sem fracionar (Mux, Modem Óptico ou outro equipamento);      4. Seguir o padrão DSCP (DiffServ Code Point), RFC 2474;      5. Possuir suporte à tradução de endereços IP (NAT);      6. Possuir suporte a classe de serviço para fragmentação de pacotes;      7. Possuir suporte a classe de serviço para reserva de banda;      8. Possuir suporte a classe de serviço para listas de controle de acesso;      9. A topologia da rede SEBRAE deverá ser full-mesh.  PADRÃO DE DESEMPENHO:  * 1. A CONTRATADA deverá assegurar os seguintes padrões de desempenho para o serviço:      1. Deverá ser garantida uma perda de pacotes fim a fim (*end-to-end*), que consiste na taxa de sucesso na transmissão de pacotes IP que entra (*incoming*) numa ponta, e sai (*outgoing*) em outra ponta da nuvem da CONTRATADA, deverá ser de no máximo 2%;      2. Deverá ser garantida disponibilidade, que consiste no percentual de tempo no qual a nuvem da CONTRATADA está operacional em um período de tempo, de no mínimo 99,35% no concentrador e 96% nós remotos;      3. Entende-se por disponibilidade, a liberação dos links de comunicações por parte da CONTRATADA, após instalação, configuração e constatação do perfeito funcionamento dos mesmos conectados à Rede Corporativa da SEBRAE e acesso à Internet;      4. Qualquer paralisação será considerada como indisponibilidade;      5. A CONTRATADA deverá fornecer relatórios gráficos diários, mensais e anuais do tipo *MRTG* para quaisquer das interfaces LAN e WAN dos equipamentos fornecidos, através de página Web, mostrando os níveis de desempenho e de utilização dos links (velocidade real da porta x tempo), valores médios, máximos, mínimos, etc., de sorte a proporcionar à Sebrae em Rondônia ferramentas de avaliação técnica para adoção de ações preventivas ou corretivas quando requeridas.   2. A CONTRATADA deverá disponibilizar aplicativo para acesso através de interface Web que permita obter no mínimo as seguintes informações:      1. Disponibilidade (%): Diário e Mensal;      2. Utilização em relação a velocidade do circuito (%): Diário e Mensal;      3. Tráfego (Kbps): Diário e Mensal;      4. Pacotes com erro de CRC (%): Diário e Mensal;      5. Pacotes descartados (%): Diário e Mensal;      6. Picos e médias de utilização e disponibilidade do dia (%);      7. Relatório de Latência (ms);      8. Relatório de Utilização de CPU (%) e Memória do CPE (%);      9. Relatório de Utilização e Falhas de Buffers do CPE (%);      10. Atualização das informações a cada 05 minutos;      11. Visibilidade da topologia, da disponibilidade da rede, da configuração e do inventário online;      12. Acessado via Internet pública e protocolo HTTPS;      13. Proatividade na identificação e tratamento de falhas;      14. Acompanhamento online dos chamados de falhas;      15. Proatividade quanto à disponibilidade, performance/desempenho e capacidade dos enlaces;      16. Possibilidade de envio de e-mail com informações sobre chamados técnicos referentes a interrupções;      17. Prazo de instalação da solução de gerenciamento é de 30 (trinta) dias após instalação do link e configuração dos parâmetros necessários;      18. Este serviço deverá estar disponível 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, com disponibilidade mínima de 99%.  INTERNET, VELOCIDADE E FIREWALL (LOTE 01):  * + 1. A interligação do Sebrae em Rondônia com a Internet deverá ser através de Link dedicado *ponto-a-ponto* e, a CONTRATADA deverá conceder junto com este link uma sub-rede com no mínimo 16 (dezesseis) endereços IP´s, válidos para acesso a Internet juntamente com o Roteador e Firewall, devidamente instalados e configurados;     2. Velocidades respectivas estão descritas no Anexo C;   1. **Características Gerais do Firewall**      1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN, não sendo permitido appliances virtuais ou solução open source (produto montado);      2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;      3. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;      4. As funcionalidades de segurança e SD-WAN que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, e suportem gerenciamento centralizado;      5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;      6. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada;      7. Deve permitir que novas assinaturas entrem em modo “hold”, de forma que mitigue possíveis problemas de falso-positivo;      8. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;      9. Os dispositivos de proteção de rede devem possuir suporte a Vlans;      10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);      11. Deve suportar BGP, OSPF, RIP e roteamento estático;      12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;      13. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;      14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;      15. Deve suportar NAT dinâmico (Many-to-Many);      16. Deve suportar NAT estático (1-to-1);      17. Deve suportar Tradução de porta (PAT);      18. Deve suportar NAT de Origem;      19. Deve suportar NAT de Destino;      20. Deve suportar NAT de Origem e NAT de Destino simultaneamente;      21. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;      22. Deve suportar NAT64;      23. Deve implementar o protocolo ECMP;      24. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;      25. Enviar log para sistemas de monitoração externos;      26. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;      27. Deve permitir criar regras de automação, definindo ações para eventos previamente determinados;      28. Dentre as possibilidades para iniciar regras de automação, deve suportar webhooks, IOCs, logs pré-definidos e agendamento;      29. Como ação para as regras de automação, deve suportar: execução de scripts, envio de e-mails, webhooks e execução de lambda/functions;      30. Deve possuir conectores para diversas nuvens públicas e privadas, tais como: AWS, Azure, GCP, Vmware ESXi, NSX, ACI e OpenStack;      31. Deve possuir conectores para Kubernetes e soluções de NAC, MDM/endpoint;      32. Deve suportar threat feeds, tais como: listas de hashes, Ips e nomes;      33. Proteção anti-spoofing;      34. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;      35. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;      36. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;      37. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo layer 3;      38. A configuração em alta disponibilidade deve sincronizar: sessões, configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;      39. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs e tabela FIB;      40. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;      41. Deve possuir suporte a criação de sistemas virtuais (VDOMs) no mesmo appliance;      42. 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;      43. Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound), devendo 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);      44. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;      45. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.   2. **Controle de Política de Firewall**      1. Deverá suportar controles por zonas de segurança;      2. Deverá suportar controles de políticas por porta e protocolo;      3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;      4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;      5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);      6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);      7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2;      8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;      9. Suporte a objetos e regras IPV6;      10. Suporte a objetos e regras multicast;      11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.   3. **Controle de Aplicações:**      1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;      2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;      3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;      4. 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;      5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;      6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;      7. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;      8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;      9. Identificar o uso de táticas evasivas via comunicações criptografadas;      10. Atualizar a base de assinaturas de aplicações automaticamente;      11. 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;      12. 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;      13. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;      14. 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;      15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;      16. Deve alertar o usuário quando uma aplicação for bloqueada;      17. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;      18. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;      19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;      20. Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para os mesmos;      21. 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);      22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;      23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.   4. **Prevenção de Ameaças:**      1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;      2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);      3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;      4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;      5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;      6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;      7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;      8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;      9. Deve permitir o bloqueio de vulnerabilidades;      10. Deve permitir o bloqueio de exploits conhecidos;      11. Deve incluir proteção contra ataques de negação de serviços; * Deverá possuir os seguintes mecanismos de inspeção de IPS: * Análise de padrões de estado de conexões; * Análise de decodificação de protocolo; * Análise para detecção de anomalias de protocolo; * Análise heurística; * IP Defragmentation; * Remontagem de pacotes de TCP; * Bloqueio de pacotes malformados.   + 1. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;     2. Detectar e bloquear a origem de portscans;     3. Bloquear ataques efetuados por worms conhecidos;     4. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;     5. Possuir assinaturas para bloqueio de ataques de buffer overflow;     6. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;     7. 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;     8. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;     9. Identificar e bloquear comunicação com botnets;     10. 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;     11. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;     12. Os eventos devem identificar o país de onde partiu a ameaça;     13. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;     14. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;     15. 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 diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.     16. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;     17. A solução de sandbox deve ser capaz de criar assinaturas e ainda inclui-las na base de antivírus do firewall, prevenindo a reincidência do ataque;     18. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (black list), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;     19. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;     20. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;   1. **Filtro de URLs:**      1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);      2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;      3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;      4. A identificação pela base do Active Directory deve permitir SSO, de forma que o usuários não precise logar novamente na rede para navegar pelo firewall;      5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;      6. Suportar proxy explícito;      7. Suportar a criação de limites diários de tempo e banda consumida por categoria;      8. Possuir pelo menos 60 categorias de URLs;      9. Deve possuir a função de exclusão de URLs do bloqueio;      10. Permitir a customização de página de bloqueio;   2. **Análise de Malwares Modernos**      1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;      2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;      3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;      4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;      5. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;      6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10 (32 bits) e (64 bits);      7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;      8. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;      9. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;      10. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);      11. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;      12. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;      13. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;      14. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;      15. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de *dia Zero* a partir da própria interface de gerência.      16. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 10 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;      17. Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;      18. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;      19. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class) e Android APKs no ambiente controlado;      20. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência mínima de 15 minutos      21. Permitir o envio de arquivos para análise no ambiente controlado via de forma automática via API.   3. **Identificação de usuários:**      1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;      2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;      3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;      4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;      5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;      6. 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);      7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;      8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;   4. **Filtro de dados:**      1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações;      2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;      3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;      4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.      5. Geolocalização:      6. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados;      7. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;   5. **VPN:**      1. Suportar VPN Site-to-Site e Cliente-To-Site;      2. Suportar IPSec VPN;      3. Suportar SSL VPN;      4. A VPN IPSEC deve suportar:      + 3DES;      + A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;      + A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;      + A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);      + A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);      + A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;      1. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Fortinet, SonicWall;      2. 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;      3. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;      4. 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;      5. Atribuição de DNS nos clientes remotos de VPN;      6. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;      7. Suportar autenticação via AD/LDAP, certificado e base de usuários local;      8. Suportar leitura e verificação de CRL (certificate revocation list);      9. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;      10. Deverá manter uma conexão segura com o portal durante a sessão;      11. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8/8.1 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.14 ou superior).      12. Deve suportar a autenticação e autorização de usuários para acesso VPN;      13. Acesso a VPN deve possuir Multi-Factor Authentication (MFA) ou Two-factor Authentication (2FA);   6. **SD-WAN**      1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;      2. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping ou http;      3. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;      4. A solução deve permitir a definição do roteamento para cada aplicação;      5. Deve permitir balanceamento de pacotes de uma mesma sessão;      6. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e todos os links abaixo do threshold definido (estatísticas dos links);      7. Deve possibilitar a definição do link de saída para uma aplicação específica;      8. Deve implementar balanceamento de link por hash do IP de origem;      9. Deve implementar balanceamento de link por hash do IP de origem e destino;      10. 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, quatro links;      11. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;      12. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;      13. Para IPv4, deve suportar roteamento estático e dinâmico (BGP);      14. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, 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 shaping. Dentre as tratativas possíveis, a solução deve contemplar:  1. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem; 2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino; 3. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo; 4. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações; 5. Suportar a criação de políticas de QoS e Traffic Shaping por porta; 6. QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio; 7. QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc; 8. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda; 9. QoS deve possibilitar a definição de fila de prioridade; 10. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas; 11. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço; 12. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas à todos os acessos que fizerem match na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que fizerem match na regra; 13. Deve possibilitar a definição de bandas distintas para download e upload; 14. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência); 15. A solução de SD-WAN deve suportar IPv6; 16. Deve suportar o recurso de duplicação de pacotes, para mitigar cenários onde todos os links apresentam perda moderada; 17. Deve suportar recurso que permite correções de erro na transmissão; 18. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls; 19. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall;     1. **SOLUÇÃO DE LOGS**        1. Possuir capacidade de receber ao menos 50 GB diários de logs;        2. A solução de gerenciamento deverá ser entregue como virtual appliance e deve ser compatível/homologado para Acropolis Hypervisor;        3. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;        4. Deve ser do mesmo fabricante dos firewalls ofertados;        5. Permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa; caso haja a necessidade de instalação de cliente para administração da solução, o mesmo deve ser compatível com sistemas operacionais Windows e Linux; o gerenciamento deve permitir/possuir:        6. Monitoração de logs; ferramentas de investigação de logs que permitam filtros diversos;        7. Deve permitir a criação de eventos customizados, baseados em logs, que permitam à solução realizar automações variadas;        8. Acesso concorrente de administradores;        9. Mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.        10. Possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;        11. Definição de perfis de acesso à console, com permissões granulares como: acesso de escrita e leitura;        12. Autenticação integrada ao Microsoft Active Directory e servidor Radius;        13. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);        14. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;        15. Prover relatórios sobre aplicações, ameaças (IPS, Antivírus e Anti-Spware) e URLs acessadas, para melhor diagnóstico e resposta a incidentes        16. Permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS e antivírus;        17. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;        18. Possuir mecanismo "Drill-Down" para navegação nos los. Nas opções de "Drill-Down", deve ser possível identificar o usuário que fez determinado acesso;        19. Permitir que os logs e relatórios sejam rotacionados automaticamente baseados no tempo em que estão armazenados na solução, assim como no espaço em disco usado;        20. Permitir fazer o envio de logs para soluções externas de forma granular;     2. **Deve permitir o monitoramento de:**        1. Situação do dispositivo/cluster;        2. Principais aplicações;        3. Principais aplicações por risco;        4. Administradores autenticados na gerência da plataforma de segurança;        5. Número de sessões simultâneas;        6. Uso de CPU;        7. Os seguintes relatórios/dashboards devem ser suportados:        8. Resumo gráfico de aplicações utilizadas;        9. Principais aplicações por utilização de banda;        10. Principais aplicações por taxa de transferência de bytes;        11. Visibilidade sobre eventos de IPS e antivírus;        12. Estatísticas de acesso de um usuário específico;        13. Estatísticas sobre a utilização da rede de forma geral;        14. Deve permitir a criação de relatórios personalizados;        15. Deve enviar os relatórios automaticamente para e-mails pré-definidos;        16. Deve possibilitar relatórios nos formatos PDF e HTML; |
| 1. **DO LOCAL DA PRESTAÇÃO DO SERVIÇO**    1. **Link Internet de 400 MB**       1. Sede do Sebrae em Rondônia, localizado na Av. Campos Sales nº 3421 - Bairro Olaria, Porto Velho – RO CEP: 76801-281.    2. **Link MPLS Concentrador de 350 MB**       1. Sede do Sebrae em Rondônia, localizado na Av. Campos Sales nº 3421 - Bairro Olaria, Porto Velho – RO CEP: 76801-281.    3. **Link de dados MPLS de 50 MB**       1. Unidade Regional de Ariquemes – Av. Tancredo Neves,1730 – Setor Industrial – Ariquemes – RO CEP: 76.872-870       2. Unidade Regional de Jaru - Rua João Batista, 3038 - Setor 1 - Jaru - RO CEP: 76.800-000       3. Unidade Regional de Ji-Paraná - Rua Raimundo Alves de Abreu e Silva, 742 – Ji-Paraná – RO CEP: 76.900-020       4. Unidade Regional de Cacoal – Av. Castelo Branco,17020 – Incra – Cacoal – RO CEP: 76.967-247       5. Unidade Regional de Pimenta Bueno - Rua Fagundes Varela, 361 – Centro – Pimenta Bueno – RO CEP: 76.870-970       6. Unidade Regional de Rolim de Moura – Avenida 25 de Agosto, nº 6172, Bairro Planalto - Rolim de Moura – RO CEP: 76.940-970       7. Unidade Regional de Vilhena - Rua Rony de Castro Pereira, 4061 – Vilhena – RO CEP: 76.980-000 |
| 1. **OUTRAS RESPONSABILIDADES E OBRIGAÇÕES ESPECÍFICAS DAS PARTES**    1. **COMPETE A CONTRATADA**        1. Observar todas as condições e requisitos constantes neste termo de referência, e ainda:       2. Notificar o Sebrae em Rondônia, por escrito, sobre quaisquer fatos que possam pôr em risco a execução do presente objeto;       3. Providenciar um canal de contato para que os serviços de manutenção sejam solicitados via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat;       4. Respeitar as normas e políticas de segurança do Sebrae em Rondônia;       5. Cumprir com os prazos estipulados neste termo de referência;       6. Fornecer ao Sebrae em Rondônia, as certidões negativas de regularidade fiscal, que deverão estar em seus prazos de validade e acompanhada de suas respectivas autenticações, que serão obtidas nos sítios que as emitiram;       7. Prestar os serviços ficando a seu encargo todas as despesas diretas e indiretas, mesmo as que porventura não tenham sido consideradas na carta proposta, que sejam decorrentes do cumprimento das obrigações assumidas, sem qualquer ônus ao Sebrae em Rondônia, observando sempre os critérios dos serviços a serem prestados;       8. Responder pelos danos causados diretamente ao Sebrae em Rondônia ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento do Sebrae em Rondônia;       9. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e, inclusive, às recomendações aceitas pela boa técnica, de forma meticulosa e constante, mantendo-se sempre em adequado padrão de qualidade;       10. Disponibilizar mão de obra especializada para realização dos serviços e responsabilizar-se por quaisquer acidentes que possam ser vítimas seus empregados e prepostos durante a prestação do serviço, devendo adotar as providencias que, a respeito, exigir a legislação em vigor;       11. Não subcontratar total ou parcialmente a realização do objeto deste termo de referência;       12. A CONTRATADA deverá efetuar a prestação do objeto deste Termo de Referência em conformidade com as concessões, autorizações e permissões que lhe forem outorgadas pela ANATEL;       13. Responder pelo cumprimento dos postulados legais vigentes de âmbito federal, estadual ou municipal, bem como, ainda, assegurar os direitos e cumprimentos de todas as obrigações estabelecidas por regulamentação da ANATEL, inclusive quanto aos preços praticados;       14. Será vedada à CONTRATADA, sob pena de rescisão contratual, caucionar ou utilizar o contrato a ser firmado entre as partes, para qualquer operação financeira, sem a prévia e expressa anuência do Sebrae em Rondônia;       15. Manter atendimento às solicitações do Sebrae em Rondônia durante 07 (sete) dias por semana, 24 (vinte e quatro) horas por dia, por meio de um Serviço de Atendimento ao Cliente (SAC) gratuito possibilitando a abertura de chamados de suporte e, inclusive, permitindo a emissão de faturas vencidas e/ou a vencer;       16. Disponibilizar, sempre que solicitado pelo Sebrae em Rondônia, em um prazo máximo de 05 dias úteis, informações sobre a utilização dos links (latência, perda de pacotes, disponibilidade, utilização e demais estatísticas de tráfego) dos últimos 30 dias antecessores a solicitação;       17. Ressarcir ao Sebrae em Rondônia eventuais custos decorrentes da necessidade deste recorrer a outras empresas, na eventualidade da licitante não conseguir disponibilizar o (s) equipamento(s) em perfeitas condições de funcionamento, nem substituí-los por outro, por sua exclusiva culpa;       18. Manter, durante todo o período de vigência do contrato a ser firmado entre as partes, um preposto que deverá tratar as solicitações do Sebrae em Rondônia além de representar a CONTRATADA junto a este. Este preposto deverá atender ao Sebrae em Rondônia sempre que o mesmo necessitar de atendimento de urgência, quando não conseguir atendimento e/ou quando não se sentir satisfeito com o atendimento prestado pelo canal disponibiliza contratada, conforme item 6.1.15 deste Termo de Referência;       19. Reconhecer somente o gestor do contrato, ou outros empregados que forem indicados formalmente pelo Sebrae em Rondônia, para realizar solicitações relativas a esta contratação, tais como mudanças de endereço, mudanças de configuração de equipamentos, e outras providências junto a CONTRATADA;       20. Disponibilizar ao Sebrae em Rondônia usuário e senha com permissão de leitura para acesso às configurações de roteadores (concentradores e roteadores nas localidades), para validação, verificação e solicitação de ajustes, se necessários.    2. **COMPETE AO SEBRAE EM RONDÔNIA**       1. Observar e fazer cumprir fielmente o que estabelece este termo de referência, em particular no que se refere aos níveis de serviço e sanções administrativas, se houverem;       2. Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham ser solicitados pelo preposto designado pela licitante;       3. Acompanhar a prestação dos serviços e execução do contrato por meio de empregado a ser designado como gestor do contrato;       4. Dirimir as dúvidas que surgirem no curso da prestação dos serviços por intermédio do gestor do contrato, que de tudo dará ciência ao Sebrae em Rondônia;       5. Efetuar o pagamento dos serviços de acordo com as condições contratuais; |
| 1. **NÍVEIS DE SERVIÇO E SANÇÕES ADMINISTRATIVAS**   **7.1 NÍVEIS DE SERVIÇOS – SLA**  7.1.1 A LICITANTE, ao participar deste pleito, estará automaticamente aceitando as condições de acordo de níveis de serviço (SLA) descritos a seguir:   * + - 1. Os serviços de acesso à Internet deverão possuir obrigatoriamente garantia mínima de 98,5% (noventa e nove por cento) da velocidade de banda estipulada neste instrumento, para download e upload;     1. A latência deverá ser de no máximo de 150ms;     2. Taxa de erros máxima admitida de 10-6;   **INDICADORES**  **INDICADOR 1: DISPONIBLIDADE DO LINK:**   |  |  | | --- | --- | | Descrição do Indicador | 1.1. Percentual de tempo, durante o período do mês de operação, em que o LINK (incluindo o CPE) venha a permanecer em condições normais de funcionamento;  1.2. O chamado somente deverá ser fechado/finalizado mediante autorização do Sebrae em Rondônia após testes de restabelecimento do LINK. | | Fórmula de  Cálculo | 1.1. IDM=[(To-Ti)/To]\*100;  1.2. Onde: IDM = índice de disponibilidade mensal do LINK em % (porcentagem);  1.3. To = período de operação (um mês) em minutos;  1.4. Ti = somatório dos tempos de inoperância durante o período de operação (um mês) em minutos;  1.5. No caso de inoperância reincidente num período inferior a 3 (três) horas, contado a partir do restabelecimento do link da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o link estiver totalmente operacional;  1.6. Os tempos de inoperância serão os tempos em que os links apresentarem problemas que serão obtidos dos chamados abertos no sistema de abertura de chamados técnicos (Trouble Ticket) e os tempos de indisponibilidade computados pela violação do indicador de Retardo;  1.7. Somente serão desconsiderados os tempos de inoperância, causados por manutenções programadas com o Sebrae em Rondônia, ressalvados, contudo, os casos fortuitos e de força maior. | | Periodicidade de Aferição | 1.1. Mensal. | | Limiar de  Qualidade | 1.1. Disponibilidade mensal mínima (em %) - 99,35%. | | Pontos de  Controle | 1.1. O FORNECEDOR REGISTRADO realizará, por meio da solução de gerenciamento, a coleta e o armazenamento de informações a respeito dos links estipulados neste instrumento pelo tempo de duração de prestação dos serviços. | | Relatórios de  Níveis de Serviço  (SLR) | 1.1. O FORNECEDOR REGISTRADO deverá disponibilizar mensalmente ao Sebrae em Rondônia, relatórios com os índices apurados diariamente, totalizados e apresentados mensalmente por link;  1.2. Para todos os links, inclusive para os que apresentarem operabilidade plena, deverão ser apresentados: o tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas e o tempo de interrupções de responsabilidade do **SEBRAE/RO**;  1.3. O FORNECEDOR REGISTRADO deverá disponibilizar relatório analítico com os tempos de falhas (com hora de início e fim da inoperância), minutos excedentes ao prazo máximo para reparo e disponibilidade no período (mês). | | Glosa de não  atendimento deste indicador | 1.1. 1% (um por cento) por percentual (%) de perda de pacotes acima do estipulado no limiar de qualidade. Calculado sobre o valor mensal do enlace no mês de referência. |   **INDICADOR 2: PERDA DE PACOTES:**   |  |  | | --- | --- | | Descrição do Indicador | 1.1. Representa a quantidade de pacotes perdidos. | | Periodicidade de  Aferição | 1.1. Mensal. | | Limiar de  Qualidade | 1.1. Menor ou igual a 2%. | | Relatórios de  Níveis de Serviço  (SLR) | 1.1. O FORNECEDOR REGISTRADO deverá disponibilizar, quando solicitado pelo **SEBRAE/RO**, relatórios com os valores das medições solicitadas referentes ao percentual de perda de pacotes. | | Glosa de não  atendimento deste  indicador | 1.1. 1% (um por cento) por percentual (%) de perda de pacotes acima do estipulado no limiar de qualidade. Calculado sobre o valor mensal do enlace no mês de referência. |   **INDICADOR 3: PRAZO DE REPARO/RESTABELECIMENTO DE UM LINK:**   |  |  | | --- | --- | | Descrição do Indicador | 1.1. Prazo limite para reparo/restabelecimento de um link ( com 100% de operabilidade ou pleno), na ocorrência de inoperância ou falha. | | Fórmula de  Cálculo | 1.1. Apuração do tempo de restabelecimento de um enlace, a partir de consulta na base de dados relativa à solução de gerenciamento do FORNECEDOR REGISTRADO e comparação com o valor descrito no limiar de qualidade deste indicador. | | Periodicidade de  Aferição | 1.1. Mensal. | | Limiar de  Qualidade | 1.1. 8 (oito) horas. Salvo em situações que tiverem necessidades específicas, sendo necessário a operadora apresentar as considerações de alongamento de prazo nestes casos. | | Pontos de  Controle | 1.1. Solicitações abertas na central de atendimento do FORNECEDOR REGISTRADO para reparo de um enlace. | | Relatórios de  Níveis de Serviço  (SLR) | 1.1. O FORNECEDOR REGISTRADO deverá disponibilizar mensalmente ao **SEBRAE/RO** relatório com os valores apurados, por link;  1.2. Os relatórios deverão fornecer, para cada unidade predial, os valores de tempo de atendimento gasto para reparo/restabelecimento do link com indicação das violações dos prazos e consolidação mensal por unidade regional. | | Glosa de não  atendimento deste  indicador | 1.1. 1% (um por cento) por hora acima do estipulado no limiar de qualidade. Calculado sobre o valor mensal do enlace no mês de referência para cada evento. |   **7.2 SANÇÕES ADMINISTRATIVAS**   * + 1. A CONTRATADA vencedora que, convocada dentro do prazo de validade da sua proposta, não assinar o contrato, deixar de entregar documentação exigida no Edital apresentar documentação falsa, não mantiver a proposta, fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal ficará impedida de licitar e de contratar com o Sistema SEBRAE, pelo prazo de até 02 (dois) anos, sem prejuízo das multas e demais cominações legais;     2. Os serviços deverão ser prestados de forma ininterrupta, com disponibilidade anual mínima em 99,35% (noventa e nove por cento e cinquenta e nove centésimos) do tempo contratado;     3. Na hipótese de ocorrência de interrupções, as falhas deverão ser corrigidas e o serviço restabelecido em no máximo 04 (quatro) horas;     4. Todas as ocorrências serão registradas pelo SEBRAE/RO, que notificará a CONTRATADA, atribuindo pontos para as ocorrências segundo a tabela abaixo:  |  |  | | --- | --- | | **Ocorrências** | **Pontos** | | Cobrança fora do prazo estabelecido | 0,3 | | Cobrança de valores em desacordo com o contrato | 0,3 | | Atraso na ativação dos serviços, para cada 10 dias contínuos de atraso. | 0,3 | | Alterações de características técnicas, para cada 5 dias contínuos fora das caraterísticas contratadas | 0,3 | | Atraso na prestação de informações e esclarecimentos solicitados pelo SEBRAE/RO, para cada 24 horas de atraso. | 0,3 | | Descumprimento das cláusulas especificadas no item 6.1 "Compete a CONTRATADA" | 0,3 |  * 1. A cada registro de ocorrência será apurado sempre o somatório da pontuação decorrente das ocorrências acumuladas no período de 12 (doze) meses anteriores ao fato gerador;   2. Esta pontuação servirá como base para que o SEBRAE/RO aplique as sanções administrativas a seguir, de modo que, atingindo o "quantum" necessário à configuração de uma sanção, esta será imediatamente aplicada, observando o processo administrativo:  |  |  | | --- | --- | | **Pontuação Acumulada** | **Sanção** | | 01 (um) ponto | Advertência | | 02 (dois) pontos | Advertência | | 03 (três) pontos | Multa correspondente a 2% do valor faturado do mês de aplicação dessa sanção | | 04 (quarto) pontos | Multa correspondente a 4% do valor faturado do mês de aplicação dessa sanção | | 05 (cinco) pontos | Multa correspondente a 6% do valor faturado do mês de aplicação dessa sanção | | 06 (seis) pontos | Multa correspondente a 8% do valor faturado do mês de aplicação dessa sanção | | 07 (sete) pontos | Multa correspondente a 10% do valor faturado do mês de aplicação dessa sanção | |
| 1. **DOTAÇÃO ORÇAMENTÁRIA:**    1. As despesas decorrentes deste contrato correrão por conta dos recursos orçamentários do SEBRAE/RO, estando classificados:   **Projeto/Atividade:** Gestão da Tecnologia da Informação  **Ação:** Administração da Infraestrutura e Segurança  **Natureza de despesa:** 03.15.07 - Serviço de Transmissão de Dados em rede  **Fonte de recurso:** CSO  **Unidade:** UTIC |
| 1. **FORMA DE PAGAMENTO:**     1. A CONTRATADA deverá emitir Nota Fiscal/Fatura, até o 15º (décimo quinto) dia útil subsequente do mês de execução dos serviços;    2. Pela prestação dos serviços, objeto do presente termo de referência, o SEBRAE/RO pagará o valor acordado a CONTRATADA, por meio de fatura mensal expedida pela empresa, no prazo de até 10 (dez) dias após a apresentação de fatura com detalhamento do objeto a que se refere e acompanhada do relatório Níveis de Serviço (SLR) mensal, definido no item 7.1;   Do valor contratual serão deduzidos os descontos previstos em Lei;   * 1. É condição para o recebimento dos créditos decorrentes da prestação dos serviços, a CONTRATADA apresentar juntamente com as notas fiscais as Certidões que comprovem sua regularidade fiscal relativa ao INSS, FGTS, Municipais, Estaduais, federais e Trabalhistas, acompanhadas de suas respectivas autenticações.  1. **DOS PRAZOS E CONDIÇÕES DE ENTREGA**    1. O FORNECEDOR REGISTRADO deverá iniciar a implantação dos links a partir da solicitação, conforme especificações técnicas deste Termo de Referência, proposta comercial, ata de registro de preços e demais condições estipuladas no edital e seus anexos;    2. Os links deverão ser implantados em até 60 (sessenta) dias, contados após a solicitação da contratante via Ordem de Serviço, podendo esse prazo ser prorrogado por igual período, mediante justificativa previa do FORNECEDOR REGISTRADO entregue ao **SEBRAE/RO** antes de findar o prazo inicial, e a critério do **SEBRAE/RO**;       1. Este prazo poderá ser prorrogado por igual período mediante justificativa entregue ao **SEBRAE/RO** antes de findar o prazo inicial.    3. O recebimento dos serviços ficará a cargo de servidores responsáveis pelo acompanhamento e fiscalização da execução do objeto de acordo com as especificações contidas neste Termo de Referência;    4. Os serviços deverão ser aceitos por meio da emissão e assinatura de termo de recebimento de serviço. 2. **DA QUALIFICAÇÃO TÉCNICA**   Para fins de aferimento da qualificação técnica das empresas interessadas em participar do certame, deverá ser apresentado pelas mesmas: Atestado(s) de Capacidade Técnica (declaração ou certidão) fornecidos por pessoa jurídica de direito público ou privado, comprovando o desempenho, características, quantidades e prazos com o objeto da licitação, conforme art. 12, II do Regulamento de Licitações e de Contratos do Sistema SEBRAE. Considerando:   1. Entende-se por pertinente e compatível **em quantidades:** Atestado que comprove que a empresa efetivamente prestou ou presta serviço de acesso à Internet nas especificações demandadas no edital desta licitação, cujo quantitativo de links, seja pelo menos 60% (sessenta) atingido na tecnologia proposta e com pelo menos 100% (Cem por cento) das velocidades. E os Circuitos MPLS/L2L interurbanos entregues em um único ponto Concentrador com distância geodésica entre os municípios de pelo menos 50 km, sejam de 100% da (Cem por cento) das velocidades, e que atenderam a quantidade total da solicitação do Edital, ou seja 07 pontos interligados a um único ponto concentrador. 2. Entende-se por pertinente e compatível **em prazos:** Atestado que comprove que a empresa prestou ou presta serviços com as especificações demandadas no Edital desta licitação, pelo período mínimo de 12 (Doze) meses; 3. Entende-se por pertinente e compatível **em características**: Atestado que demonstre em sua individualidade ou soma do serviço/fornecimento do objeto desta licitação, com serviço de acesso à Internet de acordo com as especificações do presente Edital.    1. O (s) atestado (s) de capacidade técnica apresentado(s) estará sujeito à confirmação de autenticidade, exatidão e veracidade conforme previsto no art. 15, do Regulamento de Licitações e de Contratos do Sistema SEBRAE, sujeitando o emissor às penalidades previstas em lei caso ateste informações inverídicas.    2. O atestado deverá indicar dados da entidade emissora (razão social, CNPJ, endereço, telefone, fax, data de emissão) e dos signatários do documento (nome, telefone, etc.). Além da descrição do objeto, quantidades e prazos de prestação dos serviços. 4. Apresentar Atestado que comprove que o backbone, tenha conectividade a sistemas autônomos através de canais próprios e dedicados. 5. Serviço de Segurança Centralizado (SOC – Security Operations Center) com Certificação ISSO 27001 para os serviços contratados de Mitigação de Ataques de negação de serviços DDoS. Comprovado através de Declaração emitida para a empresa. Deverá ser apresentada DECLARAÇÃO pela licitante com os seguintes dados da empresa: Nome, CNPJ, endereço;   **12. DISPOSIÇÕES GERAIS**  12.1 É vedada a subcontratação total ou parcial dos serviços, sem expressa anuência do Sebrae em Rondônia, assim como não serão admitidos consórcio, associações, cessões ou transferências, fusões, cisões ou incorporações, para a execução dos serviços relativos a esta contratação;  12.2 A CONTRATADA responderá ainda, civil e criminalmente, por danos causados a terceiros, consoante o que determina o artigo 186 e 187 do Novo Código Civil Brasileiro. |
| 1. **VIGÊNCIA**    1. O contrato gerado após a licitação, advindo deste termo de referência terá vigência por 24 (vinte e quatro) meses, contados a partir data de sua assinatura pelas partes, podendo ser prorrogado por sucessivos períodos com vista à obtenção de preços e condições mais vantajosas para o SEBRAE/RO, até o limite de 60 (sessenta) meses, de acordo com o REGULAMENTO LICITAÇÕES E DE CONTRATOS DO SISTEMA SEBRAE. |

ANEXO A

**DETALHAMENTO DOS EQUIPAMENTOS**

Os roteadores e equipamentos necessários para a conexão entre os pontos, deverão ser fornecidos pela empresa contratada, com as seguintes características mínimas, conforme abaixo relacionadas;

**LOTE 01**

* 1. **CPE Tipo 1 - FIREWALL UTM/NGFW (HA) Segurança de Perímetro Configurações mínimas:**
     1. Throughput de, no mínimo, 18 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
     2. Suporte a, no mínimo, 1,4 Milhões conexões simultâneas;
     3. Suporte a, no mínimo, 50.000 novas conexões por segundo;
     4. Throughput de, no mínimo, 11 Gbps de VPN IPSec;
     5. Estar licenciado para, ou suportar sem o uso de licença, 02 mil túneis de VPN IPSEC Site-to-Site simultâneos;
     6. Estar licenciado para, ou suportar sem o uso de licença, 02 mil túneis de clientes VPN IPSEC simultâneos;
     7. Throughput de, no mínimo, 01 Gbps de VPN SSL;
     8. Suporte a, no mínimo, 400 clientes de VPN SSL simultâneos;
     9. Suportar no mínimo 2.5 Gbps de throughput de IPS;
     10. Suportar no mínimo 01 Gbps de throughput de Inspeção SSL;
     11. Throughput de, no mínimo, 01 Gbps para funcionalidades de Proteção contra Ameaças;
     12. Possuir ao menos 8 interfaces 1Gbps;
     13. Possuir ao menos 8 Slots SFP Gigabit;
     14. Possuir ao menos 2 interfaces 10 GE SFP+ Slots;
     15. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por equipamento;
     16. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por equipamento.
     17. Os 02 (dois) appliances de segurança em alta disponibilidade, deverão suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais

**LOTE 02**

**2.1. CPE Tipo 1 - Serviço de Transmissão de dados de 350 Mbps - CONCENTRADOR MPLS configurações mínimas:**

1. O roteador deve possuir pelo menos duas interfaces SFP Full-Duplex;
2. Montável em rack, com espaçamento de 1U;
3. Suporte ao protocolo SNMP v2c e v3 para monitoramento do desempenho, incluindo as classes de serviço, e deverá configurá-lo com acesso somente leitura via comunidade, e traps;
4. Suportar DHCP de acordo com a RFC 2131;
5. Suportar NAT RFC1631 e VLAN IEEE802.1Q;
6. Gerenciamento via Telnet e Console, SNMP v1/v2/v3

**Energia**

* + 1. O equipamento deve operar nas tensões entre 100 e 240 VCA/60Hz, selecionáveis automaticamente.
    2. Deve vir acompanhado de todos os itens necessários para sua instalação elétrica e perfeito funcionamento, inclusive com

1. compatibilidade de tomadas com o Datacenter deste Órgão.
   * 1. Implementar de forma nativa mecanismo de monitoramento e detecção de falhas em suas fontes de alimentação individuais.

**Camada de enlace**

1. Permitir a criação de vlans, conforme especificação 802.1q.
2. Permitir a criação de links agregados e dinâmicos, conforme especificação 802.3ad06/10/2020
3. Permitir a inserção de registros estáticos na tabela de endereços da camada de enlace.

**Camada de rede**

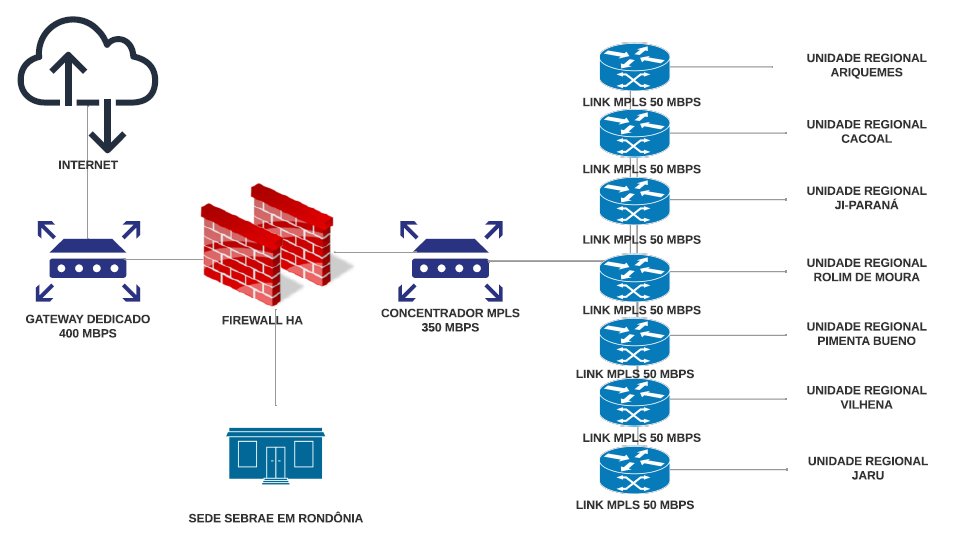
1. Deve possuir os protocolos WANs necessários a implementação do serviço contratado;
2. Deve possuir suporte aos protocolos LAN: IPv4, IPv6 e listas de acesso que possam ser construídas baseadas em:
3. Endereços IP de origem e destino;
4. Portas TCP e UDP de origem e destino;
5. Código e tipo de pacote ICMP (ICMP code e ICMP type);
6. Campo IP Precedence;
7. Protocolo IP;
8. Flags TCP;
9. IP Options;
10. Deve possuir os protocolos de roteamento: RIPv2, OSPF e BGP;
11. Multicast

**2.2. CPE Tipo 2 - Serviço de Transmissão de dados de 50 Mbps - Rede MPLS configurações mínimas:**

1. Os roteadores devem possuir pelo menos duas interfaces Ethernet 100/1000Base-T Full-Duplex superiores às velocidades que pontualmente atenderão;
2. Suporte ao protocolo SNMP v2c e v3 para monitoramento do desempenho, incluindo as classes de serviço, e deverá configurá-lo com acesso somente leitura via comunidade, e traps;
3. Suportar DHCP de acordo com a RFC 2131;
4. Suportar NAT RFC1631 e VLAN IEEE802.1Q;
5. Processamento CPU mínima de 1000MHz;
6. Performance mínima de 1.000.000 pps com pacotes de 64 bytes;
7. Memória mínima RAM de 256MB e memória Flash de 128MB;
8. Fonte de alimentação 110/220V
9. Gerenciamento via Telnet e Console, SNMP v1/v2/v3
10. Suportar o protocolo roteável IP, roteamento estático, OSPFv2 e BGPv4, MPLS.

ANEXO B

DIAGRAMA DA TOPOLOGIA DE REDE



ANEXO C

VELOCIDADE DOS LINKS (BANDA)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LOTE** | **N°** | **LOCAL** | **CIDADE** | **VELOCIDADE** |
| 01 | 1 | SEBRAE – Sede (Link Internet Dedicado) | Porto Velho | 400 Mbps |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LOTE** | **N°** | **LOCAL** | **CIDADE** | **VELOCIDADE** |
| 02 | 1 | SEBRAE – Sede (CONCENTRADOR) | Porto Velho | 350 Mbps |
| 2 | Unidade Regional de Ariquemes | Ariquemes | 50 Mbps |
| 3 | Unidade Regional de Jaru | Jaru | 50 Mbps |
| 4 | Unidade Regional de Ji-Paraná | Ji-Paraná | 50 Mbps |
| 5 | Unidade Regional de Cacoal | Cacoal | 50 Mbps |
| 6 | Unidade Regional de Pimenta Bueno | Pimenta Bueno | 50 Mbps |
| 7 | Unidade Regional de Rolim de Moura | Rolim de Moura | 50 Mbps |
| 8 | Unidade Regional de Vilhena | Vilhena | 50 Mbps |
|  |  |  |  |