



GOVERNO DO ESTADO DE MINAS GERAIS

Ata de Audiência Pública - Diretoria Central de Gestão de Serviços e Infraestrutura de TIC - Secretaria de Estado de Planejamento e Gestão

O Estado de Minas Gerais por meio da Diretoria Central de Gestão de Serviços e Infraestrutura de TIC, situada na Secretaria de Estado de Planejamento e Gestão, realizou a Audiência Pública para contratação de serviços de telecomunicações, necessários à operação, manutenção e gerenciamento de rede ip multisserviços abrangendo o estado de minas gerais e pontos nas cidades de São Paulo, Brasília e Rio de Janeiro, de serviços de valor adicionado, além de fornecimento de informações para a administração integrada do contrato, via Pregão Eletrônico, para atendimento pleno a todos os órgãos e entidades da Administração Pública Direta, Autárquica e Fundacional do Estado de Minas Gerais, no dia 25 de Março de 2024, recebendo as considerações até o dia 05 de Abril de 2024. Isto posto, segue as ponderações realizadas:

AMERICAN TOWER DO BRASIL – COMUNICAÇÃO E MULTIMÍDIA LTDA

1. O Anexo A – define as especificações técnica do lote 100 do Serviço de Virtualização de Comunicação de Dados (SD-WAN) e tem como requisitos técnicos básicos:

1. REQUISITOS TÉCNICOS BÁSICOS

Padrões e Topologia de Rede - A rede contratada deverá ser implementada conforme os padrões TCP/IP, devendo suportar o tráfego dos protocolos desenvolvidos segundo essa padronização. A solução pretendida é a disponibilização de acesso a comunicação de dados de forma que as Unidades de Governo possam se conectar ao ponto central, na UGO.

Será tratado como controladora o conjunto de equipamentos e soluções instalados on premise na UGO responsáveis por todas as ações necessárias para o correto funcionamento e conexão dos equipamentos CPE's instalados nas unidades dos clientes em conformidade com o solicitado neste termo de referência.

Não serão admitidas soluções concentradoras baseadas somente em tecnologia VPN (Virtual Private Network);

Os serviços de conectividade IP deverão estar completamente protegidos, tanto de redes públicas, como de outras VPN's e deverá seguir os padrões de segurança especificados no item 7.13 do Termo de Referência.

As redes locais das Unidades de Governo não poderão ser acessadas diretamente a partir da Internet. São considerados acessos provenientes da Internet somente aqueles que ingressam no equipamento CPE fora do túnel estabelecido entre o CPE e a controladora SD-WAN.

Acessos externos à unidade deverão obrigatoriamente ter origem dentro da rede corporativa do Estado. O tráfego dentro dos túneis da solução SD-WAN será considerado como pertencente à rede corporativa do Estado.

Não será permitido o uso dos IPs públicos relativos aos links para o provimento do serviço para acesso ao ambiente interno da unidade, para qualquer finalidade.

Todo o acesso a recursos externos à unidade será controlado pelos equipamentos CPE SD-WAN instalado na unidade. Para manter o controle da segurança da informação, não poderá ser instalado na unidade links de acesso à Internet que não estejam conectados ao CPE SD-WAN, pois este acesso seria um ponto de conexão sem controle do mundo externo e representaria um risco de entrada de malwares, ransomware e vazamento de dados na rede corporativa do Estado de Minas Gerais.

Plano de Endereçamento - O plano de endereçamento IP nas redes locais dos clientes deverá ser definido pela UGO.

CPEs – O fornecedor vencedor do lote 100 deverá prover os recursos necessários à interligação dos equipamentos que serão instalados na unidade dos clientes aos links de comunicação de dados disponibilizados pelo cliente, em suas unidades. A conectividade aos equipamentos das unidades locais será feita através de interfaces Ethernet padrão 10/100/1000 BaseTx, conector RJ45.

Deverão ser permitidos todos os tipos de acessos e protocolos necessários para o gerenciamento dos roteadores, gateways, CPEs e/ou servidores e estações de trabalho nas redes de clientes.

Suporte a gerenciamento - O equipamento de conexão disponibilizado pelo fornecedor deverá suportar, pelo menos, o protocolo SNMP-(V2 e V3), para gerenciamento remoto, monitoração e estatísticas de tráfego, entre outros. Neste equipamento deverá ser permitido à UGO a coleta de informações por meio de

Anexo A - Termo de Referência (83038906) SEI 1500.01.0079973/2024-83 / pg. 32

Entendemos que no lote 100 não será fornecida a conectividade, apenas o equipamento de SD-WAN.
Nosso entendimento está correto?

Resposta: [Sim, está correto o entendimento](#)

2. Embora seja permitida a subcontratação, sugerimos que as localidades abaixo que fazem parte do LOTE 70 sejam migradas para o LOTE 80.

ARAÇUAÍ
CAMPO BELO
CARANGOLA
FRUTAL
GUANHÃES
JANAÚBA
JANUÁRIA
MANHUMIRIM
NANUQUE
NOVA ERA
PEDRA AZUL

Nossa solicitação será atendida?

Resposta:

A mudança nos lotes não é interessante, pois atende a necessidade da ATC. Não temos como avaliar se a mudança solicitada irá acarretar uma mudança favorável ao Estado em relação à competitividade dos lotes. Como foi mantida a distribuição dos lotes que é utilizada atualmente, nosso entendimento é que as empresas que já pretendem participar e que vem se preparando para esta concorrência a algum tempo, podem ser prejudicadas na mudança de distribuição das cidades dentro dos lotes. Neste caso, a mudança pode ser prejudicial à competitividade dos lotes.

3. Em relação ao técnico residente, o item 3.2.2.2 do edital cita: “*Para todos os Lotes a Prestadora vencedora de cada lote deverá manter presencialmente na Prodemge, no horário compreendido entre 08:00h as 12:30h e 13:30h às 17:48h, nos dias úteis, 1 supervisor de operações com conhecimento em configuração de ativos de rede e monitoramento e solução de falhas de rede convergente. Este será responsável pela interação entre UGO e a Prestadora. Os técnicos que estiverem atuando fora das dependências da UGO, deverão dar suporte à rede por meio do uso de acesso remoto, utilizando infraestrutura de Virtual Private Network (VPN) da UGO. A exigência do técnico não é o definidor do tamanho da quantidade nem do conhecimento da equipe que a operadora deve manter em sua operação para o atendimento adequado dos incidentes e demandas relativas ao seu lote.*”

Considerando que a ATC tem um NOC em Belo Horizonte, solicitamos que seja avaliada a possibilidade deste supervisor ficar alocado no ambiente da Contratada. Desta forma haverá mais recursos na gestão da rede.

Resposta: Nossa experiência com diversos fornecedores, incluindo operadoras, demonstra que a falta de presença do técnico residente prejudica o tratamento das solicitações, principalmente quando se trata de incidentes. Com o técnico dedicado ao ambiente e residente na Prodemge, este terá maior vivência no projeto e poderá facilmente ser acionado pela equipe de suporte da Rede Governo, sendo o canal de comunicação entre a Prodemge e a operadora acelerando a tramitação das solicitações.

EMPRESA BRASILEIRA DE TELECOMUNICACOES S A EMBRATEL

1. Planilha de endereços e demandas por órgão: Importante termos uma planilha com a relação dos endereços para a cotação e que estes endereços estejam formatados de forma estruturada, como uma tabela contendo as seguintes colunas preenchidas e padronizadas: [Tipo do Logradouro], [Nome do Logradouro], [Número], [Bairro], [Município], [UF], [CEP], [Latitude em grau decimal], [Longitude em grau decimal] e demais informações referentes à [Lote], [Velocidade do link], [Tipo de Redundância] e demais informações pertinentes. Importante que esta planilha não tenha seu layout e formatação alterada em todo o processo e a entrada e saída de informações seja controlada em uma coluna

adicional, para termos agilidade na identificação das alterações e celeridade na nova precificação.

Resposta: A planilha em questão é somente como referência, os endereços ali inseridos são uma estimativa de contratação, podendo ou não serem efetivados, algumas linhas não possuem o endereço completo para instalação, nesses casos o fornecedor deverá se atentar que o órgão poderá solicitar o link em qualquer uma das cidades presentes no lote.

2. Para que a SEPLAG possa contratar uma solução fim-a-fim de SD-WAN, sugerimos a unificação dos lotes 90 e 100, dessa forma teremos um provedor responsável pela entrega da solução completa. O fracionamento em um lote de equipamento e outro lote de banda larga, poderá gerar sérios problemas de implantação e garantia da qualidade do serviço prestado. Na atual formatação, teremos uma elevada quantidade de fornecedores de banda larga (lote 90), conectados a um equipamento de outro fornecedor (lote 100). Dessa forma não há como garantir a identificação correta de pontos de falha, nem melhorias na qualidade do serviço. Um único provedor, responsável por toda a entrega, pode tratar de forma adequada da qualidade e melhorias, junto aos possíveis subcontratados.

Resposta:

Entendemos que a adoção do modelo proposto teria alguns benefícios, como os relatados, porém trariam perdas ao processo, sendo os principais:

Diminuição da concorrência em relação ao fornecimento da solução SD-WAN, o que pode acarretar aumento dos valores obtidos na prestação deste serviço;

Manutenção dos problemas relatados em relação à conectividade de circuitos, visto que está sendo previsto que poderão ser contratados circuitos de todos os lotes para a conectividade ao equipamento CPE SD-WAN.

3. Com relação serviço de virtualização do SD-WAN, seguem alguns questionamentos:
 - a. Com relação ao item "Ser composta por uma Console Central na UGO (on-premises), que será responsável por fazer toda a configuração dos appliances SD-WAN, incluindo priorização de tráfego, configurações de QoS, que deverão ocorrer de forma centralizada via software de gerência.", direciona para soluções que são baseadas em appliance, retirando da concorrência as baseadas em nuvem que são, geralmente, as que possuem maior atualização, evolução da tecnologia e operação mais robusta. Solicitamos a flexibilização para que soluções baseadas em nuvem possam ser implementadas.

Resposta:

A opção pela solução *on-premises* está justificada na página 33 do documento "Anexo-I-TR-Rede-IP-Multisservicos.pdf", publicado na página da audiência pública (<https://compras.mg.gov.br/licitacao/audiencia-publica-rede-ip-multisservicos/>)

- a. Com relação ao item "Deverá ser utilizado o link Internet disponibilizado pela Prodemge para que a concentradora receba as conexões advindas dos CPE's SD-WAN instalados nas unidades de Governo remotas." faz com que este link da PRODEMGE interfira no SLA final da solução. No caso da unificação dos lotes 90 e 100, esse item ficaria dispensado, ficando o SLA de responsabilidade unicamente do contratado para prestar o serviço do lote (90 +100).

Resposta:

O tráfego previsto para a comunicação dos CPE's à controladora é baixo em comparação à conectividade à Internet com alta capacidade de transmissão e alta disponibilidade utilizada pela Prodemge. Entendemos que o tráfego entre os CPE's e controladora não será ofensivo ao ambiente da Prodemge e não haverá necessidade de contratação de link de Internet exclusivo para esta comunicação. A solicitação de uma conectividade específica para esta comunicação seria um custo adicional ao projeto e aumentaria o valor final obtido na prestação do serviço.

- a. Mais um ponto que seria minimizado com a unificação: "Deverá ser ministrado treinamento oficial do fabricante de no mínimo 40 horas para 06 (seis) técnicos da UGO habilitando-os administração da solução, operação e configuração dos equipamentos CPE. Os detalhes do treinamento serão acordados com a UGO durante a fase do acordo operacional e deve ser ministrado antes do período da conclusão da fase de transição." Como teremos uma única empresa responsável pela solução, não

haveria necessidade de conhecimento especializado no CPE, ficando essa responsabilidade com a Contratada. Caberia à SEPLAG apenas a apuração do SLA.

Resposta:

O treinamento está previsto para a solução completa e não somente para a administração dos equipamentos do tipo CPE's. O treinamento é essencial para que a UGO possa fazer a gestão da segurança da comunicação das unidades que utilizarem a solução SD-WAN.

A questão de IPv6 poderia ser flexibilizada na solicitação do item "A solução deverá ser capaz de realizar NAT (Network Address Translation), a exemplo de NAT64, NAT46, NAT1:1, NAT dinâmico e eventuais outras categorias de tradução de endereços, de forma a garantir o perfeito funcionamento e a integração da Rede IP, no que diz respeito à implementação tanto protocolo IPv4 quanto protocolo IPv6;"

Resposta:

A utilização do protocolo IPV6 se faz necessário devido ao esgotamento de endereçamento do protocolo IPV4 e estamos em implantação deste protocolo na rede corporativa do Estado de Minas Gerais. Desta forma, não podemos abrir mão do uso do protocolo IPV6, porém não ficou claro no item se a flexibilização deveria ser somente em relação a capacidade de realizar no NAT nas formas solicitadas.

Com relação ao item "Deverão suportar vários links de acesso, suportando pelo menos os links previstos nos lotes informados neste termo de referência." deve ser informado na Planilha de endereços e Demanda a quantidade de links previstos por cada site.

Resposta:

A planilha em questão é somente como referência, os endereços ali inseridos são uma estimativa de contratação, podendo ou não serem efetivados, algumas linhas não possuem o endereço completo para instalação, nesses casos o fornecedor deverá se atentar que o órgão poderá solicitar o link em qualquer uma das cidades presentes no lote.

Com relação ao item "Deverá implementar OSPF; Deverá implementar BGP;" avaliar se pode ser apenas BGP.

Resposta:

Utilizamos o protocolo OSPF em nosso ambiente de rede corporativa, não sendo possível retirar a exigência deste protocolo.

Com relação aos itens seguintes sugiro que sejam revistos pois, em geral, os fornecedores de solução de SDWAN não disponibilizam esta granularidade de interfaces tipo WAN em seus dispositivos. Seguem itens:

Os equipamentos modelos 1, 2, 3, 4 e 5 deverão possuir pelo menos 4 conexões/interfaces de rede que poderão ser utilizadas por links banda larga, MPLS, satélite ou rádio e comunicação 4G ou superior. Os equipamentos modelos 6, 7, 8, 9, 10 e 11, deverão possuir pelo menos 8 conexões/interfaces de rede que poderão ser utilizadas por links banda larga, MPLS, satélite ou rádio e comunicação de dados 4G ou superior.

Resposta:

Sugestão será avaliada conforme necessidade dos órgãos. Sugestão é diminuir a quantidade de portas dos modelos superiores para 6 portas.

Com relação ao item "1.5.1.4.8. Suportar H.323." peço avaliar pois H.323 é uma tecnologia que vem ficando em desuso e substituído por SIP.

Resposta:

Embora haja uma tendência pela substituição do protocolo H.323 ele ainda é utilizado. Como os órgãos possuem soluções diversas, algumas já adquirida a alguns anos, não podemos descartar o uso deste protocolo no momento.

Com relação ao item "1.5.1.4.10. Suportar IPv6." peço avaliar a possibilidade de flexibilizar.

Resposta:

O protocolo IPV6 já se encontra no mercado a muitos anos. O Estado está em fase de implantação do protocolo IPV6 em suas unidades e não podemos descartar esta tecnologia no momento, principalmente para um contrato para um período de 60 meses.

O item "1.5.1.5. Função IPS dos equipamentos CPE" direciona para a necessidade de uso de UTM. Essa solicitação cria uma complexidade adicional que encarece a solução. Verificar a possibilidade de exclusão do item.

Resposta:

Revisaremos esta solicitação, porém poderá ser mantida a depender das manifestações de outros fornecedores a respeito deste item.

Alguns pontos adicionais importantes:

Solicitar a apresentação de atestados de qualificação técnica como um item adicional do tópico 11. QUALIFICAÇÃO TÉCNICA. Essa medida garantirá a contratação de fornecedores adequados às necessidades de qualidade e criticidade de atendimento ao Governo de Minas. A não exigência de atestados poderá acarretar a participação de empresas sem as devidas credenciais de qualidade que o atendimento requer. Essa exigência permitirá o conhecimento do fornecedor e a avaliação de sua competência, antes de se efetivar a contratação.

Resposta:

Sugestão será avaliada

- Conforme o item 10.1.7. *Por tais razões, considerando ser a parte menor e de pouca relevância frente ao valor total do certame, a subcontratação somente será admitida para serviços de conexão de última milha.* Entendemos que a subcontratação de última milha é medida que garante o atendimento a pontos específicos, onde o investimento necessário ao atendimento o tornaria inviável. No entanto, a subcontratação indiscriminada da última milha, acarreta uma perda de qualidade na prestação do serviço, dada a possibilidade de inúmeros fornecedores, muitas vezes despreparados. Sugerimos que seja especificado um percentual mínimo de acessos próprios da contratada nos lotes MPLS, para que a qualidade requerida seja alcançada.

Resposta:

Não será atendida a solicitação, tendo em vista que o trecho para atendimento do terceiro é somente de última milha, sendo a operadora vencedora responsável pelo maior trecho do circuito, limitar a subcontratação poderá impactar no atendimento dos órgãos/entidades espalhados nos diversos municípios do Estado.

Sugerimos a retirada do ANEXO E. O Projeto da Rede IP Multisserviços é extremamente complexo, envolvendo serviços customizados para o governo de Minas, que são muito diferentes dos prestados a outros clientes. A utilização das métricas propostas pode não ser adequada para a apuração de um reequilíbrio financeiro.

Resposta: Será avaliado.

- Entendemos que a medida proposta no item 3.2.4 poderá trazer sérios problemas na prestação do serviço. Entendemos que essa medida deveria ser adotada apenas em casos de extrema criticidade. As medidas de apuração de acessos e configurações indevidas ficariam mitigadas, ficando somente a contratada responsável pela execução de gravação nos CPE's.

As Prestadoras se obrigam a fornecer exclusivamente à UGO, imediatamente após a emissão do aceite técnico de cada Ponto de Acesso, as senhas que permitam a execução de leitura e gravação (Read/Write) de todos os CPEs (switches, switches applications, routers, balanceadores de tráfego, controladores de QoS da Rede) e demais equipamentos e software que estejam instalados nas

dependências da UGO e das Unidades de Governo. A recusa ou postergação do cumprimento desta obrigação, além de sujeitar a Prestadora às penalidades contratuais dará direito à CONTRATANTE de considerar o Ponto de Acesso, cujas senhas não foram fornecidas, como inoperante.

Resposta:

Esta é uma premissa necessária para que a UGO possa fazer a supervisão técnica do serviço prestado. Este item se fez presente em todas as edições do projeto da Rede IP Multisserviços e nunca foi motivo de problema.

- O item 4.1.1 nos traz a seguinte especificação: *Perfil I – Aplicável aos Lotes 20 a 80, exigindo redes com conexões dedicadas (meios de transmissão cabeados, satélite ou via rádio digital), não sendo admitida solução xDSL. Este Perfil abrange acessos nas áreas urbanas e rurais dos municípios. As características técnicas deste Perfil estão descritas neste Termo de Referência.*

Entendemos que, pela característica desses lotes, o atendimento deveria ficar restrito às áreas urbanas. A solicitação, por parte de um cliente, de um atendimento em um dos lotes citados, em zona rural, poderia trazer um desequilíbrio financeiro ao contrato, tendo em vista o nível típico de investimento necessário para esse tipo de atendimento. Entendemos que o atendimento pelos lotes 90 a 120 cumprem essa finalidade e possuem uma maior flexibilidade para atendimento.

Resposta:

Os lotes 90 a 120 não apresentam os mesmos padrões de qualidade exigidos para os lotes 20 a 80 e em alguns casos não atendem às necessidades dos órgãos participantes do projeto, mesmo a unidade se encontre em zona rural. Já existe previsão de diferenciação de custos entre os links entregues em zona Urbana e Zona Rural e desta forma entendemos que a previsão de entrega dos circuitos em zona rural não irá gerar desequilíbrio financeiro para o contrato.

- Na planilha enviada, com os endereços previstos, aparecem indicações de lotes 10, 11 e 22. Creio ser apenas uma questão de adequação aos números dos lotes previstos no termo de referência.

Resposta:

A numeração será corrigida.

- A partir dos dados extraídos da planilha de locais de atendimento, entendemos que já é premissa de projeto que os sites atendidos por SD-WAN utilizarão sempre mais de um meio de acesso, tendo em vista a quantidade de equipamentos previstos (652) e de acessos solicitados (2.682). Estamos corretos?

LOTE 100	LOTE 110	LOTE 120	LOTE 90
652	796	261	1625
652	796	261	1625

Resposta: Não está correto o entendimento, o cliente poderá utilizar somente uma conexão no equipamento SDWAN, a depender das suas características de utilização.

SEMPRE TELECOMUNICAÇÕES LTDA

Qual o MTU será trabalhado nos lotes?

Resposta: 1500

Onde está as informações do lote 10? Fará parte do edital?

Resposta: O lote 10 teve sua numeração alterada para 20 porém observamos posteriormente à publicação que ainda permaneceu a referência ao lote 10 Termo de Referência. A informação será corrigida na versão final do documento

Onde está as informações de localidade do lote 25?

Resposta: A numeração será corrigida o lote 25 é referente a Brasília

Onde está as informações de localidade do lote 26?

Resposta: A numeração será corrigida o lote 25 é referente ao município do Rio de Janeiro

Onde está as informações de localidade do lote 27?

Resposta: A numeração será corrigida o lote 25 é referente ao município de São Paulo

Poderá ser usado para aferir e validar os links os certificadores de RFC 2544 e ITU Y.1564?

Resposta: Na entrega dos links deve ser enviado o TERMO DE ACEITE TÉCNICO. Para a geração deste termo é necessário apresentar algumas informações que comprovem a qualidade do link entregue. Dentre as informações estão o gráfico comprovando que o link suporta a banda contratada e outras informações relativas a qualidade do link, como latência e perda de pacotes. Os detalhes deste relatório são discutidos no acordo operacional

Em relação ao SD-WAN deverá suportar exportação de registros Flow e/ou IPFIX?

Resposta: Este item será revisado. O que será solicitado é que a solução deverá ser capaz de gerar informações relativas a fluxo de tráfego para análise

O colaborador presente na Prodemge poderá através de VPN acessar o ambiente da Prestadora?

Resposta: Sim

O colaborador presente na Prodemge poderá acessar plataforma de vídeo conferência da Prestadora?

Resposta: Sim

Será disponibilizado Infra Estrutura para o colaborador dentro da Prodemge (Mesas, cadeiras, elétrica redundante e etc)?

Resposta: Sim

Em relação ao SD-WAN, o que será exigido como requisitos a serem entregues de funcionalidade (Políticas de segurança, serviços entregues e integrações entre sistemas)?

Resposta: As políticas de segurança serão definidas pela Prodemge e os órgãos.

Qual o critério para divisão do lotes, existe a possibilidade de redefini-los?

Resposta: Foi avaliado que a manutenção da divisão de lotes do contrato atual seria o melhor cenário para o momento. Não foi identificada uma alteração nos lotes que trouxesse benefícios técnicos e financeiros para o Estado, desta forma, não existe previsão de redefinição para os mesmos

ALTAS NETWORKS & TELECOM LTDA

1 – Sugestão de item para esclarecimento

Pag 33 – Tabela 1

Para o dimensionamento dos firewalls, sugerimos que o número de Threat Protection (controle de aplicação, IPS e antivírus) seja o balizador. Ex: o modelo 1 deve atingir 300 Mbps com os recursos de Threat Protection habilitados, simultaneamente.

Justificativa: a performance do equipamento varia muito em função dos recursos em uso. Sem um baseline concreto, cada proponente usará prerrogativas distintas e, conseqüentemente, custos muito variados. E, na ocasião de um fornecedor considerar recursos de firewalls apenas (camada 4, throughput elevado) e o cliente da PRODEMGE habilitar camada 7, o firewall não suportará, gerando paradas no serviço.

Resposta: Os fabricantes utilizam métricas diferentes para o dimensionamento dos equipamentos o que dificulta uma base de comparação adequada entre os modelos ofertados. Ao invés disto, optamos por dimensionar o equipamento pela capacidade de consumo de sua CPU durante o funcionamento do equipamento no ambiente de produção, durante todo o período do contrato. Desta forma, resguardamos o Estado do oferecimento de equipamentos com capacidade aquém do solicitado e damos maior autonomia para o fornecedor dimensionar os recursos dos equipamentos que serão disponibilizados com base em seu expertise em relação ao comportamento dos equipamentos em ambiente de tráfego real.

2 – Alteração

Pág 33

Deverá monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente em intervalos mínimos de 500 milissegundos.

Justificativa: 5 segundos, para monitoramento e eventual posterior chaveamento de link, é um tempo muito alto. Principalmente para aplicações multimídia. Se o intervalo de medição é longo, a troca para um melhor link também será.

Resposta: A alteração solicitada poderá restringir a quantidade de equipamentos e fornecedores aptos a participar do certame. Em nossa análise de custo/benefício, foi avaliado que o benefício que a redução do intervalo de monitoramento traria em relação à quantidade de vezes em que esta seria benéfica em relação ao intervalo de 5 segundos solicitado, não justificaria o aumento de custos ao projeto que ela iria acarretar

3 – Alteração

Pág 34

O equipamento CPE das unidades remotas deverá ter recurso para se recuperar automaticamente de uma atualização de software ou configuração mal sucedida. Deverá ter um controle, que, caso ele fique inoperante ou sem gerência, retorne à configuração anterior em um prazo máximo de 5 minutos ou após reboot automático, reestabelecendo a comunicação da unidade.

Justificativa: O FortiGate não realiza rollback por atualização de firmware mal sucedida, mas sim de configuração errada que causou perda da gerência.

Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada

4 – Alteração

Pág 35

A solução deve suportar a marcação DSCP dos pacotes, inclusive nos CPE'S, de acordo com a aplicação (camada 7) e as políticas configuradas para que a UGO dê o tratamento adequado aos pacotes.

Justificativa: deixar claro que a intenção é marcar DSCP de acordo com a aplicação (camada 7). Ex: YouTube, Facebook, Salesforce etc.

Resposta: A marcação dos pacotes na camada 7 é opcional para nosso projeto. O objetivo principal é poder fazer marcação de pacotes de camadas inferiores, conseguindo priorizar pacotes de voz, vídeo, web, entre outros.

5 – Alteração

Pág 35

Nas unidades remotas, em caso de indisponibilidade dos equipamentos da controladora do serviço SDWAN, a solução deverá manter sob o controle das últimas políticas de segurança aplicadas no equipamento remoto, todo e qualquer tráfego destinado ou proveniente da Internet. A falha da unidade controladora do serviço de SD-WAN não deverá deixar indisponível a comunicação direta com a internet

na unidade remota nem inibir que os elementos remotos sejam configurados diretamente.

Justificativa: a queda da controladora não pode gerar indisponibilidade do serviço, nem inviabilizar que o firewall remoto seja configurado, acessando sua console diretamente. O firewall deve possuir funcionamento totalmente independente, mesmo sem gerência centralizada operacional.

[Resposta: Nosso objetivo é que as alterações possam ser feitas somente a partir da controladora, desta forma, não vemos necessidade de incluir o texto referenciado.](#)

6 – Alteração

Pág 36

Deverá implementar a função DHCP Relay Agent e DHCP Server para múltiplas VLANs. Em Ipv4 e Ipv6.

Justificativa: por se tratar de um backbone, é importante que os elementos suportem Ipv6, garantindo interoperabilidade futura.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

7 – Alteração

Pág 37

O sistema de gerenciamento deverá informar a utilização de Inbound e Outbound de cada circuito de comunicação. Esta capacidade deverá cobrir todos os circuitos contratados e manter a informação de utilização dos circuitos por pelo menos 1 ano.

Justificativa: a Fortinet não faz referência da banda utilizada com banda contratada. Porém, tendo em mente essa informação, fica simples calcular manualmente o % de banda ocupada.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

8 – Alteração

Pág 39

Suportar no mínimo 128 VLANS

Justificativa: equipamentos de menor porte geralmente não suportam 512 VLANs. O FortiGate 40F suporta 128 VLANs no máximo;

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

9 – Alteração

Pág 39

Suportar os esquemas de autenticação de usuários tanto para Firewall quanto para VPN's como token's (exemplo SecureID), TACACS ou TACACS+ (gerência), RADIUS, senha do próprio Firewall, diretório LDAP e Microsoft Active Directory.

Justificativa: TACACS/TACACS+ são usados para acesso de gerência apenas.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

10 – Alteração

Pág 40

O IPS deve incluir a habilidade de interromper temporariamente as proteções para fins de troubleshooting ou, pelo menos, suportar que o profile de IPS possa ser configurado em modo monitor.

Justificativa: no FortiGate, a forma de “desabilitar os bloqueios” é mudando a ação do profile de IPS de block para monitor (apenas log).

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

11 – Retirar trecho

Pág 40

O administrador deve ser capaz de ativar novas proteções baseado em parâmetros configuráveis (severidade da ameaça, proteção dos clientes, proteção dos servidores).

Justificativa: O FortiGate não possui como parâmetro em suas assinaturas de IPS o “impacto na performance”.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

12 – Alteração

Pág 40

Para cada assinatura, ou para todas as assinaturas de IPS, deve incluir a opção de adicionar exceções baseadas na origem e destino

Justificativa: “proteção” é muito vago, dando margem para variadas interpretações.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

11 – Alteração

Pág 40

A solução deve fazer captura de pacotes para assinaturas de IPS específicas

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

12 – Retirar trecho

Pág 40

Deve incluir a habilidade de detectar e bloquear ataques conhecidos e desconhecidos, protegendo de, pelo menos, os seguintes ataques conhecidos: IP Spoofing, Ping of death, ICMP Flooding, Port Scanning, SQL Injection, Cross-site scripting, ataques de força bruta e man-in-the-middle.

Justificativa: O FortiGate não suporta força bruta a IKE e man-in-the-middle para VPN. Porém, de forma geral, ele suporta esses métodos de ataque para outras situações.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

12 – Retirar trecho

Pág41

A solução deve ser capaz de inspecionar/filtrar portas conhecidas (como http 80 e https 443) a fim de buscar aplicações que possam comprometer a segurança, como P2P (KaZaa, Gnutella, BitTorrent) e IMs (ICQ), mesmo quando elas pareçam ser tráfego válido.

Justificativa: Morpheus, Yahoo! E MSN são aplicações legadas/descontinuadas. O FortiGate não as possui mais em sua base. Havendo necessidade, elas podem ser criadas manualmente.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

13 – Retirar trecho

Pág41

Reconhecer aplicações de tráfego relacionado, no mínimo, 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, e os softwares bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, anydesk, ultraviewer, ms-rdp, vnc, gmail, youtube, httpproxy, httptunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, googledocs, dentre outras.

Justificativa: O FortiGate não possui a assinatura do Skydrive em sua base. Havendo necessidade, elas podem ser criadas manualmente.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

14 – Alteração

Pág 41

Deve possibilitar permitir ou bloquear aplicações ou páginas da Internet por:

Categorias ou sub-categorias;

Justificativa: o web filter do FortiGate não usa sub-categorias.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

15 – Alteração/Retirar trecho

Pág43

A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, usando posição no payload dos pacotes TCP e UDP para a criação de assinaturas, minimamente, dos protocolos: HTTP,

HTTPS, FTP, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC/DCE-RPC e RTSP.

Justificativa: o FortiGate não suporta assinatura customizada com SMB e, para RPC, a documentação menciona "DCE-RPC".

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

16 – Retirar trecho

Pág43

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

Justificativa: O FortiGate não possui a assinatura do neonet em sua base. Havendo necessidade, elas podem ser criadas manualmente.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

17 – Alteração

Pág43

Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Google Meet e bloquear a transferência de arquivos ou postagem de mensagens.

Justificativa: não há assinatura para transferência de arquivos no google meet, mas sim postagem de mensagens.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

18 – Retirar trecho

Pág43

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

O FortiGate não possui a assinatura do Ghostsurf em sua base. Havendo necessidade, elas podem ser criadas manualmente.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

19 – Alteração

Pág44

A solução deve suportar diferentes perfis de administração, disponibilizando, pelo menos, os seguintes: read/write, read only, gerenciamento de usuários/configurações de sistema e visualização de logs.

Justificativa: o FortiManager não possui permissão específica para gerenciamento de usuários. Ela está dentro de "configurações de sistema"

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

20 – Alteração

Pág44

A solução deve incluir a capacidade de confiar em CAs externas ilimitadas com a opção de verificar o certificado de cada gateway externo ou deve, pelo menos, criptografar a conexão com os gateways gerenciados.

Justificativa: o FortiManager não checa o certificado dos gateways gerenciados. Mas criptografa a conexão com os mesmos utilizando método próprio.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

21 – Alteração

Pág44

A solução deve possuir a opção de segmentar as regras de segurança através de rótulos ou sessões, com a finalidade de organizar as políticas.

Justificativa: o FortiManager faz a organização das políticas por meio de sessões.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

22 – Alteração

Na consulta às logs deve ser possível a filtragem de eventos baseado em diversas categorias (IP origem, porta origem, IP destino, porta destino, interface, categoria ou nome do ataque, translated IP, translated port, entre outras) simultaneamente e possibilitar a filtragem de eventos relacionados a ação do administrador, tais como login/logout e alterações de política.

Justificativa: o FortiManager permite o filtro pelo nome do ataque.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

23 – Retirar trecho

A solução deve permitir ao administrador o agrupamento de eventos baseado em qualquer uma das opções de filtragem.

Justificativa: o FortiManager não realiza a filtragem em distintos níveis de alinhamento.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

24 – Alteração

A solução deve prover mecanismo de visualização de eventos de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações: funções de segurança mais utilizadas ou painel consolidando o uso de tais recursos, origem mais utilizada, destino mais utilizado, regras mais utilizadas e usuários com maior atividade.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

25 – Alteração

Pág45

A ferramenta de relatórios deve fornecer relatórios consolidados das logs dos CPEs. Caso não possua alguma informação em relatório padrão, deve permitir a customização do mesmo, inserindo não apenas o que se pede abaixo, mas também outras estatísticas úteis:

Justificativa: o FortiManager, para algumas informações solicitadas, não possui em relatório default. Porém, elas existem na base, permitindo ao administrador alterar/criar relatórios que as incluam.

[Resposta: Iremos avaliar a possibilidade de efetuar a alteração indicada](#)

Novos itens que pedimos que sejam acrescentados:

CPE

1-Deve permitir e estar licenciado para a criação de VRF, em Ipv4 e Ipv6, permitindo a criação de múltiplas tabelas de roteamento no mesmo equipamento.

Justificativa: a PRODEMGE já utiliza VRF no backbone, sendo interessante, portanto, estender o uso desse recurso até o CPE.

[Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência](#)

2-Deve permitir a segmentação de tráfego em um único overlay do SD-WAN. Ou seja, separar em diferentes VRFs tráfegos que usam o mesmo túnel SD-WAN.

Justificativa: a PRODEMGE já usa VRF no backbone. Com esse recurso, é possível manter a separação de tráfego inclusive ao usar SD-WAN, mas sem a necessidade de contratar mais links e/ou dedicar links para tráfegos específicos.

[Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência](#)

3-A solução deve ser capaz de mensurar o MOS (Mean Opinion Score) ao rotear tráfego de voz e, também, permitir a definição de um MOS mínimo para utilizar um link.

Justificativa: o uso de telefonia IP tornou-se um padrão. É importante que o backbone seja capaz de mensurar a experiência do usuário ao usar serviços de voz, bem como alterar automaticamente o roteamento quando ela não estiver satisfatória.

[Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência](#)

4-A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check,

permitindo testes de resposta por ping, http, tcp/udp, echo, dns, tcp-connect e twamp. Bem como permitir health checks passivos, utilizando o tráfego real para medição das estatísticas.

Justificativa: o texto não especifica os métodos de health checks. É importante que o faça, visto que cada aplicação demanda protocolos específicos para o teste. Ex: tráfego web deve usar probe HTTP e telefonia, por sua vez, geralmente usa twamp.

[Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência](#)

5-A solução deve suportar VPNs dinâmicas junto ao SD-WAN de forma que túneis subam automaticamente entre pontas remotas, encurtando o caminho e melhorando a experiência do usuário. E o SD-WAN deve ser capaz de monitorar a qualidade dos túneis dinâmicos.

Justificativa: caso uma secretaria possua vários sites usando sd-wan, com esse recurso, tornase possível criar uma rede full mesh dinâmica (similar ao MPLS), estabelecendo VPNs automaticamente mediante tráfego entre pontas remotas, bypassando o hub e, assim, provendo melhor serviço aos usuários finais.

[Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência](#)

6-A solução de firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, hashes de malwares e domínios

Justificativa; com esse recurso, é possível criar listas centralizadas (páginas em web server local ou na Internet), para que os firewalls as leia e, automaticamente, atualize seus objetos, liberando facilmente novos IPs/sites ou bloqueando IPs maliciosos.

[Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência](#)

7-Os CPEs devem estar homologados na ANATEL na data do certame.

Justificativa: questões legais.

[Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência](#)

8-Os CPEs devem suportar e estar licenciados para uso de contextos virtuais, permitindo que sejam criados firewalls distintos em um mesmo hardware, segregando ambientes.

Justificativa: podem haver secretarias que compartilham a mesma estrutura e, por questões de organização, queiram possuir firewalls distintos. Uma forma fácil de resolver essa questão é com o contexto virtual, em que um único hardware, do ponto de vista lógico, pode ser dividido em duas ou mais unidades lógicas, independentes.

Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência

9-Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
Justificativa; inibir acesso a conteúdo indevido a partir de buscas em sites como Google etc.

Resposta: Iremos avaliar as sugestões de acréscimo itens à solução no termo de referência

OI S.A. - EM RECUPERACAO JUDICIAL

1- DIMENSIONAMENTO DOS APPLIANCES SD-WAN

O item 1 do TR cita “Capacidade dos equipamentos SD-WAN das unidades – Deverão ser disponibilizados 11 modelos de equipamentos, que suportam as capacidades de processamento informadas na tabela 1”

Modelo	Capacidade
Modelo 1	300 Mbps (4 interfaces)
Modelo 2	500 Mbps (4 interfaces)
Modelo 3	700 Mbps (4 interfaces)
Modelo 4	1,5 Gbps (4 interfaces)
Modelo 5	3 Gbps (4 interfaces)
Modelo 6	300 Mbps (8 interfaces)
Modelo 7	500 Mbps (8 interfaces)
Modelo 8	700 Mbps (8 interfaces)
Modelo 9	1,5 Gbps (8 interfaces)
Modelo 10	3 Gbps (8 interfaces)
Modelo 11	10 Gbps (8 interfaces)

O TR também menciona:

“Os equipamentos modelos 1, 2, 3, 4 e 5 deverão possuir pelo menos 4 conexões/interfaces de rede que poderão ser utilizadas por links banda larga, MPLS, satélite ou rádio e comunicação 4G ou superior.” e “Os equipamentos modelos 6, 7, 8, 9, 10 e 11, deverão possuir pelo menos 8 conexões/interfaces de rede que poderão ser utilizadas por links banda larga, MPLS, satélite ou rádio e comunicação de dados 4G ou superior.”

a) Estamos entendendo que as interfaces citadas na tabela se refiram a interfaces Ethernet.

Nosso entendimento está correto?

Resposta: Sim, está correto o entendimento.

b) Entendemos que os quantitativos de interfaces informadas na tabela se refiram ao total de interfaces (ETH) do appliance SD-WAN (Considerando a soma das interfaces utilizadas para WAN e LAN).

Nosso entendimento está correto?

Resposta: Sim, está correto o entendimento, porém será melhor detalhado no termo de referência, em sua versão final, que não poderá haver restrição ao uso das interfaces como LAN e WAN, ou seja, as interfaces poderão ser utilizadas para qualquer finalidade e caso haja restrição, deverá haver um adicional de 2

interfaces para uso para rede LAN.

2- INSTALAÇÃO DOS APPLIANCES SD-WAN

O TR cita que “Caso seja necessário ou solicitado pelo gestor do cliente o deslocamento do técnico do fornecedor da solução até a unidade para fazer as configurações dos acessos ao CPE, será cobrado o valor de 50 UFEMG. Este valor será cobrado somente 1 vez por solicitação, independentemente do número de visitas que se fizerem necessárias pelo técnico, até que as conexões ao equipamento sejam concluídas, Caso seja necessário ou solicitado pelo gestor do cliente o deslocamento do técnico do fornecedor da solução até a unidade para fazer as configurações dos acessos ao CPE, será cobrado o valor de 50 UFEMG. Este valor será cobrado somente 1 vez por solicitação, independentemente do número de visitas que se fizerem necessárias pelo técnico, até que as conexões ao equipamento sejam concluídas, exceto se, nas visitas, for constatado pelo técnico e aceito pelo gestor do Órgão, que existem pendências por parte do cliente para que se possa fazer as conexões dos acessos ao CPE SD-WAN. Neste caso, será cobrado novo valor para a uma nova solicitação.”

a) Solicitamos esclarecimento o que seja “50 UFEMG”.

Nossa dúvida será esclarecida?

Resposta: UFEMG é a Unidade Fiscal do Estado de Minas Gerais. Neste caso o valor cobrado será 50 vezes o valor estabelecido para a UFEMG.

Os valores da UFEMG podem ser consultados em

https://www.fazenda.mg.gov.br/empresas/legislacao_tributaria/resolucoes/ufemg.html

b) Entendemos que nos casos de instalação de appliance SD-WAN, a CONTRATADA do Lote 100 deverá agendar com o Órgão a instalação do appliance SD-WAN após a CONTRATANTE sinalizar que o link do determinado endereço já tenha sido instalado e testado pela CONTRATADA fornecedora do link.

Nosso entendimento está correto?

Resposta: Sim, está correto o entendimento.

3- CONSUMO DE MEMÓRIA NOS APLIANCES SD-WAN

O TR cita que “O consumo de CPU do equipamento não poderá ter sua média de utilização acima de 65% no horário compreendido entre 09:00h e 11:30h e 14:30h e 16:30h, exceto se os equipamentos estiverem sob ataque de malware.”

É de nosso entendimento que Soluções de SD-WAN, diferentemente de roteadores, trabalham com alocação de memória. Quando o firmware é carregado, é comum que a solução de SD-WAN reserve memória para uso em eventual necessidade emergencial. Além disso, há soluções que fazem aceleração em hardware, tornando-as menos dependentes da memória. Visando evitar o sobredimensionamento da solução de SD-WAN, sugerimos a seguinte alteração na redação deste item: “Os equipamentos não deverão exceder 80% de utilização de CPU ou de memória de forma contínua, por um tempo igual ou maior a 24 horas”.

Nosso pleito será aceito?

Resposta: Não aceitaremos o pleito. Entendemos que a carga de CPU de 80% sugerida deixa o equipamento muito próximo de sua capacidade total de processamento. Para diversos fabricantes, é comum que, para cargas de processamento acima de 65%, os equipamentos comecem a ter o seu funcionamento comprometido, gerando perdas de pacotes e lentidões. Por estarem estes equipamentos expostos na Internet, queremos ter uma margem de processamento para que eles possam suportar aumentos de processamento esporádicos devidos a diversos fatores, como varreduras, ataques de malware, entre outros eventos, comuns a equipamentos com função de proteção expostos na Internet, sem que isto comprometa a performance do link

da Unidade. É sabido que, este aumento poderá ocorrer eventualmente e poderá comprometer a performance da comunicação da unidade, mesmo com a solicitação que os equipamentos estejam com a carga de CPU abaixo dos 65%, mas com esta medida, pretendemos diminuir a quantidade de vezes que este comprometimento venha a ocorrer.

4- ESPECIFICAÇÕES DA SOLUÇÃO SDWAN

O Termo de Referência cita as especificações mínimas da Solução SD-WAN (Lote 100).

Entendemos que as especificações do Termo de Referência relativas ao SD-WAN estão superficiais, possibilitando que as Proponentes Licitantes contemplem em suas respectivas propostas soluções SD-WAN que podem não atender em plenitude as necessidades do Governo de Minas.

Exemplificando o nosso pleito, na descrição do TR está explícito que a CONTRATANTE pretende utilizar a rede para o tráfego de voz e vídeo. Tratando-se de tráfego sensível à qualidade dos links, entendemos que seja de suma importância a CONTRATANTE exigir no TR as seguintes características da solução SD-WAN:

1- “A solução de SD-WAN deve possuir suporte ao MOS (Mean Opinion Score), para calcular a qualidade de chamadas de voz, considerando jitter, perda de pacote e codec utilizado.”

2- “A solução de SD-WAN deve suportar as funcionalidades de Forward Error Correction (FEC) e Duplicação de pacote entre os links simultaneamente e deduplicação de pacote no appliance SD-WAN de destino, com intuito de melhorar a experiência do usuário quanto as aplicações críticas de negócio.”

Outras funcionalidades para o SD-WAN que entendemos serem importantes de serem contempladas no TR:

1- “Deverá ser entregue no dia da licitação o certificado comprovando que os equipamentos estão em conformidade com as normas IEC e RoHs.”

2- “Os appliances SD-WAN deverão suportar IPSEC VPN Load Balancing”.

3- “Toda a solução SD-WAN deverá ser fabricada por uma única empresa, incluindo o Hardware, Software e a Controladora.”

4- “Os equipamentos SD-WAN não devem apresentar portas nos padrões RS-232, RS232C DB-9, DB15.”

5- “Os equipamentos SD-WAN deverão suportar VRF, possibilitando implementar e suportando tabelas virtuais de roteamento (completamente isoladas logicamente) para permitir segmentação local”

Ante ao exposto, sugerimos que a CONTRATANTE inclua no TR as especificações acima referentes ao SDWAN.

Nossas sugestões serão acatadas?

Resposta: As sugestões serão avaliadas e poderão ser acatadas, desde que não sejam excludentes para vários fabricantes e diminuam a competitividade do certame.

5- SOLUÇÃO SD-WAN

O TR cita que “As unidades para as quais forem contratados acessos nos lotes 90, 110 e 120 deverão obrigatoriamente ter um equipamento CPE SD-WAN e terão todo o tráfego direcionado a estes equipamentos. Embora a unidade possa navegar na Internet sem a necessidade que este tráfego vá até a controladora, ele deverá obrigatoriamente passar pelo equipamento SD-WAN que fará o controle de navegação a com políticas implantadas a partir da console central e em conformidade com os recursos solicitados nos itens abaixo”

Estamos entendendo que os lotes 90, 110 e 120 não contemplem o fornecimento de equipamentos SD-WAN. E devido à obrigatoriedade de se ter equipamento SD-WAN nos casos das unidades contratarem links dos lotes 90, 110 e 120, a unidade também deverá contratar o appliance SD-WAN disponíveis no Lote 100.

Nosso entendimento está correto?

Resposta: Sim, está correto o entendimento.

TELEFONICA (VIVO)

Ser composta por uma Console Central na UGO (on-premises), que será responsável por fazer toda a configuração dos appliances SD-WAN, incluindo priorização de tráfego, configurações de QoS, que deverão ocorrer de forma centralizada via software de gerência

O uso de controladora on-premises é obrigatória devido a criticidade do serviço contratado. Com esta configuração diminuimos a quantidade de elementos existentes na comunicação entre a controladora e a rede corporativa, permitindo maior eficiência na comunicação das unidades remotas com a rede corporativa. O uso de controladoras em nuvem faria com que toda a comunicação das unidades fosse ao ambiente em nuvem e tivesse que retornar para a rede corporativa, aumentando o número de elementos que participariam desta comunicação.

Resposta: Será reavaliado pela equipe técnica a possibilidade de flexibilização desta exigência sem que isto comprometa a prestação dos serviços solicitados

A solução deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão;

Resposta: Este item será revisado para melhor adequação à necessidade do projeto, visando a melhor relação custo/benefício do serviço a ser prestado.

HUAWEI

em relação ao item:

3.1.3.3. Caso a Prestadora seja vencedora de um lote ao qual ela já seja detentora da prestação do serviço na Rede IP e considerando que não haverá intervenção técnica para migração dos links, tal migração se dará somente no âmbito contratual, por meio do Portal da Rede IP, obedecendo a regra estabelecida no item 3.1.3.1 para este caso específico.

Comentário: Visando a isonomia e a fim de preservar a competitividade do certame, sugerimos a obrigatoriedade de substituição completa dos equipamentos que compõem a rede atual.

Resposta: A obrigatoriedade de substituição dos equipamentos acarretará custos desnecessários ao projeto. A possibilidade de manter os equipamentos atuais permitirá ao Estado obter o melhor cenário econômico para o projeto. Caso seja mais interessante economicamente a substituição dos equipamentos isto será refletido pelo mercado nos preços oferecidos. A possibilidade de manutenção dos equipamentos atuais está em conformidade com as tendências de sustentabilidade, ao permitir prolongar o uso dos recursos instalados no parque computacional em operação sem forçar a obsolescência de equipamentos ainda aptos a manutenção do serviço.

Para o maior controle da rede implementada, com o fornecimento de uma solução de roteamento de um único fabricante, com gerenciamento centralizado e disponível para a PRODEMGE e Governo do Estado, além de assegurar a qualidade dos equipamentos que irão compor a rede especificando detalhadamente as capacidades portas, encaminhamento e protocolos, sugerimos a separação em lote de equipamentos (em apenas um único lote para toda a rede) e lotes dos demais serviços de conectividade.

Comentário: Ainda evidenciamos que a separação de um lote para os equipamentos que irão compor a rede resultará em maior economicidade, tendo em vista fornecedores de equipamentos podem ser mais competitivos em relação a preços comparado a fornecedores de links.

Resposta: Nossa avaliação é que a separação de um lote exclusivo para os equipamentos, independente dos links de comunicação, que foi nosso entendimento em relação ao comentário 2), não trará benefício ao Estado. Caso este modelo seja adotado, perderemos todos os benefícios que os prestadores de serviço já possuem hoje em relação aos seus parceiros, sejam fornecedores de equipamentos ou de serviços de comunicação, e traremos para o Estado o custo operacional da gestão das soluções e recursos advindos deste lote exclusivo para equipamentos. Esse modelo só se demonstrou vantajoso para o Estado no lote 100, sendo adotado neste.

Quando olhamos os requisitos de serviço de suporte e manutenção, teremos um único tópico com definição de preço, aparecendo apenas no anexo D - LINK SATÉLITE OTB.

Questionamento: Estes mesmos critérios devem ser aplicados para o suporte de garantia de produto? Está correto nosso entendimento?

Resposta: Todos os lotes devem atender aos critérios de prestação de serviço definidos de forma global no termo de referência. Quando há necessidade de definição de critérios específicos para um lote, esta informação é descrita no anexo relativo ao lote, como ocorreu no caso do anexo D.

1.1. A opção de se ter mais de uma Prestadora traz a necessidade de integração de suas redes em um ambiente multisserviços. A arquitetura de rede adotada para tal integração utiliza a tecnologia VPN/MPLS, que possibilita a comunicação entre as Unidades de Governo transpassando os backbones das Prestadoras, de forma transparente, preservando a qualidade dos serviços.

8.1.2. A solução de rede adotada e implantada utiliza um núcleo de rede composto por roteadores das diversas Prestadoras operando com a tecnologia VPN/MPLS, com abrangência desde esse núcleo de rede até a camada de acesso (CE), conforme demonstrado na figura 4.

Comentário: Sugerimos a modernização da tecnologia exigida para interconexão da rede de multisserviços com a implementação de SRv6. Citamos as vantagens da utilização do SRv6 em comparação com MPLS:

Arquitetura simplificada: O SRv6 simplifica a arquitetura de rede, eliminando a necessidade de protocolos de sinalização complexos, como LDP ou RSVP-TE, o que resulta em menos sobrecarga de configuração e gerenciamento.

Roteamento de origem: Com o SRv6, o nó de origem determina o caminho que os pacotes percorrem na rede, oferecendo controle granular e flexibilidade para direcionamento de tráfego e encadeamento de serviços.

Programação de rede: O SRv6 permite que os operadores de rede programem o comportamento dos roteadores usando instruções de roteamento de origem, tornando o gerenciamento da rede mais ágil e adaptável.

Engenharia de tráfego: O SRv6 permite a engenharia de tráfego dinâmica, direcionando facilmente o tráfego por caminhos específicos, otimizando a utilização da rede e evitando links congestionados.

Encadeamento de serviços: O SRv6 simplifica o encadeamento de serviços ao especificar uma sequência de segmentos que o tráfego deve percorrer, facilitando a criação de caminhos de serviços complexos.

Escalabilidade: A arquitetura simplificada e a sobrecarga de sinalização reduzida do SRv6 contribuem para uma melhor escalabilidade, tornando-o adequado para redes grandes e complexas.

Transição para o IPv6: o SRv6 aproveita os endereços e cabeçalhos IPv6, tornando-o compatível com a transição global para o IPv6 e permitindo uma abordagem unificada para o roteamento de rede.

Resposta: MPLS é um protocolo amplamente utilizado no mercado. Entendemos que ainda é a melhor opção para a rede corporativa do Estado.

5) Em relação ao requisito descrito para solução de SD-WAN:

A solução SD-WAN deverá ser suportar exportação de registros Netflow / IPFIX;

Questionamento: Entendemos que serão aceitos também solução SD-WAN que suporte a exportação de registro Netstream. Está correto nosso entendimento?

Resposta: Iremos revisar este item retirando a menção a protocolos proprietários.

Alber Vinicius Duque da Silveira

Diretoria Central de Gestão de Serviços e Infraestrutura de TIC

Daniel Machado Maia

Diretor Central de Gestão de Serviços e Infraestrutura de TIC

Cláudio Rinco Dutra Pereira

Gerente de Redes Prodemge



Documento assinado eletronicamente por **Claudio Rinco Dutra Pereira, Gerente**, em 02/05/2024, às 08:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 47.222, de 26 de julho de 2017](#).



Documento assinado eletronicamente por **Alber Vinicius Duque da Silveira, Servidor(a) Público(a)**, em 02/05/2024, às 08:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 47.222, de 26 de julho de 2017](#).



Documento assinado eletronicamente por **Daniel Machado Maia, Diretor (a)**, em 02/05/2024, às 09:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 47.222, de 26 de julho de 2017](#).



A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **87443893** e o código CRC **6A07A9A9**.

Referência: Processo nº 1500.01.0079973/2024-83

SEI nº 87443893