



GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL

RESPOSTA

TERMO DE RESPOSTA AOS PEDIDOS DE ESCLARECIMENTOS

PREGÃO ELETRÔNICO Nº 90273/2024/CEL/SUPEL/RO

PROCESSO ADMINISTRATIVO: 0037.002497/2024-69

OBJETO: Registro de Preços para futura e eventual Aquisição de Ativos de Segurança de Rede Firewalls Next Generation (NGFW) com SD-WAN integrado, Switch Core, Switch de Borda, Controlador de Wi-fi, Access Point e licenças de antivírus com tecnologia EDR para desktops e servidores, contemplando os serviços de Instalação, Configuração, Treinamento, Suporte Técnico e garantia de 60 meses, para atender todo o Parque Tecnológico da Polícia Civil do Governo do Estado de Rondônia, órgãos de segurança pública vinculados a SESDEC, devendo ser entregues e instalados nas respectivas localidades, de acordo com os termos e condições do termo de referência.

A Superintendência Estadual de Licitações - SUPEL, através da Pregoeira nomeada por força da **Portaria nº 83/GAB/SUPEL, publicada no DOE de 17.10.2024**, vem neste ato responder aos pedidos de esclarecimentos enviados por e-mail por empresas interessadas.

Nos dias 18 e 19.12.2024 esta equipe recebeu os pedidos de esclarecimentos referente ao Pregão citado.

1. DA ADMISSIBILIDADE

Em sede de admissibilidade, verificou-se que foram preenchidos os pressupostos de legitimidade, interesse processual, fundamentação e tempestividade, nos termos do Art. 164, da Lei nº 14.133, de 2023 e do item 6 do Instrumento Convocatório, conforme comprovam os documentos colacionados ao processo administrativo SEI relacionado a este PE 90273/2024/SUPEL, pelo que passo a formulação das Respostas aos Pedidos de Esclarecimento. Informamos ainda, que de acordo com o **AVISO DE ADIAMENTO (0055985499)**, houve a necessidade de adiamento, para que seja respeitado o disposto no **item 6.3 do Instrumento Convocatório**.

2 - DOS PEDIDOS DE ESCLARECIMENTO E DA RESPOSTA DA UNIDADE TÉCNICA DA SESDEC

Considerando que as questões levantadas nos pedidos de esclarecimentos tem sua origem no Termo de Referência, enviados os pedidos e anexos via SEI! à SESDEC-FUNESP, para manifestação, e, em resposta, vem neste ato, esclarecer o que se segue:

2.1. DO PEDIDO DE ESCLARECIMENTO DA EMPRESA NEXA TECNOLOGIA DE ID. Nº. (0055893949)

Perguntamos:

1) **Questionamento nº. 01: Item 4.6.** "A Solução deve concentrar a gestão em um único equipamento, podendo esse appliance ser físico ou virtual, e que o mesmo possa gerenciar as funcionalidades de firewall de próxima geração (NGFW) com SD-WAN integrado, Switch e Access Point (Wi-Fi)".

Perguntamos: A exigência de concentrar a gestão em um único equipamento, capaz de gerenciar funcionalidades de NGFW com SD-WAN integrado, Switch e Access Point, restringe a participação de fabricantes que utilizam arquiteturas de gerenciamento distribuídas e especializadas. Essa abordagem exclusiva favorece soluções específicas, como as da Fortinet, e ignora alternativas mais modernas e escaláveis disponíveis no mercado. Além disso, concentrar múltiplas funcionalidades críticas em um único dispositivo pode impactar a performance e a segurança da solução.

Está correto nosso entendimento?

Resposta da PC-DETEINF: Não está correto o seu entendimento.

Concentrar o gerenciamento das funcionalidades em único equipamento permite uma gestão mais centralizada, simplificando a complexidade operacional e aumentando a eficiência no gerenciamento das funcionalidades de segurança e conectividade.

2) **Questionamento nº. 02: Item 4.7.** *A contratação de um Firewall NGFW (Next-Generation Firewall) com SD-WAN integrado e Wi-Fi Seguro para a Polícia Civil pode ser justificada com base na necessidade de garantir a segurança da rede e dos dados sensíveis da instituição. A Polícia Civil lida com informações altamente sensíveis, como investigações criminais, dados pessoais de vítimas e suspeitos, registros criminais, entre outros. Um Firewall NGFW é capaz de monitorar e filtrar o tráfego de rede, identificando e bloqueando potenciais ameaças, como ataques cibernéticos e invasões. Isso ajuda a garantir a confidencialidade e integridade dos dados, protegendo as informações confidenciais da Polícia Civil contra acessos não autorizados.*

Perguntamos: A justificativa apresentada no edital para a contratação de um Firewall NGFW com SD-WAN integrado e Wi-Fi seguro, ainda que válida, restringe a competitividade ao especificar a integração de todas essas funcionalidades em um único equipamento. Soluções de fabricantes que utilizam arquiteturas distribuídas, permitindo a integração de tecnologias especializadas para firewall, SD-WAN e Wi-Fi, oferecem o mesmo nível de segurança e desempenho, sem a necessidade de concentrar tudo em um único dispositivo. Essa abordagem, além de ampliar as opções de fornecedores, favorece a flexibilidade, escalabilidade e otimização dos recursos.

Está correto nosso entendimento?

Resposta da PC-DETEINF: Seu entendimento não está correto.

A Integração é um Fator Estratégico: A integração de funcionalidades em um único equipamento não apenas simplifica a administração da rede, mas também aumenta a eficiência operacional. Em uma instituição como a Polícia Civil, que lida com dados altamente sensíveis, é fundamental reduzir a complexidade e os pontos de falha na infraestrutura de segurança. As soluções distribuídas exigiram maior esforço de integração e manutenção, o que pode impactar em termos de disponibilidade e confiabilidade dos serviços.

3) **Questionamento nº. 03: Item 4.18.2.38 - 4.18.2.38.** O Gerenciamento centralizado, deve possibilitar a visualização integrada de todas as ferramentas adquiridas, sendo que os equipamentos (Firewall, Switch e Access Point) podem ser gerenciados por esta plataforma integrada, ou plataforma distinta desde todos os log's destes dispositivos sejam enviados para uma Plataforma de Gestão de Log Centralizada.

Perguntamos: A exigência do edital de que o gerenciamento centralizado de firewall, switch e access point seja realizado preferencialmente por uma única plataforma integrada limita a competitividade e direciona para fabricantes específicos, como a Fortinet, que oferecem essa abordagem

nativamente. Essa exigência desconsidera soluções de mercado que utilizam plataformas distintas para gerenciamento, mas que garantem integração plena através do envio de logs para uma plataforma centralizada, atendendo às mesmas necessidades de visibilidade e controle.

Está correto nosso entendimento?

Resposta da PC-DETEINF: Seu entendimento não está correto.

Ressaltamos que o objetivo principal é garantir uma gestão centralizada, eficiente e integrada, com plena visibilidade e controle dos dispositivos, de modo a atender às necessidades da Polícia Civil.

4) Questionamento nº. 04: Item 4.18.2.48. Dessa forma, a integração de um Antivírus NGAV (NextGeneration Antivirus) ao Firewall NGFW (Next-Generation Firewall) traz uma série de vantagens significativas para a segurança da rede: Ao integrar um Antivírus NGAV ao Firewall NGFW, é possível obter uma camada adicional de detecção de malware. O Antivírus NGAV utiliza técnicas avançadas, como análise comportamental, machine learning e detecção baseada em assinaturas, para identificar e bloquear ameaças conhecidas e desconhecidas. Isso aumenta significativamente a eficácia na detecção e remoção de malware na rede:

A integração permite uma resposta mais rápida a ameaças em tempo real. Quando o Antivírus NGAV detecta uma ameaça, ele pode enviar alertas e informações de eventos de segurança para o Firewall NGFW, que pode agir imediatamente para bloquear o tráfego malicioso ou isolar dispositivos infectados. Isso ajuda a reduzir o tempo de resposta a incidentes e minimiza o impacto de ataques em potencial.

Ao integrar o Antivírus NGAV ao Firewall NGFW, é possível obter uma visão centralizada das atividades de segurança. Isso permite monitorar e analisar o tráfego de rede, eventos de segurança e alertas em um único console de gerenciamento. Essa visibilidade unificada simplifica a administração e facilita a identificação de possíveis ameaças ou padrões de comportamento malicioso. A integração facilita a criação de políticas de segurança unificadas. Sendo possível definir regras no Firewall NGFW para bloquear ou permitir o tráfego com base nas informações e detecções do Antivírus NGAV. Isso garante uma aplicação consistente das políticas de segurança em toda a rede, reduzindo as lacunas de segurança e as chances de exploração de vulnerabilidades.

A integração entre o Antivírus NGAV e o Firewall NGFW pode levar a uma melhor eficiência e desempenho da rede. Ao trabalharem em conjunto, eles podem otimizar a utilização de recursos, evitando a duplicação de tarefas e minimizando o impacto no desempenho da rede. Isso resulta em uma proteção mais eficaz, sem comprometer a velocidade e a qualidade da conectividade.

Em suma, a integração de um Antivírus NGAV ao Firewall NGFW oferece uma camada adicional de proteção contra malware, aumenta a visibilidade e controle sobre as atividades de segurança, facilita a resposta rápida a ameaças e melhora a eficiência geral do ambiente de segurança da rede.

Perguntamos: A exigência de integração de um Antivírus NGAV (Next-Generation Antivirus) ao Firewall NGFW (Next-Generation Firewall) no edital pode restringir a competitividade e direcionar para um único fabricante, como a Fortinet. Embora a integração de funções de segurança possa ser vantajosa em alguns casos, muitos fornecedores líderes do mercado oferecem soluções altamente eficientes por meio de arquiteturas descentralizadas, com antivírus baseados em endpoints ou em soluções de segurança na nuvem (como EDRs ou XDRs) que complementam a funcionalidade do firewall, sem comprometê-lo. A centralização excessiva dessas funções em um único equipamento pode gerar limitações em termos de escalabilidade, flexibilidade e interoperabilidade.

Está correto nosso entendimento?

Resposta da PC-DETEINF: Seu entendimento não está correto.

A integração entre o Antivirus NGAV e Firewall NGFW complementa as camadas de segurança do Datacenter da Polícia Civil. A integração soma-se com a solução de proteção de endpoints já

em produção no parque da Polícia Civil.

5) Questionamento nº. 05: Item 2.5.6. *Suportar proxy explícito;*

Perguntamos: A exigência de suporte a proxy explícito restringe a participação de fornecedores que oferecem soluções de segurança mais modernas e eficientes. A maioria dos fabricantes líderes de segurança, como Cisco, não implementa mais o proxy explícito como parte de suas soluções de firewall, optando por arquiteturas mais avançadas de segurança em nuvem e inspeção de tráfego. O proxy explícito é uma tecnologia mais antiga, que está sendo substituída por abordagens mais dinâmicas e eficientes, como o uso de segurança baseada em nuvem (SASE), proxies transparentes e soluções de inspeção TLS. Essas abordagens modernas oferecem menor impacto na performance, melhor escalabilidade e uma experiência de usuário mais fluida, sem a necessidade de configurar os dispositivos dos usuários para um proxy explícito.

Resposta da PC-DETEINF: Seu entendimento não está correto.

A exigência de suporte a procuração explícita foi exigida com base nas necessidades operacionais específicas da Polícia Civil no momento. Reconhecemos que tecnologias mais recentes, como SASE, proxies transparentes e soluções avançadas de inspeção de tráfego TLS, oferecem vantagens significativas em termos de desempenho, escalabilidade e experiência do usuário. No entanto, essas abordagens serão consideradas e apresentadas em contratações futuras

6) Questionamento nº. 06: Item 3.1. Throughput de, no mínimo, 79.5 Gbps com a funcionalidade de firewall, considerando 1518 bytes UDP;

Perguntamos: Throughput Exigido (79,5 Gbps): A exigência de 79,5 Gbps de throughput no ponto 3.1 do edital é exagerada para o uso prático e acaba direcionando para um fornecedor específico, como a Fortinet. O que realmente importa no ambiente é o desempenho com as funcionalidades de segurança ativadas (firewall, controle de aplicação, IPS, antivírus, etc.), que estaria mais próximo dos 9 Gbps, conforme o ponto 3.11 do edital. Esse tipo de requisito superdimensionado compromete a competitividade e pode aumentar os custos desnecessariamente.

Está correto nosso entendimento?

Resposta da PC-DETEINF: Seu entendimento não está correto.

Entende-se que o throughput exigido no item 3.1 se refere ao desempenho do equipamento apenas com a funcionalidade de firewall e considerando pacotes de 1518 bytes UDP. O desempenho com as funcionalidades de segurança habilitadas é especificado separadamente no item 3.11.

7) Questionamento nº. 07: Item 3.12. *Possuir ao menos 18 interfaces 1 GE RJ45; / 3.13. Possuir ao menos 8 interfaces 10 GE SFP+; / 3.14. Possuir ao menos 8 interfaces 1 GE SFP; / 3.15. Possuir ao menos 1 interface console RJ45.*

Perguntamos: Os itens 3.12, 3.13, 3.14 e 3.15 especificam um número exato de interfaces e tipos, o que pode direcionar a escolha para um fabricante específico. Essas exigências limitam a competitividade ao excluir soluções igualmente eficazes e compatíveis que possuem arquiteturas diferentes, mas atendem às mesmas necessidades funcionais. Além disso, exigir configurações específicas de portas pode não refletir as reais necessidades do ambiente. É importante priorizar a flexibilidade para que diferentes fabricantes possam propor soluções tecnicamente equivalentes e economicamente mais vantajosas, ajustadas à demanda do ambiente do cliente.

Resposta da PC-DETEINF: Seu entendimento parcialmente correto.

No entanto, gostaríamos de esclarecer que os itens 3.12, 3.13, 3.14 e 3.15 foram definidos

com base em uma análise técnica detalhada das necessidades do ambiente em questão. O objetivo é garantir que a solução atenda de forma plena às demandas operacionais e seja compatível com a infraestrutura existente, proporcionando a melhor eficiência e desempenho. Os requisitos apresentados servem como referência mínima para o objeto. Caso a preponente ofereça equipamento de um número maior de portas a proposta será aceita.

8) Questionamento nº. 08: Item 3.16. Permitir gerenciar até 512 Access Points.

Perguntamos: Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Resposta da PC-DETEINF: Seu entendimento não está correto.

A integração das funcionalidades satisfaz as necessidades e traduz a eficácia estratégica da Polícia Civil.

9) Questionamento nº. 09: Item 3.17. Permitir gerenciar até 72 Switches.

Perguntamos: Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Resposta da PC-DETEINF: Seu entendimento não está correto.

O entendimento apresentado no questionamento inicial está alinhado com boas práticas recomendadas por especialistas na área de redes e segurança, a integração das funcionalidades satisfaz as necessidades e traduz a eficácia estratégica da Polícia Civil.

10) Questionamento nº. 10: Item 3.18. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

Perguntamos: 1. VDOMs não são a única opção para segmentação virtual no mercado. Soluções como multi-context da Cisco ou VRFs também atendem bem às necessidades de segurança e segmentação. Além disso, 10 VDOMs podem ser desnecessários dependendo da escala da rede, e outras soluções poderiam ser mais flexíveis e econômicas, sem perder performance ou segurança.

Resposta da PC-DETEINF: Seu entendimento não está correto.

Embora reconheçamos que outras soluções possam ser viáveis, acreditamos que os VDOMs são a melhor opção para atender às nossas necessidades específicas de escalabilidade, segurança e gerenciamento, mantendo uma relação custo-benefício favorável. A solicitação de sistemas virtuais lógicos (contextos) por appliance não limita a oferta de tecnologias como multi-context da Cisco e outras de mercado.

11) Questionamento nº. 11: Item 4.0.1. Throughput de, no mínimo, 5 Gbps com a funcionalidade de firewall, considerando 1518 bytes UDP.

Perguntamos: A exigência de 5 Gbps de throughput no ponto 4.0.1 do edital é exagerada para o uso prático e acaba direcionando para um fornecedor específico, como a Fortinet. O que realmente

importa no ambiente é o desempenho com as funcionalidades de segurança ativadas (firewall, controle de aplicação, IPS, antivírus, etc.), que estaria mais próximo dos 600 Mbps, conforme o ponto 4.0.11 do edital. Esse tipo de requisito superdimensionado compromete a competitividade e pode aumentar os custos desnecessariamente.

Resposta da PC-DETEINF: Seu entendimento não está correto.

Entende-se que o throughput exigido no item 4.0.1 se refere ao desempenho do equipamento apenas com a funcionalidade de firewall e considerando pacotes de 1518 bytes UDP. O desempenho com as funcionalidades de segurança habilitadas é especificado separadamente no item 4.0.11.

12) Questionamento nº. 12: Item 4.0.14. Permitir gerenciar ao menos 16 Access Points.

Perguntamos: Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Resposta da PC-DETEINF: Seu entendimento não está correto.

Nosso objetivo é garantir uma infraestrutura robusta, eficiente e segura, utilizando as melhores práticas de design de rede, a integração das funcionalidades satisfaz as necessidades e traduz a eficácia estratégica da Polícia Civil.

13) Questionamento nº. 13: Item Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Resposta da PC-DETEINF: Seu entendimento não está correto.

Nossa política de gestão de TI busca adotar soluções especializadas para cada necessidade, priorizando eficiência e robustez. A integração das funcionalidades satisfaz as necessidades e traduz a eficácia estratégica da Polícia Civil.

14) Questionamento nº. 14: Item 4.0.16. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

Perguntamos: VDOMs não são a única opção para segmentação virtual no mercado. Soluções como multi-context da Cisco ou VRFs também atendem bem às necessidades de segurança e segmentação. Além disso, 10 VDOMs podem ser desnecessários dependendo da escala da rede, e outras soluções poderiam ser mais flexíveis e econômicas, sem perder performance ou segurança.

Resposta da PC-DETEINF: Seu entendimento não está correto.

Gostaríamos de esclarecer que nosso entendimento sobre o uso de VDOMs está alinhado às necessidades específicas do nosso ambiente de rede.

VDOMs e outras soluções de segmentação: Concordamos que existem diversas alternativas no mercado, como VRFs e multi-contexts da Cisco, que também oferecem segmentação e segurança. No entanto, a escolha pelos VDOMs foi baseada em uma análise detalhada de requisitos

técnicos e operacionais, considerando fatores como flexibilidade, facilidade de gerenciamento e integração com nossa infraestrutura existente.

Número de VDOMs (10): Entendemos que 10 VDOMs podem parecer excessivos dependendo do cenário. Contudo, a decisão foi fundamentada no crescimento projetado de nossa rede e na necessidade de segmentação granular para diferentes departamentos e aplicações críticas. Esse número nos proporciona margem para expansão futura, evitando a necessidade de reconfigurações complexas.

Custo-benefício: Analisamos cuidadosamente o impacto financeiro e técnico da solução escolhida. Apesar de alternativas como VRFs serem viáveis, identificamos que os VDOMs atendem melhor às nossas expectativas em termos de desempenho e segurança sem comprometer a eficiência econômica a longo prazo.

15) Questionamento nº. 15: Item 03 – MÓDULO DE GERENCIAMENTO CENTRALIZADO.

Perguntamos: A exigência do edital que trata do módulo de gerenciamento centralizado (item 03) e do módulo de relatoria e retenção de logs (item 04) parece estar fortemente alinhada com uma solução específica (Fortinet), limitando a participação de outros fabricantes e restringindo a competitividade. Cada fabricante de soluções de segurança de rede, como Cisco, Palo Alto, ou Fortinet, possui diferentes abordagens e ferramentas para o gerenciamento e monitoramento de segurança e rede. Insistir em uma arquitetura específica impõe barreiras injustas a outros fornecedores, prejudicando o princípio de igualdade de condições em processos licitatórios.

Resposta da PC-DETEINF: Seu entendimento não está correto.

Módulos de gerenciamento centralizado são uma prática comum do mercado para melhorar a eficiência operacional dos equipamentos e soluções. As especificações técnicas apresentadas não possuem complexidades técnicas ou arquitetura específica.

16) Questionamento nº. 16: Item 04 - MÓDULO DE RELATORIA E RETENÇÃO DE LOGS.

Perguntamos: A exigência do edital que trata do módulo de gerenciamento centralizado (item 03) e do módulo de relatoria e retenção de logs (item 04) parece estar fortemente alinhada com uma solução específica (Fortinet), limitando a participação de outros fabricantes e restringindo a competitividade. Cada fabricante de soluções de segurança de rede, como Cisco, Palo Alto, ou Fortinet, possui diferentes abordagens e ferramentas para o gerenciamento e monitoramento de segurança e rede. Insistir em uma arquitetura específica impõe barreiras injustas a outros fornecedores, prejudicando o princípio de igualdade de condições em processos licitatórios.

Resposta da PC-DETEINF: Seu entendimento não está correto.

A especificação técnica descrita nos itens 03 e 04 visa atender às necessidades específicas da Polícia Civil, assegurando a compatibilidade com a infraestrutura existente e o atendimento aos requisitos funcionais e de segurança. Essas especificações não se limitam a uma única solução ou fabricante.

Adicionalmente, salientamos que os requisitos foram descritos de maneira técnica e genérica, permitindo que diferentes fabricantes, como Cisco, Palo Alto, Fortinet e outros, possam oferecer soluções compatíveis, desde que atendam às exigências funcionais do edital.

Módulos de análises de logs são uma prática comum do mercado para melhorar a eficiência operacional dos equipamentos e soluções. As especificações técnicas apresentadas não possuem complexidades técnicas ou arquitetura específica.

17) Questionamento nº. 17: Item 22.5. PARCELA DE MAIOR RELEVÂNCIA: a parcela

de maior relevância e valor significativo dos lotes desta licitação ficam determinadas na forma abaixo: b) Solução de Conectividade Wireless do tipo Indoor, com suporte aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac Wave 2, com garantia e suporte pelo período contratual de 60 meses.

Perguntamos: Ao exigir apenas a tecnologia IEEE 802.11ac Wave 2 (Wi-Fi 5), o edital está selecionando uma tecnologia que já está em declínio e próxima de End of Life (EOL) em diversos fabricantes. Equipamentos baseados nesse padrão podem se tornar rapidamente obsoletos, principalmente considerando que o contrato é para um período de 60 meses (5 anos). Durante esse período, é altamente provável que os equipamentos baseados em Wi-Fi 5 deixem de ser suportados ou recebam atualizações limitadas, comprometendo a eficiência da rede no longo prazo.

Resposta da PC-DETEINF: Seu entendimento está parcialmente correto.

O padrão Wi-Fi 5 ainda é amplamente utilizado no mercado e possui grande compatibilidade com a maioria dos dispositivos atualmente em operação. Essa escolha busca garantir o equilíbrio entre desempenho e acessibilidade financeira, considerando o orçamento público e a realidade tecnológica da maioria dos usuários.

Custo-Benefício: A adoção de tecnologias mais recentes, como o **Wi-Fi 6 (IEEE 802.11ax)**, implica em custos significativamente mais elevados, tanto na aquisição quanto na manutenção, o que pode comprometer a viabilidade financeira do projeto dentro dos limites orçamentários.

Ciclo de Vida do Contrato: Apesar de a tecnologia Wi-Fi 5 estar em um estágio mais avançado de seu ciclo de vida, muitos fabricantes continuam oferecendo suporte e atualizações durante períodos significativos, alinhados ao prazo contratual de 60 meses. Para mitigar riscos, a especificação do edital exige **garantia e suporte por todo o período do contrato**, garantindo a funcionalidade dos equipamentos. A especificação atual atende aos requisitos mínimos de conectividade esperados para o período de vigência do contrato.

18) Questionamento nº. 18: Item 11.2.51. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax.

Perguntamos: O edital apresenta inconsistências ao solicitar tecnologias de Wi-Fi 5 (802.11ac) em algumas seções, sem especificar claramente a exigência de equipamentos mais modernos, como Wi-Fi 6 (802.11ax). Essa falta de clareza pode gerar propostas que não atendam às expectativas futuras do projeto ou resultem na entrega de equipamentos de diferentes categorias, comprometendo a padronização e a longevidade da solução.

Resposta da PC-DETEINF: O questionamento é pertinente, devendo ser considerado as tecnologias 802.11ac, a fim de que não haja dimensionamentos equivocados na elaboração de propostas garantindo clareza e uniformidade nas especificações.

2.2. DO PEDIDO DE ESCLARECIMENTO DA EMPRESA UNITY SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO LTDA DE ID Nº. (0055941949)

Perguntamos:

1) Questionamento nº. 1, Item “24.4. Entende-se por pertinente em quantidades o (s) atestado (s) que em sua individualidade ou soma de atestados, demonstrem que a licitante forneceu, em conformidade com a sua proposta, mobiliário e equipamentos, na quantidade correspondente a no mínimo 10% (dez por cento) do quantitativo total do lote/item que apresentar proposta.” (RETIRADO DO EDITAL Considerando que o item 24.5 b) referência soluções dos itens “Solução de Conectividade Wireless do tipo Indoor, com suporte aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac Wave 2, com garantia e suporte pelo período contratual de 60 meses” e

“Solução de Firewall do tipo Next Generation (NGFW), com SD-WAN integrado – TIPO 02 (Unidades Remotas), com garantia e suporte pelo período contratual de 60 meses.”, entendemos que o quantitativo de 10% solicitado no item 24.4 se refere ao item de maior quantidade, item 8 Solução de Conectividade Wireless do tipo Indoor, com suporte aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac Wave 2, com garantia e suporte pelo período contratual de 60 meses.

Está correto nosso entendimento?

Resposta da PC-DETEINF: Seu entendimento esta parcialmente correto.

Entende-se que ambos os itens se integram, permitindo um somatório dos quantitativos.

2) Questionamento nº. 2, Item - 8.3, 9.0.5 e 10.5 8.3. Deve possuir capacidade de comutação de pelo menos 126 Gbps e ser capaz de encaminhar até 200 Mpps (milhões de pacotes por segundo). 9.0.5. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo). 10.5. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo).

Referente aos cálculos de packets per second (PPS) e os fatores que influenciam o desempenho de velocidade e capacidade de processamento de switches e roteadores, entendemos que uma margem de 5% dentro de um contexto técnico, onde o desempenho real depende de variáveis como tamanho dos pacotes e características específicas da rede, não comprometeria o desempenho da operação nem o atendimento aos requisitos funcionais solicitados nos itens 8.3, 9.0.5 e 10.5. Em cálculos de PPS, a quantidade de pacotes por segundo processados por um dispositivo depende diretamente da largura de banda e do tamanho dos pacotes trafegados. Quando se considera uma variação de 5%, o que implicaria uma redução do valor de 200 Mpps para 190 Mpps no item 8.3, 250 Mpps para 237,5 Mpps no item 9.0.5 e 180 Mpps para 171 Mpps no item 10.5, isso não representaria um comprometimento no desempenho, desde que os demais itens de desempenho, como largura de banda, capacidade de comutação e latência, estejam atendidos adequadamente. O valor de PPS, embora importante, deve ser analisado juntamente com outros aspectos da performance da rede, e, neste caso, a variação não causaria impacto no funcionamento da rede, uma vez que se encontra dentro de uma margem técnica aceitável.

Está correto nosso entendimento?

Resposta da PC-DETEINF: eu entendimento esta parcialmente correto.

Em relação aos cálculos de *packets per second* (PPS) e os requisitos de desempenho mencionados nos itens 8.3, 9.0.5 e 10.5, entendemos que uma margem de 5% de variação nos valores de PPS não comprometeria o desempenho da operação, desde que os outros requisitos, como a capacidade de comutação e a largura de banda, sejam atendidos adequadamente.

Essa margem de variação (redução de 200 Mpps para 190 Mpps no item 8.3, 250 Mpps para 237,5 Mpps no item 9.0.5 e 180 Mpps para 171 Mpps no item 10.5) está dentro de uma faixa técnica aceitável, considerando que o desempenho geral do dispositivo depende de vários fatores, como o tamanho dos pacotes e as características específicas da rede.

Portanto, a variação de 5% no PPS não impactaria o funcionamento da rede, e o desempenho da operação continuaria sendo atendido de forma satisfatória, desde que os demais parâmetros técnicos sejam cumpridos.

3) Questionamento nº. 3, Item 11.2.55 – Sensibilidade de Access Point 11.2.55. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);

Considerando o atendimento integral a todos os demais itens especificados, como os que envolvem potência de irradiação, operação MIMO, suporte a MU-MIMO, modulação avançada, recursos como TWT e BSS Coloring, compatibilidade com diferentes larguras de canal em 5 GHz e antenas de ganho mínimo especificado, entendemos que a exigência de sensibilidade mínima de -94 dBm ao operar

em 5 GHz com MCS0 (HT20) pode ser flexibilizada para -93 dBm sem comprometer o desempenho geral da solução ofertada. Essa flexibilização não impactaria a capacidade do equipamento de atender às necessidades funcionais e técnicas do ambiente, considerando que todos os demais requisitos foram plenamente atendidos.

Está correto nosso entendimento?

Resposta da PC-DETEINF: Seu entendimento está parcialmente correto.

É fundamental destacar que a sensibilidade de -94 dBm foi estabelecida com o objetivo de garantir a qualidade da recepção e o desempenho adequado do Access Point em diferentes condições de sinal e interferência. Os requisitos apresentados servem como referência mínima para o objeto. Desde que não haja prejuízo técnico serão analisadas pequenas variações de margens com intuito de promover maior competitividade.

4) Questionamento nº. 4, Item 3.13. Possuir ao menos 8 interfaces NGFW - 10 GE SFP+; 3.14. Possuir ao menos 8 interfaces 1 GE SFP.

Referente aos itens 3.13 e 3.14, que exigem, respectivamente, a presença de ao menos 8 interfaces 10 GE SFP+ e 8 interfaces 1 GE SFP, não foi especificado no edital o número de transceivers necessários. Considerando o item 7.63, que determina que todos os transceivers para slots de fibra óptica dos switches devem ser fornecidos e do mesmo fabricante do equipamento, entendemos que essa mesma exigência também se aplica à Solução de Firewall do tipo Next Generation (NGFW) com SDWAN integrado – TIPO 01 (Concentrador).

Está correto nosso entendimento?

Resposta da PC-DETEINF: Seu entendimento está correto.

Em relação aos itens 3.13 e 3.14, que exigem a presença de ao menos 8 interfaces 10 GE SFP+ e 8 interfaces 1 GE SFP, e considerando o disposto no item 7.63 do edital, que determina que todos os transceivers para slots de fibra óptica dos switches devem ser fornecidos e do mesmo fabricante do equipamento, confirmamos que a mesma exigência se aplica à Solução de Firewall do tipo Next Generation (NGFW) com SDWAN integrado – TIPO 01 (Concentrador). Portanto, é necessário que os transceivers para as interfaces mencionadas nos itens 3.13 e 3.14 sejam fornecidos e sejam do mesmo fabricante da solução de firewall.

Informo que esta resposta será publicada no site desta SUPEL, COMPRASNET e demais meios legais.

Fica REAGENDADA a data de abertura da sessão conforme abaixo, nos termos do parágrafo único do Art. 164, da Lei nº 14.133, de 2023, para que seja respeitado o disposto no **item 6.3 do Instrumento Convocatório.**

Data de Abertura: 27/12/2024 às 10h00min (horário de Brasília – DF).

Endereço: no site de licitações: www.comprasnet.gov.br

Prevalecem inalteradas as demais cláusulas do Instrumento Convocatório.

Eventuais dúvidas poderão ser sanadas junto a Comissão Especial de Licitação, através do

telefone (69) 3212-9243, no e-mail da Equipe: cel@supel.ro.gov.br ou no endereço sito ao Palácio Rio Madeira, Ed. Rio Pacaás Novos/Edif. Central, 2º Andar, Av. Farquar, nº 2986, B. Pedrinhas, CEP 76.801-470, Porto Velho/RO

Porto Velho, 23 de dezembro de 2024.

Bruna Gonçalves Apolinário

Pregoeira da Comissão Especial de Licitações - CEL
Superintendência Estadual de Compras e Licitações - SUPEL/RO



Documento assinado eletronicamente por **Bruna Gonçalves Apolinário, Pregoeiro(a)**, em 23/12/2024, às 12:34, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do [Decreto nº 21.794, de 5 Abril de 2017.](#)



A autenticidade deste documento pode ser conferida no site [portal do SEI](#), informando o código verificador **0055997705** e o código CRC **2A85EDB6**.

Referência: Caso responda este(a) Resposta, indicar expressamente o Processo nº 0037.002497/2024-69

SEI nº 0055997705