

RESPOSTA AO PEDIDO DE ESCLARECIMENTO Nº 4 - COFEN/PRES/CPL

Processo nº 00196.004611/2024-62

PREGÃO ELETRÔNICO Nº 90.028/2024

Trata-se de solicitação de esclarecimento relativo ao Edital do Pregão Eletrônico nº 90.028/2024, que tem por objeto a contratação, por meio do Sistema de Registro de Preços (SRP), de Solução Integrada de Serviços de Segurança e de Serviços de Conectividade de Rede, compreendendo: provimento de serviços de segurança de rede e endpoints; monitoramento e administração dos serviços providos; resposta a incidentes de segurança; fornecimento de solução de conectividade para rede local e wireless; instalações e configurações das soluções providas e treinamento para a equipe do Cofen, conforme condições e exigências estabelecidas no Termo de Referência e seus anexos.

Informamos que a Área Técnica do Cofen respondeu ao questionamento.

QUESTIONAMENTO Nº 1

No Termo de Referência:

Item 8.12.1 - "Os preços inicialmente contratados são fixos e irremovíveis no prazo de um ano contado da data do orçamento estimado."

Desta forma, para efeito de solicitação de reajuste, questionamos: qual a data do orçamento estimado?

RESPOSTA: A pesquisa de preços foi consolidada e apensada ao processo dia 23 de agosto de 2024, conforme art. 33 e § único da Portaria 122/2023 do TCU.

"Art. 33. Independentemente do prazo de duração do contrato, será obrigatória a previsão no edital de índice de reajustamento de preço, com data-base vinculada à data do orçamento estimado.

Parágrafo único. **A data do orçamento estimado mencionada no caput deste artigo refere-se à data em que os dados de pesquisa de preço foram consolidados e juntados aos autos, de forma a evidenciar o preço estimado do produto ou serviço orçado.**" (grifamos)

QUESTIONAMENTO Nº 2

No Termo de Referência:

Item 9.4.4.9 ("c") - *"por não inviabilizar o certame, pelo rol de fabricantes que possuem tais certificações, deverão apresentar"*

A redação da alínea "c", aparentemente, não está completa. Assim, questionamos: qual a exigência deste subitem?

RESPOSTA: Este item pode ser desconsiderado.

QUESTIONAMENTO Nº 3

No Caderno de Especificações Técnicas (Anexo B):

Item 2.6.1 (i) e 6.2 (i) - "Possuir 2 (duas) fontes 100-240VAC sendo pelo menos 1 opção hot-swap."

Gostaríamos de solicitar um esclarecimento sobre o objetivo específico da exigência de fonte hot-swap, considerando que o requisito de alta disponibilidade e redundância de energia pode ser plenamente atendido por soluções com fontes redundantes, ainda que estas não possuam funcionalidade hot-swap.

Entendemos que, quando o equipamento é implantado em um ambiente de cluster ativo-ativo ou ativo-passivo, ele oferece um nível ainda maior de disponibilidade e resiliência. Nessas condições, em caso de manutenção ou falha em um dos dispositivos, o outro assume automaticamente as operações, garantindo a continuidade do serviço sem interrupções. Além disso, essa configuração atende integralmente à necessidade de fontes redundantes, permitindo a operação contínua mesmo em caso de falha de uma das fontes.

Nosso entendimento está correto ao assumir que o equipamento pode atender ao requisito utilizando fontes redundantes, sem a exigência de funcionalidade hot-swap, desde que seja possível sua implementação em modo de alta disponibilidade?

RESPOSTA: Sim, está correto o entendimento.

QUESTIONAMENTO Nº 4

No Caderno de Especificações Técnicas (Anexo B):

Item 2.6.4.24 - "Deve implementar balanceamento entre os links WAN com método Spillover."

Gostaríamos de solicitar esclarecimentos sobre o objetivo da exigência do método específico de balanceamento de carga WAN chamado Spillover, considerando que existem outras metodologias amplamente utilizadas que oferecem resultados semelhantes ou superiores em termos de desempenho, disponibilidade e eficiência na utilização dos links WAN.

Soluções que utilizam métodos de balanceamento de carga avançados, como SD-WAN Policies, que permitem o controle granular do tráfego e oferecem maior flexibilidade para atender às necessidades específicas da rede.

Dado que o objetivo principal do balanceamento é otimizar a utilização dos links WAN e garantir alta disponibilidade, o entendimento está correto ao considerar que soluções que atendem a esses objetivos, ainda que utilizem métodos diferentes de Spillover, podem ser aceitas como equivalentes no cumprimento do requisito?

RESPOSTA: Sim, está correto o entendimento.

QUESTIONAMENTO Nº 5

No Caderno de Especificações Técnicas (Anexo B):

Item do Edital: 2.6.6.23 (c) - "O gateway de email incluso no appliance deve ter pelo menos as seguintes proteções:

1. c) Domain-based Message Authentication, Reporting & Conformance (DMARC)."

Gostaríamos de solicitar um esclarecimento sobre o objetivo do requisito referente ao suporte ao DMARC diretamente no gateway de e-mail incluso no appliance, considerando que o gerenciamento e a aplicação de políticas DMARC, SPF e DKIM são geralmente configurados e gerenciados diretamente nos servidores de e-mail ou serviços de DNS, e não necessariamente no gateway de e-mail do firewall.

O Sophos Firewall permite a configuração de regras avançadas para inspeção e controle do tráfego de e-mail, como análise de cabeçalhos, bloqueio de mensagens não autenticadas e reforço de políticas de segurança, que podem complementar o suporte a DMARC já implementado no servidor de e-mail da organização (como Microsoft 365 ou Google Workspace). Essa abordagem reduz a complexidade operacional, ao mesmo tempo em que garante a segurança esperada.

É correto o entendimento de que o requisito do item pode ser atendido ao complementar as políticas de segurança aplicadas no servidor de e-mail, sem necessidade de soluções adicionais específicas para gerenciamento de DMARC?

RESPOSTA: Sim, está correto o entendimento.

QUESTIONAMENTO Nº 6

No Caderno de Especificações Técnicas (Anexo B):

Item 2.6.7.3 - "O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384."

Gostaríamos de solicitar esclarecimentos sobre a exigência referente ao reconhecimento de todos os algoritmos listados pelo motor de análise de tráfego criptografado. Em particular, gostaríamos de entender o objetivo operacional de incluir algoritmos considerados obsoletos ou inseguros, como RC4, 3DES, IDEA e MD5, que não são recomendados pelas melhores práticas de segurança atuais.

Focar no reconhecimento e análise de algoritmos modernos e amplamente utilizados, como AES128/256, SHA256/384, ECDH/ECDHE/ECDSA, ChaCha20-Poly1305, entre outros, que garantem a compatibilidade com os padrões de segurança atuais e evitam a exposição a vulnerabilidades conhecidas associadas a algoritmos mais antigos.

Nosso entendimento está correto ao considerar que o reconhecimento de algoritmos modernos e seguros é suficiente para atender ao objetivo de análise de tráfego criptografado, mesmo que algoritmos obsoletos ou inseguros, como RC4 e 3DES, não sejam suportados?

RESPOSTA: Sim, está correto o entendimento.

QUESTIONAMENTO Nº 7

No Caderno de Especificações Técnicas (Anexo B):

Item 2.6.12.11 - "Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de rollback de configurações para mudanças indesejadas."

Gostaríamos de solicitar esclarecimentos sobre o objetivo detalhado deste requisito, especialmente em relação à obrigatoriedade de realizar o processo de rollback de configurações diretamente no equipamento.

Entendemos que é possível atender ao objetivo do item ao permitir o registro e controle detalhado das alterações realizadas por usuários administrativos, por meio de logs robustos e completos. Além disso, a exportação de backups de configuração, com a possibilidade de restauração para uma versão anterior em caso de alterações indesejadas, garante a recuperação do estado operacional esperado de forma eficiente e prática.

Dessa forma, o mecanismo de rollback pode ser realizado por meio dos backups, mesmo que não esteja diretamente na interface da gerência centralizada.

Nosso entendimento está correto ao considerar que o registro de alterações administrativas, combinado com a capacidade de restauração a partir de backups manuais, atende ao objetivo do item de gerenciar alterações e reverter configurações, mesmo sem a funcionalidade específica de rollback automático?

RESPOSTA: Sim, está correto o entendimento.

QUESTIONAMENTO Nº 8

No Caderno de Especificações Técnicas (Anexo B):

Item 2.10.2.2 (IX) - "Possuir tecnologia 802.11ac Wave 2."

Gostaríamos de solicitar esclarecimentos sobre o objetivo específico da exigência do padrão 802.11ac Wave 2, considerando que padrões mais avançados, como o 802.11ax (Wi-Fi 6), oferecem benefícios adicionais significativos, como maior capacidade de rede, melhor desempenho em ambientes densos e maior eficiência energética, além de serem totalmente compatíveis com o padrão 802.11ac Wave 2.

Entendemos que o padrão 802.11ax é uma evolução tecnológica que supera a 802.11ac Wave 2, e é totalmente retrocompatível com dispositivos que utilizam este padrão mais antigo. Dado o avanço das tecnologias de Wi-Fi, acreditamos que o objetivo do edital pode ser plenamente atendido ou superado com o uso de soluções baseadas no padrão 802.11ax.

Nosso entendimento está correto ao considerar que soluções baseadas no padrão 802.11ax, com suporte completo ao 802.11ac Wave 2, atendem ou superam os requisitos estabelecidos no edital?

RESPOSTA: Sim, está correto o entendimento. Minimamente deve atender ao descrito no edital, e adicionalmente, novos padrões.

ROGÉRIO WOLNEY LEITE

Chefe da Comissão Permanente de Licitação



Documento assinado eletronicamente por **ROGERIO WOLNEY LEITE - Matr. 579, Chefe da Comissão Permanente de Licitação**, em 09/01/2025, às 10:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.cofen.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0537792** e o código CRC **4C6DF71C**.
