



MUNICÍPIO DE CAÇAPAVA  
SECRETARIA DE ADMINISTRAÇÃO

04/02/2022

ESCLARECIMENTO

Pregão Eletrônico nº. 44/21

**CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE IP DEDICADO PARA ACESSO A INTERNET E INTERLIGAÇÃO DAS UNIDADES CARACTERIZADO POR UM ACESSO DIRETO E DEDICADO PONTO A PONTO VIA FIBRA ÓTICA.**

Referente aos questionamentos dos licitantes, temos a esclarecer:

**PERGUNTA 1** – Dos vícios PRESENTES no ato convocatório: O Edital ora impugnado possui graves vícios e ilegalidades, que ferem os princípios constitucionais e os que regem as contratações públicas, prejudicam a ampla participação e caracterizam o direcionamento do certame, conforme segue: • Aglutinação Explícita e Indevida; • Modalidade de Licitação Incompatível com o Objeto; • Exigência de documento Flagrante Direcionamento para tecnologias específicas. Os vícios ora apontados prejudicam a competitividade e restringem a ampla participação, caracterizando o DIRECIONAMENTO do certame, ferindo os ditames legais e os princípios basilares que orientam as contratações públicas, tornando o Edital nulo, o que, se não sanados em tempo, tais vícios ocasionarão enorme prejuízo não só para a Administração, mas também para as empresas interessadas e para o erário. • O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

**RESPOSTA 1** –Existem atualmente no mercado nacional para livre aquisição. No mínimo 4 (quatro) fabricantes que possuem certificações que atendem ao solicitado e que se enquadram em diferentes tecnologias. A exigência de certificações que está se tornando muito comum, tem evitado que fornecedores desqualificados ou inidôneos tumultuem as licitações. Portanto, sem alteração no edital.

**PERGUNTA 2** –Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes. • Da participação POR VALOR GLOBAL: Algumas empresas não tem como participar de todos os serviços.

**RESPOSTA 2** – O valor global não trará qualquer prejuízo a administração pública, todos os itens têm a mesma natureza técnica, e acarretará os seguintes benefícios: redução dos custos com vários contratos; centralização da responsabilidade do serviço em um único fornecedor, assim não ficando passando para o outro, gerando transtorno e demora na resolução do atendimento, portanto sem alteração do edital.

**PERGUNTA 3** –Devido ao exposto, sugerimos as seguintes alterações: Como estamos dentro de Território Brasileiro e com não temos leis valide tal certificação e sempre levando o princípio da ampla competição que busca sempre incluir o maior número de competidores interessados no objeto licitado. solicitamos que o item seja alterado: De: • O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito

1

Rua Capitão Carlos de Moura, 243, Vila Pantaleão, Caçapava – SP

CEP: 12.280-050 / Tel. (12) 3654-6616 E-mail: secretaria.administração@cacapava.sp.gov.br







MUNICÍPIO DE CAÇAPAVA  
SECRETARIA DE ADMINISTRAÇÃO

certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período, e baseado em normas nacionais e internacionais de segurança da informação. • Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes. Para: Deve ser realizado teste de bancada.

**RESPOSTA 3** – Existem atualmente no mercado nacional para livre aquisição, no mínimo 4 (quatro) fabricantes que possuem certificações que atendem ao solicitado e que se enquadram em diferentes tecnologias. O questionante não deixa explícito o pretendido, informando “Deve ser realizado teste de bancada” ficando dessa maneira impossível de avaliar. Portanto, sem alteração no edital.

**PERGUNTA 4** – CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DA SOLUÇÃO DE FIREWALL de CORE Entendemos que o órgão se pauta nos princípios da transparência e economicidade. Para trazer uma ampliação, principalmente no que tange uma competição mais saudável, o órgão poderia contar com uma oferta mais abrangente de dispositivos caso realize ajustes no termo de referência, proporcionando a participação de equipamentos com melhor custo-benefício e que atende aos requisitos técnicos impostos. Tais equipamentos não impactariam uma futura expansão da infraestrutura. Essa sugestão seguiria os parâmetros de adequação ao interesse público, de economia na aquisição por esse respeitado órgão bem como garantindo o princípio da ampla competição que busca sempre incluir o maior número de competidores interessados no objeto lícitado.

**RESPOSTA 4** – As características desses equipamentos foram dimensionados objetivando o menor custo possível e ao mesmo tempo atender a demanda atual e possíveis incrementos para melhoria da performance da solução, e de fácil acesso para aquisição. Portanto, sem alteração no edital.

**PERGUNTA 5** – Solicitamos a seguinte alteração: De: Throughput de, no mínimo, 750 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Para: Throughput de, no mínimo, 600 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Entendemos que o órgão se pauta nos princípios da transparência e economicidade. Para trazer uma ampliação, principalmente no que tange uma competição mais saudável, o órgão poderia contar com uma oferta mais abrangente de dispositivos caso realize ajustes no termo de referência, proporcionando a participação de equipamentos com melhor custo-benefício e que atende aos requisitos técnicos impostos. Tais equipamentos não impactariam uma futura expansão da infraestrutura. Essa sugestão seguiria os parâmetros de adequação ao interesse público, de economia na aquisição por esse respeitado órgão bem como garantindo o princípio da ampla competição que busca sempre incluir o maior número de competidores interessados no objeto lícitado.





-312  
CP



MUNICÍPIO DE CAÇAPAVA  
SECRETARIA DE ADMINISTRAÇÃO

**RESPOSTA 5** – Essas configurações são mínimas e necessárias, encontradas em diversas marcas, de fácil acesso para aquisição. Portanto, sem alteração no edital.

**PERGUNTA 6** –Solicitamos a seguinte alteração: De: Possuir ao menos interface, 8xGE RJ45 Para: Possuir ao menos interface, 6xGE RJ45 **CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE FIREWALL** •?O antivírus integrado com Anti-Malweres deverá ser executado em até 1.100 (Hum mil e cem) equipamentos (Microcomputadores e Notebooks) sem depender de um ponto concentrador da CONTRATANTE para sua distribuição, ou seja, deverá ser disponibilizado através do Firewall baixando das nuvens. Entendemos que o item supracitado trata de Antivírus de endpoint destoando completamente do Objeto do Certame. Caso seja do interesse do órgão a aquisição de tal solução sugerimos que seja licitando a solução de segurança para endpoint em um lote separado removendo assim tal exigência no lote de NGFW; **CARACTERÍSTICAS DIVERSAS** Item: Deve ter suporte à proteção e identificação de hosts possivelmente infectados com "botnets". A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

**RESPOSTA 6** – O Hardware solicitado de 8 portas RJ45, foi dimensionado para possíveis aumentos de demanda tecnológica, tendo o melhor custo-benefício para essa finalidade. Portanto, sem alteração no edital.O Antivírus faz parte integrante da solução da segurança das bordas e do core, uma vez chegando aos equipamentos via firewall, trará uma economia significativa ao município, sendo assim, devendo permanecer no mesmo lote e não destoa do objeto.

**PERGUNTA 7** –Entendemos que o item supracitado trata de Antivírus de endpoint destoando completamente do Objeto do Certame. Caso seja do interesse do órgão a aquisição de tal solução sugerimos que seja licitando a solução de segurança para endpoint em um lote separado removendo assim tal exigência no lote de NGFW; Item: Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques dos (denial-of-service) e DDoS devidamente licenciados. Entendemos que o item de DDoS deve ser um serviço Ofertado por Operadas para que tenha eficiência. Solicitamos que o item supracitado seja alterado para: Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques dos (denial-of-service) Item: Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica. Solicitamos a alteração para: Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. Como estamos dentro de Território Brasileiro e com não temos leis valide tal certificação e sempre levando o princípio da ampla competição que busca sempre incluir o maior número de competidores interessados no objeto licitado. solicitamos que o item seja alterado:

**RESPOSTA 7** – O Antivírus faz parte integrante da solução da segurança devendo permanecer no mesmo lote que faz parte integrante do objeto, as configurações exigidas são necessárias para maximização dos seus recursos. Portanto, sem alteração no edital.







MUNICÍPIO DE CAÇAPAVA  
SECRETARIA DE ADMINISTRAÇÃO

**PERGUNTA 8** –De: O fabricante ou o produto deve possuir certificado ICISA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICISA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período, e baseado em normas nacionais e internacionais de segurança da informação. Para: Deve ser realizado teste de bancada Levando o princípio da ampla competição que busca sempre incluir o maior número de competidores interessados no objeto licitado. solicitamos que os itens abaixo sejam removidos • A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android. • Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego. • A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

**RESPOSTA 8** – A questionante não deixa explícito o pretendido, informando “Deve ser realizado teste de bancada” ficando dessa maneira impossível de avaliar. As configurações exigidas são necessárias para maximização dos seus recursos. Portanto, sem alteração no edital.

**PERGUNTA 9** –Levando o princípio da ampla competição que busca sempre incluir o maior número de competidores interessados no objeto licitado. solicitamos que os itens abaixo sejam alterados De: Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream. Para: Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança De: A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH. Para: A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS

**RESPOSTA 9** – As configurações foram dimensionadas para otimização da solução. Portanto, sem alteração no edital.

**PERGUNTA 10** –PROTEÇÃO CONTRA ATAQUES AVANÇADOS Para detectar melhor as APTs (advanced persistent threat), muitos fabricantes de segurança estão implantando tecnologias de detecção de ameaça avançadas que, muitas vezes, incluem sandboxes virtualizados, que analisam o comportamento de arquivos suspeitos e detectam malwares ocultos anteriormente desconhecidos. No entanto, as ameaças estão ficando mais inteligentes e várias técnicas de sandbox dos fornecedores simplesmente não as acompanharam. Muitas vezes as soluções de SANDBOX não chegam a uma conclusão de análise de um ATP até que ele já tenha entrado no perímetro da rede. O Malware moderno, está agora sendo projetado para detectar a presença de um sandbox virtual e evitar a descoberta, limitando a eficácia das tecnologias de sandbox de primeira geração. As soluções de sandbox de mecanismo único apresentam um destino particularmente fácil para técnicas de evasão. Além disso, as técnicas de mecanismo único criam lacunas de análise. Por exemplo, as análises que buscam chamadas entre aplicativos e sistemas operacionais podem ser menos granulares do que as análises que buscam chamadas entre hardware e sistemas operacionais, já que a maioria dessas chamadas está oculta das camadas de aplicativos. Diante dos fatos acima mencionados indicamos que o Órgão busque um segundo







MUNICÍPIO DE CAÇAPAVA  
SECRETARIA DE ADMINISTRAÇÃO

lote com foco em SANDBOX, pois tratará com maior economicidade o pleito de Firewall UTM. Pois conforme esclarecemos acima soluções embarcadas de SANDBOX podem não ser eficientes. Devido aos itens expostos solicitamos a remoção dos seguintes itens: • Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android. • A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas. • Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados. • A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede). • Suporte a submissão manual de arquivos para análise através do serviço de Sandbox

**RESPOSTA 10** – Foi questionado o uso de solução de SANDBOX no descritivo, mas solicita uma solução de SANDBOX sem detalhar seus novos mecanismos de detecção e proteção, sendo assim não apresenta condições para avaliação. Os requisitos solicitados no edital utilizando plataforma de nuvem, até o momento são suficientes para nós prover de segurança cibernética necessária e com baixo custo, portanto não será necessário uma complementação dessa solução. E um eventual segundo lote seria desnecessário e só acarretaria mais custo para a implantação do objeto, dessa maneira onerando os cofres públicos sem necessidade. Portanto, sem alteração no edital.

**PERGUNTA 11 –CARACTERÍSTICAS DE ADMINISTRAÇÃO** Entendemos que para melhor administração a solução a administração deve ser feita via Browser independentemente da plataforma ou sistema operacional. Pelo motivo exposto solicitamos a remoção dos seguintes itens: A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android. • O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB. • O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW. • O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW. • O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW. • O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS. • O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

**RESPOSTA 11** – Adequação atendida. Será alterado no Termo de Referência e edital.

**PERGUNTA 12 –SOLUÇÃO PARA PROTEÇÃO AVANÇADA DE ENDPOINTS** Levando o princípio da ampla competição que busca sempre incluir o maior número de competidores interessados no objeto licitado e tendo em vista a existência de várias empresas especializadas e desenvolvedoras de soluções de proteção avançada de endpoint. solicitamos que a solução de proteção avançada de endpoint seja tratada em um lote separado e não vinculada a solução de NGFW.

**RESPOSTA 12** – A proteção de endpoints faz parte integrante da solução da segurança do objeto, uma vez que chega aos equipamentos através de link de Internet entre outras situações, existem no mínimo 3 (três) fabricantes independentes de softwares de endpoints disponíveis no mercado nacional para







MUNICÍPIO DE CAÇAPAVA  
SECRETARIA DE ADMINISTRAÇÃO

comercialização, permanecendo no mesmo lote, acarretará economia de recursos financeiros e administrativos, abreviamento do atendimento a solicitação de suporte, onde somente uma empresa se encarregará de sincronizar seus dispositivos e resolver em um curto período de tempo, não ficando a Prefeitura indo para um lado e para o outro para resolver a sua solicitação. sendo assim, deverá permanecer no mesmo lote, não destoando do objeto. Portanto, sem alteração no edital.

**PERGUNTA 13** – Que seja admitida a subcontratação de eventual serviço necessário ao atendimento do objeto (conforme autorizada pelo artigo 72 da Lei 8.666/93), de maneira clara e coerente, tornando possível atendimento por várias empresas.

**RESPOSTA 13** – Informamos que neste instrumento convocatório não é permitida a subcontratação, mantendo-se da mesma forma o edital.

**PERGUNTA 14** – Verifica-se que o Anexo IX apresenta planilha contendo os itens objetos de contrato com seus respectivos quantitativos. No que tange a pretensão de Bordas Com Proteção de Endpoints Avançada e Gerenciamento Centralizado o Anexo descreve quantitativo para “Solução em Endpoint Detection and Response 500 unidades” e “Gerenciamento em Cloud Centralizado 1 unidade”. Contudo, não foi observado a inserção dos itens nas planilhas de preços dispostas no Anexo I, impossibilitando a elaboração de proposta de preços pelas empresas interessadas em participar do certame. A especificação de todos os itens objetos de contrato em planilha detalhada de preços, é necessária não apenas para a análise de viabilidade de atendimento pelas empresas como também para que, no curso do certame, se possa verificar eventual exequibilidade dos preços propostos, inclusive em relação a todos os componentes que repercutem na formação do preço final. Deste modo, solicitamos que o edital seja aditado com inclusão dos itens em planilha de preços.

**RESPOSTA 14** – Será adequado o TR e Edital.

**PERGUNTA 15** – O Anexo IX do edital aponta a infraestrutura necessária para a contratação, destacando aos serviços de monitoramento que: “Os processos utilizados pela equipe do SOC devem seguir as melhores práticas de mercado. O ITIL (Information Technology Infrastructure Library), ISO 27001 (Information security incident management) deve ser utilizados como modelos de referência pelo SOC para operação e gerenciamento de processos e serviços de TI”. E, dentre as características diversas, destaca: • O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação. • Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes. No entanto, os itens do edital não deixam claro o momento em que tais







MUNICÍPIO DE CAÇAPAVA  
SECRETARIA DE ADMINISTRAÇÃO

documentos deverão ser apresentados pelos licitantes, restando dúvidas se seriam documentos exigíveis para comprovação de habilitação das licitantes. Desta forma, o edital deve ser esclarecido quanto ao momento em que os documentos transcritos deverão ser fornecidos, de modo a não haver dúvidas na contratação.

**RESPOSTA 15** – Conforme item 2.6 do presente TR será apresentado na assinatura de contrato.

**PERGUNTA 16** – Verifica-se que a Cláusula 4.2 da Minuta de contrato estabelece que ao pagamento não caberá “qualquer reajuste financeiro”. Todavia, tendo em vista que a Cláusula 5.2 prevê a possibilidade de prorrogação do contrato, é inadmissível que durante todo esse lapso temporal não ocorra o reajuste do preço, sob pena dos valores sofrerem depreciação e causarem prejuízos à contratada. Desta forma, devem ser aditados o edital de modo a indicar a possibilidade de reajuste dos valores do contrato, a cada 12 (doze meses), com base no índice autorizado pela ANATEL para as concessionárias prestadoras do serviço objeto de contrato.

**RESPOSTA 16** – Informamos que o item 4.2 refere-se a parcelas em atraso, que não caberá reajuste, no item 12 prevê tal possibilidade.

**PERGUNTA 17** – O edital apresenta previsões divergentes acerca do prazo para instalação da solução, sendo previsto no Anexo IX, o prazo de 30 (trinta) dias: A implantação da solução de hardware e software deverá ser realizada no prazo de até 30 dias para Internet e 60 dias para Firewall e VPN/MPLS/PONTA A PONTA contados a partir da emissão da ordem de serviço seguindo um cronograma de instalação informado pela CONTRATANTE. Contudo, a Cláusula 3.4 do Anexo VIII estabelece prazo de até 90 (noventa) dias: 3.4 - O prazo de instalação, configuração e início de operação efetiva de todos os recursos necessários à prestação do serviço contratado é de até 90 (noventa) dias a partir da assinatura do contrato entre a Prefeitura e a Contratada. Ora, para garantir a efetiva implantação da solução é necessária mão-de-obra especializada e avaliação das condições do local, além do fornecimento de equipamentos que dependem da disponibilidade pelos fabricantes, o que, necessita de maior lapso temporal para efetivo cumprimento da obrigação. Contudo, a divergência de informações inviabiliza a análise de viabilidade de atendimento pelas empresas interessadas em participar do certame. Assim, solicitamos seja suprida a divergência apontada com indicação e prazo único para implantação da solução.

**RESPOSTA 17** – Feita a correção, 90 dias, em acompanhamento ao TR.

**PERGUNTA 18** – A licitação constitui um procedimento que se destina precipuamente, nos termos do artigo 3.º da lei 8666/1993, a estabelecer a observância do princípio da isonomia entre os potenciais fornecedores e a selecionar a proposta mais vantajosa para a Administração. Tais objetivos não podem ser considerados isoladamente, devendo ambos se interpenetrar para configurar uma proposta administrativa adequada a tais pressupostos. Neste contexto, o edital estabelece condições e especificações que merecem ser esclarecidas ou alteradas, conforme o caso, a fim de garantir a possibilidade de adimplemento das obrigações e a competitividade no certame. Abaixo, transcrevem-se os itens questionados e, em seguida, os comentários e requerimentos pertinentes: ANEXO IX 4.19





