Governo do Distrito Federal
Defensoria Pública do Distrito Federal
Unidade de Inovação, Tecnologia da Informação e Comunicação
Diretoria de Infraestrutura de Rede

Despacho – DPDF/DPG/ASSESP/UNITIC/DIRE Brasília, 28 de dezembro de 2023.

À Unidade de Licitação (UNILIC),
Diretoria de Licitação (DILIC),

Assunto: Análise da Documentação referente ao Pregão Eletrônico nº 22/2023-DPDF

Com os cordiais cumprimentos, reportamo-nos ao Documento 129976132, cujo teor consiste na documentação enviada pela licitante, a fim de comprovar o atendimento aos requisitos previstos na Tabela de Conformidade Técnica, conforme Item 9.2.5 do Termo de Referência.

1. DA ANÁLISE DA TABELA DE CONFORMIDADE TÉCNICA

1.1. A licitante enviou a Tabela de Conformidade Técnica em desconformidade ao Item 9.2.5 do Termo de Referência, peça integrante do Edital do Pregão Eletrônico nº 22/2023-DPDF;

1.2. A licitante enviou em planilha, conforme consta na página n° 14 do documento Proposta + Documentação Complementar (129976132);

1.3. Ao analisar a planilha ponto a ponto, bem como os links enviados pela licitante, **foram encontradas inconsistências e link's que não comprovam o atendimento DAS ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS.**

1.4. Tendo em vista a documentação analisada, a licitante não comprovou através da documentação em análise os seguintes itens:

1.4.1. *11.1.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW).*

1.4.2. *11.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.*

1.4.3. *11.1.3. Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.*

1.4.4. *11.1.4. Define-se o termo "appliance" como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço.*

1.4.5. *11.1.5. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de "appliance" que utilizam hardware e software de fabricantes diferentes.*

1.4.6. *11.1.6. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.*

1.4.7. *11.1.7. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.*

1.4.8. *11.1.30. Detectar e bloquear a origem de portscans.*

1.4.9. *11.1.31. Deve permitir o bloqueio de ataques.*

1.4.10. *11.1.32. Deve permitir o bloqueio de exploits conhecidos.*

1.4.11. *11.1.36. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de*

endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

1.4.12. *11.1.44. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.*

1.4.13. *11.1.45.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Antivírus e Anti-Bot integrado ao próprio appliance de segurança;*

1.4.14. *11.1.45.2. A solução de Antivírus integrada deve ter capacidade de analisar arquivos de até ao menos 150 MB de tamanho;*

1.4.15. *11.1.45.3. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;*

1.4.16. 11.1.45.5. Implementar funcionalidade de detecção e bloqueio de “call-backs”;

1.4.17. 11.1.45.7. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP;

1.4.18. 11.1.46.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

1.4.19. 11.1.46.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar, pelo menos, arquivo PDF com até 10Mb;

1.4.20. 11.1.46.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

1.4.21. 11.1.46.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

1.4.22. 11.1.46.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

1.4.23. 11.1.46.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde esta seja responsável por atualizar toda a base de segurança dos appliances através de assinaturas;

1.4.24. 11.1.46.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

1.4.25. 11.1.46.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

1.4.26. 11.1.46.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

1.4.27. 11.1.46.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;

1.4.28. 11.1.46.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro;

1.4.29. 11.1.46.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

1.4.30. 11.1.46.23. Mitigar ameaças de dia zero via tráfego de internet;

1.4.31. 11.1.46.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;

1.4.32. 11.1.46.25. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado;

1.4.33. 11.1.46.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo;

1.4.34. 11.1.46.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

1.4.35. 11.1.46.28. Conter e mitigar exploits avançados;

1.4.36. 11.1.46.29. 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 a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Antivírus e AntiSpyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

1.4.37. 11.1.46.31. As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real;

1.4.38. 11.1.47.6. Deve permitir submissão de novos sites para categorização;

1.4.39. 11.1.47.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

1.4.40. 11.1.48.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Linux, de forma simultânea;

1.4.41. 11.1.48.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API;

1.4.42. 11.1.48.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW;

1.4.43. 11.1.49.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto;

1.4.44. 11.1.49.21. O monitoramento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW;

1.4.45. 11.1.49.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW;

1.4.46. 11.1.49.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW;

1.4.47. 11.1.49.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS;

1.4.48. 11.4.1. Deve fornecer solução de gerenciamento centralizado para todos os dispositivos e recursos da solução.

1.4.49. 11.4.2. A solução poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos firewalls, não sendo aceita solução de software livre.

1.4.50. 11.4.3. Caso seja entregue em appliance virtual, dever ser compatível com VMware ESXi ou Hyper-V.

1.4.51. 11.4.4. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções dos usuários da console que determinem:

1.4.52. 11.4.4.1. Grupos de firewalls permitidos;

1.4.53. 11.4.4.2. Funcionalidades permitidas por firewall ou grupo de firewalls de acordo com o perfil de uso designado;

1.4.54. 11.4.4.3. Perfil de nível de acesso (escrita, leitura, administração, relatórios);

1.4.55. 11.4.5. Deve suportar organizar os dispositivos administrados em grupos. Estes grupos devem permitir isolamento tanto de acesso para os administradores como de configuração massiva ou individual.

1.4.56. 11.4.6. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular ou em grupos de firewalls.

1.4.57. 11.4.7. Deve apresentar estado dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

1.4.58. 11.4.8. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

1.4.59. 11.4.9. O gerenciamento deve permitir/possuir:

1.4.60. 11.4.9.1. Criação e administração de políticas de firewall e controle de aplicação;

1.4.61. 11.4.9.2. Monitoramento de logs;

1.4.62. 11.4.9.3. Investigação de eventos de segurança e falhas (debugging);

1.4.63. 11.4.9.4. Acesso concorrente de administradores, conforme políticas e perfis previamente definidos;

1.4.64. 11.4.10. Deve permitir o provisionamento e configuração sem intervenção de operadores (Zero-Touch). Os firewalls devem se conectar automaticamente à plataforma de gerência, e a partir desta conexão receberem as configurações previamente determinadas pelos operadores da plataforma.

1.4.65. 11.4.11. A solução de gerenciamento deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL.

1.4.66. 11.4.12. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

1.4.67. 11.4.13. A solução deve possuir tela situacional com todo inventário de firewalls gerenciados de forma centralizada, informando no mínimo para o administrador:

1.4.68. 11.4.13.1. Id (nome) do firewall;

1.4.69. 11.4.13.2. Número de série;

1.4.70. 11.4.13.3. Modelo do equipamento;

1.4.71. 11.4.13.4. Versão do firmware e estado da conectividade do equipamento com a gerência em online ou offline;

1.4.72. 11.4.14. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez.

1.4.73. 11.4.15. Deve centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento, possibilitando comparação de configurações que evitem sobreposição de regras e conflitos de configuração.

1.4.74. 11.4.16. A solução deve possuir Dashboard com sumario de alertas e informação de status de licença.

1.4.75. 11.4.17. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo.

1.4.76. 11.4.18. Deve manter um canal de comunicação segura, com encriptação baseada em HTTPS, entre todos os componentes que fazem parte da solução de firewall e gerência.

1.4.77. 11.4.19. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade de o administrador utilizar endereço IP do dispositivo, URL ou FQDN.

1.4.78. 11.4.20. A solução deve permitir a criação de modelos de configuração (templates) para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls.

1.4.79. 11.4.21. A solução deve possibilitar a geração de templates de configuração à partir da configuração vigente em um firewall selecionado pelo administrador da plataforma, e possibilitar que este template possa ser editado e utilizado em outros firewalls gerenciados pela plataforma.

1.4.80. 11.4.22. Os modelos de configuração (templates) devem suportar configurações de interfaces físicas ou virtuais.

1.4.81. 11.4.23. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

1.4.82. 11.4.24. Deverá permitir visualizar a diferença nas mudanças antes que as configurações sejam implantadas.

1.4.83. De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento.

1.4.84. 11.4.26. Deve incluir console de configuração e monitoramento SD-WAN, possibilitar a criação de políticas SD-WAN em todos os elementos gerenciados, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

1.4.85. 11.4.27. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

1.4.86. 11.4.28. Durante as alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

1.4.87. 11.4.29. A solução deve oferecer monitor de auditoria de configurações aplicadas aos firewalls gerenciados pela plataforma, permitindo comparativo diferencial entre registros para rápida identificação de configurações e alterações aplicadas.

1.4.88. 11.4.30. A solução deve oferecer módulo centralizado que possibilite realização e armazenamento de backup de configurações dos firewalls gerenciados.

1.4.89. 11.4.31. A solução deve oferecer possibilidade de auditoria de configurações.

1.4.90. 11.4.32. A solução deve possibilitar o monitoramento em tempo real dos firewalls gerenciados, informando minimamente:

1.4.91. 11.4.32.1. Utilização de CPU/Processamento;

1.4.92. 11.4.32.2. Aplicações em uso e seu consumo de banda;

1.4.93. 11.4.32.3. Interfaces em uso e utilização de banda;

1.4.94. 11.4.32.4. Conexões concorrentes em uso;

1.4.95. 11.4.33. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls.

1.4.96. 11.4.34. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a geração de relatórios e monitoramento em tempo real.

1.4.97. 11.4.35. A solução deverá prover relatórios com no mínimo histórico de 365 dias.

1.4.98. 11.4.36. A solução deverá prover relatórios referente as atividades dos usuários.

1.4.99. 11.4.37. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações:

1.4.100. 11.4.37.1. Nome da aplicação;

1.4.101. 11.4.37.2. Quantidade de conexões;

1.4.102. 11.4.37.3. Percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados;

1.4.103. 11.4.38. A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações:

1.4.104. 11.4.38.1. Nome do usuário;

1.4.105. 11.4.38.2. Quantidade de conexões;

1.4.106. 11.4.38.3. Percentual que tráfego do usuário representa na rede;

1.4.107. 11.4.38.4. Quantidade de Megabytes trafegados;

1.4.108. 11.4.39. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações:

1.4.109. 11.4.39.1. Endereço IP;

1.4.110. 11.4.39.2. Quantidade de conexões;

1.4.111. 11.4.39.3. Percentual que tráfego que o IP representa na rede;

1.4.112. 11.4.39.4. Quantidade de Megabytes trafegados;

1.4.113. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede.

1.4.114. 11.4.41. A solução deverá arquivar relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF.

1.4.115. 11.4.42. A solução deverá permitir geração e envio agendado de relatórios.

1.4.116. 11.4.43. A solução deve permitir a customização de alertas e notificações, possibilitando o envio de e-mail com as informações relativas a este evento.

1.4.117. 11.4.44. A solução deve possibilitar configuração e monitoramento centralizados de VPNs entre os firewalls gerenciados.

1.4.118. 11.4.45. A solução deve apresentar consoles de indicação com os principais eventos, riscos e ameaças contendo:

1.4.119. 11.4.45.1. Aplicações de maior risco, e volume de dados consumido por estas;

1.4.120. 11.4.45.2. Aplicações de maior utilização, por volume de dados transferidos e conexões consumidas;

1.4.121. 11.4.45.3. Aplicações de maior utilização, por categoria;

1.4.122. 11.4.46. A solução deve apresentar consoles de indicação dos principais usuários contendo:

1.4.123. 11.4.46.1. Usuários utilizando mais conexões;

1.4.124. 11.4.46.2. Usuários consumindo mais dados;

1.4.125. 11.4.47. A solução deve apresentar console de indicação de:

1.4.126. 11.4.47.1. Virus/Spyware bloqueados;

1.4.127. 11.4.47.2. Intrusões bloqueadas;

1.4.128. 11.4.47.3. Botnets bloqueados;

1.4.129. 11.4.47.4. Origens e destinos mais utilizados;

1.4.130. 11.4.48. A solução deve apresentar console de indicação de Aplicações indicando:

1.4.131. 11.4.48.1. Aplicações identificadas;

1.4.132. 11.4.48.2. Categorização e uso das aplicações;

1.4.133. 11.4.48.3. Risco das aplicações;

1.4.134. 11.4.49. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:

1.4.135. 11.4.49.1. Lista de eventos correlacionados com opção de navegação "drilldown"; ou

1.4.136. 11.4.49.2. Modo gráfico; ou

1.4.137. 11.4.49.3. Lista de logs;

1.4.138. 11.4.50. A solução deve apresentar console de monitoramento de atividade dos usuários, indicando suas características de navegação por meio das URL´s e categorias de serviços mais acessadas.

1.4.139. 11.4.51. A solução deve permitir visualização de topologia do firewall e elementos a ele conectados (dispositivos de rede complementares, dispositivos de usuários, Access Points).

A documentação e os link's fornecidos pela licitante, limitaram-se a trazer informações genéricas sobre o portfólio do fabricante, sem apontar diretamente para os itens fornecidos na proposta.

A solução oferecida na proposta não atende integralmente os Itens 16.1 e 16.2 referentes a Transição Contratual e Transferência de Conhecimento da Tecnologia.

Os itens foram objetos de questionamento, conforme observado abaixo:

> "Em relação aos itens 16.1 e 16.2 do Termo de Referência, que abordam a transferência de conhecimento técnico e documentação pela Contratada à DPDF, visando capacitar a equipe técnica para o perfeito funcionamento da infraestrutura de TIC, gostaríamos de confirmar a necessidade de sustentabilidade e autonomia operacional após o término do contrato. Assim, entendemos que os equipamentos NGFW especificados no item 11.1.ESPECIFICAÇÕES TÉCNICAS COMUNS devem ser fornecidos com funcionalidades de Controle de Aplicação, IPS e Antivírus em caráter permanente. Estas funcionalidades devem ser utilizáveis por tempo indeterminado, com a base de assinaturas disponíveis até o final do contrato, independente de renovação de suporte e garantia do fabricante. Esse entendimento está alinhado com os objetivos do edital?"

> "Resposta: Sim, o entendimento está correto. Conforme os itens 16.1 e 16.2 do Termo de Referência, é essencial que a DPDF adquira todo o conhecimento e documentação necessários para manter a infraestrutura de TIC disponível e íntegra após o término do serviço contratado. Assim, os equipamentos NGFW especificados no item 11.1.ESPECIFICAÇÕES TÉCNICAS COMUNS devem ser fornecidos com as funcionalidades de Controle de Aplicação, IPS e Antivírus de forma permanente. Esta providência assegura que a DPDF possa continuar a usar efetivamente essas funções críticas de segurança com a base de assinaturas disponíveis até o final do contrato e, idealmente, além deste período, mesmo sem a renovação de suporte e garantia do fabricante. Esta abordagem garante a continuidade e a integridade da segurança na infraestrutura da DPDF."

Ao consultar o link fornecido pela licitante https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-security_services.pdf (pg. 17), observa-se a seguinte redação:

> "Gateway Anti-Virus Expiration Date indicates the date when the SonicWall Gateway Anti-Virus service expires. If your SonicWall Gateway Anti-Virus subscription expires, the SonicWall IPS inspection is stopped and the SonicWall Gateway Anti-Virus configuration settings are removed from the SonicWall network security appliance. These settings are automatically restored after renewing your SonicWall Gateway Anti-Virus license to the previously configured state."

Tradução Livre

> "A data de expiração do Gateway Anti-Virus indica a data em que o serviço SonicWall Gateway Anti-Virus expira. Se a sua assinatura do SonicWall Gateway Anti-Virus expirar, a inspeção do SonicWall IPS é interrompida e as definições de configuração do SonicWall Gateway Anti-Virus são removidas do dispositivo de segurança de rede SonicWall. Essas definições são restauradas automaticamente após a renovação da licença do SonicWall Gateway Anti-Virus para o estado configurado anteriormente."

A solução não atende integralmente ao Item 11.1.20.

O item foi objeto de questionamento, conforme observado abaixo:

> Questionamento 1:
> "Em referência do item 11.1.20."Deve suportar modo misto de trabalho Sniffer em L2 e L3". Entendemos que a solução ofertada poderá realizar essa separação diretamente no mesmo appliance mesmo em cluster. Está correto nosso entendimento?
>
> Resposta: Não, o entendimento não está correto. Conforme o item 11.1.20, é necessário que a solução suporte modo misto de trabalho Sniffer em L2 e L3, e isso implica a necessidade de contextos virtuais no mesmo appliance, mesmo em um ambiente de cluster. A
> exigência de contextos virtuais é crucial para garantir a eficácia e a flexibilidade da solução em diferentes cenários e configurações de rede. Especificamente, a implementação de pelo menos dois contextos virtuais no mesmo dispositivo sem custo adicional, é essencial para manter a separação e a segurança dos diferentes fluxos de tráfego que estão sendo monitorados e analisados. Esses contextos
> virtuais permitem a operação simultânea de múltiplas funções de segurança e monitoramento, sem comprometer o desempenho, mesmo em cluster, no equipamento como um todo. Portanto, qualquer solução proposta deve atender a especificação técnica, com no mínimo dois contextos virtuais no mesmo dispositivo.

Ao consultar o link fornecido pela licitante https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-gen-7-nssp-series.pdf (pg. 2), observa-se a seguinte redação:

> ***Multi-instance Firewall (only for NSsp 15700)***
>
> *Multi-instance is the next generation of multi-tenancy*

Each tenant is isolated with dedicated compute resources to avoid resource starvation

It features physical and logical ports/tenants

It supports independent tenant policy and configuration management

Leverage version independence and High Availability (HA) support for tenants

Os modelos ofertados na proposta, **NSa 4700 e NSa 5700**, não suportam Multi-Instance, conforme revela o documento fornecido no link supracitado.

Após extensa análise referente aos documentos fornecidos pela licitante a área técnica de tecnologia da informação da Defensoria chegou a entendimento que os modelos oferecidos na proposta não estão aderentes ao objeto do Pregão Eletrônico nº 22/2023-DPDF, conforme Anexo VI - Tabela de Conformidade Técnica dos Produtos.

Este é o relatório.

Atenciosamente,

Documento assinado eletronicamente por **DIEGO DE SOUSA MATOS - Matr.0242303-0**, **Diretor(a) de Infraestrutura de Redes**, em 28/12/2023, às 11:05, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **WILLIAM DA SILVA GANZELA - Matr.0254297-8**, **Analista de Apoio à Assistência Judiciária**, em 28/12/2023, às 11:07, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **130186148** código CRC= **FF294671**.