PROCESSAMENTO DE DADOS AMAZONAS S.A

RESPOSTA AO RECURSO ADMINISTRATIVO

Referência : Pregão Eletrônico-SRP nº **09/2022**
Assunto : Recurso Administrativo
Objeto : Contratação de empresa especializada para prestação de serviços de natureza continuada, especializada em gerenciamento de segurança lógica, no modelo 24hs por dia, 7 dias por semana, 365 dias por ano, incluindo o conjunto de hardware e software, fornecidos em regime de comodato, conforme especificações detalhadas no Termo de Referência, constante do Anexo I, deste Instrumento convocatório.

Recorrente:

NCT INFORMÁTICA LTDA.

Recorrida:

NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.

1 CONSIDERAÇÕES GERAIS

1.1 Trata-se de análise de Recurso interposto em face da decisão do Pregoeiro de desclassificar do certame a licitante NCT INFORMATICA LTDA. e declara vencedora da disputa a licitante NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.

1.2 Razões e contrarrazões encontram-se disponíveis para consulta, **na íntegra**, no portal de compras do Governo Federal, site: www.gov.br/compras/pt-br e transparência da PRODAM, site https://www.prodam.am.gov.br/licitacoes/pregoes/

2 DA TEMPESTIVIDADE

2.1 No Pregão Eletrônico, a manifestação da intenção de recorrer deve ser apresentada em campo específico no sistema Comprasnet, sítio de compras do governo, que se oportuniza a partir da habilitação da última proposta ou o cancelamento dos itens, logo após se abrir o prazo para interposição de intenção recursos.

2.2 Desta feita, havendo registrada prévia e motivada intenção de recorrer, e, sendo-lhe aceita, inicia-se a contagem do prazo legal para apresentação das razões recursais, que é de 3 (três) dias úteis, sendo igual o prazo para apresentação das contrarrazões.

2.3 A intenção de recurso da empresa NCT INFORMÁTICA LTDA. foi aceita e esta apresentou TEMPESTIVAMENTE as razões recursais.

2.4 A empresa: NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA. apresentou TEMPESTIVAMENTE as contrarrazões recursais.

3 DO RECURSO

3.1 No mérito, a empresa NCT INFORMÁTICA LTDA. apresentou, em síntese, os seguintes pontos a serem analisados, os quais transcrevo em partes, não detalhando a resposta a cada item do edital:

3.1.1 O edital de licitação trata da “contratação de empresa especializada para prestação de serviços de natureza continuada, especializada em gerenciamento de segurança lógica, no modelo 24hs por dia, 7 dias por semana, 365 dias por ano, incluindo o conjunto de hardware e software, fornecidos em regime de comodato”. O que se pretende contratar, portanto, é a prestação de um serviço, sem fornecimento de bens à Administração, cabendo ao futuro contratado prover toda a infraestrutura de hardware e software necessária para o atendimento do objeto.

3.1.2 A proposta da NCT tinha o valor de R$ 2.449.000,00. No entanto, após o exame técnico que, s.m.j., não avaliou corretamente o que se ofertava à Administração, foi excluída da disputa, com a convocação da segunda colocada no certame. Ao fim e ao cabo, a PRODAM optou por aceitar a oferta final da recorrida, após negociação, no valor de R$ 3.295.529,30, com um gasto a maior de cerca de R$ 850 mil.

3.1.3 A recorrente alega que proposta da NCT atende inteiramente o edital e que a proposta da NTSEC descumpre ela própria requisitos técnicos claros.

3.1.4 Para demonstrar o pleno atendimento a todas as condições do edital, serão indicados, abaixo, os itens apontados pela PRODAM como descumpridos pela recorrente, com a explicação ao lado dos motivos pelos quais a proposta é plenamente aderente ao instrumento de convocação da licitação.

3.1.5 Destacamos que todos os links e documentos foram apresentados e, mais uma vez, que se trata de serviços, motivo pelo qual a obrigação quanto ao cumprimento daquilo que se demanda é da Contratada. Quanto às exigências, a PRODAM poderia ter diligenciado, conforme preceitua o próprio edital.

3.1.6 (...)

3.1.7 E, para arrematar, não se deve esquecer que a proposta da recorrente representa a MELHOR OFERTA DE PREÇO PARA A ADMINISTRAÇÃO, o que deve ser valorizado na apreciação do tema. Nesse sentido, no Acórdão 3381/2013-Plenário, inserido no Informativo de Licitações e Contratos n. 180, do Tribunal de Contas da União, aquela Corte de Contas destaca a relevância da proposta mais vantajosa, o que não pode ser desconsiderado:

3.1.7.1 O disposto no caput do art. 41 da Lei 8.666/93, que proíbe a Administração de descumprir as normas e o edital, deve ser aplicado mediante a consideração dos princípios basilares que norteiam o procedimento licitatório, dentre eles o da seleção da proposta mais vantajosa. (...) Acórdão 3381/2013-Plenário, TC 016.462/2013-0, relator Ministro Valmir Campelo, 4.12.2013.

3.1.8 A oferta da NCT significa uma economia de quase um milhão de reais, e trata de um produto líder de mercado, com inegável capacidade de atender à demanda da Administração Pública.

3.1.9 Quanto a esse ponto, é no mínimo estranho, por assim declarar, que fabricante líder do Gartner e detentor da maior parcela de soluções de segurança implementadas no Brasil, assumindo essa posição em 2020. Fonte: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/fortinet-consolida-liderazgo-en-2020-de-dispositivos-de-ciberseguridad-en-america-latina, não consiga atender tecnicamente a PRODAM-AM, considerando que atende a diversos órgãos, bancos, empresas, agências, dentre outros.

3.1.10 Por todas essas razões, impõe-se o provimento do recurso e a reforma da decisão que desclassificou a proposta da recorrente.

3.1.11 Além da análise indevida da proposta da recorrente, há, também, clara aceitação de oferta que, esta sim, não cumpre o edital, que é o equipamento proposto pela NTSEC. Inicialmente, a oferta da NTSEC não informou os partnumbers das Gibcs, conforme seria exigido para demonstrar cumprimento ao item 2.18 do Anexo 1-A.

3.1.12 A oferta realizada foi dos partnumbers CPAC-4-10F-C - 4 Port 10GBase-F SFP+ interface card. Compulsando a lista de produtos da Checkpoint, contudo, vê-se que deveriam ter sido ofertados os seguintes partnumbers: CPAC-TR-10SR-C - SFP+ transceiver module for 10G fiber ports - short range (10GBase-SR).

3.1.13 Seguindo, foi descumprido claramente o item 52 do edital, que trata do seguinte: “52. Deve suportar configuração em alta disponibilidade para fins de redundância”. Isso porque a oferta contém apenas um item, como detalhamento da proposta, 1.2.1 TABELA DE MARCA/ MODELO, CPSM-NGSM25, Next Generation Security Management Software for 25 gateways (SmartEvent & Compliance 1 year), 1 e CPSB-EVS-25-2Y, SmartEvent and SmartReporter blade for 25 gateways (Smart-1 & open server) 2 year subscription, 1.

3.1.14 Seguem descumprimentos. A solução ofertada pela NTSEC é formada pela integração do firewall da Checkpoint com a solução “PRTG Network Monitor”, algo que se extrai da sua planilha ponto a ponto em relação aos requisitos do Anexo 1-C do edital, 1.1

(PRODAM) P2P_PE92022, ANEXO 1-C - CARACTERÍSITCAS DA SOLUÇÃO DE MONITORAMENTO, PRTG User Manual.pdf.

3.1.15 Contudo, a NTSEC não apresentou as licenças de monitoramento na proposta e nem a carta do fabricante da licença de monitoramento, violando o previsto no subitem 7.1 do Anexo 1-A do edital, conforme segue: 7.1. A LICITANTE deve ser revenda autorizada e/ou canal integrador qualificado pelos fabricantes das soluções por ela ofertadas. Sua comprovação será realizada através de declaração do fabricante dirigido especificamente à CONTRATANTE e a este processo licitatório;

3.1.16 Além disso, a recorrida também deixou de cumprir a exigência do item 6.7.2 do mesmo Anexo 1-A, verbis: 6.7.2. A Licitante Vencedora deverá apresentar juntamente a sua Proposta uma Carta de cada Fabricante do item proposto declarando que seja Revenda Autorizada/Parceiro e uma empresa capacitada como Prestador de Serviços do Fabricante;

3.1.17 Por todas essas razões, deve ser desclassificada.

3.1.18 Diante do exposto, requer-se: a) provimento quanto ao pedido de retratação da decisão que desclassificou a proposta da recorrente, aceitando-a; b) seja proferida retratação da decisão que declarou vitoriosa a proposta da recorrida; c) caso mantida a decisão, seja o recurso encaminhado à autoridade superior para provimento.

3.2 DO PEDIDO

3.2.1 Requer-se julgar totalmente procedente o presente recurso, para o fim de rever a decisão de inabilitação da recorrente, declarando a nulidade de todos os atos praticados a partir da declaração de inabilitação da recorrente.

4 DAS CONTRARRAZÕES

4.1 Nas contrarrazões, a empresa NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA. apresentou, em síntese, os seguintes pontos, os quais transcrevo em partes, novamente não detalhando a resposta a cada item do edital:

4.2 De início, no que concerne à alegação da recorrente de que preencheu todos os requisitos do Edital e, por isso, deveria ter sido classificada no certame, importa-nos esclarecer as questões a seguir:

4.3 Esta D. Comissão de licitação, acertadamente, entendeu que a empresa NCT não comprovou o pleno atendimento às especificações técnicas do instrumento convocatório do presente certame.

4.4 Alega a recorrente que “a proposta da NCT tinha o valor de R$ 2.449.000,00. No entanto (...) a PRODAM optou por aceitar a oferta final da recorrida, após negociação, no valor de R$ 3.295.529,30, com um gasto a maior de cerca de R$ 850 mil”.

4.5 Preliminarmente, é cediço que a proposta mais vantajosa não significa MENOR PREÇO, mas sim o conjunto de condições e atendimento ao objeto almejado pela Administração Pública.

4.6 Ora, seria óbvio a diferença de valores entre a proposta da recorrida e da recorrente, tendo em vista que conforme demonstramos nesta peça, a solução proposta pela ora RECORRENTE é cercada por obscuridades inobservâncias e claro descumprimento ao objeto licitado.

4.7 (...)

4.8 Expressamente previsto no art. 4º do Decreto nº 3.555/00, o princípio do justo preço impõe que a Administração realize a aquisição dos bens e serviços comuns por preços módicos, dentro daqueles praticados pelo mercado para produtos de qualidade satisfatória.

4.9 Este princípio não impõe que se busque pelo pregão tão-somente o menor preço, mas deve-se buscar o menor preço dentre aquelas propostas que ofereçam os produtos de qualidade satisfatória.

4.10 Assim, deve ser descartada a oferta daqueles produtos/serviços de qualidade duvidosa, que poderão ocasionar o descumprimento parcial ou total do contrato administrativo firmado pelo Poder Público com particular.

4.11 Percebe-se, de imediato, que a comprovação que a recorrente demonstra se restringe à impossibilidade de verificação da solução ofertada e, ainda, sua total displicência quanto à atenção aos requisitos editalícios.

4.12 (...)

4.13 Alega a recorrente que a oferta da NTSEC supostamente não atenderia ao item 2.18 – ANEXO 1-A, por não informar os part numbers dos GBICs, conforme exigido para demonstrar atendimento ao requisito supracitado.

4.14 Ao contrário das alegações da recorrente, a recorrida não realizou qualquer conduta ilegal que a pudesse desclassificá-la. Engana-se a recorrente, por falta de atenção ou má-fé, que a solução ofertada pela recorrida, a saber o appliance Quantum 7000 Plus, já inclui todos os transceivers necessários para o uso. Uma simples conferência na documentação do produto (datasheet) poderia ter sanado a dúvida da recorrente, senão vejamos:

4.15 Para facilitar a compreensão da recorrente, sinalizamos no arquivo anexado "check point 7000 securitygateway datasheet.pdf" ou ainda através de acesso pelo link público: https://www.checkpoint.com/downloads/products/7000-security-gateway-datasheet.pdf, é possível atentar na página 4, no tópico "Ordering Quantum 7000 Security Gateways", na tabela "Base Configuration", a segunda linha que diz: "7000 Security Gateway Plus configuration, includes 10x 1GbE copper ports, 4x 10GbE SFP+ ports, 4x SRtransceivers (grifo nosso), 32 GB RAM, 2x SSD, 2x AC PSU, Lights-out Management, telescopic rails, SandBlast(SNBT) Security Subscription Package for 1 Year". 69.

4.16 Como se observa notadamente, o pacote Plus ofertado já inclui os transceivers necessários para a operação das portas também ofertadas, tornando inválida qualquer alegação nesse sentido.

4.17 Para além de qualquer dúvida, conforme indicação na comprovação ponto-a-ponto entregue pela recorrida, no item 2.18, a recorrida atesta através “de acordo” com a entrega dos itens solicitados, sem qualquer tipo de alteração no custo final.

4.18 Do contrário, poderíamos nos utilizar aqui do argumento da própria recorrente que alega em suas razões recursais que se a licitante “indicou plena concordância com os seus termos (...), como se pode indicar descumprimento?”. O que não torna-se necessário, dado a clara comprovação de atendimento da solução ofertada por esta recorrida aos requisitos técnicos do presente certame.

4.19 Do exposto, conclui-se que não há como se admitir a desclassificação da RECORRIDA, pois esta apresentou a documentação relativa à todos os itens em conformidade com o termo de referência e o ato convocatório, devendo, portanto, ser mantida a decisão administrativa que a sagrou vencedora do certame, mormente em razão da redação do art. 31, “caput”, da Lei nº. 13.303/2016.

4.20 Alega a recorrente, quando diz que o item 52 do edital foi descumprido, uma vez que a NTSEC posicionou apenas um item do software de gerenciamento, quando o item solicita que: “Deve SUPORTAR configuração em alta disponibilidade para fins de redundância;”.

4.21 Equivoca-se mais uma vez a recorrente, por desatenção ou descuidado com o processo, em questão simples de interpretação textual. Basta uma simples leitura do item em pauta, pois este é muito claro em solicitar da solução ofertada a CAPACIDADE, ou seja, o SUPORTE a uma configuração específica, que neste caso é a de redundância, como muito bem demonstrado pela documentação da solução, indicada na comprovação ponto-a-ponto entregue.

4.22 Reiteramos aqui a comprovação na página 345, conforme indicação da comprovação, o tópico “Overview of Management High Availability”, em tradução livre “Visão Geral da Alta Disponibilidade da Gerência”. Logo no primeiro parágrafo assinala: “High Availability is redundancy and database backup for management servers” que em tradução livre mostra “Alta disponibilidade é a redundância e salvaguarda de bancos de dados dos servidores de gerenciamento”. Para além, até a página 354, o manual discorre em todas as características do gerenciamento em alta disponibilidade e suas possibilidades de configuração, restando completamente demonstrada a capacidade da solução ofertada de trabalhar em modo de alta disponibilidade, conforme solicita o item.

4.23 Diante do exposto, resta claro a comprovação do atendimento da oferta proposta por esta recorrida.

4.24 Alega a recorrente que a NTSEC supostamente não teria apresentado as licenças de monitoramento na proposta e não teria apresentado carta do fabricante da licença de monitoramento.

4.25 Inicialmente vale ressaltar que o objeto licitado busca a prestação de serviços, conforme “lembrado” pela própria NCT em suas razões recursais. Desta forma, a solução de monitoramento deve ser a composição do serviço ofertado pelas interessadas, tendo sido todos os requisitos do Anexo 1-C comprovados por esta recorrida, em observância ao cumprimento dos requisitos do edital.

4.26 A recorrente demonstra total insipiência da oferta necessária ao chamamento da PRODAM no Pregão em tela. Ora, a presente contratação do item almeja a solução de “NEXT GENERATION FIREWALL” o qual esta recorrida devidamente comprovou todos os requisitos, conforme a própria NCT atesta em sua peça, alegando que “a solução ofertada pela NTSEC é formada pela integração do Firewall Check Point com a solução “PRTG Network Monitor”.

4.27 O serviço de monitoramento 24x7 deverá ser prestado pela CONTRATADA, OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center), conforme disposto no item 7.16 do anexo 1– TERMO DE REFERÊNCIA e a ferramenta apresentada e devidamente comprovada pela NTSEC em atendimento ao Anexo 1-C é tão somente o que viabiliza o requerido neste serviço.

4.28 (...)

4.29 Por todo o exposto, protesta-se pela total improcedência do recurso ofertado em razão do não atendimento ao instrumento convocatório no que diz respeito à não comprovação da RECORRENTE a diversos requisitos do edital.

4.30 Requer-se ainda que este D. Pregoeiro mantenha a acertada decisão que declarou a NCT desclassificada no presente certame, mantendo-se assim intacta a decisão administrativa que desclassificou a recorrente e declarou a NTSEC como vencedora do PREGÃO ELETRÔNICO Nº 09/2022 da PRODAM – Processamento de Dados Amazonas S.A, dando-se regular seguimento ao certame, com a contratação da empresa vencedora.

5 DA ANÁLISE

5.1 Imperioso ressaltar que todos os julgados da Administração Pública estão embasados nos princípios insculpidos no art. 31 da Lei 13.303/16, conforme segue:

> Art. 31. As licitações realizadas e os contratos celebrados por empresas públicas e sociedades de economia mista destinam-se a assegurar a seleção da proposta mais vantajosa, inclusive no que se refere ao ciclo de vida do objeto, e a evitar operações em que se caracterize sobrepreço ou superfaturamento, devendo observar **os princípios da impessoalidade, da moralidade, da igualdade, da publicidade, da eficiência, da probidade administrativa, da economicidade, do desenvolvimento nacional sustentável, da vinculação ao instrumento convocatório, da obtenção de competitividade e do julgamento objetivo. (grifo nosso).**

5.2 Ressalta-se que tal disposição é corroborada pelo disposto no Decreto n.º 10.024/2019:

> Art. 2º O pregão, na forma eletrônica, é condicionado aos **princípios da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da eficiência, da probidade administrativa, do desenvolvimento sustentável, da vinculação ao instrumento convocatório, do julgamento objetivo, da razoabilidade, da competitividade, da proporcionalidade e aos que lhes são correlatos. (grifo nosso).**

5.3 Dito isto, após apreciação dos fundamentos elencados no recurso interposto pela recorrente NCT INFORMÁTICA LTDA. e das contrarrazões interpostas pela recorrida NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA., passamos a análise do mérito:

5.4 Os questionamentos levantados pela recorrente NCT foram analisados pela equipe técnica da PRODAM quanto ao atendimento dos itens exigidos no edital e seus anexos e em conformidade ao parágrafo único do item 8 do Edital que trata da solicitação de manifestação técnica.

5.5 Há de se registrar que os documentos encaminhados na peça recursal da recorrente NCT são referentes a versões defasadas do produto e anterior à versão ofertada na proposta, o que contradiz a três itens do termo de referência, os quais são:

> Item: 6.3.9. As versões dos softwares ofertados pela CONTRATADA sempre deverão estar com a versão mais atual disponível no mercado. A versão anterior:
>
> Subitem 6.3.9.1. Não poderá permanecer instalada mais do que 03 (três) meses, após o lançamento da última versão homologada;
>
> Item: 6.7.1. Todos os equipamentos ou componentes necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de endof-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Caso o equipamento venha ser descontinuado, a CONTRATADA deverá substitui-lo antes sem custos adicionais para a CONTRATANTE.

5.6 Portanto, é coerente que, quando da apresentação das documentações comprobatórias dos requisitos técnicos do certame para os produtos ofertados, esta comprovação também seja evidenciada na versão da documentação dos sistemas operacionais ou produtos, equivalente ao produto ofertado ou numa versão mais nova. Nunca uma versão anterior.

5.7 Considerando este contexto, a equipe técnica da PRODAM analisou minuciosamente nas novas fontes de comprovação documentais apresentadas pela recorrente NCT conforme Parecer Técnico anexo e publicado no Portal de Transparência através do link: https://www.prodam.am.gov.br/transparencia/.

5.8 Assim sendo, verificou-se que a recorrente NCT não atende às exigências editalícias, visto que foram identificados 11 (onze) itens do edital que permanecem sem evidências documentais suficientes para comprovar que a solução ofertada pela empresa atende a tais requisitos.

5.9 Quanto a alegação que a proposta da recorrida NTSEC não atende aos requisitos, foi realizada a mesma análise do atendimento aos itens pela equipe técnica da PRODAM conforme segue:

> ITEM 2.18 – ANEXO 1-A: Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

5.9.1 Na análise da proposta apresentada pela recorrida NTSEC, entendeu-se que o Produto ofertado, cujo Part-Number é CPAP-SG7000-PLUS-SNBT, está de acordo, e conforme o próprio datasheet informa, já traz contemplado um Módulo com 4 portas 1/10gb com seus respectivos módulos GBICs. A comprovação foi apresentada originalmente na planilha ((PRODAM) P2P_PE92022) enviada pela NTSEC e que pode ser acessado no link: https://www.checkpoint.com/downloads/products/7000-security-gateway datasheet.pdf.

> ITEM 52 – ANEXO 1-B: Deve suportar configuração em alta disponibilidade para fins de redundância;

5.9.2 A referida alegação apresentada pela recorrente NTC não tem relação com o Item 52 do Edital. Está claro na documentação apresentada originalmente pela recorrida NTSEC, especificamente na comprovação informada em sua planilha ponto a ponto ((PRODAM) P2P_PE92022), que o produto ofertado suporta configuração em alta disponibilidade para fins de redundância.

> ITEM 7.1 – ANEXO 1-A: A LICITANTE deve ser revenda autorizada e/ou canal integrador qualificado pelos fabricantes das soluções por ela ofertadas. Sua comprovação será realizada através de declaração do fabricante dirigido especificamente à CONTRATANTE e a este processo licitatório;

5.9.3 Entende-se também que a declaração (Carta_PRODAM_NTSec_November22.pdf) apresentada pela recorrida NTSEC está de acordo com o solicitado no respectivo item (7.1 do Anexo 1-A do edital) questionado pela recorrente NCT.

> ITEM 6.7.2 – ANEXO 1-A: A Licitante Vencedora deverá apresentar juntamente a sua Proposta uma Carta de cada Fabricante do item proposto declarando que seja Revenda Autorizada/Parceiro e uma empresa capacitada como Prestador de Serviços do Fabricante;

5.9.4 Os atestados de capacidade técnicas apresentados e consolidados no documento (Atestados_Capacidade_Tecnica.pdf) de comprovação apresentado pela recorrida NTSEC estão de acordo com o solicitado no respectivo item (6.7.2. do Anexo 1-A do edital) questionado pela recorrente NCT.

5.10 Considerando que o Pregoeiro oportunizou iguais condições de participação e competição aos licitantes interessados, considerando as contrarrazões interpostas pela recorrida e considerando, ainda, o parecer técnico sobre o recurso apresentado, considera-se indeferido o pedido da recorrente, classificada em 2º lugar, e declará-la desclassificada do Pregão Eletrônico SRP– Nº 09/2022.

6 DA DECISÃO

Isto posto, sem mais nada a considerar, respeitados os princípios constitucionais do contraditório, da ampla defesa e do devido processo legal, CONHEÇO das razões e das contrarrazões ao recurso por tempestivos, para, NO MÉRITO**, NEGAR-LHE PROVIMENTO**, mantendo assim inalterada a decisão anterior que inabilitou a empresa NCT INFORMÁTICA LTDA**.** e declarou como vencedora do certame a empresa NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.

Mantendo a decisão, encaminho a presente manifestação à autoridade competente para deliberação, nos termos da legislação de regência.

Manaus AM, 20 de dezembro de 2022.

Atenciosamente,

GILSON DE SENA DA SILVA
Assinado de forma digital por GILSON DE SENA DA SILVA
Dados: 2022.12.20 16:58:22 -04'00'

GILSON DE SENA DA SILVA
Pregoeiro

DE ACORDO:

LINCOLN NUNES DA SILVA
Diretor-Presidente

PARECER TÉCNICO

Após conclusão da sessão pública realizada no dia 17/11/2022 que tratou do **Pregão Eletrônico de Nº 09/2022** cujo objeto é a contratação de uma empresa especializada para prestação de serviços de natureza continuada, especializada em gerenciamento de segurança lógica - no modelo 24hs por dia, 7 dias por semana, 365 dias por ano, incluindo o conjunto de hardware e software, fornecidos em regime de comodato, foi solicitado a equipe técnica da Prodam que realizasse análise de conformidade da documentação entregue pela LICITANTE NCT INFORMÁTICA LTDA, 2ª classificada do certame.

Com o resultado da análise de conformidade da documentação quanto aos requisitos técnicos do Edital supracitado, entregue através do PARECER TÉCNICO emitido em **21/11/2022** e anexado ao **SIGED 1200/2022-77**, a empresa LICITANTE não comprovou o atendimento de vários itens, de acordo com o especificado no Edital. Portanto, a nossa conclusão foi a de que "*a menos que sejam apresentadas evidências documentais de que evidenciem, inequivocadamente, que atendem os itens citados como não estando de acordo, a empresa LICITANTE (NCT INFORMÁTICA LTDA) não pode ser considerada apta a atender o objeto solicitado no certame*".

Então, no dia 06/12/2022, a empresa LICITANTE (NCT INFORMÁTICA LTDA) entrou com um recurso alegando que atendia aos itens informados no parecer técnico e apresentou novas fontes de comprovação documentais em seu recurso.

Diante da apresentação deste recurso, foi solicitado a equipe técnica da Prodam que, novamente, realizasse análise da documentação entregue no recurso e emitisse um novo PARECER TÉCNICO.

Inicialmente, gostaríamos de destacar 02 (dois) itens importantes neste contexto do Termo de Referência, são eles:

- Do Item 6.3. *(Prestação dos Serviços Contínuos)* o subitem:
  - 6.3.9. As versões dos softwares ofertados pela CONTRATADA sempre **deverão estar com a versão mais atual** disponível no mercado. A versão anterior:
    - 6.3.9.1. **Não poderá permanecer instalada mais do que 03 (três) meses, após o lançamento da última versão homologada**;
- Do Item 6.7. *(Solução de Hardware e Software da CONTRATADA)* o subitem:
  - 6.7.1. Todos os equipamentos ou **componentes necessários à prestação dos serviços** deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em **listas de end-of-sale, end-of-support ou end-of-life do fabricante**, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Caso o equipamento venha ser descontinuado, a CONTRATADA deverá substitui-lo antes sem custos adicionais para a CONTRATANTE.

Desta forma, é coerente que, quando da apresentação das documentações comprobatórias dos requisitos técnicos do certame para os produtos ofertados, esta comprovação também seja evidenciada na versão da documentação

dos sistemas operacionais ou produtos, equivalente ao produto ofertado ou numa versão mais nova. Nunca numa versão anterior.

Considerando este contexto, realizou-se a análise minuciosa nas novas fontes de comprovação documentais apresentadas pela LICITANTE.

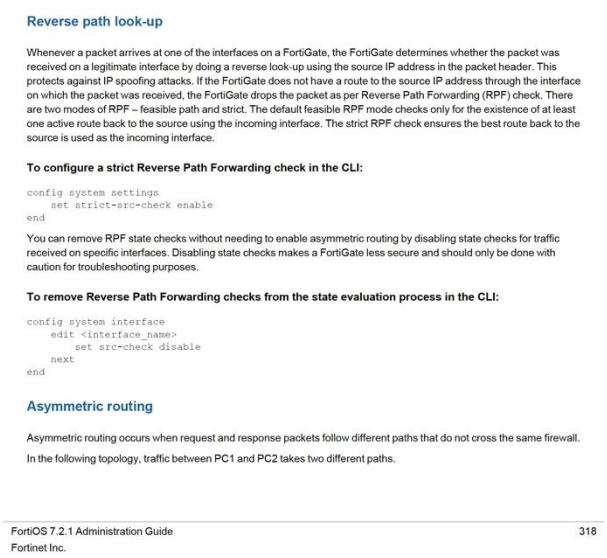
Abaixo seguem as **análises dos recursos apresentados para cada item questionado**:

ITEM 3.16 do Edital	3.16. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A página (304) informada na documentação enviada não diz respeito ao solicitado no item e sim, trata sobre "**DHCP relay information option**" ou seja, trata-se de um recurso do DHCP que, se habilitado, ajuda a proteger contra-ataques como IP Spoofing.

Dando continuidade na leitura do Manual (FortiOS-7.2.1-Administration_Guide) encontramos na página 318 um texto que fala a respeito do IP Spoofing Attacks.



Reverse path look-up

Whenever a packet arrives at one of the interfaces on a FortiGate, the FortiGate determines whether the packet was received on a legitimate interface by doing a reverse look-up using the source IP address in the packet header. This protects against IP spoofing attacks. If the FortiGate does not have a route to the source IP address through the interface on which the packet was received, the FortiGate drops the packet as per Reverse Path Forwarding (RPF) check. There are two modes of RPF – feasible path and strict. The default feasible RPF mode checks only for the existence of at least one active route back to the source using the incoming interface. The strict RPF check ensures the best route back to the source is used as the incoming interface.

To configure a strict Reverse Path Forwarding check in the CLI:

```
config system settings
    set strict-src-check enable
end
```

You can remove RPF state checks without needing to enable asymmetric routing by disabling state checks for traffic received on specific interfaces. Disabling state checks makes a FortiGate less secure and should only be done with caution for troubleshooting purposes.

To remove Reverse Path Forwarding checks from the state evaluation process in the CLI:

```
config system interface
    edit <interface_name>
        set src-check disable
    next
end
```

Asymmetric routing

Asymmetric routing occurs when request and response packets follow different paths that do not cross the same firewall.

In the following topology, traffic between PC1 and PC2 takes two different paths.

FortiOS 7.2.1 Administration Guide 318
Fortinet Inc.

Ao lado, temos o print retirado da página que trata sobre o "**Reverse path look-up**" e nela está dizendo que: "Whenever a packet arrives at one of the interfaces on a FortiGate, the FortiGate determines whether the packet was received on a legitimate interface **by doing a reverse look-up using the source IP address in the packet header. This protects against IP spoofing attacks. If the FortiGate does not have a route to the source IP address through the interface on which the packet was received, the FortiGate drops the packet as per Reverse Path Forwarding (RPF) check**. There are two modes of RPF – feasible path and strict. The default feasible RPF mode checks only for the existence of at least one active route back to the source using the incoming interface. The strict RPF check ensures the best **route back** to the source is used as the incoming interface."

Com esse texto fica claro que o mecanismo de proteção contra IP Spoofing utiliza tabela de roteamento, portanto, no nosso entendimento, não atende o referido Item do Edital.

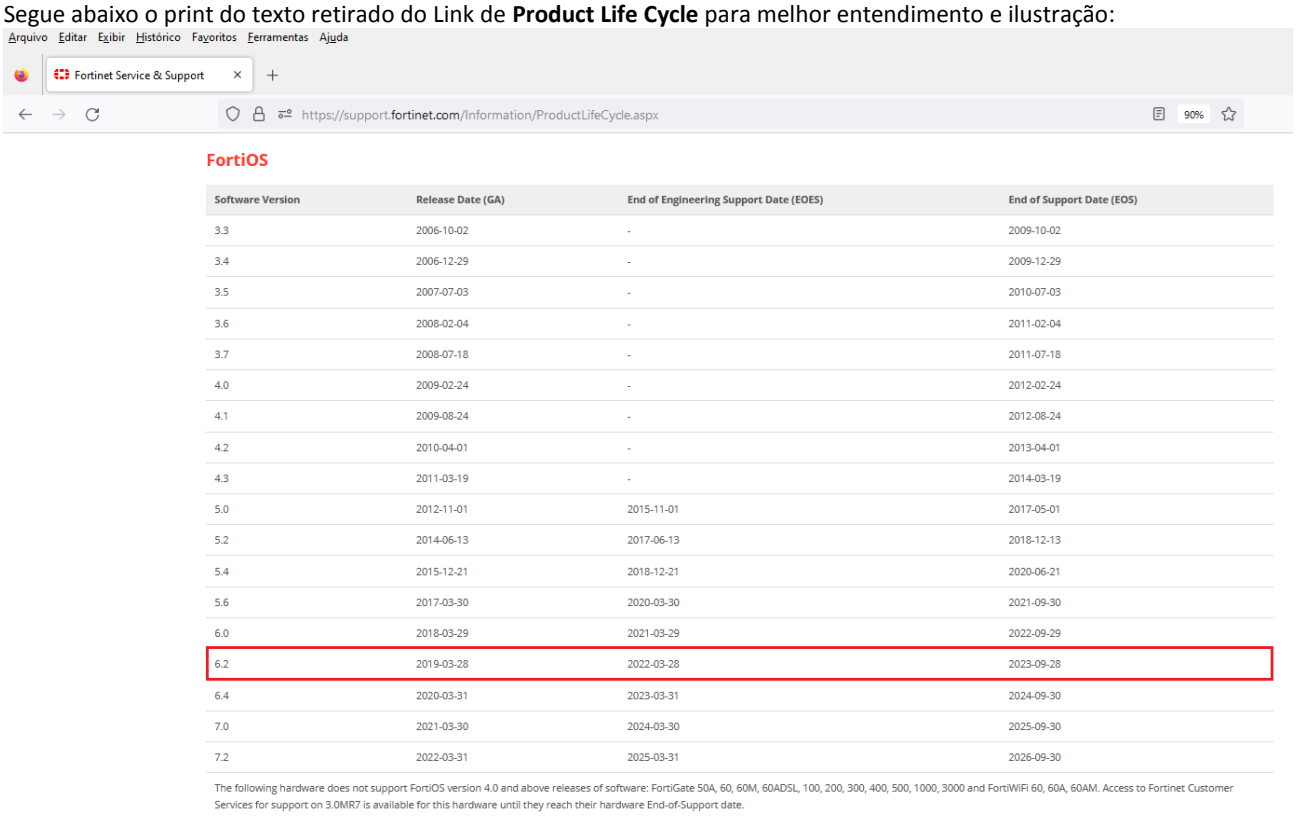
ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações enviada pela licitante, originalmente: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

No recurso, o fornecedor afirma que o item é atendido pela solução, e envia a seguinte URL adicional: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/861490/zero-touch-provisioning-with-fortimanager

Analisando a documentação do recurso apresentada, de início podemos observar "Zero touch provisioning with FortiManager - You can use this feature only when the FortiGate boots up from factory reset. This feature is for FortiGate devices that cannot access the Internet.", evidenciado que não se trata de comprovação relacionada ao que trata o item 3.16.
Além disto, a Licitante apresenta documentação de uma versão Legada e que vai contra aos subitens 6.3.9. e 6.7.1., ou seja, está bem claro que estamos solicitando que o produto ofertado esteja "**com a versão mais atual** disponível no mercado" e que não pode ofertar um produto com uma versão que esteja mais do que **03 (três) meses após o lançamento da última versão homologada**. Logo, em análise do link https://support.fortinet.com/Information/ProductLifeCycle.aspx podemos observar que a última versão lançada e homologada do produto ofertado é a FortiOS 7.2.0 e tal versão foi lançada há pouco mais de 03 (três) anos da versão ofertada na documentação dos recursos. De acordo com a informação do link, a versão (FortiOS 6.2.0) apresentada na documentação do recurso teve seu Release Gate (Data de Lançamento) em 28/03/2019 e também, seu End of Engineering Support Date (Fim da Data de Suporte de Engenharia) em 28/03/2022.

Segue abaixo o print do texto retirado do Link de **Product Life Cycle** para melhor entendimento e ilustração:



FortiOS

Software Version	Release Date (GA)	End of Engineering Support Date (EOES)	End of Support Date (EOS)
3.3	2006-10-02	-	2009-10-02
3.4	2006-12-29	-	2009-12-29
3.5	2007-07-03	-	2010-07-03
3.6	2008-02-04	-	2011-02-04
3.7	2008-07-18	-	2011-07-18
4.0	2009-02-24	-	2012-02-24
4.1	2009-08-24	-	2012-08-24
4.2	2010-04-01	-	2013-04-01
4.3	2011-03-19	-	2014-03-19
5.0	2012-11-01	2015-11-01	2017-05-01
5.2	2014-06-13	2017-06-13	2018-12-13
5.4	2015-12-21	2018-12-21	2020-06-21
5.6	2017-03-30	2020-03-30	2021-09-30
6.0	2018-03-29	2021-03-29	2022-09-29
6.2	2019-03-28	2022-03-28	2023-09-28
6.4	2020-03-31	2023-03-31	2024-09-30
7.0	2021-03-30	2024-03-30	2025-09-30
7.2	2022-03-31	2025-03-31	2026-09-30

The following hardware does not support FortiOS version 4.0 and above releases of software: FortiGate 50A, 60, 60M, 60ADSL, 100, 200, 300, 400, 500, 1000, 3000 and FortiWiFi 60, 60A, 60AM. Access to Fortinet Customer Services for support on 3.0MR7 is available for this hardware until they reach their hardware End-of-Support date.

Mesmo a documentação apresentada no recurso não estando de acordo com os itens do Termo de Referência citados, ainda assim, procedeu-se a análise. De acordo com a análise a comprovação apresentada no recurso ainda se trata de uma funcionalidade disponibilizada a partir do DHCP na Intranet que, se habilitado, ajuda a proteger contra-ataques como IP Spoofing. Mesmo considerando os segundos links enviados, não há evidências que o equipamento ofertado irá proteger contra os ataques de IP Spoofing externos sem utilizar a tabela de roteamento, conforme solicitado no edital. Ainda devemos considerar a página 318 do FortiOS-7.2.1-Administration_Guide que indica o uso das tabelas de roteamento, em contradição com o que é solicitado no Edital. Desta forma, a segunda documentação enviada no recurso **não comprova** (1) o atendimento a este item do Edital.

ITEM 3.26 do Edital	Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, suportando, no mínimo: Office 365, AWS e Azure;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A documentação apresentada indica a página 260 do manual FortiOS-7.2.1. Nela, após leitura e análise identificamos apenas instruções para a criação de regras onde o usuário somente acesse o "tenant" específico do órgão em algum serviço de nuvem, citando Office 365, Google Workspace e Dropbox. O item do Edital solicita que seja possível criar regras de firewall e NAT utilizando objeto de serviços online, para, pelo menos, Office 365, AWS e Azure. Com isso, a comprovação apresentada não demonstra ser possível fazer isso. Ainda que atendesse ao item, não atuaria para AWS e Azure, requisitos imprescindíveis do item em tela.
Segue abaixo o print do texto retirado do Manual FortiOS-7.2.1 para melhor entendimento e ilustração:

Restricted SaaS access

Large organizations may want to restrict SaaS access to resources like Microsoft Office 365, Google Workspace, and Dropbox by tenant to block non-company login attempts and secure the users from accessing non-approved cloud resources. Many cloud vendors enable this by applying tenant restrictions for access control. For example, users accessing Microsoft 365 applications with tenant restrictions through the corporate proxy will only be allowed to log in as the company's tenant and access the organization's applications.

To implement this, access requests from the clients pass through the company's web proxy, which inserts headers to notify the SaaS service to apply tenant restrictions with the permitted tenant list. Users are redirected the SaaS service login page, and are only allowed to log in if they belong to the permitted tenant list.

For more information, refer to the vendor-specific documentation:

- Office 365: Restrict access to a tenant
- Google Workspace: Block access to consumer accounts
- Dropbox: Network control

FortiOS 7.2.1 Administration Guide 260
Fortinet Inc.

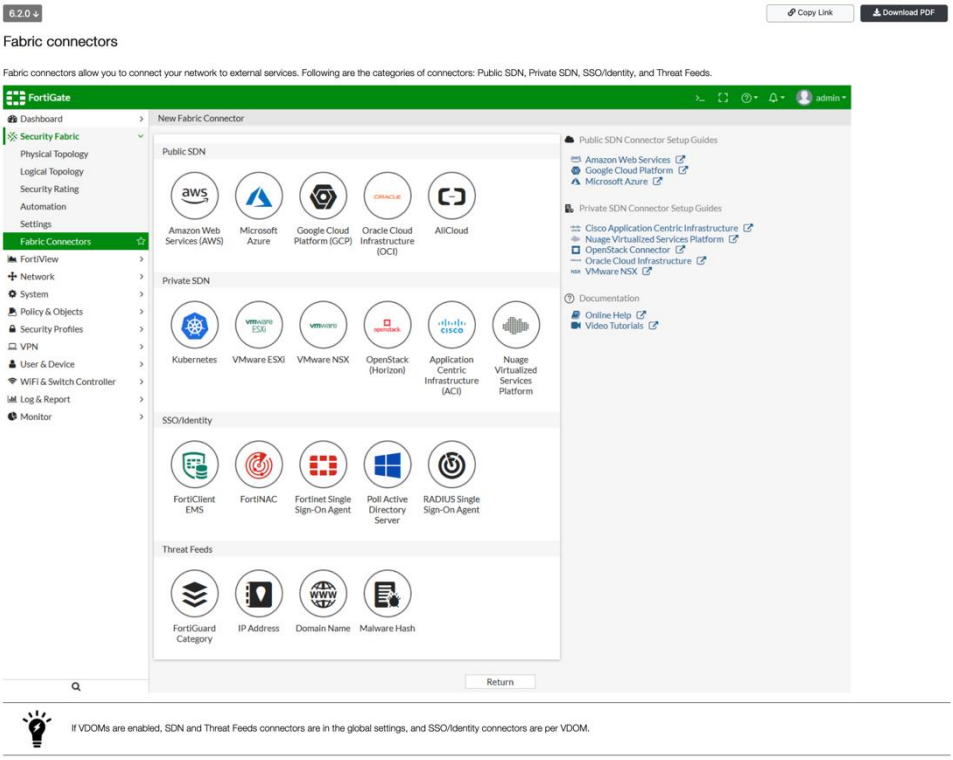
ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações enviada, originalmente, pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

No recurso, o fornecedor afirma que item é atendido pela solução, indicando o seguinte link adicional:

- https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/753961/fabric-connectors
- https://www.fortinet.com/products/public-cloud-security/usecases/m365

Analisando a documentação do recurso apresentada (primeiro link), apesar de comprovar a compatibilidade com conexão de serviços externos como a AWS e Azure, se trata de uma documentação da versão do Forti-OS 6.2.0, versão anterior à que foi entregue na documentação da proposta original. Mais uma vez a documentação do recurso apresentada pela Licitante vai contra aos subitens 6.3.9. e 6.7.1., ou seja, está bem claro que estamos solicitando que o produto ofertado esteja "**com a versão mais atual** disponível no mercado" e que não pode ofertar um produto com uma versão que esteja mais do que **03 (três) meses após o lançamento da última versão homologada**.



Com relação a comprovação apresentada no recurso referente ao Office 365, já havia sido comprovado que o equipamento oferecido atende. O que havia ficado pendente era a comprovação com o AWS e Microsoft Azure. Portanto, para o nosso entendimento não ficou claro que a Versão mais atual ainda possui essa integração com o AWS e Microsoft e, apesar de o segundo link enviado discorrer de forma genérica sobre a integração do Fortinet com Microsoft 365, não fica explicitamente evidenciado de que "permite a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, suportando, no mínimo: Office 365, AWS e Azure;", conforme solicitado no item.

Desta forma, a segunda documentação enviada no recurso **não comprova (2)** claramente o atendimento a este item do Edital.	
ITEM 3.28 do Edital	Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A documentação da comprovação indica na página 792 diz que o equipamento ofertado atende ao referido item, no entanto, logo em seguida na página 793 o Manual diz "para que o tráfego flua pelo Firewall FortiGate, **deve** haver uma política que corresponda à alguns parâmetros", são eles:

- Incoming interface(s);
- Outgoing interface(s);
- Source address(es);
- User(s) identity;
- Destination address(es);
- Internet service(s);
- Schedule;
- Service;

Para o nosso entendimento, o referido Manual diz que para a solução ofertada obrigatoriamente devemos ter todos os parâmetros acima informados para que o tráfego possa fluir, **inclusive**, como mostram os parâmetros destacados na cor amarela, as interfaces de entrada e saída. O Item do Edital fala de forma muito clara que não deve ser aceito soluções onde, em uma regra de firewall, precise-se explicitar qual a interface de origem e interface de destino dessa regra, logo, não estaria atendendo o referido Item.
Segue abaixo o print do texto retirado do Manual FortiOS-7.2.1 para melhor entendimento e ilustração:

Firewall policy parameters

For traffic to flow through the FortiGate firewall, there must be a policy that matches its parameters:

- Incoming interface(s)
- Outgoing interface(s)
- Source address(es)
- User(s) identity
- Destination address(es)
- Internet service(s)
- Schedule
- Service

Traffic parameters are checked against the configured policies for a match. If the parameters do not match any configured policies, the traffic is denied.

Traffic flow initiated from each direction requires a policy, that is, if sessions can be initiated from both directions, each direction requires a policy.

Just because packets can go from point A to point B on port X does not mean that the traffic can flow from point B to point A on port X. A policy must be configured for each direction.

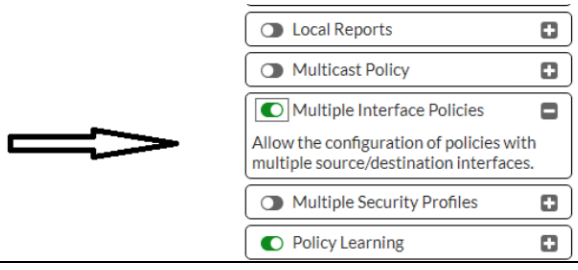
When designing a policy, there is often reference to the traffic flow, but most communication is two-way so trying to determine the direction of the flow might be confusing. If traffic is HTTP web traffic, the user sends a request to the

ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações enviada, originalmente, pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

O fornecedor informa que o item é atendido pela solução, conforme verifica nova URL apresentada: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-allow-the-configuration-of-policies-with/ta-p/191941

--> No nosso entendimento, este link ainda mostra que se faz necessário informar as interfaces de entrada e saída, o que ele está informando de fato é que é possível configurarmos com múltiplas interfaces de entrada e saída.



O fornecedor informa que o item também pode ser atendido pela solução, conforme nova URL apresentada: https://docs.fortinet.com/document/fortigate/6.4.5/administration-guide/118429/topology

Este segundo Link, além de referir-se a uma versão defasada do IOS, não deixa claro a comprovação afirmada pelo fabricante. O documento apresenta a topologia de um ambiente e não mostra explicitamente que, quando se configura uma regra, ele dispensa a obrigatoriedade de explicitar-se as interfaces de origem e destino, conforme é solicitado neste item do edital.
Desta forma, a segunda documentação enviada no recurso **não comprova** (3) o atendimento a este item do Edital.

ITEM 3.27 do Edital	Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A documentação da comprovação indica na página 496 do Manual FortiOS-7.2.1-Administration_Guide como se realiza a **configuração do IPv4 sobre o IPv6 no serviço de DS-Lite em um túnel VNE** (Virtual Network Enabler). Além disso, informa também que o modo fixo de IP suporta autenticação de nome de usuário e senha, não apresentando assim, nenhuma ligação com o Item do Edital. A comprovação deveria apresentar a possibilidade da criação de regras para IPv4 e IPv6 sem a duplicação da base de objetos e regras, conforme se pede no Item do Edital. Concluímos, portanto, que a comprovação apresentada não estaria atendendo o referido Item.
Segue abaixo o print do texto retirado do Manual FortiOS-7.2.1 para melhor entendimento e ilustração:

Network

2. Configure the IPv6 tunnel:

```
config system ipv6-tunnel
    edit "D_2_B"
        set source 2000:172:16:202::2
        set destination 2000:172:16:202::1
        set interface "port3"
    next
end
```

3. Configure the tunnel interface:

```
config system interface
    edit "D_2_B"
        set vdom "root"
        set ip 172.16.210.2 255.255.255.255
        set allowaccess ping https http
        set type tunnel
        set remote-ip 172.16.210.1 255.255.255.255
        set snmp-index 36
        config ipv6
            set ip6-address 2000:172:16:210::2/64
            set ip6-allowaccess ping
            config ip6-extra-addr
                edit fe80::4424/10
                next
            end
        end
        set interface "port3"
    next
end
```

4. Verify the interface lists:

```
# diagnose netlink interface list port3
# diagnose netlink interface list D_2_B
```

Configuring IPv4 over IPv6 DS-Lite service

IPv4 over IPv6 DS-Lite service can be configured on a virtual network enabler (VNE) tunnel. In addition, VNE tunnel fixed IP mode supports username and password authentication.

```
config system vne-tunnel
    set status enable
    set mode {map-e | fixed-ip | ds-lite}
    set ipv4-address <IPv4_address>
    set br <IPv6_address or FQDN>
    set http-username <string>
    set http-password <password>
end
```

`mode {map-e | fixed-ip | ds-lite}`	Set the VNE tunnel mode: • map-e: MAP-E • fixed-ip: fixed IP • ds-lite: DS-Lite

FortiOS 7.2.1 Administration Guide 496
Fortinet Inc.

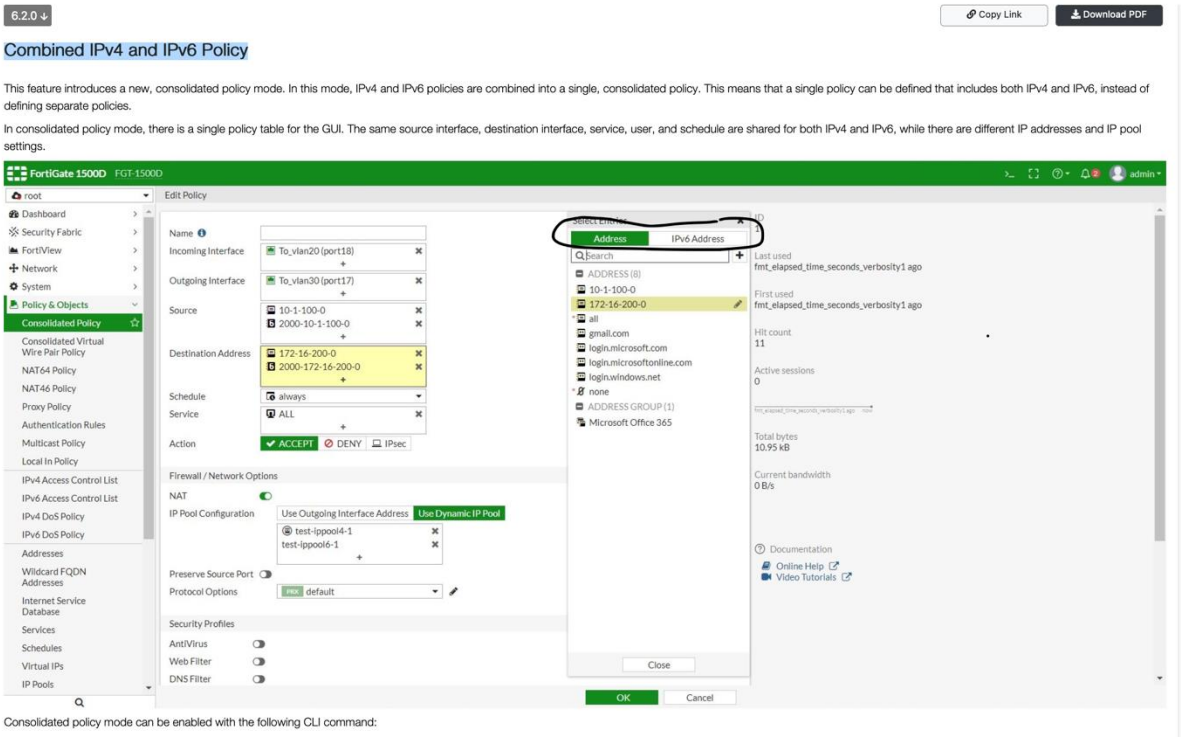
ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

O fornecedor informa que o item é atendido pela solução, e fornece a seguinte URL adicional: https://docs.fortinet.com/document/fortigate/6.2.0/new-features/516182/combined-ipv4-and-ipv6-policy

O link enviado na nova comprovação, mais uma vez, se trata de uma documentação da versão do FortiOS 6.2.0 anterior à que foi entregue na documentação original. Logo fica a dúvida, a versão originalmente apresentada (FortiOS 7.2.1) consta com esses mesmos recursos, porque não foi apresentado na documentação com o

FortiOS mais atualizado. Mesmo assim, neste link afirma que é possível combinarmos políticas para IPv4 e IPv6 uma única política consolidada. Contudo, não fica claro que para a criação desta regra, o usuário fica isento da criação da base de Objetos conforme é solicitado neste Item do Edital. Tanto que no print abaixo temos duas abas de base de Objetos, uma para IPV4 e outra para IPV6. Logo, no nosso entendimento, se faz necessário a criação de um mesmo Objeto em ambas as abas para consolidação das regras que é apresentado.



Desta forma, a segunda documentação (desatualizada) enviada no recurso **não comprova (4)** de forma inequívoca o atendimento a este item do Edital, uma vez que pela evidência enviada há uma aba para cada tipo de endereçamento.

ITEM 4.7.2 do Edital	Reconhecer pelo menos 3.600 (três mil e seiscentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na página 138 do Manual FortiOS-7.2.1-Administration_Guide apresenta a demonstração de instruções de “Monitoring network traffic SSl deep inspection” que se inicia na página 137, ou seja, monitoramento de aplicação. Com isso, a comprovação apresentada não indica qualquer ligação com a solicitação do referido Item do Edital e, portanto, não é possível aferir o quantitativo e as categorias de aplicações que são solicitadas no Item do Edital.

Segue abaixo o print da página 138 indicada na comprovação e retirada do Manual FortiOS-7.2.1 para melhor entendimento e ilustração:

Dashboards and Monitors

- *Log Allowed Traffic* is set to *All Sessions*.

2. Go to *Security Profiles* > *Application Control*.
3. Select a relative Application Control profile used by the firewall policy and click *Edit*.
4. Because YouTube cloud applications are categorized into *Video/Audio*, ensure the *Video/Audio* category is monitored. Monitored categories are indicate by an eye icon.
5. Click *View Application Signatures* and hover over YouTube cloud applications to view detailed information about YouTube application sensors.
6. Expand *YouTube* to view the Application Signatures associated with the application.

Application Signature	Description	Application ID
YouTube_Video.Access	An attempt to access a video on YouTube.	16420
YouTube_Channel.ID	An attempt to access a video on a specific channel on YouTube.	44956
YouTube_Comment.Posting	An attempt to post comments on YouTube.	31076
YouTube_HD.Streaming	An attempt to watch HD videos on YouTube.	33104
YouTube_Messenger	An attempt to access messenger on YouTube.	47858
YouTube_Video.Play	An attempt to download and play a video from YouTube.	38569
YouTube_Video.Upload	An attempt to upload a video to YouTube.	22564
YouTube	An attempt to access YouTube. This application sensor does not depend on SSL deep inspection so it does not have a cloud or lock icon.	31077
YouTube_Channel.Access	An attempt to access a video on a specific channel on YouTube.	41598

To view the application signature description, click the ID link in the information window.

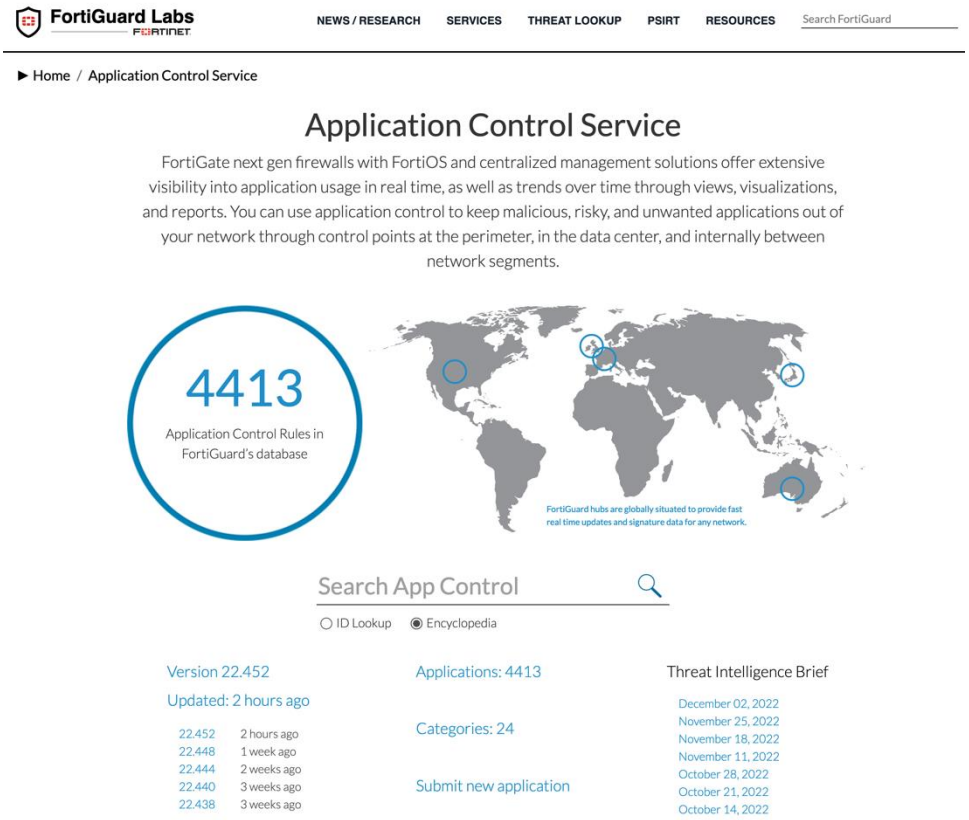
7. On the test PC, log into YouTube and play some videos.
8. On the FortiGate, go to *Log & Report* > *Security Events* and look for log entries for browsing and playing YouTube videos in the *Application Control* card.

FortiOS 7.2.1 Administration Guide 138
Fortinet Inc.

ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

A solução da Fortinet cotada tem 4341 aplicações cadastradas, conforme informação disponível em novo link apresentado:
https://www.fortiguard.com/services/appcontrol, atendendo, assim, inteiramente o solicitado.

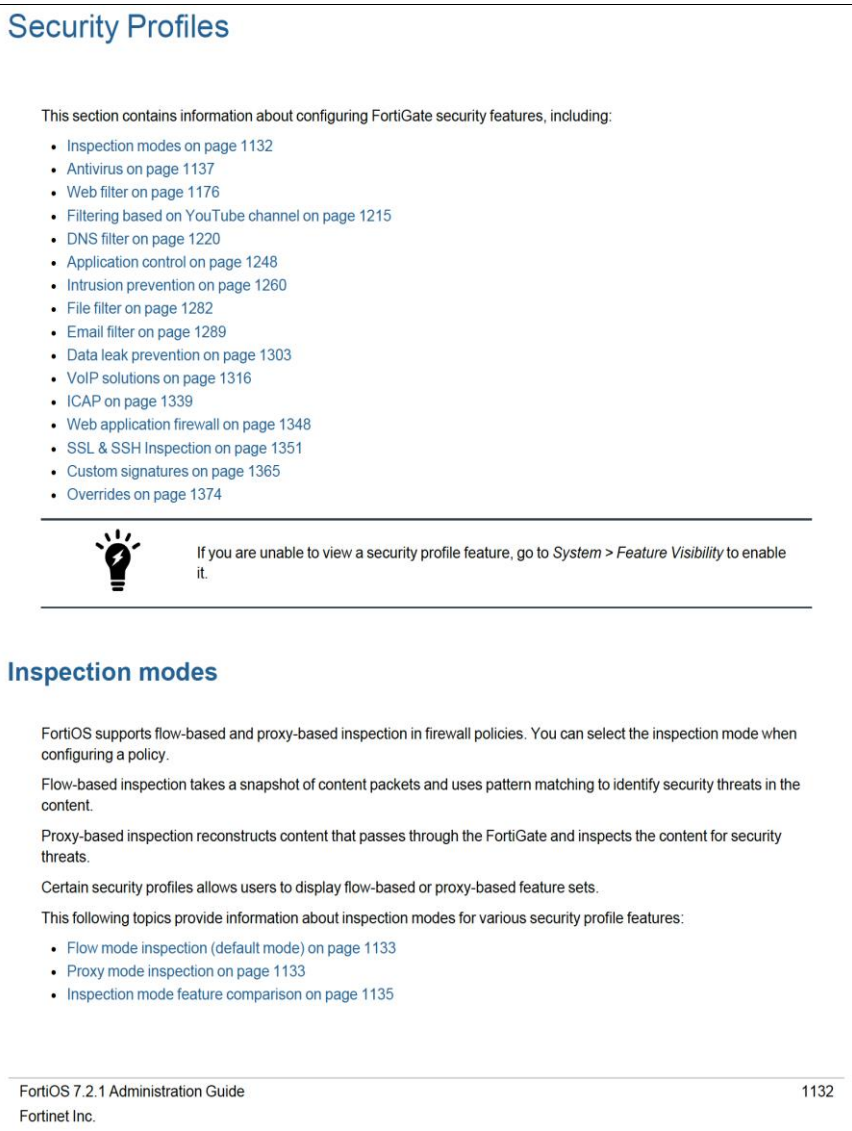


Analisando a documentação do recurso apresentada, o Link apresentado comprova o item solicitado no edital, portanto para o nosso entendimento, essa segunda documentação fica claro que o produto oferecido pela licitante atende ao referido Item do Edital.

ITEM 4.10 do Edital	A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload";

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na página 1132 do Manual FortiOS-7.2.1-Administration_Guide apresenta o início das informações sobre a configuração dos recursos de segurança do FortiGate e não indica qualquer ligação com a solicitação do referido Item do Edital, portanto, entendemos que não é possível comprovar o atendimento. Segue abaixo o print da página 1132 indicada na comprovação e retirada do Manual FortiOS-7.2.1 para melhor entendimento e ilustração:



Security Profiles

This section contains information about configuring FortiGate security features, including:

- Inspection modes on page 1132
- Antivirus on page 1137
- Web filter on page 1176
- Filtering based on YouTube channel on page 1215
- DNS filter on page 1220
- Application control on page 1248
- Intrusion prevention on page 1260
- File filter on page 1282
- Email filter on page 1289
- Data leak prevention on page 1303
- VoIP solutions on page 1316
- ICAP on page 1339
- Web application firewall on page 1348
- SSL & SSH Inspection on page 1351
- Custom signatures on page 1365
- Overrides on page 1374

If you are unable to view a security profile feature, go to *System* > *Feature Visibility* to enable it.

Inspection modes

FortiOS supports flow-based and proxy-based inspection in firewall policies. You can select the inspection mode when configuring a policy.

Flow-based inspection takes a snapshot of content packets and uses pattern matching to identify security threats in the content.

Proxy-based inspection reconstructs content that passes through the FortiGate and inspects the content for security threats.

Certain security profiles allows users to display flow-based or proxy-based feature sets.

This following topics provide information about inspection modes for various security profile features:

- Flow mode inspection (default mode) on page 1133
- Proxy mode inspection on page 1133
- Inspection mode feature comparison on page 1135

FortiOS 7.2.1 Administration Guide 1132
Fortinet Inc.

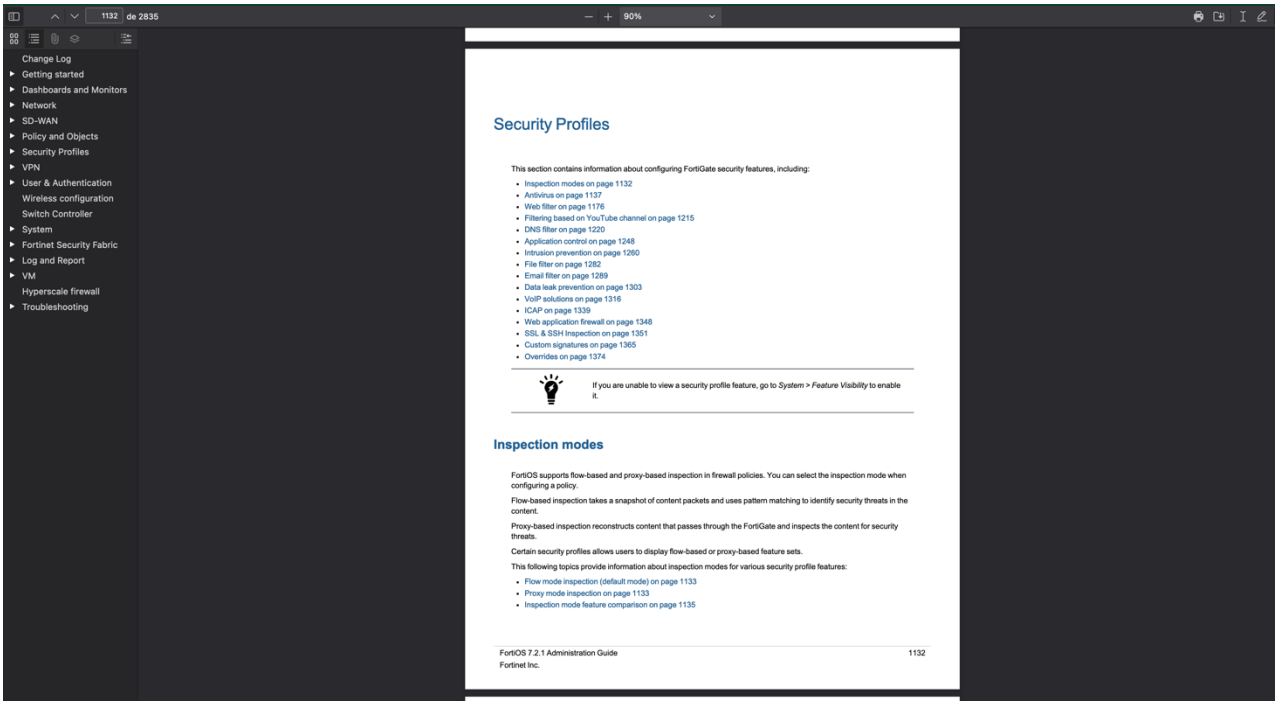
ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

Segundo o fornecedor, o item é atendido pela solução, conforme se verifica do documento FortiOS-7.2.1-Administration_Guide enviado originalmente, na página 1132 da planilha ponto a ponto de atendimento, especificamente em:

To configure a file filter in the GUI: => ""Configure the settings as required."" Traffic: Incoming, Outgoing e Both"

--> Contudo, o texto citado no recurso como comprobatório não consta no conteúdo da página citada. Segue abaixo o print retirado da página e não pudemos identificar essa "planilha ponto a ponto de atendimento que informam que consta na referida página. Segue abaixo o print da página informada:



Para lisura da análise, esse print foi retirado direto do Manual FortiOS-7.2.1-Administration_Guide do link público https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf.

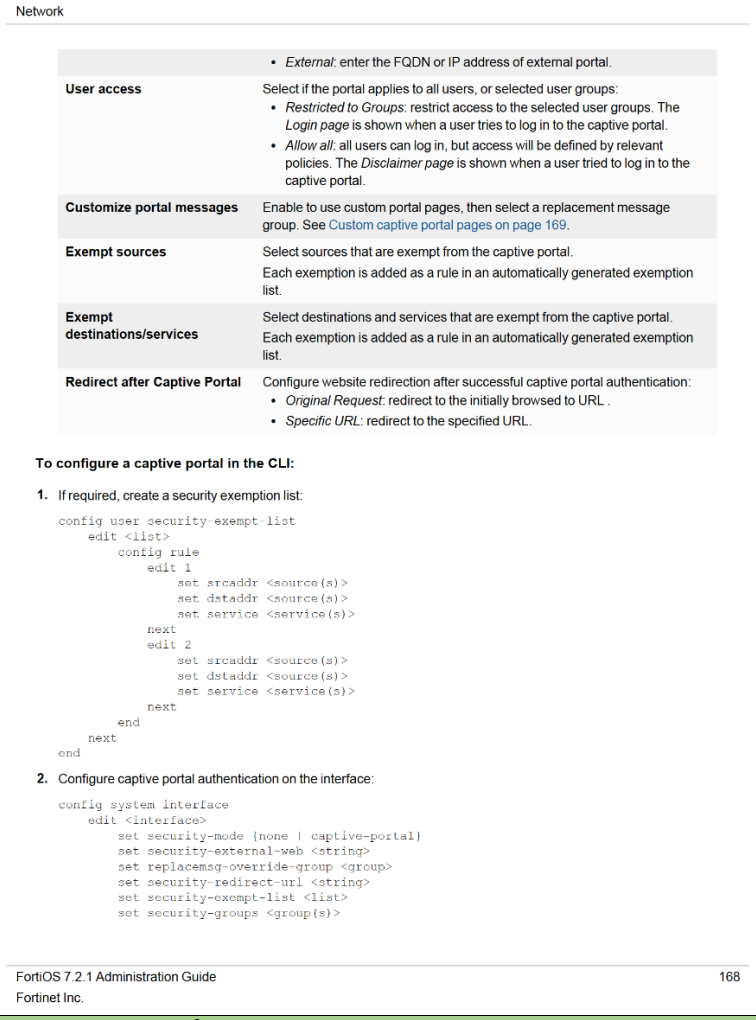
Desta forma, a segunda documentação enviada no recurso **não comprova (5)** o atendimento a este item do Edital.

ITEM 4.11 do Edital	A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na página 168 do Manual FortiOS-7.2.1-Administration_Guide apresenta instruções de configuração da funcionalidade do Captive Portal, no entanto, o Item do Edital está solicitando que a notificação ou redirect seja enviado ao usuário quando ocorrer o match em uma das categorias dos Itens 4.9.1 a 4.9.7. Como a comprovação informada foi referente a funcionalidade de Captive Portal que, não tem

nenhuma relação com a aplicação de políticas, mais sim, na autenticação de usuários fica claro o não atendimento do referido Item do Edital.
Segue abaixo o print da página 168 indicada na comprovação e retirada do Manual FortiOS-7.2.1 para melhor entendimento e ilustração:



Network

	• *External*: enter the FQDN or IP address of external portal.
User access	Select if the portal applies to all users, or selected user groups: • *Restricted to Groups*: restrict access to the selected user groups. The *Login page* is shown when a user tries to log in to the captive portal. • *Allow all*: all users can log in, but access will be defined by relevant policies. The *Disclaimer page* is shown when a user tried to log in to the captive portal.
Customize portal messages	Enable to use custom portal pages, then select a replacement message group. See Custom captive portal pages on page 169.
Exempt sources	Select sources that are exempt from the captive portal. Each exemption is added as a rule in an automatically generated exemption list.
Exempt destinations/services	Select destinations and services that are exempt from the captive portal. Each exemption is added as a rule in an automatically generated exemption list.
Redirect after Captive Portal	Configure website redirection after successful captive portal authentication: • *Original Request*: redirect to the initially browsed to URL . • *Specific URL*: redirect to the specified URL.

To configure a captive portal in the CLI:

1. If required, create a security exemption list:

```
config user security-exempt-list
    edit <list>
        config rule
            edit 1
                set srcaddr <source(s)>
                set dstaddr <source(s)>
                set service <service(s)>
            next
            edit 2
                set srcaddr <source(s)>
                set dstaddr <source(s)>
                set service <service(s)>
            next
        end
    next
end
```

2. Configure captive portal authentication on the interface:

```
config system interface
    edit <interface>
        set security-mode {none | captive-portal}
        set security-external-web <string>
        set replacemsg-override-group <group>
        set security-redirect-url <string>
        set security-exempt-list <list>
        set security-groups <group(s)>
```

FortiOS 7.2.1 Administration Guide 168
Fortinet Inc.

ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

Segundo o fornecedor, o item é atendido pela solução, conforme se verifica no trecho “New replacement messages” disponível em:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-file-filtering/ta-p/197098

Em um primeiro momento, após avaliação da nova comprovação, o referido link descreve como usar a filtragem de arquivo que é usada para bloquear/logar certos tipos de arquivo usando filtro da web e filtro de e-mail. Não identificamos em nenhum momento a parte onde o administrador possa realizar a configuração do envio de uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias mencionada no referido edital.

Web Filter File Filter action as *Block*:

```
1: date=2019-03-19 time=09:42:15 logid="0346012673" type="utm" subtype="webfilter"
eventtype="file_filter" level="warning" vd="vd1" eventtime=1548438135 policyid=1
sessionid=29449 srcip=10.1.100.22 srcport=52816 srcintf="dmz" srcintfrole="undefined"
dstip=172.16.200.55 dstport=80 dstintf="wan1" dstintfrole="undefined" proto=6
service="HTTP" hostname="172.16.200.55" profile="webfilter-filefilter" action="blocked"
reqtype="direct" url="/app_data/test1.pdf" sentbyte=0 rcvdbyte=0 direction="incoming"
filename="test1.pdf" filtername="filter1" filetype="pdf" msg="File was blocked by file
filter."
```

Web Filter File Filter action as *Log*:

```
2: date=2019-03-19 time=10:48:23 logid="0346012672" type="utm" subtype="webfilter"
eventtype="file_filter" level="notice" vd="vd1" eventtime=1548442102 policyid=1
sessionid=521 srcip=10.1.100.22 srcport=52894 srcintf="dmz" srcintfrole="undefined"
dstip=172.16.200.55 dstport=80 dstintf="wan1" dstintfrole="undefined" proto=6
service="HTTP" hostname="172.16.200.55" profile="webfilter-filefilter"
action="passthrough" reqtype="direct" url="/app_data/park.jpg" sentbyte=0 rcvdbyte=0
direction="incoming" filename="park.jpg" filtername="filter2" filetype="jpeg" msg="File
was detected by file filter."
```

Email Filter File Filter action as *Block*:

```
1: date=2019-01-25 time=15:20:16 logid="0554020511" type="utm" subtype="emailfilter"
eventtype="file_filter" level="warning" vd="vdom1" eventtime=1548458416 policyid=1
sessionid=2881 srcip=10.1.100.12 srcport=45974 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.56 dstport=143 dstintf="port1" dstintfrole="undefined" proto=6
service="IMAP" action="blocked" from="emailuser1@qa.fortinet.com"
to="emailuser2@qa.fortinet.com" recipient="emailuser2" direction="incoming" subject="EXE
file block" size="622346" attachment="yes" filename="putty.exe" filtername="filter1"
filetype="exe"
```

Email Filter File Filter action as *Log*:

```
1: date=2019-01-25 time=15:23:16 logid="0554020510" type="utm" subtype="emailfilter"
eventtype="file_filter" level="notice" vd="vdom1" eventtime=1548458596 policyid=1
sessionid=3205 srcip=10.1.100.12 srcport=55664 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.56 dstport=25 dstintf="port1" dstintfrole="undefined" proto=6
service="SMTP" profile="emailfilter-file-filter" action="detected"
from="emailuser1@qa.fortinet.com" to="emailuser2@qa.fortinet.com"
sender="emailuser1@qa.fortinet.com" recipient="emailuser2@qa.fortinet.com"
direction="outgoing" subject="PDF file log" size="390804" attachment="yes"
filename="fortiauto.pdf" filtername="filter2" filetype="pdf"
```

New replacement messages.

Web Filter File Filter blocking upload:

```
You are not permitted to upload the file "%%FILE%%".
```

Web Filter File Filter blocking download:

```
Your attempt to access the file "%%FILE%%" has been blocked by your system
administrator.
```

Email Filter File Filter blocking emails:

```
This email has been blocked. The file %%FILE%% was blocked due to its file type or
properties
```

Ao final, contudo, podemos identificar que o equipamento ofertado pela licitante envia notificações para o usuário quando há match de regras, sempre que um arquivo malicioso for reconhecido em Uploads, Downloads e Anexos em e-mails. Logo, atende ao que se pede no item deste edital.

ITEM 5.11 do Edital	O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na página 599 do Manual FortiOS-7.2.1-Administration_Guide apresenta um exemplo de configuração de uma funcionalidade de SD-WAN utilizando traffic shaping e QoS. O referido Item do Edital está bem claro ao solicitar quais comandos FTP são aceitos e quais são bloqueados através da funcionalidade de IPS, portanto, fica claro o não atendimento do referido Item do Edital.

Segue abaixo o print da página 599 indicada na comprovação e retirada do Manual FortiOS-7.2.1 para melhor entendimento e ilustração:

SD-WAN

Sample configuration

This example shows a typical customer usage where the customer's SD-WAN uses the default zone, and has two member: wan1 and wan2, each set to 10Mb/s.

An overview of the procedures to configure SD-WAN traffic shaping and QoS with SD-WAN includes:

1. Give HTTP/HTTPS traffic high priority and give FTP low priority so that if there are conflicts, FortiGate will forward HTTP/HTTPS traffic first.
2. Even though FTP has low priority, configure FortiGate to give it a 1Mb/s guaranteed bandwidth on each SD-WAN member so that if there is no FTP traffic, other traffic can use all the bandwidth. If there is heavy FTP traffic, it can still be guaranteed a 1Mb/s bandwidth.
3. Traffic going to specific destinations such as a VOIP server uses wan1 to forward, and SD-WAN forwards with an Expedited Forwarding (EF) DSCP tag 101110.

To configure SD-WAN traffic shaping and QoS with SD-WAN in the GUI:

1. On the FortiGate, add wan1 and wan2 as SD-WAN members, then add a policy and static route.
   See SD-WAN quick start on page 519.
2. Add a firewall policy with *Application Control* enabled. See Configuring firewall policies for SD-WAN on page 522.
3. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shapers* tab, and edit *low-priority*.
   a. Enable *Guaranteed Bandwidth* and set it to *1000* kbps.
4. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
   a. Name the traffic shaping policy, for example, *HTTP-HTTPS*.
   b. Set the following:

Source	*all*
Destination	*all*
Service	*HTTP* and *HTTPS*
Outgoing interface	*virtual-wan-link*
Shared Shaper	Enable and set to *high-priority*
Reverse Shaper	Enable and set to *high-priority*

   c. Click *OK*.
5. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
   a. Name the traffic shaping policy, for example, *FTP*.
   b. Set the following:

Source	*all*
Destination	*all*
Service	*FTP*, *FTP_GET*, and *FTP_PUT*
Outgoing interface	*virtual-wan-link*
Shared Shaper	Enable and set to *low-priority*
Reverse Shaper	Enable and set to *low-priority*

   c. Click *OK*

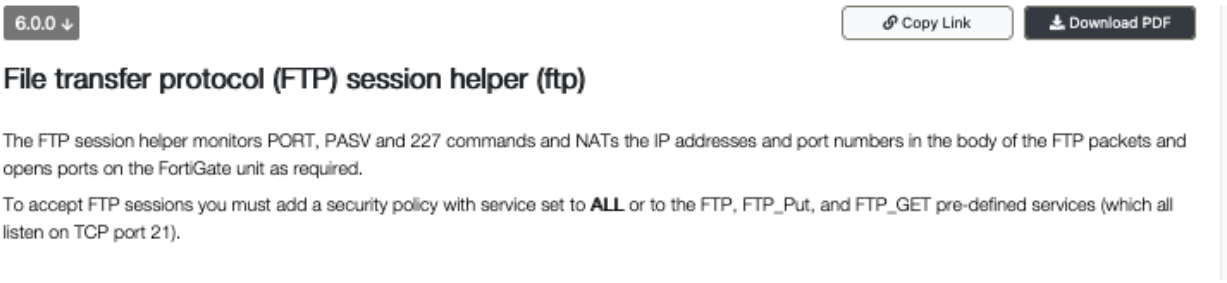
FortiOS 7.2.1 Administration Guide 599
Fortinet Inc.

ANÁLISE DO RECURSO APRESENTADO

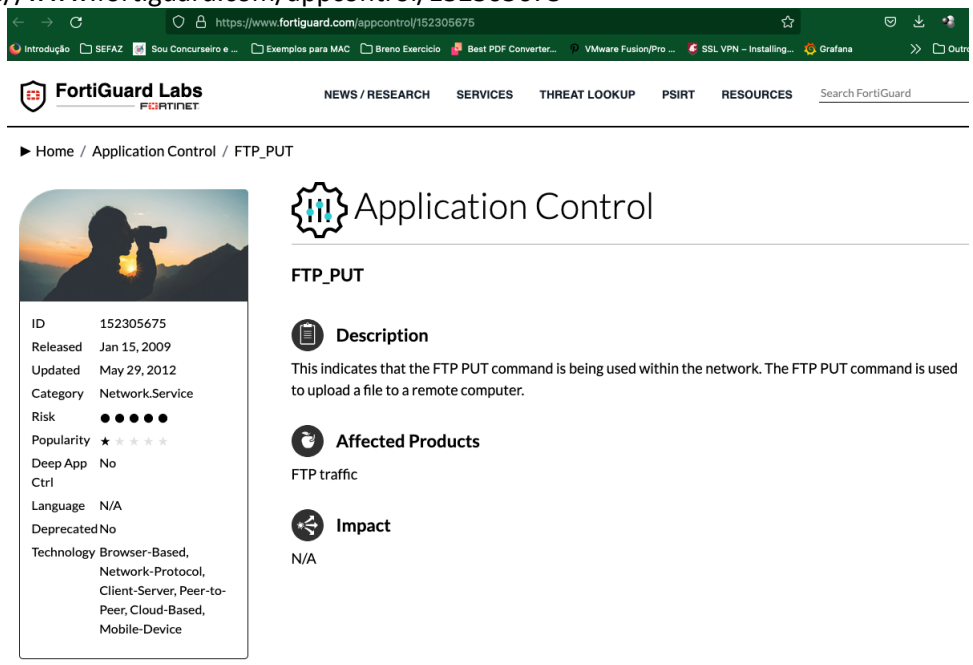
URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7e513936-06c7-11ed-bb32-fa163e15d75b/FortiOS-7.2.1-Administration_Guide.pdf

Já no recurso, segundo o fornecedor, o item é atendido pela solução ofertada, conforme é apresentado nos links abaixo com seus respectivos prints de tela:

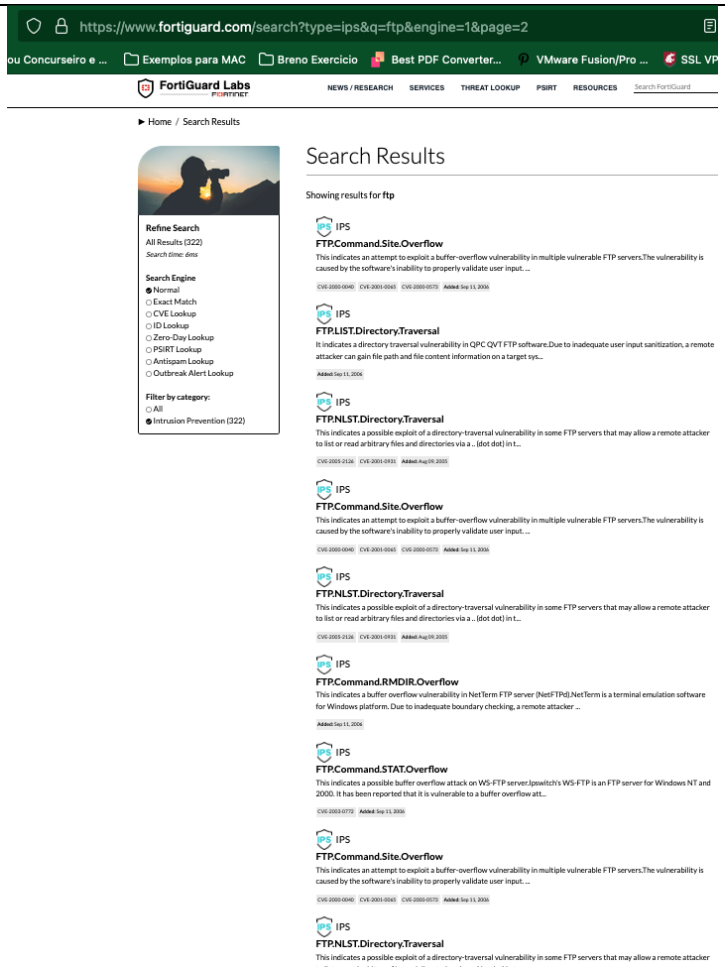
- https://docs.fortinet.com/document/fortigate/6.0.0/handbook/932390/file-transfer-protocol-ftp-session-helper-ftp



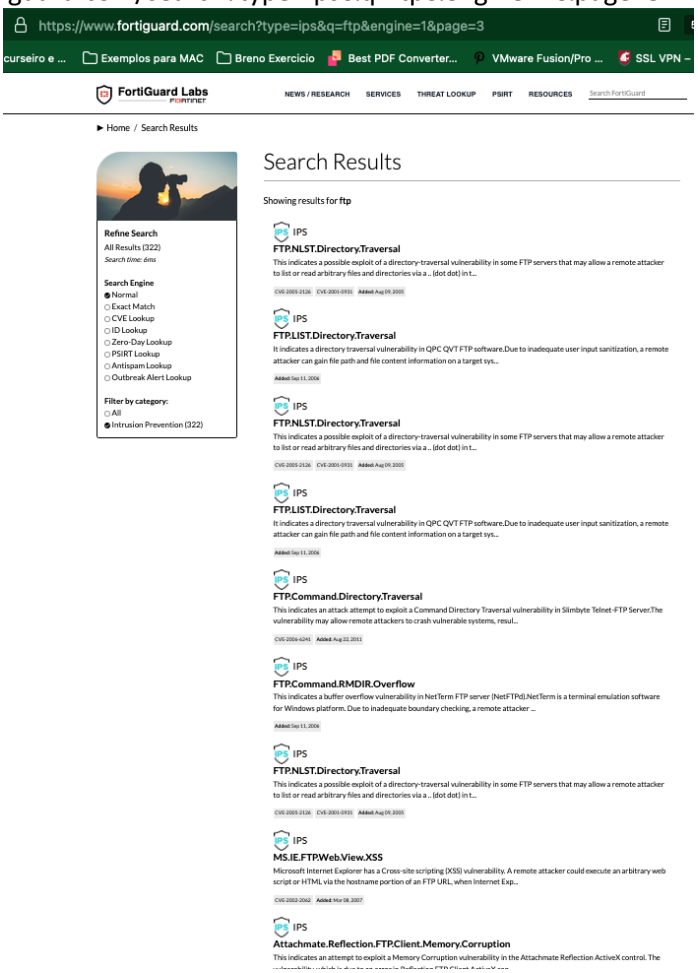
- https://www.fortiguard.com/appcontrol/152305675



- https://www.fortiguard.com/search?type=ips&q=ftp&engine=1&page=2


https://www.fortiguard.com/search?type=ips&q=ftp&engine=1&page=2
FortiGuard Labs
NEWS / RESEARCH
SERVICES
THREAT LOOKUP
PSIRT
RESOURCES
► Home / Search Results
Search Results
Showing results for ftp
Refine Search
All Results (322)
Search Engine
Normal
Exact Match
CVE Lookup
ID Lookup
Zero-Day Lookup
PSIRT Lookup
Antispam Lookup
Outbreak Alert Lookup
Filter by category:
All
Intrusion Prevention (322)
IPS
FTP.Command.Site.Overflow
IPS
FTP.LIST.Directory.Traversal
IPS
FTP.NLST.Directory.Traversal
IPS
FTP.Command.Site.Overflow
IPS
FTP.NLST.Directory.Traversal
IPS
FTP.Command.RMDIR.Overflow
IPS
FTP.Command.STAT.Overflow
IPS
FTP.Command.Site.Overflow
IPS
FTP.NLST.Directory.Traversal

- https://www.fortiguard.com/search?type=ips&q=ftp&engine=1&page=3



Após análise da nova documentação (defasada) apresentada e para o nosso entendimento, a solução ofertada pela LICITANTE atendeu a este item do edital na versão 6.0.0. Contudo, para ser considerado válido, a comprovação a ser apresentada deveria ser da documentação na versão FortiOS-7.2.1 ou superior.
Desta forma a segunda documentação enviada, **não comprova** (6) o atendimento a este item do Edital.

ITEM 8.4 do Edital	A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A comprovação **não** indica, na página 7 do "FortiSandbox datasheet", especificamente o suporte às versões do Office solicitadas no referido Item do Edital. Portanto, no nosso entendimento a comprovação não atende o referido Item do Edital.

Segue abaixo o print da página 7 indicada na comprovação e retirada do “FortiSandbox datasheet” para melhor entendimento e ilustração:

INTEGRATION MATRIX

	FORTIGATE	FORTICLIENT	FORTIMAIL	FORTIWEB	FORTIADC	FORTIPROXY
FortiSandbox Appliance and VM	FortiOS V5.6+	FortiClient for Windows OS V5.6+	FortiMail OS V5.4+	FortiWeb OS V5.6+	FortiADC OS V5.0+	FortiProxy OS V1.2.3+
FortiSandbox Cloud - PaaS/ Hosted	FortiOS V6.4.2+, 6.2.5+	FortiClient for Windows OS V6.4.4+, 7.0+	FortiMail V6.4.3+			
FortiGuard AI-based Inline Sandbox Service	FortiOS V7.2.1+					

ORDER INFORMATION

PRODUCT	SKU	DESCRIPTION
FortiSandbox 500F	FSA-500F	Advanced Threat Protection System - 4 x GE RJ45, 2 licensed Windows/Linux/Android VMs with Win7, Win10, and (1) MS Office licenses included. Upgradable to a maximum of 6 VMs, refer to FSA-500F-UPG-LIC-4 and/or FC-10-FS5HF-176-02-DD SKU
FortiSandbox 1000F/-DC	FSA-1000F FSA-1000F-DC	Advanced Threat Protection System - 4 x GE RJ45, 4 x GE SFP slots, 2 licensed Windows/Linux/Android VMs with Win7, Win10, and (1) MS Office licenses included. Upgradable to a maximum of 14 licensed VMs, refer to FSA-1000FUPG-LIC-6 and/or FC-10-FS1KF-176-02-DD SKU. Redundant PSU (optional), refer to SP-FSA1000F-PS SKU.
FortiSandbox 2000E	FSA-2000E	Advanced Threat Protection System - 4 x GE RJ45, 2 × 10 GbE SFP+ Slots, redundant PSU, 4 licensed Windows/ Linux/Android VMs with Win7 , Win8 , Win10 and (1) MS office licenses included. Upgradable to a maximum of 24 VMs, refer to FSA-2000E-UPG-LIC-10 and/or FC-10-SA20K-176-02-DD SKU.
FortiSandbox 3000F	FSA-3000F	Advanced Threat Protection System - 4 x GE RJ45, 2 × 10 GbE SFP+ Slots, redundant PSU, 8 VMs with (6) Win10, (2) Win7 and (1) MS office licenses included. Upgradable to a maximum of 72 licensed VMs, refer to FSA-3000F-UPGLIC-32 and/or FC-10-SA3KF-176-02-DD SKU.
FortiSandbox-VM	FSA-VM-00	FortiSandbox-VM Virtual Appliance with 0 VMs included and maximum expansion limited to 8 total VMs per node, up to 99 nodes per cluster.
FortiSandbox Windows Cloud VM	FC-10-FSA01-195-02-DD	FortiSandbox Windows Cloud VM Service for (5) Windows VMs and maximum expansion limited to (200) Windows Cloud VMs per FortiSandbox VM.
FortiSandbox macOS Cloud VM	FC-10-FSA01-192-02-DD	macOS Cloud VM Service for (2) macOS X VMs and maximum expansion limited to (8) macOS X VMs per FortiSandbox (Appliance/VM).
FortiSandbox Cloud Service	FC1-10-SACLP-433-01-DD	Cloud VM Service for FortiSandbox Cloud. Expands Cloud VM for Windows/macOS/Linux/Android by 1. Maximum of 200 VMs per FortiSandbox. Requires FortiCloud Premium SKU FC-15-CLDPS-219-02-DD
	FC2-10-SACLP-433-01-DD	Cloud VM Service for FortiSandbox Cloud. Expands Cloud VMs for Windows/MacOS/Linux/Android by 5. Maximum of 200 VMs per FortiSandbox. Requires FortiCloud Premium SKU FC-15-CLDPS-219-02-DD
FortiGuard AI-Based Inline Sandbox Service	FC-10-0060F-577-02-DD	A-la-carte service, which includes inline blocking for sandbox and AI/NDR detections, plus log enrichment for SOC teams.
Optional Accessories		
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
AC Power Supply	SP-FSA1000F-PS	AC power supply for FSA-1000F, FDC-1000F, and FIS-1000F modules only.
AC Power Supply	SP-FSA3000F-PS	AC power supply for FSA-3000F and FAC-3000F modules only.
DC Power Supply	SP-FSA1000F-DC-PS	DC power supply for FSA-1000F-DC module only.

FORTINET

www.fortinet.com

FSA-DAT-R46-20220913

ANÁLISE DO RECURSO APRESENTADO

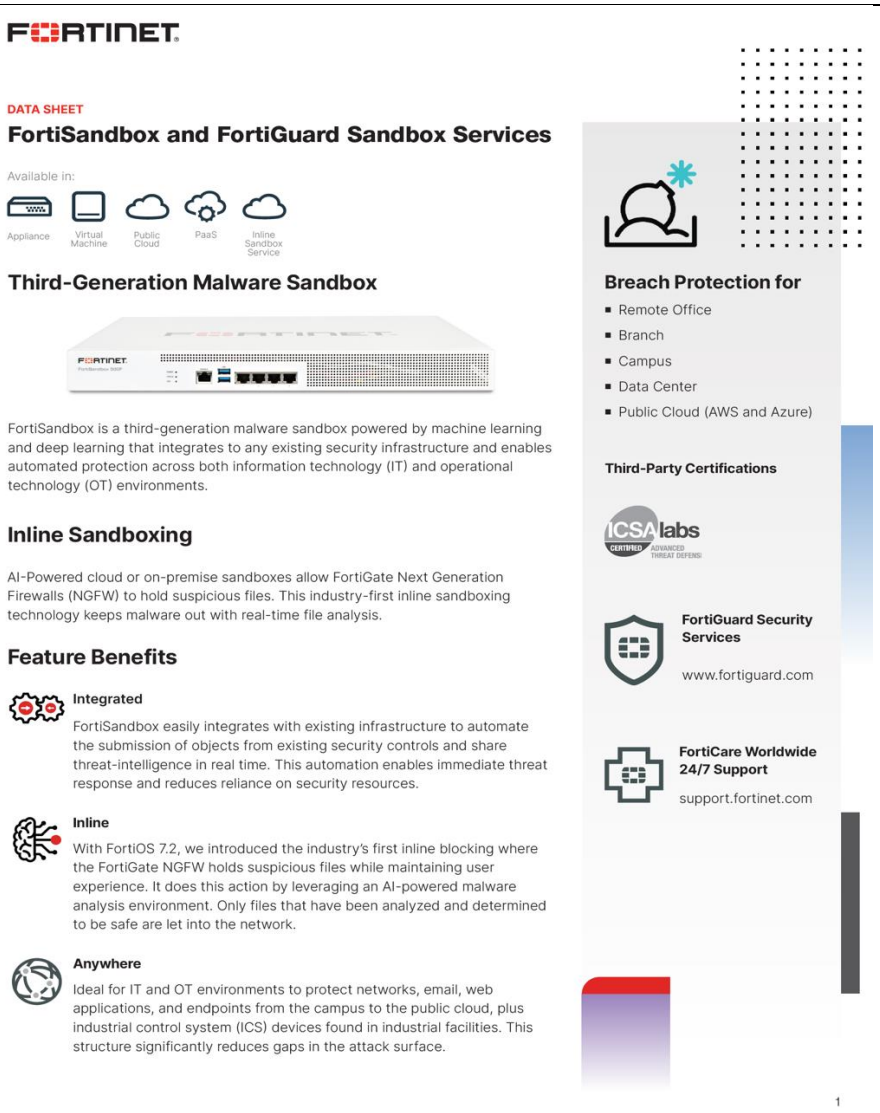
URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

Segundo o fornecedor, o item é atendido pela solução, conforme os novos links abaixo enviados:

- https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/inline-sandboxing

• https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf Especificamente, na página 5, do FortiSandbox Data-Sheet apresentado neste segundo link. Tem-se na seguinte menção: “OS type supported: Windows 10, Windows 8.1, Windows 7, macOS, Linux, Android, and ICS systems”. O questionamento realizado anteriormente não foi referente aos tipos de sistemas operacionais suportados e sim, sobre as distribuições Office suportadas. Com relação aos tipos de sistemas operacionais a solução ofertada pela LICITANTE está de acordo com o solicitado neste item do edital, no entanto, da mesma forma da comprovação anterior, assim como nesta mencionada nos 02 (dois) links acima, não foi possível comprovar a compatibilidade com as seguintes distribuições do Office 2003, 2010, 2013 e 20016. Com o exposto acima e para o nosso entendimento, enquanto não for apresentado a comprovação da compatibilidade com as distribuições do Office, a solução ofertada pela LICITANTE não atende integralmente a este Item do Edital. Desta forma, mesmo considerando a segunda documentação enviada no recurso, **não há comprovação** (7) do atendimento a este item do Edital.

ITEM 8.9 do Edital	A solução de prevenção de ameaças avançadas (Sandboxing) contra-ataques persistentes e Zero-Day, deve ser habilitada e funcionar de forma independente, ou seja, não sendo obrigatório o uso e ativação de funcionalidades ou engines de anti-virus para a mesma ter o seu devido funcionamento;
ANÁLISE DA COMPROVAÇÃO APRESENTADA	
Não foi possível visualizar na comprovação indicada da página 1 do “FortiSandbox datasheet” o atendimento do referido Item do Edital, portanto, no nosso entendimento a comprovação não atende. Segue abaixo o print da página 1 indicada na comprovação e retirada do “FortiSandbox datasheet” para melhor entendimento e ilustração:	



FORTINET

DATA SHEET

FortiSandbox and FortiGuard Sandbox Services

Available in:

Appliance · Virtual Machine · Public Cloud · PaaS · Inline Sandbox Service

Third-Generation Malware Sandbox

FortiSandbox is a third-generation malware sandbox powered by machine learning and deep learning that integrates to any existing security infrastructure and enables automated protection across both information technology (IT) and operational technology (OT) environments.

Inline Sandboxing

AI-Powered cloud or on-premise sandboxes allow FortiGate Next Generation Firewalls (NGFW) to hold suspicious files. This industry-first inline sandboxing technology keeps malware out with real-time file analysis.

Feature Benefits

Integrated

FortiSandbox easily integrates with existing infrastructure to automate the submission of objects from existing security controls and share threat-intelligence in real time. This automation enables immediate threat response and reduces reliance on security resources.

Inline

With FortiOS 7.2, we introduced the industry's first inline blocking where the FortiGate NGFW holds suspicious files while maintaining user experience. It does this action by leveraging an AI-powered malware analysis environment. Only files that have been analyzed and determined to be safe are let into the network.

Anywhere

Ideal for IT and OT environments to protect networks, email, web applications, and endpoints from the campus to the public cloud, plus industrial control system (ICS) devices found in industrial facilities. This structure significantly reduces gaps in the attack surface.

Breach Protection for

- Remote Office
- Branch
- Campus
- Data Center
- Public Cloud (AWS and Azure)

Third-Party Certifications

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

FortiGuard Security Services

www.fortiguard.com

FortiCare Worldwide 24/7 Support

support.fortinet.com

1

ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

O item é atendido pela solução, conforme se verifica em: https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/inline-sandboxing.

Após análise da segunda documentação enviada, fica claro o funcionamento do recurso de Sandboxing e que o referido recurso não faz o uso obrigatório e ativação de funcionalidades ou engines de anti-virus para que tenha seu devido funcionamento. Portanto, para o nosso entendimento, a solução ofertada estaria de acordo com o Item deste Edital.	
ITEM 8.10 do Edital	8.10. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;
ANÁLISE DA COMPROVAÇÃO APRESENTADA	
No nosso entendimento, a lista de part-numbers informada não consta quais e quantas licenças de Windows e pacote Office estarão disponíveis para a solução do FortiSandbox, portanto, não foi possível comprovar o atendimento do referido Item do Edital.	
ANÁLISE DO RECURSO APRESENTADO	
Segundo o fornecedor, o item é atendido pela solução, conforme se verifica nos links abaixo: • https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/inline-sandboxing • https://www.fortinet.com/content/dam/fortinet/assets/datasheets/FortiSandbox.pdf Especificamente, na página 5, do FortiSandbox Data-Sheet apresentado neste segundo link. Tem-se na seguinte menção: “OS type supported: Windows 10, Windows 8.1, Windows 7, macOS, Linux, Android, and ICS systems”. Desta forma, mesmo considerando a segunda documentação enviada no recurso, **não ficou claro a comprovação (8), principalmente quanto as distribuições Office;**	
ITEM 8.14 do Edital	A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
ANÁLISE DA COMPROVAÇÃO APRESENTADA	
A comprovação indicada na página 84 do Manual FortiSandbox-4.2.0-Administration_Guide apresenta a continuação do recurso de “URL Job Search” iniciada na página 83 e não possui nenhuma relação com o Item do Edital, portanto, para o nosso entendimento não foi possível comprovar o atendimento. Segue abaixo o print das páginas 83 e 84 indicada na comprovação e retirada do Manual FortiSandbox-4.2.0-Administration_Guide para melhor entendimento e ilustração:	

The following information is displayed:

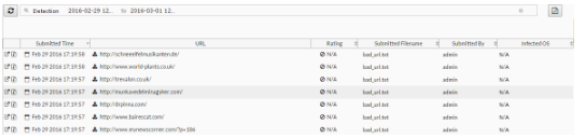
Total Jobs	The number of jobs displayed and the total number of jobs.

The displayed columns are determined by settings defined in *System > Job View Settings > File Detection Columns* page. For more information, see Job View Settings on page 176.

URL Job Search

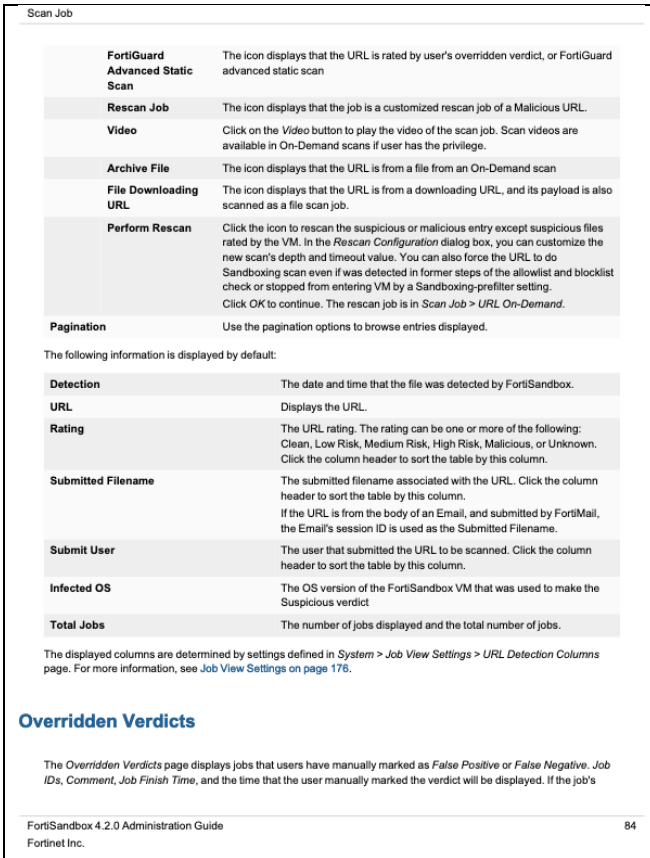
To view all URL scan jobs and search URLs, go to *Scan Job > URL Job Search*. You can apply search filters to drill down the information displayed. URLs can be searched based on different criteria, and a snapshot report can be created for all search results.

If the device is the primary node of a cluster, all jobs processed by the cluster are available to be searched. If the device is a worker node of a cluster, only jobs processed by this device are available to be searched.



The following options are available:

Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Search Field	Enter the detection time frame and click to add additional search filters for Destination, Device, Infected OS Job ID, Job Status, Rated By, Rating, Scan Unit, Submit User, Submitted Filename and URL. When the search criteria is *Submitted Filename*, click the = sign to toggle between the exact and pattern search.
Time Period	Select a time period to apply to the search.
Export to Report	Select to open the Report Generator dialog box. Select to generate a PDF or CSV report. During generation, do not close the dialog box or navigate away from the page. You can wait till the report is ready to view, or navigate away and find the report later in *Log & Report > Report Center* page.
Customize	Click the *Customize* icon to customize the Job View settings page. For more information, see Job View Settings on page 176.
Action	
View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.



Scan Job

FortiGuard Advanced Static Scan	The icon displays that the URL is rated by user's overridden verdict, or FortiGuard advanced static scan
Rescan Job	The icon displays that the job is a customized rescan job of a Malicious URL.
Video	Click on the *Video* button to play the video of the scan job. Scan videos are available in On-Demand scans if user has the privilege.
Archive File	The icon displays that the URL is from a file from an On-Demand scan
File Downloading URL	The icon displays that the URL is from a downloading URL, and its payload is also scanned as a file scan job.
Perform Rescan	Click the icon to rescan the suspicious or malicious entry except suspicious files rated by the VM. In the *Rescan Configuration* dialog box, you can customize the new scan's depth and timeout value. You can also force the URL to do Sandboxing scan even if was detected in former steps of the allowlist and blocklist check or stopped from entering VM by a Sandboxing-prefilter setting. Click *OK* to continue. The rescan job is in *Scan Job > URL On-Demand*.
Pagination	Use the pagination options to browse entries displayed.

The following information is displayed by default:

Detection	The date and time that the file was detected by FortiSandbox.
URL	Displays the URL.
Rating	The URL rating. The rating can be one or more of the following: Clean, Low Risk, Medium Risk, High Risk, Malicious, or Unknown. Click the column header to sort the table by this column.
Submitted Filename	The submitted filename associated with the URL. Click the column header to sort the table by this column. If the URL is from the body of an Email, and submitted by FortiMail, the Email's session ID is used as the Submitted Filename.
Submit User	The user that submitted the URL to be scanned. Click the column header to sort the table by this column.
Infected OS	The OS version of the FortiSandbox VM that was used to make the Suspicious verdict
Total Jobs	The number of jobs displayed and the total number of jobs.

The displayed columns are determined by settings defined in *System > Job View Settings > URL Detection Columns* page. For more information, see Job View Settings on page 176.

Overridden Verdicts

The *Overridden Verdicts* page displays jobs that users have manually marked as *False Positive* or *False Negative*. *Job IDs*, *Comment*, *Job Finish Time*, and the time that the user manually marked the verdict will be displayed. If the job's

FortiSandbox 4.2.0 Administration Guide 84
Fortinet Inc.

ANALISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4f5a6250-a945-11ec-9fd1-fa163e15d75b/FortiSandbox-4.2.0-Administration_Guide.pdf

Segundo o fornecedor, o item é atendido pela solução, conforme se verifica em: https://docs.fortinet.com/document/fortigate/6.2.0/new-features/628165/external-block-list-threat-feed-file-hashes

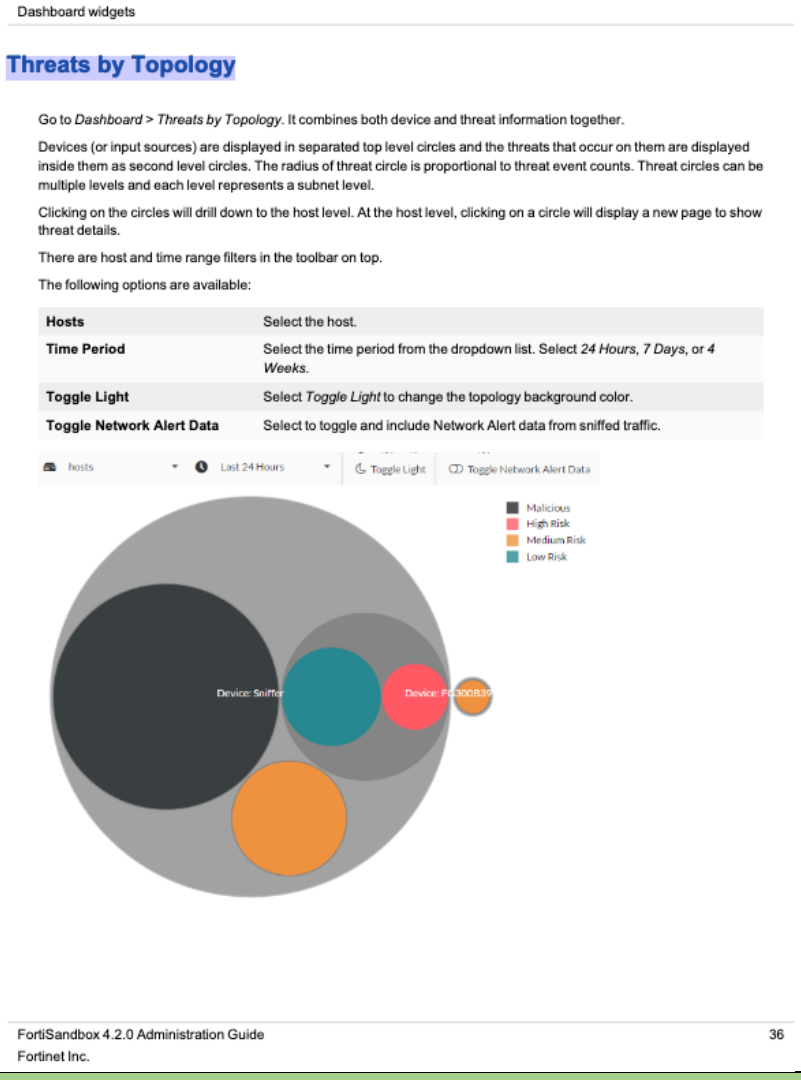
Após análise da segunda documentação (defasada) apresentada pela LICITANTE, ficou claro que a solução ofertada permite a criação de Whitelists baseados no Hash MD5. Contudo, para o nosso entendimento, a documentação comprobatória apresentada deveria ser a partir da versão vigente do IOS 7.2.1, e não 6.2.0, conforme apresentado.
Desta forma, **não se pode aceitar (7)** esta documentação enviada como evidência de comprovação de conformidade com este Item do Edital.

ITEMS 8.16 e 8.17 do Edital	Quantidade de arquivos que estão em emulação; Número de arquivos emulados;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na página 36 do Manual FortiSandbox-4.2.0-Administration_Guide apresenta como acessar e operar o Dashboard widgets do Theats by Topology e não possui nenhuma relação com os Items do Edital, portanto, para o nosso entendimento não foi possível comprovar o atendimento.

Segue abaixo o print da página 36 indicada na comprovação e retirada do Manual FortiSandbox-4.2.0-Administration_Guide para melhor entendimento e ilustração:



Dashboard widgets

Threats by Topology

Go to *Dashboard* > *Threats by Topology*. It combines both device and threat information together.

Devices (or input sources) are displayed in separated top level circles and the threats that occur on them are displayed inside them as second level circles. The radius of threat circle is proportional to threat event counts. Threat circles can be multiple levels and each level represents a subnet level.

Clicking on the circles will drill down to the host level. At the host level, clicking on a circle will display a new page to show threat details.

There are host and time range filters in the toolbar on top.

The following options are available:

Hosts	Select the host.
Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Toggle Light	Select *Toggle Light* to change the topology background color.
Toggle Network Alert Data	Select to toggle and include Network Alert data from sniffed traffic.

ANALISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4f5a6250-a945-11ec-9fd1-fa163e15d75b/FortiSandbox-4.2.0-Administration_Guide.pdf

Segundo o fornecedor, o item é atendido pela solução, conforme se verifica no link enviado posteriormente:

- https://docs.fortinet.com/document/fortigate/7.2.0/new-features/351054/display-detailed-fortisandbox-analysis-and-downloadable-pdf-report

--> O Link acima apresenta como gerar um relatório detalhado da análise dos recursos de Sandbox e não apresenta a visão solicitada neste item do Edital que é a quantidade de arquivos que estão em emulação e o número de arquivos emulados.

- https://docs.fortinet.com/document/fortigate/7.2.3/administration-guide/215077

--> O próximo link, apresenta como um usuário pode adicionar um widget FortiView a um painel ou menu de árvore como um monitor. Portanto, também não apresenta a visão solicitada neste item do Edital que é a quantidade de arquivos que estão em emulação e o número de arquivos emulados.

Desta forma, no nosso entendimento, a comprovação apresentada nesta segunda documentação também **não apresenta evidências (8)** de que a solução ofertada pela LICITANTE atende este item do Edital.

ITEMS 8.19 e 8.20 do Edital	Arquivos scaneados; Arquivos maliciosos;

ANÁLISE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na página 37 do Manual FortiSandbox-4.2.0-Administration_Guide apresenta como acessar e operar o Dashboard widgets do Theats by Hosts e não possui nenhuma relação com os Itens do Edital, portanto, para o nosso entendimento não foi possível comprovar o atendimento.
Segue abaixo o print da página 37 indicada na comprovação e retirada do Manual FortiSandbox-4.2.0-Administration_Guide para melhor entendimento e ilustração:

Dashboard widgets

Threats by Hosts

On this page you can view and drill down all threats grouped by hosts. The Host can be a user name or email address (if it is available) or a device that is the target of a threat. This page displays all threats that have occurred to the user or victim host during a time period. Click the *View Jobs* icon or double-click an entry in the table to view the second level.

Threats by Hosts - level 1

The following options are available:

Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Export Data	Click the *Export Data* button to create a PDF or CSV snapshot report. You can wait till the report is ready to view, or navigate away and find the report later in *Log & Report* > *Report Center* page.
Search	Show or hide the search filter field.
Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Add Search Filter	Click the *Search Filter* field to add search filters. Click the *Cancel* icon to the left of the search filter to remove the specific filter. Click the *Clear All Filters* icon in the search filter field to clear all filters. In this page, the threat target host or user name can be the search criteria. You can input a partial value to search all records that contain it. Search filters can be used to filter the information displayed in the GUI.
View Job	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

Host/Username	The device and username that is the target of threats. Click the column header to sort the table by this column. **Note**: A duplicate user name or host from a different VDOM is considered a different user.
Device Name	The device name. Click the column header to sort the table by this column.
# of Malicious Files	The number of unique malicious files associated with the user for the time period selected. Click the column header to sort the table by this column.
# of Suspicious Files	The number of unique suspicious files associated with the user for the time period selected. Click the column header to sort the table by this column.
# of Network Threats	The number of unique network threats (attacker, botnet, and suspicious URL events) associated with the user for the time period selected. Click the column header to sort the table by this column.

FortiSandbox 4.2.0 Administration Guide 37
Fortinet Inc.

ANÁLISE DO RECURSO APRESENTADO

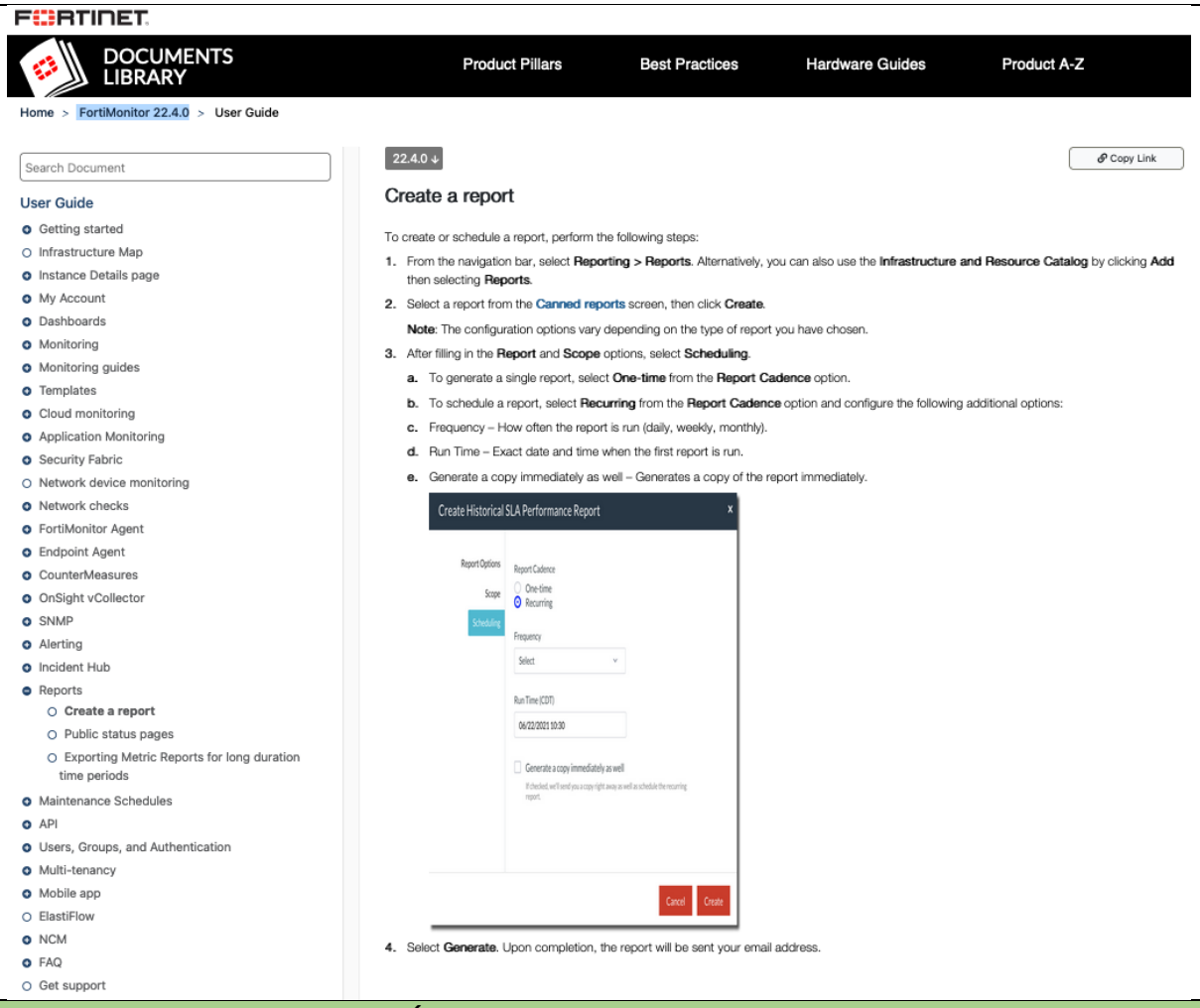
URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4f5a6250-a945-11ec-9fd1-fa163e15d75b/FortiSandbox-4.2.0-Administration_Guide.pdf

Segundo o fornecedor, o item é atendido pela solução, conforme se verifica em:

- https://docs.fortinet.com/document/fortigate/7.2.0/new-features/351054/display-detailed-fortisandbox-analysis-and-downloadable-pdf-report

--> O Link acima apresenta como gerar um relatório detalhado da análise dos recursos de Sandbox e não apresenta a visão solicitada neste item do Edital que são os arquivos scaneados e maliciosos. • https://docs.fortinet.com/document/fortigate/7.2.3/administration-guide/215077 --> O link acima apresenta como um usuário pode adicionar um widget FortiView a um painel ou menu de árvore como um monitor. Portanto, também não apresenta a visão solicitada neste item do Edital que são os arquivos scaneados e maliciosos. Portanto, para o nosso entendimento, **não há comprovação clara (9)** nem mesmo nesta segunda documentação apresentada de que a solução ofertada pela LICITANTE atende este item do Edital.

ITEM 10 do ANEXO I-C Edital	A solução deve possibilitar a exportação dos relatórios em pelo menos dois dos seguintes formatos: a. PDF. b. HTML. c. CSV.
ANÁLISE DA COMPROVAÇÃO APRESENTADA	
A comprovação indicada na URL "https://docs.fortinet.com/document/fortimonitor/22.4.0/user-guide/54183/create-a-report" da documentação on-line do FortiMonitor 22.4.0 apesar de apresentar como criar um Relatório, não foi possível comprovar em quais formatos é possível realizar a exportação dos relatórios. Ainda que se faça uma busca no manual on-line pelos textos "PDF" ou "CSV", nenhum resultado é encontrado. Portanto, no nosso entendimento, não foi possível comprovar o referido Item do Edital. Segue abaixo o print da URL indicada na comprovação e retirada do da documentação on-line do FortiMonitor 22.4.0 para melhor entendimento e ilustração:	



ANÁLISE DO RECURSO APRESENTADO

URL comprobatória do documento informado na planilha de comprovações, originalmente, enviada pela licitante:
https://docs.fortinet.com/document/fortimonitor/22.4.0/user-guide/54183/create-a-report

No recurso, segundo o fornecedor, o item é atendido pela solução, conforme enviado em novo link comprobatório:

- https://docs.fortinet.com/document/fortianalyzer/7.2.1/administration-guide/108255/creating-output-profiles

--> Após análise da segunda documentação apresentada pela LICITANTE, ficou claro que a solução ofertada onde se permite a exportação dos relatórios nos seguintes formatos HTML, PDF, XML, CSV e JASON, é a do produto FortyAnalyser e não FortiMonitor, conforme primeiro link comprobatório enviado e produto ofertado pelo fornecedor.
Desta forma, nem as documentações enviadas no recurso comprovam o atendimento a este item do Edital. Portanto, a segunda documentação enviada no recurso **não comprova (10)** o atendimento a este item do Edital.

ANÁLISE DA DOCUMENTAÇÃO APRESENTADA	
ITEM 12.1 do Edital	A LICITANTE deve apresentar no mínimo 03 (três) ATESTADOS de CAPACIDADE TÉCNICA focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde foram prestados os serviços: Firewall/VPN, IPS, Filtro Web, conferido por empresas públicas ou privadas e que possuam, pelo menos, 300 (trezentos) hosts gerenciados, devidamente emitidos por entidades públicas e/ou privadas.

DESPACHO SOBRE A ANÁLIDE DOS ATESTADOS DE CAPACIDADE TÉCNICA APRESENTADOS

A empresa Licitante apresentou 5 (cinco) atestados de capacidade técnica dentre eles, 2 (dois) não estariam de acordo com o item do edital, são eles:

- **PMSA_CT_212.2011-PJ_UTM_08.12.2011:** Após análise e para o nosso entendimento, o referido documento trata-se conceitualmente de um Atestado para Serviço Gerenciado de Segurança, porém, para uma solução de software e não em appliance. Sendo outro objeto em relação a este certame, não está de acordo com o solicitado no Item do Edital;
- **SUSEP_CT_35.2012_UTM_19.12.2012_18.12.2015:** Após análise e para o nosso entendimento, o referido documento também se trata da Gestão de Solução de Segurança da informação, porém, de uma solução para gerenciamento unificado de ameaças do tipo appliance e não está especificando a devida compatibilidade com o objeto solicitado no Edital. Portanto, não está de acordo com o solicitado no Item do Edital;

ANÁLISE DO RECURSO APRESENTADO

Conforme errata que corrigiu o referido item deste edital conforme print retirado do portal de transparência da PRODAM abaixo:

AMAZONAS
GOVERNO DO ESTADO

Nível de Classificação	Grupo de acesso
Público	**GERAL**

1

PREGÃO ELETRÔNICO Nº 09/2022

ERRATA 1

1. **No item 17 do Termo de Referência:**

Onde se lê:

12.1 "A LICITANTE deve apresentar no mínimo 03 (três) ATESTADOS de CAPACIDADE TÉCNICA focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde foram prestados os serviços: Firewall/VPN, IPS, Filtro Web, conferido por empresas públicas ou privadas e que possuam, pelo menos, 300 (trezentos) hosts gerenciados, devidamente emitidos por entidades públicas e/ou privadas"

.

Leia-se:

12.1 "A LICITANTE deve apresentar 01 (um) ou mais ATESTADOS de CAPACIDADE TÉCNICA focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde foram prestados os serviços: Firewall/VPN, IPS, Filtro Web, conferido por empresas públicas ou privadas e que possuam, pelo menos, 300 (trezentos) hosts gerenciados, devidamente emitidos por entidades públicas e/ou privadas."

Manaus, 01 de novembro de 2022

GILSON DE SENA DA SILVA
Assinado de forma digital por GILSON DE SENA DA SILVA
Dados: 2022.11.01 10:20:07 -04'00'

Gilson de Sena da Silva
Pregoeiro

Link da Errata 1: https://www.prodam.am.gov.br/wp-content/uploads/2015/08/19-Errata.pdf

Logo para o nosso entendimento e de acordo com as comprovações apresentadas, a empresa LICITANTE estaria de acordo com este Item do Edital.

ITEM 4 do ANEXO 1-B do Edital	Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;

DESPACHO SOBRE A ANÁLIDE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na **Aba "Solução"** da planilha enviada informando todas as comprovações apresenta uma relação de part-numbers e nela, denota o posicionamento de 4 itens **FAZ-VM-GB25**. No nosso entendimento, o referido Item do Edital deixa muito claro que a solução deve ser ofertada com a maior capacidade suportada ou limitada e por isso, dando continuidade na análise das documentações foi visto no datasheet do FortiAnalyzer (https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf) que, para se respeitar o item deveria ter sido posicionado o part-number **FAZ-VM-**

GB2000 que é o de maior capacidade suportada. Portanto, não está de acordo com o solicitado no Item do Edital.

ANÁLISE DO RECURSO APRESENTADO

Conforme justificado pelo fornecedor no recurso: "Aqui, a explicação da razão pela qual a desclassificação não se sustenta é o fato de que para os APPLIANCES VIRTUAIS da Fortinet, não existe licença referente a armazenamento para gerenciamento e relatórios, motivo pelo qual o item não se aplica e o conjunto de licenças ofertadas atendem plenamente ao apresentado. "

Em nenhum momento citamos a questão do não atendimento deste item ter relação com o armazenamento para relatórios e gerenciamento para os APPLIANCES VIRTUAIS. O questionamento foi a não comprovação de que o produto ofertado não seria entregue na sua maior capacidade suportada ou ilimitada. Tendo em vista a inclusão de 4 itens FAZ-VM-GB25 e, para o nosso entendimento, como não foi ofertado na sua maior capacidade, como pede o item do Termo de Referência, seria necessária a aquisição de novos itens para a ampliação deste recurso gerando assim, custos adicionais.

Encontramos na página 8 da documentação enviada, que consta o item de licenciamento do produto ofertado na proposta F1001F com 32T de storage e com a possibilidade máxima de **200GB/Dia** de log, enquanto o ofertado foi de até **25GB/Dia**. No nosso entendimento, não foi apresentado a proposta com a capacidade máxima ofertada.
Desta forma, a segunda documentação enviada também **não evidência (11)** o atendimento a este item.

ITEM 2.18 do ANEXO 1-A do Edital	Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

DESPACHO SOBRE A ANÁLIDE DA COMPROVAÇÃO APRESENTADA

A comprovação indicada na **Aba "Solução"** da planilha enviada informando todas as comprovações apresenta uma relação de part-numbers e nela, não foi possível validar se realmente todos os transceivers serão devidamente entregues. No nosso entendimento, todos os part-numbers referente a todos os transceivers de todas as portas ofertadas pelo equipamento devem ser devidamente informadas na documentação. Portanto, há um descumprimento do referido Item do Edital.

ANÁLISE DO RECURSO APRESENTADO

Explicação da LICITANTE apresentada na segunda documentação referente ao despacho deste Item do Edital: *Comecemos pelos itens do Anexo 1-A: 2.18. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização; A desclassificação amparada neste item não se sustenta em absoluto. A*

uma, a proposta comercial da NCT continha o seguinte texto: "Serão Fornecidos os transceivers necessários para atendimento aos itens do Edital e seus Anexos".
Lembrando que o edital trata de prestação de serviços, e que a NCT indicou plena concordância com os seus termos (que apontavam a obrigação do futuro contratado de apresentar todas as interfaces com os transceivers/transceptores necessários), como se pode indicar descumprimento?
Obviamente, ao indicar que os forneceria e que estava de acordo com as condições do edital, a NCT atendeu ao que se exigia, o que requer a revisão da desclassificação.

--> Após análise da segunda documentação enviada, mesmo se tratando de prestação de serviços, a PRODAM exigiu que todas as portas que acompanharam o equipamento entregue pela LICITANTE estejam licenciadas e com seus respectivos transceivers para plena utilização. O serviço gerenciado foi especificado como serviço de "APOIO" para a equipe técnica da PRODAM, e não como serviço principal. A administração do equipamento firewall de borda será de responsabilidade da equipe técnica da PRODAM e o acionamento do serviço gerenciado será apenas eventual, em caso de necessidade. Desta forma, esta equipe não quer ter a surpresa de no momento que for utilizar as portas do equipamento, tenha que solicitar ativação ou tenha que se deparar com custos extras para sua ativação ou aquisição de transceivers. Além disto, devido a Guerra entre Ucrânia e Russia, os fabricantes estão com prazos logos para entrega de equipamentos devido à falta de insumos. Portanto a equipe técnica reforça a necessidade de que o equipamento ofertado seja entregue com todas as portas e transceivers para sua plena utilização.
Por estes motivos, apesar da LICITANTE informar que "Serão Fornecidos os transceivers necessários para atendimento aos itens do Edital e seus Anexos" entendemos que os respectivos part-numbers dos transceivers devem estar informados na proposta comercial enviada pela LICITANTE, conforme solicitado no Edital.
No nosso entendimento, a LICITANTE deverá acrescentar em sua proposta comercial os part-numbers dos tranceivers de todas as portas que não sejam metálicas da solução ofertada, garantindo sua plena utilização a qualquer tempo.

ANÁLISE DO RECURSO APRESENTADO PELA LICITANTE NCT SOBRE A PROPOSTA DA LICITANTE NTSEC

A LICITANTE NCT apresentou em seu recurso (*27 - Recurso NCT INFORMÁTICA LTDA.pdf*) alguns questionamentos sobre a análise realizada em cima da proposta enviada pela empresa NTSEC. Resolvemos responde-los pontualmente conforme segue abaixo:

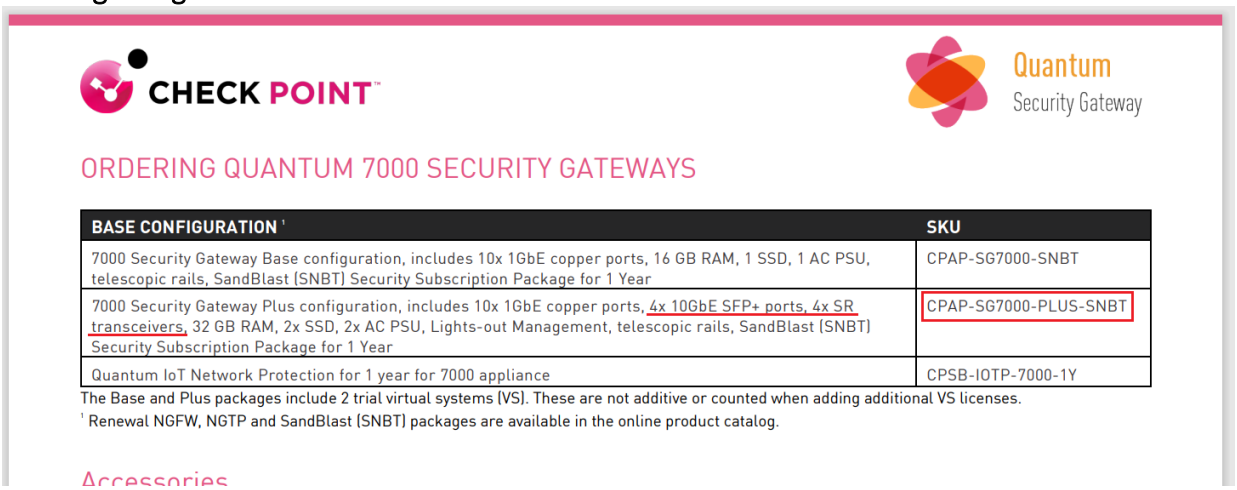
Proposta da NTSEC
Além da análise indevida da proposta da recorrente, há, também, clara aceitação de oferta que, esta sim, não cumpre o edital, que é o equipamento proposto pela NTSEC.

- Sempre presamos pela lisura do processo e analisamos criteriosamente cada PROPOSTA apresentada e suas respectivas documentações de comprovações e, com base nelas, emitimos seu Parecer Técnico.

Inicialmente, a oferta da NTSEC não informou os partnumbers das Gibcs, conforme seria exigido para demonstrar cumprimento ao item 2.18 do Anexo 1-A.

A oferta realizada foi dos partnumbers CPAC-4-10F-C - 4 Port 10GBase-F SFP+ interface card. Compulsando a lista de produtos da Checkpoint, contudo, vê-se que deveriam ter sido ofertados os seguintes partnumbers: CPAC-TR10SR-C - SFP+ transceiver module for 10G fiber ports - short rang (10GBase-SR).

- Entendemos que o Produto ofertado, cujo Part-Number é CPAP-SG7000-PLUS-SNBT, conforme o próprio datasheet informa, já contempla os Módulos tranceivers. Para lisura do processo, segue abaixo o print retirado da Página 4 do referido datasheet, cuja comprovação já havia sido apresentada na planilha *((PRODAM) P2P_PE92022)* enviada, originalmente, pela NTSEC. Os itens seguem grifados:



CHECK POINT

Quantum
Security Gateway

ORDERING QUANTUM 7000 SECURITY GATEWAYS

BASE CONFIGURATION [1]	SKU
7000 Security Gateway Base configuration, includes 10x 1GbE copper ports, 16 GB RAM, 1 SSD, 1 AC PSU, telescopic rails, SandBlast (SNBT) Security Subscription Package for 1 Year	CPAP-SG7000-SNBT
7000 Security Gateway Plus configuration, includes 10x 1GbE copper ports, 4x 10GbE SFP+ ports, 4x SR transceivers, 32 GB RAM, 2x SSD, 2x AC PSU, Lights-out Management, telescopic rails, SandBlast (SNBT) Security Subscription Package for 1 Year	CPAP-SG7000-PLUS-SNBT
Quantum IoT Network Protection for 1 year for 7000 appliance	CPSB-IOTP-7000-1Y

The Base and Plus packages include 2 trial virtual systems (VS). These are not additive or counted when adding additional VS licenses.
[1] Renewal NGFW, NGTP and SandBlast (SNBT) packages are available in the online product catalog.

Accessories

- Dando continuidade na análise deste item e conforme descrição detalhada para o part number CPAC-4-10F-C-INSTALL, onde diz "*Requires an additional 10GBase SFP+ Transceiver per interface port*", entendemos que é uma exigência, para o pleno funcionamento do módulo, ser fornecido com seus respectivos transceivers, o que é confirmado pelo "*de acordo*" da planilha *((PRODAM) P2P_PE92022) ponto a ponto* enviada, originalmente, pela NTSEC.

Seguindo, foi descumprido claramente o item 52 do edital, que trata do seguinte: "52. Deve suportar configuração em alta disponibilidade para fins de redundância". Isso porque a oferta contém apenas um item, como detalhamento da proposta, 1.2.1 TABELA DE MARCA/ MODELO, CPSM-NGSM25, Next Generation Security Management Software for 25 gateways (SmartEvent & Compliance 1 year), 1 e CPSB-EVS-25-2Y, SmartEvent and SmartReporter blade for 25 gateways (Smart-1 & open server) 2 year subscription, 1.

- No nosso entendimento, a referida alegação apresentada pela empresa LICITANTE NCT não tem relação com o Item 52 do Edital. Está muito claro na documentação apresentada originalmente pela empresa LICITANTE NTSEC, *especificamente na comprovação informada em sua planilha*

ponto a ponto ((PRODAM) P2P_PE92022), que o produto ofertado suporta configuração em alta disponibilidade para fins de redundância.

Seguem descumprimentos. A solução ofertada pela NTSEC é formada pela integração do firewall da Checkpoint com a solução "PRTG Network Monitor", algo que se extrai da sua planilha ponto a ponto em relação aos requisitos do Anexo 1-C do edital, 1.1 (PRODAM) P2P_PE92022, ANEXO 1-C - CARACTERÍSITCAS DA SOLUÇÃO DE MONITORAMENTO, PRTG User Manual.pdf.

- O Edital é bem claro no item 8.3 da Clausula Oitava (Da Garantia dos Serviços) do Anexo 5 (Minuta do Contrato) e para o nosso entendimento, a comprovação apresentada pela LICITANTE NTSEC em sua planilha ponto a ponto (*(PRODAM) P2P_PE92022*) como solução de monitoramento, atende a todos os itens exigidos no ANEXO 1-C *(CARACTERÍSITCAS DA SOLUÇÃO DE MONITORAMENTO)* deste Edital.

Contudo, a NTSEC não apresentou as licenças de monitoramento na proposta e nem a carta do fabricante da licença de monitoramento, violando o previsto no subitem 7.1 do Anexo 1-A do edital, conforme segue:

7.1. A LICITANTE deve ser revenda autorizada e/ou canal integrador qualificado pelos fabricantes das soluções por ela ofertadas. Sua comprovação será realizada através de declaração do fabricante dirigido especificamente à CONTRATANTE e a este processo licitatório;

- Para o nosso entendimento, a declaração (*Carta_PRODAM_NTSec_November22.pdf*) apresentada pela LICITANTE NTSEC está de acordo com o solicitado no respectivo item (*7.1 do Anexo 1-A do edital)* questionado pela LICITANTE NCT.

Além disso, a recorrida também deixou de cumprir a exigência do item 6.7.2 do mesmo Anexo 1-A, verbis: 6.7.2. A Licitante Vencedora deverá apresentar juntamente a sua Proposta uma Carta de cada Fabricante do item proposto declarando que seja Revenda Autorizada/Parceiro e uma empresa capacitada como Prestador de Serviços do Fabricante;

- Para o nosso entendimento, os atestados de capacidade técnicas apresentados e consolidados no documento (*Atestados_Capacidade_Tecnica.pdf*) de comprovação apresentado pela LICITANTE NTSEC estão de acordo com o solicitado no respectivo item (*6.7.2. do Anexo 1-A do edital)* questionado pela LICITANTE NCT.

CONCLUSÃO

Os documentos enviados adicionalmente pelo fornecedor foram analisados minuciosamente pela equipe técnica. Há de se registrar ainda que, várias das novas evidências enviadas na tentativa de comprovar o atendimento a requisitos técnicos, foram de versões de documentos defasados, cujo IOS era anterior ao produto ofertado originalmente na proposta. O Edital deixa muito claro que não aceitará produtos e softwares nas versões que não sejam as mais recentes disponíveis no mercado. Desta forma, continuamos SEM evidências documentais suficientes para comprovar que a solução ofertada pela empresa LICITANTE atende, pelo menos, **11 (onze) itens** do Edital.

Assim sendo, no nosso entendimento, mesmo oportunizando a comprovação dos argumentos de atendimento a todos os requisitos técnicos deste edital (conforme anteriormente afirmado pela a empresa LICITANTE (NCT INFORMÁTICA LTDA)) a empresa foi incapaz de evidenciar o atendimento a todos os itens reclamados e, portanto, conclui-se que ela não estaria apta a atender totalmente o objeto solicitado no certame.