AO(À) SENHOR(A) PREGOEIRO(A) DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ – TJCE

Pregão Eletrônico nº 032/2026
Processo Administrativo nº 8515550-95.2025.8.06.0000
Lote 1 – Controlador de Entrega de Aplicações (ADC)

ASSUNTO: APRESENTAÇÃO DE CONTRARRAZÕES AO RECURSO ADMINISTRATIVO

Objeto: Contratação de solução de balanceamento de carga e proteção de aplicações web, compreendendo o fornecimento de Controlador de Entrega de Aplicações (*Application Delivery Controller – ADC*), em appliance físico, incluindo hardware, software, licenciamento perpétuo, garantia, instalação/configuração, suporte técnico especializado e treinamento, conforme especificações do Edital e de seus anexos.

CONTRARRAZÕES AO RECURSO ADMINISTRATIVO - L8 GROUP S.A.

A **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, já qualificada no processo em referência, apresenta suas CONTRARRAZÕES ao recurso administrativo interposto por **L8 GROUP S.A**. contra o aceite de sua proposta e sua habilitação no Lote 1 do Pregão Eletrônico nº 032/2026, relativo ao fornecimento de Controlador de Entrega de Aplicações (ADC), com instalação, configuração, suporte e treinamento.

A presente manifestação retoma os esclarecimentos prestados nos Ofícios nº 191/2026 e nº 207/2026, complementando-os na medida necessária para examinar as alegações recursais. A Recorrente reúne exigências autônomas em oito blocos e extrai conclusões globais de limitações circunscritas a determinados mecanismos. Para preservar a objetividade do julgamento, os requisitos são examinados individualmente, confrontando-se a redação de cada item, a função técnica por ele exigida e a documentação já apresentada pela Recorrida.

Cabe distinguir três situações: (i) recursos nativos objetivamente documentados; (ii) formas de atendimento funcional que dependem do contexto de implementação e da redação do requisito; e (iii) pontos que demandam confirmação técnica específica, sem substituir tal confirmação por mera inferência. Essa distinção permite à Administração valorar as provas existentes e, se entender necessário, solicitar demonstração ou manifestação do fabricante para eliminar dúvida delimitada.

I. DA TEMPESTIVIDADE E DO CABIMENTO

As presentes contrarrazões são apresentadas em face do recurso administrativo interposto contra o aceite da proposta e a habilitação da Recorrida no Lote 1 do Pregão Eletrônico nº 032/2026, em observância ao contraditório, à ampla defesa e ao regular processamento dos recursos administrativos no âmbito das contratações públicas.

Nos termos do art. 165, inciso I, alínea “c”, e § 4º, da Lei nº 14.133/2021, cabe a apresentação de contrarrazões ao recurso administrativo no prazo de 3 (três) dias úteis, contado da intimação pessoal ou da divulgação da interposição do recurso, conforme o caso.

Considerando que o prazo estabelecido pela Administração para apresentação das contrarrazões se encerra em **20 de outubro de 2026**, a presente manifestação, protocolada até a data-limite indicada, deverá ser recebida como tempestiva, observadas as condições de apresentação previstas no instrumento convocatório e nas comunicações oficiais do certame.

Diante disso, requer-se o conhecimento das presentes contrarrazões e o exame dos fundamentos apresentados, à luz das disposições do edital, das especificações técnicas do objeto e dos documentos constantes dos autos.

Ao final, requer-se o não provimento do recurso administrativo, caso constatada a improcedência de suas alegações, com a manutenção do aceite da proposta e da habilitação da Recorrida no Lote 1, desde que reconhecida a conformidade da solução ofertada e da documentação apresentada com as exigências estabelecidas no instrumento convocatório.

II. DA SÍNTESE DO RECURSO ADMINISTRATIVO

A Recorrente insurge-se contra o aceite da proposta e a habilitação de nossa empresa no Lote 1 do Pregão Eletrônico nº 032/2026, promovido pelo Tribunal de Justiça do Estado do Ceará – TJCE, cujo objeto compreende o fornecimento de Controladores de Entrega de Aplicações (*Application Delivery Controller – ADC*), em *appliance* físico, além dos serviços e demais componentes previstos no instrumento convocatório.

Em suas razões recursais, a Recorrente apresenta dois fundamentos principais para pleitear a reforma da decisão administrativa, sustentando, de um lado, o suposto descumprimento de requisitos técnicos obrigatórios da solução ofertada e, de outro, a alegada insuficiência da comprovação de nossa qualificação técnico-operacional.

Quanto ao primeiro fundamento, a Recorrente afirma que a solução ofertada, baseada no equipamento FortiADC FAD-2000G, não atenderia a oito grupos de requisitos técnicos previstos no Anexo I do Termo de Referência. Para sustentar sua argumentação, invoca documentação pública da fabricante Fortinet e apresenta interpretações acerca das funcionalidades e limitações que atribui ao equipamento.

No tocante à qualificação técnico-operacional, a Recorrente questiona a suficiência dos cinco atestados de capacidade técnica apresentados por nossa empresa, alegando que nenhum deles comprovaria a implementação de solução ADC com capacidade mínima de 20 Gbps de *throughput*, conforme exigido pelo item 15.3.3.2.6.1 do Termo de Referência. Questiona, ainda, o alcance do Certificado de Parceria emitido pela Fortinet, sob o argumento de que o documento indicaria especialização em SD-WAN, o que, em seu entendimento, não seria suficiente para comprovar nossa qualificação para o objeto licitado.

Diante dessas alegações, **buscamos demonstrar, ao longo destas contrarrazões, que os questionamentos apresentados pela Recorrente devem ser examinados à luz das exigências efetivamente estabelecidas no edital, das características técnicas da solução ofertada e do conjunto documental apresentado no procedimento licitatório**. Para tanto, enfrentaremos individualmente os pontos levantados, confrontando as interpretações apresentadas no recurso com os requisitos correspondentes e com as evidências técnicas e documentais pertinentes.

No que se refere à qualificação técnico-operacional, demonstraremos, a partir da análise dos atestados e dos demais documentos apresentados, o atendimento às exigências editalícias aplicáveis, observados os critérios de capacidade, porte, complexidade e equivalência tecnológica previstos no instrumento convocatório.

Assim, **pretendemos evidenciar a ausência de fundamento suficiente para a reforma das decisões de aceite da proposta e de habilitação de nossa empresa**, requerendo o não provimento do recurso administrativo e a consequente manutenção dos atos praticados pela Administração, desde que confirmada, no exame individualizado dos pontos controvertidos, a conformidade da solução ofertada e da documentação apresentada com as exigências do edital.

III. NOTA PRELIMINAR - PERTINÊNCIA TEMPORAL DAS FONTES TÉCNICAS

Em sua fundamentação, a L8 Group invoca manuais do FortiADC 7.2.6 (VDOM), 7.4.3 (modo transparente), 7.4.9 (métodos de balanceamento), 7.4.11 (HTTP/3), 7.6.0 (peso nos pools) e 7.6.6 (HTTP/3), embora a documentação apresentada pela Network Secure nas diligências tenha adotado a versão FortiADC 8.0.3. O recurso também cita documentos 8.0.3 e 8.0.4, sobretudo para HA e políticas L7. Por conseguinte, não se trata de recurso integralmente apoiado em versões antigas, e cada referência deve ser avaliada em seu próprio contexto.

A existência de documentação anterior não a torna automaticamente inválida, mas impede que a ausência de determinada funcionalidade na versão antiga seja tomada, isoladamente, como prova de sua ausência no sistema disponibilizado pela solução ofertada. Para fins de julgamento, é indispensável confrontar cada alegação com o Administration Guide, CLI Reference, New Features e Release Notes da versão pertinente, distinguindo recursos introduzidos ou ampliados de limitações que permaneceram vigentes.

Há evolução documentada: a linha 7.6.1 passou a registrar conexões HTTP/2 com o backend, inclusive a possibilidade arquitetural de HTTP/3 no frontend com HTTP/2 no backend, e o guia FortiADC 8.0.3 descreve a opção Backend HTTP2. O FortiADC 8.0.3 também passou a documentar inspeção WAF por assinaturas em Virtual Servers HTTP/2 e HTTP/3. Esses recursos precisam ser considerados ao analisar a afirmação

genérica de inexistência de comunicação HTTP/2 no backend e o escopo de proteção do tráfego HTTP/3.

IV. DA SELETIVIDADE DOCUMENTAL E DAS INCONSISTÊNCIAS NA ARGUMENTAÇÃO RECURSAL

No item III.7 de seu recurso, a L8 Group ampara parte da alegação de inexistência de comunicação HTTP/2 com os servidores de backend em documentos de versões anteriores, especialmente o Handbook FortiADC 7.4.11 e a CLI Reference 7.6.6. Ocorre que o fabricante já havia anunciado, nas novidades da versão 7.6.1, o suporte a conexões HTTP/2 no backend, incluindo configuração de perfis com frontend HTTP/3 e backend HTTP/2. A versão 8.0.3, utilizada nas diligências, igualmente documenta o parâmetro Backend HTTP2 e perfis predefinidos correspondentes. Trata-se de evolução oficial disponível antes da apresentação da proposta, de modo que a afirmação genérica de inexistência dessa capacidade, sem confronto com as fontes supervenientes, oferece quadro técnico incompleto à Administração.

A seleção de referências antigas não é irregular por si só. Todavia, quando uma limitação apontada como absoluta foi superada ou passou a ter tratamento funcional diverso em documentação posterior do próprio fabricante, a omissão dessa evolução pode comprometer a boa-fé objetiva, a lealdade procedimental e o julgamento técnico do certame. Na avaliação da Network Secure, a apresentação de conclusão categórica fundada em recorte documental superado, sem explicitar avanços já publicados, constitui indício relevante de atuação recursal temerária e de possível má-fé, especialmente em manifestação apresentada por empresa que se propõe a discutir tecnicamente a solução. Requer-se que o TJCE considere essa circunstância ao valorar a credibilidade das alegações, sem pressupor, de forma automática, a existência de intenção deliberada de induzir o órgão a erro, cuja constatação exige elementos adicionais. Essa objeção é restrita às afirmações efetivamente desatualizadas ou incompletas.

a) Da operação em cluster e dos cenários IPv4/IPv6 — recurso, item III.2 Item 1.1.4 — Da vedação à entrega da solução em modo *standalone*

> “1.1.4. Não será aceita a entrega de equipamentos para operação isolada (standalone), ainda que atendam individualmente às especificações técnicas.”
>
> “1.3.2.7. Suporte a alta disponibilidade em modo ativo-ativo e failover automático.”

A alegação apresentada pela Recorrente quanto ao suposto não atendimento do item 1.1.4 desconsidera a composição da solução ofertada pela Network Secure e os mecanismos nativos de alta disponibilidade disponibilizados pelo FortiADC, conforme documentação oficial do fabricante.

Inicialmente, cumpre esclarecer que a proposta comercial apresentada pela Network Secure contempla o fornecimento de 02 (duas) unidades FortiADC FAD-2000G, equipamentos idênticos, do mesmo fabricante e modelo, acompanhados dos respectivos serviços de suporte e implantação, destinados à operação conjunta em arquitetura de alta disponibilidade.

Dessa forma, a solução ofertada não se caracteriza pelo fornecimento de dois equipamentos independentes para operação isolada, mas pela implementação de uma arquitetura integrada de balanceamento de aplicações, composta por dois appliances físicos.

A documentação oficial do fabricante, no FortiADC 8.0.3 Administration Guide, seção *Configuring HA Settings*, estabelece expressamente a disponibilidade dos seguintes modos operacionais:

- Standalone;
- Active-Passive;
- Active-Active;
- Active-Active-VRRP.

A existência dessas diferentes modalidades demonstra a flexibilidade de implementação disponibilizada pelo fabricante, permitindo selecionar a arquitetura de alta disponibilidade conforme os requisitos do ambiente.

Para a presente contratação, a arquitetura prevista pela Network Secure contempla a operação dos equipamentos em cluster ativo-ativo, conforme estabelecido no item 1.1.5 do Termo de Referência.

Portanto, a disponibilidade do modo Standalone como alternativa de configuração não representa limitação técnica para a implementação do modo de operação exigido, tampouco caracteriza que os equipamentos serão fornecidos para funcionamento isolado.

Conforme documentação oficial do FortiADC 8.0.3, a implementação do cluster Active-Active contempla mecanismos específicos para integração e operação conjunta dos equipamentos, incluindo:

- Identificação dos membros pertencentes ao mesmo cluster por meio de Group ID;
- Identificação individual dos nós por meio de Local Node ID;
- Interfaces dedicadas à comunicação de heartbeat;
- Interfaces utilizadas para sincronização de dados entre os membros;
- Sincronização de configurações entre os equipamentos;
- Mecanismos de sincronização de estados de conexão e persistência, observadas as funcionalidades suportadas pelo fabricante.

Essas características demonstram que o FortiADC dispõe de arquitetura nativa de alta disponibilidade, na qual os equipamentos operam como membros de um mesmo agrupamento lógico, compartilhando informações necessárias ao gerenciamento e à continuidade operacional dos serviços.

Dessa forma, não se trata de dois appliances configurados independentemente, mas de uma solução com mecanismos próprios de integração, sincronização e operação conjunta.

Importante destacar que o item 1.1.4 estabelece uma condição relacionada à forma de fornecimento e implantação da solução, vedando expressamente a entrega dos equipamentos para funcionamento independente.

Nesse contexto, a Network Secure reafirma que a arquitetura ofertada contempla a implantação das duas unidades FortiADC FAD-2000G como integrantes de uma única solução lógica de balanceamento de aplicações, configurada para operação em cluster ativo-ativo.

O fornecimento dos equipamentos deverá, portanto, ser acompanhado da configuração dos respectivos mecanismos de alta disponibilidade, integração dos membros, sincronização e testes necessários à validação da operação conjunta.

Assim, a existência da modalidade Standalone no sistema operacional do fabricante não implica que os equipamentos serão entregues nessa condição, uma vez que a arquitetura prevista para atendimento ao objeto contratual é de operação integrada em cluster.

Diante dos esclarecimentos apresentados, não procede a afirmação de que a solução ofertada pela Network Secure se caracteriza pelo fornecimento de equipamentos destinados à operação isolada.

A proposta contempla duas unidades físicas FortiADC FAD-2000G, enquanto a documentação oficial comprova o suporte nativo à operação em cluster ativo-ativo, com mecanismos próprios de integração e sincronização entre os membros.

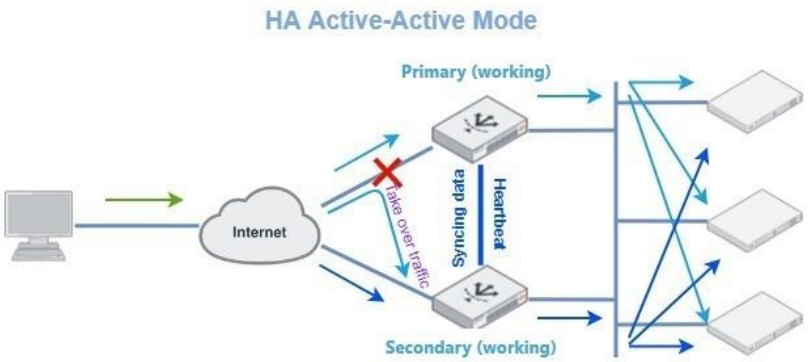
Ressalta-se que a configuração prevista para a implantação observa a exigência de operação conjunta estabelecida no instrumento convocatório, não estando prevista a entrega dos appliances como soluções independentes em modo Standalone.

Diante do exposto, requer-se que seja afastada a alegação de descumprimento do item 1.1.4, considerando-se a composição da proposta apresentada, a arquitetura de implantação prevista e a documentação oficial do fabricante que demonstra o suporte à operação em cluster ativo-ativo.

O FortiADC 2000G atende ao requisito, conforme demonstrado na documentação oficial da Fortinet referente à alta disponibilidade (High Availability) e à implantação de clusters em modo ativo-ativo (*Active-Active Cluster*).

No modo Active-Active, os equipamentos são configurados para operar conjuntamente, permitindo a distribuição do processamento das requisições entre os membros do cluster, conforme a arquitetura e as configurações estabelecidas.

A documentação também descreve os mecanismos de alta disponibilidade e sincronização de informações entre os equipamentos, incluindo estados de conexões e tabelas de persistência das camadas 4 e 7, conforme os recursos suportados.



Em caso de falha de um dos membros, o mecanismo de failover permite que o equipamento remanescente assuma o processamento das funções e do tráfego aplicáveis, favorecendo a continuidade dos serviços publicados e reduzindo a indisponibilidade.

Ressalta-se que o suporte às funcionalidades IPv6 nas interfaces de comunicação e gerenciamento do FortiADC é independente do tipo de endereçamento IP utilizado para a comunicação de alta disponibilidade (HA) entre os equipamentos do cluster. Portanto, a utilização de IPv4 ou IPv6 no estabelecimento da comunicação entre os membros do cluster não determina nem restringe, por si só, a capacidade da solução de operar com funcionalidades IPv6 nas interfaces e nos serviços correspondentes, respeitadas as especificações e condições de configuração documentadas pelo fabricante.

Dessa forma, a documentação oficial comprova a existência dos recursos de alta disponibilidade em modo ativo-ativo e dos mecanismos de failover, atendendo ao requisito técnico apresentado.

i. Item 1.1.5 - cluster ativo-ativo e continuidade operacional

A Recorrente inclui o item 1.1.5 entre os requisitos supostamente não atendidos, entretanto, não apresenta, neste ponto do recurso, fundamentação técnica específica que demonstre a impossibilidade de operação do FortiADC 2000G em cluster ativo-ativo.

Sua argumentação concentra-se na restrição documental referente ao endereçamento utilizado na configuração de alta disponibilidade, associando-a

indevidamente à inexistência de suporte ao processamento de tráfego IPv6 pela solução.

Cumpre destacar que o atendimento ao referido requisito já foi objeto de esclarecimento técnico apresentado pela Network Secure na primeira diligência realizada pelo TJCE, oportunidade em que foram demonstrados os mecanismos de operação ativo-ativo, sincronização de estados de conexão e persistência disponibilizados pelo FortiADC, com fundamento na documentação oficial da versão 8.0.3.

Adicionalmente, a documentação oficial do fabricante, na seção *Advanced Mode: Configuring a Layer 4 Virtual Server*, estabelece expressamente a possibilidade de configuração de Virtual Servers com endereçamento IPv4 ou IPv6, contemplando também o parâmetro Traffic Group, destinado à associação dos servidores virtuais aos grupos de tráfego utilizados em ambientes de alta disponibilidade.

Dessa forma, é necessário distinguir o endereçamento empregado na configuração e na comunicação entre os membros do cluster daquele utilizado pelos Virtual Servers para o processamento das aplicações. A restrição documental apresentada pela Recorrente, isoladamente, não demonstra que a configuração do mecanismo HA com endereçamento IPv4 impossibilite o processamento de tráfego IPv6 pelos equipamentos integrantes da solução.

Portanto, a inclusão do item 1.1.5 entre os requisitos supostamente descumpridos, com fundamento exclusivo nessa restrição, não constitui demonstração técnica suficiente da inexistência da funcionalidade de cluster ativo-ativo, cuja implementação e mecanismos de sincronização já foram apresentados pela Network Secure durante a fase de diligência.

Diante do exposto, requer-se que seja afastada a alegação de descumprimento do item 1.1.5 nos termos apresentados neste tópico do recurso, considerando a documentação oficial do FortiADC 8.0.3 e os esclarecimentos técnicos anteriormente prestados à Administração.

ii. Item 1.1.6 - demais requisitos de alta disponibilidade

O item 1.1.6 do Termo de Referência estabelece:

> “1.1.6. Os equipamentos devem ser projetados especificamente para aceleração e balanceamento de tráfego de aplicações, garantindo compatibilidade técnica para operação em alta disponibilidade (HA), com sincronização de estado e sessões, nos modos ativo-ativo e/ou ativo-passivo.”

A Recorrente sustenta que as limitações documentadas do FortiADC quanto à sincronização de determinadas sessões e ao suporte a HA em IPv6 comprometeriam a compatibilidade da solução com os requisitos de alta disponibilidade estabelecidos no Termo de Referência.

Entretanto, a documentação oficial do FortiADC 8.0.3 demonstra que a plataforma possui arquitetura nativa de alta disponibilidade, com mecanismos específicos de detecção de falhas, sincronização de configurações, estados de conexão e tabelas de persistência.

O FortiADC 2000G é um appliance desenvolvido especificamente para entrega, aceleração e balanceamento de aplicações, dispondo de recursos de hardware e software destinados ao processamento de tráfego L4/L7.

Adicionalmente, o equipamento possui interfaces físicas destinadas à comunicação entre os membros do cluster, permitindo configurar separadamente as interfaces de heartbeat e de sincronização de dados, conforme as orientações do fabricante.

A documentação oficial do FortiADC 8.0.3, na seção Configuring HA Settings, descreve os seguintes mecanismos nativos de alta disponibilidade:

a) Operação em cluster ativo-ativo e ativo-passivo: a solução disponibiliza nativamente os modos Active-Active, Active-Passive e Active-Active-VRRP, permitindo configurar a arquitetura de alta disponibilidade de acordo com as características do ambiente.

b) Detecção de falhas por heartbeat: o FortiADC permite configurar intervalos de comunicação e limiares de perda de heartbeat (Heartbeat Interval e Lost Heartbeat Threshold), utilizados na identificação de indisponibilidade dos membros do cluster.

c) Monitoramento de conectividade (Remote IP Monitor): a solução disponibiliza mecanismos de monitoramento de endereços IP remotos, permitindo detectar indisponibilidade de caminhos de rede e, nos modos compatíveis e mediante configuração, acionar procedimentos de failover.

d) Failover Hold Time: mecanismo destinado a estabelecer um período de retenção após determinadas operações de failover, reduzindo o risco de alternâncias sucessivas de papel entre os membros do cluster em cenários de instabilidade.

e) Sincronização de configurações: o FortiADC disponibiliza sincronização automática de configurações entre os membros do cluster, permitindo manter consistência dos parâmetros operacionais e administrativos da solução.

f) Sincronização de estados e persistência: a documentação oficial, na seção HA Synchronization, confirma a sincronização dos estados de conexões TCP em camada 4, das tabelas de persistência em camada 4 e das tabelas de persistência em camada 7 baseadas em endereço de origem (Source Address Persistence).

Dessa forma, é possível correlacionar objetivamente as exigências do item 1.1.6 às funcionalidades documentadas do fabricante: Equipamentos projetados para aceleração e balanceamento de aplicações: atendidos pela própria arquitetura e finalidade do FortiADC 2000G, equipamento dedicado à entrega e ao balanceamento de aplicações em camadas 4 e 7.

Compatibilidade com operação em alta disponibilidade: demonstrada pelos modos Active-Active, Active-Passive e Active-Active-VRRP, associados aos mecanismos de heartbeat, monitoramento de conectividade e failover.

Sincronização de estados e sessões: demonstrada pelos mecanismos de sincronização de estados TCP em L4, persistência L4 e persistência L7 baseada em endereço de origem.

Operação nos modos ativo-ativo e/ou ativo-passivo: comprovada pela documentação oficial do fabricante, que apresenta expressamente ambas as modalidades de operação.

Importante destacar que a limitação relacionada à sincronização da persistência por SSL Session ID não representa ausência generalizada de mecanismos de sincronização de estados e sessões na plataforma.

Conforme esclarecido durante as diligências anteriores, essa limitação está relacionada a um método específico de persistência e deve ser distinguida das funcionalidades nativas de sincronização disponibilizadas para os demais mecanismos suportados. Cabe observar, contudo, que a sincronização de estados TCP em L4 e das tabelas de persistência documentadas não equivale à preservação integral de todas as conexões de aplicação L7 ou SSL/TLS em qualquer cenário de falha. Quanto à restrição de HA em IPv6 apontada pela Recorrente, trata-se de aspecto específico de compatibilidade que deverá ser considerado na avaliação conjunta dos requisitos de IPv6 e alta disponibilidade, não afastando a existência dos mecanismos nativos de HA documentados para as modalidades suportadas.

Diante do exposto, verifica-se que o FortiADC 2000G dispõe de arquitetura específica para aceleração e balanceamento de aplicações, com suporte nativo aos modos de alta disponibilidade e mecanismos de sincronização de estados e persistência, conforme descrito na documentação oficial do fabricante.

Assim, requer-se o afastamento da alegação genérica de ausência de compatibilidade técnica com alta disponibilidade, considerando-se os mecanismos comprovados e os esclarecimentos anteriormente prestados pela Network Secure.
Requer-se, ainda, que eventuais limitações específicas sejam avaliadas individualmente, à luz dos requisitos correspondentes do Termo de Referência, observando-se os princípios da vinculação ao instrumento convocatório e do julgamento objetivo.

Links de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/886000/configuring-ha-settings
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/657374/ha-synchronization
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/984372/deploying-an-active-active-cluster

iii. Item 1.4.6 - suporte à pilha IPv6 e Item 1.4.18 - endereçamento das interfaces e instâncias

A alegação apresentada pela Recorrente quanto ao suposto não atendimento dos itens 1.4.6 e 1.4.18 do Termo de Referência desconsidera as funcionalidades de endereçamento IPv4 e IPv6 expressamente documentadas pelo fabricante, bem como as evidências técnicas anteriormente apresentadas pela Network Secure na planilha de referência cruzada encaminhada ao TJCE.Inicialmente, cumpre destacar que os requisitos estabelecem:

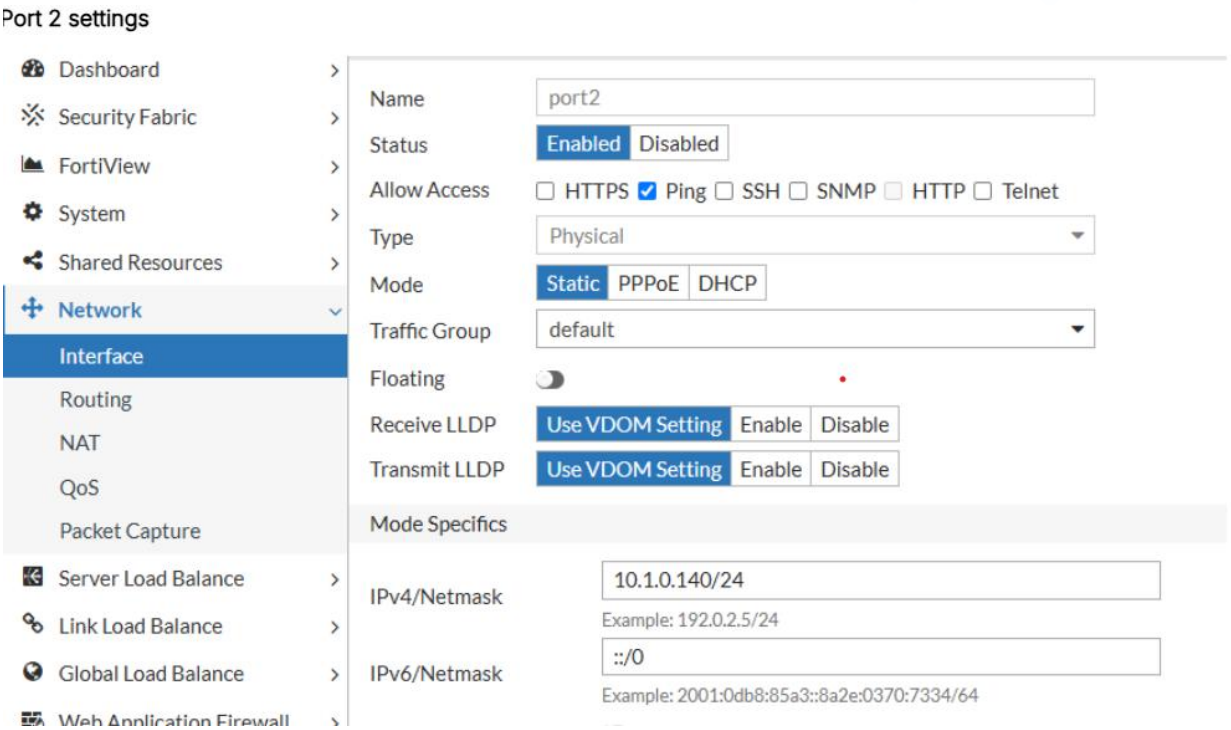
> “1.4.6. Suportar a definição de endereços IPv4 e IPv6 nas interfaces de comunicação.”
> “1.4.18. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs).”

Conforme se observa, ambos os dispositivos estabelecem requisitos objetivos de suporte ao endereçamento IPv4 e IPv6 nas interfaces de rede, sendo que o item 1.4.18 específica expressamente a necessidade de atendimento também nas interfaces lógicas do tipo VLAN.

A documentação oficial do FortiADC 8.0.3, na seção Configuring Network Interfaces, demonstra expressamente que a solução disponibiliza mecanismos nativos para configuração de endereços IPv4 e IPv6 em suas interfaces de comunicação.
Por meio da interface administrativa, no menu Network → Interface, o administrador pode configurar os parâmetros de endereçamento IP das interfaces físicas e lógicas disponíveis no equipamento.A documentação apresenta expressamente os campos:

- IPv4/Netmask: destinado à configuração do endereço IPv4 e da respectiva máscara de rede no formato CIDR.
- IPv6/Netmask: destinado à configuração do endereço IPv6 e do respectivo prefixo de rede no formato CIDR.

Esses parâmetros demonstram que a solução disponibiliza suporte nativo aos dois protocolos, permitindo a configuração dos respectivos endereços nas interfaces de comunicação do appliance.



Além das interfaces físicas, a documentação oficial estabelece que o FortiADC permite criar interfaces lógicas do tipo VLAN, compatíveis com o padrão IEEE 802.1Q. Conforme descrito na seção Configuring Network Interfaces, o administrador pode criar uma interface VLAN por meio da opção Create New, associando-a à interface física correspondente e definindo seu identificador VLAN ID. A estrutura de configuração contempla a definição de endereços IPv4 e IPv6 nas interfaces lógicas, utilizando os mesmos parâmetros de endereçamento disponíveis para as interfaces físicas.

Dessa forma, o suporte aos protocolos IPv4 e IPv6 não está restrito às portas físicas do equipamento, abrangendo também as interfaces virtuais utilizadas para segmentação lógica da infraestrutura de rede.

Complementarmente, o FortiADC 8.0.3 CLI Reference, na seção config system interface, apresenta os parâmetros utilizados para a configuração das interfaces físicas e virtuais.

Entre os comandos documentados encontram-se:

- set ip — configuração do endereço IPv4;
- set ip6 — configuração do endereço IPv6;
- set type vlan — definição de interface lógica do tipo VLAN;
- set vlanid — definição do identificador da VLAN;
- set interface — associação da VLAN à interface física;
- set vdom — associação da interface ao domínio virtual correspondente.

A existência desses parâmetros, expressamente documentados na versão 8.0.3, comprova que a plataforma disponibiliza mecanismos nativos e configuráveis para definição de endereços IPv4 e IPv6 em interfaces físicas e VLANs.
Portanto, as funcionalidades estabelecidas nos itens 1.4.6 e 1.4.18 encontram respaldo direto na documentação oficial do fabricante.

Links de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/943981/configuring-network-interfaces
https://docs.fortinet.com/document/fortiadc/8.0.3/cli-reference/202041/config-system-interface
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/708124/interface

iv. Item 1.6.18 - cenários de comunicação cliente/servidor IPv4 e IPv6

Em resposta ao recurso referente ao item 1.6.18 do edital, apresentamos como evidência a documentação oficial do fabricante Fortinet, FortiADC 8.0.3 Administration Guide, na seção Advanced Mode: Configuring a Layer 4 Virtual Server.

Link de Referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/85256/advanced-mode-configuring-a-layer-4-virtual-server

1. Comprovação técnica do fabricante

A documentação oficial descreve os mecanismos de encaminhamento e tradução de endereços disponíveis para servidores virtuais de Camada 4, incluindo:

Full NAT – Comunicação entre endereçamentos da mesma versão

"Full NAT — Replaces both the destination and source IP addresses. IPv4 to IPv4 or IPv6 to IPv6 translation."

Tradução: Substitui os endereços IP de origem e destino, permitindo a tradução IPv4–IPv4 ou IPv6–IPv6.

NAT46 – Comunicação IPv4 para IPv6

"*NAT46 — (If Address Tpye is IPv4) Replaces both the destination and source IP addresses, translating IPv4 addresses to IPv6 addresses*."

Tradução: Substitui os endereços IP de origem e destino, traduzindo endereços IPv4 para IPv6.

NAT64 – Comunicação IPv6 para IPv4

"*NAT64 — (If Address Type is IPv6) Replaces both the destination and source IP addresses, translating IPv6 addresses to IPv4 addresses*."

Tradução: Substitui os endereços IP de origem e destino, traduzindo endereços IPv6 para IPv4.

Item 1.6.18.1 – Cliente IPv4 e backend IPv4: ATENDE, por meio de encaminhamento compatível e Full NAT IPv4–IPv4.

Item 1.6.18.2 – Cliente IPv4 e backend IPv6: ATENDE, por meio do mecanismo NAT46.

Item 1.6.18.3 – Cliente IPv6 e backend IPv4: ATENDE, por meio do mecanismo NAT64.

Item 1.6.18.4 – Cliente IPv6 e backend IPv6: ATENDE, por meio de encaminhamento compatível e Full NAT IPv6–IPv6.

É importante destacar que o endereçamento empregado na configuração de Alta Disponibilidade (HA – High Availability) entre os equipamentos FortiADC constitui uma característica distinta do endereçamento utilizado nas interfaces virtuais de serviço e na comunicação com os servidores de backend. Dessa forma, o atendimento aos cenários previstos no item 1.6.18 não está condicionado à utilização exclusiva de IPv4

ou de IPv6 no endereçamento de HA. A capacidade de atender aos quatro cenários decorre dos recursos de encaminhamento e tradução de endereços disponibilizados pelo FortiADC, conforme demonstrado na documentação oficial.

Assim, desde que respeitadas as condições de configuração e compatibilidade previstas pelo fabricante, o equipamento poderá processar os cenários IPv4–IPv4, IPv4–IPv6, IPv6–IPv4 e IPv6–IPv6, independentemente da versão IP empregada no endereçamento de comunicação entre os membros do cluster HA.

Ressalta-se que essa independência se refere à capacidade funcional de encaminhamento e tradução IP, não dispensando os requisitos próprios de conectividade, sincronização e configuração do cluster de alta disponibilidade.

A documentação oficial comprova a disponibilidade dos mecanismos Full NAT, NAT46 e NAT64 no FortiADC, contemplando os quatro cenários de endereçamento previstos no edital.

Adicionalmente, o endereçamento utilizado na comunicação entre os equipamentos em HA não deve ser confundido com o endereçamento das conexões de serviço, uma vez que são aspectos distintos da arquitetura da solução.

Além dos recursos de encaminhamento e tradução de endereços já apresentados, a Fortinet **introduziu, a partir da versão FortiADC 7.6.3**, o suporte à **configuração de endereços IPv6 nas interfaces de gerenciamento de HA**, conforme documentado em:

Documentação oficial: IPv6 Support for HA Management Interface – FortiADC 7.6.3
https://docs.fortinet.com/document/fortiadc/7.6.0/new-features/278424/ipv6-support-for-ha-management-interface-7-6-3

A documentação apresenta o seguinte trecho original:

“FortiADC now supports configuration of an IPv6 address on the HA management interface, allowing administrators to access the system using either IPv4 or IPv6.”

Tradução: O FortiADC passou a permitir a configuração de um endereço IPv6 na interface de gerenciamento de HA, possibilitando que os administradores acessem o sistema utilizando IPv4 ou IPv6.

O fabricante esclarece ainda que essa funcionalidade foi introduzida na versão 7.6.3 por meio da nova opção Management IPv6, disponível na interface gráfica e na CLI, ampliando a flexibilidade de gerenciamento em ambientes IPv4, IPv6 e dual-stack. É fundamental destacar que o endereçamento das interfaces de gerenciamento não determina a versão IP utilizada pelas funcionalidades de balanceamento e encaminhamento dos serviços. São aspectos distintos da configuração do equipamento: o gerenciamento permite o acesso administrativo ao FortiADC, enquanto os servidores virtuais utilizam os mecanismos de encaminhamento e tradução IP apropriados para atender às conexões dos clientes e dos servidores de backend.

Dessa forma, os recursos de serviço documentados — Full NAT, NAT46 e NAT64 — permitem contemplar os quatro cenários exigidos no edital, independentemente de a interface de gerenciamento estar configurada com endereço IPv4 ou IPv6, desde que respeitadas as condições de configuração e compatibilidade previstas pelo fabricante. Diante do exposto, solicitamos que os subitens 1.6.18.1 a 1.6.18.4 sejam considerados ATENDIDOS, reconhecendo-se a conformidade técnica do FortiADC 2000G com o requisito estabelecido no edital.

b) Da sincronização de estado e da persistência de sessão — recurso, item III.3 Item 1.1.5 — Do alcance da sincronização de estado em alta disponibilidade (HA)

A alegação apresentada pela Recorrente quanto ao suposto não atendimento do requisito de alta disponibilidade e sincronização de estados entre os membros do cluster desconsidera os mecanismos nativos disponibilizados pelo FortiADC, bem como os esclarecimentos técnicos já apresentados pela Network Secure durante a segunda diligência, formalizada por meio do Ofício nº 207/2026.

Inicialmente, cumpre destacar que o item 1.1.5 do Termo de Referência estabelece:

> “A solução deverá operar em cluster ativo-ativo, assegurando alta disponibilidade, com sincronização de estado entre os nós, incluindo tabelas de sessão, persistência e conexões ativas, de modo a evitar interrupção de sessões em caso de falha.”

Conforme anteriormente esclarecido, a interpretação apresentada pela Recorrente associa requisitos distintos e atribui ao item 1.1.5 condições técnicas específicas que não estão expressamente individualizadas em sua redação.

O item 1.3.2.5, utilizado pela Recorrente para fundamentar parte de sua alegação, integra o requisito 1.3.2, referente ao Serviço de Balanceamento Global de Aplicações (GSLB), devendo ser interpretado no contexto funcional em que foi estabelecido.

Dessa forma, a previsão de mecanismos de persistência por cookie, endereço IP de origem e SSL Session ID no contexto de GSLB não implica, automaticamente, que o item 1.1.5 exija sincronização simultânea e integral de todos esses mecanismos entre os membros de um cluster ativo-ativo.

A documentação oficial do fabricante, no FortiADC 8.0.3 Administration Guide, seção *Configuring HA Settings*, estabelece expressamente a disponibilidade dos modos de operação Active-Passive, Active-Active e Active-Active-VRRP. No modo Active-Active, os membros do cluster podem processar tráfego simultaneamente, permitindo a distribuição das conexões entre os equipamentos e proporcionando redundância para os serviços de balanceamento de aplicações. A arquitetura contempla mecanismos de comunicação entre os membros, interfaces destinadas ao heartbeat e à sincronização de dados, bem como recursos específicos para transferência de estados de conexão e informações de persistência.

Portanto, a solução ofertada disponibiliza nativamente a arquitetura de cluster ativo-ativo exigida pelo instrumento convocatório. A documentação oficial do FortiADC 8.0.3 estabelece que os mecanismos de sincronização de alta disponibilidade contemplam os estados das conexões TCP em camada 4. Por meio da funcionalidade *Layer 4 Connection Synchronization*, o equipamento sincroniza as informações das conexões TCP entre os membros do cluster. Quando essa funcionalidade está habilitada, os estados das sessões TCP são compartilhados, permitindo que outro membro do cluster processe o tráfego pertencente a uma conexão anteriormente estabelecida, caso ocorra redistribuição do tráfego em razão de falha de um dos equipamentos. Conforme descrito na seção *Configuring HA Settings*, o fabricante estabelece que, quando a sincronização da tabela de sessões TCP está habilitada, as sessões podem ser

retomadas sem interrupção caso o tráfego subsequente seja encaminhado a outro membro do cluster em decorrência de failover.

Dessa forma, encontra-se documentalmente comprovada a existência de mecanismo nativo de sincronização de conexões ativas em camada 4, destinado à preservação da continuidade operacional dos serviços.

Além da sincronização dos estados de conexão TCP, o FortiADC disponibiliza mecanismos específicos de sincronização das tabelas de persistência.

A documentação oficial do fabricante, na seção *HA Synchronization*, apresenta expressamente os seguintes componentes:

- Layer-4 TCP connection states;
- Layer-4 persistence tables;
- Layer-7 persistence tables (Source Address Persistence only).

Essas funcionalidades demonstram que a sincronização de alta disponibilidade não se restringe exclusivamente à manutenção das configurações dos equipamentos, abrangendo também informações relacionadas ao estado das conexões e à persistência das sessões.

Em camada 4, o mecanismo permite sincronizar as tabelas de persistência baseadas no endereço IP de origem, preservando as informações utilizadas para associar os clientes aos respectivos servidores de backend. Em camada 7, o FortiADC também disponibiliza sincronização das tabelas de persistência baseadas em Source Address, conforme expressamente documentado pelo fabricante.

Portanto, não procede a interpretação de que a solução não possui mecanismos de sincronização de persistência em camada 7. Importante esclarecer que a sincronização de persistência L7 por endereço de origem não se confunde com a sincronização integral dos estados das conexões de aplicação em camada 7. Tratam-se de mecanismos distintos, com finalidades e abrangências específicas.

A Recorrente também utiliza a limitação relacionada à sincronização da persistência por SSL Session ID como fundamento para questionar o atendimento ao requisito de alta disponibilidade.

Entretanto, cabe distinguir a disponibilidade do mecanismo de persistência da capacidade de sincronização de sua tabela entre os membros do cluster.

O FortiADC disponibiliza nativamente persistência baseada em SSL Session ID, conforme estabelecido na documentação oficial do fabricante.

Por outro lado, a documentação esclarece que a tabela de persistência baseada nesse identificador não é sincronizada entre os membros do cluster, de modo que, em caso de encerramento da conexão no primeiro nó, poderá ser necessário estabelecer uma nova conexão SSL por meio do segundo equipamento.

Essa limitação específica não descaracteriza a existência dos demais mecanismos de sincronização disponibilizados pela solução, incluindo estados TCP em L4, tabelas de persistência L4 e persistência L7 baseada em endereço de origem.

Adicionalmente, os mecanismos de persistência baseados em cookies e algoritmos hash possuem características próprias de funcionamento, não exigindo necessariamente a sincronização de tabelas de persistência para que o direcionamento continue utilizando o mesmo servidor de backend, conforme esclarecido pelo fabricante. Assim, a limitação referente ao SSL Session ID deve ser examinada em seu contexto funcional específico, não sendo tecnicamente adequado generalizá-la como ausência de sincronização de estados ou de recursos de alta disponibilidade na plataforma.

Link de Referencia:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/657374/ha-synchronization
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/886000/configuring-ha-settings
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/984372/deploying-an-active-active-cluster
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/469954/layer-7-capabilities-for-http-https-traffic
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/932874/configuring-persistence-rules

i. Item 1.3.2.5 - persistência em contexto GSLB

A alegação apresentada pela Recorrente quanto ao suposto não atendimento do item 1.3.2.5 desconsidera a distinção entre os requisitos de persistência de sessão e de sincronização de estados em alta disponibilidade, bem como os esclarecimentos técnicos já apresentados pela Network Secure durante a primeira diligência, formalizada por meio do Ofício nº 191/2026.

Inicialmente, cumpre destacar que o item 1.3.2.5 integra o requisito “1.3.2. Serviço de Balanceamento Global de Aplicações (GSLB)”, estando, portanto, inserido no contexto específico do serviço de Global Server Load Balancing, relacionado ao direcionamento e à disponibilidade global das aplicações.

O referido subitem estabelece:

> “1.3.2.5. Mecanismos de persistência de sessão (cookie, source IP, SSL session ID);”

Conforme esclarecido na diligência anterior, não se mostra tecnicamente adequado utilizar isoladamente esse subitem para acrescentar ao requisito de cluster ativo-ativo, previsto no item 1.1.5, uma obrigação específica de sincronização integral das tabelas de persistência associadas a todos os mecanismos relacionados.

O item 1.1.5 estabelece a necessidade de operação em cluster ativo-ativo, com sincronização de estados entre os nós, incluindo tabelas de sessão, persistência e conexões ativas. Entretanto, não individualiza expressamente quais métodos de persistência devem possuir sincronização de suas respectivas tabelas, tampouco determina que essa funcionalidade seja obrigatoriamente implementada para todos os mecanismos de persistência relacionados em outros subitens do Termo de Referência.

Sob o aspecto técnico, é necessário distinguir a disponibilidade de determinado mecanismo de persistência da capacidade de sincronizar suas informações entre os membros de um cluster. A persistência de sessão possui a finalidade de manter a associação entre clientes e servidores de destino, conforme os critérios definidos para o serviço de balanceamento. A sincronização em alta disponibilidade, por sua vez, destina-se ao compartilhamento de determinadas informações de estado e persistência entre os membros do cluster, de modo a possibilitar a continuidade das operações nos cenários suportados.

Dessa forma, a limitação relacionada à sincronização de determinada tabela de persistência não permite concluir, isoladamente, pela inexistência do respectivo mecanismo de persistência na solução.

Conforme já demonstrado pela Network Secure durante a diligência, a documentação oficial do FortiADC 8.0.3, na seção *HA Synchronization*, estabelece expressamente que a solução contempla os seguintes mecanismos:

- Layer-4 TCP Connection States;
- Layer-4 Persistence Tables;
- Layer-7 Persistence Tables (Source Address Persistence only).

Portanto, a documentação oficial comprova que o FortiADC possui mecanismos nativos de sincronização dos estados de conexão TCP em camada 4, das tabelas de persistência em camada 4 e das tabelas de persistência em camada 7 baseadas em endereço de origem.

Essas funcionalidades demonstram que a sincronização entre os membros do cluster não se limita aos parâmetros administrativos ou às configurações do equipamento, abrangendo também informações operacionais relacionadas às conexões e à persistência.

A Recorrente utiliza a impossibilidade de sincronização da tabela de persistência por SSL Session ID como fundamento para questionar o atendimento ao requisito.

Entretanto, conforme já esclarecido, essa restrição deve ser analisada em seu contexto técnico específico.

A documentação oficial do fabricante estabelece que a tabela de persistência baseada em SSL Session ID não é sincronizada entre os membros do cluster. Tal limitação pode exigir o estabelecimento de uma nova conexão SSL após um evento de failover. Contudo, essa restrição não elimina os demais mecanismos de sincronização disponibilizados pela plataforma, incluindo a sincronização de estados TCP em L4 e de tabelas de persistência em L4 e L7 por endereço de origem, nos respectivos cenários suportados. Assim, a existência de uma limitação específica não deve ser generalizada como ausência de mecanismos de persistência ou de sincronização de estados na solução ofertada.

Conforme sustentado pela Network Secure na diligência anterior, a avaliação de conformidade deve observar a redação objetiva, o contexto e a finalidade de cada requisito. O item 1.3.2.5 encontra-se inserido no conjunto de funcionalidades relacionadas ao GSLB, enquanto o item 1.1.5 estabelece as características da arquitetura de alta disponibilidade.

Embora os requisitos possuam relação funcional, a interpretação conjunta não deve resultar automaticamente na imposição de condições técnicas adicionais não expressamente individualizadas no instrumento convocatório.

Nesse sentido, a limitação documental relacionada à sincronização de SSL Session ID deve ser avaliada considerando sua efetiva abrangência, sem afastar os mecanismos de sincronização expressamente suportados e documentados pelo FortiADC.

Diante do exposto, a argumentação apresentada pela Recorrente não demonstra, por si só, a inexistência dos mecanismos de persistência previstos na solução, uma vez que se fundamenta, principalmente, em uma limitação específica relacionada à sincronização da tabela de persistência por SSL Session ID. A documentação oficial do FortiADC 8.0.3 comprova a existência de mecanismos nativos de sincronização de estados e persistência em diferentes camadas de processamento, conforme já apresentado pela Network Secure durante a primeira diligência.

Ressalta-se que esses esclarecimentos foram formalmente encaminhados ao TJCE antes da interposição do presente recurso administrativo, integrando o conjunto de informações técnicas submetidas à apreciação da Administração. Dessa forma, requer-se que a alegação recursal seja apreciada considerando a distinção entre os mecanismos de persistência e suas respectivas capacidades de sincronização em alta disponibilidade, evitando-se que uma limitação específica seja interpretada como ausência generalizada de funcionalidades.

Requer-se, ainda, que a Administração considere integralmente os esclarecimentos anteriormente prestados em atendimento ao Ofício nº 191/2026 e as referências oficiais do fabricante, observando os princípios da vinculação ao instrumento convocatório, da motivação e do julgamento objetivo.

Link de referência:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/469954/layer-7-capabilities-for-http-https-traffic
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/932874/configuring-persistence-rules

ii. Item 1.6.25 - persistência em comunicações criptografadas

A alegação apresentada pela Recorrente quanto ao suposto não atendimento do item 1.6.25 decorre de uma interpretação equivocada das funcionalidades de persistência de sessão disponibilizadas pelo FortiADC, especialmente ao associar a capacidade de manter a persistência em comunicações criptografadas às limitações específicas de sincronização de determinadas tabelas de persistência entre membros de um cluster de alta disponibilidade.

Inicialmente, cumpre destacar que o item 1.6.25 do Termo de Referência estabelece:

> "Deve possibilitar a utilização da persistência de sessão mesmo para comunicações que utilizem criptografia."

O FortiADC 8.0.3 possui suporte nativo à persistência de sessão em comunicações HTTPS, disponibilizando diferentes mecanismos para manter o direcionamento das requisições de um mesmo cliente ao servidor backend previamente selecionado. Conforme a documentação oficial do fabricante, na seção *Configuring Persistence Rules*, a plataforma disponibiliza mecanismos de persistência baseados em endereço IP de origem, cookies HTTP e identificador de sessão SSL (*SSL Session ID*), entre outros. Esses mecanismos permitem manter a afinidade entre o cliente e o servidor de aplicação, mesmo quando a comunicação utiliza criptografia SSL/TLS, observadas as características e os requisitos de configuração de cada método. A comprovação pode ser realizada diretamente por meio do *FortiADC 8.0.3 CLI Reference*, na seção *config load-balance persistence*, na qual o fabricante documenta expressamente a criação de uma política de persistência baseada no identificador da sessão SSL, utilizando os seguintes comandos:

```
config load-balance persistence
  edit "ssl-session-id"
```

```
        set type ssl-session-id
        set timeout 300
    next
end
```

O comando set type ssl-session-id demonstra de forma objetiva que a persistência por identificador de sessão SSL constitui uma funcionalidade nativa e configurável do FortiADC, não dependendo de desenvolvimento adicional ou de mecanismos externos à solução. Para aplicações HTTPS, o FortiADC permite utilizar mecanismos de persistência como Source Address, Source Address Hash, Cookie Hash, Persistent Cookie, Insert Cookie e SSL Session ID, observadas as condições de processamento SSL/TLS e compatibilidade do perfil configurado.

Adicionalmente, o texto do item 1.6.25 não estabelece como condição específica a sincronização da tabela de persistência SSL Session ID entre nós HA, limitando-se a exigir que o mecanismo de persistência possa ser utilizado em comunicações que empreguem criptografia. Dessa forma, a documentação oficial da versão 8.0.3 demonstra que o FortiADC dispõe de recursos nativos e configuráveis para estabelecimento de persistência em comunicações HTTPS, inclusive mediante identificador de sessão SSL, atendendo à capacidade funcional expressamente descrita no item 1.6.25.

Diante do exposto, requer-se que seja afastada a alegação de descumprimento do item 1.6.25, uma vez que o fabricante documenta expressamente a existência de mecanismos de persistência compatíveis com comunicações criptografadas

Link de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/397561/ssl-decryption-by-forward-proxy
https://docs.fortinet.com/document/fortiadc/8.0.3/cli-reference/58382/config-load-balance-virtual-server
https://docs.fortinet.com/document/fortiadc/8.0.3/cli-reference/234711/config-load-balance-persistence

iii. Item 1.6.26 - mecanismo SSL Session ID

1.6.26. A persistência de sessão deve se basear, no mínimo, nos seguintes parâmetros:

1.6.26.1. IP DE ORIGEM, operando com, no mínimo, os protocolos HTTP, HTTPS, TCP, UDP;

1.6.26.2. URL, operando com os protocolos HTTP e HTTPS;

1.6.26.3. COOKIE HTTP, operando com os protocolos HTTP e HTTPS;

1.6.26.4. SSL SESSION ID.

A documentação oficial do fabricante comprova o suporte aos mecanismos de persistência exigidos:

IP de origem: Source Address, suportado nos perfis TCP, UDP, HTTP e HTTPS.

URL: mecanismos baseados em requisições HTTP, incluindo HTTP Request Hash, nos perfis HTTP e HTTPS.

Cookie HTTP: mecanismos como Cookie Hash, Persistent Cookie, Insert Cookie, Embedded Cookie, Rewrite Cookie e Passive Cookie.

SSL Session ID: mecanismo de persistência disponível para o perfil HTTPS.

Predefined persistence rules

Predefined	Description
LB_PERSIS_SRC_ADDR	Persistence based on source IP address or subnet.
LB_PERSIS_HASH_SRC_ADDR	Persistence based on a hash of source IP address.
LB_PERSIS_HASH_SRC_ADDR_PORT	Persistence based on a hash that includes source IP address and port.
LB_PERSIS_HASH_COOKIE	Persistence is based on a hash of a cookie provided by client request.
LB_PERSIS_RDP_COOKIE	Persistence based on RDP cookie sent by RDP clients in the initial connection request.
LB_PERSIS_SSL_SESS_ID	Persistence based on the SSL session ID.
LB_PERSIS_SIP_CALL_ID	Persistence based on the SIP call ID.
LB_PERSIS_PASSIVE_COOKIE	Persistence based on a passive cookie generated by the server. FortiADC does not generate or manage the cookie, but only observes it in the HTTP stream, thus the name "passive cookie". Also known as "server cookie".

Link de Referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/932874/configuring-persistence-rules

A comprovação dos mecanismos de persistência encontra-se demonstrada na documentação oficial do fabricante, conforme Figura 1 – Tipos de perfis de aplicação e mecanismos de persistência suportados pelo FortiADC. A captura evidencia a disponibilidade de persistência por endereço IP de origem nos perfis TCP, UDP, HTTP

e HTTPS, bem como dos mecanismos baseados em requisições HTTP e cookies, conforme as compatibilidades indicadas pelo fabricante.

Link de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/559628/configuring-application-profiles

Application Profile Types

Each Application Profile Type requires specific parameters to be configured. The following table lists the supported Application Profile Types and their usage and compatibilities. Use the links under the **Profile Type** column to navigate to the configuration parameters applicable to each Application Profile Type and view its available predefined Profile configuration.

Profile Type	Usage	VS Type	LB Methods	Persistence
TCP	Use for other TCP protocols.	Layer 4	Round Robin, Least Connection, Fastest Response, Dynamic Load	Source Address, Source Address Hash, Source Address-Port Hash
		Layer 2	Round Robin, Least Connection, Fastest Response, Destination IP Hash, Dynamic Load	
UDP	Use with UDP servers.	Layer 4	Round Robin, Least Connection, Fastest Response, Dynamic Load	Source Address, Source Address Hash, Source Address-Port Hash
		Layer 2	Round Robin, Least Connection, Fastest Response, Dynamic Load, Destination IP Hash	
HTTP	Use for standard, unsecured web server traffic.	Layer 7	Round Robin, Least Connection, URI Hash, Full URI Hash, Host Hash, Host Domain Hash, Dynamic Load	Source Address, Source Address Hash, Source Address-Port Hash, HTTP Header Hash, HTTP Request Hash, Cookie Hash, Persistent Cookie, Insert Cookie, Embedded Cookie, Rewrite Cookie, Passive Cookie
		Layer 2	Round Robin, Least Connection, URI Hash, Full URI Hash, Host Hash, Host Domain Hash, Dynamic Load, Destination IP Hash	
HTTPS	Use for secured web server traffic when offloading TLS/SSL from the backend servers. You must import the backend server certificates into FortiADC and select them in the HTTPS profile.	Layer 7	Round Robin, Least Connection, URI Hash, Full URI Hash, Host Hash, Host Domain Hash, Dynamic Load	Source Address, Source Address Hash, Source Address-Port Hash, HTTP Header Hash, HTTP Request Hash, Cookie Hash, Persistent Cookie, Insert Cookie, Embedded Cookie, Rewrite Cookie, Passive Cookie, SSL Session ID
		Layer 2	Round Robin, Least Connection, URI Hash, Full URI Hash, Host Hash, Host Domain Hash, Dynamic Load, Destination IP Hash	

A documentação oficial Fortinet – HA synchronization esclarece expressamente que o FortiADC sincroniza os seguintes estados entre os membros do cluster:
Layer-4 TCP connection states, Layer-4 persistence tables, and Layer-7 persistence tables (Source Address Persistence only). Essa documentação constitui evidência objetiva de que a solução implementa mecanismos de sincronização de conexões TCP de camada 4 e de tabelas de persistência de camada 4 e camada 7, incluindo a persistência por endereço de origem na camada 7.

Portanto, não procede eventual alegação de que a solução seja incapaz de sincronizar tabelas de persistência em ambiente de alta disponibilidade. O fabricante documenta expressamente esse recurso, cujo alcance deve ser avaliado conforme os mecanismos e as condições técnicas especificados na documentação.

Link de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/657374/ha-synchronization

Diante do exposto, resta demonstrado o atendimento aos requisitos dos itens 1.6.26 e 1.1.5, considerando-se individualmente os mecanismos de persistência exigidos e as funcionalidades de sincronização em alta disponibilidade comprovadas pela documentação oficial do fabricante.

Ressalta-se que o edital não estabelece, em nenhum item específico, a obrigatoriedade de sincronização da tabela de persistência baseada em SSL Session ID em ambiente HA. O item 1.6.26.4 exige o suporte à persistência por SSL Session ID, enquanto o item 1.1.5 estabelece os requisitos de sincronização de estados entre os nós do cluster, sem determinar expressamente que todos os mecanismos de persistência relacionados no item 1.6.26 devam ter suas tabelas sincronizadas simultaneamente.

Nesse contexto, entende-se que a empresa L8 Group está agrupando requisitos distintos para atribuir ao edital uma exigência que não foi expressamente estabelecida, utilizando essa interpretação como fundamento para contestar uma solução que comprova o atendimento às funcionalidades requeridas.

iv. Item 1.1.7 - risco de sobrecarga no failover ativo-ativo

> “1.1.7. Os equipamentos deverão possuir quantidade de memória e capacidade de processamento suficiente para atendimento de todas as funcionalidades e desempenho solicitados neste documento, sem degradação de performance com todas as funcionalidades habilitadas simultaneamente.”

O FortiADC 2000G possui recursos de hardware significativamente superior aos requisitos mínimos de capacidade e desempenho estabelecidos no edital. O equipamento dispõe de **128 GB de memória RAM ECC, correspondendo ao dobro dos 64 GB exigidos**, além de capacidade divulgada pelo fabricante de 90 Gbps de throughput L4/L7, 60 Gbps de throughput de criptografia TLS e 2.500.000 requisições L7 por segundo. Em comparação com os parâmetros mínimos do edital, o FortiADC 2000G apresenta os seguintes indicadores: **2 vezes a memória RAM exigida**, throughput L4/L7 divulgado equivalente a **2,25 vezes o mínimo solicitado**, capacidade de criptografia TLS equivalente a **2 vezes o requisito** e processamento de requisições L7 correspondente a **5 vezes o mínimo exigido**. Essas especificações evidenciam a elevada capacidade de hardware do equipamento e sua margem de desempenho em relação aos parâmetros estabelecidos. A avaliação da operação simultânea de todas as funcionalidades deve considerar as condições de dimensionamento e as métricas específicas aplicáveis a cada requisito, de modo a fundamentar tecnicamente o atendimento à exigência de desempenho sem degradação. Dessa forma, o FortiADC 2000G apresenta capacidade de memória e processamento substancialmente superior aos mínimos quantitativos previstos no edital, devendo a comprovação da operação simultânea de todas as funcionalidades ser complementada, quando necessário, pela documentação técnica específica do fabricante.

Link Referência:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC.pdf

c) Virtualização, isolamento e recursos por instância (recurso, item III.4) Item 1.3.21 - isolamento lógico dos domínios virtuais

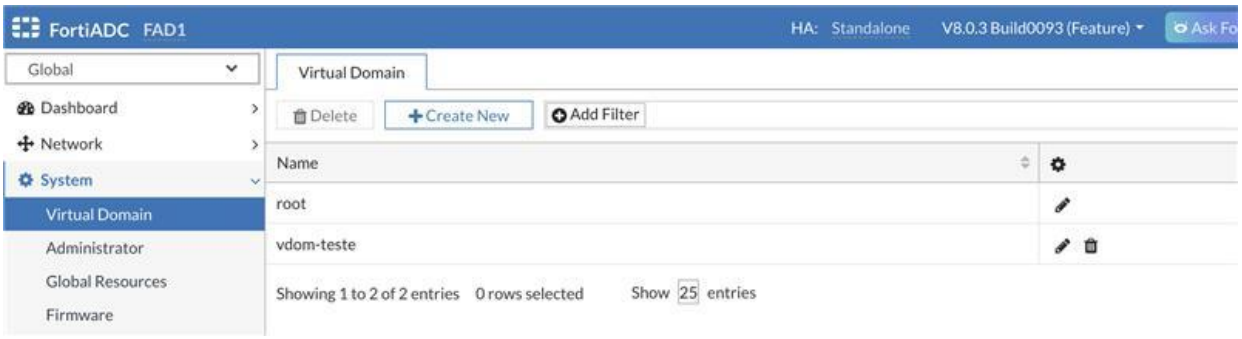
A alegação apresentada pela Recorrente quanto à suposta ausência de isolamento entre instâncias virtuais do FortiADC desconsidera os mecanismos nativos de segregação disponibilizados pela solução, bem como os esclarecimentos técnicos e as evidências apresentados pela Network Secure durante a segunda diligência, formalizada por meio do Ofício nº 207/2026.

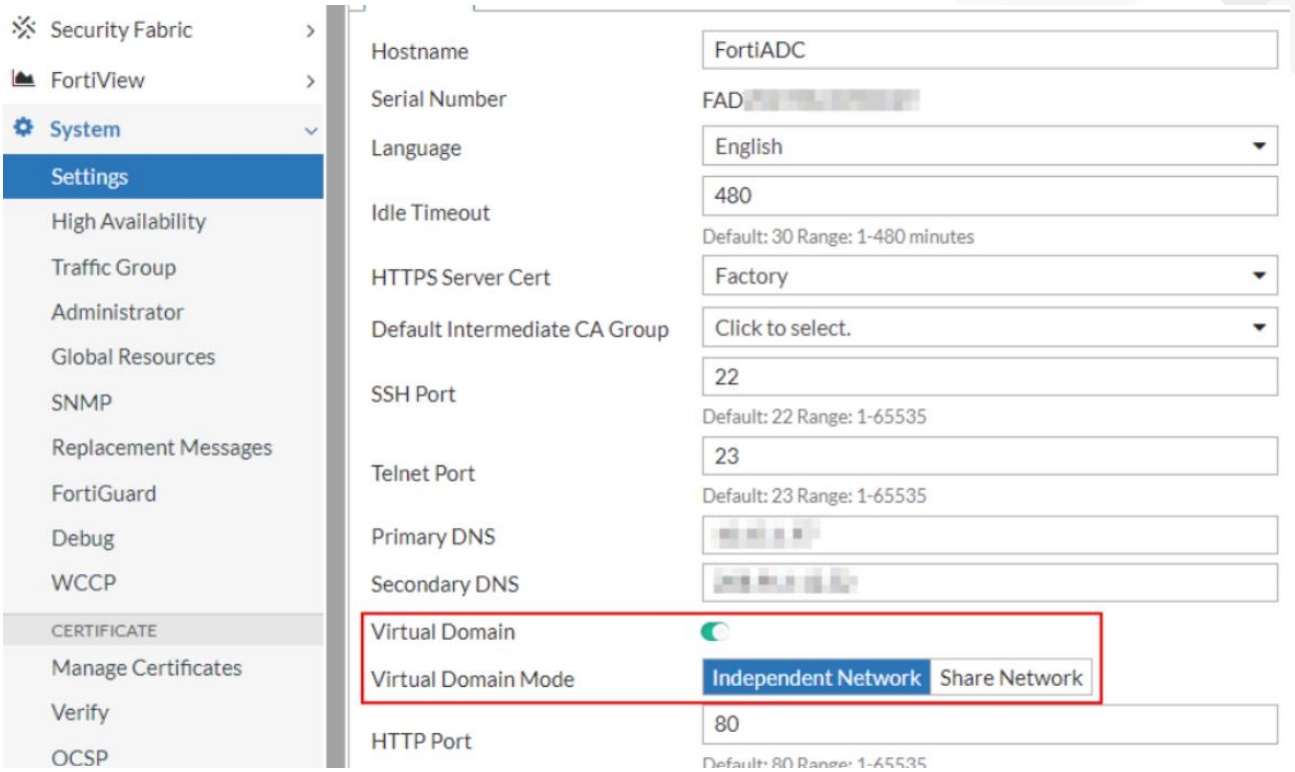
Conforme anteriormente demonstrado, o FortiADC 8.0.3 dispõe da funcionalidade Virtual Domains (VDOMs), que permite particionar um único appliance físico em

múltiplas instâncias lógicas independentes, proporcionando segregação de tráfego, configurações, interfaces de rede, objetos administrativos e políticas de segurança.

Segundo a documentação oficial do fabricante, na seção *Virtual Domain*, essa arquitetura foi desenvolvida para ambientes multi-tenant, permitindo que diferentes instâncias compartilhem a infraestrutura física do equipamento, mantendo separados seus respectivos contextos lógicos de operação e administração. Para a implementação dessa arquitetura, o FortiADC disponibiliza o modo Independent Network, no qual cada VDOM opera independentemente em seu próprio contexto de rede, com interfaces, configurações e políticas associadas à respectiva instância.

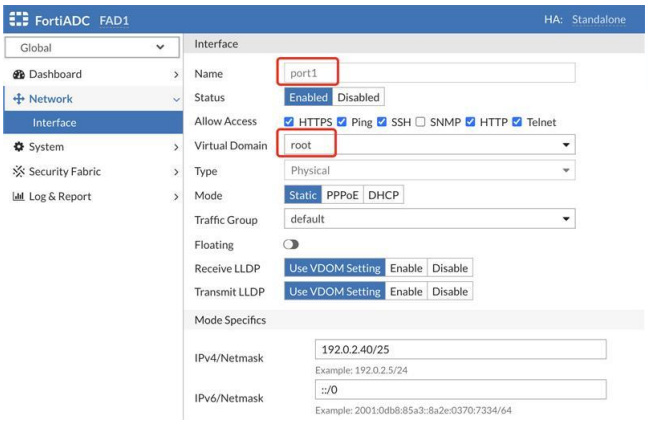
A documentação oficial da versão 8.0.3 estabelece expressamente que, nesse modo, cada VDOM funciona de maneira independente dentro de sua própria rede, sem ser afetada pelas atividades das demais VDOMs existentes no equipamento. Em complemento às referências documentais anteriormente apresentadas, a Network Secure disponibiliza evidências extraídas da interface administrativa do FortiADC 8.0.3, demonstrando o comportamento das instâncias virtuais em ambiente configurado para essa finalidade. As primeiras capturas demonstram a existência de duas instâncias virtuais distintas, identificadas como root e vdom-teste, bem como a habilitação da funcionalidade Virtual Domain no modo Independent Network. A configuração evidencia que as instâncias operam sob o modelo de separação lógica de rede disponibilizado nativamente pelo fabricante, diferentemente do modo Share Network, no qual ocorre compartilhamento da infraestrutura lógica de rede entre domínios administrativos.

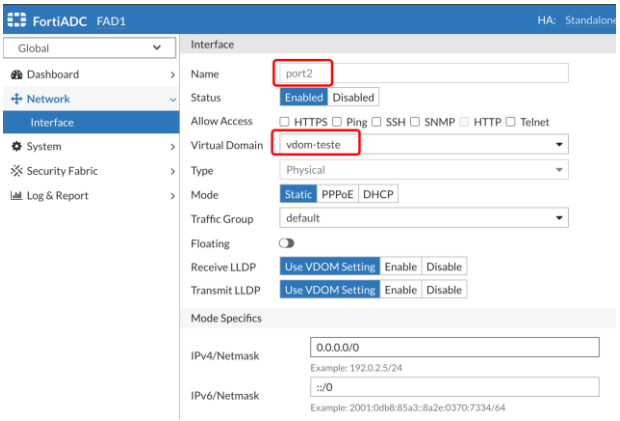


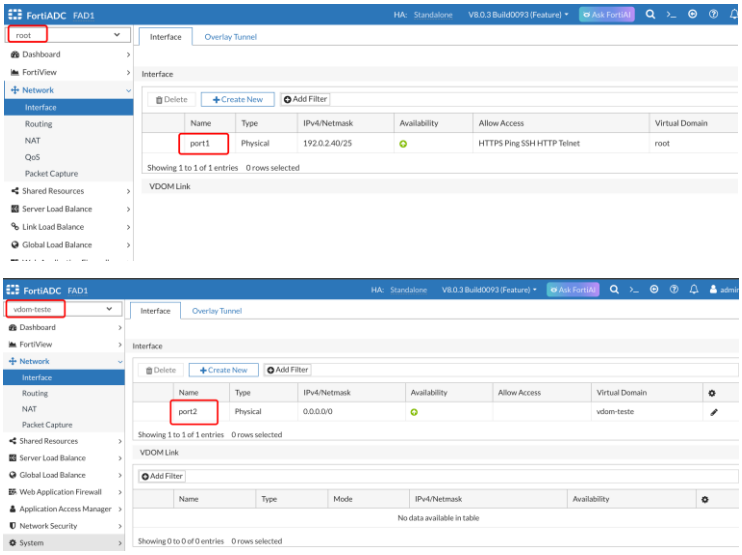


As capturas seguintes demonstram a atribuição individualizada das interfaces físicas às respectivas instâncias virtuais. Na configuração apresentada, a interface port1 encontra-se associada à VDOM root, enquanto a interface port2 está vinculada à VDOM vdom-teste. Ao acessar individualmente cada contexto administrativo, observa-se que a VDOM root apresenta somente a interface port1, enquanto a VDOM vdom-teste apresenta exclusivamente a interface port2. Essa demonstração evidencia que a associação das interfaces não representa apenas uma organização visual da configuração global, mas constitui mecanismo de delimitação dos recursos de rede disponibilizados para cada domínio virtual.

Conforme descrito na documentação oficial, o administrador global é responsável pela atribuição das interfaces e pela definição dos administradores vinculados às VDOMs, estabelecendo os limites de gerenciamento e de utilização dos recursos de rede pertencentes a cada instância.



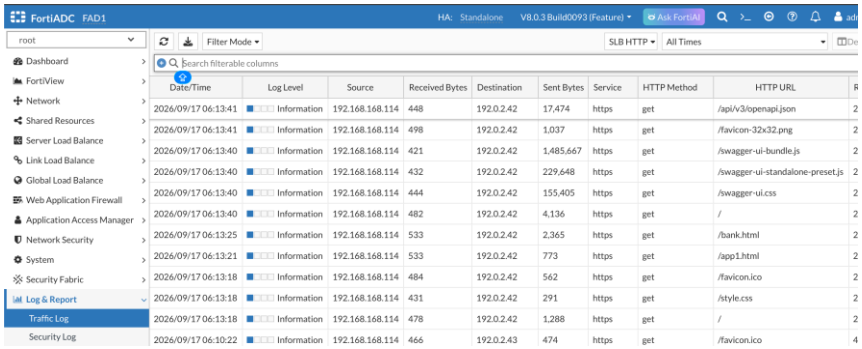


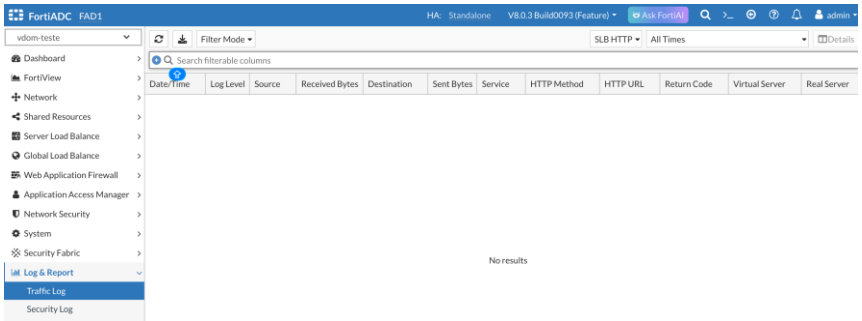


Além da separação das interfaces, as evidências apresentadas demonstram a individualização da visualização dos registros de tráfego entre as instâncias virtuais. Ao selecionar a VDOM root, a interface administrativa apresenta registros de tráfego correspondentes ao contexto selecionado, incluindo informações de origem, destino, serviço, método HTTP e demais atributos das conexões.

Por outro lado, ao selecionar a VDOM vdom-teste, os registros apresentados anteriormente deixam de constar da visualização, sendo exibida a consulta correspondente ao contexto da segunda instância, sem registros para o período demonstrado. Esse comportamento evidencia a existência de contextos individualizados de consulta e monitoramento, nos quais os registros são apresentados conforme a VDOM selecionada.

A documentação oficial do fabricante também estabelece que administradores com permissões restritas a determinada VDOM podem acessar somente as configurações, os logs e os relatórios correspondentes aos domínios que lhes foram atribuídos, enquanto o administrador global permanece responsável pelo gerenciamento centralizado do appliance.





A arquitetura de Virtual Domains do FortiADC também contempla segregação administrativa, permitindo a criação de contas com permissões específicas para cada instância virtual.

Dessa forma, o administrador global mantém a capacidade de criar e gerenciar os domínios, atribuir interfaces e definir permissões, enquanto os administradores vinculados às instâncias possuem acesso restrito aos respectivos ambientes.

Complementarmente, o FortiADC disponibiliza o mecanismo Virtual Domain Policies, destinado ao estabelecimento de limites individualizados para utilização de

recursos dinâmicos e estáticos, incluindo L4 CPS, L7 CPS, L7 RPS, SSL CPS, SSL Throughput, sessões concorrentes e taxas de tráfego. Esses mecanismos permitem administrar o consumo dos recursos compartilhados do appliance e estabelecer limites operacionais para cada domínio, complementando a segregação lógica proporcionada pela arquitetura Independent Network. Cabe distinguir que o controle de consumo por limites máximos não equivale, isoladamente, à reserva física exclusiva de CPU ou memória. A comprovação desses aspectos específicos deve observar as características documentadas do mecanismo de gerenciamento de recursos da plataforma.

Diante das evidências apresentadas, não se sustenta a afirmação genérica de que o FortiADC se limita à criação de contextos administrativos sem mecanismos efetivos de segregação entre instâncias. A documentação oficial e as capturas de tela demonstram a existência de recursos nativos para separação dos domínios virtuais, atribuição independente das interfaces de rede, individualização dos contextos de configuração, segregação administrativa e visualização de registros de tráfego por VDOM. Essas características evidenciam que a virtualização disponibilizada pelo FortiADC possui mecanismos de isolamento lógico e operacional que ultrapassam a simples divisão visual da interface administrativa.

Ressalta-se, ainda, que os mecanismos descritos já foram apresentados ao TJCE durante a segunda diligência, não constituindo alteração das características da solução ofertada, mas complementação das evidências anteriormente disponibilizadas para comprovação de suas funcionalidades nativas.

Dessa forma, requer-se que a Administração considere integralmente as referências oficiais do fabricante, os esclarecimentos anteriormente prestados e as evidências adicionais apresentadas, afastando a alegação de inexistência de mecanismos de isolamento lógico entre instâncias virtuais do FortiADC.

A avaliação dos aspectos específicos relacionados à garantia de recursos de hardware deverá considerar os mecanismos efetivamente documentados de Virtual Domain Policies e as exigências correspondentes do Termo de Referência, distinguindo-se o isolamento lógico de rede e administração da reserva física de recursos de processamento.

Link de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/648330/virtual-domain
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/654503/configuring-basic-system-settings
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/602431/selecting-the-optimal-mode-vdom-vs-adom
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/120920/virtual-domain-policies
https://docs.fortinet.com/document/fortiadc/8.0.3/cli-reference/210026/appendix-a-virtual-domains
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/493988/enabling-the-virtual-domain-feature-and-selecting-the-virtual-domain-mode

i. Item 1.3.22 - alocação e limitação de recursos por VDOM

A alegação apresentada pela Recorrente quanto à suposta ausência de mecanismos de alocação e limitação de recursos entre instâncias virtuais do FortiADC desconsidera as funcionalidades nativas disponibilizadas pela solução, bem como os esclarecimentos técnicos e as evidências apresentados pela Network Secure durante a segunda diligência, formalizada por meio do Ofício nº 207/2026.

Conforme anteriormente demonstrado, o FortiADC 8.0.3 dispõe do mecanismo **Virtual Domain Policies**, que permite estabelecer políticas individualizadas de controle e limitação de recursos para cada domínio virtual (VDOM), especialmente quando configurado no modo de operação Independent Network.

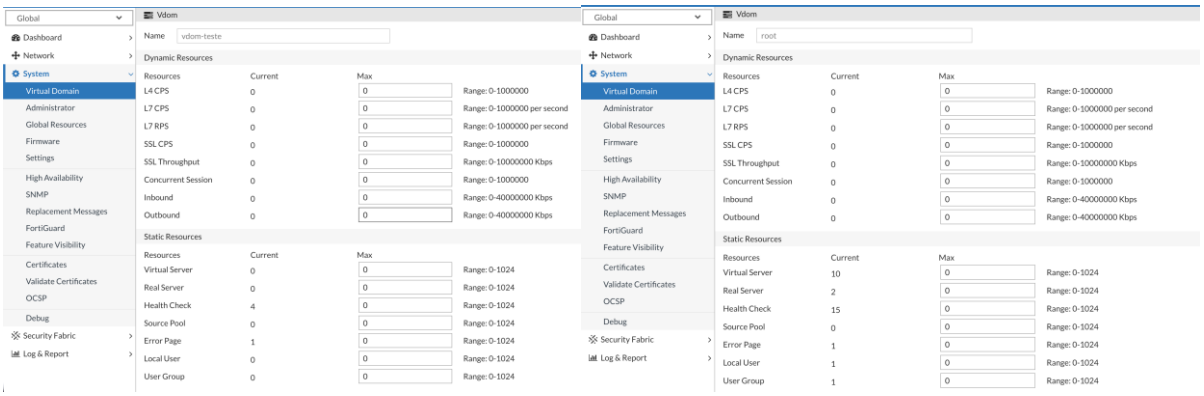
A documentação oficial da Fortinet estabelece que essas políticas possibilitam a definição de parâmetros específicos para cada instância, organizados em duas categorias: Dynamic Resources e Static Resources.

O mecanismo Virtual Domain Policies permite estabelecer limites individuais para os seguintes recursos:

- L4 CPS: quantidade de novas conexões de camada 4 por segundo;

- L7 CPS: quantidade de novas conexões de camada 7 por segundo;
- L7 RPS: quantidade de requisições HTTP processadas por segundo;
- SSL CPS: quantidade de novas conexões SSL por segundo;
- SSL Throughput: capacidade de processamento de tráfego SSL;
- Concurrent Sessions: quantidade de sessões concorrentes;
- Inbound: limite de tráfego de entrada;
- Outbound: limite de tráfego de saída.

Os parâmetros são definidos individualmente para cada VDOM, permitindo que o administrador global estabeleça políticas de consumo distintas conforme as necessidades operacionais dos ambientes virtualizados. As capturas de tela apresentadas demonstram a disponibilidade desses parâmetros tanto na VDOM root quanto na VDOM vdom-teste, evidenciando que os mecanismos de controle são configuráveis por instância, e não exclusivamente de maneira global para todo o appliance.



Além dos recursos relacionados ao processamento de tráfego, a solução permite estabelecer limites para objetos de configuração associados às instâncias virtuais, incluindo:

- Virtual Servers;
- Real Servers;
- Health Checks;
- Source Pools;
- Error Pages;

- Local Users;
- User Groups.

As evidências demonstram que cada VDOM possui contadores próprios de utilização desses objetos, possibilitando ao administrador definir limites específicos de configuração para cada ambiente. Dessa forma, a solução disponibiliza mecanismos de controle tanto sobre parâmetros de desempenho quanto sobre a quantidade de objetos administrativos e operacionais utilizados por cada domínio virtual.
Importante destacar que os parâmetros disponibilizados pelo FortiADC não constituem exclusivamente indicadores de monitoramento.

Conforme descrito no FortiADC 8.0.3 CLI Reference, seção Appendix A: Virtual Domains, os valores definidos nas políticas representam limites operacionais aplicados pelo próprio equipamento. No caso do parâmetro L4 CPS, por exemplo, a documentação estabelece que, quando a taxa de criação de novas conexões ultrapassa o valor configurado, o equipamento admite somente a quantidade de conexões correspondente ao limite estabelecido. Da mesma forma, para o parâmetro Concurrent Sessions, o fabricante documenta que novas conexões deixam de ser admitidas quando o número de sessões existentes atinge o limite definido para a instância.

Esses comportamentos demonstram que as políticas possuem mecanismos nativos de imposição de limites, restringindo o consumo dos recursos controlados de acordo com os parâmetros estabelecidos para cada VDOM.

A configuração desses controles pode ser realizada por meio da interface gráfica ou da interface de linha de comando (CLI), utilizando a estrutura config global e config system vdom, na qual cada domínio possui parâmetros próprios de utilização de recursos.

Adicionalmente, o FortiADC disponibiliza o comando get system vdom-status, que permite consultar individualmente, para cada domínio virtual, os indicadores de utilização dos recursos e os respectivos limites configurados.

Conforme exemplo apresentado na documentação oficial do fabricante, o comando disponibiliza informações como L4 CPS, L7 CPS, L7 RPS, SSL CPS, SSL Throughput, Concurrent Sessions, Inbound, Outbound e quantidade de objetos de configuração.

A saída do comando apresenta os valores de utilização corrente e os limites estabelecidos, permitindo ao administrador verificar os recursos consumidos em cada contexto virtual.

The following example shows the system with two VDOMs set.

```
FortiADC-300D # get system vdom-status
root:
  l4cps: 4.87/-
  l7cps: 90.2/-
  l7rps: 0.0/-
  SSLcps: 3.7/-
  SSLThroughput(KB/S): 1550.0/-
  ConcurrentSession: 47.0/-
  Inbound(KB/S): 255.6/-
  Outbound(KB/S): 104669.0/-
  VirtualServer: 21/-
  RealServer: 33/33
  Health Check: 5/-
  Source Pool: 0/-
  Error-Page: 1/-
  LocalUser: 0/-
  UserGroup: 2/-
  vdom1:
  l4cps: 0.0/-
  l7cps: 0.0/-
  l7rps: 0.0/-
  SSLcps: 0.0/-
  SSLThroughput(KB/S): 0.0/-
  ConcurrentSession: 0.0/-
  Inbound(KB/S): 0.0/-
  Outbound(KB/S): 0.0/-
  VirtualServer: 0/-
  RealServer: 0/-
  Health Check: 4/-
  Source Pool: 0/-
  Error-Page: 0/-
  LocalUser: 0/-
  UserGroup: 0/-
```

The first number represents the current usage. The second number represents the limit set. A dashed line means no limit has been set.

Essa funcionalidade complementa os mecanismos de configuração e controle, permitindo acompanhar individualmente a utilização dos recursos e verificar os limites definidos para cada instância. A própria documentação oficial da Fortinet esclarece que a finalidade das Virtual Domain Policies é estabelecer limites de consumo que evitem a utilização indiscriminada dos recursos compartilhados do equipamento por uma única instância virtual.

Na ausência de limites individuais, uma VDOM poderia consumir parcela significativa dos recursos disponíveis no appliance, comprometendo a capacidade operacional das demais instâncias. Por esse motivo, o fabricante disponibiliza políticas de limitação individualizada, permitindo ao administrador definir restrições específicas

para cada contexto virtual e reduzir o risco de esgotamento dos recursos compartilhados.

Dessa forma, o FortiADC não se limita à criação de instâncias administrativas independentes, oferecendo também controles individualizados de utilização de recursos dinâmicos e estáticos, com mecanismos de aplicação dos limites configurados. Cabe esclarecer, sob o aspecto técnico, que a definição de limites máximos de consumo não equivale automaticamente à reserva de uma capacidade mínima de processamento para cada instância. A documentação apresentada comprova os mecanismos de limitação individualizada e sua aplicação operacional, devendo a análise da exigência de garantia mínima considerar especificamente essa distinção.
Diante das evidências apresentadas, não se sustenta a afirmação genérica de que o FortiADC não dispõe de mecanismos nativos para gerenciamento, alocação administrativa e limitação individualizada de recursos por domínio virtual.

A documentação oficial da versão 8.0.3 demonstra a existência de parâmetros configuráveis por VDOM, mecanismos de enforcement e funcionalidades de monitoramento destinadas ao controle dos recursos compartilhados.

Ressalta-se que essas funcionalidades já foram objeto de esclarecimento pela Network Secure durante a segunda diligência conduzida pelo TJCE, não constituindo alteração da solução ofertada ou introdução posterior de funcionalidades.

Dessa forma, requer-se que a Administração considere integralmente os esclarecimentos anteriormente prestados, as referências oficiais do fabricante e as evidências técnicas apresentadas, reconhecendo a existência de mecanismos nativos de limitação e controle individualizado de recursos por VDOM.

Quanto à exigência específica de reserva ou garantia mínima de capacidade, requer-se que sua avaliação seja realizada de forma individualizada, distinguindo os mecanismos de limitação máxima efetivamente documentados daqueles destinados à garantia de recursos mínimos, para que a decisão observe precisamente as capacidades técnicas demonstradas.

Link de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/120920/virtual-domain-policies

https://docs.fortinet.com/document/fortiadc/8.0.3/cli-reference/210026/appendix-a-virtual-domains
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/648330/virtual-domain

ii. Item 1.3.25 - níveis de garantia e dedicação de recursos

A alegação apresentada pela Recorrente quanto à ausência de mecanismos de gerenciamento e dedicação de recursos entre as instâncias virtuais do FortiADC desconsidera as funcionalidades nativas de controle de capacidade disponibilizadas pela solução, bem como os esclarecimentos técnicos apresentados pela Network Secure durante a segunda diligência, formalizada por meio do Ofício nº 207/2026.

Inicialmente, cabe destacar que o item 1.3.25 estabelece:

> "Deve permitir a definição de níveis de garantia de recursos para as instâncias virtuais, possibilitando a dedicação de recursos para determinados contextos."

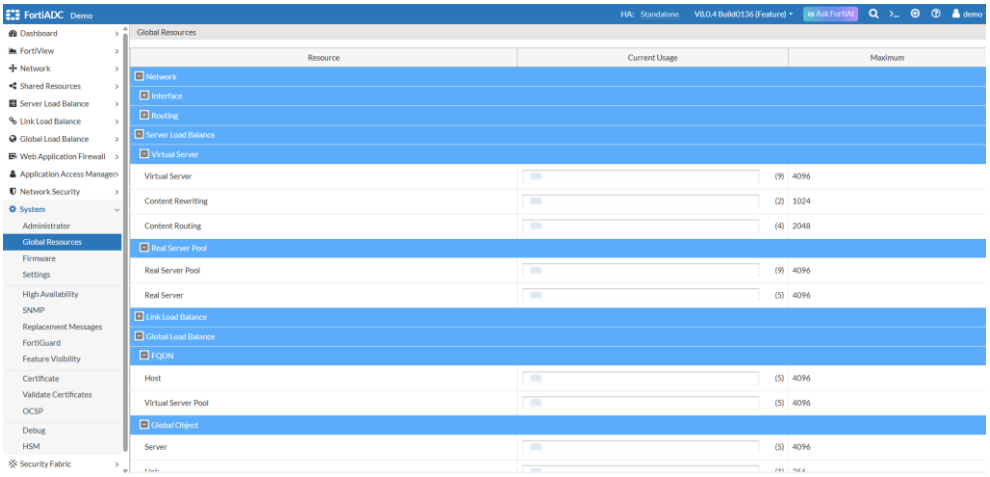
Observa-se que o requisito não determina expressamente que a dedicação de recursos deva ocorrer exclusivamente mediante reserva física de CPU e memória RAM, tampouco estabelece a obrigatoriedade de utilização de mecanismos específicos de prioridade de escalonamento entre instâncias. Entretanto, a exigência de garantia de recursos deve ser analisada em seu sentido técnico, distinguindo-se os mecanismos de controle de consumo daqueles destinados à reserva mínima de capacidade.

Conforme anteriormente apresentado, o FortiADC disponibiliza, na interface administrativa, a funcionalidade System → Global Resources, responsável pelo acompanhamento da utilização dos recursos da plataforma. A documentação oficial do fabricante estabelece que essa funcionalidade apresenta informações sobre a utilização corrente e os limites máximos dos objetos de configuração existentes no appliance, contemplando diferentes componentes da solução, incluindo:

- Virtual Servers;
- Real Servers;

- Real Server Pools;
- Content Routing e Content Rewriting;
- Recursos de Global Server Load Balancing (GSLB);
- Demais objetos de configuração relacionados às funcionalidades disponíveis.

A interface disponibiliza uma visão consolidada da utilização dos recursos, permitindo ao administrador acompanhar o consumo da plataforma, identificar situações de aproximação dos limites operacionais e planejar a distribuição dos serviços. Adicionalmente, a documentação oficial esclarece que, quando acessada no contexto de VDOM, a funcionalidade pode apresentar informações agregadas da utilização dos recursos dos domínios virtuais, contribuindo para o acompanhamento da capacidade total consumida pelo equipamento.



Complementarmente, o FortiADC 8.0.3 disponibiliza o mecanismo nativo Virtual Domain Policies, destinado à configuração de políticas individualizadas de utilização de recursos por instância virtual.

Conforme estabelecido na documentação oficial da Fortinet, para VDOMs operando em modo Independent Network, o administrador pode configurar limites específicos relativos aos Dynamic Resources e Static Resources de cada domínio.

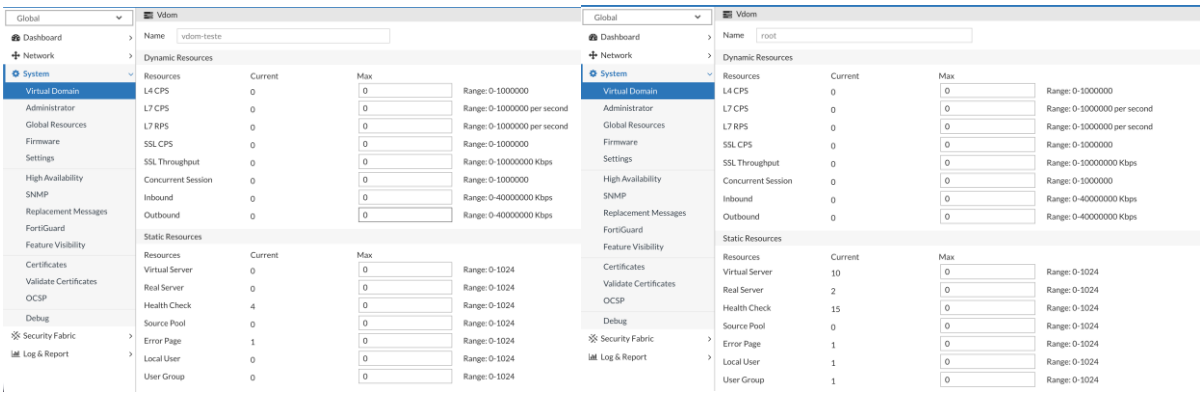
Entre os parâmetros de desempenho individualmente configuráveis encontram-se:

- L4 CPS — conexões de camada 4 por segundo;
- L7 CPS — conexões de camada 7 por segundo;

- L7 RPS — requisições de camada 7 por segundo;
- SSL CPS — conexões SSL por segundo;
- SSL Throughput — processamento de tráfego SSL;
- Concurrent Sessions — sessões concorrentes;
- Inbound e Outbound — limites de tráfego de entrada e saída.

Além dos recursos dinâmicos, o mecanismo contempla limites relacionados à quantidade de objetos estáticos utilizados pelas instâncias, como Virtual Servers, Real Servers, Health Checks e demais elementos de configuração.

As capturas de tela apresentadas demonstram a existência desses parâmetros individualmente nas VDOMs root e vdom-teste, evidenciando que cada instância dispõe de contexto próprio para definição de políticas de consumo.



Importante destacar que as Virtual Domain Policies não constituem exclusivamente mecanismos de monitoramento, mas permitem configurar restrições operacionais aplicadas nativamente pelo FortiADC. Conforme documentado no FortiADC 8.0.3 CLI Reference, os parâmetros configurados estabelecem limites de utilização que são impostos pelo equipamento, restringindo o consumo de determinados recursos por uma instância virtual. No caso de L4 CPS, por exemplo, a configuração permite limitar a quantidade de novas conexões admitidas por segundo em determinado domínio. Da mesma forma, o parâmetro Concurrent Sessions estabelece uma quantidade máxima de sessões simultâneas para a instância. A própria documentação do fabricante destaca que, na ausência de limites individuais, uma VDOM pode consumir recursos necessários ao funcionamento das demais instâncias, recomendando a configuração de restrições específicas para prevenir esse comportamento. Dessa forma, a utilização combinada dos Virtual Domains e das Virtual Domain Policies permite estabelecer

diferentes níveis de consumo operacional para contextos de aplicação distintos, reduzindo o risco de utilização indiscriminada da capacidade compartilhada.

A configuração desses parâmetros pode ser orientada pelas necessidades de cada ambiente, considerando indicadores diretamente associados ao processamento das aplicações, como conexões simultâneas, conexões por segundo, requisições por segundo e throughput. Sob a perspectiva operacional, é importante observar que a capacidade de processamento de uma solução ADC não depende exclusivamente da quantidade de CPU ou memória RAM disponível. O desempenho das aplicações publicadas também está relacionado ao volume de conexões, à quantidade de requisições processadas, ao tráfego SSL/TLS e à utilização dos recursos de balanceamento. Nesse contexto, os parâmetros disponibilizados pelas Virtual Domain Policies permitem ao administrador estabelecer limites de consumo diretamente relacionados às características das cargas de trabalho processadas pelas instâncias.

Tal abordagem proporciona mecanismos de dimensionamento e controle adequados à natureza da solução, permitindo estabelecer restrições operacionais individualizadas para cada contexto de aplicação.

Deve-se distinguir, contudo, a definição de limites máximos de consumo da reserva mínima garantida de recursos. Embora as políticas permitam restringir a utilização de capacidade por uma instância, essa funcionalidade não comprova, isoladamente, que determinada quantidade mínima de CPU, memória ou throughput permaneça exclusivamente reservada para outra VDOM.

Diante dos esclarecimentos e evidências apresentados, não se sustenta a afirmação genérica de que o FortiADC carece de mecanismos nativos de gerenciamento e controle individualizado da capacidade utilizada pelas instâncias virtuais. A documentação oficial comprova a existência de funcionalidades de acompanhamento dos recursos globais, definição individualizada de políticas por VDOM e aplicação de limites operacionais relacionados diretamente ao desempenho das aplicações.

Ressalta-se que tais mecanismos foram apresentados ao TJCE durante a segunda diligência e estão disponíveis na arquitetura nativa do FortiADC, não constituindo funcionalidades adicionais ou alterações posteriores da solução ofertada.

Nesse sentido, a Network Secure sustenta que a análise do requisito deve considerar os mecanismos de gerenciamento de capacidade efetivamente disponibilizados pela plataforma, observando que o texto do item 1.3.25 não especifica exclusivamente CPU, memória ou prioridade de escalonamento como meios obrigatórios de implementação.

Por outro lado, a comprovação de reserva mínima garantida ou dedicação exclusiva de recursos de processamento requer evidência específica, distinta da demonstração dos controles de limites máximos apresentados.

Diante do exposto, requer-se que a Administração considere integralmente a documentação oficial do fabricante, as evidências apresentadas e os esclarecimentos anteriormente prestados em resposta ao Ofício nº 207/2026, reconhecendo a existência dos mecanismos nativos de gerenciamento e controle individualizado de recursos por VDOM.

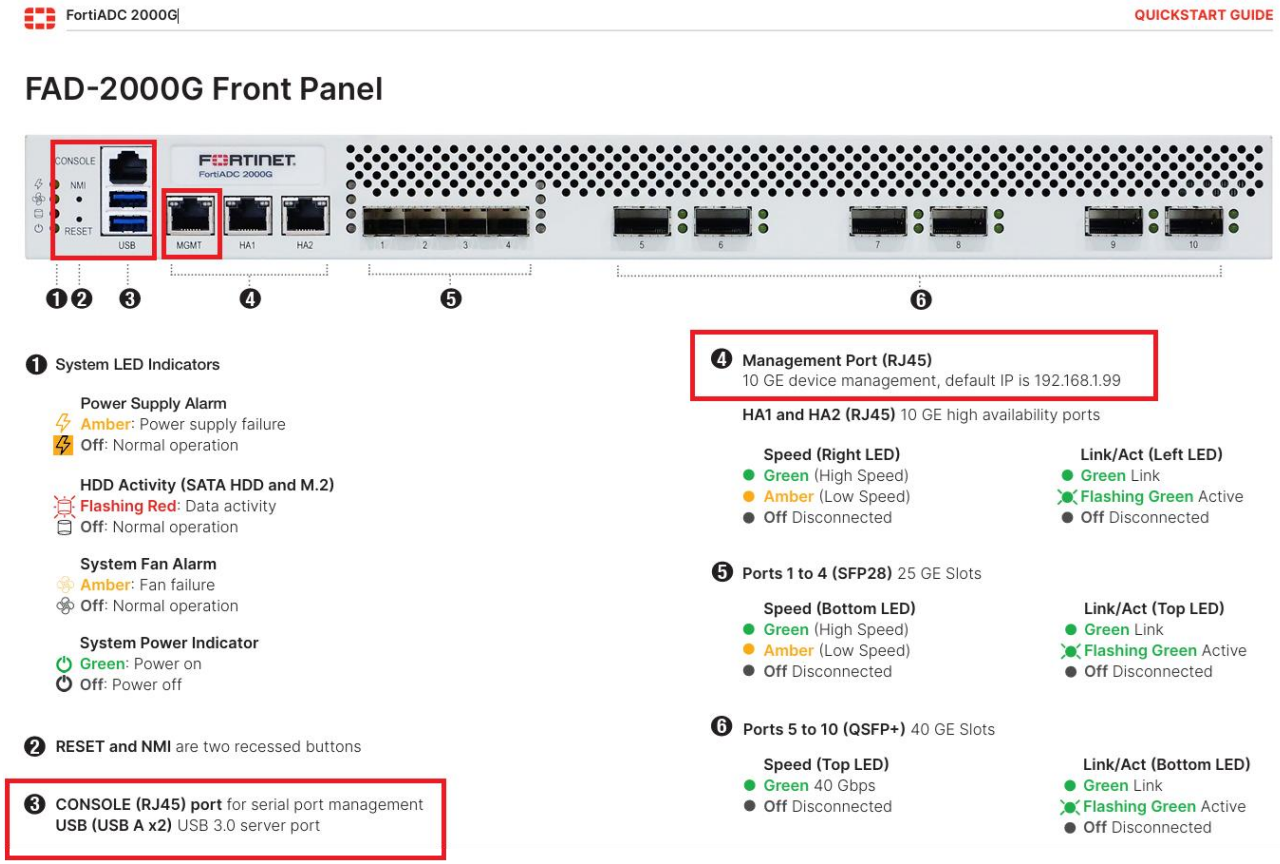
Link de referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/120920/virtual-domain-policies
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/227684/global-resources
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/648330/virtual-domain

d) Gerenciamento fora de banda (recurso, item III.5)

Referente aos itens:

> "1.3.30. Deve possuir interface dedicada para gerenciamento remoto fora de banda (out-of-band), permitindo acesso equivalente à porta console física, incluindo operações de reinicialização e diagnóstico remoto."
>
> "1.3.31. Esta interface de gerência não deve ser a interface de console e não será contabilizada para o atendimento daquelas originalmente especificadas para o tráfego de dados do equipamento."

A documentação oficial do fabricante apresenta a interface dedicada de gerenciamento e a interface de console (RJ-45) e USB e suas respectivas configurações, demonstrando sua utilização para administração remota do FortiADC



3 - CONSOLE (RJ-45) port for serial port management USB (USB A x2) USB 3.0 server port

4 - Management Port (RJ45): 10 GE device management, default IP is 192.168.1.99

Link de Referência:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a8aee65e-1c02-11f1-b31d-02356ffb40d9/FortiADC-2000G-QSG.pdf

O FortiADC possui interface de gerenciamento dedicada, permitindo a administração do equipamento por meio de uma porta específica, separada das interfaces utilizadas para o tráfego de produção. Conforme documentado no guia oficial da Fortinet, é possível configurar os parâmetros de rede dessa interface para viabilizar

o acesso administrativo ao equipamento. Essa separação permite estabelecer uma rede exclusiva para atividades de gerenciamento, reduzindo a exposição da interface administrativa ao tráfego de produção. Além disso, possibilita maior controle sobre o acesso ao equipamento, facilitando a aplicação de políticas de segurança e a segmentação da infraestrutura. Dessa forma, o FortiADC atende ao requisito de gerenciamento por interface dedicada, contribuindo para o isolamento do plano administrativo e para a segurança operacional da solução.

Link de Referência:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/271958/configuring-the-management-interface

Adicionalmente, por meio dessa interface de gerenciamento é possível disponibilizar acesso remoto aos recursos administrativos do equipamento por interface gráfica ou CLI incluindo SSH, além das funcionalidades de diagnóstico e manutenção documentadas pelo fabricante. A documentação oficial também comprova a possibilidade de execução de procedimentos de diagnóstico e de reinicialização remota do equipamento:

Rebooting, resetting, and shutting down the system

From the CLI console, enter the following command: execute reboot

From the CLI console, enter the following command: execute factoryreset

From the CLI console, enter the following commands: execute factoryreset2

From the CLI console, enter the following command: execute shutdown

Link de Referência:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/121802/rebooting-resetting-and-shutting-down-the-system

A documentação do fabricante também comprova que, através das funções administrativas do FortiADC, são disponibilizados recursos de diagnóstico, como ping, traceroute, packet capture, tcpdump e comandos de debug.

Link de Referência:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/74843/tools

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/239435/execute-commands

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/4902/diagnose-commands

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/813390/system-dump

Adicionalmente às características da interface física dedicada de gerenciamento, é importante destacar que o FortiADC dispõe de arquitetura de Virtual Domains (VDOMs), permitindo a segregação lógica das funções administrativas e de rede.

A documentação oficial do fabricante, no tópico “Virtual Domain (VDOM) and Administrative Domain (ADOM) overview”, estabelece que os VDOMs configurados no modo Independent Network funcionam de forma independente dentro de sua própria rede. Nessa modalidade, o administrador do VDOM possui acesso completo e irrestrito às configurações pertencentes ao seu próprio VDOM, sem que alterações realizadas nesse domínio afetem os demais VDOMs do sistema.

Essa característica permite que o FortiADC seja implementado com um VDOM específico e dedicado à administração/gerenciamento, possibilitando a separação lógica da rede de gerenciamento das redes utilizadas para o processamento de tráfego das aplicações.

Nesse cenário, o gerenciamento pode ser estruturado de maneira segregada, com:

- Interface física dedicada de Management para acesso administrativo;
- VDOM específico para gerenciamento, quando adotada essa arquitetura;

- Rede de gerenciamento independente das redes de produção;
- Controle administrativo próprio sobre o VDOM;
- Acesso remoto à administração do equipamento por protocolos como SSH/HTTPS;
- Execução de funções de configuração, manutenção e diagnóstico;
- Possibilidade de execução de procedimentos de reinicialização remota.

Links de Referência:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/442832

e) V. Licenciamento e infraestrutura de gestão (recurso, item III.6) Item 1.1.1 - composição da solução ofertada

A composição ofertada identifica dois FAD-2000G, cobertura FortiCare Premium, transceivers, FortiADC Manager e FortiAnalyzer-VM. A documentação de proposta e de diligência apresenta os respectivos part numbers e quantidades. A existência de componentes virtualizados não implica ausência de fornecimento: o próprio TJCE informou infraestrutura VMware disponível para sua instalação.

i. Item 1.1.20 - ausência de necessidade de licenciamento adicional

O Ordering Guide do fabricante classifica FAZ-VM-GB5 como licença perpétua de capacidade por ingestão de logs, combinável com outras licenças da mesma modalidade. Não se trata necessariamente de licença de upgrade isolada. A composição de duas unidades FAZ-VM-GB5, para 10 GB/dia, somada ao FortiCare de 60 meses correspondente ao tier de 1 a 11 GB/dia, coincide com a lógica de composição de nova implantação indicada no exemplo de pedido do fabricante.

A interpretação da Recorrente sobre a inexistência de licença-base evidencia desconhecimento técnico acerca do modelo de licenciamento da solução FortiAnalyzer-VM e demonstra falta de domínio sobre as regras de composição comercial

estabelecidas pelo fabricante. Tal equívoco compromete a credibilidade da argumentação apresentada, uma vez que a Recorrente fundamenta seu pedido de desclassificação em uma interpretação equivocada da documentação oficial, atribuindo à solução ofertada uma deficiência de licenciamento que não se sustenta diante das orientações do fabricante.

ii. Item 1.12.3 - hardware e software necessários à plataforma de gerenciamento

A alegação apresentada pela Recorrente quanto à suposta ausência de infraestrutura necessária à implantação da plataforma de gerenciamento desconsidera esclarecimento formal e vinculante emitido pelo próprio Tribunal de Justiça do Estado do Ceará, anteriormente à apresentação das propostas.

Inicialmente, cumpre destacar que o item 1.12.3 do Termo de Referência estabelece:

“Devem ser fornecidos todos os hardwares, softwares e licenças necessários para instalação e configuração da plataforma de gerenciamento.”

Entretanto, a interpretação desse dispositivo deve considerar os esclarecimentos oficialmente prestados pela Administração durante a fase externa do procedimento licitatório. Nesse sentido, o **Ofício nº 167/2026, referente ao Esclarecimento 01 do Pregão Eletrônico nº 032/2026, publicado em 28 de agosto de 2026**, tratou especificamente da possibilidade de fornecimento da plataforma de gerenciamento em formato virtual, utilizando a infraestrutura de virtualização do próprio TJCE.

Em resposta ao questionamento, a Administração confirmou expressamente que seria aceita a oferta da plataforma de gerenciamento em formato de appliance virtual, hospedada na infraestrutura de virtualização do Tribunal, dispensando o fornecimento de hardware físico dedicado para essa finalidade.

Adicionalmente, o TJCE estabeleceu que disponibilizaria uma máquina virtual com capacidade de até 16 vCPUs, 64 GB de memória RAM e 2 TB de armazenamento, esclarecendo que eventuais necessidades superiores ou incompatibilidades com a infraestrutura existente seriam de responsabilidade da CONTRATADA, sem ônus adicional à Administração.

Dessa forma, a alegação da Recorrente de que a ausência de servidores físicos ou licenças de hipervisor na composição comercial caracterizaria, automaticamente,

descumprimento do item 1.12.3 não encontra respaldo na interpretação oficialmente estabelecida pelo próprio órgão contratante.

A proposta apresentada pela Network Secure contempla soluções de gerenciamento e análise de logs em formato virtual, incluindo o FortiADC Central Manager e o FortiAnalyzer, modalidade de implantação expressamente admitida pelo TJCE no esclarecimento mencionado.

Diante do exposto, requer-se que seja afastada a alegação de obrigatoriedade de fornecimento de servidores físicos dedicados para a plataforma de gerenciamento, considerando-se o conteúdo do Ofício nº 167/2026 e a interpretação oficial do item 1.12.3 nele estabelecida.

f) Suporte a HTTP/2 e HTTP/3 (recurso, item III.7) Item 1.6.7 - alcance do suporte aos protocolos HTTP/2 e HTTP/3

> "1.6.7. Deve suportar todas as funcionalidades para comunicação HTTP/2 e HTTP/3."

Em relação ao questionamento apresentado, esclarecemos que a avaliação técnica da solução FortiADC 2000G foi fundamentada na versão de firmware 8.0.3, considerando a documentação oficial do fabricante aplicável a essa versão. A observação de que o suporte a HTTP/3 foi introduzido como funcionalidade experimental na versão 7.4.0 refere-se ao contexto inicial de disponibilização do protocolo na plataforma. Assim, a análise técnica deve considerar os recursos documentados para a versão utilizada na comprovação, evitando que a avaliação se restrinja ao registro histórico de introdução da funcionalidade.

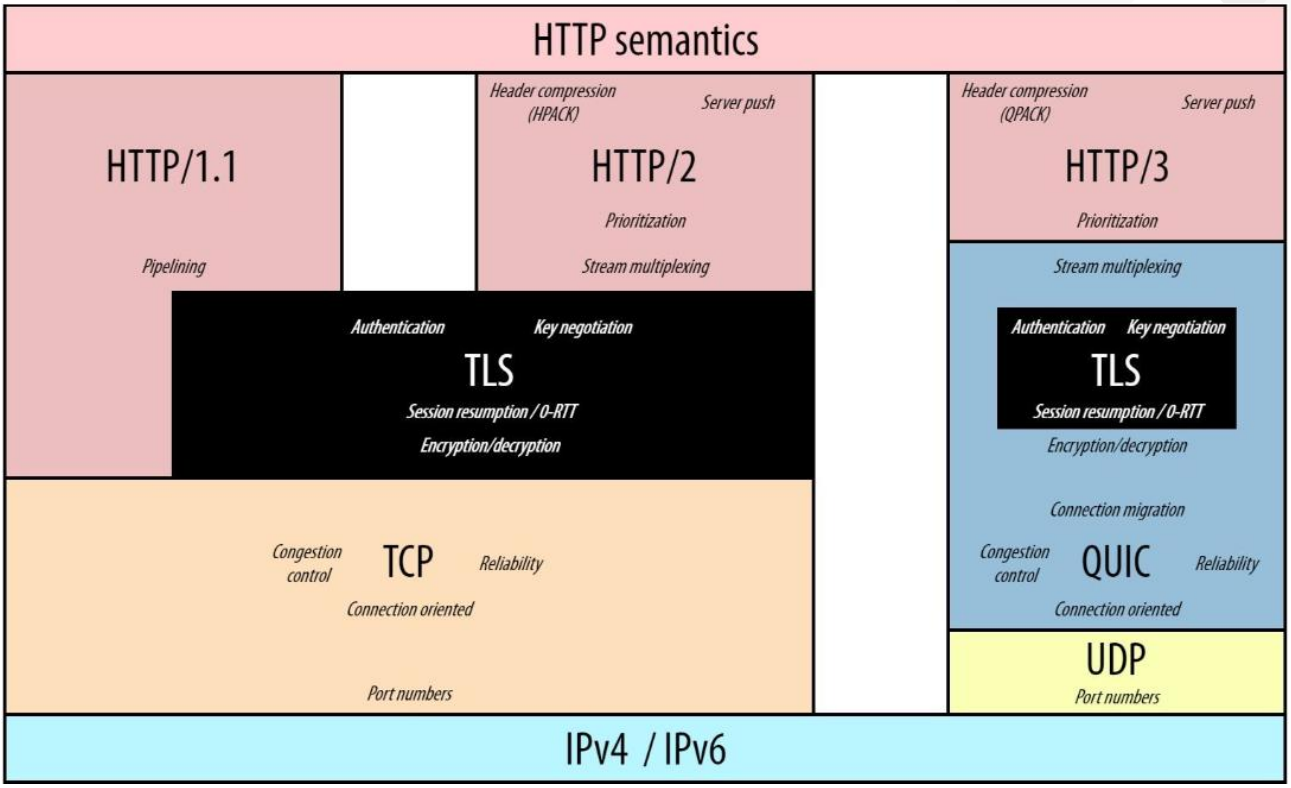
Na versão 8.0.3, a documentação oficial contempla um perfil específico para HTTP/3, integrado aos perfis HTTPS e aos servidores virtuais de camada 7, permitindo o recebimento de conexões HTTP/3 dos clientes por meio do protocolo QUIC sobre UDP. A implementação disponibiliza parâmetros configuráveis para o gerenciamento das conexões, incluindo algoritmos de controle de congestionamento QUIC — Cubic e New Reno —, quantidade máxima de streams simultâneos, tempo limite de inatividade, buffers de transmissão e modos de multiplexação das conexões no backend.

A documentação também descreve métodos de balanceamento de carga compatíveis com HTTP/3, mecanismos de persistência de sessão e suporte a assinaturas de ataques web, observadas as condições específicas estabelecidas pelo fabricante para cada funcionalidade.

Referência oficial:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/397943/configuring-http3-profiles
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/561757/application-resources

Para HTTP/2, a documentação oficial contempla recursos de enquadramento binário, compressão de cabeçalhos HPACK e multiplexação de streams, permitindo o processamento de múltiplas requisições e respostas em uma única conexão TCP.

Referência oficial:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/561757/application-resources
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/588548/configuring-http2-profiles



Arquitetura e evolução dos protocolos HTTP/2 e HTTP/3

Essa representação complementa a análise das funcionalidades documentadas para o FortiADC 2000G, contextualizando os mecanismos de comunicação associados aos protocolos previstos no requisito 1.6.7. Extraída da documentação técnica de referência, ilustra a evolução da pilha de comunicação HTTP, destacando os mecanismos de multiplexação de streams, compressão de cabeçalhos e segurança criptográfica. Evidencia-se que o HTTP/3 utiliza o protocolo QUIC sobre UDP, diferentemente do HTTP/2, que utiliza TCP, mantendo os conceitos fundamentais da semântica HTTP e incorporando mecanismos de transporte projetados para melhorar o desempenho e a eficiência das conexões.

Dessa forma, a solução apresenta recursos específicos para o processamento e balanceamento de tráfego HTTP/2 e HTTP/3, devendo a conformidade ser avaliada com base nas funcionalidades efetivamente exigidas pelo instrumento convocatório e na documentação correspondente à versão utilizada na comprovação técnica.
Ressalta-se que o edital deve ser interpretado conforme seu objeto e seus requisitos funcionais, sem presumir exigências adicionais que não estejam expressamente

previstas. Assim, solicita-se que o questionamento seja apreciado considerando a documentação oficial da versão 8.0.3 e os recursos efetivamente disponibilizados para a comunicação HTTP/2 e HTTP/3.

g) Métodos de balanceamento (recurso, item III.8) Item 1.6.19.2.2 - Least Connection com peso administrativo, Item 1.6.19.2.4 - menor número de requisições em camada 7 e Item 1.6.19.2.5 - Least Connection por serviço/porta com peso

Em relação aos questionamentos apresentados pela empresa L8 Group acerca dos subitens 1.6.19.2.2, 1.6.19.2.4 e 1.6.19.2.5, esclarecemos que a argumentação apresentada pela recorrente não considera integralmente a documentação oficial do FortiADC 2000G, especialmente a compatibilidade dos métodos de balanceamento com os diferentes perfis de aplicação e as possibilidades de configuração dos parâmetros dos servidores integrantes dos pools.

A análise deve considerar as funcionalidades efetivamente documentadas pela fabricante, e não apenas a nomenclatura dos métodos apresentada em uma lista geral.

1. Item 1.6.19.2.2 – Menor número de conexões com Peso Administrativo (Weight)

A documentação oficial do FortiADC 8.0.3 apresenta expressamente o método LB_METHOD_LEAST_CONNECTION, descrito como responsável por selecionar o servidor com o menor número de conexões.

Referência oficial:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/201314/configuring-load-balancing-lb-methods

Adicionalmente, a documentação de configuração dos pools de servidores demonstra a disponibilidade do parâmetro Weight, que permite atribuir diferentes níveis de preferência aos servidores membros.

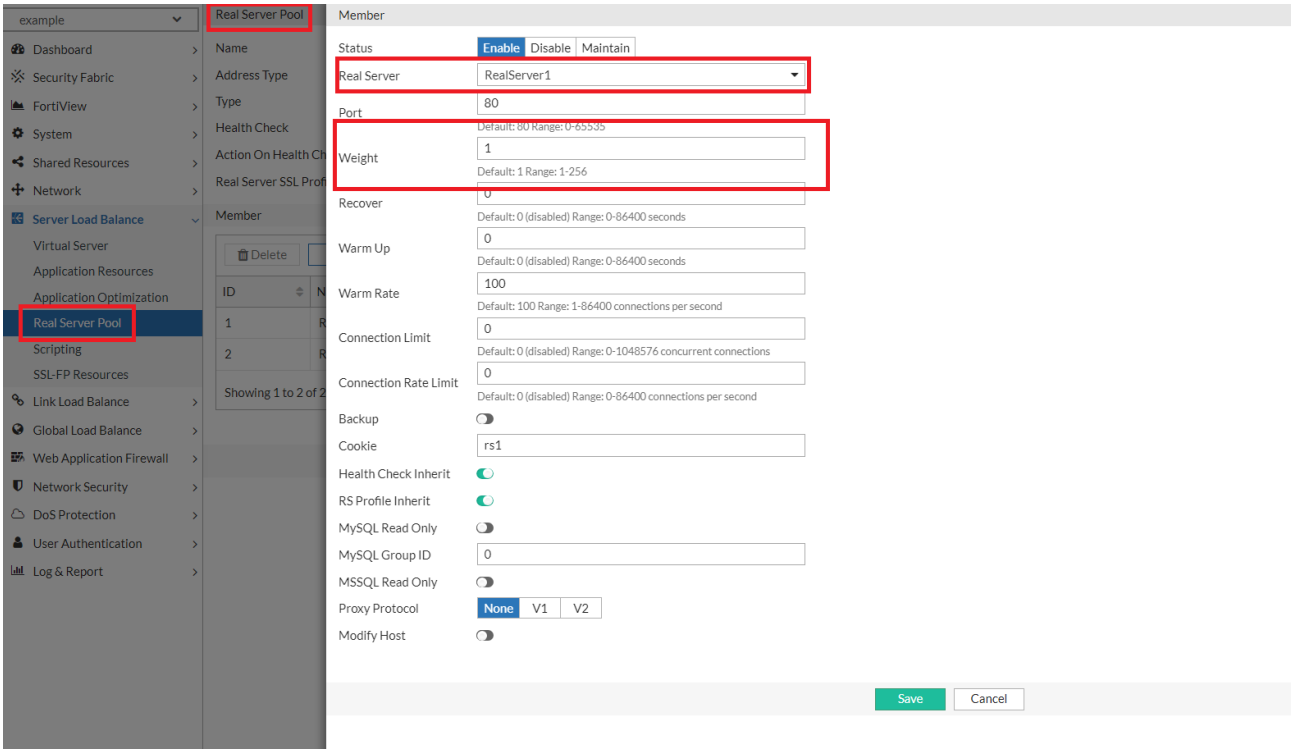
Referência oficial:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/740387/using-real-server-pools

A documentação do fabricante esclarece que o peso é considerado pelos métodos de balanceamento, embora sua influência varie conforme o algoritmo selecionado.

Weight

Assigns relative preference among members—higher values are more preferred and are assigned connections more frequently. The default is 1. The valid range is 1 to 256. **All load balancing methods consider weight. Servers are dispatched requests proportional to their weight, relative to the sum of all weights.**



Portanto, a solução disponibiliza o método de menor número de conexões e permite configurar o peso administrativo dos servidores, devendo ser observado o comportamento específico documentado para cada algoritmo.

i. Item 1.6.19.2.4 – Menor número de requisições em camada 7 (L7)

A recorrente afirma que o FortiADC não disponibiliza o método de menor número de requisições em camada 7, fundamentando sua alegação na ausência de um algoritmo denominado especificamente Least Requests na relação geral de métodos. Entretanto, a documentação oficial Configuring Application Profiles apresenta a matriz de compatibilidade entre os perfis de aplicação e seus respectivos métodos de balanceamento, identificando expressamente Layer 7: Least Connections para os perfis L7 TCP e L7 UDP, além de perfis como HTTP e FTP.

Referência oficial:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/559628/configuring-application-profiles#application-profile-types

Figura 1 – Métodos de balanceamento disponíveis para os perfis L7 TCP e L7 UDP.

Application Profile Usage

Profile	Usage	VS Type	LB Methods	Persistence
L7 TCP	Use for generic TCP-based applications that do not require application-specific parsing. Supports both standard Layer 3 routed deployments and transparent proxy deployments (Layer 2 or Layer 3). TCP optimization parameters (receive window, send buffer, window clamp, MSS, congestion control) can be tuned per profile for client and server sides.	Layer 7, Layer 2 (Transparent Proxy)	Layer 7: Round Robin, Least Connections Layer 2: Round Robin, Least Connection	Layer 7: Source Address, Source Address Hash Layer 2: Source Address, Source Address Hash
L7 UDP	Use with UDP servers.	Layer 7	Layer 7: Round Robin, Least Connections	Source Address, Source Address Hash
HTTP	Use for standard, unsecured web server traffic.	Layer 7	Round Robin, Least Connection, URI Hash, Full URI Hash, Host Hash, Host Domain Hash, Dynamic Load	Source Address, Source Address Hash, Source Address-Port Hash, HTTP Header Hash, HTTP Request Hash, Cookie Hash, Persistent Cookie, Insert Cookie, Embedded Cookie, Rewrite Cookie, Passive Cookie
		Layer 2	Round Robin, Least Connection, URI Hash, Full URI Hash, Host Hash, Host Domain Hash, Dynamic Load, Destination IP Hash	
FTP	Use with FTP servers.	Layer 7	Round Robin, Least Connection	Source Address, Source Address Hash

A evidência demonstra que o método Least Connections está disponível em camada 7, contrariando a afirmação genérica de que a solução não oferece esse método nessa camada.

Dessa forma, a análise apresentada pela L8 Group é incompleta ao desconsiderar a matriz específica de compatibilidade dos perfis de aplicação e considerar exclusivamente a nomenclatura dos algoritmos na lista geral. Cabe apenas distinguir que a documentação comprova Least Connections em camada 7, baseado no número de conexões.

ii. Item 1.6.19.2.5 – Menor número de conexões por serviço TCP ou UDP com Peso Administrativo (Weight)

A documentação oficial do FortiADC apresenta perfis de aplicação para os protocolos TCP e UDP e relaciona os métodos de balanceamento compatíveis com cada perfil.

Referência oficial:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/559628/configuring-application-profiles#application-profile-types

Complementarmente, a documentação Load Balancing for Layer 4 Virtual Servers demonstra o procedimento de criação de pools de servidores reais e a possibilidade de atribuir pesos aos servidores membros.

Referência oficial:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/19595/load-balancing-for-layer-4-virtual-servers#step-2-create-the-real-server-pool

A fabricante informa expressamente que o peso do servidor real pode ser configurado no pool, permitindo estabelecer preferências entre os membros. Assim, a solução contempla a configuração do parâmetro Weight e os métodos de balanceamento compatíveis com os perfis de aplicação documentados.

Ressalta-se que, no método Least Connection, o peso atua como critério de desempate, conforme a documentação da fabricante. Essa característica deve ser

considerada na avaliação do requisito, sem confundir a disponibilidade do parâmetro com uma ponderação proporcional independente do algoritmo.

Diante do exposto, a documentação oficial da Fortinet comprova que o FortiADC 2000G disponibiliza o método Least Connections, contempla sua utilização em perfis de camada 7, incluindo L7 TCP e L7 UDP, e permite configurar o parâmetro Weight nos membros dos pools de servidores.

A argumentação da L8 Group não considera integralmente essas possibilidades de configuração e a matriz de compatibilidade dos perfis de aplicação. Por isso, a conclusão de inexistência dos recursos não pode ser sustentada apenas pela ausência de determinada nomenclatura na relação geral de algoritmos.

Solicita-se, portanto, que a avaliação técnica considere integralmente a documentação oficial da fabricante e as funcionalidades efetivamente disponibilizadas pela solução, observando a correspondência entre cada requisito do edital e o comportamento técnico documentado.

h) Motor de políticas de camada 7 (recurso, item III.9) Item 1.7.6 - atributos avaliados no roteamento de conteúdo, Item 1.7.7 - AND, OR, NOT, agrupamento e precedência e Item 1.7.10 - igualdade, prefixo, sufixo e normalização

Referente aos itens:

> “1.7.7. Definição de políticas com operadores lógicos (AND, OR, NOT), incluindo agrupamento, aninhamento (nested) e controle de precedência.”
>
> “1.7.9. Mecanismo estruturado de políticas, não sendo aceito que o atendimento aos requisitos de lógica condicional complexa dependa exclusivamente do uso de expressões regulares (regex) ou da criação de múltiplas regras independentes para representar um mesmo comportamento funcional;”
>
> “1.7.10. Suporte a múltiplos modos de comparação de URL e path (igualdade, prefixo, sufixo e equivalência após normalização).”

O FortiADC disponibiliza mecanismos de correspondência de condições para o direcionamento de conteúdo (Content Routing), permitindo definir critérios de análise das requisições e combinar condições para determinar a aplicação de uma política.

Conforme descrito na documentação oficial do fabricante, na seção Configuring Content Routes:

"*Layer 7 content route rules are based on literal **or** regular expression matches*".

Em tradução livre: "As regras de direcionamento de conteúdo da Camada 7 são baseadas em correspondências literais **ou** em expressões regulares."

Esse mecanismo permite utilizar expressões regulares para definir critérios de correspondência sobre informações das requisições HTTP, incluindo cabeçalhos e URLs, possibilitando a construção de condições de direcionamento conforme as características do tráfego.

Conforme demonstrado na captura de tela da interface administrativa do FortiADC abaixo, a funcionalidade "***Match Condition"*** permite configurar múltiplas condições em uma mesma regra. No exemplo apresentado, são utilizados os seguintes operadores lógicos:

a) Operador AND (E)

As condições cadastradas em linhas distintas são combinadas de forma que todas devem ser satisfeitas para que a regra corresponda à requisição. Dessa forma, o atendimento simultâneo dos critérios de endereço IP de origem, cabeçalho HTTP Host e URL determina a correspondência da regra.

b) Operador OR (OU)

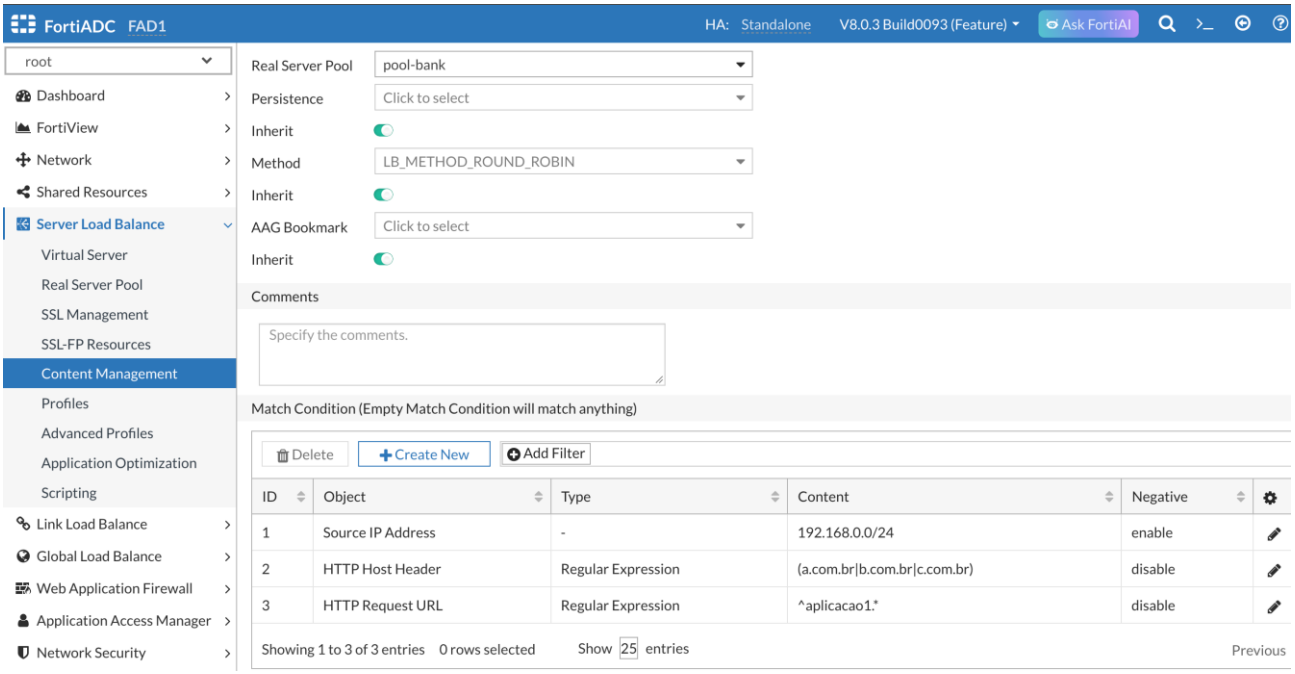
No campo HTTP Host Header, é utilizada a expressão regular (a.com.br | b.com.br | c.com.br). Nessa expressão, o caractere "|" representa uma alternativa lógica, permitindo que o cabeçalho Host corresponda a qualquer um dos três domínios especificados. Os parênteses agrupam as alternativas em uma única expressão regular.

c) Operador NOT (NÃO)

Na condição Source IP Address, o campo “Negative” está configurado como “enable”, indicando a negação da condição correspondente. Assim, a regra considera como válida essa condição quando o endereço IP de origem não pertence à rede 192.168.0.0/24.

d) Agrupamento e precedência das expressões

O exemplo demonstra o agrupamento de alternativas por meio dos parênteses da expressão regular (PCRE) aplicada ao cabeçalho HTTP Host. A expressão permite tratar os três domínios como alternativas de uma mesma condição, enquanto as demais condições são combinadas por AND.



A utilização de expressões regulares possibilita organizar alternativas dentro de uma condição. A comprovação de combinações aninhadas mais complexas e de regras específicas de precedência entre operadores deve considerar a sintaxe efetivamente suportada pelo mecanismo de correspondência e sua documentação técnica.

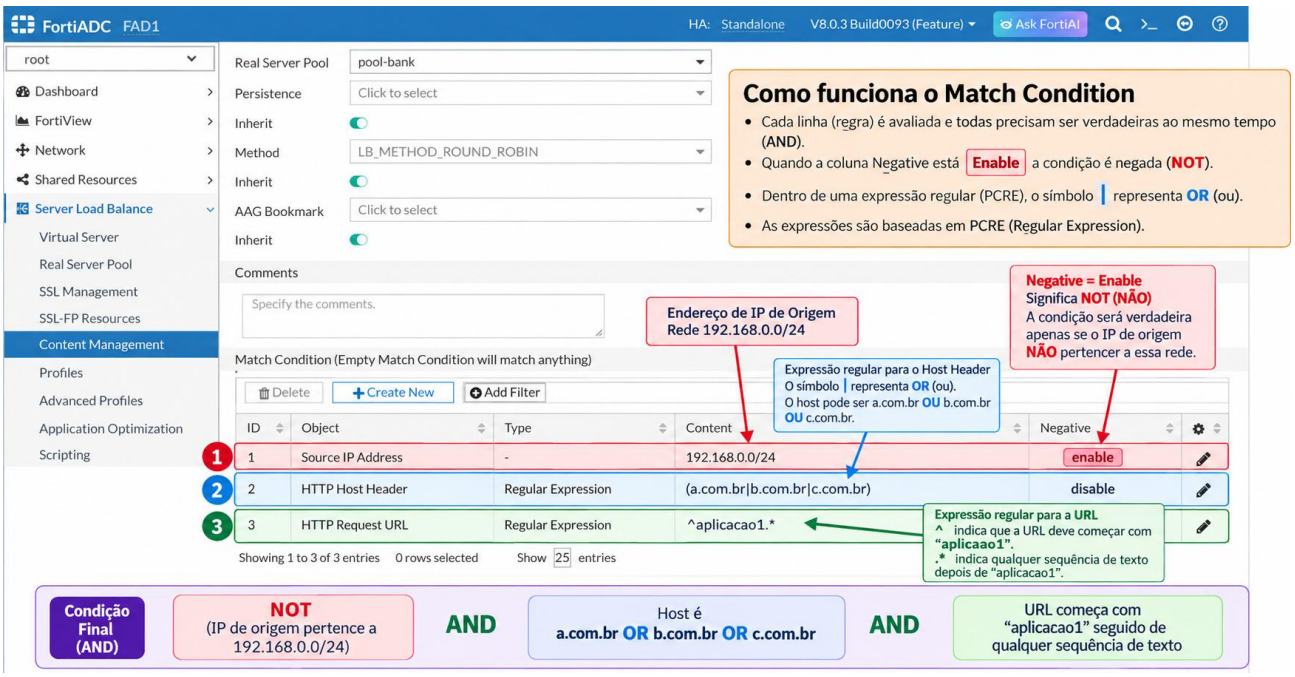
Portanto, a captura de tela evidencia a utilização dos operadores AND, OR e NOT na definição das condições de correspondência, bem como o agrupamento de alternativas em uma expressão regular (PCRE).

Conforme exemplo abaixo, colocamos uma expressão regular como condição para match onde cada linha é avaliada e todas precisam ser verdadeiras (**AND**):

Linha (ID) 1: "Endereço de IP de Origem" **NOT** (NÃO) por de ser da rede "192.168.0.0/24" configurado na coluna Negative "**Enable**"

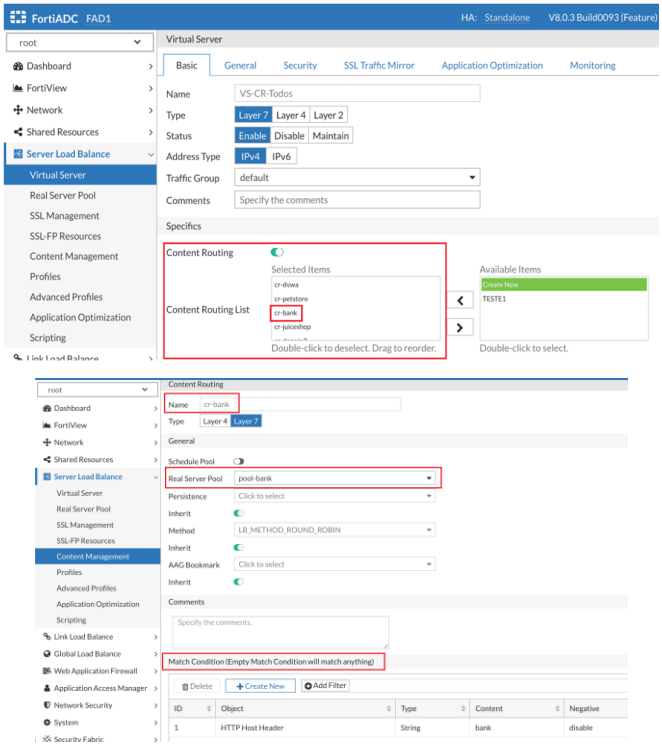
Linha (ID) 2: **AND** (E) o host pode ser "a.com.br" **OR** "b.com.br" **OR** "c.com.br" representada pela "|"

Linha (ID) 3: **AND** (E) a URL precisa começar (^) com "aplicação1." seguida de qualquer sequência de texto (*):



As capturas de tela a seguir demonstram a aplicação da regra de Content Routing previamente apresentada, associada à configuração de um Virtual Server no FortiADC. Essa associação permite que o equipamento utilize os critérios definidos na regra para avaliar as requisições recebidas e determinar o direcionamento do tráfego conforme as condições configuradas.

Dessa forma, evidencia-se que as condições de correspondência não se limitam à sua definição isolada, podendo ser vinculadas a um Virtual Server para aplicação efetiva da lógica de direcionamento de conteúdo. A regra reúne os critérios de endereço IP de origem, cabeçalho HTTP Host e URL da requisição, combinando-os conforme os operadores lógicos configurados, de modo que o direcionamento ocorra quando as condições estabelecidas forem atendidas.



As evidências acima comprovam a disponibilidade de diferentes mecanismos de correspondência, que podem ser selecionados conforme a necessidade da política, sem depender exclusivamente de expressões regulares. Esses mecanismos estão integrados à estrutura de Content Routing, permitindo definir condições, combiná-las com outros critérios e associá-las ao respectivo grupo de servidores de destino.

Conforme demonstrado na captura de tela apresentada anteriormente, a condição HTTP Request URL utiliza o padrão ^aplicacao1.*, que identifica requisições cuja URL começa com aplicacao1. Nesse exemplo, o caractere ^ indica o início da sequência avaliada, enquanto .* representa qualquer sequência de caracteres subsequente, demonstrando a aplicação de um critério de correspondência por prefixo.

Adicionalmente, os mecanismos de correspondência disponíveis permitem estruturar critérios para diferentes necessidades de comparação, conforme ilustrado pelos exemplos abaixo:

Igualdade: utilização de correspondência literal (String) para um caminho específico, como /resource/index.html. Quando necessário delimitar uma correspondência exata por expressão regular, pode-se utilizar ^/resource/index\.html$.

Prefixo: utilização de um padrão que identifica caminhos iniciados por determinado texto, como **^/aplicacao1.**

Sufixo: utilização de um padrão que identifica caminhos terminados em determinado texto, como **\.pdf$.**

Os exemplos demonstram possibilidades de configuração dos critérios de correspondência e não implicam que a solução dependa exclusivamente de expressões regulares. O FortiADC oferece correspondência literal e por padrões, permitindo estruturar regras de direcionamento de acordo com o comportamento funcional desejado.

O FortiADC dispõe de mecanismos nativos de Content Routing e recursos programáveis de HTTP Scripting, que permitem definir critérios de correspondência, tratar informações das requisições HTTP e implementar lógica complementar de direcionamento de tráfego.

A documentação oficial do fabricante demonstra que o Content Routing permite selecionar grupos de servidores de destino com base em condições relativas ao cabeçalho HTTP Host, URL da requisição, Referer, SNI e endereço IP de origem. Adicionalmente, a documentação de HTTP Scripting apresenta recursos específicos para analisar URLs, obter e modificar caminhos HTTP e comparar URLs por meio da função url_compare(url1, url2).

Esses recursos complementam as condições de correspondência do Content Routing, possibilitando implementar critérios de comparação e tratamento de URLs conforme a necessidade funcional, sem limitar a solução exclusivamente à utilização de expressões regulares.

Como referência, o fabricante disponibiliza exemplos de scripts para seleção de Content Routes por correspondência de URI, além de documentar as funções url_parser(), url_compare(), HTTP:path_get() e HTTP:path_set().

Link de referência:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/561482/configuring-content-routes

https://docs.fortinet.com/document/fortiadc/8.0.3/script-reference-guide/127924/http-scripting-examples

https://docs.fortinet.com/document/fortiadc/8.0.3/script-reference-guide/397453

i) Pontos adicionais destacados no recurso (recurso, item III.10) Item 1.4.15 - modo passivo / sniffer

Em relação à alegação apresentada pela empresa L8 Group quanto ao suposto não atendimento ao item 1.4.15 do instrumento convocatório, cabe esclarecer que a análise da conformidade técnica deve considerar a redação integral do requisito e as funcionalidades documentadas pelo fabricante para a solução ofertada, FortiADC 2000G, com referência à versão 8.0.3.

O edital estabelece:

> "1.4.15. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), passivo, ou 'Sniffer' (Offline) e inline transparente (Bridge)."

Inicialmente, observa-se que o requisito apresenta modalidades alternativas de implementação, mediante o emprego da conjunção "ou". Portanto, a interpretação do item deve respeitar a possibilidade de atendimento por uma das modalidades previstas, sem presumir a obrigatoriedade de implementação simultânea de todas elas, salvo disposição expressa em contrário no instrumento convocatório.

A solução FortiADC 2000G possui documentação oficial que descreve a implementação em modo Proxy Reverso, conforme as seguintes referências do fabricante:

Full NAT mode (Full Reverse Proxy):

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/916462/fullnat-mode-full-reverse-proxy

Layer 7 deployment mode – Reverse Proxy deployment:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/95582/layer-7-deployment-mode-reverse-proxy-deployment

Essas referências documentam a modalidade de implantação em que o FortiADC atua como intermediário nas conexões entre clientes e servidores de aplicação, realizando o processamento das conexões conforme a configuração estabelecida. Dessa forma, a documentação apresentada comprova o suporte à modalidade Proxy Reverso, expressamente contemplada no requisito editalício.

Além do modo Proxy Reverso, a documentação oficial do fabricante contempla o modo transparente e a implantação em camada 2, inline transparente, ampliando as evidências técnicas relativas às modalidades previstas no edital.

São apresentados os seguintes documentos:

Transparent mode: https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/592141/transparent-mode

Layer 2 deployment mode – Inline transparent deployment: https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/728687/layer-2-deployment-mode-inline-transparent-deployment

Essas referências são pertinentes à comprovação do modo transparente e da implantação inline transparente, respectivamente. Em especial, o documento Layer 2 deployment mode – Inline transparent deployment constitui referência específica para a modalidade de implantação inline transparente (Bridge) mencionada no edital.

Assim, a análise técnica não deve se limitar aos documentos inicialmente apresentados, uma vez que existem referências oficiais adicionais do fabricante diretamente relacionadas às modalidades de implementação questionadas. Para complementar a documentação apresentada, são incluídas referências oficiais relativas às funcionalidades de replicação e espelhamento de tráfego disponíveis no FortiADC.

Using Clone Pools:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/159364/using-clone-pools

SSL Traffic Mirroring:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/609686/ssl-traffic-mirroring

O documento Using Clone Pools trata do recurso de clonagem de tráfego para destinos configurados, enquanto o documento SSL Traffic Mirroring apresenta a funcionalidade específica de espelhamento de tráfego SSL.

A interface de administração apresentada como evidência complementar demonstra a opção de habilitação do SSL Traffic Mirroring e a seleção dos destinos disponíveis para recebimento do tráfego espelhado. Esses recursos evidenciam capacidades adicionais de replicação e disponibilização de tráfego para outros destinos.A apresentação desses documentos tem, portanto, caráter complementar, não sendo necessária a equiparação conceitual entre espelhamento de tráfego e operação passiva para fundamentar o atendimento às modalidades documentadas de Proxy Reverso e implantação transparente.

A alegação apresentada pela empresa L8 Group de que não haveria documentação comprobatória suficiente não considera o conjunto de referências oficiais disponibilizadas pelo fabricante para a versão 8.0.3.

A documentação apresentada contempla:

Proxy Reverso, por meio dos documentos Full NAT mode (Full Reverse Proxy) e Reverse Proxy deployment;

Modo transparente, por meio do documento Transparent mode;

Implantação inline transparente (Bridge), por meio do documento Layer 2 deployment mode – Inline transparent deployment;

Recursos complementares de espelhamento de tráfego, por meio dos documentos Using Clone Pools e SSL Traffic Mirroring.

Portanto, há documentação oficial específica para sustentar a análise de diferentes modalidades previstas no requisito, não sendo adequado desconsiderar essas evidências na avaliação da conformidade técnica.

Adicionalmente, a redação do item 1.4.15 deve ser interpretada em sua integralidade, respeitando o caráter alternativo das modalidades introduzidas pela conjunção “ou”. Não cabe transformar essa previsão em uma obrigação de atendimento cumulativo a todas as modalidades sem fundamento expresso no instrumento convocatório.

a) Item 1.6.29 - cabeçalhos HTTP de pelo menos 128 KB

Referente ao item:

> *“1.6.29. A solução deve suportar processamento de cabeçalhos HTTP com tamanho mínimo de 128 KB por requisição, sem degradação de desempenho ou limitação funcional na aplicação de políticas de camada 7.”*

O FortiADC disponibiliza, em seu perfil de aplicação HTTP/HTTPS, os parâmetros Tune Buffer Size e Max HTTP Headers, destinados justamente ao ajuste da capacidade de processamento de requisições HTTP/HTTPS. A documentação oficial define o Tune Buffer Size como o tamanho do buffer de conexão do Virtual Server e o Max HTTP Headers como a quantidade máxima de headers que o Virtual Server pode processar por requisição ou resposta.

Conforme demonstrado na interface de configuração da solução:

Tune Buffer Size: faixa configurável de 128 a 1.048.576 bytes;

Max HTTP Headers: faixa configurável de 10 a 10.000 headers.

Para o requisito de **128 KB**, temos:

128 KB = 131.072 bytes

A solução permite configurar o Tune Buffer Size em até 1.048.576 bytes.

Portanto:

1.048.576 ÷ 131.072 = 8

Ou seja, a capacidade configurável de **buffer é 8 vezes superior ao mínimo de 128 KB exigido.**

Além disso, o parâmetro Max HTTP Headers permite até 10.000 headers por requisição/resposta, eliminando uma limitação relacionada à quantidade de cabeçalhos que poderia impedir o atendimento do requisito. A documentação confirma expressamente essa função do parâmetro.

Como exemplo simples, mesmo considerando apenas 30 bytes por header:

10.000 × 30 = 300.000 bytes ≈ 293 KB

Esse valor também é superior aos 128 KB requeridos.

Portanto, considerando conjuntamente os parâmetros Max HTTP Headers e Tune Buffer Size, o FortiADC possui capacidade configurável para atender integralmente ao requisito de processamento de HTTP/HTTPS Headers de 128 KB, não havendo limitação funcional que impeça o atendimento do requisito.

"*Max HTTP Headers, Adjust the max header number that HTTP/HTTPS VS can process for every request or response*"

Links de Referência:

https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/559628/configuring-application-profiles#HTTP

b) Item 1.6.19.4.1 - métricas customizadas para balanceamento

> "1.6.19.4.1. O equipamento deverá ser capaz de encaminhar requisições com base em métricas de carga customizadas (como uso de CPU, memória ou latência de banco de dados), obtidas através de monitores de saúde externos e integrados à solução."

Conforme a documentação do fabricante, o método "**Dynamic Load**" "**LB_METHOD_DYNAMIC_LOAD**" seleciona os servidores com base nos pesos

atribuídos a cada membro do pool, considerando informações obtidas por meio de verificações de saúde via SNMP.

A documentação especifica que o mecanismo considera métricas de utilização de CPU, memória e disco, permitindo avaliar a carga dos servidores de destino e ajustar a distribuição das requisições conforme os pesos atribuídos. Os limites e parâmetros de avaliação podem ser definidos de acordo com os recursos de configuração disponibilizados pela solução.

Portanto, há comprovação documental de que o FortiADC implementa balanceamento dinâmico orientado por métricas de carga dos servidores, incluindo expressamente o uso de CPU e memória, que são duas das alternativas mencionadas no requisito editalício.

"*Dynamic load-balancing relies on the* ***status of SNMP health check to calculate the load on each real server****. The* ***health check covers a real server's CPU, memory, and disk usage****. When a real server has exceeded its health check thresholds, it will be marked as "down".*"

Link de Referência:
https://docs.fortinet.com/document/fortiadc/8.0.3/administration-guide/201314/configuring-load-balancing-lb-methods

A redação do requisito apresenta exemplos de métricas de carga, utilizando a expressão "como" e o conectivo "ou" para relacionar o uso de CPU, o uso de memória e a latência de banco de dados. Sob a perspectiva da interpretação técnica do requisito, tais expressões indicam alternativas de métricas, não estabelecendo expressamente a obrigatoriedade de suporte simultâneo a todas elas. Assim, a comprovação do atendimento deve considerar a capacidade efetivamente exigida pelo edital, sem transformar exemplos alternativos em obrigações cumulativas não previstas na especificação. Diante do exposto, verifica-se que o FortiADC 2000G possui funcionalidade de balanceamento dinâmico baseada em métricas de carga dos servidores, com suporte documental para utilização de CPU e memória, conforme demonstrado no Administration Guide oficial da Fortinet, versão 8.0.3.

Considerando que o requisito apresenta tais métricas como alternativas, e não como condições cumulativas, a ausência de demonstração específica de encaminhamento baseado em latência de banco de dados não é suficiente para caracterizar o descumprimento do item. Assim, sob o aspecto técnico e documental, requer-se que o argumento apresentado pela empresa L8 Group seja rejeitado quanto à alegação de ausência de suporte ao balanceamento baseado em métricas de carga, reconhecendo-se o atendimento do FortiADC 2000G ao requisito por meio das métricas de CPU e memória devidamente documentadas.

c) Item 2.2.6 - Best Practice Assessment mensal e Item 2.2.7 - reuniões técnicas conduzidas por profissional do fabricante

A alegação apresentada pela Recorrente quanto ao suposto não atendimento dos itens 2.2.6 e 2.2.7 demonstra uma interpretação equivocada da composição dos serviços ofertados pela Network Secure, ao confundir o suporte técnico continuado prestado pela CONTRATADA, o contrato de suporte do fabricante (FortiCare) e os serviços profissionais especializados da Fortinet.

Inicialmente, cumpre esclarecer que o item 2 do Termo de Referência estabelece a prestação de suporte técnico continuado pelo período de 57 meses, contemplando as atividades operacionais, preventivas e corretivas previstas no instrumento convocatório. Por sua vez, a proposta apresentada pela Network Secure contempla o fornecimento de contratos FortiCare Premium pelo período de 60 meses, conforme demonstrado pelos respectivos SKUs de suporte do fabricante, associado aos appliances FortiADC 2000G.

Dessa forma, os 57 meses correspondem ao período de prestação do serviço continuado contratado pelo TJCE, enquanto os 60 meses representam a vigência do suporte técnico do fabricante para os produtos ofertados.

Tratam-se, portanto, de obrigações distintas e complementares, não sendo tecnicamente correto utilizar o quantitativo de diárias de serviços profissionais como referência para determinar a vigência ou a abrangência do suporte técnico da solução. Adicionalmente, o SKU FP-10-PS001-801-01-01, identificado como *Per Day Charge for Remote Resource Service*, corresponde à contratação de serviços profissionais

especializados da Fortinet, não constituindo licença de suporte técnico, extensão de garantia ou substituto dos contratos FortiCare Premium.

Sua inclusão na composição da proposta está relacionada à disponibilização de recursos técnicos especializados do fabricante para acompanhamento, avaliação e otimização das configurações da solução, em complemento às atividades de suporte continuado assumidas pela Network Secure.

Quanto ao quantitativo de serviços profissionais, a proposta contempla cinco diárias de atendimento remoto. Considerando a jornada de referência de oito horas por diária, esse quantitativo corresponde a 40 horas de atividades especializadas, que podem ser organizadas em sessões técnicas de acordo com o planejamento das atividades e as necessidades identificadas durante a avaliação do ambiente.

Cabe destacar que o item 2.2.7 estabelece a realização de duas reuniões técnicas semanais, conduzidas por profissional do fabricante, até que o Best Practice Assessment alcance aproximadamente 95% de conformidade ou até a ocorrência da condição alternativa prevista no Termo de Referência.

O dispositivo não estabelece duração fixa para cada reunião, tampouco determina que as diárias contratadas devam ser consumidas integralmente em períodos consecutivos. Assim, a conclusão apresentada pela Recorrente, de que cinco diárias seriam necessariamente insuficientes para três semanas de reuniões, baseia-se em uma premissa de duração e distribuição das atividades que não consta do instrumento convocatório.

Importante destacar, ainda, que a quantidade de horas contratadas representa o esforço técnico inicialmente previsto para as atividades especializadas do fabricante, não afastando a responsabilidade da Network Secure de assegurar o cumprimento das obrigações contratuais efetivamente assumidas.

No que se refere ao item 2.2.6, a realização mensal do Best Practice Assessment constitui atividade integrante do serviço continuado de suporte técnico da CONTRATADA, devendo utilizar como referência as recomendações e diretrizes oficiais da Fortinet para o FortiADC.

A documentação do fabricante disponibiliza orientações de melhores práticas para segurança, desempenho, alta disponibilidade, manutenção e configuração da plataforma, que podem subsidiar a metodologia de avaliação periódica do ambiente.

Dessa forma, não se deve confundir a execução mensal das avaliações estruturadas, cuja responsabilidade integra o serviço continuado, com a contratação pontual de serviços profissionais do fabricante para acompanhamento técnico especializado e evolução das configurações.

A proposta apresentada pela Network Secure contempla, portanto, componentes com finalidades distintas: contratos FortiCare Premium de 60 meses, prestação de suporte técnico continuado pelo período de 57 meses e contratação específica de serviços profissionais especializados do fabricante.

Diante do exposto, requer-se que seja afastada a interpretação da Recorrente segundo a qual as cinco diárias de serviços profissionais representariam a totalidade da cobertura de suporte técnico prevista na proposta.

d) Qualificação técnico-operacional (recurso, item IV) Item 15.3.3.1 - experiência de complexidade tecnológica pertinente

Não procede a alegação da Recorrente quanto à ausência de comprovação de aptidão técnico-operacional da Network Secure para execução de serviços de complexidade tecnológica pertinente ao objeto da presente contratação.

Cumpre esclarecer que os aspectos relacionados à experiência técnica da Network Secure já foram objeto de análise pelo TJCE durante a segunda diligência, formalizada por meio do Ofício nº 207/2026, especificamente nos apontamentos H-1, H-2 e H-3, ocasião em que foram apresentados esclarecimentos técnicos e documentação complementar ao Atestado de Capacidade Técnica emitido pela Empreendimentos Pague Menos S/A.

A documentação apresentada demonstra a experiência efetiva da Network Secure no fornecimento, instalação, configuração e implementação de soluções Application Delivery Controller (ADC), incluindo a implantação de 02 (duas) unidades FortiADC 700D em arquitetura de Alta Disponibilidade (HA), no modo Ativo-Passivo, integradas à infraestrutura de rede do cliente.

Ressalta-se que a implementação ocorreu em ambiente corporativo de abrangência nacional, destinado a aproximadamente 10.000 usuários distribuídos em 26 Estados brasileiros, demonstrando a relevância operacional, o porte e a complexidade da infraestrutura atendida. Adicionalmente, foi devidamente encaminhada ao TJCE

declaração complementar emitida pela Empreendimentos Pague Menos S/A, assinada por seu representante legal, contendo informações sobre a solução e as funcionalidades efetivamente implementadas, complementando o atestado originalmente apresentado e permitindo à Administração avaliar a experiência técnica comprovada.

Importante destacar que a experiência demonstrada não se restringe à comercialização ou ao fornecimento de equipamentos, abrangendo atividades técnicas relacionadas à implementação e configuração de uma solução dedicada à entrega e ao balanceamento de aplicações, incluindo sua integração à infraestrutura existente e a configuração de arquitetura redundante. Dessa forma, não se sustenta a tentativa da Recorrente de caracterizar a experiência da Network Secure como limitada à implementação de soluções de segurança de perímetro ou conectividade, uma vez que a documentação apresentada comprova atuação anterior na implementação de equipamentos pertencentes à própria categoria tecnológica exigida no Lote 1.

Cabe destacar, ainda, que os esclarecimentos e a documentação complementar foram apresentados ao TJCE durante a fase de diligências, anteriormente à interposição do presente recurso administrativo, integrando o conjunto documental submetido à análise da Administração.

Diante do exposto, requer-se que a avaliação do atendimento ao item 15.3.3.1 considere integralmente o Atestado de Capacidade Técnica da Empreendimentos Pague Menos S/A, a declaração complementar assinada por seu representante legal e os esclarecimentos técnicos apresentados em resposta ao Ofício nº 207/2026, afastando-se a alegação de inexistência de experiência em serviços de complexidade tecnológica pertinente ao objeto da contratação.

e) Item 15.3.3.2.1 - quantitativos mínimos

Não procede a alegação da Recorrente quanto à ausência de comprovação dos quantitativos mínimos exigidos pelo Termo de Referência.

Conforme estabelecido no item 15.3.3.2.1, os atestados deverão comprovar a execução de contrato cujo objeto contemple quantitativo mínimo correspondente a 50% (cinquenta por cento) do previsto na contratação. Considerando que o Lote 1 contempla

o fornecimento de 02 (dois) equipamentos Application Delivery Controller (ADC), o quantitativo mínimo exigido corresponde a 01 (um) equipamento.

Nesse contexto, o Atestado de Capacidade Técnica emitido pela Empreendimentos Pague Menos S/A comprova o fornecimento e a implementação de 02 (duas) unidades FortiADC 700D pela Network Secure, quantitativo equivalente a 100% daquele previsto para o Lote 1, superando, portanto, o mínimo de 50% estabelecido no instrumento convocatório.

Cumpre destacar que essa informação já foi devidamente apresentada e esclarecida ao TJCE durante a segunda diligência, formalizada por meio do Ofício nº 207/2026, especificamente no apontamento H-1, ocasião em que a Network Secure apresentou informações complementares acerca da arquitetura efetivamente implementada no ambiente da Pague Menos.

A documentação apresentada demonstra que os dois appliances foram instalados em racks distintos e configurados em arquitetura de Alta Disponibilidade (HA), no modo Ativo-Passivo, comprovando que ambos integraram efetivamente a solução fornecida e implementada.

Adicionalmente, foi encaminhada declaração complementar emitida pela Empreendimentos Pague Menos S/A, devidamente assinada por seu representante legal, reforçando as informações relativas à implementação realizada.

Dessa forma, encontra-se demonstrado o atendimento ao quantitativo mínimo de equipamentos previsto no item 15.3.3.2.1, não havendo fundamento para alegação de insuficiência quantitativa quanto ao número de appliances ADC implementados.

Diante do exposto, requer-se que seja afastada a alegação de descumprimento do item 15.3.3.2.1, considerando-se o Atestado de Capacidade Técnica da Empreendimentos Pague Menos S/A e a documentação complementar já apresentada ao TJCE em atendimento ao Ofício nº 207/2026.

f) Item 15.3.3.2.3 - similaridade em porte, capacidade e complexidade

Não procede a alegação da Recorrente de que a Network Secure deixou de demonstrar experiência na implementação de soluções de natureza similar, com porte, capacidade e complexidade tecnológica compatíveis com o objeto da contratação.

Cumpre esclarecer que esse questionamento já foi objeto de análise pelo TJCE durante a segunda diligência, formalizada por meio do Ofício nº 207/2026, especificamente nos apontamentos H-1, H-2 e H-3, ocasião em que a Network Secure apresentou esclarecimentos técnicos e documentação complementar ao Atestado de Capacidade Técnica emitido pela Empreendimentos Pague Menos S/A.

Conforme documentação apresentada, a implementação contemplou 02 (duas) unidades FortiADC 700D, instaladas em racks distintos e configuradas em arquitetura de Alta Disponibilidade (HA), no modo Ativo-Passivo, integradas à infraestrutura de rede do cliente. Importante destacar que o ambiente atendido contemplava uma infraestrutura destinada a aproximadamente 10.000 usuários, distribuídos nacionalmente em 26 Estados do Brasil, evidenciando a abrangência operacional e a relevância da implementação realizada. Adicionalmente, a Network Secure apresentou declaração complementar, devidamente assinada pelo representante legal da Empreendimentos Pague Menos S/A, contendo informações sobre a solução e as funcionalidades efetivamente implantadas no ambiente, permitindo à Administração avaliar a similaridade tecnológica e a complexidade dos serviços anteriormente executados. Quanto à capacidade de processamento, a questão também foi expressamente abordada no apontamento H-2 da segunda diligência, no qual a Network Secure demonstrou que a solução implementada contemplava capacidade nominal instalada de 30 Gbps em camada 7, considerando os dois appliances FortiADC 700D, cada um com capacidade nominal de 15 Gbps.

Conforme esclarecido naquela oportunidade, essa capacidade corresponde ao conjunto de equipamentos instalados em arquitetura redundante, não representando throughput simultaneamente agregado, tendo sido submetida à apreciação da Administração a interpretação do requisito em relação à capacidade da solução implementada. Dessa forma, a análise da qualificação técnico-operacional não deve desconsiderar o conjunto de evidências apresentadas, incluindo o porte do ambiente atendido, a abrangência nacional da infraestrutura, a arquitetura de alta disponibilidade, as funcionalidades efetivamente implementadas e a experiência da Network Secure no fornecimento, instalação, configuração e treinamento de soluções da categoria ADC.

Ressalta-se, ainda, que os esclarecimentos e documentos complementares foram devidamente encaminhados ao TJCE durante a fase de diligências, anteriormente à interposição do presente recurso administrativo.

Diante do exposto, requer-se que a análise do requisito 15.3.3.2.3 considere integralmente o Atestado de Capacidade Técnica da Empreendimentos Pague Menos S/A, a declaração complementar assinada por seu representante legal e os esclarecimentos apresentados em atendimento ao Ofício nº 207/2026, observando-se a natureza tecnológica, o porte e a complexidade da solução efetivamente implementada.

g) Item 15.3.3.2.4 - equivalência tecnológica entre ADC e outros produtos

Não procede a alegação da Recorrente quanto à ausência de equivalência tecnológica da solução apresentada no Atestado de Capacidade Técnica emitido pela Empreendimentos Pague Menos S/A.

Cumpre esclarecer que esse questionamento já foi objeto de análise pelo próprio TJCE durante a segunda diligência, formalizada por meio do Ofício nº 207/2026, especificamente no apontamento H-3, que contemplou expressamente os requisitos 15.3.3.2.3, 15.3.3.2.4 e 15.3.3.2.5 do Termo de Referência.

Em atendimento à solicitação, a Network Secure apresentou documentação complementar, incluindo declaração formal emitida e devidamente assinada pelo representante legal da Empreendimentos Pague Menos S/A, com informações referentes à solução e às funcionalidades efetivamente implantadas no ambiente atestado. Ressalta-se que a implementação realizada contemplou 02 (duas) unidades FortiADC 700D, equipamentos pertencentes à categoria Application Delivery Controller (ADC), implementados em arquitetura de Alta Disponibilidade (HA), no modo Ativo-Passivo. Dessa forma, a experiência comprovada não se refere exclusivamente a soluções de segurança de perímetro, conectividade ou tecnologias distintas, conforme tenta caracterizar a Recorrente, mas à efetiva implementação de equipamentos da mesma categoria tecnológica exigida no Lote 1 da presente contratação.

Importante destacar que os esclarecimentos e a documentação complementar foram apresentados ao TJCE ainda durante a fase de diligências, anteriormente à

interposição do recurso administrativo, integrando o conjunto documental submetido à apreciação da Administração.

Portanto, a alegação de ausência de equivalência tecnológica desconsidera a documentação já apresentada, que demonstra experiência da Network Secure na implementação de soluções de Application Delivery Controller, com arquitetura e funcionalidades pertinentes ao objeto licitado.

Diante do exposto, requer-se que seja afastada a alegação de inexistência de equivalência tecnológica, considerando-se o atestado original e a declaração complementar apresentada em atendimento ao Ofício nº 207/2026.

h) Item 15.3.3.2.5 - descrição de funcionalidades efetivamente implantadas

Não procede a alegação apresentada pela Recorrente quanto à ausência de comprovação das funcionalidades efetivamente implantadas no ambiente da Empreendimentos Pague Menos S/A.

Cumpre esclarecer que esse questionamento já foi objeto de diligência conduzida pelo próprio TJCE, por meio do Ofício nº 207/2026, especificamente no apontamento H-3, ocasião em que a Network Secure apresentou os esclarecimentos técnicos solicitados, acompanhados de documentação complementar ao Atestado de Capacidade Técnica originalmente apresentado.

Dentre os documentos encaminhados, destaca-se a declaração complementar emitida pela Empreendimentos Pague Menos S/A, devidamente assinada por seu representante legal, na qual são formalizadas as informações referentes às funcionalidades efetivamente implementadas no ambiente atestado, permitindo à Administração verificar a compatibilidade técnica da experiência comprovada com as exigências do instrumento convocatório. Dessa forma, a comprovação apresentada não se limita às características ou funcionalidades disponíveis no datasheet do FortiADC 700D, mas encontra respaldo em declaração formal do próprio contratante dos serviços, responsável por atestar as características da solução efetivamente implementada pela Network Secure. Importante destacar que a referida documentação foi apresentada durante a fase de diligências, anteriormente à interposição do presente recurso administrativo, integrando, portanto, o conjunto documental já submetido à apreciação do TJCE.

Assim, a alegação da L8 Group desconsidera documentação complementar já disponibilizada à Administração, não se sustentando a afirmação de que a Network Secure deixou de comprovar as funcionalidades efetivamente implantadas no ambiente da Pague Menos. Diante do exposto, requer-se que seja afastada a alegação de ausência de comprovação documental, considerando-se os esclarecimentos e a declaração complementar regularmente apresentados em atendimento ao Ofício nº 207/2026, para fins de avaliação do requisito 15.3.3.2.5 do Termo de Referência.

i) Item 15.3.3.2.6.1 - capacidade mínima de 20 Gbps de throughput

A documentação oficial do fabricante apresenta, para cada FortiADC 700D, as seguintes capacidades nominais:
L4 Throughput: 18 Gbps por appliance;
L7 Throughput: 15 Gbps por appliance. Dessa forma, a implementação realizada contemplou uma capacidade nominal instalada correspondente a 36 Gbps em camada 4 e 30 Gbps em camada 7, considerando os dois appliances físicos efetivamente fornecidos e implementados no ambiente.

Para fins de correlação com o item 15.3.3.2.6.1, a licitante entende como indicador tecnicamente mais aderente o L7 Throughput, tendo em vista que o objeto da contratação é uma solução de Application Delivery Controller e que o próprio Anexo I utiliza throughput de camada 7 como parâmetro de capacidade de processamento das aplicações.

Nesse sentido, a solução implementada na Pague Menos apresentava 30 Gbps de capacidade nominal L7 instalada, resultante da implantação de duas unidades FAD-700D com capacidade nominal de 15 Gbps cada. A relevância da segunda unidade para fins de capacidade e porte da implementação está associada à disponibilidade da capacidade integral da solução: ambos os appliances implementados eram equipamentos completos e com a mesma capacidade nominal, estando o nó passivo disponível para assumir a função do nó ativo em cenário de contingência.

Assim, a arquitetura implementada disponibilizava dois ADCs de capacidade equivalente, cada qual apto a assumir integralmente o papel operacional do serviço, preservando a disponibilidade da plataforma diante da falha de um dos nós.

A documentação oficial da Fortinet caracteriza o FortiADC como plataforma voltada à disponibilidade das aplicações, incluindo automatic failover, e documenta expressamente suporte aos modos Active/Passive Failover e Active/Active Failover.

Dessa forma, a referência aos 30 Gbps deve ser compreendida como capacidade nominal L7 total instalada no ambiente atestado, correspondente aos dois equipamentos efetivamente integrantes da implementação, e não como declaração de throughput agregado simultâneo de um cluster ativo-passivo. Considerando que o item 15.3.3.2.6.1 não especificou expressamente se os 20 Gbps deveriam ser aferidos individualmente por appliance ou sobre a capacidade da solução implementada, a licitante entende que, para fins de qualificação técnico-operacional e demonstração do porte da experiência anterior, deve ser considerada a solução efetivamente implantada como conjunto, composta por dois ADCs físicos e capacidade nominal instalada de 30 Gbps L7, associada a arquitetura redundante de alta disponibilidade.

j) Certificação de parceiro e cabimento dos esclarecimentos Certificado de parceria Fortinet

A Recorrente sustenta que a condição de parceira autorizada da Fortinet não constitui, isoladamente, comprovação da experiência técnico-operacional da Network Secure na implementação de soluções Application Delivery Controller (ADC).

Embora seja correto afirmar que o certificado de parceria não substitui os atestados de capacidade técnica exigidos pelo instrumento convocatório, a argumentação apresentada pela L8 Group desconsidera que a Network Secure já apresentou documentação específica e formalmente emitida para comprovar sua experiência na implementação da tecnologia em questão.

Nesse sentido, destaca-se o Atestado de Capacidade Técnica emitido pela Empreendimentos Pague Menos S/A, acompanhado de declaração complementar devidamente assinada por seu representante legal, contendo informações sobre a arquitetura e as funcionalidades efetivamente implementadas no ambiente, documentação esta já encaminhada ao TJCE durante a segunda diligência, formalizada por meio do Ofício nº 207/2026. Portanto, a comprovação da experiência técnica da Network Secure não se fundamenta exclusivamente em sua condição de parceira autorizada da Fortinet, mas em documentação emitida pelo próprio contratante dos

serviços, que atesta a efetiva participação da empresa no fornecimento e na implementação da solução FortiADC. Ao direcionar sua argumentação à natureza e ao alcance do certificado de parceria, sem considerar adequadamente os atestados e a documentação complementar já apresentados, a Recorrente incorre em interpretação parcial do conjunto probatório, atribuindo ao certificado uma finalidade comprobatória que não lhe foi conferida pela Network Secure. Tal abordagem compromete a consistência da argumentação recursal, uma vez que a ausência de comprovação técnico-operacional não pode ser inferida das limitações de um certificado de parceria quando existem documentos específicos, emitidos pelo próprio contratante, destinados justamente à demonstração da experiência anteriormente executada.

Dessa forma, requer-se que a Administração desconsidere a tentativa de desqualificação da experiência técnica da Network Secure com fundamento exclusivo no alcance do certificado de parceria Fortinet, procedendo à análise integral dos atestados e documentos complementares já apresentados, em observância aos princípios do julgamento objetivo, da motivação e da vinculação ao instrumento convocatório.

V. DA QUALIFICAÇÃO TÉCNICO-OPERACIONAL E DA IMPROCEDÊNCIA DAS ALEGAÇÕES RECURSAIS

A Recorrente sustenta que nossa empresa não teria comprovado a qualificação técnico-operacional exigida para o Lote 1 do Pregão Eletrônico nº 032/2026, sob o argumento de que os atestados de capacidade técnica apresentados não demonstrariam a implementação de solução do tipo *Application Delivery Controller* (ADC) com capacidade mínima de 20 Gbps de *throughput*. Questiona, ainda, a similaridade dos serviços comprovados e invoca o Certificado de Parceria Fortinet para sustentar que a especialização nele indicada, relacionada à tecnologia SD-WAN, não seria suficiente para demonstrar aptidão para o objeto licitado.

As alegações devem ser examinadas à luz dos critérios expressamente estabelecidos no item 15.3.3 do Termo de Referência, especialmente quanto à aptidão para execução de serviços de complexidade tecnológica e operacional equivalente ou superior, aos quantitativos mínimos exigidos, à similaridade das soluções, à

equivalência tecnológica e à comprovação específica da capacidade de *throughput* prevista para o Lote 1.

Nesse sentido, a análise da qualificação técnico-operacional deve se fundamentar no conteúdo dos documentos apresentados e em sua correspondência com os requisitos do instrumento convocatório, sem confundir a comprovação da experiência efetivamente executada com a certificação ou a classificação comercial atribuída pelo fabricante à empresa licitante.

a) Dos atestados de capacidade técnica e da comprovação da experiência operacional

Para comprovar sua aptidão técnica, nossa empresa apresentou atestados de capacidade técnica emitidos por entidades públicas e privadas, identificadas nos autos como Tribunal de Contas do Estado do Ceará (TCE/CE), Ministério Público do Estado de Mato Grosso (MPMT), Tribunal de Justiça do Rio Grande do Norte (TJRN), GOL Linhas Aéreas e Pague Menos.

A suficiência desses documentos deve ser examinada individualmente, considerando os objetos dos contratos executados, os serviços efetivamente prestados, os quantitativos comprovados e as características técnicas das soluções implantadas ou operadas. Essa análise permite verificar a correspondência entre a experiência demonstrada e os critérios de qualificação previstos no edital.

O item 15.3.3.2.1 do Termo de Referência exige a comprovação de execução contratual em quantitativo mínimo correspondente a 50% do previsto na contratação, enquanto o item 15.3.3.2.2 admite a soma de atestados, observadas as condições estabelecidas para serviços executados de forma concomitante.

Por sua vez, o item 15.3.3.2.3 determina que os documentos demonstrem a execução de equipamentos, soluções ou serviços de natureza similar, com porte, capacidade, complexidade e relevância técnica equivalentes ou superiores ao objeto licitado.

Dessa forma, a análise não deve se limitar à denominação atribuída a cada solução ou à identificação do fabricante, mas considerar as características efetivamente comprovadas nos documentos apresentados. Requeremos, portanto, que os atestados

sejam apreciados em seu conteúdo integral, confrontando-se as informações neles registradas com os requisitos objetivos de habilitação.

b) Da equivalência tecnológica e das funcionalidades comprovadas

O item 15.3.3.2.4 do Termo de Referência estabelece que não serão aceitos atestados referentes a soluções de capacidade inferior, menor criticidade ou sem equivalência tecnológica, tampouco aqueles que não apresentem funcionalidades equivalentes às exigidas para as soluções ADC e WAF.

O item 15.3.3.2.5, por sua vez, exige descrição clara da solução implantada ou operada e de suas principais funcionalidades técnicas, de modo a permitir a verificação de sua compatibilidade com o objeto contratado.

Essas disposições impõem uma análise material da experiência comprovada. Assim, a compatibilidade dos atestados deve ser aferida a partir das informações técnicas neles constantes, observando-se a natureza dos serviços, as funcionalidades efetivamente executadas e a correspondência com as exigências editalícias.

No caso em exame, a Recorrente deverá demonstrar, de maneira objetiva e individualizada, em que medida os documentos apresentados deixariam de satisfazer os critérios estabelecidos no instrumento convocatório. A simples contestação genérica da similaridade dos serviços, sem o confronto entre as características comprovadas e os requisitos exigidos, não substitui a análise técnica dos documentos.

Nossa defesa, portanto, deve se apoiar na demonstração documental da compatibilidade entre a experiência efetivamente comprovada e o objeto licitado, respeitando os limites e as condições previstos no edital.

c) Da exigência específica de capacidade mínima de 20 Gbps de throughput — item 15.3.3.2.6.1

A Recorrente sustenta que nenhum dos atestados apresentados comprovaria a implementação de equipamento ADC com capacidade mínima de 20 Gbps de *throughput*, conforme exigido pelo item 15.3.3.2.6.1 do Termo de Referência.

Esse requisito merece análise específica, uma vez que estabelece expressamente a comprovação da implementação de equipamento do tipo ADC com capacidade mínima de 20 Gbps, equivalente a, no mínimo, 50% da capacidade prevista para o objeto da contratação.

Por se tratar de exigência objetiva de qualificação técnico-operacional, sua verificação deve se fundamentar em documentação que permita identificar o equipamento efetivamente implementado e a respectiva capacidade de processamento. A capacidade nominal do equipamento ofertado nesta licitação, por si só, não comprova necessariamente que a empresa já executou contrato anterior envolvendo equipamento com a capacidade mínima exigida.

Assim, para afastar a alegação recursal, é necessário demonstrar, por meio dos atestados ou de documentação complementar admissível, que a experiência anterior de nossa empresa atende ao parâmetro estabelecido no item 15.3.3.2.6.1. Essa demonstração deve identificar expressamente o documento comprobatório e a informação técnica correspondente, de modo a permitir a verificação objetiva pela Administração.

d) Do alcance probatório do Certificado de Parceria Fortinet

A Recorrente também invoca o Certificado de Parceria Fortinet, afirmando que a especialização nele indicada seria relacionada a SD-WAN, e não especificamente à tecnologia ADC.

A esse respeito, é necessário distinguir a finalidade do certificado de parceria daquela dos atestados de capacidade técnica. O certificado deve ser interpretado nos limites das informações que efetivamente registra, enquanto os atestados se destinam a comprovar a experiência operacional decorrente da execução de contratos anteriores.

Consequentemente, a classificação comercial indicada no certificado não deve ser confundida com a totalidade da experiência operacional da empresa. Da mesma forma, o certificado não deve ser utilizado isoladamente como prova de experiência específica com ADC, caso não contenha informação expressa nesse sentido.

A análise da qualificação técnico-operacional deve considerar, portanto, os atestados e os demais documentos pertinentes, verificando se eles demonstram o

atendimento às exigências editalícias, independentemente da função probatória específica do certificado de parceria.

e) Da necessidade de julgamento objetivo e da manutenção da habilitação

A controvérsia apresentada pela Recorrente exige o confronto entre os critérios de habilitação estabelecidos no Termo de Referência e a documentação efetivamente apresentada por nossa empresa.

Nesse contexto, requeremos que os atestados de capacidade técnica sejam avaliados de forma individualizada e conjunta, conforme permitido pelo edital, considerando-se os quantitativos comprovados, a natureza dos serviços executados, a equivalência tecnológica e a capacidade do equipamento implementado, especialmente quanto ao requisito de *throughput* mínimo de 20 Gbps.

A decisão administrativa deve estar fundamentada nos elementos constantes dos autos e na aplicação objetiva das exigências previamente estabelecidas no instrumento convocatório. Por essa razão, não se deve presumir o descumprimento de requisito sem a análise correspondente dos documentos, assim como não se deve considerar comprovada exigência específica sem evidência documental suficiente.

Diante do exposto, requeremos o não acolhimento das alegações recursais relativas à qualificação técnico-operacional, desde que reconhecido, após o exame da documentação apresentada, o efetivo atendimento aos requisitos dos itens 15.3.3.2.1 a 15.3.3.2.6.1 do Termo de Referência, com a consequente manutenção da decisão de habilitação de nossa empresa no Lote 1.

VI. DA CONCLUSÃO GERAL

Diante de todo o exposto, verifica-se que as alegações apresentadas pela Recorrente devem ser examinadas à luz das disposições do Edital do Pregão Eletrônico nº 032/2026, do respectivo Termo de Referência, dos esclarecimentos oficiais prestados pela Administração e do conjunto documental apresentado pela Recorrida ao longo do procedimento licitatório.

No que se refere aos questionamentos técnicos relacionados à solução ofertada, a Recorrida apresentou esclarecimentos fundamentados na documentação do fabricante

aplicável à versão considerada na análise, buscando demonstrar a compatibilidade dos recursos disponibilizados com as exigências do instrumento convocatório e esclarecer as limitações apontadas pela Recorrente, cuja interpretação deve ser confrontada individualmente com a redação de cada requisito e com as evidências técnicas correspondentes.

Quanto à qualificação técnico-operacional, destaca-se a documentação relativa à implementação de duas unidades FortiADC 700D no ambiente da Empreendimentos Pague Menos S/A, complementada por declaração emitida pelo próprio contratante e pelos esclarecimentos apresentados em atendimento ao Ofício nº 207/2026. Tais elementos devem ser apreciados de forma conjunta, considerando a natureza da solução implementada, as funcionalidades descritas, a arquitetura de alta disponibilidade e a capacidade nominal informada, observados os critérios objetivos estabelecidos no Termo de Referência.

Do mesmo modo, a análise da proposta comercial e dos serviços associados deve considerar a composição efetivamente ofertada e a distinção entre suporte técnico continuado, cobertura do fabricante e serviços profissionais especializados, evitando-se conclusões baseadas na análise isolada de componentes que possuem finalidades distintas.

A Recorrida ressalta que a avaliação de sua proposta e de sua habilitação deve observar os princípios da vinculação ao instrumento convocatório, do julgamento objetivo, da isonomia, da razoabilidade, da motivação e da competitividade, em conformidade com a Lei nº 14.133/2021. Isso exige que eventuais desconformidades sejam identificadas de maneira objetiva, mediante correlação entre a exigência editalícia, a solução ofertada e as provas constantes dos autos, não sendo suficiente a formulação de conclusões genéricas ou dissociadas do conjunto documental.

Assim, requer-se que as razões recursais sejam apreciadas de forma individualizada e fundamentada, considerando-se os esclarecimentos e documentos já apresentados pela Recorrida, de modo que a decisão administrativa resulte da aplicação objetiva dos critérios previstos no edital e no Termo de Referência.

VII. DOS PEDIDOS

Diante do exposto, a Recorrida requer:

a) O recebimento e o conhecimento das presentes contrarrazões, por serem apresentadas no exercício do direito previsto no art. 165 da Lei nº 14.133/2021 e no item 7.1 do Edital do Pregão Eletrônico nº 032/2026;

b) No mérito, o **não provimento do recurso administrativo interposto pela Recorrente**, afastando-se as alegações que não encontrem respaldo na análise objetiva das exigências editalícias e das provas constantes dos autos;

c) A apreciação integral e conjunta dos documentos e esclarecimentos técnicos apresentados pela Recorrida, especialmente aqueles encaminhados em atendimento aos Ofícios nº 191/2026 e nº 207/2026, incluindo a documentação complementar relativa ao Atestado de Capacidade Técnica emitido pela Pague Menos S/A;

d) Quanto à qualificação técnico-operacional, que a Administração examine o atendimento aos itens 15.3.3.1 e 15.3.3.2.1 a 15.3.3.2.6.1 do Termo de Referência com base no conjunto probatório disponível, considerando a experiência demonstrada na implementação de soluções ADC, o quantitativo de equipamentos implantados, a similaridade tecnológica, as funcionalidades descritas e os esclarecimentos relativos à capacidade nominal da solução;

e) Quanto aos questionamentos técnicos referentes à solução ofertada, que cada requisito seja apreciado individualmente, com base na documentação técnica pertinente, nas respostas já apresentadas e nos esclarecimentos oficiais da Administração, afastando-se conclusões que não decorram diretamente das exigências do instrumento convocatório e das evidências técnicas correspondentes;

f) Subsidiariamente, caso remanesça dúvida técnica objetiva e relevante sobre algum requisito específico, que seja avaliada a possibilidade de realização de diligência ou solicitação de esclarecimento técnico complementar ao fabricante, nos limites legalmente admitidos, com vistas ao esclarecimento dos fatos e à adequada instrução do julgamento, sem alteração indevida da proposta ou das condições essenciais do certame;

g) Ao final, sendo reconhecido o atendimento às exigências editalícias aplicáveis, a **manutenção da decisão que classificou a proposta e habilitou a Recorrida no Lote 1**, com o regular prosseguimento do procedimento licitatório.

Requer-se, por fim, que a decisão administrativa enfrente os argumentos relevantes apresentados pelas partes, mediante fundamentação compatível com as exigências do edital, com a documentação constante dos autos e com a legislação aplicável.

Termos em que,
pede deferimento.

Fortaleza/CE, 20 de outubro de 2026.



Yure Leopoldo Sabino de Freitas
Network Secure Segurança da Informação
Representante Legal