



**AO SENHOR(A) PREGOEIRO(A) DO TRIBUNAL REGIONAL DO
TRABALHO DA 9ª REGIÃO**

UASG 080012)

PREGÃO ELETRÔNICO Nº 90022/2025

Processo Administrativo Nº 2199/2025

L8 GROUP SA, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o n.º 19.952.299/0012-65, representada na sua forma estatutária, vem respeitosamente, perante Vossa Senhoria, com fundamento no item 12 e seguintes do edital e demais legislações aplicáveis, interpor o presente **RECURSO ADMINISTRATIVO** em face da decisão de adjudicação do objeto à empresa **COMPWIRE**, pelas razões de fato e de direito a seguir expostas.

I. DA TEMPESTIVIDADE E DO OBJETO

O presente Recurso é interposto tempestivamente, dentro do prazo legal, após a devida análise da proposta vencedora.

O objeto deste recurso é a desclassificação da proposta da empresa **COMPWIRE** por descumprimento das exigências e especificações técnicas do TR, o que quebra a isonomia e o julgamento objetivo.

II. DOS FUNDAMENTOS DE FATO E DE DIREITO



O presente edital tem por objeto o Registro de Preços para eventual aquisição de switches LAN (acesso e topo de rack), módulos ópticos, plataforma de gerenciamento e solução de controle de acesso à rede (NAC), incluindo licenças, serviços de instalação, ativação, treinamento e suporte técnico especializado, bem como prestação de garantia técnica on-site pelo período de 60 (sessenta) meses para os switches de acesso, a plataforma de gerenciamento e o NAC, e de 36 (trinta e seis) meses para os switches topo de rack, nos termos da tabela do termo de referência, conforme condições e exigências estabelecidas no edital e seus anexos.

Referido Pregão é regido pela Lei nº 14.133, de 2021, pelo Decreto nº 11.462, de 31 de março de 2023, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas no Edital e anexos.

A proposta vencedora deve ser desclassificada imediatamente por dois motivos principais, ambos configurando a inobservância da legislação e do instrumento convocatório: (A) Não atendimento de requisitos técnicos de extrema relevância pela solução e que comprometem o uso, a segurança e a funcionalidade da solução nos termos e natureza exigidas pelo TRT9 e (B) Ausência de comprovação de itens relevantes.

II.I. Da Arquitetura NAC Proposta (Single-Node com Arbitration Server). Contexto e Requisitos de Alta Disponibilidade no Edital (TRT9 – Itens 17.13.1.6 a 17.13.1.8)



O Tribunal Regional do Trabalho da 9ª Região (TRT9), em seu edital de aquisição da solução de controle de acesso à rede (NAC), estabeleceu requisitos claros de alta disponibilidade. Em especial, os itens 17.13.1.6 a 17.13.1.8 do Termo de Referência exigem que a plataforma de gerenciamento/NAC disponha de:

- (i) alta disponibilidade para as funções de administração e monitoração do NAC;
- (ii) redundância por meio de outro appliance virtual (ou seja, dois appliances NAC operando de forma redundante); e
- (iii) continuidade dos serviços sem interrupção, mesmo em caso de falhas, garantindo failover imediato e transparente.

Tais exigências visam resguardar a disponibilidade do sistema NAC, evitando pontos únicos de falha e assegurando que eventuais panes não interrompam a segurança e o acesso à rede corporativa.

Portanto, qualquer proposta deve, obrigatoriamente, contemplar uma arquitetura de NAC com alta disponibilidade sem interrupção dos serviços, atendendo a essas condições de redundância e continuidade ininterrupta.

A empresa Compwire, em sua proposta, descreveu a instalação do **Huawei iMaster NCE-Campus** (plataforma que incorpora as funções de NAC) e do módulo CampusInsight em modo **single-node**.

A topologia apresentada consiste em dois servidores físicos configurados em arranjo ativo/standby (isto é, um servidor principal ativo e outro em espera passiva) e um terceiro servidor atuando como nó árbitro (*arbitration server*).



Em resumo, apenas um único nó de aplicação NAC estaria em funcionamento ativo por vez, enquanto o segundo permaneceria em *standby* aguardando eventual falha do primeiro; a coordenação do failover ficaria a cargo do terceiro nó (árbitro), responsável por decidir qual nó deve estar ativo.

Essa configuração difere de um cluster tradicional de alta disponibilidade ***sem interrupção de serviços***.

Em vez de dois appliances NAC ativos simultaneamente compartilhando carga ou em espelhamento contínuo, a solução compõe-se de um **único appliance ativo** (single-node) com uma réplica e um árbitro para mediar a troca de papéis em caso de falha.

A Compwire apresenta tal mecanismo como forma de fornecer disponibilidade ao NAC, alegando que o nó *standby*, **assumiria sem interrupção de serviço**, em caso de queda do ativo.

É essencial, contudo, confrontar tecnicamente essa arquitetura com os requisitos editalícios supracitados, examinando se de fato atende à alta disponibilidade plena, à exigência de dois appliances redundantes e à continuidade ininterrupta de todas as operações e funcionalidades do NAC.

II.II. Falhas Técnicas da Arquitetura Proposta Frente aos Requisitos do item 17.13.1.8.

Estabelece o item 17.13.1.8:

No caso de falha de um dos componentes do conjunto, o outro deve ser capaz de assumir todas as operações e funcionalidades **sem interrupção dos serviços**;



Ao analisar a solução *single-node* com arbitration server da Huawei (iMaster NCE-Campus) à luz do edital, identificam-se claramente inconformidades técnicas em relação às exigências de alta disponibilidade.

O requisito **17.13.1.8** estabelece um padrão de **Alta Disponibilidade (HA) Local Efetiva** que, de fato, a arquitetura *single-node* (nó único) com servidor de arbitragem (witness server) da Huawei (iMaster NCE-Campus), não pode cumprir.

Isso porque a arquitetura de nó único é inerentemente contrária ao requisito de não interrupção

A Alta Disponibilidade Efetiva requer uma arquitetura de *cluster* (tipicamente Active-Standby ou Active-Active, com 2 ou mais nós ativos/redundantes) que mantenha o estado do serviço (sessões, configurações recentes, dados de *runtime*) sincronizado em tempo real.

Isso permite que, em caso de falha do nó primário, o nó secundário assuma a operação de forma imediata, garantindo a continuidade das funcionalidades (e.g., autenticações de usuário, gerenciamento de dispositivos autenticados, visibilidade da rede).

Por natureza, uma solução *Single-Node* significa que todos os serviços e componentes críticos (servidor de aplicação, banco de dados) estão em uma única instância física ou virtual. Se essa única instância falhar, **não há outro componente para assumir I-M-E-D-I-A-T-A-M-E-N-T-E**.

Assim, a interrupção é inevitável, e mesmo que haja um mecanismo automatizado de *Warm Standby* ou a recriação do serviço (que é o que o arbitration server geralmente facilita em configurações mínimas), o tempo necessário para:

- 1) Detectar a falha (o arbiter atua aqui),



2) Promover o nó *standby* (se houver) ou iniciar a aplicação em uma nova instância,

3) Carregar o banco de dados e os serviços de aplicação e

4) Restabelecer a conectividade com os dispositivos de rede (APs, switches, roteadores), **configura uma interrupção de serviço (downtime), que pode durar de dez segundos a vários minutos, violando diretamente o requisito de ser "sem interrupção dos serviços."**

Essa característica pode ser comprovada nos links abaixo:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100331202&id=EN-US_TOPIC_0000001205751626

“... Automatic switchover (with a third arbitration site)

There are three equipment rooms, and the status of the primary and secondary sites is monitored in real time. If a site- or application-level fault occurs, an active/standby switchover is immediately triggered **to restore services...**”

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100331202&id=EN-US_TOPIC_0000001250271601

“... Process restart: Process status is monitored in real time. If a process is stopped or faulty, iMaster NCE-Campus attempts to **restart the process...**”



A interrupção afeta diretamente as funcionalidades críticas que deveriam permanecer operacionais:

Funcionalidade	Impacto na Arquitetura Single-Node	Violação de 17.13.1.8
Gerenciamento de Dispositivos	Perda de visibilidade de monitoramento e falhas durante o período de reinicialização.	Interrupção na operação de monitoramento e coleta de dados.
Autenticação (RADIUS/Portal)	Dispositivos de acesso (APs, switches) perdem o contato com o servidor de autenticação central. Novas autenticações (novos usuários, reautenticações) falham.	Interrupção na funcionalidade crítica de acesso à rede.
Sincronização de Configurações	Novas configurações feitas pouco antes da falha podem ser perdidas (<i>RPO</i> não zero) ou demoram a ser aplicadas no <i>standby</i> durante o <i>switchover</i> .	Interrupção na aplicação de políticas e perda potencial de dados.

O item 17.13.1.8 exige **Tolerância a Falhas** ("sem interrupção dos serviços"), que só é alcançada com redundância N+1 ou N+N (e.g., um cluster Active-Standby/Active-Active) onde os estados são sincronizados.

A solução *Single-Node* com *arbiter*, na melhor das hipóteses, oferece **Recuperação de Falhas** (o serviço retorna após um período de inatividade), o que é inaceitável para o requisito.



Portanto, a solução proposta pela empresa Compwire, baseada na arquitetura Huawei iMaster NCE-Campus em modo Single-Node com Arbitration Server, não atende ao disposto no Item 17.13.1.8 do Edital.

Tal arquitetura não configura uma Alta Disponibilidade Local Efetiva (True HA), uma vez que a falha do único nó operacional (Single Point of Failure) exige um tempo de Switchover/Failover para que o serviço seja restabelecido (tempo de detecção de falha, inicialização do serviço e recuperação do banco de dados).

Este processo, mesmo que totalmente automatizado, implica em uma interrupção dos serviços que viola o requisito de continuidade 'sem interrupção dos serviços', caracterizando-se, na melhor das hipóteses, como uma solução de *Warm Standby* (Standby Quente) ou *Disaster Recovery*, e não de **Fault Tolerance** (Tolerância a Falhas) conforme exigido."

No link:

["https://support.huawei.com/hedex/hdx.do?docid=EDOC1100331202&id=EN-US_TOPIC_0000001250271601"](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100331202&id=EN-US_TOPIC_0000001250271601), está evidenciado em *protection capability* a interrupção dos serviços para as camadas da aplicação.

Isso evidencia que além do não atendimento técnico, há, portanto, flagrantemente, um desequilíbrio competitivo, eis que a proposta dos concorrentes assume os custos adicionais de softwares, licenciamento e serviços necessários à implantação em cluster, em conformidade com a exigência de alta disponibilidade do NAC sem interrupção de serviços.

Contrapartida, a proposta concorrente apresenta preço inferior porque se baseia em uma topologia simplificada, que não proporciona a disponibilidade requerida e expõe o órgão a risco de interrupção do serviço de controle de acesso.



Cabe ressaltar que a Huawei, assim como as concorrentes, possui arquitetura como "Minimum cluster", "Distributed cluster" e "Multi-cluster system" que entregam design sem interrupção de serviço, porém necessitam de mais servidores e componentes que devem ser fornecidos no projeto.

III. Inadequação da solução Huawei iMaster NCE-Campus (CampusInsight) ao item 17.11.25 do Edital

O item 17.11.25 do edital estabelece que **a solução de gerenciamento de rede deve medir a experiência do usuário, possibilitando a instalação de hardware ou software em pontos da rede definidos pela Contratante (Administração).**

Em outras palavras, a infraestrutura de gerenciamento deve permitir à Administração posicionar sondas ativas ou agentes de medição em locais estratégicos de sua escolha, para avaliar a qualidade da experiência do usuário nesses pontos específicos.

Esse requisito visa oferecer flexibilidade máxima na monitoração da rede, garantindo que a percepção de desempenho do usuário final seja aferida onde e como o órgão desejar, e não apenas pelos switches que serão adquiridos nesse projeto.

Diante dessa exigência, passamos a demonstrar que a solução proposta pela Compwire baseada nos produtos Huawei iMaster NCE-Campus e CampusInsight não atende a tal requisito.

Os pontos a seguir elencados detalham os aspectos técnicos que evidenciam a inadequação da solução Huawei em relação ao item 17.11.25 do edital.



III.I. Dependência exclusiva de telemetria de equipamentos Huawei (sem agentes independentes)

A arquitetura Huawei iMaster NCE-Campus/CampusInsight está fundamentada em telemetria nativa dos dispositivos de rede Huawei, como switches de acesso, pontos de acesso sem fio (APs) e controladoras de WLAN.

Conforme a própria documentação da Huawei, a plataforma coleta dados da rede em tempo real via tecnologia de *Streaming Telemetry* embutida nos equipamentos¹.

Além disso, a solução de monitoramento inteligente da Huawei atualmente suporta apenas switches e APs da marca Huawei (“Huawei cloud switches and cloud APs”) para realizar as análises inteligentes de rede.

Isso significa que toda a visibilidade e medição de desempenho na solução Huawei baseia-se nos dados fornecidos pelos próprios dispositivos Huawei instalados na rede (uso de CPU/porta, logs de cliente, estatísticas de tráfego, etc.), não havendo, no design do sistema, a previsão de instalar agentes de software em estações de trabalho nem de colocar sondas dedicadas de hardware em pontos arbitrários da rede.

Diferentemente de plataformas que admitem sondas independentes, o iMaster NCE-CampusInsight funciona de forma dependente do seu próprio hardware, extraindo informações unicamente da infraestrutura de comunicação existente.

Essa característica já demonstra, de plano, o desalinhamento com o item 17.11.25: **a solução não oferece mecanismos para implantação**

¹. [5] iMaster NCE-CampusInsight - Huawei Enterprise

<https://e.huawei.com/en/products/network-analysis/campusinsight>



de componentes de medição nos locais escolhidos pela Administração, pois restringe-se à telemetria dos equipamentos do fabricante.

III.II. Análise da experiência do usuário baseada em fluxos passivos (sem sondas ativas nos terminais)

O CampusInsight, módulo de análise da Huawei, mede a experiência do usuário de forma indireta, observando os fluxos de tráfego e eventos coletados pela própria rede. Ou seja, o sistema infere métricas de qualidade (latência, perda de pacotes, throughput etc.) a partir do tráfego real capturado nos switches e APs, sem gerar tráfego sintético de teste ou executar transações simuladas a partir da perspectiva do usuário final.

Não há, portanto, “sondas ativas” ou *agents* instalados nos terminais (estações de trabalho dos usuários) ou em pontos independentes gerando medições dedicadas. Toda a inteligência é centrada na malha de equipamentos de rede: o sistema detecta um eventual problema de experiência do usuário, por exemplo, ao notar que um fluxo de vídeo apresenta perda de pacotes acima do normal ou que um cliente Wi-Fi teve múltiplas reassociações, tudo isso a partir dos registros internos dos switches/controladoras.

Essa abordagem, limita-se a uma monitoração passiva – ou seja, depende do tráfego existente e dos pontos de coleta fornecidos pelos equipamentos da Huawei.

Não há funcionalidade de se implantar um agente em um PC remoto ou uma sonda de geração de tráfego em um enlace específico para, por exemplo, medir continuamente a latência até um servidor crítico sob a ótica do usuário naquele local.



Em suma, a “experiência do usuário” é aferida por observação da rede, e não por medições ativas originadas em pontos escolhidos livremente, o que contraria a solução pretendida no edital.

III.III. Inferência da experiência por dispositivos de rede, sem componentes em estações ou links críticos

A própria documentação oficial da Huawei confirma explicitamente que o monitoramento da experiência de aplicações e da “jornada” do cliente na rede é feito por intermédio dos dispositivos de comunicação.

Para viabilizar as métricas de qualidade end-to-end, a Huawei esclarece que é necessário apenas habilitar recursos nos switches, controladoras (AC) e Aps.

Ou seja, a Huawei confere aos próprios equipamentos de rede o papel de “sensores” da experiência, extraíndo deles todos os dados sobre a sessão do cliente (autenticação, sinal Wi-Fi, uso de banda, perdas, etc.).

Em nenhum trecho dos manuais da Huawei há menção a dispositivos-sonda autônomos ou módulos de software instaláveis externamente para aferição de desempenho. Pelo contrário, a solução é apresentada como integrada e intrínseca à rede Huawei – “*CampusInsight can manage and provide intelligent analysis for Huawei cloud switches and cloud*



APs”² –, reforçando que a visibilidade de experiência se limita ao que os equipamentos Huawei conseguem enxergar ou inferir.

Em consequência, não há como cumprir a parte do item 17.11.25 que exige colocar pontos de medição onde a Administração julgar necessário, já que a solução não dispõe de nenhum componente portátil ou instalável em enlaces críticos (por exemplo, em um link de operadora ou em um segmento de rede legado não-Huawei) para medir a experiência ali. Toda a inferência depende da presença de um switch/AP Huawei coletando telemetria naquele ponto – o que não equivale à “sonda” independente prevista no edital.

Importante salientar que na própria especificação técnica, no item 17.11.26, a CONTRATANTE pede TAMBÉM telemetria a partir dos switches que serão fornecidos no projeto. Ou seja, está nítida as exigências do item 17.11.25 e a falha de atendimento ao cumprimento técnico do mesmo na proposta da Compwire.

III.IV. Limitação à flexibilidade de posicionamento de pontos de medição pela Administração



Diante dos fatos técnicos expostos, fica claro que a solução Huawei proposta impõe restrições significativas à flexibilidade da Administração em monitorar a rede conforme seus interesses estratégicos.

O item 17.11.25 buscou assegurar ao TRT9 a possibilidade de posicionar ferramentas de medição ativamente onde houvesse maior relevância, por exemplo, em uma localidade remota com reclamações de lentidão, ou junto a um servidor específico para auditar a qualidade de experiência dos usuários daquele serviço.

Com o Huawei CampusInsight, essa liberdade não existe: a monitoração fica necessariamente vinculada aos pontos onde há equipamentos Huawei e aos dados que estes conseguem prover.

Caso a Administração deseje medir a experiência em um ponto da rede sem um dispositivo Huawei de borda (ou mesmo fora do âmbito LAN, como numa conexão WAN ou internet), a solução não oferece um meio nativo para tal – não há *probe* móvel que se possa implantar nessa ponta, nem agente de software que rode em um computador realizando testes periódicos.

Essa limitação compromete a abrangência do gerenciamento: a Administração fica presa à topologia da rede Huawei para coletar dados, em vez de ter autonomia plena para dispor sondas onde julgar necessário.

Em termos práticos, isso inviabiliza atender o intuito do requisito editalício, que era permitir uma personalização da monitoração da experiência do usuário de acordo com as necessidades do órgão. A solução Huawei, portanto, não satisfaz a finalidade esperada – em vez de servir à estratégia do administrador da rede, impõe a sua própria arquitetura como delimitação dos pontos de visibilidade.



IV. Não Comprovação de Integração NAC–NGFW

O edital do Tribunal Regional do Trabalho da 9ª Região (TRT9) exige expressamente que a solução de *Network Access Control* (NAC) possua integração funcional com **firewalls de próxima geração (NGFW)** de fabricantes específicos – Check Point, Cisco, Fortinet e Palo Alto – conforme os subitens 17.13.8.1 a 17.13.8.1.4 do edital.

Tal integração deve viabilizar **segmentação dinâmica de rede e compartilhamento de informações de segurança** entre o NAC e os NGFW, de modo a permitir políticas coordenadas de acesso e proteção em todo o ambiente. Em outras palavras, o NAC deve ser capaz de comunicar-se com os firewalls dessas marcas, trocando dados de autenticação, grupos de usuários ou contextos de ameaça, para que os NGFW apliquem políticas conforme a postura de cada dispositivo ou usuário autenticado no NAC.

Essa exigência visa assegurar que, independentemente do fabricante do firewall já instalado ou licitado futuramente pelo órgão (Check Point, Cisco, Fortinet ou Palo Alto), a solução NAC contratada consiga **interoperar plenamente com ele.**

Assim, garante-se que a Administração não fique limitada a um único fabricante e que a solução de segurança seja abrangente, atendendo ao princípio da padronização ampla e da melhor tecnologia disponível, sem prejudicar investimentos já realizados em firewalls de ponta.

IV.I. Da Documentação Apresentada pela Proponente (Compwire)



A empresa Compwire, ao tentar demonstrar conformidade com essa exigência, apresentou um único link: uma página de documentação da Huawei, fabricante da solução NAC ofertada (Huawei iMaster NCE-Campus). Todavia, conforme análise do conteúdo, trata-se de uma documentação genérica sobre templates ou modelos de configuração, sem qualquer comprovação técnica pontual de integração funcional específica com os produtos listados no edital.

Em primeiro lugar, não há menção nominal a Check Point, Fortinet ou Palo Alto nos documentos apresentados pela Compwire. E sobre Cisco, no ponto-a-ponto apresentado, omitiu-se os nomes completos, dentro da coluna comprovação, que se trata de switches e controladores wireless (Cisco Catalyst, Cisco WLC) e não tem relação com NGFW como exigido na especificação.

Não se identifica no texto nenhuma referência a interfaces, protocolos ou módulos específicos para conversar com, por exemplo, o Check Point NGFW ou o Cisco Secure Firewall, etc.

Além disso, não há guias de configuração, cases ou topologias de integração no documento apresentado.

Em documentação técnica de integração, seria esperado encontrar instruções do tipo “como configurar o NAC para conectar-se ao firewall X”, ou “exemplo de política aplicada no firewall Y com dados provenientes do NAC”.

No entanto, o link fornecido não contém **nenhum procedimento de configuração ou interoperabilidade** concreto envolvendo os NGFW de terceiros – apenas descrições conceituais.

Portanto, a simples apresentação desse link **genérico** não atende ao requisito editalício: **falta evidência técnica específica** de que o



Huawei iMaster NCE-Campus NAC integra-se efetivamente com os firewalls da Check Point, Cisco, Fortinet e Palo Alto, conforme exigido.

A seguir, detalhamos porque a ausência dessas evidências inviabiliza o atendimento do edital.

IV.II. Integração NAC–NGFW: Diligência que confirma a não integração

O Termo de Referência, em seu item 17.13.8, estabelece que a **solução ofertada** deve permitir integração com o firewall NGFW do CONTRATANTE, provendo troca de informações e segmentação dinâmica de rede, **contemplando, no mínimo, compatibilidade com os seguintes fabricantes: Check Point, Cisco, Fortinet e Palo Alto.**

Na diligência realizada por esse Tribunal, foi corretamente apontado que “os links fornecidos [...] descrevem conceitos de *third-party devices* classificados como *admission devices*, mas não detalham de forma explícita a integração com NGFWs específicos”.

Em resposta, a Compwire afirmou, em síntese, que:

- o **Huawei iMaster NCE-Campus** realiza integração com firewalls NGFW de forma “agnóstica a fabricante”, utilizando RADIUS/CoA/DM;
- qualquer equipamento que suporte RADIUS pode ser cadastrado como *Admission Device*, incluindo firewalls NGFW;
- o padrão RADIUS CoA/DM seria suportado, “em maior ou menor grau”, por todos os fabricantes citados.



A partir desses pontos, a Compwire tenta concluir que o NAC Huawei atenderia integralmente ao item 17.13.8. Como se demonstrará, tal conclusão **não se sustenta**.

Inversão indevida do objeto do edital

O objeto do edital, nesse ponto, é inequívoco: trata-se da **aquisição de solução NAC** que **já deve ser compatível** com o firewall NGFW do CONTRATANTE e, minimamente, com os fabricantes expressamente listados (Check Point, Cisco, Fortinet, Palo Alto).

A defesa da Compwire, entretanto, acaba por **inverter essa lógica**, ao condicionar o atendimento do requisito a que o firewall:

- funcione como cliente RADIUS (NAS) para o NCE;
- implemente extensões específicas de **RADIUS CoA/DM**, de acordo com a forma como o fabricante Huawei as utiliza.

Em outras palavras, a solução só seria considerada compatível se o **equipamento do CONTRATANTE** se adequar operacionalmente ao NAC fornecido pela Compwire.

Isso contraria a interpretação mais básica do item 17.13.8: Quem deve demonstrar capacidade de integração é **o NAC licitado**. O NAC é que precisa ter iniciativa e condições técnicas para se integrar com os firewalls citados na especificação técnica, e não o contrário.

A própria documentação citada não demonstra integração com NGFW específicos

Na resposta, a Compwire transcreve o conceito de *Admission Device* na arquitetura do iMaster NCE-Campus, segundo o qual:



“qualquer dispositivo de rede que suporte RADIUS pode ser cadastrado como um *Admission Device*, como um switch ou WAC [...]”

A partir daí, a empresa **conclui por conta própria** que um firewall NGFW “compatível com RADIUS” poderia atuar nesse papel.

Observe-se:

- A definição oficial exemplifica **switch** e **controladora wireless (WAC)**;
- A inclusão de “firewall NGFW” como *Admission Device* é **inferência da Compwire**, não afirmação inequívoca do fabricante Huawei;
- Em nenhum ponto da defesa são apresentados **manuals, notas técnicas ou guias de integração** que mencionem nominalmente como firewalls NGFW com integração certificada ao iMaster NCE-Campus:
 - Check Point,
 - Cisco,
 - Fortinet,
 - Palo Alto

Portanto, a documentação juntada apenas demonstra que o NAC atua como servidor RADIUS e que **qualquer dispositivo que “fale RADIUS” pode, em tese, ser cadastrado como ponto de admissão**, mas isso não comprova a **compatibilidade concreta** com os NGFW dos fabricantes exigidos no Termo de Referência.



RADIUS/CoA é extensão opcional e não pode ser imposto ao ambiente do CONTRATANTE

A Compwire afirma que “a integração é realizada através de protocolo padrão RADIUS (CoA/DM), e que o mesmo é padrão para todos os NGFW, incluindo Check Point, Cisco, Fortinet e Palo Alto”.

Contudo:

- RADIUS CoA/DM é uma **extensão de autorização dinâmica** do protocolo RADIUS, não uma obrigação técnica universal;
- O suporte a essas extensões depende de **implementação específica por fabricante, modelo e versão** de software dos equipamentos de rede.

Apesar disso, a Compwire não traz ao processo **qualquer prova** de que:

Os NGFW mencionados na especificação técnica aceite funcionar como *Admission Device* do NCE Huawei com todas as funcionalidades de CoA/DM e segmentação dinâmica que estão sendo descritas em termos genéricos.

Ao invés de comprovar a integração do NAC com os produtos listados no TR, a licitante **pressupõe** que os NGFW do TRT9:

- tem suporte integral às extensões RADIUS e entenderão atributos CoA/DM,
- está habilitado como “outros equipamentos” a se adequar ao NAC da Huawei,
- e poderá ser configurado para atuar como NAS do NAC.



Essa linha de raciocínio transfere ao CONTRATANTE o ônus e o risco tecnológico, o que é incompatível com o princípio da vinculação ao instrumento convocatório:

Quem deve se ajustar ao TR é a solução ofertada, e não a infraestrutura preexistente do órgão. O objeto do edital é o NAC. O NAC é que deve prover mecanismos de integração com os produtos listados e não ao contrário.

O edital exige compatibilidade mínima com fabricantes específicos, não mera interoperabilidade genérica

O Termo de Referência, ao listar expressamente os fabricantes Check Point, Cisco, Fortinet e Palo Alto, revela uma preocupação clara com **integrações específicas e consolidadas de mercado**, partindo do NAC, objeto deste edital, que terão incumbência e responsabilidade de se integrarem com os NGFW.

A resposta da Compwire, porém, limita-se a afirmar que:

- firewalls de terceiros são classificados genericamente como “Other” na documentação Huawei;
- Os fabricantes “em maior ou menor grau” implementam o padrão RFC de CoA/DM, viabilizando a interação com o NAC.

Novamente, trata-se de declarações **infundadas**, sem mencionar:

- indicação de modelos suportados de cada fabricante;
- guias oficiais de integração “Huawei iMaster NCE-Campus + [fabricante X]”;
- evidência de integrações mínimas do NAC com os fabricantes de NGFW.



Desse modo, permanece sem atendimento a exigência específica do item 17.13.8, que não se satisfaz com mera possibilidade teórica de interoperabilidade, mas demanda **compatibilidade efetiva e demonstrada** com NGFW dos fabricantes ali enumerados.

Quando se analisa a documentação dos principais fabricantes citados no TR, observa-se que:

Palo Alto Networks:

Usa o recurso **User-ID** para mapear IPs a usuários, integrando-se a diretórios (AD, LDAP), agentes e outros serviços; a integração de identidade se dá por agentes, monitoramento de logs e APIs, não simplesmente por tratá-lo como “NAS RADIUS CoA.

Fortinet (FortiGate):

Integra-se com soluções NAC (como FortiNAC) e com outros componentes da Security Fabric via conectores e **REST API**, sso-Attribute key, integrações via scripts de ssh, “dynamic address tags” e objetos dinâmicos de firewall para segmentação baseada em usuários/grupos.

Check Point:

Oferece **Identity Awareness**, que consome identidades de diversas fontes (RADIUS accounting, syslog, agentes, APIs) ou integrações com scripts que autenticam no gateway e populem informações de usuários. A própria documentação cita integração com NACs de terceiros por meio de **Identity Awareness Web API**, entre outros mecanismos

Ou seja:



- Cada fabricante de NGFW possui **arquiteturas específicas** para receber instruções de identidade e contexto de NAC;
- A integração avançada (segmentação dinâmica, grupos, políticas por usuário) geralmente é feita através de **métodos próprios (APIs, agentes, WebAPI, Fabric connectors, etc.)**, e não simplesmente tratando o NGFW como um “switch RADIUS” qualquer.

Transferência indevida de risco e incerteza operacional

A arquitetura descrita pela Compwire pressupõe que o firewall do CONTRATANTE e/ou listados no TR seja configurado como ponto de autenticação/enforcement, responsável por:

- encaminhar autenticações ao NCE via RADIUS;
- receber atributos de autorização, Security Groups e demais informações;
- implementar segmentação dinâmica a partir desses dados.

Na prática, isso significa condicionar o pleno funcionamento do NAC a uma série de hipóteses:

- capacidade do NGFW atual de operar como NAS dentro do modelo Huawei;
- suporte correto a CoA/DM;
- compatibilidade com o conceito de *Security Groups* do NCE;

Nenhuma dessas premissas é comprovada de forma objetiva na resposta da Compwire. Ao contrário: a solução é descrita em termos abstratos, com menções vazias a “qualquer dispositivo RADIUS” e “todos os



fabricantes mencionados”, sem demonstrar aderência ao **cenário concreto** do TRT9.

Assim, o que se apresenta é uma solução que **não atenderá ao Termo de Referência, na medida em que o firewall do CONTRATANTE e/ou mencionados no TR deva se moldar às necessidades do NAC Huawei**, situação que não foi comprovada nem pode ser exigida no edital, pois a licitação é do NAC, **não é uma licitação de NGFW**.

Um usuário que se autentica no ambiente do NAC, e é autorizado a utilizar a rede, precisa ter suas credenciais compartilhadas para o NGFW por iniciativa do próprio NAC, objeto desse edital, para evitar duplos logins, quando por exemplo, o usuário acessar a internet e atravessar o firewall.

O que propõem a Compwire, é que o firewall seja obrigado a enviar pedidos de autenticação como um switch, isso não faz o menor sentido considerando as exigências do edital. Se um usuário está autenticando no ambiente do NAC para entrar na rede, conseqüentemente, essa autenticação ainda não chegou no firewall.

O NAC, como solicitado na especificação, precisa informar ao firewall os atributos desse usuário já conhecido no NAC para evitar múltiplos logins. O NAC que precisa conceber a integração.

Fazendo uma analogia com a portaria de um prédio:

O NAC é a Recepção (Cérebro): Verifica quem é o visitante e suas credenciais.

- O Firewall é a Segurança dos Corredores/Salas (Controle de Tráfego): Controla o que o usuário pode acessar depois de entrar.



O Fluxo Correto (Proposto no Edital):

Um visitante chega na recepção:

1. O recepcionista verifica a identidade/credenciais.

Após a verificação:

2. A Recepção diz: "Pode entrar".

3. Simultaneamente, a Recepção avisa a Segurança Interna (Firewall) via API/Integração: "O visitante acabou de entrar, ele irá ao 5o andar.".

4. O visitante passa pela recepção e, quando chegar no corredor, o Segurança (Firewall) já sabe quem ele é.

O Fluxo Errado (Proposto pela Compwire na Diligência): A Compwire afirmou explicitamente: "O iMaster NCE atua como servidor RADIUS... enquanto o firewall NGFW é configurado como cliente RADIUS (NAS), denominado no contexto Huawei de 'Admission Device'". Nessa arquitetura:

1. O visitante entra pela porta, que fica aberta, sem controle de identidade..

2. O visitante caminha até o 5o andar, quando se encontra com a Segurança Interna (Firewall).

3. A segurança (Firewall agindo como NAS) pergunta quem ele é, e o encaminha para a Recepção (NAC), para fazer a verificação das credenciais.

4. Só então, depois de chegar no 5o andar, é que ele vai até a recepção para se identificar.



Portanto, a proposta deve ser desclassificada por não comprovar objetivamente, via documentação técnica exigida (item K), a aderência aos subitens 17.13.8.1.1 a 17.13.8.1.4 do edital.

Caso o TRT9 entenda em sentido diverso, entende-se que deve ser solicitado em sede de diligência para a recorrida que apresente, em prazo hábil, o **Guia de Configuração (Admin Guide)** oficial da fabricante Huawei que contenha a *string* "Palo Alto", "Cisco" ou "Check Point" demonstrando a tela de configuração da integração. Haja vista que a apresentação de manuais genéricos corrobora justamente o contrário, ou seja, comprova a inexistência da funcionalidade específica.

Desta feita, admitir a proposta sem esta prova configura violação aos princípios da licitação, notadamente ao princípio da vinculação ao edital e ao dever de julgamento objetivo, o que compromete a isonomia entre os concorrentes e impede a seleção da proposta realmente mais vantajosa para a Contratante.

Em respeito ao edital e à legislação aplicável, impõe-se, portanto, a desclassificação da proposta que não apresentou comprovação satisfatória, sob pena de prejuízo ao interesse público e nulidade do ato adjudicatório por inobservância das normas do certame

V. DA VINCULAÇÃO AO EDITAL, DA LEGALIDADE, DO JULGAMENTO OBJETIVO DAS PROPOSTAS E DA QUEBRA DE ISONOMIA:



É cediço que a participação no Pregão é um direito conferido ao particular, mas que resulta em obrigações que o vincula, gera compromissos com os concidadãos e por conseguinte ao Estado.

O Edital é claro e vincula todos os licitantes. É a lei da licitação no caso concreto, não sendo facultado à Administração usar de discricionariedade para desconsiderar determinada exigência prevista em lei, de ampla e irrestrita aplicação, bem como do instrumento convocatório.

Do ponto de vista jurídico e contratual, as fragilidades técnicas acima destacadas revelam um possível descompasso entre a proposta da Compwire e as exigências vinculantes do edital.

Pelo princípio da vinculação ao instrumento convocatório, a Administração está estritamente vinculada aos termos do edital e do Termo de Referência. Da mesma forma, os licitantes devem atender fielmente a essas especificações.

Em tal prol, ressalte-se lição do administrativista MARÇAL JUSTEN FILHO³:

“Depois de editado o ato convocatório, inicia-se a chamada fase externa da licitação. Os particulares apresentam as suas propostas e documentos, que serão avaliados de acordo com os critérios previstos na Lei e no ato convocatório. Nessa segunda fase, a Administração verificará quem, concretamente, preenche mais satisfatoriamente as condições para ser contratado. Também nessa etapa se exige o tratamento isonômico. Trata-se, então, da isonomia na execução da licitação. Todos os interessados e participantes merecem tratamento equivalente.”

³. [3] JUSTEN FILHO, Marçal. Comentários à Lei de Licitações e Contratos Administrativos. 15ª ed. São Paulo: Dialética, 2012. p. 61.



Se a solução ofertada não contempla a alta disponibilidade nos moldes requeridos – isto é, não provê dois appliances virtuais NAC redundantes com funcionamento concomitante e failover sem interrupção –, então há inadequação ao edital. Aceitar tal proposta incorreta violaria o princípio supracitado, pois significaria abrandar uma exigência técnica expressa, em prejuízo da isonomia e da objetividade da seleção.

Como é consabido, aquele que participa da licitação tem o dever jurídico de atentar para todas as suas exigências.

Sobre o tema, assevera JOSÉ DOS SANTOS CARVALHO FILHO⁴:

“A vinculação ao instrumento convocatório é garantia do administrador e dos administrados. Significa que as regras traçadas para o procedimento devem ser fielmente observadas por todos. Se a regra fixada não é respeitada, o procedimento se torna inválido e suscetível de correção na via administração ou judicial. O princípio da vinculação tem extrema importância. Por ele, evita-se a alteração de critérios de julgamento, além de dar a certeza aos interessados do que pretende a Administração. E se evita, finalmente, qualquer brecha que provoque violação à moralidade administrativa, à impessoalidade e à probidade administrativa. (...) Vedado à Administração e aos licitantes é o descumprimento das regras de convocação, deixando de considerar o que nele se exige, como, por exemplo, a dispensa de documento ou a fixação de preço fora dos limites estabelecidos. Em tais hipóteses, deve dar-se a desclassificação do licitante, como, de resto, impõe o art. 48, I, do Estatuto”. (grifos apostos)

⁴. CARVALHO FILHO, José dos Santos. Manual de Direito Administrativo. 25ª edição. Editora Atlas, 2012, p. 244.



Além da análise técnica, é preciso ressaltar as consequências jurídicas de aceitar-se uma solução que não cumpre o requisito do edital. No regime das licitações públicas, vigora o princípio da vinculação ao instrumento convocatório, segundo o qual os termos do edital vinculam estritamente tanto a Administração quanto os licitantes. Ou seja, a Administração não pode descumprir ou relevar uma exigência previamente estabelecida no edital sem ferir a legalidade do certame.

No caso em análise, o item 17.11.25 é parte integrante das regras do jogo (“lei interna do certame”), de modo que proposta que não o atenda deve ser desclassificada. Admitir a continuidade da solução Huawei não aderente significaria afastar-se do edital, violando o dever de observância estrita das condições editalícias.

Ademais, à luz do princípio da busca pela proposta mais vantajosa para a Administração, é questionável considerar vantajosa uma solução que, tecnicamente, não assegura o nível de disponibilidade e continuidade demandado.

A alta disponibilidade sem interrupção de serviços não é um capricho ou um requisito aleatório, mas um requisito essencial para garantir a segurança operacional da rede do TRT9.

Uma arquitetura que falha nesse aspecto representa risco de indisponibilidade do NAC (com impactos em todo acesso à rede e conformidade de segurança), o que poderia acarretar prejuízos administrativos e necessidade de intervenções corretivas durante a vigência contratual.

Em outras palavras, a proposta da Compwire, ao economizar em redundância (ofertando single-node com failover indireto), diminui a confiabilidade da solução, potencialmente gerando custos ocultos e contratempos futuros – o oposto do que seria a proposta mais vantajosa.



A Administração Pública deve selecionar a solução que melhor atenda integralmente os requisitos. Qualquer concessão indevida em um ponto crucial como disponibilidade pode inclusive ser objeto de impugnação por outros licitantes ou de questionamento pelos órgãos de controle.

Adicionalmente, vale invocar o princípio da busca pela proposta mais vantajosa para a Administração. A legislação estabelece que a finalidade da licitação é selecionar a proposta mais vantajosa ao interesse público, garantindo a observância da igualdade entre os proponentes.

Uma proposta que falha em atender um requisito técnico essencial do edital não pode ser considerada a mais vantajosa, mesmo que tenha apresentado, por exemplo, menor preço. A vantagem aqui não se mede apenas em termos econômicos imediatos, mas principalmente em adequação ao objeto pretendido.

A licitação visa permitir a participação do maior número possível de pretendentes a contratar com a Administração Pública, **em um processo seletivo que lhes permita igualdade de condições**, fazendo com que o Poder Público possa pactuar com aquele que lhe ofereça melhores condições técnicas e econômicas, com a segurança exigida.

Qualquer desvio desse rumo, que vise ou venha a beneficiar um proponente em detrimento dos demais, acarretará infração à ordem econômica.

O TCU no **Acórdão nº 1.533/2006** – Plenário, ratificado pelo Acórdão n.º 776/2008 – Plenário (modificado pelo Acórdão 3.069/2008-Plenário), reconheceu que:

“2. Na busca da proposta mais vantajosa para a Administração não se pode relegar a um segundo plano os princípios básicos do procedimento licitatório e da Administração Pública, não se podendo cogitar sobreposição



de princípios licitatórios. 3. A conduta dos agentes públicos deve atentar para o disposto na regra legal e nas condições do ato convocatório, devendo todos os licitantes receber tratamento idêntico. 4. A escolha da proposta mais vantajosa deve ser apurada segundo os critérios objetivos definidos no edital e não com base na escolha dos julgadores em considerar válida a proposta pela própria vantagem que ela traria para a Administração.” (grifo nosso)

Destarte, ainda que possa haver diferença de preço entre as propostas, tal fato não pode ser utilizado como justificativa para relegar as regras do edital, aceitando proposta que não atende a exigência do edital, passar por cima da lei, beneficiar licitante com nítida quebra de isonomia e afronta a legalidade, a vinculação, a moralidade e o julgamento objetivo.

Escolher uma solução incapaz de medir a experiência do usuário conforme delineado significa que o Tribunal não obterá a funcionalidade desejada – o que configura um resultado menos vantajoso, podendo comprometer a eficiência do serviço de TI no futuro.

Consequência lógica, a melhor proposta é aquela que atende plenamente às necessidades do edital. Contrapartida, uma solução incompleta frustra esse objetivo e, portanto, não deve ser aceita, sob pena de contrariar o interesse público buscado com a contratação.

O Termo de Referência, ao exigir HA sem interrupção de serviços no NAC, criou uma obrigação de resultado específico que a contratada deve cumprir.

Portanto, é imperativo zelar para que a contratação respeite estritamente o escopo previsto no edital. Abrir exceção para a Huawei/Compwire – tolerando um não atendimento de requisito – configuraria



tratamento díspar em relação aos demais concorrentes que se esforçaram para cumprir integralmente o edital ou que poderiam ter ofertado soluções diferentes caso soubessem da possibilidade de flexibilização.

Em linhas gerais, o respeito ao edital garante isonomia e transparência, assegurando que o procedimento siga critérios objetivos e iguais para todos. De tal sorte, relevar a não conformidade da solução Huawei afronta esse princípio basilar, potencialmente maculando a lisura da licitação.

Em conclusão, a análise técnico-jurídica evidencia que a solução Huawei iMaster NCE-Campus/CampusInsight “*conforme proposta da Compwire*” não atende ao item 17.11.25 do edital, pois não disponibiliza agentes ou sondas independentes instaláveis em qualquer ponto de rede que a Contratante deseje, baseando-se apenas em telemetria de equipamentos proprietários e limitando a flexibilidade de monitoração.

Permanecer com essa opção violaria o princípio da vinculação ao instrumento convocatório e da isonomia, além de comprometer a seleção da proposta mais vantajosa para a Administração, princípios estes fundamentais no processo licitatório.

Assim, impõe-se, do ponto de vista técnico e jurídico, o reconhecimento da inabilitação ou desclassificação dessa proposta, resguardando-se a observância estrita do edital e o interesse público pretendido com a contratação.

Diante do exposto, conclui-se que a arquitetura NAC em **single-node com servidor de arbitragem**, conforme proposta pela Compwire, **não satisfaz os requisitos técnicos de alta disponibilidade estabelecidos nos itens 17.13.1.6 a 17.13.1.8 do edital do TRT9.**

VI. DO PEDIDO



Diante do exposto, requer a Recorrente:

1. O conhecimento e provimento do presente Recurso Administrativo;
2. Requer a inabilitação e **desclassificação imediata** da proposta da empresa **COMPWIRE** por descumprimento de requisitos obrigatórios do TR nos seus itens **17.11.25, 17.13.1.6 a 17.13.1.8 e 17.13.8.1 a 17.13.8.4.**
3. Requer a continuidade da análise das propostas remanescentes, conforme a ordem de classificação do certame.

Nestes termos.

Pede deferimento.

Porto Alegre, 28 de novembro de 2025.

L8 GROUP S.A.