



AO ILUSTRÍSSIMO SENHOR ALEXANDRO FURQUIM, PREGOEIRO DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO – TRT9.

Pregão Eletrônico nº 90022/2025.

COMPWIRE INFORMÁTICA LTDA., pessoa jurídica de direito privado, inscrita no CNPJ/ME sob o nº 01.181.242/0001-91, com sede na Rua Comendador Roseira, nº 352, Prado Velho, Curitiba/PR, CEP 80.215-210, doravante denominada 'Recorrida' ou simplesmente 'COMPWIRE', comparece, respeitosamente, com fulcro no Item 12 e seguintes do Edital, por meio de seu representante legal ao final subscrito, para oferecer as presentes

CONTRARRAZÕES AO RECURSO ADMINISTRATIVO

movido pela ROOST LTDA, doravante denominada 'Recorrente' ou simplesmente 'Roost', em face da declaração de vencedora operada em favor da COMPWIRE no curso do Pregão Eletrônico nº 90022/2025, pelas razões de fato e de direito a seguir aduzidas.

I. Breve Síntese Processual:

1. O Edital de Pregão Eletrônico 90022/2025 tem como 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”*.

2. Após a Sessão Pública de Pregão, a COMPWIRE apresentou a proposta mais vantajosa para o certame. Ato contínuo, apresentou toda a documentação de qualificação nos moldes exigidos pelo Edital, sagrando-se corretamente vencedora do Lote após sua habilitação.

3. Vale dizer que sua declaração de vencedora foi objeto, ainda, de diligências pretéritas para a comprovação de funcionalidades ora questionadas em recurso administrativo, que foram devidamente comprovadas e levaram à escoreita declaração de vencedora da ora Recorrida.

4. Não obstante, irresignada com o resultado, a licitante ROOST LTDA manejou Recurso Administrativo, aduzindo o suposto não atendimento e ausência de comprovação das funcionalidades listadas nos itens 17.11.25, 17.13.1.8, 17.13.5.15, 17.13.8.1, bem como um suposto descumprimento ao item 'k' do Anexo I.

II. Comprovação de adequação e atendimento da solução ofertada em relação à experiência do usuário – Item 17.11.25 do Anexo:

5. A recorrente afirma que a solução Huawei iMaster NCE-Campus/CampusInsight não atenderia ao item 17.11.25, sustentando que o edital exigiria sondas dedicadas, agentes instaláveis ou geração de tráfego sintético:

“A solução ofertada (Huawei iMaster NCE-Campus / CampusInsight) (i) baseia-se exclusivamente em telemetria dos switches e APs Huawei; (ii) não possui agentes instaláveis em computadores, servidores ou locais arbitrários; (iii) não possui sondas ativas dedicadas (hardware ou software); (iv) não gera tráfego sintético para medir latência, perda, jitter ou disponibilidade a partir de um ponto específico da rede; (v) só permite medições nos locais onde existam equipamentos Huawei, limitando completamente a escolha dos “pontos de monitoramento” previstos no edital.”

6. Todavia, tal interpretação não corresponde ao que está efetivamente escrito no Termo de Referência, configurando leitura indevidamente restritiva e tecnicamente equivocada.

7. O item 17.11.25 exige que o monitoramento da experiência do usuário possa ser realizado por hardware ou software instalados em pontos da rede definidos pela Contratante. O texto não determina quais equipamentos devem exercer essa função, não impõe a obrigatoriedade de sondas independentes, não exige agentes instaláveis em computadores e não estabelece que as medições devam ser feitas por meio de tráfego sintético ou probes externos.

8. O fato é, a exigência do TR trata da **capacidade de posicionar pontos de monitoramento**, e não da adoção de um tipo específico de tecnologia.

9. Desta maneira a solução Huawei permite o monitoramento da experiência do usuário por meio da sua própria arquitetura, que pode ser instalada onde a Administração necessitar, passando a atuar como pontos de coleta e monitoramento, conforme previsto no TR.

10. Essa funcionalidade ocorre por meio da coleta de dados dos equipamentos de rede por meio de telemetria, que fornecem a ferramenta iMaster NCE-Campus/CampusInsight as informações necessárias para a análise de experiência do usuário. É o que se denota da documentação oficial do produto:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100331202&id=EN-US_TOPIC_0230015413

11. Denota-se de trecho da documentação que: *“Switches can report data to iMaster NCE-CampusInsight for intelligent switch fault diagnosis and user experience analysis, thereby implementing intelligent O&M”,* o que é traduzido como *“os switches podem enviar dados ao iMaster NCE-CampusInsight para o diagnóstico inteligente de falhas e análise da experiência do usuário, implementando, dessa forma, uma O&M inteligente”*.

12. Em paralelo, o edital exige medir a experiência do usuário, o que a solução Huawei executa:

- (i) Por meio da telemetria integrada;
- (ii) Por meio da observação detalhada da jornada do cliente;
- (iii) Com métricas de desempenho de rede diretamente associadas à experiência real do usuário
- (iv) A telemetria **opera de maneira ativa**, onde cada equipamento envia informações para a gerência em tempo real;
- (v) Pelo fato de cada equipamento realizar esse envio de informações, não existe a dependência de um equipamento central, assim também não existe um ponto único de coleta e de falha.

13. O CampusInsight utiliza telemetria avançada e contínua desses equipamentos para medir a experiência do usuário em cada local definido. Conforme pode ser verificado na documentação oficial:

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100331202&id=EN-US_TOPIC_0000001238746243

“Huawei's intelligent O&M solution uses Telemetry technology to enable network devices to send O&M data (such as device performance indicators and terminal logs) to Huawei's intelligent network analysis platform iMaster NCE-CampusInsight”

“A solução de O&M inteligente da Huawei utiliza a tecnologia de Telemetria para permitir que dispositivos de rede enviem dados de O&M (como indicadores de desempenho do dispositivo e logs de terminais) para a plataforma de análise de rede inteligente da Huawei, o iMaster NCE-CampusInsight”.

14. Sendo assim, a alegação de que apenas sondas ativas atenderiam o edital é equivocada e desprovida de respaldo técnico ou normativo.

15. Por fim, a Recorrente alega que a solução Huawei limitaria a capacidade da Administração de instalar pontos de medição onde desejar. Ocorre que:

- (i) os equipamentos da solução podem ser instalados nos pontos estratégicos definidos pela Administração;
- (ii) o TR não determina que esses “pontos de medição” devam ser sondas independentes;
- (iii) tampouco exige que a solução funcione fora da arquitetura contratada ou em redes legadas de terceiros.

16. O TR trata de medições dentro da solução contratada, e não de sondas independentes para redes externas ou segmentos não contemplados no projeto. Trata-se, novamente, de tentativa de desvirtuar o requisito para criar a aparência de não conformidade, de modo que não merece prosperar as alegações da Recorrente.

III. Comprovação da solução ofertada em relação à disponibilidade da solução de NAC (assumir todas as operações sem interrupção) – Item 17.13.1.8 do Anexo I do Termo de Referência:

17. A recorrente sustenta que a arquitetura Huawei iMaster NCE-Campus não atenderia ao item 17.13.1.8, alegando que o modelo single-node active/standby implicaria interrupção dos serviços no momento do failover:

“A arquitetura ofertada (i) opera em modo single-node com um servidor ativo, um standby e um nó de arbitragem; (ii) essa arquitetura é ativo/passivo – não há operação simultânea dos dois appliances; (iii) a documentação oficial da Huawei confirma que existe interrupção de serviços durante o processo de failover, até que o standby seja

promovido a ativo; (iv) o sistema depende de reinicialização de processos e “automatic switchover”, caracterizando tempo de recuperação e não continuidade imediata.”

18. Contudo, essa interpretação é incorreta, ignora o funcionamento real da solução, distorce a documentação oficial e tenta impor ao edital requisitos que não constam do Termo de Referência.

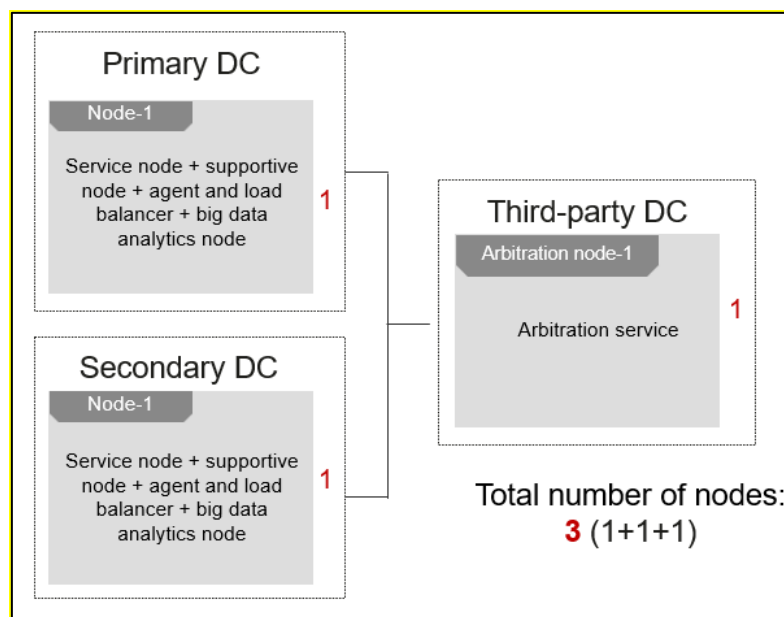
19. A argumentação da recorrente baseia-se em interpretações parciais e equivocadas da arquitetura Huawei iMaster NCE-Campus, bem como em uma tentativa de induzir, de maneira insidiosa, o entendimento de que o TR exigiria uma arquitetura exclusivamente em modo ativo/ativo, quando, na realidade, o que o edital exige é a não interrupção dos serviços em caso de falhas, resultado que pode ser alcançado por diferentes arquiteturas de alta disponibilidade, inclusive a ofertada.

20. Conforme descrito na proposta, a solução ofertada é composta por dois servidores idênticos, ambos dimensionados para suportar integralmente a solução instalada, garantindo desempenho e estabilidade. Além disso, inclui-se um terceiro servidor, de caráter arbitrário, cuja função é executar o switchover automático em caso de falhas, assegurando a continuidade operacional do ambiente. Conforme abaixo:

Servidores Primário e Secundário	
Especificações - TaiShan 200(Model2280)	
CPU	2*Kunpeng 920-32Core@2.6GHz CPU
Memory	4*32G Memory,4*1920GB SSD,Raid(2G cache)+SuperCap
Ports	2*4 GE+3*2 25GE SFP28
Power	2*900W AC 1+1 B ackup
Peso	32 kg
Dimensões	2U (86.1 mm x 447 mm x 748 mm)

Servidor Arbitrário	
Especificações - TaiShan 200(Model2280)	
CPU	2*Kunpeng 920-32Core@2.6GHz CPU
Memory	2*32G Memory,4*1920GB SSD,Raid(2G cache)+SuperCap
Ports	2*4 GE+3*2 25GE SFP28
Power	2*900W AC 1+1 B ackup
Peso	32 kg
Dimensões	2U (86.1 mm x 447 mm x 748 mm)

21. Nesta configuração, os dois servidores, denominados primário e secundário, possuem a mesma configuração de hardware, os mesmos esquemas de serviço e demais componentes operacionais. Conforme estabelecido na documentação, essa solução fornece sincronização em tempo real das bases de dados entre o site primário e o secundário, garantindo alta disponibilidade da plataforma e continuidade operacional mesmo diante de falhas no nó principal:



22. Em caso de falhas, o nó arbitrário atua imediatamente para que os serviços sejam automaticamente chaveados para o servidor secundário, garantindo a continuidade da operação e, consequentemente, o restabelecimento dos serviços do iMaster NCE-Campus:

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

Table 1 HA solutions for a DR system

Protection Solution	Description
Active/standby switchover	Two copies of iMaster NCE-Campus with the same hardware configurations, service schemes, and other configurations are deployed at the primary and secondary sites, respectively. Data in each database at the primary site is synchronized to the secondary site in real time based on the corresponding synchronization policy. If the primary site fails, users can immediately manually start the secondary site or the arbitration service automatically starts the secondary site to quickly restore iMaster NCE-Campus services.

23. De acordo com o descrito na solução de alta disponibilidade, no caso de hardware com proteção de redundância, os serviços são automaticamente chaveados para o site que permanece em operação normal, assegurando o desempenho contínuo e sem interrupção do sistema operacional do iMaster NCE-Campus e de seus serviços de aplicação.

24. Ainda, a proteção de redundância de hardware e dados oferece chaveamento instantâneo sem detecção pela camada de aplicação, conforme descrito em documentação:

Table 1 Hardware HA protection solutions

Protection Type	Protection Solution
Hardware redundancy/Data protection	Server: Power modules and fans work in redundancy mode, NICs work in 1+1 bonding protection mode, the disk cache is disabled, and RAID card cache with battery backup unit (BBU) for power-off protection is supported. <u>Hardware redundancy protection enables instant switchover, which is not detected by the application layer.</u>

25. Por fim, a fim de rechaçar a argumentação da Recorrente, indica-se que a documentação oficial do produto ofertado também prevê que “*The switchover does not affect services*” – “*A comutação não afeta os serviços*”:

Data protection	Backup and restoration: The backup and restoration function is provided for data. Data can be backed up periodically or before major changes. If iMaster NCE-Campus data is abnormal, backup files can be used to quickly restore the data to the normal state. Automatic database switchover: Database nodes are deployed in master/slave mode. In normal situations, the database on the master node is readable and writable, while the database on the slave node is read-only. If a service process on the primary node fails, iMaster NCE-Campus automatically switches to the database on the secondary node to provide services. <u>The switchover does not affect services.</u>
-----------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

26. Referida característica do produto reforça que, em caso de falhas no nó primário, a operação dos serviços é mantida, havendo chaveamento automático para a base de dados do servidor secundário.

27. A recorrente cita trechos da documentação que tratam de *process restart* e *automatic switchover*, mas o faz de maneira fragmentada e fora de contexto. O trecho sobre *process restart* refere-se exclusivamente à recuperação interna de processos isolados, não ao mecanismo de failover entre os dois servidores. Já o trecho sobre *automatic switchover* descreve o cenário em que o sistema detecta uma falha e aciona imediatamente o *standby*.

28. Assim, a alegação de indisponibilidade durante o failover não encontra respaldo na documentação, contradiz o trecho oficial que afirma ausência de impacto sobre os serviços e tenta reinterpretar equivocadamente o conceito de HA previsto no TR.

29. A solução ofertada atende plenamente ao item 17.13.1.8, garantindo que, na falha de qualquer componente, o outro assuma “todas as operações e funcionalidades sem interrupção dos serviços”, conforme exigido.

30. Portanto, a afirmação de que a solução não atende ao edital é improcedente, tecnicamente incorreta e juridicamente insustentável.

IV. Suporte a navegadores (Firefox e Chrome) – Item 17.13.5.15:

31. A recorrente afirma que não teria sido apresentada comprovação técnica para o suporte do portal de visitantes aos navegadores Firefox e Google Chrome, alegando que a evidência enviada consistiria apenas em uma carta do fabricante, a qual não seria aceita pelo edital. Entretanto, essa alegação não corresponde aos fatos e parte de uma interpretação incorreta do Termo de Referência e do procedimento de diligência conduzido por este Tribunal.

32. Primeiro, é importante esclarecer que a comprovação técnica foi sim apresentada na matriz ponto a ponto, por meio de documentação oficial do fabricante Huawei, conforme solicitado no item “k” do ANEXO I. A recorrente omite este fato e tenta fazer crer que a única evidência fornecida teria sido a carta, o que é falso.

33. Em segundo lugar, a própria equipe julgadora do TRT9, ao analisar inicialmente a documentação, solicitou diligência complementar para reforço da comprovação. A diligência foi atendida em duas etapas:

1) Carta oficial do fabricante Huawei

A carta foi apresentada como primeira resposta, esclarecendo formalmente a compatibilidade do portal com os navegadores especificados. Em momento algum o edital proíbe a apresentação de cartas ou declarações oficiais.

Uma carta emitida pelo fabricante, assinada e oficial, é meio absolutamente legítimo de comprovação, especialmente quando ratifica informações presentes em documentação técnica.

2) Complementação com documentação e evidências práticas

Atendendo integralmente à diligência, foram encaminhados prints dos testes realizados demonstrando funcionalidade plena do portal nos navegadores Firefox e Chrome, com descrições técnicas complementares e procedimentos validados com base na própria interface da solução.

34. Ou seja, além da carta inicial, houve comprovação técnica objetiva, visual, operacional e perfeitamente alinhada ao que o edital exige.

35. Além disso, a diligência existe justamente para permitir que a Administração verifique requisitos de forma complementar e suficiente. A nobre equipe técnica do Tribunal aceitou a diligência, o que demonstra que o requisito foi devidamente comprovado, as evidências foram consistentes e satisfatórias e não houve qualquer violação ao edital.

36. A recorrente tenta forçar uma restrição inexistente no edital e desconsidera completamente o procedimento legítimo de diligência já concluído por este Tribunal, cujo objetivo é justamente sanar dúvidas técnicas, o que foi acatado com sucesso.

37. Assim, o item 17.13.5.15 foi plenamente atendido, e a contestação da recorrente carece de fundamento técnico e jurídico, devendo ser rejeitada.

V. Item 17.13.8.1 – Integração do NAC com NGFW (Check Point, Cisco, Fortinet e Palo Alto):

38. A Recorrente afirma que a solução Huawei iMaster NCE-Campus não atenderia ao item 17.13.8.1, alegando ausência de integração nativa com NGFW dos fabricantes Check Point, Cisco, Fortinet e Palo Alto, e baseando-se em supostos “testes laboratoriais” e exigências técnicas que não constam do Termo de Referência.

39. Essa argumentação, além de tecnicamente equivocada, desvirtua o conteúdo do edital, ignora a arquitetura padrão de integração NAC e NGFW adotada globalmente e omite o fato de que o TRT9 já realizou diligência sobre esse exato ponto e acatou a resposta da Compwire, reconhecendo o atendimento ao requisito.

40. Antes de tudo, é preciso destacar que o edital não exige integração proprietária, tampouco menciona, em qualquer trecho, a necessidade de utilização de APIs exclusivas, plugins, templates de fabricantes, conectores específicos (como User-ID, pxGrid, RSO, FSSO, Identity Awareness) ou certificações conjuntas.

41. O requisito previsto no item 17.13.8 é claro: o NAC deve integrar-se funcionalmente com NGFW dos fabricantes listados, de modo a permitir segmentação dinâmica, compartilhamento de informações e troca de contexto.

42. Esses requisitos são atendidos por padrões amplamente adotados, como RADIUS, RADIUS Accounting e CoA/DM, protocolos que constituem justamente a base técnica de integração entre NAC e firewalls de múltiplos fabricantes, incluindo Check Point, Cisco, Fortinet e Palo Alto.

43. A documentação oficial da Huawei explicita que qualquer dispositivo de rede que suporte RADIUS pode ser cadastrado como Admission Device, incluindo firewalls NGFW, que passam a receber do NAC atributos de autorização, grupos de segurança, VLANs e demais parâmetros necessários à aplicação das políticas dinâmicas previstas no edital.

44. Em complemento, vale destacar que a coleta de identidade, por exemplo do firewall Checkpoint, não se limita a API mas também pode ser realizada via RADIUS Accounting. Conforme pode ser verificado via documentação pública do fabricante:

Identity Sources

Check Point Identity Awareness works well in these environments. We connect to these external components to map the users or devices and their IP addresses that define Access Role elements and to gain additional metadata from the source.

Directory Services	Agents	RADIUS Accounting or Identity Awareness Web API	Syslog Integrations	Integrations with Third Party APIs
Active Directory NetIQ eDirectory	Check Point Remote Access Client Check Point Identity Agent Check Point Terminal Server Agent	Cisco Wireless LAN Controller Cisco ISE Aruba ClearPass ForeScout CounterAct F5 Pulse Secure SilverFort SecurePush	Cisco ASA Fortinet	Cisco TrustSec Pulse Secure

As you can see, Check Point has several methods for connecting to various identity sources such as using RADIUS accounting and parsing syslog messages. In addition, other vendors and third parties can manage identity elements using our Check Point Identity Awareness Web API.



<https://www.checkpoint.com/downloads/products/cp-identity-awareness-reference-architecture-best-practices.pdf>

45. Em outra validação relacionada à integração com o firewall Fortinet, constatou-se, por meio de questionamento realizado em fórum oficial da própria fabricante, que a integração entre o FortiGate e o iMaster NCE-Campus foi tratada como caso resolvido, indicando que a interoperabilidade ocorre por meio do protocolo RADIUS, exatamente conforme previsto pela arquitetura Huawei.



46. Essa confirmação é reforçada pela documentação oficial disponibilizada, que aponta o uso de RADIUS como mecanismo adequado para permitir a comunicação entre o NAC e o firewall, validando, portanto, a compatibilidade exigida no edital.

47. Documentação indicativa do uso do Radius:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/85730/radius-single-sign-on-rsso-agent>

**AEK** 
SuperUser
In response to Sadhi_Jayz

Created on
12-08-2024 09:25 AM

 SOLVED


✓ Hi Sadhi
Basically you keep authenticating with your NAC via RADIUS, and FGT listens for RADIUS accounting records, and so FGT will record the user info (user, group, IP), and you can use them in your firewall rules. You can start here.
<https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/85730/radius-single-sign-on-rsso-agent>

But I guess this is not the unique existing solution for your requirement.
For example there should be a solution where you pull (or forward) login events from your (RADIUS) NAC to your FAC, and then use them on your FortiGate. Or you can configure your NAC to authenticate users from your FAC, and then use them on your FortiGate.
Hope it helps.
[View solution in original post](#)

48. Questionamento no fórum oficial da fabricante:

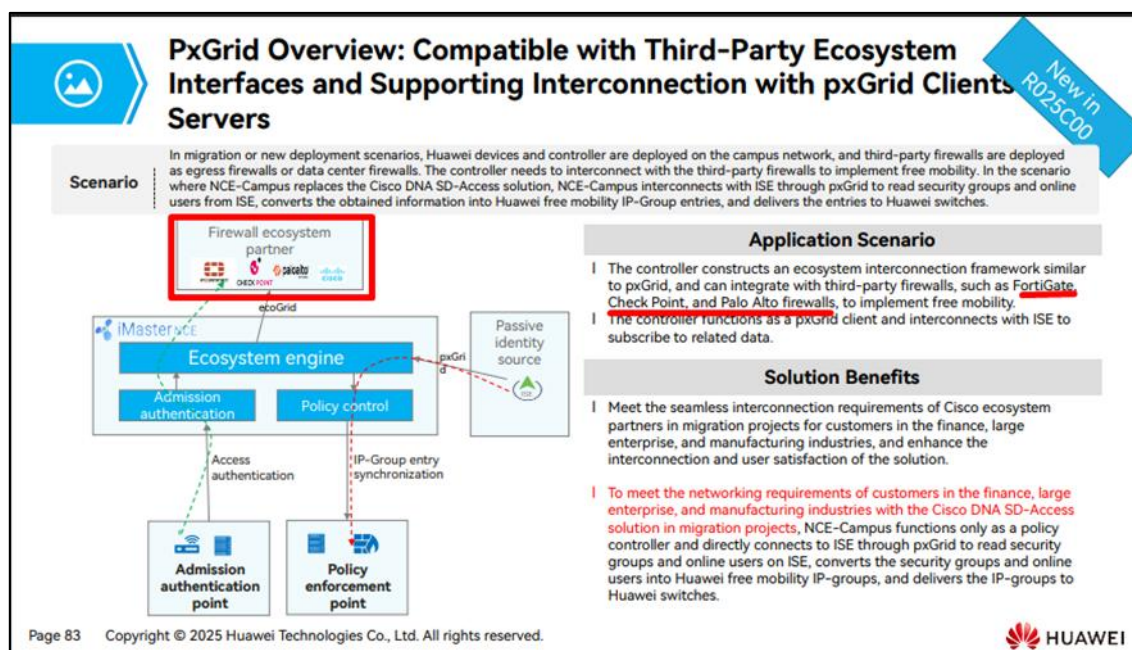
<https://community.fortinet.com/t5/Support-Forum/Integration-of-FortiGate-Huawei-NAC-and-FortiAuthenticator-for/m-p/363243>

49. A segmentação dinâmica e a troca contextual entre NAC e NGFW também são plenamente atendidas. O iMaster NCE-Campus utiliza Security Groups para classificar usuários e dispositivos, comunicando ao firewall, via RADIUS, o grupo ao qual cada usuário pertence.

50. O NGFW então aplica automaticamente as políticas correspondentes, procedimento compatível com os mecanismos de identificação e associação presentes em firewalls de Check Point, Cisco, Fortinet e Palo Alto. Esse modelo, além de atender ao TR, representa o padrão de mercado para interoperabilidade entre NAC e firewalls de múltiplos fabricantes.

51. Em adição, em documentação oficial e pública do fabricante Huawei, é apresentado a integração dos firewalls listados Check Point, Cisco, Fortinet e Palo Alto. Conforme abaixo:

<https://support.huawei.com/enterprise/en/doc/EDOC1100528950>



52. A recorrente também menciona supostos “testes laboratoriais” que teriam demonstrado ausência de integração. Contudo, tais testes não possuem qualquer validade técnica ou jurídica. A recorrente não apresenta qualquer evidência verificável desses testes.

53. Não há descrição de ambiente, topologia, versões de firmware, licenças utilizadas, parâmetros de configuração, logs, capturas de pacotes, resultados comparativos ou documentação que permita sequer compreender qual cenário teria sido testado. Trata-se de alegação genérica, desprovida de qualquer elemento técnico mínimo que permita aferir autenticidade, metodologia ou validade dos procedimentos supostamente realizados.

54. Dessa forma, as conclusões apresentadas não possuem validade técnica e não podem ser utilizadas como subsídio para qualquer análise séria. São alegações sem metodologia, sem documentação, sem vestígios de rastreabilidade e, portanto, sem credibilidade.

55. Importante reforçar que a **diligência já reconheceu a adequação da explicação e considerou satisfatória a demonstração de integração por meio de protocolos padrão**. Em outras palavras, o entendimento técnico do próprio Tribunal foi no sentido de que a solução ofertada atende ao item 17.13.8.1, não havendo exigência editalícia que determine apresentação de telas ou menções nominais a cada fabricante listado.

56. Assim, a tentativa da recorrente de reabrir discussão sobre ponto já devidamente esclarecido carece de fundamento técnico e jurídico. A solução Huawei atende ao edital, integra-se aos NGFW especificados utilizando protocolos abertos amplamente suportados e fornece segmentação dinâmica e troca de informações conforme solicitado. Portanto, a alegação de não conformidade não merece prosperar.

VI. Pleno atendimento da Recorrida aos requisitos do Edital e Termo de Referência – Arguições da Recorrente pautadas em deturpações das cláusulas do Edital – Necessidade de manutenção da declaração de vencedora – Critério de economicidade e obtenção da proposta mais vantajosa:

57. Conforme se vê, a COMPWIRE atendeu plena e satisfatoriamente todas as condições do Edital, sendo que a irrisignação da Recorrente não passa de uma tentativa frustrada de deturpar as cláusulas previstas pelo instrumento convocatório, em vista de não ter conseguido apresentar o menor preço para a licitação.

58. Fato é que COMPWIRE atende integralmente a todas as exigências e especificações do Edital e Termo de Referência, de modo que deve ser mantida sua declaração de vencedora à luz do princípio da obtenção da proposta mais vantajosa

59. Frisa-se que a obtenção de maior vantajosidade se trata de um princípio no curso do processo de contratação, por meio da economicidade:

“Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

60. O vantajosidade é ainda um dos objetivos buscados no processo licitatório, nos termos do art. 11, inc. I, da Lei nº 14.133/21:

“Art. 11. O processo licitatório tem por objetivos:

I - assegurar a seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração Pública, inclusive no que se refere ao ciclo de vida do objeto;

61. A necessidade da obtenção da maior vantajosidade possível no valor a ser dispendido pela Administração Pública em uma contratação é de extrema relevância, conforme pontua Marçal Justen Filho:

“Existe um dever de a Administração adotar a escolha mais vantajosa para a exploração dos recursos econômicos de sua titularidade. Como regra, a licitação visa a obter a solução contratual economicamente mais vantajosa para a Administração. [...]

Quando a Administração desembolsa um montante de recursos para uma contratação determinada, o referido montante não poderá ser utilizado para promover outras atividades. **Por isso, existe o dever de a Administração desembolsar o menor valor possível para obter uma prestação inclusive porque isso lhe assegurará a possibilidade de satisfazer outras necessidades com os recursos remanescentes.**

O Estado dispõe de recursos limitados para custeio de suas atividades e realização de investimento. Portanto, a vantagem para o Estado se configura com a solução que assegure os maiores benefícios para a aplicação de seus recursos econômico-financeiros. **O Estado tem o dever de realizar a melhor contratação sob o ponto de vista da economicidade. Isso significa que a contratação comporta avaliação como modalidade de relação custo-benefício.**

A economicidade é o resultado da comparação entre encargos assumidos pelo Estado e direitos a ele atribuídos, em virtude da contratação administrativa. Quanto mais desproporcional em favor do Estado o resultado dessa relação, tanto melhor atendido estará o princípio da economicidade. A economicidade exige que o Estado desembolse o mínimo e obtenha o máximo e o melhor. **Em princípio, a economicidade se retrata no menor preço pago pelo Estado ou no maior lance por ele recebido, conforme a natureza da contratação.**¹

62. É inconteste, assim, a necessidade da manutenção da r. decisão que declarou a COMPWIRE vencedora do processo de contratação em exame, ante o integral atendimento de sua proposta às exigências e especificações do Edital e Termo de Referência.

63. Ademais disso, as alegações do Recurso Administrativo deturpam as cláusulas do Edital, restringem sua interpretação e, portanto, violam o princípio julgamento objetivo, ao suscitar o

¹ JUSTEN FILHO, Marçal. **Comentários à Lei de Licitações e Contratações Administrativas: Lei 14.133/2021.** São Paulo: Thomson Reuterus Brasil, 2021., p. 144.



não atendimento do Edital pela Recorrida quando todas as funcionalidades exigidas foram comprovadas.

IV. Requerimentos:

64. Ante todo o exposto, respeitosamente e ante a fundamentação supra, requer-se seja negado provimento ao Recurso Administrativo movido pela ROOST LTDA, com a manutenção da declaração de habilitação e vencedora da licitante COMPWIRE INFORMÁTICA LTDA, e consequente adjudicação e homologação Pregão Eletrônico nº 90022/2025 em seu favor.

Nesses termos,
Pede-se deferimento.
Curitiba/PR, 03 de dezembro de 2025.

Compwire Informática Ltda.