DESPACHO - CINF

SEI nº 24.0.000011477-0

Assunto: Aquisição de Equipamentos e Soluções de TI

1 . A equipe técnica do Tribunal Regional Eleitoral de Goiás analisou detalhadamente os apontamentos realizados pela empresa recorrente NCT INFORMÁTICA LTDA. e confrontou-os com a documentação técnica da solução Check Point ofertada pela empresa NTSEC. Informa-se, por meio deste sumário, que todos os itens alegados como não conformes foram **devidamente verificados** na documentação oficial da fabricante Check Point, conforme consta nas documentações apontadas na Planilha de Atendimento de Requisitos. As especificações técnicas exigidas pelo Edital são **atendidas** pela solução proposta, conforme demonstrado a seguir.

2. Trata-se de recursos apresentado pela empresa NTC, contra a decisão proferida pelo Agente de Contratação deste Tribunal, que desclassificou as propostas das empresas Blockbit e Netware Telecomunicações, duas primeiras colocadas na fase de habilitação do certame, restando habilitada a terceira colocada.

O cerne das argumentações do recurso se concentra na premissa de que apenas soluções do fabricante Check Point permaneceram na disputa, apontando direcionamento a esse fabricante, bem como na desqualificação do produto ofertado pela empresa NTSEC.

Sustenta ainda a aplicação de rigor na análise da equipe técnica, para afastar propostas baseadas em soluções de outros fabricantes e relativizadas em face da empresa NTSEC.

As razões deste recurso apresentado, se firmam apenas em observações da sequência de eventos da licitação, sem comprovações fundamentadas, sem análise de todas as propostas das 11 licitantes que participaram do certame e simplesmente porque as duas primeiras concorrentes foram desclassificadas, uma por ter se beneficiado da condição de microempresa, em uma licitação que supera em muito os limites de faturamento anual dessa condição, e outra em que os produtos apresentados não atenderam a todas as especificações técnicas contidas no Termo de Referência.

O produto da primeira colocada sequer foi analisado pela equipe técnica, mas com base na desclassificação do produto da segunda colocada, a recorrente apresenta a tese de que somente a Check Point teria o potencial de atendimento da demanda.

Ocorre que o Termo de Referência foi construído de forma muito cuidadosa pela equipe técnica, com a análise dos equipamentos dos principais fabricantes dos produtos disponíveis no mercado, em que, mesmo diante da necessidade de soluções robustas que atendessem as demandas de conectividade de rede e cibersegurança tão importantes ao negócio da Justiça Eleitoral, houve o cuidado de garantir, que dentre os vários produtos oferecidos por uma mesma fabricante, houvesse um ou mais modelos que atendessem as especificações inseridas no Termo de Referência.

Uma evidência de que as especificações do produto não direcionam a licitação para a Check Point já aparece na análise do próprio documento dos Estudos Técnicos Preliminares (ID. 0984075 do SEI 24.0.000011477-0), em que a licitação paradigma utilizada naquele momento, inclusive para uma definição da estimativa de custos, foi a Ata de Registros de Preços da Defensoria Pública do Estado do Pará, resultado do Pregão Eletrônico SRP nº 90010/2024 – DPE (IDs. 0984074 e 0985125 do SEI 24.0.000011477-0), em que o produto vencedor foi da fabricante “Fortinet”.

Não há como sustentar o direcionamento ou restrição de competitividade em um Pregão que contou com 11 empresas participantes. A única impugnação que houve durante a fase de abertura do Edital foi da própria empresa recorrente, que em seus argumentos foram apontadas exigências nas especificações contidas no Termo de Referência, não existente nos Estudos Técnicos Preliminares.

Todavia, nem todos itens de uma especificação técnica do TR, necessariamente estarão contidas no ETP. Este instrumento é uma fase de estudo das diversas soluções possíveis para uma demanda apresentada, que a partir dele, avaliada e escolhida a melhor solução, parte-se para a construção do Termo de Referência, que aí sim, irá detalhar todos os quesitos necessários às necessidades do órgão levantadas no ETP.

Em sua manifestação sobre os itens abordados na impugnação, a equipe técnica justificou a importância de cada quesito questionado, inclusive destacando se tratarem de um padrão de mercado consolidado e encontrado em equipamentos de diversos fabricantes.

Na fase de impugnações houveram algumas dúvidas apresentadas pelas diversas empresas e todas elas foram devidamente esclarecidas e publicadas para o conhecimento dos diversos licitantes.

Abordadas essas questões importantes para contrapor as acusações de favorecimento apresentadas pela recorrente, será exposto em seguida as argumentações e evidências técnicas encontradas pela equipe técnica, em que demonstram que os itens suscitados, pela recorrente, como não aderentes no produto da licitante vencedora, atendem ao que foi especificado no TR.

3. Respostas

3.1 Do Alegado Direcionamento (Item 3.1 do Recurso)

Conforme mencionado acima, a recorrente alega haver direcionamento do edital para o fabricante Check Point.

O próprio processo licitatório refuta tal alegação, evidenciando que não houve restrição à competitividade. Durante a fase inicial, identificaram-se 11 empresas concorrentes representando os principais fabricantes do mercado (Palo Alto, Check Point, Fortinet e Sophos). Ademais, a estimativa de preço do Estudo Técnico Preliminar (ETP) baseou-se em uma Ata de Registro de Preços cujo fabricante é a Fortinet, demonstrando a pluralidade de soluções aptas.

3.2 Análise dos Itens Técnicos (Item 3.2 do Recurso)

A seguir, apresentam-se as respostas técnicas aos questionamentos específicos de funcionalidades:

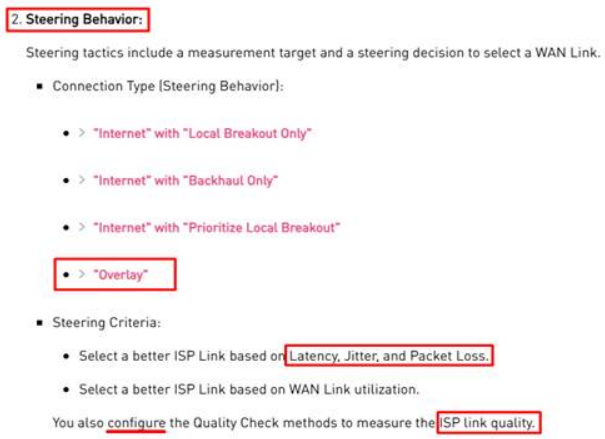
3.2.1 Recuperação de pacotes antes da alteração do caminho principal (Item 7.1.10.21.2)

Embora a recorrente alegue que a solução não atende ao item 7.1.10.21.2 do Edital, a equipe técnica identificou, na documentação apresentada, elementos e evidências que comprovam a conformidade. Os detalhes desta análise seguem abaixo.

Análise Técnica: O entendimento de que a solução oferecida atende ao requisito ocorre por meio da funcionalidade de *Forward Error Correction (FEC),* aplicada às conexões do tipo *Overlay***,** que, em conjunto com a configuração do *Steering Behavior,* através dos *Steering Candidates,* permite, para o tipo *Overlay*, o uso de todos os links WAN disponíveis ou links WAN específicos. Portanto, a plataforma recupera os pacotes perdidos (via *FEC*) mantendo o link atual estável. A mudança de caminho só será acionada posteriormente, e apenas se a degradação do link for severa o suficiente para ultrapassar a capacidade de correção do FEC.

Conclusão: A solução ofertada **atende** ao item do Termo de Referência.

Fonte: https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/FEC.htm?tocpath=SD-WAN%20Advanced%20Configuration%20%7CSD-WAN%20FEC%7C_____0#SD-WAN_FEC



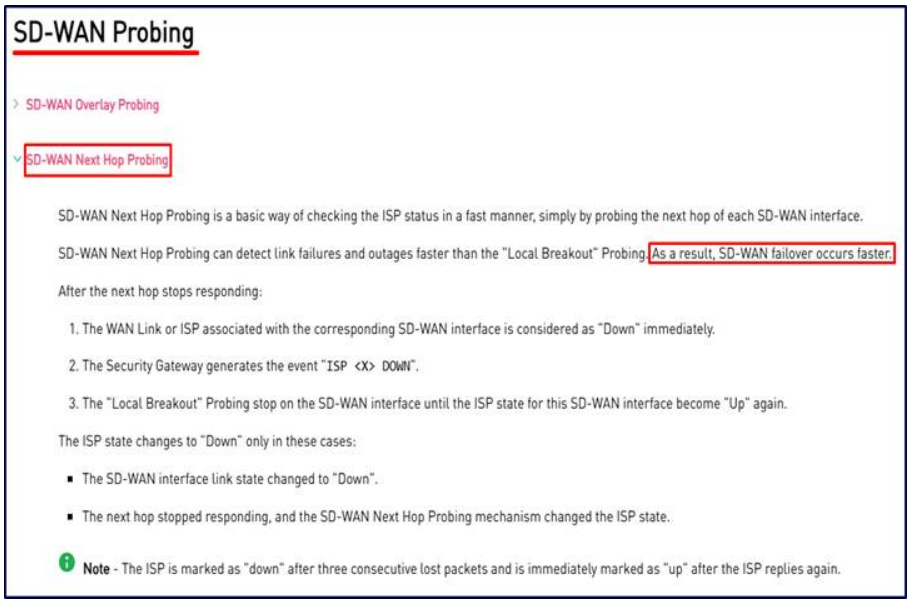
Fonte: https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/Introduction.htm?tocpath=_____2

3.2.2 Compreensão da causa da degradação (Item 7.1.10.21.6)

Embora a recorrente alegue que a solução não atende ao item 7.1.10.21.6 do Edital, a equipe técnica identificou, na documentação apresentada, elementos e evidências que comprovam a conformidade. Os detalhes desta análise seguem abaixo.

Análise Técnica: A documentação fornecida comprova a capacidade de monitoramento ponta a ponta e visibilidade da saúde da rede, incluindo métricas de SLA e desempenho de aplicações (*application performance*). A documentação afirma também a capacidade de troca de links abaixo de um segundo em caso de falhas e funcionalidade *SD-WAN Probing* garantindo a experiencia do usuário.

Conclusão: A solução ofertada **atende** ao item do Termo de Referência.



SD-WAN Probing

SD-WAN Overlay Probing

SD-WAN Next Hop Probing

SD-WAN Next Hop Probing is a basic way of checking the ISP status in a fast manner, simply by probing the next hop of each SD-WAN interface.

SD-WAN Next Hop Probing can detect link failures and outages faster than the "Local Breakout" Probing. As a result, SD-WAN failover occurs faster.

After the next hop stops responding:

1. The WAN Link or ISP associated with the corresponding SD-WAN interface is considered as "Down" immediately.
2. The Security Gateway generates the event "ISP <X> DOWN".
3. The "Local Breakout" Probing stop on the SD-WAN interface until the ISP state for this SD-WAN interface become "Up" again.

The ISP state changes to "Down" only in these cases:

- The SD-WAN interface link state changed to "Down".
- The next hop stopped responding, and the SD-WAN Next Hop Probing mechanism changed the ISP state.

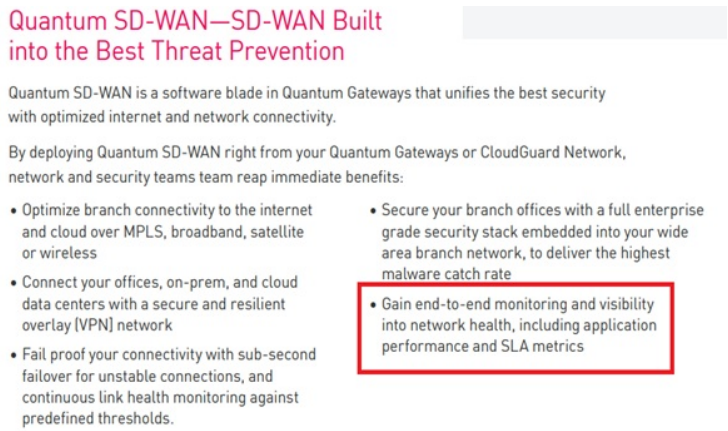
Note - The ISP is marked as "down" after three consecutive lost packets and is immediately marked as "up" after the ISP replies again.

F o n t e : https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/Best-Practices.htm?tocpath=SD-WAN%20Best%20Practices%7C____0#

SD-WAN Capabilities

- Sub-second failover for overlay and supported applications
- Link aggregation
- Link prioritization - according to Latency, Jitter, and Packet loss
- SLA monitoring – Quality of Service (QoS) per application
- Autonomous link swapping
- IPSec VPN AES 128/256, IKEv2

Fonte: https://www.checkpoint.com/downloads/products/quantum-sd-wan-datasheet.pdf



Quantum SD-WAN—SD-WAN Built into the Best Threat Prevention

Quantum SD-WAN is a software blade in Quantum Gateways that unifies the best security with optimized internet and network connectivity.

By deploying Quantum SD-WAN right from your Quantum Gateways or CloudGuard Network, network and security teams team reap immediate benefits:

- Optimize branch connectivity to the internet and cloud over MPLS, broadband, satellite or wireless
- Connect your offices, on-prem, and cloud data centers with a secure and resilient overlay (VPN) network
- Fail proof your connectivity with sub-second failover for unstable connections, and continuous link health monitoring against predefined thresholds.
- Secure your branch offices with a full enterprise grade security stack embedded into your wide area branch network, to deliver the highest malware catch rate
- Gain end-to-end monitoring and visibility into network health, including application performance and SLA metrics

Fonte: https://www.checkpoint.com/downloads/products/quantum-sd-wan-datasheet.pdf

3.2.3 Distribuição de tráfego e manutenção de conexão (Item 7.1.10.21.8.2 e 7.1.10.21.8.3)

7.1.10.21.8.2 Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresentem resultados abaixo dos limites definidos;

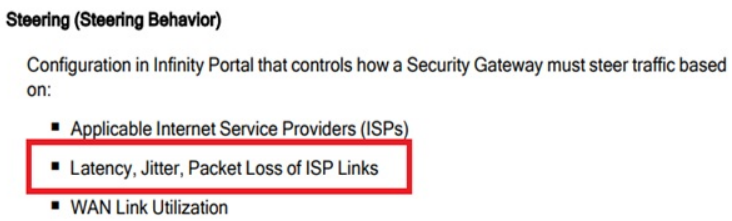
7.1.10.21.8.3 Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;

Embora recorrente alegue que a solução não atende aos itens 7.1.10.21.8.2 e 7.1.10.21.8.3 do Edital, a equipe técnica identificou, na documentação apresentada, elementos e evidências que comprovam a conformidade. Os detalhes desta análise seguem abaixo.

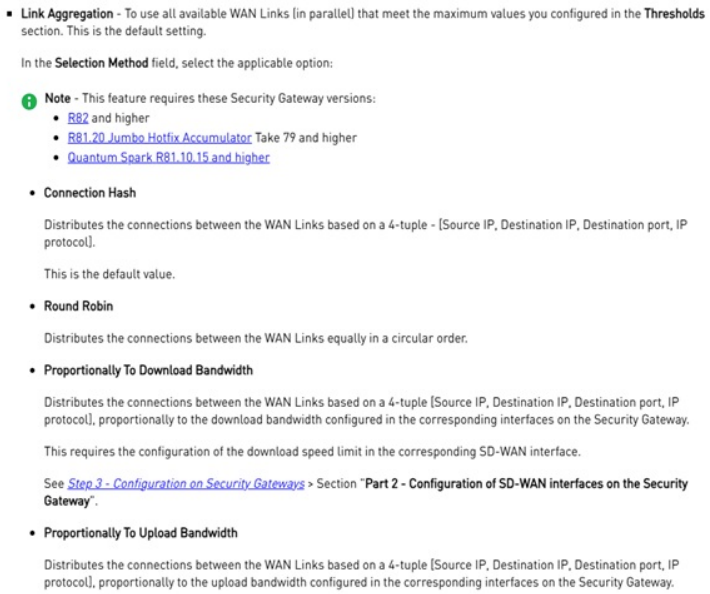
Análise Técnica: A documentação técnica da solução Quantum SD-WAN comprova o atendimento aos requisitos de distribuição baseada em métricas e perfis de origem e destino. A funcionalidade de *Steering Behavior* permite a configuração de critérios (*Criteria*) baseados especificamente em Latência, Jitter e Perda de Pacotes (*Packet Loss*), estabelecendo *Thresholds* (limites) para a utilização dos links.

No tocante à exigência de distribuição de tráfego (item 7.1.10.21.8.3) definida por origem e destino, a solução implementa a funcionalidade de *Link Aggregation*, que utiliza todos os WAN *Links* disponíveis que estejam dentro dos parâmetros de qualidade configurados. A seleção e distribuição das conexões pode utilizar o método *Connection Hash*, entre outros.

Conclusão: A solução ofertada **atende** ao item do Termo de Referência.



Fonte: Configuring Steering Behavior



Fonte: Configuring Steering Behavior

3.2.4 Uso de FEC para reparação antes do failover (Item 7.1.10.21.9)

A recorrente afirma, na conclusão do recurso 3.2.4, que no item 7.1.10.21.9 o FEC não se aplica ao tráfego *Direct Internet Access* (DIA).

Contudo, no item original do Termo de Referência é exigido que o dispositivo de SD-WAN deve utilizar "*Forward Error Correction*" (FEC) **habilitado** [...]. Não há menção sobre o **tipo de tráfego** e é suficiente que a solução possua a funcionalidade de recuperação de pacotes. Portanto, o texto reclamado pela recorrente acrescenta requisitos não existentes ao item editalício.

Análise Técnica: Conforme detalhado também na resposta ao item 3.2.1, o FEC atua inserindo pacotes *ECC* no fluxo *Overlay* para garantir a entrega bem-sucedida do tráfego. A documentação confirma que o *FEC* ajuda a melhorar a confiabilidade quando a perda de pacotes é alta, operando antes da necessidade de troca de caminho baseada em critérios de *Steering*.

Conclusão: A solução ofertada **atende** ao item do Termo de Referência.

F o n t e : https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Quantum-SD-WAN-Admin-Guide/Content/Topics-SD-WAN/FEC.htm?tocpath=SD-WAN%20Advanced%20Configuration%20%7CSD-WAN%20FEC%7C____0#SD-WAN_FEC

3.2.5 Redistribuição dinâmica com manutenção de sessões (Item 7.1.10.21.12)

A recorrente afirma, na conclusão do recurso 3.2.5, que o item 7.1.10.21.12 não é atendido porque **não mantém sessões ativas quando ocorre mudança de caminho** [...].

Segue abaixo, o texto original do item:

7.1.10.21.12 Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e **utilizar deste "path" para manter sessões ativas**, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes;

Em relação a “manter sessões ativas”, o texto original exige que o dispositivo deve validar o melhor caminho

disponível e utilizar deste “path”, ou seja, deste caminho para manter sessões ativas. Continuando, o texto exige que, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes. Não há exigência de que, na distribuição, haja manutenção de sessões ativas.

Portanto, o texto reclamado pela recorrente acrescenta requisitos não existentes ao item editalício.

Análise Técnica: Considerando que o requisito 7.1.10.21.12 não exige a manutenção de sessões ativas durante a redistribuição dinâmica, esta equipe técnica manifesta-se pela improcedência da reclamação constante no item 3.2.5.

Conclusão: A solução ofertada **atende** a este item do Termo de Referência.

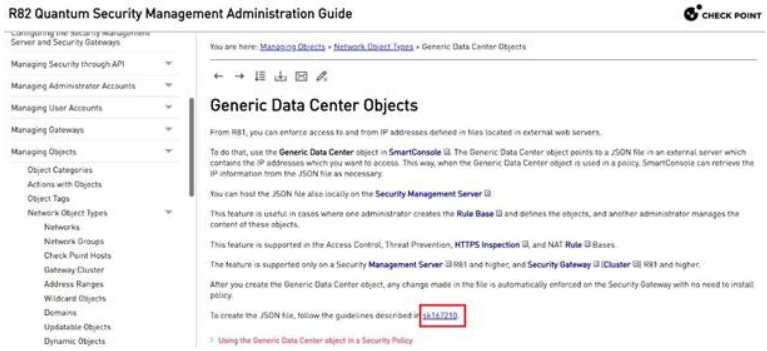
3.2.6 Integração com ambientes de nuvem e Data Center (Itens 7.1.12.4 e 7.1.12.4.1)

Embora a recorrente alegue que a solução não atende aos itens 7.1.12.4 e 7.1.12.4.1 do Edital, a equipe técnica identificou, na documentação apresentada, elementos e evidências que comprovam a conformidade. Os detalhes desta análise seguem abaixo.

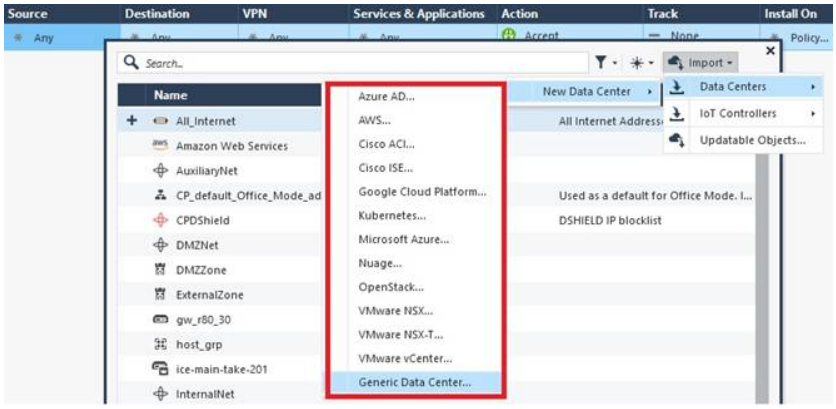
Análise Técnica: Apesar da Planilha de Atendimento de Requisitos apontar a documentação referente ao *CloudGuard Controller* como comprovação de atendimento ao item 7.1.12.4.1, a equipe técnica, na análise do item imediatamente anterior (item 7.1.12.3), mais especificamente na busca por objetos *Data Center*, encontrou o documento que demonstra a existência da integração exigida em uma interface de administração do *Security Management Software*.

A documentação demonstra a existência da integração exigida em uma interface de administração do *Security Management Software*. Concluindo que a solução ofertada atende aos itens em questão.

Conclusão: A solução ofertada **atende** a este item do Termo de Referência.



Fonte: https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityManagement_AdminGuide/Content/Topics-SECMG/Managing-Objects.htm?tocpath=Managing%20Objects%7C____0



Fonte: sk167210 - Generic Data Center feature

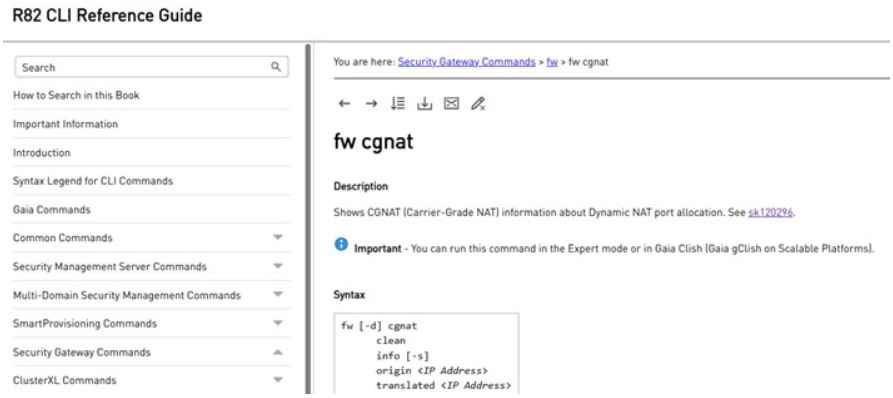
3.2.7 CGNAT com persistência de mapeamento (Item 7.1.10.14.3)

A recorrente afirma, na conclusão do recurso 3.2.7, que o item 7.1.10.14.3, não é atendido por não implementar CGNAT ***com*** persistência de mapeamento independente da porta de destino.

Contudo, no item original do Termo de Referência é exigido que a solução implemente CGNAT ***ou*** funcionalidade que implemente persistência de mapeamento independente da porta de destino [...]. Portanto, o texto posto pela recorrente altera o requisito do item editalício.

Análise Técnica: A documentação da própria fabricante comprova o suporte a CGNAT (*Carrier Grade Network Address Translation*) na solução ofertada, conforme referências técnicas disponibilizadas nos guias de referência CLI e base de conhecimento da fabricante, atendendo o requisito do Termo de Referência.

Conclusão: A solução ofertada **atende** a este item do Termo de Referência.



Fonte:https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_CLI_ReferenceGuide/Content/TopicCLIG/FWG/fw-cgnat.htm

3.2.8 Suporte a 20.000 rotas dinâmicas (Item 7.1.10.11)

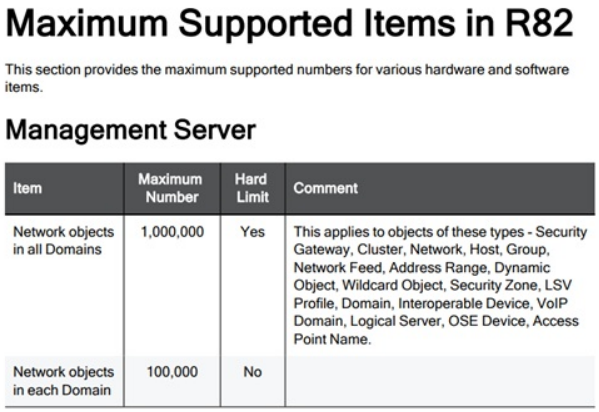
A recorrente, na sua interpretação, insere requisitos não existentes no item original. E alega que a documentação apresentada trata de elemento distinto do solicitado no item 7.1.10.11.

Análise Técnica: O documento de comprovação apresentado aponta para uma página cujo título é "*Maximum Supported Items in R82*". Desse título denota-se que as limitações do sistema do equipamento ofertado, são listadas nas tabelas subsequentes. Ao realizar busca por limite máximo de rotas dinâmicas, não foi encontrado nenhuma limitação. Nesse sentido, entende-se que não há limite para número de rotas dinâmicas.

Mais além, dentro da mesma documentação, encontra-se um link que apresenta as limitações conhecidas do sistema do equipamento ofertado. Neste documento são apresentadas as limitações e as características não suportadas desse sistema. E nele não consta qualquer limitação no número de rotas dinâmicas.

Adicionalmente, a solução ofertada implementa protocolos de roteamento dinâmico, incluindo OSPF e o BGP (*Border Gateway Protocol*). Considerando que o protocolo BGP pode gerenciar tabelas de roteamento (superiores a 1.000.000 de prefixos) e que o fabricante não estipula limitações nos documentos consultados, depreende-se que o equipamento suporta mais de 20.000 rotas dinâmicas.

Conclusão: A solução ofertada **atende** a este item do Termo de Referência.



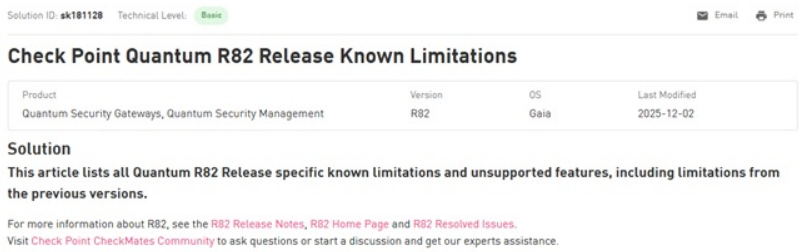
Maximum Supported Items in R82

This section provides the maximum supported numbers for various hardware and software items.

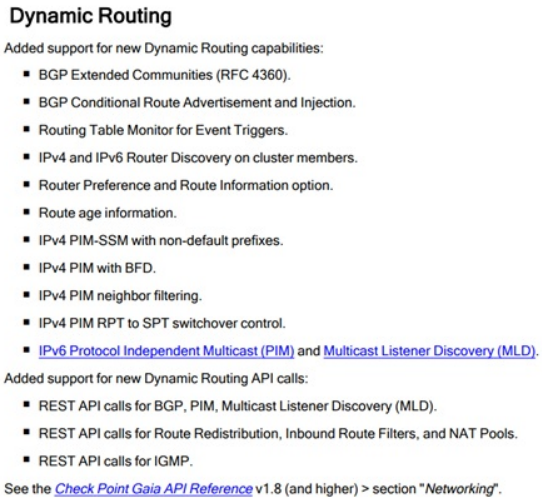
Management Server

Item	Maximum Number	Hard Limit	Comment
Network objects in all Domains	1,000,000	Yes	This applies to objects of these types - Security Gateway, Cluster, Network, Host, Group, Network Feed, Address Range, Dynamic Object, Wildcard Object, Security Zone, LSV Profile, Domain, Interoperable Device, VoIP Domain, Logical Server, OSE Device, Access Point Name.
Network objects in each Domain	100,000	No	

Fonte: https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/CP_R82_ReleaseNotes.pdf



Fonte: sk181128 - Check Point Quantum R82 Release Known Limitations



Dynamic Routing

Added support for new Dynamic Routing capabilities:

- BGP Extended Communities (RFC 4360).
- BGP Conditional Route Advertisement and Injection.
- Routing Table Monitor for Event Triggers.
- IPv4 and IPv6 Router Discovery on cluster members.
- Router Preference and Route Information option.
- Route age information.
- IPv4 PIM-SSM with non-default prefixes.
- IPv4 PIM with BFD.
- IPv4 PIM neighbor filtering.
- IPv4 PIM RPT to SPT switchover control.
- IPv6 Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD).

Added support for new Dynamic Routing API calls:

- REST API calls for BGP, PIM, Multicast Listener Discovery (MLD).
- REST API calls for Route Redistribution, Inbound Route Filters, and NAT Pools.
- REST API calls for IGMP.

See the *Check Point Gaia API Reference* v1.8 (and higher) > section "*Networking*".

Fonte: https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/CP_R82_ReleaseNotes.pdf

3.3 Da Aplicabilidade da Documentação e Modelo Ofertado (Item 3.3 do Recurso)

A reclamação da recorrente é a respeito do documento informado não se aplicar ao produto ofertado para comprovar os atendimentos aos requisitos do item 7.5. A recorrente relaciona os itens onde afirma ter encontrado tais documentos comprobatórios: 7.5.7.4.1.1, 7.5.7.4.1.5, 7.5.7.4.1.9, 7.5.7.4.1.11, 7.5.7.4.1.13 e 7.5.7.4.1.14. Todos os itens são relacionados às especificações de SD-WAN.

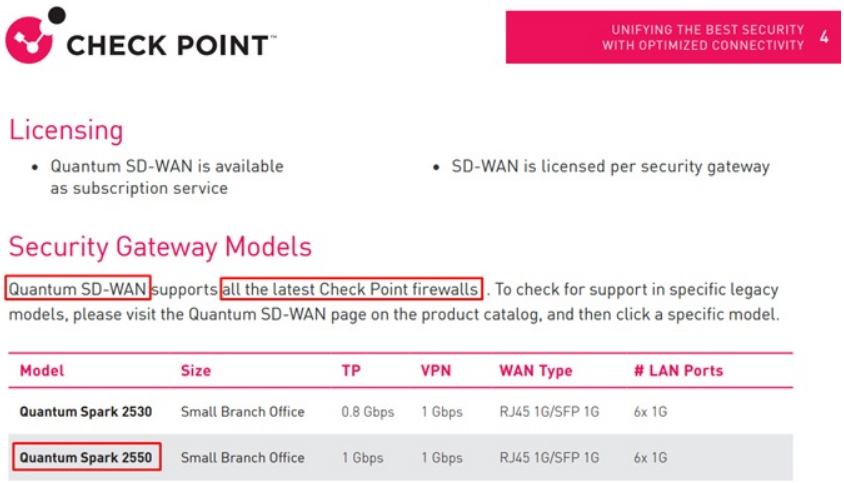
O produto ofertado é o appliance Quantum Spark 2550.

O documento apontado, na Planilha de Atendimento de Requisitos, para comprovação do item 7.5.7.4.1.1 da relação acima, é referente ao Quantum-SD-WAN. Esse documento informa que o Quantum SD-WAN é compatível com ***todos*** os firewalls Check Point mais recentes onde, na relação desses firewalls, figura o Quantum Spark 2550.

Em todos os demais itens a Planilha de Atendimento de Requisitos aponta documentações relativas ao Quantum-SD-WAN.

Análise Técnica: O Quantum SD-WAN é suportado por **todos** os *firewalls* Check Point recentes, incluindo o modelo Quantum Spark 2550 ofertado, validando integralmente a documentação apresentada para comprovação dos requisitos dos itens relacionados.

Conclusão: A solução ofertada **atende** a este item do Termo de Referência.



CHECK POINT

UNIFYING THE BEST SECURITY WITH OPTIMIZED CONNECTIVITY 4

Licensing

- Quantum SD-WAN is available as subscription service
- SD-WAN is licensed per security gateway

Security Gateway Models

Quantum SD-WAN supports all the latest Check Point firewalls. To check for support in specific legacy models, please visit the Quantum SD-WAN page on the product catalog, and then click a specific model.

Model	Size	TP	VPN	WAN Type	# LAN Ports
Quantum Spark 2530	Small Branch Office	0.8 Gbps	1 Gbps	RJ45 1G/SFP 1G	6x 1G
Quantum Spark 2550	Small Branch Office	1 Gbps	1 Gbps	RJ45 1G/SFP 1G	6x 1G

Fonte: https://www.checkpoint.com/downloads/products/quantum-sd-wan-datasheet.pdf

3.4 Do pedido de desclassificação da recorrida

Conforme se observa, o pedido de desclassificação da empresa vencedora se fundamenta exclusivamente na suposição de descumprimento de requisitos técnicos, que conforme analisado nos itens anteriores, tais argumentos não se sustentaram.

Constatado que os requisitos suscitados apresentam comprovação suficiente para conclusão de sua aderência às especificações técnicas, não há de se discutir o cabimento de oportunidade de saneamento de falhas cabíveis de correção, uma vez que a documentação juntada ao processo se mostrou suficiente para sua verificação.

Nestes termos, resta verificado e constatado que a solução apresentada pela empresa NTSEC atende aos requisitos técnicos do Termo de Referência, não havendo motivo para que se promova sua desclassificação.

4 Conclusão

Diante da revisão da planilha de conformidade e de toda a documentação apresentada pela empresa NTSEC, com ênfase nos itens destacados pela recorrente, e mais uma vez comprovada a aderência da solução em análise às especificações contidas no Termo de Referência, com os esclarecimentos apresentados na fase inicial do Pregão, dentro do prazo de impugnação do Edital, a equipe técnica conclui, mais uma vez, pela aprovação técnica dos equipamentos cotados.

Goiânia, 23 de dezembro de 2025.

Roberto César Rodrigues

Coordenador de Infraestrutura

Documento assinado eletronicamente por **ROBERTO CÉSAR RODRIGUES**, **COORDENADOR(A)**, em 23/12/2025, às 10:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei4.tre-go.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1289428** e o código CRC **407626A3**.