Despacho de Pregoeiro n° 003/2017-SLC/ANEEL

Em 26 de janeiro de 2017.

Processo: 48500.002554/2016-11
Licitação: Pregão Eletrônico nº 43/2016
Assunto: Análise do recurso interposto pela sociedade NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA-ME.

I – JUIZO DE ADMISSIBILIDADE

1. A sociedade NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA-ME registrou seu recurso contra a aceitação da proposta apresentada pela sociedade NCT INFORMÁTICA LTDA no Pregão Eletrônico nº 43/2016. O registro ocorreu dentro do prazo fixado no sistema Comprasnet. A NCT INFORMÁTICA LTDA também se manifestou, apresentando suas contrarrazões.

2. A recorrente participou do certame, classificando-se em 1º lugar após a fase de lances, e foi desclassificada em face de recurso interposto pela NCT INFORMÁTICA LTDA.

3. O interesse de agir encontra-se evidentemente atendido, em vista do recurso ser manejado por aquele que o aproveita, caso esse seja julgado procedente.

4. O pressuposto da sucumbência recursal é atendido já que a adjudicação da recorrida representaria o insucesso definitivo no certame.

5. O recurso está regularmente motivado, devolvendo à Administração fatos e direitos.

6. O recurso foi apresentado conforme o previsto no inciso XVIII, art. 4º da Lei n. 10.520/02 e no caput do art. 26 do Decreto Federal n. 5.450/05.

7. Assim posto, conheço do recurso.

II – DA ANÁLISE DO JUÍZO DE RETRATAÇÃO

8. A recorrente concentra sua argumentação na tese de que o produto ofertado pela recorrida, modelo Fortinet FG-2000E, não atende aos requisitos de desempenho previstos no instrumento convocatório,

uma vez que "no data sheet do fabricante do produto ofertado consta informação de rodapé que atesta o atingimento de 5.4 Gbps de Threat Protection Trhoughput, **sem que todas as funcionalidade estejam habilitadas.**"

9. Discorre ainda a recorrente:

> 7. O Edital exige no item 28.1.2.3, que a amostra deve ser configurada para atuar com as seguintes funcionalidades habilitadas simultaneamente: Firewall, IPS, Controle de Aplicação, Filtro de URL, Prevenção de Ameaças(Antivírus, Antispyware e Antibot), Proteção de Malwares Avançados e Inspeção de Tráfego SSL/TLS.
>
> 8. Porém, de acordo com a nota de rodapé do Datasheet do Fabricante FortGate 2000E (pag.4), consta o seguinte:
>
> > "5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
>
> 9. Fica claro que para mensurar o Througput de 5.1 solicitado no presente certame, a funcionalidade de Inspeção de Tráfego SSL/TLS não é utilizada. Ainda, o tráfego exigido no caderno de testes, item 12. pág 47, é mais complexo e exige mais recursos dos equipamentos, tornando a comprovação por meio de documentação uma forma ineficiente e inadequada para habilitação da proponente.
>
> 10. Adotando-se a mesma metodologia utilizada para desclassificar a Requerente, não há como a licitante vencedora permanecer no presente certame. Caso contrário, o flagrante desrespeito à isonomia não resistirá ao controle externo exercido pelo Tribunal de Contas da União.
>
> 11. Assim, com base no princípio da isonomia e da vinculação ao instrumento convocatório, a licitante declarada vencedora deverá ser desclassificada do presente certame eis que não atende aos requisitos de capacidade exigidos no Edital.

9. Acrescenta que caso a Administração entenda que a recorrida atende às exigências editalícias, deverá a Administração convocar a vencedora para o teste de bancada.

10. Por sua vez, a recorrida contra argumenta que:

> A inconformidade da recorrente não se justifica, todavia. Quanto a Throughput, o mesmo documento técnico utilizado pela recorrente para fundamentar a sua pretensão – "FortiGate_2000E.pdf" – traz informações importantes para o correto entendimento sobre o funcionamento da solução ofertada.
>
> Nesse documento, pode-se ler que, ao atingir o Throughput de 5.4Gbps, o tráfego utilizado já é "based on Enterprise Traffic Mix", ou seja, UM TRÁFEGO REAL-WORLD MUITO SEMELHANTE AO TRÁFEGO SOLICITADO NESTE CERTAME. Vale ressaltar que todos os equipamentos Fortinet são testados com tráfego nessas condições, e nunca mediante subterfúgios argumentativos como "condições de testes ideais", tal qual realizado por outros fabricantes.
>
> Além do mais, os equipamentos Fortinet modelo FG-2000E possuem um processador dedicado para o processamento de conteúdo (Content Processor), do tipo CP9.
>
> Com relação à ativação da engine responsável pela inspeção de tráfego SSL/TLS, a Fortinet, diferentemente de outros fabricantes, torna público em todos os seus documentos oficiais esse Throughput, que é realizado por processadores de última geração e específicos para este fim.
> No documento, pode-se ler claramente que o Throughput atingido para inspeção SSL com o equipamento ofertado é de 12.5Gbps utilizando TLS v1.2 comm AES256-SHA, que sabidamente é uma chave de alta criptografia. O

> Throughput de inspeção disponível de SSL/TLS é QUASE DUAS VEZES E MEIA SUPERIOR o valor solicitado para este certame.
> Os serviços realizados pelo processador principal não incluem as funções de IPsec e SSL/TLS, ou seja, o processamento dessas funcionalidades é realizado por processadores à parte (CP9), não onerando a CPU,
> Sendo assim, independentemente de se ativar as funções de SSL/TLS, o Throughput de Threat Prevention, que já inclui IPS na sua medição, atinge um valor acima do exigido no edital. O tráfego SSL/TLS é realizado por outro processador.

11. A área técnica demandante, Superintendência de Gestão Técnica da Informação – SGI, foi convocada a se pronunciar.

12. Reproduzo o posicionamento apresentado pela área.

> Inicialmente foi verificado que a solução ofertada pela empresa NCT Informática, da marca *Fortinet,* tem qualidade reconhecida e consagrada mundialmente no mercado de segurança cibernética, conforme diversos relatórios elaborados pelo *Gartner* (Empresa mundial líder em consultoria de TI) e *NSS Labs* (Empresa mundial líder em testes de performance de soluções de segurança).
>
> No que diz respeito à discussão inicial sobre o padrão de tráfego utilizado na medição de performance da solução ofertada, foi verificado que o padrão a ser utilizado no Teste de Conformidade da ANEEL também é uma "Mistura de Tráfegos Corporativos" e que estes tráfegos são padronizados pela indústria para realização de testes de performance de equipamentos de segurança cibernética em ambientes corporativos. Nesse padrão, são utilizados uma mistura de protocolos, que podem ser do tipo *http, https, smtp, ftp*, smnp, entre outros.
>
> Sendo assim, uma vez que o documento da *Fortinet* (*"Fortigate_2000E.pdf"*) informa que a medição do *troughput* de *Threat Prevention* é realizada em condições de tráfego denomina de "*Enterprise Traffic Mix*" ou "Mistura de Tráfegos Corporativos" e a empresa NTSec Teleinformática não inseriu no documento protocolado evidências que demonstrassem o contrário deste aspecto, a dúvida levantada pela mesma não foi suficiente para ensejar, do ponto de vista técnico, a necessidade de realização do Teste de Conformidade pela ANEEL visando a averiguação de performance da solução.
>
> No que diz respeito ao segundo ponto, onde o *troughput* de 5.4 Gbps para *Threat Prevention* (*Firewall* + IPS + *Application Control* + *AntiMalware*) informado pela *Fortinet* no *Datasheet* da solução não inclui a funcionalidade de Inspeção de Tráfego SSL/TLS habilitada, verificou-se que, após análise das contrarrazões enviadas pela NCT Informática, tal funcionalidade é tratada por processadores independentes, chamados de *Content Processors* (CP-9), cujo *troughput* informado é de 12.5 Gbps estando, portanto, acima dos 5.1 Gbps exigidos no Teste de Conformidade do Edital.
>
> Além disso, entendeu-se que, caso habilitada a funcionalidade de Inspeção de Tráfego SSL/TLS, não será onerada a CPU principal que trata as demais funcionalidades de *Threat Prevention*, cujo *troughput* já é de 5.4 Gbps, acima, desse modo, dos 5.1 Gbps exigidos no Teste de Conformidade do Edital.
>
> Portanto, aceita-se que esta independência de processadores para tratamento das funcionalidades de *Threat Prevention* e Inspeção de Tráfego SSL/TLS também justifica a existência de *troughputs* diferentes, um de 5.4 Gbps e outro de 12.5 Gbps respectivamente, estando ambos acima dos 5.1 Gbps exigidos no Teste de Conformidade do Edital.

13. Passando à análise, destacamos que a ANEEL buscou por meio do estudo das ferramentas de Firewall disponíveis no mercado, elaborar as especificações que permitissem à Agência usufruir de uma solução que aliasse a melhor técnica com o investimento mais adequado. Para isso, consolidou características que pudessem atender com excelência a sua demanda, projetando um cenário que abarcasse um período de

cinco a oito anos sem nova aquisição. Nesse contexto foram estabelecidos requisitos mínimos de performance que se adequassem a esse cenário.

14. O foco do recurso foi a suposta falta de comprovação na documentação técnica da NCT de atendimento ao item 28.1.2.3 do Anexo I ao Edital. Ora, a recorrida esclareceu que para o atingimento de 5.4 Gbps de Threat Protection Trhoughput, as funcionalidades (exigidas no item 28.1.2.3) estavam, sim, habilitadas, contudo, foi informado que a funcionalidade de Inspeção de Tráfego SSL/TLS, é tratada por processadores independentes, chamados de *Content Processors* (CP-9), cujo *troughput* informado é de 12.5 Gbps.

15. Tais informações já constavam de documento técnico apresentado na fase de habilitação, "Fortigate_2000E.pdf", e ao que parece não foram devidamente interpretadas pela recorrida, senão vejamos a tabela:

SPECIFICATIONS

	FORTIGATE 2000E
Hardware Specifications	
Hardware Accelerated 10 GE SFP+ Slots	6
Hardware Accelerated GE RJ45 Ports	32
GE RJ45 Management / HA Ports	2
USB Ports	1
Console Port	1
Onboard Storage	480 GB
Included Transceivers	2x SFP+ (SR 10GE)
System Performance	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	90 / 90 / 60 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	90 / 90 / 60 Gbps
Firewall Latency (64 byte, UDP)	2 µs
Firewall Throughput (Packet per Second)	90 Mpps
Concurrent Sessions (TCP)	20 Million
New Sessions/Second (TCP)	500,000
Firewall Policies	100,000
IPsec VPN Throughput (512 byte)	65 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	20,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	6 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	10,000
IPS Throughput (HTTP / Enterprise Mix) [1]	25 / 11.5 Gbps
SSL Inspection Throughput [2]	12.5 Gbps
Application Control Throughput [3]	15 Gbps
NGFW Throughput [4]	9 Gbps
Threat Protection Throughput [5]	5.4 Gbps
CAPWAP Throughput [6]	21 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiAPs (Total / Tunnel)	4,096 / 1,024
Maximum Number of FortiTokens	5,000
Maximum Number of Registered Endpoints	8,000
High Availability Configurations	Active-Active, Active-Passive, Clustering

Note: All performance values are "up to" and vary depending on system configuration. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. SSL Inspection is measured with IPS enabled and HTTP traffic, using TLS v1.2 with AES256-SHA. 3. Application Control performance is measured with 64 Kbytes HTTP traffic. 4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix. 6. CAPWAP performance is based on 1444 byte UDP packets. LAG support and redundant interfaces are limited to certain port configurations, please refer to technical documentation.

16. O posicionamento técnico da SGI, também é objetivo no sentido de atestar que os índices de desempenho da solução FORTIGATE 2000E superaram os patamares indicados no item 28.1.2.3, e que, inclusive, o Teste de Conformidade não seria necessário. Aliás, sobre esse aspecto, privilegiando ao princípio da isonomia e utilizando a mesma metodologia que resultou na desclassificação a Requerente, qual seja a análise documental, entendo que não deve prosperar a demanda pela desclassificação da recorrida.

17. Importante frisar que diferentemente da recorrida, a recorrente teve os índices de desempenho da ferramenta de firewall avaliados pela área técnica e estes expressavam valores de performance inferiores ao exigido pelo Edital.

18. Por fim, estranhamento a peça recursal finaliza pedindo que caso a Administração entenda que a ferramenta atende às exigências editalícias, a licitante deverá se submeter ao teste de bancada. Avaliando o Edital, resta claro o caráter facultativo do teste de conformidade, e respaldada na posição da área técnica, que por duas vezes, avaliou os documentos técnicos apresentados pela recorrida e manifestou-se pela aceitação da ferramenta ofertada, mantenho a posição anterior trazida no Despacho de habilitação n. 005/2017-SLC.

19. Interessante notar que a recorrente, já havia se manifestado sobre a questão do teste de bancada, em sede de contrarrazões de recurso ofertado pela NCT INFORMÁTICA LTDA, e naquela ocasião assim posicionou-se:

> *"O Edital, ao tornar facultativa a realização da prova de conceito não violou o princípio da transparência ou do julgamento objetivo, pois não há margem para interpretação subjetiva na análise dos data sheets da solução".*

III – CONCLUSÃO

20. Assim, aceito o presente recurso, para no mérito, pois presentes os pressupostos processuais, contudo, no mérito, sou pelo não provimento do recurso, porque o aspecto técnico arguido pela recorrente, está devidamente explicitado na documentação apresentada pela empresa NCT INFORMATICA LTDA.

ANGELICA LUISA PINTO NOGUEIRA PINHEIRO
Pregoeira