TERMO DE AVALIAÇÃO DE AMOSTRA - LOTE 4

PREGÃO ELETRÔNICO: Nº 5/2017

OBJETO: REGISTRO DE PREÇOS, para eventual aquisição, de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, incluindo todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades dos contratantes.

Lote: 04 – LICITANTE: NCT INFORMÁTICA.

1. FINALIDADE

O teste de conformidade da amostra visa à aferição da real capacidade técnica dos equipamentos ofertados pela Licitante Convocada no cumprimento do disposto nos requisitos constantes da especificação técnica do Anexo B do Termo de Referência do Pregão nº 5/2017, referentes ao Lote 4.

Na avaliação dos testes de conformidade e no presente Termo de Avaliação de Amostra - TAM, serão levados em consideração o Relatório dos Testes da Amostra – RTA, entregue pela empresa NCT INFORMÁTICA no arquivo "*MPOG_PE_5.2017_NCT_INFORMATICA_v4_LOTE_4_Relatorio.pdf*" e as evidências coletadas pela equipe técnica durante a execução dos testes.

2. CONSIDERAÇÕES GERAIS

Os testes de conformidade do LOTE 4 foram realizados entre os dias 24 e 25 de setembro de 2018, entre 08:30h e 18:30h, nas dependências do Ministério do Planejamento, bloco situado na quadra 516 Norte, em Brasília-DF. Foi informado que os testes seriam realizados de acordo com as regras e condições contidas no Anexo E do Termo de Referência, em consonância com o caderno de testes previamente aprovado pelo grupo técnico de apoio ao pregoeiro.

Lembrou-se aos participantes que os testes constituem sessão pública e que, durante a realização dos testes, não deveriam ser realizadas intervenções indevidas das empresas ouvintes ou interessados presentes à sessão pública, bem como questionamentos não deveriam ser realizados durante a sessão, com exceção de esclarecimentos pontuais, uma vez que tais questionamentos deveriam seDanr formalizados e endereçados ao pregoeiro, em momento posterior, em sede de recurso administrativo com as devidas fundamentações.

Reiterou-se à ocasião que, conforme especificado nos itens 2.16 e 2.17 do anexo E do edital PE nº 05/2017, ao grupo técnico de apoio ao pregoeiro é conferida a prerrogativa de, a qualquer tempo durante a realização dos testes, solicitar as alterações, adequações ou informações que julgar necessárias ao esclarecimento de todas as eventuais dúvidas em relação aos testes e itens da especificação técnica. Salientou-se, da mesma forma, a necessidade de se manter o registro e documentação de *logs*, *prints* e evidências para a comprovação do atendimento dos quesitos avaliados nos testes complementares, bem como a necessidade de assinatura de lista de presença, por período (matutino e vespertino).

Dando prosseguimento aos trabalhos dos testes de conformidade, deve-se indicar que a licitante atendeu de forma satisfatória a execução dos itens pertinentes às disposições gerais constantes do Anexo E do instrumento editalício, respondendo aos pedidos de informações complementares e esclarecimentos, bem como executou a instalação, configuração, operação e acesso à solução ofertada, conforme previsto no item 2.22 do mesmo anexo.

Os testes foram executados de forma organizada, conforme sequenciamento previsto no caderno de testes e os representantes da empresa avaliada apresentaram capacidade técnica adequada, organização e pontualidade. A empresa também atendeu o disposto no item 2.20 do Anexo E do edital, providenciando toda a infraestrutura necessária para execução dos testes.

A estrutura do RTA (Relatório Técnico da Amostra). entregue pela NCT apresentou-se de forma compatível para atendimento ao disposto no item 2.25 do Anexo E. Também foram coletadas, com sucesso, em mídia digital fornecida pela CONTRATANTE, evidências produzidas durante a execução de todos os testes, como *prints*, *logs*, arquivos de configuração e relatórios do gerador de tráfego, todos com os respectivos *hashes* que asseguram sua inviolabilidade e autenticidade (as evidências podem ser, a qualquer tempo, disponibilizadas para consulta, caso haja interesse).

A amostra apresentada para os testes estava em conformidade com o produto ofertado em proposta, atendendo ao que determina o item 3.1 do Anexo E. As páginas 8, 16 e 17 do RTA detalham a lista de equipamentos submetidos ao teste de bancada e os equipamentos geradores de tráfego utilizados.

Quanto à preparação inicial da amostra para os testes, todos os procedimentos foram executados de forma satisfatória, como instalação do *firmware*, comprovação de integridade dos arquivos junto ao site do fabricante, execução de atualizações e de *backup* das configurações iniciais, conforme apresenta o RTA entre suas páginas 9, 16 e 17.

O grupo técnico observou que as versões de *firmware* utilizadas nos equipamentos *firewall* e gerência centralizada da amostra (respectivamente, FortiOS v6.0.2 Build 0163 e FortiOS v6.0.2 Build 0205) possuíam menos de três meses de liberação para uso. À luz do item 4.2 do Anexo E, apesar de admitir o uso de versão estável imediatamente anterior, a LICITANTE demonstrou tratar-se das versões mais recentes, estáveis, oficiais e disponíveis pelos canais oficiais de suporte do fabricante para todos os clientes da solução. O grupo técnico, então, concluiu pela compatibilidade do uso das referidas versões nos testes de bancada. A verificação da disponibilização ampla das versões de

firmware utilizadas na amostra, bem como seus *checksums* associados, podem ser observados nos *prints* "*Screen Shot 2018-09-24 at 10.19.51.png*", "*Screen Shot 2018-09-24 at 10.20.33.png*", "*Screen Shot 2018-09-24 at 10.21.00.png*" e "*Screen Shot 2018-09-24 at 10.22.05.png*".

Os equipamentos *firewall* FortiGate 1500D e de gerenciamento centralizado Fortimanager 300E foram reiniciados para as configurações de fábrica e formatados, conforme *prints* nas páginas 9 a 16 do RTA. A cópia de todas as evidências foi entregue ao Grupo Técnico, em mídia desta, com os respectivos *hashes*.

A LICITANTE também executou as configurações e testes em *loop* do equipamento gerador de tráfego, de forma a atender o disposto no item 4.9 do Anexo E. Os relatórios dos testes em loop fazem parte da documentação comprobatória e se encontram no diretório "*24092018/Spirent/Relatorios/Teste_Loop*", a saber: "*L4_Assert_Summary_Client_Loop.csv*", "*L4_Assert_Summary_server_Loop.csv*", "*Lote4_Full_Assert_detail_Loop.PNG*", "*Lote4_Full_Assert_summary_Loop.PNG*", "*UDP_report.pdf*" e "*L4_Full_ UDP_Loop.PNG*". Reitera-se que, durante a execução dos testes, o grupo técnico armazenou em mídia externa própria, com os respectivos *hashes*, as informações que a empresa avaliada produziu, como *prints* e arquivos de configuração.

3. DOS TESTES DE CONFORMIDADE

3.1) Das Configurações Dos Testes

A amostra foi configurada para os testes conforme topologia apresentada nas páginas 5 a 7 do RTA, atendendo ao disposto no item 5.1.6 do Anexo E. As configurações relativas a quantidade de clientes, servidores, regras, redes e perfil de tráfego gerado foram validados pelo Grupo Técnico, tanto por meio dos *scripts* de configuração (apresentados entre as páginas 66 e 298 do RTA) quanto por meio de verificação direta na amostra e no equipamento gerador de tráfego.

As configurações solicitadas no item 5.1.1 a 5.1.12 do anexo E foram evidenciadas pela LICITANTE nas páginas 17 a 25 do relatório e nos *scripts* anexos, além das capturas de imagens da execução das configurações, evidenciando as funcionalidades habilitadas no *firewall*. Foram apresentadas as listas de ameaças/ataques, URLs e aplicações do equipamento gerador de tráfego, conforme consta nas páginas 61 a 65 do RTA à luz do disposto no item 5.1.2.1 do Anexo E.

O firewall multifuncional avaliado foi configurado de modo a atender ao item 5.1.3 do Anexo E, que cita que "*a amostra deve ser configurada de forma a realizar a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo*". Restou constatado que a solução apresentada foi capaz de ser configurada para atender o referido item, de modo a executar a inspeção de todos os pacotes em um único fluxo de dados, assim como fazê-la independentemente de sua direção, conforme o exposto na página 78 do RTA (regra única com todos os serviços de segurança habilitados/habilitáveis sob demanda).

O equipamento de gerência centralizada FortiManager 300E foi configurado para a coleta e processamento dos *logs* do *firewall*, conforme apresentam as páginas 21 a 24 do RTA, em atendimento ao disposto no item 5.1.5 do Anexo E, bem como foram realizados os *backups* dos equipamentos.

3.2) Dos Testes De Assertividade

A equipe técnica da LICITANTE realizou os testes de assertividade conforme o disposto 5.2 do Anexo E - Testes de Conformidade. A empresa licitante optou por executar os testes de assertividade separadamente, de forma que apenas a funcionalidade relacionada ao serviço de segurança objeto de avaliação dos subitens "i" a "iv" do item 5.2.4 analisasse o fluxo de dados injetado pelo equipamento gerador de tráfego. Como resultado, observa-se o seguinte:

3.2.1) a assertividade do subitem 5.2.4-i – "*Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS*" foi avaliada e está evidenciada nas páginas 28 e 29 do RTA entregue pela licitante e nos resultados coletadas, sendo que dos 2479 ataques distintos gerados pelo equipamento Spirent, 2362 foram bloqueados pela amostra em análise, distribuídos em 1461 categorias/assinaturas. Conforme *print* "*Screen Shot 2018-09-24 at 14.57.19.png",* todas as 11824 assinaturas da base IPS da amostra foram ativadas para uso nos testes.

O grupo técnico observou que o total de categorias/assinaturas distintas identificadas pela amostra era menor do que o total de ataques reportados como bloqueados. Em esclarecimento junto à LICITANTE, o grupo técnico constatou nos *logs* da amostra, à luz do item 5.2.5.2 do Anexo E, que determinadas assinaturas categorizaram mais de um ataque (sendo cada ataque, na ferramenta geradora, associado a um único código CVE), mas que a referência e o somatório das ocorrências de ataques das assinaturas com múltiplas detecções e daquelas com apenas uma detecção, listadas no arquivo de relatório "*S-9_t9-MPOG - IPS Events-2018-09-24-1525_9.pdf*" (e arquivos de *logs* associados) são compatíveis e equivalentes com o total de ataques bloqueados reportados pela ferramenta geradora de tráfego (perfazendo, portanto, índice de 95,28% de assertividade. E dentro dos limites estabelecidos nas exigência editalícias).

Ainda para dirimir dúvidas e avaliar em maior detalhe tal comportamento da amostra e sua capacidade de detecção, classificação e bloqueio dos ataques tanto em tráfego não criptografado quanto em tráfego criptografado, o grupo técnico, sob a égide do item 5.2.3 do Anexo E, solicitou a alteração da massa de ataques utilizada para testes, oportunidade na qual o grupo técnico selecionou, diretamente no equipamento gerador, os ataques adicionais que deveriam ser utilizados, tendo por base listas de ataques reais identificados nas redes de órgãos da Administração Pública Federal, bem como ataques utilizados na massa de testes de outros Lotes objetos do PE05/2017 – como é o caso de ataque de *SQL Injection* em protocolo HTTPS.

Submetendo-se a nova massa de testes modificada a partir do equipamento gerador – um total de 2504 ataques, conforme relatório "*L4_Assert_IPS_Modif.pdf*" –, foram bloqueados 2376, sendo categorizados pela amostra em 1583 assinaturas distintas, conforme *print* "*Screen Shot 2018-09-25 at 12.09.10.png".* O grupo técnico observou o

comportamento idêntico em relação à primeira massa de testes e foi capaz de validar tanto a compatibilidade das assinaturas com múltiplas detecções/classificações quanto as assinaturas com uma única detecção/classificação em equivalência à nova massa de testes, perfazendo, portanto, taxa de assertividade de 94,88%. Tendo por base tais resultados, o grupo técnico comprovou a capacidade e assertividade da amostra para bloqueio e classificação dos ataques IPS. Os relatórios, *prints*, *logs* e arquivos que listam os ataques das duas massas de testes, bem como as capturas de pacotes dos testes efetuados foram salvos na mídia fornecida pelo grupo técnico. Os resultados dos testes adicionais observados na amostra, solicitados pelo grupo técnico, estão evidenciados nas páginas 46 e 47 do RTA entregue pela LICITANTE.

O grupo técnico também solicitou que a nova massa de testes modificada fosse a doravante utilizada para os demais testes (performance e sessões).

3.2.2) a assertividade do subitem 5.2.4-ii – "*Categorizar e bloquear as ameaças em, no mínimo 2.000 (duas mil) assinaturas de malwares distintas*" foi comprovada e está evidenciada na página 27 do RTA entregue pela licitante e nas evidências coletadas, sendo que, dos 2032 *malwares* gerados, 1859 foram bloqueados e categorizados em 1713 tipos diferentes, conforme mostra o *print* "*Screen Shot 2018-09-24 at 14.32.10.png*" e o relatório "*S-6_t6-MPOG - Malware-2018-09-24-1431_1.pdf*".

De forma semelhante ao item 3.2.1 supracitado, algumas assinaturas de *malware* classificaram mais de um artefato submetido pelo gerador de tráfego, resultando em múltiplas detecções em tais assinaturas, mas o somatório foi compatível aos resultados observados pelo gerador (perfazendo, portanto, índice de 91,48% de assertividade). A lista de *malwares* e os resultados do equipamento gerador de tráfego Spirent foram salvos no relatório "*L4_Assert_Relatorio_AV.pdf*" e, dos resultados da amostra, nas evidências "*Assertividade_Malware.csv.log.gz*" e "*Assertividade_Malware.txt.log.gz*".

3.2.3) a assertividade do subitem 5.2.4-iii – "*Categorizar e bloquear, pelo menos, 100 (cem) aplicações distintas*" foi comprovada e está evidenciada nas páginas 31 a 45 do RTA entregue pela licitante e nas evidências coletadas, sendo que, das 100 aplicações submetidas pelo gerador, 98 foram bloqueadas e classificadas em 94 tipos distintos, (perfazendo, portanto, índice de 98% de assertividade). De forma semelhante aos itens anteriores, a diferença entre os valores de bloqueio e categorização foi justificada pela classificação realizada pela amostra, que categoriza, em alguns casos, mais de uma aplicação gerada pelo equipamento *Spirent* em um mesmo tipo de aplicação. A lista de aplicações geradas foi exportada em arquivo PDF a partir do equipamento gerador e anexada às evidências coletadas durante os testes, no arquivo "*L4_Assert_app.pdf*". Foram coletadas também capturas de tela e os *logs* resultantes, contidos nos arquivos "*Assertividade_Aplicacoes.txt.log.gz*" e "*Assertividade_Aplicacoes.csv.log.gz*", que contém as categorias identificadas pela amostra.

De forma complementar, motivado por conhecida limitação do equipamento gerador acerca da geração de tráfego em aplicações específicas que utilizam criptografia e ainda por aplicações obrigatórias que não constavam nos tipos identificados, foram

executados manualmente testes de identificação e bloqueio de mais 26 aplicações indicadas no caderno de testes, sendo que todas foram identificadas e bloqueadas pela amostra, conforme apresentado às páginas 33 a 45 do RTA.

3.2.4) a assertividade do subitem 5.2.4-iv – "*Classificar os acessos em, no mínimo, 5.000 (cinco mil) sites distintos de internet, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias distintas sendo bloqueados 25% deste total escolhidos por categorias específicas definidas pelo grupo técnico de apoio ao pregoeiro no momento do teste*" foi comprovada e está evidenciada nas páginas 27 e 28 do RTA entregue pela LICITANTE e nas evidências coletadas durante os testes. Os resultados coletados indicaram a categorização de 5500 URLs distribuídas em 70 categorias distintas, incluindo a categoria "Unrated", na qual foram contabilizadas 7 URLs.

Durante a execução dos testes, o grupo técnico de apoio à contratante selecionou categorias para bloqueio, atendendo ao que estava disposto nesta mesma alínea, perfazendo um total de 26,83% de URLs bloqueadas. O relatório do equipamento gerador de tráfego *Spirent* foi nomeado como "*L4_Assert_URL.pdf*" e apresenta o resultado na página 2, bem como a lista de URLs utilizadas. O arquivo "*S-8_t8-MPOG - Website and Category-2018-09-24-1453_3.pdf*" e os *log*s contidos em "*Assertividade_URLs.txt.log.gz*" e "*Assertividade_URLs.csv.log.gz*" evidenciam as categorizações realizadas pela amostra.

Após a realização dos Testes de Assertividade, a LICITANTE executou os procedimentos para apagar os *logs* e configurações da amostra, de forma a atender o disposto no item 5.2.7 do Anexo E - Testes de Conformidade. Os comandos executados estão indicados na página 48 do RTA entregue pela licitante.

3.3) Dos Testes De Desempenho

A equipe técnica da LICITANTE realizou os testes de desempenho conforme o disposto no item 5.2 do Anexo E - Testes de Conformidade, sendo a amostra configurada de acordo com o determinado pelos itens 5.3.1 a 5.3.6 do Anexo E. Foram utilizados os comandos dos scripts anexos ao RTA, nas páginas 66 a 298, para a criação das regras, NAT's e objetos necessários para os testes, sendo sua execução acompanhada e validada *in loco* pelo grupo técnico. A topologia do ambiente de testes de desempenho foi apresentada nas páginas 6 e 7 do RTA. Após execução dos procedimentos, foi realizado um backup das configurações da amostra, sendo este nomeado de "*Backup_FG-1500D_Performance.conf*" e anexado às evidências produzidas pela licitante, atendendo ao disposto no item 5.3.5 do Anexo E. A LICITANTE evidenciou os resultados dos testes de desempenho entre as páginas 49 e 55 do RTA.

A parametrização prevista no item 5.3.7 do Anexo E foi coletada a partir do equipamento gerador de tráfego e foi evidenciada no RTA entre as páginas 49 e 52. O perfil de tráfego especificado no item 5.1.12 foi coletado no *print* "*L4_Perf_25_ProtDistrib_30Min.PNG*", proveniente do equipamento gerador, e apresentado na página 50. Também coletou-se e somou-se a esse perfil o tráfego

proveniente do protocolo UDP ("*L4_Perf_25_UDP_30min.PNG*") e do tráfego VPN IPSec ("*L4_Perf_25_IPSec_30min.PNG*"), de forma a perfazer o total de 25% do *throughtput* especificado para o Lote 4 (valor alcançado de 1,263Gbps) e viabilizar, assim, a coleta dos valores de latência média e *Jitter* (268us e 252us, respectivamente, evidenciados na página 43 do relatório do equipamento gerador de tráfego nomeado como "*UDP_report.pdf*").

O relatório "*UDP_report.pdf*", página 29 e "*L4_Perf _25_final.pdf*", no seu quadro *Transport Error Analysis* na página 2, mostram que houve perda de pacotes e erros de transações TCP durante a parametrização menores que 0,0005%. Durante toda a parametrização, o tráfego proveniente dos testes de assertividade foi submetido à amostra, de forma a evidenciar que as funcionalidades de segurança estavam habilitadas em modo detecção, conforme reza o item 5.3.4 do Anexo E. A comprovação de tais detecções é evidenciada nos arquivos "*L4_Assert_25_client_summary.csv*" e "*L4_Assert_25_server_summary.csv*", retirado do equipamento gerador e os *logs* contidos no arquivo "*FGTADOM3_tlog_from_2018-09-25_14_40_00_to_2018-09-25_15_40_00.csv.log.gz*".

Após parametrização da amostra, foram executados procedimentos para zerar contadores e *logs*, conforme previsto no item 5.3.7.1 do Anexo E, sendo que estes procedimentos ficaram evidenciados no *print* "*Screen Shot 2018-09-25 at 15.47.17.png*".

Os dados referentes ao item 5.3.8, relacionados ao Teste de Desempenho total executado após a parametrização, foram coletados pelo grupo técnico, em mídia própria, e apresentados pela LICITANTE nas páginas 52 a 55 do RTA. Foi comprovada a geração suficiente e tratamento de *throughput* mínimo de 4,25Gbps, que corresponde a 85% da vazão prevista para o Lote 4, conforme especifica o item 5.3.8 do Anexo E. Os dados referentes à banda total gerada e submetida à amostra indicaram um valor de aproximadamente 4,45Gbps, respeitando a mesma distribuição verificada na fase de parametrização. Tais volumes podem ser observados nos *prints* coletados diretamente do equipamento gerador, "*L4_Perd_Throughput_Full_30min.PNG*", "*L4_Perf_UDP_Full_30min.PNG*" e "*L4_Perf_IPSec_Full_30min.PNG*".

A amostra foi monitorada pelo grupo técnico e mostrou-se capaz de suportar e tratar o volume supracitado sem prejuízo em sua performance, dentro dos parâmetros estabelecidos pelo item 5.3.8.3, comprovando-se tanto por meio dos *prints* de tela coletados (a exemplo do apresentado na página 55 do RTA) quanto pelos *logs* do firewall (conteúdo do arquivo "*FGTADOM3_tlog_from_2018-09-25_15_50_00_to_2018-09-25_16_40_00.csv.log.gz*") e pelos *prints* de tela do equipamento *firewall* e da ferramenta de gerência centralizada (a exemplo dos *prints* "*Screen Shot 2018-09-25 at 16.28.18.png*" e "*Screen Shot 2018-09-25 at 16.27.55.png*").

Os dados referentes à "latência média" e à "variação média de latência (jitter)" foram coletados pelo grupo técnico e apresentados pela LICITANTE na página 53 do RTA, sendo de aproximadamente 1810us e 871us, respectivamente. Tais valores são menores, portanto, que 10 vezes quando comparados a aqueles observados na fase de parametrização. O relatório "*L4_quarter.csv"*, mostra que houve 0% de perdas absolutas de pacotes. Tais valores foram inferiores, portanto, ao limite máximo para aprovação, à luz dos subitens 5.3.8.3.i e 5.3.8.3.iii do Anexo E.

Quanto aos "erros absolutos irrecuperáveis de transações TCP/layer-7", foi verificado no relatório "*Relatorio_L4_Perf_100.pdf*", em seus quadros *Transport Error Analysis* para todos os protocolos, que houve erros de aproximadamente 0,0003%, inferior, portanto, ao limite máximo para aprovação, à luz do subitem 5.3.8.3.ii.

Quanto à "detecção de ameaças, aplicações, ataques e URLs", conforme disposto no subitem 5.3.8.3.iv, foram coletados *prints* e *logs* no diretório \NCT_MPOG_PE052017_Lote4\25092018\NCT, da mídia utilizada para coletar as evidências, que evidenciam as detecções das ameaças geradas pelos serviços de segurança da amostra, assim como suas funcionalidades ativas e configurações, atingindo o resultado de aprovação especificado pelo referido item. Os logs de tais detecções estão listados no conteúdo do arquivo "*FGTADOM3_tlog_from_2018-09-25_15_50_00_to_2018-09-25_16_40_00.csv.log.gz*".

3.4) Dos Testes De Sessão

A equipe técnica da LICITANTE realizou os testes de sessão conforme disposto no item 5.4 do Anexo E - Testes de Conformidade, sendo a amostra configurada e seu *backup* realizado de acordo com o determinado pelos itens 5.4.2.1 e 5.4.3.1 do referido anexo. Os resultados referentes aos Testes de Sessão estão indicados entre as páginas 56 e 59 do RTA enviado pela LICITANTE. Conforme determina o Anexo E, os dois testes de sessão foram realizados na ordem estipulada (primeiro e segundo testes), com a amostra sendo considerada aprovada por atingir os resultados do segundo teste, a saber:

3.4.1) Primeiro teste: conforme apresentado pela LICITANTE e evidenciado nos *prints* coletados do gerador de tráfego e *firewall*, não foi possível gerar com o *Spirent*, na quantidade necessária e com o perfil de tráfego solicitado pelo item 5.1.12, o número mínimo de novas sessões por segundo e de conexões simultâneas requerido para o teste - um total de 50% do número determinado para o Lote 4, respectivamente, nos itens 3.22.1.9 e o total do item 3.22.1.8 do Anexo B, que equivale a 45 mil novas conexões por segundo e 2 milhões de conexões simultâneas. Conforme evidenciam os *prints* "*Screen Shot 2018-09-25 at 16.59.23.png*", "*Screen Shot 2018-09-25 at 16.59.37.png*" e demais evidências coletadas pelo grupo técnico, foi atingido um valor aproximado de apenas 1.400 novas conexões por segundo e 15,2 mil sessões simultâneas, utilizando-se o mesmo *throughput* dos testes de desempenho específicos do Lote 4.

3.4.2) Segundo teste:

Após efetuar o *factory reset*, zeragem dos contadores e reconfiguração do equipamento, a partir do *backup* previamente gerado (em atendimento ao item 5.4.2.6 do Anexo E), foi realizado o segundo teste de sessão, com perfil de tráfego simplificado, em acordo ao especificado no item 5.4.3.

Evidenciado pelos *prints* "*L4_Test CPS OK.PNG*" e "*Screen Shot 2018-09-25 at 17.36.13.png*", a amostra atingiu um processamento aproximado de 162 mil novas sessões por segundo, superior, portanto, ao mínimo de 90 mil novas sessões por segundo exigidas para o Lote 4. De forma semelhante, conforme atestam o print "*L4_Teste CC*

ok.PNG" e o *print* "*Screen Shot 2018-09-25 at 17.19.02.png*", foi atingido um total aproximado de 2,4 milhões de conexões simultâneas, superior, portanto, ao mínimo de 2 milhões exigidos para o referido lote.

3.5) Dos Testes Complementares

A LICITANTE realizou os testes complementares solicitados pelo grupo técnico, de forma a esclarecer dúvidas acerca do funcionamento da amostra e do sistema de gerenciamento centralizado. Os resultados são referenciados na página 60 do RTA.

Em relação ao esclarecimento do item 2.1.32 do Anexo B - Especificações Técnicas, no que diz respeito especificamente à capacidade de detecção e bloqueio de ataques envolvendo variações de reflexão, a amostra mostrou-se capaz de detectar e bloquear tais ameaças. A LICITANTE indicou no relatório imagens do resultado (*prints* das páginas 29 a 31), além do relatório "*L4_Assert_DNSreflection.pdf*" e do arquivo pcap obtido no gerador de tráfego (arquivo "*L4_Assert_DNSreflection_client.pcap*") e dos *logs* obtidos na amostra, contidos no arquivo "*Logs_Ataque_Reflexao_csv.log.gz*".

Em relação ao esclarecimento do item 2.2.4 do Anexo B - Especificações Técnicas, a LICITANTE indicou no relatório que o equipamento FortiManager 300E possui a funcionalidade de executar, além das funções de gerenciamento dos equipamentos, todas as funcionalidades relacionadas à captura e análise de logs e eventos de todos os equipamentos gerenciados, ou seja, "captura e filtragem de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade". Da mesma forma, foi esclarecido pela LICITANTE que o equipamento gerenciador em questão não possui limitação quanto à sua capacidade de recebimento dos *logs* e eventos dos equipamentos, não havendo perda de informações, sendo a limitação de dimensionamento do equipamento determinados pela quantidade de equipamentos *firewall* que é capaz de gerenciar e o espaço em disco para guarda de *logs* e eventos. Para o FortiManager 300E apresentado, suas especificações permitem até 100 dispositivos gerenciados e 5.5GB de espaço de armazenamento, superiores aos requisitos exigidos para o Lote 4, conforme itens 3.22.1.7 e 3.28.1.2 do Anexo B – Especificações Técnicas.

Esclareceu-se que, em eventuais períodos em que a taxa de recebimento extrapola o valor de 2GB de logs por dia, o equipamento emite um alerta, mas todas as informações recebidas são processadas e inseridas em seu banco de dados e filtros – tal afirmação mostrou-se compatível com as evidências verificadas e coletadas pela equipe técnica durante os testes de desempenho e sessões, apresentado em *prints* de tela, a exemplo dos arquivos "*Screen Shot 2018-09-25 at 17.40.30.png*" e "*Screen Shot 2018-09-25 at 18.17.01.png*".

Em relação ao esclarecimento do item 3.22.1.5 do Anexo B – Especificações Técnicas, no que diz respeito à capacidade do equipamento a discos locais em RAID 1 para armazenamento de *logs*, foi demonstrada e esclarecida a presença de dois discos do tamanho mínimo requerido e sua configuração em RAID 1, conforme exposto à página 60 do RTA e observado pelo grupo técnico durante as preparações iniciais para os testes de conformidade.

4. CONCLUSÃO

Tendo em vista as evidências observadas e coletadas durante a execução dos testes, juntamente com a documentação do fabricante, assim como os resultados apresentados no RTA ora analisado e entregue pela LICITANTE, a equipe técnica de apoio ao pregoeiro concluiu que a amostra apresentada para testes referentes ao Lote 4 comprovou integralmente o atendimento aos itens propostos no caderno de testes, atendendo e obedecendo aos requisitos técnicos constantes do edital do Pregão eletrônico nº 5/2017.