TERMO DE AVALIAÇÃO DE AMOSTRA - LOTE 3

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 3: Empresa avaliada - NCT INFORMÁTICA.

1. OBJETIVO

O teste de conformidade da amostra visa à aferição da real capacidade técnica dos equipamentos ofertados pela Licitante Convocada. Busca-se comprovar, juntamente com a documentação do fabricante, se os equipamentos de fato atendem aos requisitos constantes da especificação técnica do Anexo B do Termo de Referência do Pregão nº 5/2017.
Na avaliação dos Testes de Conformidade, serão levados em consideração o Relatório dos Testes da Amostra entregue pela licitante e as evidências coletadas pela equipe técnica durante a execução dos testes.

2. DA DISPOSIÇÕES GERAIS, DA AMOSTRA E DA PREPARAÇÃO INICIAL

A licitante atendeu de forma satisfatória a execução dos itens pertinentes às disposições gerais durante a execução dos testes, respondendo aos pedidos de "alterações nas gerações das ameaças, ataques, aplicações, percentuais ajustáveis de tamanho de pacote, políticas, tipos de tráfego, dentre outros, para todos os componentes da solução", conforme previsto no item 2.17 do Anexo E, 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 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 Relatório dos Testes da Amostra do lote 3 entregue apresentou-se de forma organizada, atendendo ao que está disposto no item 2.25 do mesmo Anexo E. Além do relatório entregue pela licitante, foram coletadas em mídia digital fornecida pela contratante evidências produzidas durante a execução dos testes, como *prints*, arquivos de configuração e relatórios do gerador de tráfego, todos com os respectivos *hashes* para comprovar a sua inviolabilidade e autenticidade.

A amostra apresentada na bancada estava em conformidade com o produto ofertado em proposta, atendendo ao que determina o item 3.1 do Anexo E. A página 7 do Relatório dos Testes da Amostra apresenta a lista de equipamentos utilizados no teste de bancada.

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. O relatório evidencia esses procedimentos entre as páginas 8 e 16. A

cópia de todas as evidências foi entregue ao grupo técnico da CONTRATANTE, em mídia desta, com os respectivos *hashes*. O *backup* das configurações iniciais foi nomeado como "Backup_FGT-500D_C1", para o equipamento Fortigate 500D e "Backup_FMG-200D_C1" para o equipamento Fortimanager 200D. Na mesma mídia digital também foram salvos os *hash* MD5 das pastas de evidências.

A empresa avaliada também executou o teste 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 "Spirent/Relatorios/Teste em Loop". Os relatórios foram nomeados como "L3_Assert_Full_Client_Loop", "L3_Assert_Full_ Server_Loop", "L3_Perf_Full_Client _Loop" e "L3_Perf_Full_Server_Loop".

Ressalte-se que durante a execução dos testes, diariamente, a equipe técnica que acompanhou os testes 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

a. DAS CONFIGURAÇÕES DOS TESTES E TOPOLOGIA

A amostra foi configurada para os testes conforme topologia apresentada nas páginas 5 e 6 do relatório entregue pela licitante, atendendo ao disposto no item 5.1.6 do Anexo E – Testes de Conformidade. Além disso, as configurações como quantidade de clientes, servidores, regras, redes e perfil de tráfego gerado também foram validados pelo grupo técnico da CONTRATANTE, sendo que algumas configurações, como regras/políticas e ativação de funcionalidades, foram verificadas na amostra, assim como em *scripts* executados, e outras, como quantidade de clientes, servidores e perfil de tráfego, verificadas no equipamento gerador de tráfego.

As configurações solicitadas no item 5.1.2 foram evidenciadas pela empresa avaliada nas páginas 18 e 19 do relatório, através da execução de *scripts* e capturas de imagens da execução dos testes, evidenciando as funcionalidades habilitadas no *firewall*. Além disso, anexo ao caderno de testes apresentado, foram entregues as listas de ataques, ameaças, sites e aplicações que foram utilizados nos testes, conforme 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 - Testes de Conformidade, 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". Ou seja, a solução apresenta na amostra foi capaz de ser configurada de modo a executar a inspeção de todos dos pacotes em um único fluxo de dados, assim como fazê-la independentemente de sua direção, conforme definido no edital em epígrafe.

A Solução de Gerência Centralizada também foi integrada ao *firewall* multifuncional, de forma que a execução do item 5.1.5 do Anexo E - Testes de Conformidade ficasse comprovada, conforme apresentado entre as páginas 21 e 23 do relatório entregue pela licitante.

Após a configuração inicial, foi executado o *backup* das configurações e o arquivo, salvo juntamente com as demais evidências anexas ao relatório, nomeado como "Backup_FGT-500D_C2".

b. DOS TESTES DE ASSERTIVIDADE

O representante da empresa responsável pelo equipamento gerador de tráfego fez as alterações solicitadas pela equipe técnica de apoio à CONTRATANTE, atendendo ao disposto no item 5.2.3 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 item do objeto em avaliação avaliasse o fluxo de dados injetado pelo equipamento de testes.

A assertividade quanto à alínea "i) Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS" do item 5.2.4 do Anexo E está evidenciada nas páginas 45 e 46 do Relatório dos Testes da Amostra entregue pela licitante, sendo que dos 2483 ataques gerados, 2417 foram identificados e bloqueados pelo *firewall* multifuncional. A lista de ataques identificados também foi exportada, a partir da amostra avaliada, em arquivo PDF e anexada às evidências salvas em mídia digital da contratante. O Relatório do equipamento gerador de tráfego Spirent foi nomeado como "L3_Assert_Ataques_client" e apresenta o resultado na página 2, indicando que 97,34% dos ataques foram identificados e bloqueados pela amostra em avaliação.

A assertividade quanto à alínea "ii) Categorizar e bloquear as ameaças em, no mínimo 2.000 (duas mil) assinaturas de malwares distintas" do item 5.2.4 do Anexo E está evidenciada nas páginas 26 e 27 do Relatório dos Testes da Amostra entregue pela licitante, sendo que 1984 *malwares* foram bloqueados. A lista de *malwares* também foi exportada em arquivo PDF a partir da amostra avaliada e anexada às evidências coletadas durante os testes. O Relatório do equipamento gerador de tráfego Spirent, que possui o nome "L3_Assert_Ameacas_client_reteste", apresenta o resultado na página 2, indicando que 97,54% dos ataques injetados na amostra foram identificados e bloqueados.

A assertividade quanto à alínea "iii) Categorizar e bloquear, pelo menos, 100 (cem) aplicações distintas" do item 5.2.4 do Anexo E ficou evidenciada entre as páginas 27 e 45 do relatório entregue pela licitante. A lista de aplicações também foi exportada em arquivo PDF a partir da amostra avaliada e anexada às evidências coletadas durante os testes. Além disso, também foram registradas capturas de telas dos testes complementares de identificação e bloqueio de aplicações solicitados no caderno de testes. O relatório do equipamento gerador de tráfego, nomeado como "L3_Assert_APPs_client" apresenta o resultado na página 2, indicando que das 118 aplicações analisadas pela amostra, 117 foram identificadas e bloqueadas. De forma complementar, foram executados testes de identificação e bloqueio de mais 40 aplicações indicadas no caderno de testes, sendo que todas foram identificadas e bloqueadas pela amostra.

A assertividade quanto à alínea "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" do item 5.2.4 do Anexo E está evidenciada na página 6 do Relatório dos Testes da Amostra entregue pela licitante. Os resultados apresentados no relatório citado indicaram a categorização de 5500 URLs distribuídas em 71 categorias distintas, incluindo a categoria "Unrated", na qual foram contabilizadas 18 URLs. As listas de categorias e de URLs foram exportadas em arquivo PDF a partir da amostra avaliada e anexada às evidências coletadas durante os testes. Durante a execução dos testes, o grupo técnico de apoio à contratante selecionou categorias para bloqueio, atendendo ao que estava disposto nesta mesma alínea. O relatório do equipamento gerador de

tráfego Spirent nomeado como “L3_Assert_URLs_Adicio_Client” apresenta o resultado na página 2. Quanto ao bloqueio de sites, que deveria apresentar resultado superior a 25%, o número apresentado neste mesmo relatório foi de 39,14% das URLs analisadas.

Após a realização dos Testes de Assertividade, a empresa avaliada executou os procedimentos para apagar os *logs* e configurações da amostra, de forma a atender o item 5.2.7 do Anexo E - Testes de Conformidade. Os comandos executados estão indicados nas páginas 46 e 47 do Relatório de Testes da Amostra entregue pela licitante.

c. DOS TESTES DE DESEMPENHO

Para os Testes de Desempenho, o grupo técnico da licitante executou os procedimentos para configurar a amostra avaliada de acordo com o que determina o item 5.1 do Anexo E - Testes de Conformidade. Foram utilizados, além de comandos executados durante os testes, *scripts* de configuração listados no arquivo “Script_MPOG.rtf”. A licitante evidenciou os resultados dos testes de desempenho entre as páginas 47 e 52 do Relatório de Testes da Amostra. A topologia do ambiente de testes foi apresentada nas páginas 5 e 6 e as configurações solicitadas entre os itens 5.1.8 e 5.1.11 foram apresentadas nas páginas 23 e 24, todas no mesmo relatório entregue pela licitante. Após execução dos procedimentos, foi realizado um backup das configurações da amostra, sendo este nomeado de “Backup_FGT-500D_C3.conf” e anexado às evidências produzidas pela licitante. Desta forma, atendendo ao que está disposto no item 5.3.5 do Anexo E.

A parametrização prevista no item 5.3.7 do Anexo E - Testes de Conformidade foi evidenciada em relatório entre as páginas 47 e 49. O perfil de tráfego especificado no item 5.1.12 foi apresentado em *print* anexado ao relatório, nomeado como “Distribuicao de Protocolos.PNG”. Esta captura de tela foi retirada do equipamento gerador de tráfego Spirent. A distribuição apresentada atendeu ao que está disposto no Anexo E. Além disso, testes com o protocolo UDP e com tráfego em VPN IPSec também foram executados.

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 pela empresa avaliada na página 48 do relatório entregue.

As evidências referentes ao item 5.3.7 (25% da vazão prevista para lote 3) do mesmo Anexo, relacionados à parametrização, indicam que os dados referentes à taxa de transferência indicaram um resultado de 250 Mbps para o perfil de tráfego, sendo, aproximadamente, 12 Mbps para UDP e entre 12 Mbps e 13 Mbps para vazão de VPN IPSec. Esses dados são apresentados nos relatórios do equipamento gerador de tráfego, nomeados como “realtime client perf” e “UDP_25”, e em capturas de telas (*prints*) anexados às evidências, como os de nomes “ETH_IPsec”, “ETH0”, “ETH1”, “ETH3”, “ETH4”, “ETH7” e “Trafego Assert cliente e server”.

Os dados referentes à “latência média” e “variação média de latência (*jitter*)”, apresentados na página 48 do relatório, foram de aproximadamente 96us e 35us, respectivamente. Estes dados também foram evidenciados na página 2 do relatório do equipamento gerador de tráfego nomeado como “UDP_25”.

Quanto aos “erros absolutos irrecuperáveis de transações TCP/layer-7”, foi verificado no relatório em PDF de nome “*report client perf*”, exportado do equipamento gerador de tráfego, indicando que não ocorreram erros de transação.

Quanto à “detecção de ameaças, aplicações, ataques e URLs”, o Relatório de Testes da Amostra entregue pela licitante aponta na página 48 que no diretório \NCT_MPOG_PE052017\26042018\NCT da mídia utilizada para coletar as evidências, são apresentados os *prints* evidenciando o registro de *logs* na amostra, assim como suas funcionalidades ativas e configurações. Além disso, os *logs* foram exportados para o arquivo de nome “FGTADOM3_alog_from_2018-04-26_13_54_00_to_2018-04-26_14_24_00.csv.log” e salvo no mesmo diretório.

Os dados referentes ao item 5.3.8, relacionados ao Teste de Desempenho executado após a parametrização, foram apresentados pela licitante a partir da página 50 do relatório entregue, na qual apresenta inicialmente os comandos para executar o *reset* de todos os *logs* e estatísticas da amostra.

As evidências referentes ao item 5.3.8.2 (85% da vazão prevista para o lote 3) do mesmo Anexo estão indicados entre as páginas 50 e 52 do relatório. Os dados referentes à taxa de transferência indicaram um resultado de aproximadamente 1 Gbps para o perfil de tráfego, sendo, aproximadamente, 50 Mbps para UDP e entre 37 e 39 Mbps para vazão de VPN IPSec. Esses dados são apresentados nos relatórios do equipamento gerador de tráfego, nomeados como “*report perf client realtime*” e “UDP_100”, e em *prints* anexados às evidências, como os de nomes “ETH_IPSec”, “ETH_0”, “ETH_1”, “ETH_3”, “ETH_4”, “ETH_7, “Trafego Client All” e “Trafego Server All”, salvos no diretório \NCT_MPOG_PE052017\26042018\Spirent\Relatorios\Teste 100porcento da mídia utilizada para coletar as evidências.

Os dados referentes à “latência média” e à “variação média de latência (*jitter*)”, apresentados na página 50 do relatório, foram de aproximadamente 186us e 67us, respectivamente. Estes dados também foram evidenciados na página 2 do relatório do equipamento gerador de tráfego nomeado como “UDP_100”.

Quanto aos “erros absolutos irrecuperáveis de transações TCP/layer-7”, foi verificado no relatório em PDF de nome “*report perf client summary*”, exportado do equipamento gerador de tráfego, que não ocorreram erros de transação.

Quanto à “detecção de ameaças, aplicações, ataques e URLs”, o Relatório de Testes da Amostra entregue pela licitante aponta na página 51, que no diretório \NCT_MPOG_PE052017\26042018\NCT da mídia utilizada para coletar as evidências, são apresentados os *prints* evidenciando o registro de *logs* na amostra, assim como suas funcionalidades ativas e configurações. Além disso, os logs foram exportados para o arquivo de nome FGTADOM3_tlog_from_2018-04-26_16_09_00_to_2018-04-26_16_39_00.csv.log.gz e salvo no mesmo diretório.

A comparação entre os resultados, solicitada no item 5.3.8.3 do Anexo E - Testes de Conformidade, não apresentou “perda absoluta de pacotes” e o registro de “erros absolutos irrecuperáveis de transações TCP/layer-7”, conforme já citado, também foi zerado. Os valores de “latência média” e de “variação média de latência (*jitter*)” apresentaram aumento em relação aos que foram coletados na parametrização, sendo que em ambas o aumento foi inferior a 10 vezes.

As evidências quanto à “deteção de ameaças, ataques, aplicações e URLs”, conforme já citado, foram apresentados em *prints* e arquivos de *log* exportados da amostra, ambos anexados às evidências coletadas.

d. DOS TESTES DE SESSÃO

As evidências referentes aos Testes de Sessão estão indicadas entre as páginas 53 e 56 do Relatório de Testes da Amostra enviado pela licitante. Inicialmente, a licitante utilizou as mesmas configurações utilizadas para os testes de desempenho, conforme disposto no item Após execução dos procedimentos para configurar a amostra, foi realizado o *backup* das configurações, conforme disposto no item 5.3.5 do Anexo E.

A amostra avaliada não alcançou os resultados determinados para o primeiro teste de sessões indicados nos itens 5.4.2.2 e 5.4.2.3, conforme evidenciado na página 53 do relatório. Após execução do primeiro teste de sessão, os *logs* e estatísticas da amostra foram zerados, conforme demonstrado na mesma página. Além disso, suas configurações foram restauradas, de forma que fosse atendido o item 5.4.2.6. Feitos os ajustes para o segundo teste, o backup do arquivo de configuração foi salvo com o nome de "Backup_FGT-500D_C4".

Segundo imagens exportadas do equipamento gerador de tráfego, o segundo teste de sessão atingiu 500.000 conexões simultâneas, atendendo ao que está disposto no item 5.4.3.2.1. do Anexo E - Testes de Conformidade. O resultado do teste de mensuração de novas sessões por segundo apresentou a taxa de aproximadamente 86.500 novas conexões por segundo, atendendo ao que está disposto no item 5.4.3.1.1. do mesmo anexo e, por conseguinte, atendendo ao disposto no item 5.4.1 do referido Anexo E.

As imagens apresentadas no relatório foram validadas entre as capturas de tela (*prints*) que foram colhidas durante a execução dos testes.

e. DOS TESTES COMPLEMENTARES

O Relatório de Testes da Amostra entregue pela licitante apresenta, nas páginas 57 e 58, os resultados dos testes complementares solicitados pela contratante quando da avaliação do caderno de testes proposto. Em relação ao 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 licitante indicou no relatório imagens do resultado, além de arquivo pcap e de *logs* dos testes, sendo este último nomeado como "Ataque_Reflexao_Logs_IPS.csv.log.gz".

Quanto ao item 2.2.4 do Anexo B - Especificações técnicas, a empresa licitante indicou no relatório que o equipamento Fortimanager 200D possui a capacidade de executar todas as funcionalidades relacionadas à solução FortiAnalyzer, ou seja, "captura e filtragem de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade".

O item 3.15.1.2 foi comprovado através da execução dos Testes de Desempenho em conjunto com as evidências coletadas durante os testes, de forma que ficou evidenciada a capacidade de performance, assim como a inspeção integral dos pacotes independentemente da direção do fluxo de dados.

4. CONCLUSÃO

Diante do que foi observado durante a execução dos testes, assim como verificado no Relatório de Testes da Amostra entregue pela licitante e analisado pelos técnicos para compor este Relatório, a equipe técnica concluiu que a **amostra apresentada para testes comprovou o atendimento aos itens propostos no caderno de testes**, juntamente com a documentação do fabricante, e com demais evidências coletadas, obedecendo aos requisitos técnicos constantes do edital do Pregão eletrônico nº 5/2017.