# TERMO DE AVALIAÇÃO DA AMOSTRA - LOTE 2

**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 2** – LICITANTE: Teltec Solutions.

## 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 2.

Para a avaliação dos testes de conformidade por meio do presente Termo de Avaliação de Amostra - TAM foram levados em consideração o Relatório de Testes da Amostra apresentado pela empresa LICITANTE, assim como as evidências observadas e coletadas pela equipe técnica durante o período destinado aos testes de conformidade.

## 2. CONSIDERAÇÕES GERAIS, DA AMOSTRA E DA PREPARAÇÃO INICIAL

O período destinado à realização dos testes de conformidade do LOTE 2 consistiu no prazo das 40 horas úteis (5 dias úteis) entre os dias 17 e 21 de dezembro de 2018, das 08:30h às 18:30h, nas dependências do Ministério do Planejamento - MP, bloco situado na quadra 516 Norte, em Brasília-DF.

Cabe ressaltar, que a LICITANTE informou, antes do início do período dos testes (17 a 21 de dezembro), que não executaria a preparação do ambiente no período convocado (período entre os dias 10 a 14 de dezembro). Após análise do grupo técnico e consulta ao pregoeiro, à luz do Anexo E, entendeu-se não haver óbice a tal prosseguimento de ajustes e preparação dentro do prazo concedido para execução dos testes, por opção da LICITANTE.

Iniciado os trabalhos, no dia 17 de dezembro, 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 enviado pela LICITANTE e previamente analisado 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 deverão ser 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 de conformidade, os quais deveriam ser salvos em mídia própria fornecida pelo grupo técnico.

A amostra disponibilizada pela LICITANTE correspondia ao que estava descrito em proposta comercial, a saber: Equipamento firewall ASA 5516-X com Cisco FirePOWER Services, incluindo funcionalidades de *Threat Protection*, *Malware Protection*, *URL Filtering* e *Control*, além do *Cisco Firepower Management Center* - FMC.

As imagens do *firmware, softwares e appliances* virtuais da solução em análise foram baixadas do site do fabricante CISCO e seus *hashes* comprovados, conforme acompanhado pelo grupo técnico e evidenciado entre as páginas 4 e 7 do Relatório de Testes da Amostra. As figuras (*prints*) utilizadas no relatório também estão salvas no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-17\capturas" da mídia disponibilizada pela CONTRATANTE.

A configuração da amostra foi realizada quase que totalmente através de acesso direto ao *firewall* por meio de linha de comando e da plataforma de gerência centralizada *Cisco Firepower Management Center* - FMC. A interface gráfica *Cisco Adaptative Secutity Device Manager* - ASDM, que na verdade se trata de um aplicativo cliente instalado no *desktop* utilizado para acesso ao *firewall*, praticamente não foi utilizada, prejudicando a sua avaliação. Outro módulo ou componente instalado, mas que não ficou clara a sua utilidade dentro do escopo da solução ofertada, pois também não foi evidenciada a sua utilização, é o *Security Manager*.

As evidências relacionadas a equipamentos, *downloads*, instalação, configuração, atualização e endereçamentos ficaram registradas entre as páginas 2 e 62 do Relatório de Testes da Amostra, sendo os respectivos *prints*, arquivos de texto e demais arquivos, como *hashes*, disponibilizados em mídia da CONTRATANTE.

Dando continuidade aos testes, no dia 17 de dezembro a equipe técnica da LICITANTE solicitou alteração de ordem, de forma que primeiramente executassem os testes complementares exigidos pela equipe técnica da CONTRATANTE. Os testes complementares foram indicados pela equipe técnica da CONTRATANTE, após a análise inicial do produto ofertado em proposta, assim como do respectivo caderno de testes apresentado pela LICITANTE, e tem por objetivo evidenciar, de forma inequívoca, o atendimento de requisitos técnicos para o pleno funcionamento da solução.

A equipe técnica da CONTRATANTE sinalizou que poderiam ser executados os testes complementares que não tivessem relação com os testes de desempenho e de sessões, pois estes careciam de execução anterior dos testes de assertividade e respectivas configurações, ou que pudessem ser evidenciados durantes a execução dos testes de conformidade. Desta forma, a LICITANTE iniciou a comprovação dos itens 2.1.14, 2.1.23.2, 2.1.23.3, 2.1.23.4, 2.1.23.5, 2.1.23.6, 2.1.23.7, 2.1.35, 2.1.48, 2.1.64, 2.3.11, 2.3.14, 2.5.3 e 2.6.7. Posteriormente, devido a falhas apresentadas durantes a execução de itens dos testes complementares relacionados à integração da amostra com serviços de autenticação de usuários, como o *Microsoft Active Directory*, a equipe técnica da LICITANTE indicou a necessidade de dar continuidade ao

caderno. De forma que fosse oportunizado o andamento dos trabalhos, a equipe técnica da CONTRATANTE sinalizou que a LICITANTE poderia dar continuidade ao caderno e retornar aos testes complementares em momento oportuno. Os detalhes a respeito dos testes complementares são apresentados no item 3.5 a seguir.

Por fim, ressalta-se que, antes do final do prazo determinado para execução dos testes de conformidade, a equipe técnica da CONTRATANTE, em acordo com o grupo técnico, informou e concedeu 3 (três) horas como forma de compensar dois episódios, de forma que a LICITANTE não fosse prejudicada por eventos que estivessem sob o controle da CONTRATANTE, a saber: 1. atraso para abertura da sala reservada para os testes de conformidade, no primeiro dia de testes; e 2. bloqueio, pelo *firewall* da rede da CONTRATANTE, de conexão da amostra em avaliação com o site do respectivo fabricante.

## 3. DOS TESTES DE CONFORMIDADE

### 3.1) Das Configurações Dos Testes

Em relação ao item 5.1.1 e seu subitem, foi observado que a amostra possuía as funcionalidades exigidas, contudo a administração da funcionalidade de controle de largura de banda (QoS) **não** pode ser demonstrada a partir da interface de gerência centralizada.

As configurações solicitadas no item 5.1.2 foram evidenciadas pela empresa LICITANTE em imagens capturadas durante os testes, como nas páginas 62 e 87 do relatório de testes da amostra, nas quais apresentam as funcionalidades habilitadas no *firewall*, assim como atualização das respectivas bases junto ao fabricante. Além disso, foram apresentadas pela empresa avaliada, listas de ataques, ameaças, sites e aplicações que foram utilizados nos testes, conforme disposto no item 5.1.2.1 do Anexo E.

Conforme solicitado no item "5.1.3 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" do Anexo E - Testes de Conformidade, foi verificado que a amostra possui a capacidade de habilitar todos os controles de segurança em um único fluxo de dados.

A Solução de Gerência Centralizada também foi integrada ao *firewall* multifuncional, conforme solicitado no item 5.1.5 do Anexo E - Testes de Conformidade.

### 3.2) Dos Testes De Assertividade

A empresa LICITANTE registrou os resultados dos testes de assertividade a partir da página 116 do Relatório de Testes da Amostra entregue. Após realizar a configuração para execução do primeiro teste de assertividade, foi executado o *backup* das configurações e o arquivo, nomeado como "asa1-assertividade-ips-v2.conf", foi salvo em mídia disponibilizada pela CONTRATANTE.

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 entre as páginas 116 e 138 do Relatório dos Testes da Amostra, sendo que, segundo os resultados apresentados pelo equipamento gerador de tráfego, das 3121 tentativas de ataques gerados, 2870 foram identificadas e bloqueadas pelo *firewall* multifuncional. O Relatório do equipamento gerador de tráfego Spirent, arquivo "report.pdf" salvo no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-19\avalanche\Ataques", apresenta o resultado na

página 2, indicando que 91,95% dos ataques injetados na amostra em avaliação foram identificados e bloqueados.

No entanto, foi identificada uma inconsistência em relação aos *logs* apresentados pelo *firewall* em avaliação. O número de transações realizadas, conforme indicado no arquivo "Assertividade_-_ataques-20181219123510-12862_1_Table_View_of_Connection_Events.csv", gerada pelo *firewall* e coletada durante os testes de bancada, foi de **3864**. Tal número também é apresentado pela planilha "RTA - Teste de Assertividade IPS-IDS.xlsx", entregue pela LICITANTE anexa ao Relatório de Testes da Amostra. Contudo, desse total, apenas **1126** apresentam a ação ***Block***, com a razão ***Intrusion Block,*** o que representa 29,14% do total. Além disso, a coluna que descreve a o nome das assinaturas/ataques possui apenas **948** valores exclusivos restantes.

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 138 e 139 do Relatório dos Testes da Amostra entregue pela licitante. A lista de malwares também foi disponibilizada no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-19\avalanche\Malwares" da mídia disponibilizada pela CONTRATANTE, assim como o arquivo CSV, nomeado como "Assertividades_-_Malwares_-_conexoes-20181219143425-23359_1_Table_View_of_Connection_Events". O Relatório do equipamento gerador de tráfego Spirent, denominado de "report.pdf", salvo no mesmo diretório, indica que 91,40% (2339) dos ataques injetados (2559) na amostra foram identificados e bloqueados. Observa-se que o arquivo ""MPOG_Malwares_-_detections-20181219143211-22643_0_Detection_Name"", salvo no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-19\arquivos\MPOG_Malwares_-_detections-20181219143211-22643_csv" da mídia utilizada pela CONTRATANTE para coleta de evidências, possuía 1922 linhas distintas devido ao agrupamento de assinaturas em categorias denominadas "*Detection names*".

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 139 e 143 do relatório entregue pela licitante. A lista de aplicações, contendo 262 linhas distintas, também foi exportada em arquivo CSV, a partir da amostra avaliada, e salva no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-19\arquivos\MPOG_-_Assertividade_-_apps-20181219203911-27101_csv". O relatório do equipamento gerador de tráfego, nomeado como "report.pdf", salvo no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-19\avalanche\APPs", indica que das 306 aplicações analisadas pela amostra, apenas 3 não foram identificadas e bloqueadas, perfazendo um total de 99,02% de bloqueio. Dentre as 303 aplicações identificadas, 15 eram de clientes específicos, sendo estes listados na página 142 do Relatório de Testes da Amostra. De forma complementar ao caderno de testes e idêntica ao que ocorreu em todos os lotes, foram solicitados, pela equipe técnica da CONTRATANTE, testes complementares de identificação e bloqueio de mais **40 aplicações**. Contudo, o Relatório de Testes da Amostra **não** evidenciou a comprovação pontual da identificação e bloqueio destas aplicações, salvo algumas que foram identificadas nos testes automatizados, via gerador de tráfego, e que puderam ser validadas pela equipe técnica da CONTRATANTE, embora não tenham sido apontadas em relatório.

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 entre as páginas 143 e 145 do Relatório dos Testes da Amostra entregue pela licitante. Os resultados apresentados no relatório citado indicaram a categorização de 5111 URLs distribuídas em 64 categorias listadas na página 145. Essa lista de categorias e URLs foi exportada, a partir da amostra avaliada, em arquivo CSV, com o nome de "MPOG_URLs-20181220204752-31385_4_Table_View_of_Connection_Events" e salva no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-20\arquivos\MPOG_URLs-20181220204752-31385_csv" da mídia disponibilizada pela CONTRATANTE. 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, salvo no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-20\avalanche\SpirentEvidencias\Assertividade\URLs", indica que 44,81% das URLs analisadas foram bloqueadas.

**3.3) Dos Testes De Desempenho**

Para os Testes de Desempenho, o grupo técnico da LICITANTE restaurou o último backup executado após os testes de assertividade, que possui o nome de "assertividade-urls-v1-2018-12-20T18-53-37.tar".

A LICITANTE evidenciou os resultados dos testes de desempenho entre as páginas 145 e 165 do Relatório de Testes da Amostra. A topologia do ambiente de testes foi apresentada na página 105, e a execução das configurações solicitadas nos itens 5.1.8 e 5.1.11 do "Anexo E - Testes de Conformidade" foi apresentada entre as páginas 106 e 115 do relatório.

Após o início do primeiro teste de parametrização, observou-se que a configuração inicial mínima exigida pelo item 5.1 do Anexo E foi prejudicada pelo fato de a LICITANTE não ter implementado topologia que disponibilizasse, de forma simultânea, a operação da solução de gerência centralizada e de gerência local, conforme dita o item 5.1.5, *in verbis*:

*"5.1.5 Durante a realização dos testes, será avaliada a solução de gerência local e centralizada, que devem permanecer acessíveis, possibilitando a modificação e aplicação de políticas de segurança, bem como a visualização dos logs de acesso e de detecção de ameaças e aplicações, por CLI e/ou por GUI (interface gráfica) a critério do grupo técnico de apoio ao pregoeiro"*

O grupo técnico solicitou a correção e adequação da topologia, para que se iniciasse novamente o teste de parametrização e fosse dada continuidade aos testes, entretanto, mesmo após readequação da topologia, a interface de gerência local, utilizando-se de um aplicativo *desktop*, pouco foi utilizada e demonstrada durante os testes de desempenho, de forma que a avaliação do comportamento da interface de gerência local ficasse prejudicada.

Após execução dos procedimentos de configuração pela empresa LICITANTE, de forma que se tentasse refletir as exigências dos itens 5.1.8 a 5.1.11 do Anexo E, foi executado um backup das configurações da amostra, sendo este nomeado de "asa1-config-final.conf", sendo este salvo no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-

21\arquivos" da mídia disponibilizada pela CONTRATANTE. Desta forma, atendendo ao que está disposto no item 5.3.5 do Anexo E.

Esse mesmo procedimento foi executado para o *firewall* que foi configurado para o teste de tráfego em VPN IPSec, sendo que para este o nome do arquivo é "asa2-vpn-config-final.conf".

As evidências referentes ao item 5.3.7.2 do mesmo Anexo, relacionados à parametrização, estão entre as páginas 145 e 153 do Relatório de Testes da Amostra apresentado pela LICITANTE. O perfil de tráfego especificado no item 5.1.12 foi apresentado na página 152 através de captura de tela retirada do equipamento gerador de tráfego Spirent. Além disso, testes com o protocolo UDP e com tráfego em VPN IPSec também foram executados.

Os dados referentes à taxa de transferência indicaram um resultado um pouco superior a 69 Mbps, conforme evidência apresentada na página 147. Os *prints* coletados durante os testes de parametrização, incluindo imagens do equipamento gerador de tráfego, estão no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-21\avalanche\Testes21Dez\Teste25percent" da mídia disponibilizada pela CONTRATANTE.

A evidência referente ao tráfego em UDP está na imagem 123 da página 146 do Relatório de Testes da Amostra entregue pela licitante. O *print*, figura 125 da página 147 do relatório, apresentado como evidência do tráfego em VPN IPSec, foi capturado da tela do equipamento gerador de tráfego e anexado ao relatório, de modo a atender o item 5.1.12.3.1.

Os dados referentes à "latência média" e "variação média de latência (*jitter*)", apresentados na página 145 do relatório, foram de aproximadamente 50us e 22us, respectivamente. Estes dados também foram evidenciados em *prints* salvos na pasta "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-21\avalanche\Testes21Dez\Teste25percent" da mídia disponibilizada pela CONTRATANTE.".

Quanto aos "erros absolutos irrecuperáveis de transações TCP/layer-7", foi verificado nos relatórios do equipamento gerador de tráfego, que 12 transações não foram realizadas com sucesso. Desta forma, um total de aproximadamente 0,0001% das 61.784 transações realizadas. Esses dados foram retirados dos relatórios do equipamento gerador de tráfego com os nomes de "test25PercAsserReport.pdf" e "testPerf25percReport".

Quanto à "detecção de ameaças, aplicações, ataques e URLs", o Relatório de Testes da Amostra não cita nenhuma evidência. Entretanto, foi verificado no relatório do equipamento gerador de tráfego Spirent que as ameaças, aplicações, ataques e URLs estavam sendo injetados na amostra avaliada. O relatório possui o nome de "report25percentAssertividade" e está salvo na pasta "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-21\avalanche\Testes21Dez\Teste25percent".

Após parametrização da amostra, foram executados procedimentos para zerar contadores e *logs*, conforme previsto no item 5.3.7.1 do Anexo E.

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 153 do relatório entregue. Os dados referentes à taxa de transferência indicaram um resultado um pouco superior a 355 Mbps, conforme evidência apresentada na página 161. Os *prints* coletados

durante os testes de desempenho, incluindo imagens e relatórios do equipamento gerador de tráfego, estão no diretório "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-21\avalanche\Testes21Dez\Teste100percent" da mídia disponibilizada pela CONTRATANTE.

A evidência referente ao tráfego UDP está na imagem 149 da página 159 do Relatório de Testes da Amostra entregue pela licitante. A figura 151 da página 160 do relatório, apresentado como evidência do tráfego em VPN IPSec, é um *print* capturado da tela do equipamento gerador de tráfego e anexado ao relatório, de modo a atender o item 5.1.12.3.1.

Os dados referentes à "latência média" e "variação média de latência (*jitter*)", apresentados na página 162 do relatório, foram de aproximadamente 65us e 34us, respectivamente. Estes dados também foram evidenciados em *prints* salvos na pasta "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-21\avalanche\Testes21Dez\Teste100percent" da mídia disponibilizada pela CONTRATANTE.".

Quanto aos "erros absolutos irrecuperáveis de transações TCP/layer-7", foram apresentados os mesmos 12 erros, dentre as 196.950 transações, representando uma taxa de inferior a que fora apresentada na parametrização. Esses dados foram coletados de forma conjunta nos relatórios "Assert_100pc_report.pdf" e "Perf_100pc_report", do equipamento gerador de tráfego.

Quanto à "detecção de ameaças, aplicações, ataques e URLs", o Relatório de Testes da Amostra não cita nenhuma evidência. Entretanto, foi verificado no relatório do equipamento gerador de tráfego Spirent que as ameaças, aplicações, ataques e URLs estavam sendo injetados na amostra avaliada. O relatório possui o nome de "Assert_100pc_report" e está salvo na pasta "TELTEC-PE52017-LOTE2\Lote 2 - Teltec - 2018-12-21\avalanche\Testes21Dez\Teste100percent".

A comparação dos resultados, solicitadas no item 5.3.8.3 do Anexo E - Testes de Conformidade, não foi evidenciada pela empresa LICITANTE em seu relatório. A "perda absoluta de pacotes" apresentada no resultado do equipamento gerador de tráfego foi de 0% e o registro de "erros absolutos irrecuperáveis de transações TCP/layer-7", conforme já citado, foi inferior a 0,5%. Em relação aos valores de "latência média" e de "variação média de latência (*jitter*)" apresentaram aumento em relação aos que foram coletados na parametrização, sendo que ambas apresentaram um aumento inferior a 10 vezes. As evidências quanto à "deteção de ameaças, ataques, aplicações e URLs", conforme já citado, foram verificadas em relatórios do equipamento gerador de tráfego.

Por fim, foi observado que durante os testes de assertividade **não** foi habilitado nenhum perfil de administração de largura de banda (QoS) nas políticas criadas no firewall, conforme previsto no item *"5.1.1. A amostra deverá ser configurada com as funcionalidades de firewall, tal como previstas na especificação técnica do Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso (controle de aplicações e filtragem de URL's), sistema de detecção/prevenção a intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e Anti-malware), administração de largura de banda de serviço (QoS), descriptografia, inspeção de tráfego SSL e suporte para conexões VPN IPSec."* do Anexo E. Essa funcionalidade poderia ser habilitada com limitação superior ao mínimo exigido para o *throughput* do lote, de forma que não gerasse impacto nos testes.

**3.4) Dos Testes De Sessão**

As evidências referentes ao primeiro teste de sessão, realizado com o mesmo perfil de tráfego do Teste de Desempenho, estão nas páginas 165 e 166 do Relatório de Testes da Amostra enviado pela LICITANTE. Foi realizado o *backup* das configurações da amostra e o arquivo de backup foi nomeado como "MPOG-Sessoes-v1-2018-12-21T21-49-01.tar", salvo no diretório da mídia da CONTRATANTE. A amostra avaliada não alcançou os resultados determinados para o primeiro dos testes de sessões indicados nos itens 5.4.2.2 e 5.4.2.3, conforme evidenciado nas figuras 160 e 161 do Relatório de Testes da Amostra.

Após execução do primeiro dos testes de sessão, os *logs* e estatísticas da amostra foram zerados. O segundo teste de sessão ficou evidenciado entre as páginas 166 e 172 do relatório. Segundo a figura 164, exportada do equipamento gerador de tráfego, presente na página 168 do relatório, a amostra atingiu 100.000 conexões simultâneas, atendendo ao que está disposto no item 5.4.3.2.1. do Anexo E - Testes de Conformidade. Na página 171 foi apresentado o resultado do teste de mensuração de novas sessões por segundo, sendo que o mesmo apresentou a taxa de 15.000 novas conexões por segundos , atendendo ao que está disposto no item 5.4.3.1.1. do mesmo anexo.

As imagens apresentadas no relatório foram validadas nos arquivos exportados do equipamento gerador de tráfego que foram nomeados como "reportCPS" e "reportCC", ambos salvos em mídia disponibilizada pela CONTRATANTE.

**3.5) Dos Testes dos itens complementares**

Conforme indicação do grupo técnico, relatada anteriormente, os testes dos itens complementares relacionados às dúvidas sobre as especificações técnicas solicitadas pelo Anexo B do Edital PE nº 05/2017, apontados no caderno de testes e que não dependiam de configuração da amostra poderiam ser realizados de forma independente, para viabilizar o andamento dos trabalhos. Os outros itens seriam verificados apenas após a viabilização das configurações iniciais para os testes de conformidade, já que as evidências seriam coletadas utilizando-se tais configurações. Os testes dos itens possíveis foram iniciados no dia 17 de dezembro e são listados aqui para referência. Diante das evidências coletadas, foi constatado que:

i) A amostra atendeu parcialmente ao disposto no item 2.1.14 quanto ao suporte à criação filtros de pacote por endereço IP de origem e destino, por aplicação, por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana, contudo, **não** evidenciou, nos testes, a detecção e bloqueio de aplicações "*independentemente da porta ou protocolo utilizados pela aplicação*". Ressalta-se que essa verificação poderia ser executada concorrentemente aos testes complementares de identificação e bloqueio de mais 40 aplicações indicadas para o teste de assertividade.

ii) Em relação ao item "2.1.23.2. Deve registrar a identificação do usuário em todos os eventos associados gerados pelo equipamento, tais como (mas não

restrito a) eventos de autenticação, registros de acesso ou bloqueio e eventos associados a ameaças;", a equipe técnica da LICITANTE **não** conseguiu demonstrar, durante os testes, a integração da solução com uma base de usuários, de forma que fosse possível validar o registro de cada usuário associado aos eventos, embora a interface gráfica da solução apresentasse uma coluna com a descrição "*User*".

iii) A equipe técnica da LICITANTE, após as primeiras tentativas de configuração que demonstrasse de forma inequívoca o atendimento do item, não demonstrou a capacidade da amostra, até o término do prazo estipulado para os testes, o pleno atendimento do item 2.1.23.3 do Anexo B, a saber: "*Deve prover identificação de forma transparente aos usuários autenticados por single sign on, no mínimo, por meio dos serviços Microsoft Active Directory e RADIUS;*". Cabe ressaltar que, durante as primeiras tentativas de configuração pela equipe técnica da LICITANTE, a amostra em avaliação exibia mensagem de erro, a qual não foi encontrada entre as evidências coletadas. O Relatório de Testes da Amostra também não faz referência à mensagem de erro. Por fim, como **não** restou comprovado o atendimento deste item em epígrafe, os itens complementares 2.1.23.2, 2.1.23.5 e 2.1.64 relacionados, que possuem dependência direta deste, também estariam automaticamente invalidados, no que se referisse à identificação de usuários autenticados em estrutura do *Active Directory*.

iv) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item *"2.1.23.4. Deve prover portal ou pop-up de login para identificação dos usuários dos demais serviços de LDAP não listados no item anterior"*, portanto, ficou prejudicada a sua averiguação.

v) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item *"2.1.23.5. Deve permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;"*, portanto, ficou prejudicada a sua averiguação.

vi) Em relação ao item *"2.1.23.6. Não será permitida a utilização de agentes instalados nos equipamentos dos usuários;"*, verificou-se durante os testes que não há necessidade de instalação de agentes em máquinas de usuários.

vii) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item *"2.1.23.7. Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP, tais como (mas não restritos a) aplicações HTTP, HTTPS e FTP;*, portanto, ficou prejudicada a sua averiguação.

viii) Em relação ao item "*2.1.35. Suportar no mínimo 250 regras ou políticas de firewall para os equipamentos do lote 1 e 1.000 regras ou políticas de firewall para os equipamentos dos lotes 2,3,4 e 5."*, as evidências estão registradas entre na página 176 do Relatório de Testes. A amostra atendeu ao disposto no item 2.1.35 quanto ao suporte à criação de no mínimo 1000 regras ou políticas de firewall, conforme evidenciado nas figuras 176 e 177.

ix) Em relação ao item *"2.1.48. Deve suportar a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e aplicações (por exemplo, Youtube e WhatsApp)"*, as evidências estão registradas na página 177 (Figuras 178 e 179) do Relatório de Testes. A amostra atendeu parcialmente ao disposto no item 2.1.48 quanto ao suporte à criação de políticas de controle de uso de largura de banda baseadas em porta e endereços IP de origem ou destino, porém, não evidenciou esse suporte quando se trata de protocolos ou grupos de usuários do AD e LDAP e aplicações. Além disso, cabe ressaltar que não restou comprovada a capacidade de realizar a configuração de controle de banda via solução de gerência centralizada, mas apenas através da interface *Cisco Adaptative Secutity Device Manager* – ASDM.

x) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item *"2.1.64. Implementar autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS"*, portanto, ficou prejudicada a sua averiguação.

xi) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item *"2.3.11. Permitir filtros de anomalias de tráfego estatístico de flooding, scan e source session limits;"*, portanto, ficou prejudicada a sua averiguação.

xii) A equipe técnica da LICITANTE demonstrou que a amostra possui suporte à desabilitação de assinaturas e protocolos, conforme previsto no item *"2.3.14. Possuir funcionalidade que permita desativar a análise de assinaturas e protocolos;"*. As evidências estão registradas na página 178 (Figuras 180 e 181) do Relatório de Testes.

xiii) A equipe técnica da LICITANTE demonstrou que a amostra possui suporte à reclassificação e categorização de sites, conforme previsto no item *"2.5.3. Permitir a categorização e reclassificação de sites web por URL;"*. Imagens da funcionalidade foram coletadas e salvas na mídia disponibilizada pela CONTRATANTE.

xiv) Em relação ao item *"2.5.15. Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo consideradas neste percentual categorização genérica ou similar"*, sua comprovação restou averiguada durante os Testes de Assertividade.

xv) Em relação ao item *"2.6.7. Identificar aplicações e permitir ou bloquear sua utilização, independentemente das portas e protocolos utilizados para conexão (inclusive tráfego criptografado), assim como possuir categorias para classificação das aplicações, bem como das técnicas de evasões utilizadas;"*, a equipe técnica da LICITANTE **não** demonstrou a capacidade de identificação e bloqueio de aplicações "*independentemente das portas e protocolos utilizados*". Ressalta-se que esta exigência possui relação direta com a capacidade em averiguação citada no item 2.1.14.

xvi) Em relação ao item *"3.8.1.2. Possuir, no mínimo, o throughput de inspeção de 250 Mbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E"*, sua comprovação restou averiguada de forma **parcial**, uma vez que durante os Testes de Desempenho não foi identificado perfil de controle de banda ativado, conforme já citado.

xvii) Em relação ao item *"3.8.1.5. Throughput mínimo de 50 Mbps para IPSec VPN"*, foi verificado pela equipe técnica da CONTRATANTE, em site oficial do fabricante, que o produto ofertado está homologado para alcançar a vazão de 250 Mbps para tráfego criptografado.

xviii) Em relação ao item *"3.8.1.6. Quantidade mínima de 90.000 sessões simultâneas"*, sua comprovação restou averiguada durante os Testes de Desempenho.

xix) Em relação ao item *"3.8.1.7. Quantidade mínima de 12.000 novas sessões por segundo"*, sua comprovação restou averiguada durante os Testes de Desempenho.

xx) Em relação ao item *"3.14.1.2. Possuir capacidade mínima de 250 GB para armazenamento de logs e eventos."*, a equipe técnica da LICITANTE **não** demonstrou o atendimento pela solução de gerência centralizada *Cisco Firepower Management Center* - FMC, portanto, ficou prejudicada a sua averiguação.

**4. CONCLUSÃO**

O grupo técnico de apoio ao pregoeiro, levando em consideração o Relatório de Testes da Amostra da LICITANTE, bem como os fatos observados e evidências coletadas durante a execução dos testes de conformidade, concluiu que a LICITANTE **não** foi capaz de demonstrar o atendimento integral, e de forma inequívoca, dos requisitos do edital de Pregão Eletrônico Nº 5/2017 listados a seguir:

1. Apresentar com clareza as funcionalidades e recursos fornecidos pelas interfaces *Cisco Adaptative Secutity Device Manager* - ASDM e *Cisco Security Manager*, que devem permanecer disponíveis para avaliação durante os testes de desempenho;
2. Executar e evidenciar o bloqueio de um quantitativo mínimo de 2.000 assinaturas distintas de IPS, com assertividade mínima de 80%, conforme previsto no item 5.2.4 do Anexo E: "i) Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS";
3. Executar e evidenciar a detecção e bloqueio das 40 aplicações listadas pelo grupo técnico de apoio ao pregoeiro após avaliação do caderno de testes, como complemento ao teste de assertividade da alínea "iii) Categorizar e bloquear, pelo menos, 100 (cem) aplicações distintas" do item 5.2.4 do Anexo E;
4. Executar teste de desempenho com perfil de administração de largura de banda (QoS) nas 25 políticas criadas no firewall, conforme disposto no item 5.1.1 do Anexo E;
5. Executar e evidenciar os testes complementares conforme observações citadas no item 3.5 acima e alíneas a saber: i, ii, iii, iv, v, vii, ix, x, xi, xv, xvi e xx.