PENDÊNCIAS E ADAPTAÇÕES A SEREM REALIZADAS NA SEGUNDA VERSÃO DO CADERNO DE TESTES DA EMPRESA NCT – LOTE 3

1. CONSIDERAÇÕES INICIAIS

Além das informações já apresentadas na primeira versão do Caderno de Testes, a empresa deve estruturar o caderno de testes de acordo com o modelo e premissas listadas abaixo, as quais estão de acordo com o preconizado no Anexo E, que fornece orientações gerais para a elaboração do caderno de testes.

Ressalta-se que o caderno de testes será utilizado como apoio principal, contudo, na execução dos testes, a empresa deve se atentar a todos os requisitos elencados no Anexo E – Caderno de Testes do Termo de Referência do Pregão nº 05/2017. Desta forma, o Caderno de Testes deve refletir a documentação mínima de informações para que os testes sejam executados. Entretanto, os testes poderão ser ajustados conforme dispostos nos itens 2.16 e 2.17 do Anexo E do termo de referência do Edital de Pregão nº 05/2017.

A empresa deve também colocar ou referenciar nos cadernos de testes comandos e procedimentos a nível de sessão / capítulo do caderno, a fim de deixar o caderno de teste e a realização dos testes mais transparentes.

Os *scripts*, ou seja, a automação da criação das configurações, devem ser apresentados antes da realização dos testes para avaliação do grupo técnico, pelo menos com 10 dias corridos de antecedência da data dos testes marcada pela pregoeira. Deve-se destacar que esse procedimento destina-se apenas a averiguação prévia de configuração dos equipamentos a fim de informar em maiores detalhes a equipe técnica.

E ainda, a empresa deve passar a listagem dos *malwares*, ataques e aplicações que o equipamento de teste é capaz de gerar, bem como a listagem dos malwares, ataques, aplicações e URLs que a empresa pretende ativar no equipamento de testes durante os testes de assertividade.

Por fim, deve-se indicar que, quando couber, os cadernos de testes apresentados deverão ser complementados ao que foi inicialmente proposto. Essa complementação deve ser conforme a estrutura indicada no Anexo E, os pontos aqui levantados a seguir e as observações apontadas neste documento.

2. DISPOSIÇÕES GERAIS

a) Descrição dos objetivos gerais do teste de bancada para cada item testado.

OK. Premissa atendida no tópico 3 do Caderno de Testes enviado pela NCT.

b) Descrição de todos os equipamentos acompanhados de seus modelos, incluindo o gerador de tráfego, além de todas as versões de firmwares que serão utilizadas nos testes.

OK. Premissa atendida no tópico 5 do Caderno de Testes enviado pela NCT.

c) Indicação da equipe técnica que irá acompanhar os testes, de acordo com item 2.13 do Anexo E, informando, no mínimo, nome e e-mail.

OK. Premissa atendida no tópico 4 do Caderno de Testes enviado pela NCT.

3. PREPARAÇÃO INICIAL

a) Descrição dos comandos a serem utilizados para limpeza e exclusão de dados de forma a zerar configurações, conforme o item 4.1 do Anexo E.

OK. Premissa atendida no tópico 5.3.1 na página 8 do Caderno de Testes enviado pela NCT.

b) Descrever procedimentos para verificação dos itens 4.2 e 4.3 do Anexo E.
OK. Premissa atendida no tópico 5.3.1 na página 9 do Caderno de Testes enviado pela NCT.

c) Descrever o procedimento e comandos que serão executados para criar o backup após configuração inicial, indicando em qual mídia o backup será salvo, de forma a atender o item 4.5 e 4.6 do Anexo E.
OK. Premissa atendida no tópico 5.3.1 na página 9 do Caderno de Testes enviado pela NCT.

4. CONFIGURAÇÃO DE TESTES E TOPOLOGIA

a) Descrição dos procedimentos que serão executados para comprovar que todas as funcionalidades indicadas no item 5.1.1 do Anexo E estão ativas.
OK. Premissa atendida no tópico 5.3.2 na página 13 do Caderno de Testes enviado pela NCT.

b) Apresentação da topologia de rede esquematizada e com legenda, de forma que possa ser possível identificar todos os objetos, redes, equipamentos e interfaces que farão parte do escopo do teste, compatíveis e de acordo com o preconizado nos itens 5.1.5 a 5.1.11 do Anexo E.
OK. Premissa atendida no tópico 5.2 para a topologia e tópico 5.3.2 na página 13 para os itens 5.1.5 a 5.1.11 do Caderno de Testes enviado pela NCT.

c) Apresentação da lista (que pode ser editada em planilha anexa) de todos os ataques, ameaças, site e aplicações, de forma a atender o item 5.1.2.1 do Anexo E.
OK.

Deve ser complementado com as observações listadas abaixo:

- de todos os ataques, ameaças, sites e aplicações que o equipamento de geração de tráfego é capaz de gerar e que poderá ser utilizado pela equipe de apoio ao pregoeiro, de forma a atender os itens 4.8, 2.17 e relacionados.

- de todos os ataques, ameaças, site e aplicações, de forma a atender o item 5.1.2.1 do Anexo E. A lista enviada pela empresa deve ser complementada com no mínimo as seguintes aplicações: Youtube, Livestream, Skype, Viber, Whatsapp, Google+, Google Talk, Google Docs, Google Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex, Facebook-chat, Facebook-vídeo, ms-update, Netflix, Dropbox, Http-video, Apple-appstore, Instagram, Gmail, Twitter-base, Itunes-base, OpenVPN, Google update, Apple Services, Snapchat, Google Docs, One Drive, LinkedIn, Twitter, Telegram, Instagram Video, Twitter Video, Vimeo Video, Microsoft Azure e Microsoft Outlook 365.

d) Descrição dos procedimentos e comandos que serão executados para ativar a inspeção integral de todo o tráfego, de forma a atender os itens 5.1.3 e 5.1.4 do Anexo E.
OK. Premissa atendida no tópico 5.3.2 das páginas 11 e 12 do Caderno de Testes enviado pela NCT.

5. TESTE DE ASSERTIVIDADE

a) Descrição dos procedimentos e comandos que serão executados no firewall da Amostra para atendimento do item 5.2.2 do Anexo E.

OK.

b) Breve descrição da execução dos testes e resultados esperados.

OK.

c) Descrição dos procedimentos e comandos que serão executados no firewall da Amostra para zerar contadores e apagar configurações, de forma a atender o item 5.2.7 do Anexo E.

OK.

Observação:

A categorização contabilizada será analisada pelo grupo técnico de apoio ao pregoeiro com base nos dados gerados e obtidos pelo gerador de tráfego, sendo complementado, quando necessário, pelos dados obtidos pela amostra. Ressalta-se, que quando necessário, poderão ser apurados os *logs* tanto do gerenciador quanto do firewall propriamente dito.

d) Inserir, ao final da descrição dos procedimentos de todos os testes a serem realizados campos para sinalizar resultados dos testes, como: “Teste OK.”, “Teste com falha.” e “Observação.”

OK.

6. TESTE DE DESEMPENHO

a) Descrição dos procedimentos e comandos a serem executados para restaurar o backup executado após a configuração inicial, conforme disposto no item 4.5 do Anexo E.

OK.

b) Descrição dos procedimentos e comandos a serem executados no firewall da amostra para atendimento do item 5.3.5

OK.

c) Breve descrição da execução dos testes e resultados esperados.

OK.

d) Descrição dos procedimentos e comandos que serão executados no firewall da Amostra para zerar contadores e apagar configurações, de forma a atender o item 5.3.8.5 do Anexo E.

OK.

e) Inserir, ao final da descrição dos procedimentos de todos os testes a serem realizados campos para sinalizar resultados dos testes, como: “Teste OK.”, “Teste com falha.” e “Observação.”

OK.

7. TESTE DE SESSÃO

a) Descrição dos procedimentos e comandos a serem executados para restaurar o backup executado após a configuração inicial, conforme disposto no item 4.5 do Anexo E.

OK.

b) Breve descrição da execução dos testes e resultados esperados.
OK. Premissa atendida no tópico 5.3.5 da página 16 do Caderno de Testes enviado pela NCT.

c) Descrever os procedimentos e comandos que serão executados no firewall da Amostra para zerar contadores e apagar configurações, de forma a atender o item 5.4.2.6 do Anexo E.
OK.

8. TESTES COMPLEMENTARES

Descrever procedimentos a serem executados para comprovação dos itens que foram indicados para verificação nos testes durante a fase de análise das propostas. (Itens realçados de laranja na planilha de avaliação das propostas). Isso porque, no momento dos testes, as funcionalidades deverão ser comprovadas.

a) Inserir, ao final da descrição dos procedimentos de todos os testes a serem realizados campos para sinalizar resultados dos testes, como: “Teste OK.”, “Teste com falha.” e “Observação.”

i. 2.1.32. Possuir funcionalidade de detecção e bloqueio de, no mínimo, os seguintes tipos de ataques: IP Spoofing, SYN Flood, UDP Flood, Port Scanning, ICMP Flood, ICMP sweep, Ataques de Força Bruta ataques Man-in-the-Middle e variações de reflexão;

ii. 2.2.4. Deve ser licenciada de forma a permitir a captura e filtragem de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

iii. 3.15.1.2. Possuir, no mínimo, o throughput de 1 Gbps 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.

9. ESCLARECIMENTOS DIVERSOS

Não existem esclarecimentos adicionais a serem feitos.

10. CONCLUSÃO

Indique-se que foram atendidas todas as solicitações de ajustes após a primeira revisão do documento. Portanto, a empresa deverá apresentar o caderno de teste final por meio eletrônico conforme já entregue após a 1ª revisão.