

TERMO DE AVALIAÇÃO DE AMOSTRA DOS TESTES COMPLEMENTARES - LOTE 1

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 1: Empresa avaliada em teste complementar – BLOCKBIT.

1. INTRODUÇÃO

Em 2 de maio de 2018 foram abertos os testes de conformidade complementares referentes ao Lote 1 do Pregão Eletrônico por Sistema de Registro de Preços nº 05/2017. Trata-se de um re-teste aplicado à empresa Blockbit Tecnologia Ltda., que ofertou a solução denominada “BB10”, para fins de atendimento ao exigido para o Lote 1. O interlocutor do grupo técnico agradeceu a presença de todos e passou a pontuar algumas informações importantes para a realização dos testes em questão e que estão relatados a seguir.

Na ocasião, foi informado que os testes complementares seriam realizados de acordo com as regras e condições contidas no Anexo E do Termo de Referência, que dispõe sobre os testes de conformidade, e dessa forma, seguiriam as mesmas regras gerais do teste inicial. Dentre as principais regras, informou-se aos presentes que os testes sempre são realizados com a presença de mais de um integrante técnico do grupo técnico, sendo que ao menos um deles responde pela liderança da equipe técnica. Além disso, lembrou-se aos participantes que durante a realização dos testes não deveriam ser realizadas intervenções indevidas das empresas ouvintes e ou pessoas 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. Também mereceu destaque 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. E ainda, o interlocutor do grupo técnico informou a todos que o comando previsto no item 2.28 do Edital em questão indicava a realização dos testes complementares para os horários de 8h00 às 12h00 e de 14h00 as 18h00, no período de 2 de maio a 4 de maio de 2018 (conforme informado previamente pela pregoeira), havendo a possibilidade de compensação de atrasos, caso fosse necessário.

Dando continuidade, o interlocutor do grupo técnico lembrou que o TAM do LOTE 1 apontou algumas não conformidades, que impediram a comprovação de determinados quesitos do caderno de testes, em especial, o atendimento do item 5.1.3. do Anexo E do termo de referência do pregão em questão e que diz respeito à inspeção integral dos pacotes da solução de segurança. Dessa forma, o objetivo central dos testes de conformidade complementares era o de esclarecer pontos relativos às funcionalidades da solução que, apesar de constituírem pré-requisitos previstos em Edital para a sua aprovação, não foram comprovados nos testes iniciais

anteriormente realizados. Dessa forma, os referidos testes complementares destinavam-se a sanar dúvidas apontadas pelo grupo técnico quanto à capacidade da solução apresentada de cumprir os requisitos constantes em edital do pregão eletrônico nº 5/2017.

E ainda fora destacado que, para ampliar a transparência dos testes de conformidade complementares, foi estabelecida pelo grupo técnico uma sequência mínima esperada para a execução dos testes e apresentada a todos no início da sessão. Nesse sentido, indicou-se que a primeira atividade seria a demonstração pela empresa da capacidade da solução ofertada de cumprir o item 5.1.3 do Anexo E do edital em comento, relativa à inspeção integral dos pacotes. Em seguida, esperava-se que fossem realizados os testes de assertividade da solução, uma vez que são preparatórios para os testes de desempenho. Por fim, seriam realizados os testes de desempenho em si para medir a capacidade vazão de tráfego dos equipamentos apresentados. E ainda, deixou-se claro que, caso houve necessidade ou dúvida do grupo técnico, seriam aplicados outros testes correlatos a fim de comprovar o atendimento dos requisitos técnicos em escrutínio.

Nesse momento, o interlocutor do grupo técnico passou a palavra aos representantes da Blockbit para manifestação sobre o exposto até aquele momento e questionou 2 pontos específicos, a saber: 1. Qual a sequência de testes planejada pela empresa? e 2. Quais as mudanças efetuadas pela empresa em relação ao teste inicial realizado? Em resposta, o representante da empresa informou que estava de acordo com a sequência de testes propostos inicialmente pelo grupo técnico e que estaria a disposição para realizar outros testes complementares necessários a perfeita demonstração dos requisitos exigidos. Além disso, num primeiro momento, o representante indicou que não houve alteração substancial no produto desde os testes anteriores, com exceção de atualizações de segurança para uma nova versão do produto. Após questionamentos da equipe técnica e discussões sobre o tema, entretanto, ficou constatado que, a princípio, não houve mudança estrutural na solução, mas que, efetivamente, ocorreu alteração no *firmware* da solução. Por essa razão, foi decidido que, em função da alteração do *firmware*, considerada pelo grupo técnico relevante para as comprovações do atendimento técnico do disposto no edital em questão, o grupo técnico poderia exigir a comprovação de quesitos técnicos constantes das especificações do termo de referência do pregão eletrônico nº 5/2017, além das três confirmações acima indicadas inicialmente.

Também foi assinalado que não haveria, durante a realização dos testes, manifestação do grupo técnico sobre o cumprimento ou não dos quesitos analisados, mas apenas a solicitação de execução de operações junto a solução e a devida geração de evidências que demonstrassem o atendimento dos pontos obscuros. E que essas evidências deveriam compor a materialidade dos testes realizados, por meio da apresentação de relatório dos testes complementares pela empresa Blockbit. Nesse momento posterior, o grupo técnico iria realizar a sua manifestação formal sobre o atendimento ou não dos requisitos em análise. Assim, não haveriam julgamentos durante a sessão ou discussões sobre interpretações de quesitos, uma vez que os requisitos já estavam explícitos no instrumento convocatório de maneira clara e inequívoca. E ainda, o interlocutor destacou que, por se tratar de um processo de contratação que amadureceu por mais de 2 anos e que passou por várias etapas antes de sua publicação, o grupo técnico entendia que nas exigências técnicas do edital não haviam obscuridades ou dúvidas sobre qualquer ponto posto como exigência.

Por fim, indique-se que após discussões entre o grupo técnico e com os representantes da empresa Blockbit decidiu-se por detalhar os testes propostos inicialmente para que não restassem dúvidas dos trabalhos propostos, antes do início das atividades. Todos concordaram e a sequência inicial proposta foi a seguinte:

- 1) Teste de assertividade com todas as funcionalidades de inspeção ativas com tráfego completo e simultâneo injetado para análise.
- 2) Teste de assertividade com as funcionalidades de inspeção ativadas de forma separada e a injeção de tráfego individual separado ou isolado para cada funcionalidade avaliada.
- 3) Teste de desempenho para medir a vazão ou throughput da solução apresentada com todas as funcionalidades de inspeção ativadas.

2. OBJETIVO E FUNDAMENTO DOS TESTES COMPLEMENTARES

Os presentes testes complementares tiveram por objetivo, à luz do apontado no TAM – LOTE 1, reavaliar a amostra e analisar o cumprimento do item 5.1.3 do ANEXO E do edital, *in verbis*:

"5.1.3 A amostra deve ser configurada de forma a realizar a inspeção integral de todos os pacotes de dados, independente de seu tamanho ou direção de fluxo."

A reavaliação foi necessária porque, nos testes iniciais da amostra, a configuração apresentada, o detalhamento das funcionalidades e os resultados atingidos na ocasião, registrados no RELATÓRIO DOS TESTES DE CONFORMIDADE do LOTE 1 (RTC – LOTE 1) enviado pela LICITANTE, não foram suficientes para esclarecer ao grupo técnico a capacidade do equipamento de inspecionar integralmente TODOS os pacotes de dados, independente do seu tamanho ou direção de fluxo. A LICITANTE apresentou, então, o RELATÓRIO DOS TESTES COMPLEMENTARES DA AMOSTRA - LOTE 1 (RTCOM – LOTE 1), com a sua visão acerca dos resultados obtidos para os testes complementares realizados nos dias 2, 3 e 4 de maio de 2018.

Ressalta-se que o grupo técnico de apoio ao pregoeiro efetuou seus trabalhos sob a égide do disposto na conclusão do TAM – LOTE 1 (cumprimento do item 5.1.3 supracitado) e nos itens 2.16 e 2.17 do ANEXO E do Edital de pregão eletrônico nº 05/2017, que lhe conferem a prerrogativa de, a qualquer tempo durante a realização dos testes, solicitar as alterações ou adequações que julgar necessárias ao esclarecimento de todas as dúvidas em relação aos testes e itens da especificação técnica, *in verbis*:

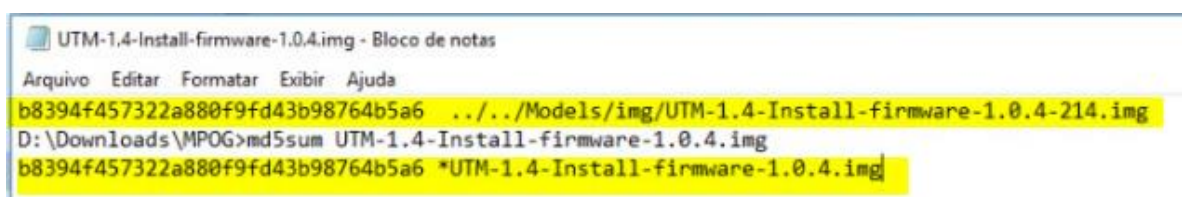
"2.16 O grupo técnico de apoio ao pregoeiro poderá solicitar alteração ou adequação durante o Teste de Conformidade, mesmo com o Caderno de Testes apresentado e aprovado, com a finalidade de dirimir quaisquer dúvidas referentes a itens da especificação técnica.

2.17 A fim de evitar quaisquer vícios nos testes, o grupo técnico de apoio ao pregoeiro, a qualquer momento e mesmo depois da validação do Caderno de Testes, poderá solicitar 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."

Frente à necessidade de se compreender os detalhes técnicos do fluxo de inspeção de tráfego que a amostra é capaz de realizar e, assim, ser possível desenvolver o entendimento acerca do funcionamento dos *engines* de proteção (tanto de forma isolada quanto em conjunto) do equipamento, o grupo técnico solicitou à LICITANTE as informações, ajustes, situações e testes que julgou necessários ao esclarecimento da capacidade de cumprimento ou não do referido item 5.1.3, de forma a coletar as evidências necessárias e avaliá-las à luz do que está especificado no edital de pregão eletrônico nº 05/2017.

3. DAS CONFIGURAÇÕES INICIAIS

A LICITANTE realizou, conforme mostra o RTCOM - LOTE 1 (páginas 8 a 29) o *download* e instalação do *firmware* de nome "UTM-1.4-Install-firmware-1.0.5.img", a partir do endereço "<http://updates.blockbit.com/downloads/img/>". Apesar das configurações iniciais básicas mínimas terem sido realizadas seguindo-se o roteiro proposto do ANEXO E do edital, culminando na obtenção do *backup* das configurações e prosseguimentos dos testes complementares, chamou a atenção do Grupo Técnico o fato de o *firmware* em questão ser mais recente do que aquele utilizado nos testes iniciais de conformidade, com códigos *hash* também diferentes, o que atesta se tratar essencialmente de um novo arquivo de *firmware* com conteúdo diverso daquele utilizado na primeira fase dos testes (uma nova versão ou *build*), conforme se vê nas imagens abaixo:



```
UTM-1.4-Install-firmware-1.0.4.img - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
b8394f457322a880f9fd43b98764b5a6 ../../Models/img/UTM-1.4-Install-firmware-1.0.4-214.img
D:\Downloads\MPOG>md5sum UTM-1.4-Install-firmware-1.0.4.img
b8394f457322a880f9fd43b98764b5a6 *UTM-1.4-Install-firmware-1.0.4.img
```

Fig. 1 - Hash do arquivo utilizado nos testes iniciais de conformidade, informado no RTC – LOTE 1, pág. 8.

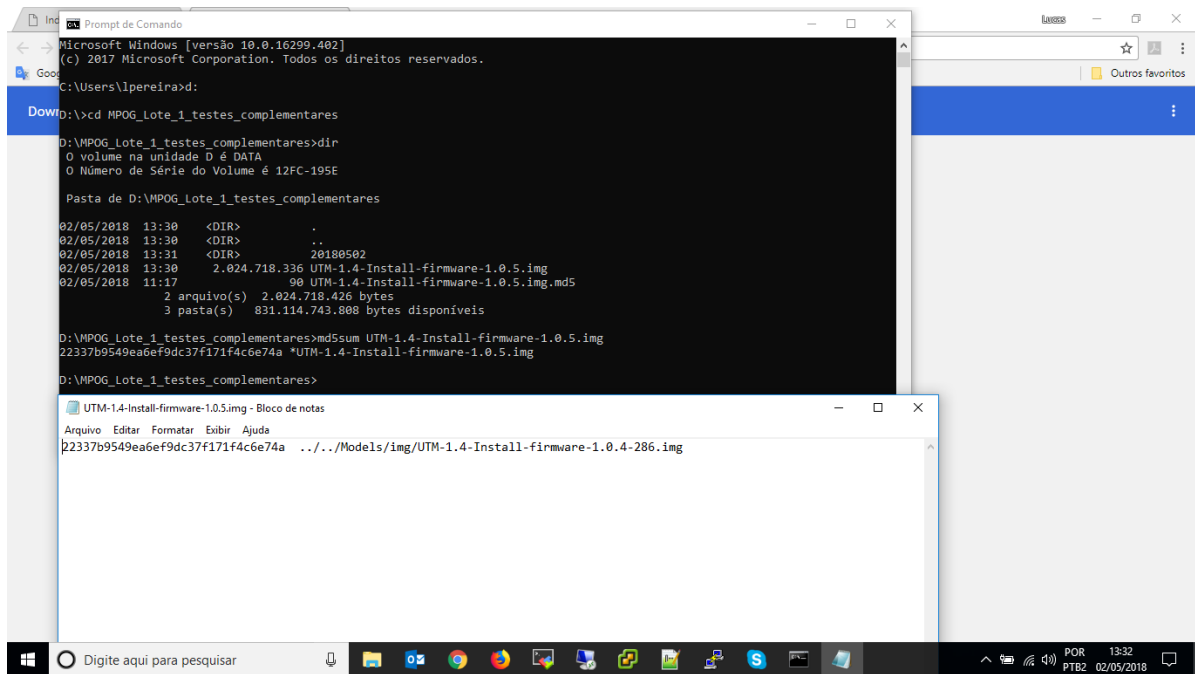


Fig. 2 - Hash do arquivo utilizado nos testes complementares, informado no RTCOM – LOTE 1, páginas 12 e 29.

Outros fatos levantaram, da mesma forma, a atenção do Grupo Técnico. Observou-se que a data de disponibilização do arquivo de *firmware* é imediatamente anterior ao dia de início dos testes (arquivo datado do dia 01/05/2018, 17:41h - conforme fig. 3). Constatou-se também que, após a realização dos testes complementares - dias 2, 3 e 4 de maio de 2018, este arquivo foi retirado do repositório oficial do fabricante, conforme fig. 4.

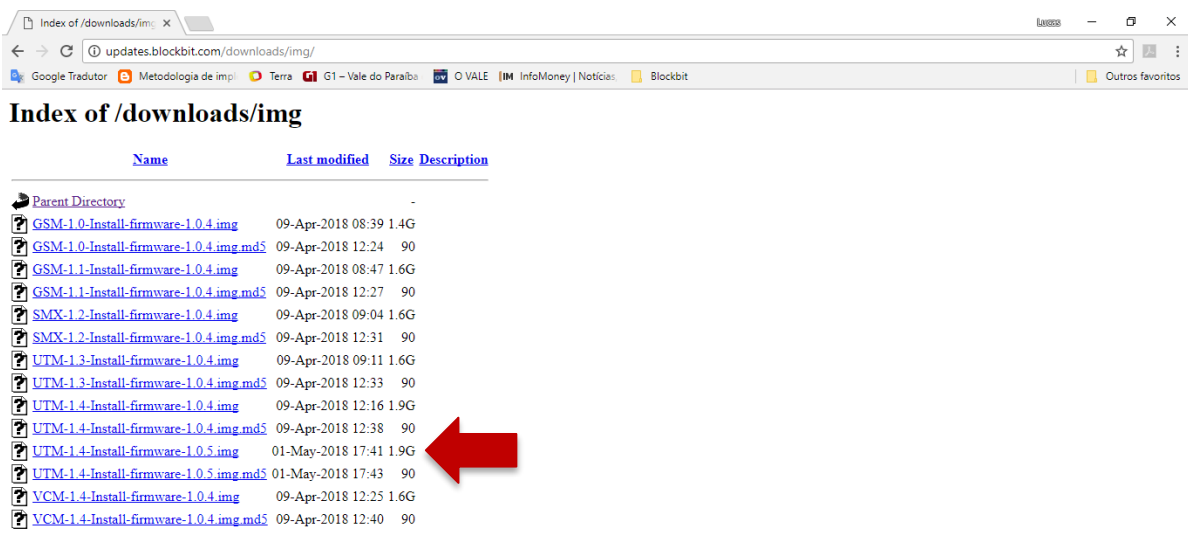


Fig. 3 – Lista dos *firmwares* disponíveis no canal de suporte oficial do fabricante, informado no RTCOM – LOTE 1, páginas 9 e 26, em destaque o arquivo “UTM-1.4-Install-firmware-1.0.5.img”.

Name	Last modified	Size	Description
Parent Directory	-	-	-
GSM-1.0-Install-firmware-1.0.4.img	09-Apr-2018 08:39	1.4G	
GSM-1.0-Install-firmware-1.0.4.img.md5	09-Apr-2018 12:24	90	
GSM-1.1-Install-firmware-1.0.4.img	09-Apr-2018 08:47	1.6G	
GSM-1.1-Install-firmware-1.0.4.img.md5	09-Apr-2018 12:27	90	
SMX-1.2-Install-firmware-1.0.4.img	09-Apr-2018 09:04	1.6G	
SMX-1.2-Install-firmware-1.0.4.img.md5	09-Apr-2018 12:31	90	
UTM-1.3-Install-firmware-1.0.4.img	09-Apr-2018 09:11	1.6G	
UTM-1.3-Install-firmware-1.0.4.img.md5	09-Apr-2018 12:33	90	
UTM-1.4-Install-firmware-1.0.4.img	09-Apr-2018 12:16	1.9G	
UTM-1.4-Install-firmware-1.0.4.img.md5	09-Apr-2018 12:38	90	
VCM-1.4-Install-firmware-1.0.4.img	09-Apr-2018 12:25	1.6G	
VCM-1.4-Install-firmware-1.0.4.img.md5	09-Apr-2018 12:40	90	

Fig. 4 – Lista dos *firmwares* disponíveis no canal de suporte oficial do fabricante, em momento posterior aos testes complementares – arquivo “UTM-1.4-Install-firmware-1.0.5.img” foi retirado. (Acesso em 17/05/2018)

Ainda em relação ao *firmware* utilizado, não foram encontradas no sítio oficial do fabricante ou no canal oficial apresentado na fig. 3 quaisquer informações ou documentações acerca dessa *build* (tais como histórico de releases e alterações ou correções), conforme se vê na fig. 5 (a última informação disponível é datada de julho de 2017, correspondente à versão 1.4.0).

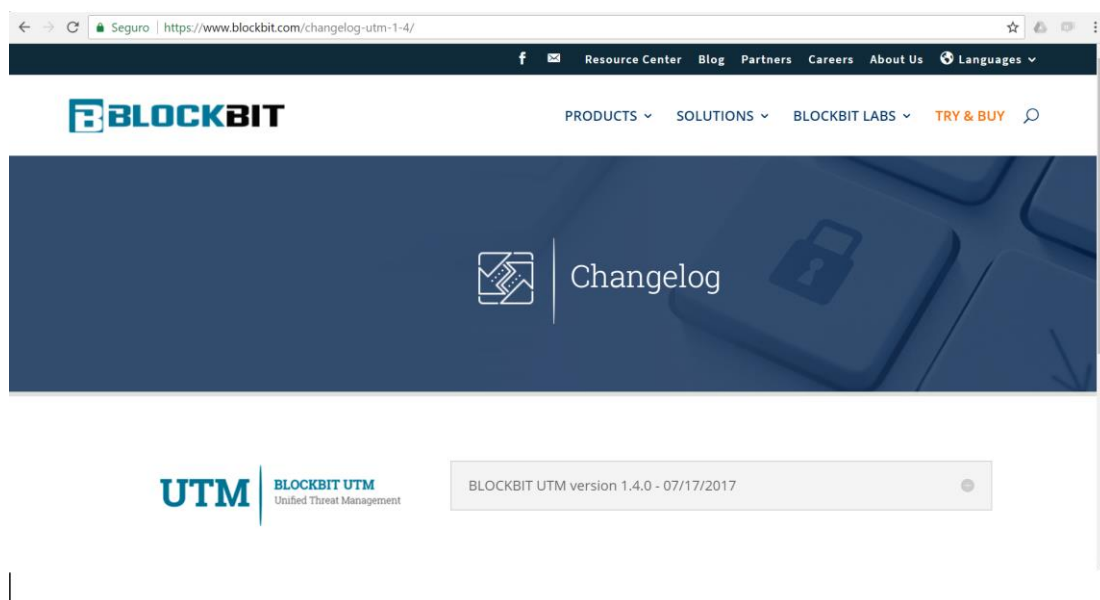


Fig. 5 – Print do sítio web oficial do fabricante, apresentando o *changelog* apenas da Versão 1.4.0, de 17/7/2017. (Acesso em 02/05/2018)

Diante das evidências ora listadas (o novo arquivo, a data do arquivo imediatamente anterior aos testes, a não disponibilização do firmware "UTM-1.4-Install-firmware-1.0.5.img" no canal oficial do fabricante em momento posterior aos testes complementares de 2 a 4 de maio de 2018 e a ausência de informações ou documentações associadas), considera-se a real possibilidade de que se trata de uma versão temporária ou não estável de *firmware*, em estágio de testes ou ainda, em tese, a possibilidade de uma versão de *firmware* específica para a realização dos testes complementares. Tal situação extrapola o disposto no item 4.2 e viola o disposto no item 4.3.3 do ANEXO E do edital, *in verbis*:

"4.2 A solução ofertada deverá então ser atualizada para a versão mais recente do firmware, software, listas de assinaturas e afins, disponíveis pelos canais oficiais de suporte técnico do fabricante da solução. Caso a versão atual tenha menos de 3 meses de liberação de uso para o mercado, será admitida a utilização da versão imediatamente anterior.

"4.3.3 Não serão aceitas versões, correções ou afins em estágio de testes (versões alfa e beta, release candidates, early availability, etc)."

Em que pese as considerações supracitadas, mesmo assim, o grupo técnico optou por seguir com a realização dos testes complementares para o Lote 1 com a utilização de uma nova versão de *firmware* não publicada nos canais oficiais do fabricante, ainda que sem registro de documentações para a versão utilizada ou sem evidências concretas de estabilidade, a fim de oportunizar a demonstração do atendimento pendente, uma vez que no Edital do Pregão Eletrônico nº 5/2017 não veda o uso de novas versões de *firmwares* para a realização dos testes de bancada -mesmo os testes complementares.

4. DOS TESTES DE ASSERTIVIDADE E TESTES ADICIONAIS

As configurações executadas para que se iniciassem os testes de assertividade ficaram registradas no RTCOM - LOTE 1 (páginas 30 a 63).

Conforme solicitado pelo grupo técnico de apoio ao pregoeiro, os testes complementares de assertividade foram executados de duas formas: 1. em conjunto, ou seja, com todo o tráfego injetado de forma simultânea e ativando todas as funcionalidades da amostra; 2. em separado, de forma que fosse ativada isoladamente cada funcionalidade de segurança responsável por analisar o tráfego simulado, quais sejam: acessos WEB (para teste

da funcionalidade de *Web Filter*), acesso a aplicações (para teste da funcionalidade de *Application Control*), ataques (para teste da funcionalidade de *IPS*) e, por fim, tráfego com *malwares* (para teste da funcionalidade de *antimalware*). Tais informações foram registradas pela licitante entre as páginas 63 e 104 do seu relatório.

Durante a execução dos testes complementares de assertividade, o grupo técnico solicitou informações e detalhamento a respeito do fluxo de inspeção de tráfego e de sua capacidade de analisar todos os pacotes em modo ativo, conforme apresentado pela LICITANTE no RTC - LOTE 1 (fig. 6), em especial relativos à inspeção de segurança e relacionamentos entre o *Deep Inspection Engine* (que, segundo informações prestadas, corresponde ao grupo dos módulo *IPS*, *ATP* e Controle de aplicações) e *Proxy-Based Inspection Engine* do equipamento.

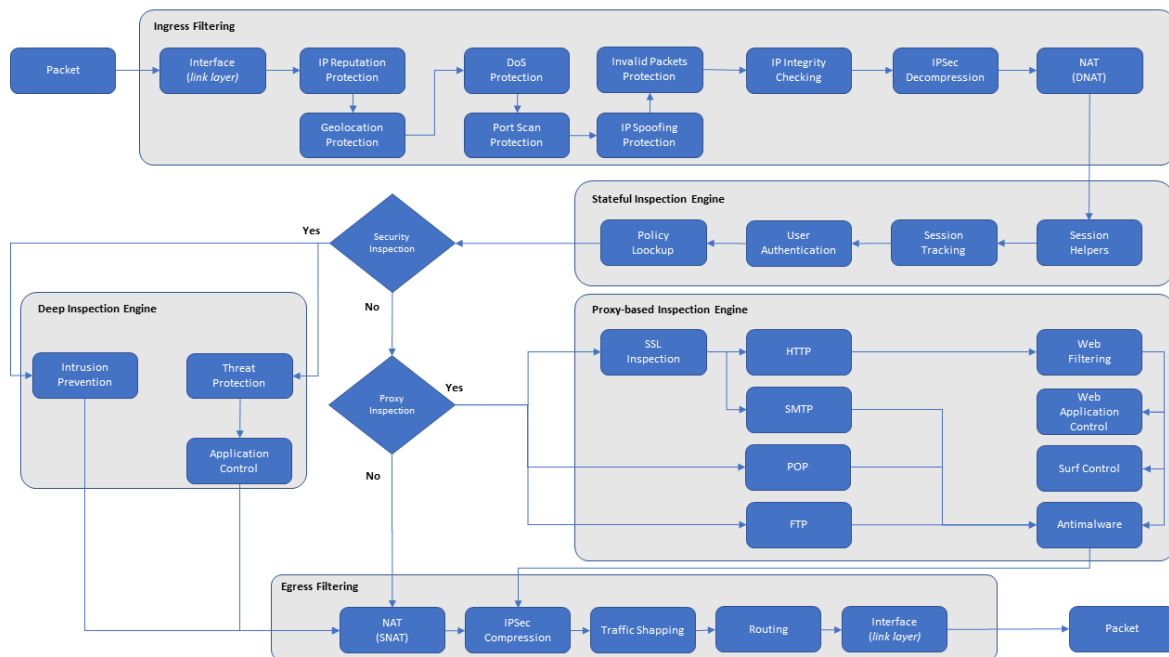


Fig. 6 – Fluxo de inspeção da amostra apresentado pela LICITANTE, informado no RTC – LOTE 1, pág. 20.

Foi informado que os dois *engines* funcionavam de forma integrada, para a inspeção total de todos os pacotes (apesar de não estar claro no fluxo de inspeção apresentado). O grupo técnico observou então recurso de interface gráfica, supostamente correspondente à essa integração, não disponível na versão de *firmware* utilizada nos testes iniciais da amostra, no tocante à essa integração, conforme se vê nas imagens abaixo:

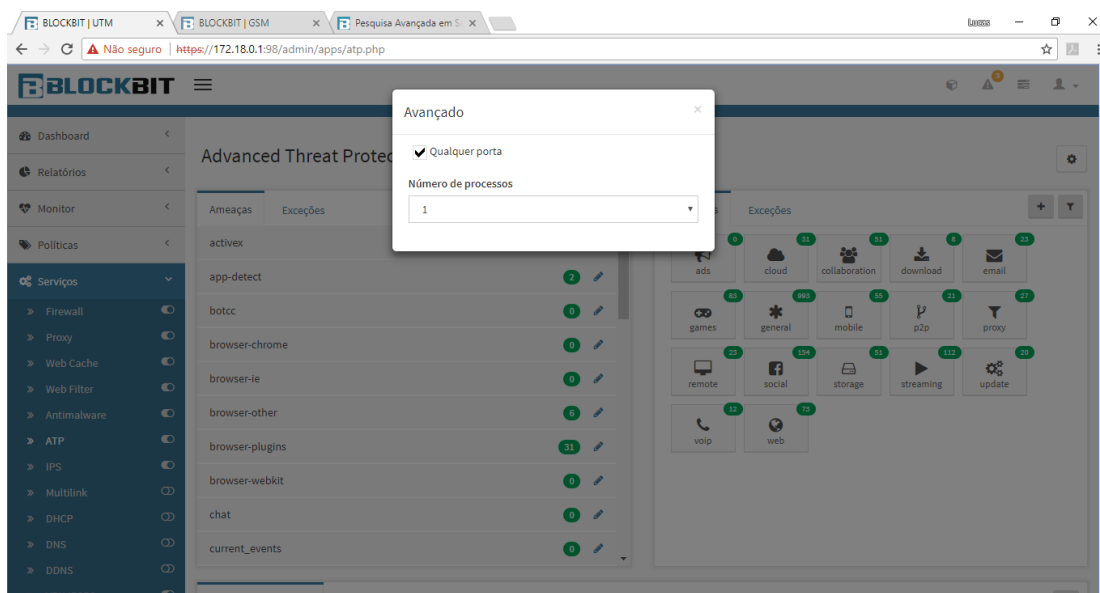


Fig. 7 – Recurso de interface gráfica apresentado pelo equipamento nos testes iniciais da amostra, informado no RTC – LOTE 1, pág. 105.

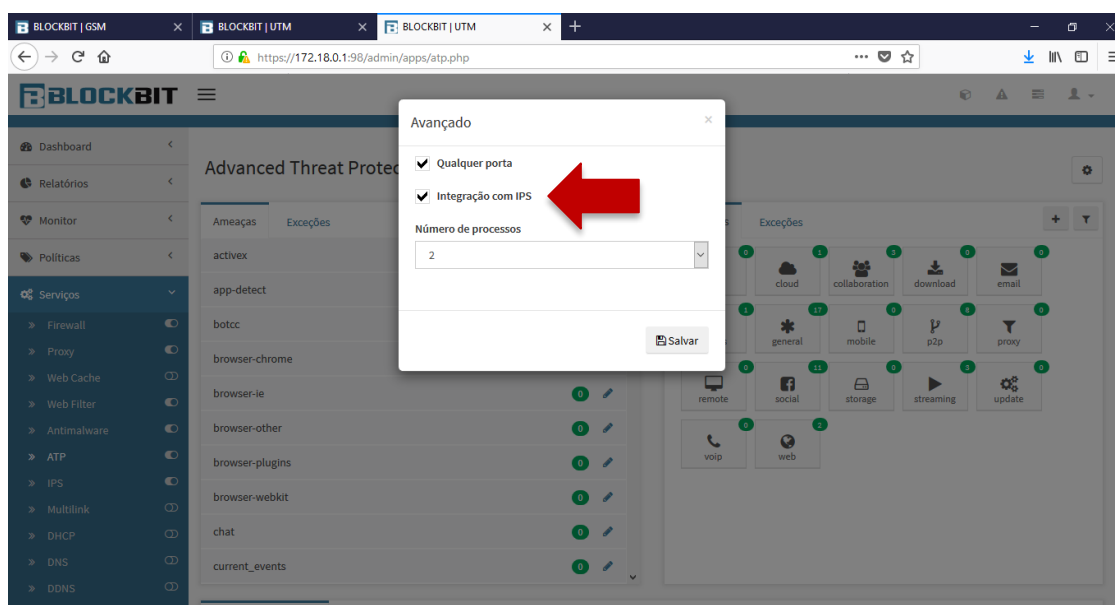


Fig. 8 – Recurso de interface gráfica (em destaque) apresentado pelo equipamento nos testes complementares da amostra, informado no RTCOM – LOTE 1, páginas 106 e 165.

Vale ressaltar que a situação apontada na conclusão do TAM - LOTE 1 foi exatamente a não comprovação de inspeção, por todos os *engines* de segurança, de todos os fluxos de dados, independente do tamanho e direção de fluxo.

Mesmo diante dos esclarecimentos prestados, de forma a dirimir as dúvidas ainda persistentes e verificar e atestar o funcionamento dessa integração e capacidade de inspeção integral, tendo em vista aparentes limitações dos *engines* de IPS e ATP, o grupo técnico requisitou que fossem configurados no equipamento, conforme pág. 152 do relatório

apresentado pela licitante (RTCOM – LOTE1), fluxos de dados típicos similares aos existentes nos filtros de segurança de redes da Administração Pública Federal (redes nas quais, caso aprovados nos testes, os equipamentos em questão poderiam ser utilizados). Tais fluxos de dados possuem direções de fluxo e requisitos de inspeção de segurança distintos entre si e são capazes de auferir, em maiores detalhes, o funcionamento da capacidade de detecção e prevenção de intrusão dos equipamentos, objeto do item 2.3 do edital, e da capacidade de inspeção de todos os pacotes por parte dos *engines* em questão.

Durante as pré-configurações do equipamento para o teste solicitado, dispostas entre as páginas 152 a 178 do RTCOM - LOTE 1, a equipe técnica da LICITANTE alegou que os fluxos de dados solicitados não poderiam ser configurados no equipamento, pois a *engine* de IPS da amostra em avaliação funciona de forma global para todos os fluxos de dados, de forma que não é possível adotar requisitos distintos de segurança (detecção e prevenção ou conjuntos diferentes de assinaturas) entre os fluxos de dados independentes e, assim, inspecionar todos os pacotes de dados. Essa limitação do equipamento faz com que seja necessário desativar completamente a inspeção de segurança da *engine* IPS para um determinado fluxo de dados em detrimento de outro, caso algum outro fluxo também requeira a inspeção do *engine* em questão, mas com qualquer requisito distinto de segurança.

Tal limitação condiciona os requisitos de segurança de uma regra para todas as outras - tanto o modo de funcionamento (detecção ou proteção), quanto o conjunto de assinaturas (na situação de teste proposta, um fluxo requeria apenas a detecção de ataques de um grupo de assinaturas, sem bloqueio, enquanto o outro fluxo requeria a proteção - bloqueio - contra ataques, ainda que utilizando o mesmo grupo de assinaturas, para simplificação).

Ainda segundo a equipe técnica da LICITANTE, somente quando o equipamento é selecionado para funcionamento em modo passivo (ou seja, apenas detecção, sem possibilidade de proteção), é viabilizada a inspeção de todo o tráfego, porém com as mesmas limitações acima mencionadas e sem bloqueio de ataques e tráfegos maliciosos.

Ressalta-se que referências claras a estas informações foram omitidas pelo fabricante no relatório disponibilizado (RTCOM – LOTE 1). As telas apresentadas no relatório, no trecho supracitado, mostram apenas que, dada a limitação, uma mesma configuração de IPS foi utilizada para ambos os fluxos, o que não corresponde à configuração necessária para atender ao teste solicitado (páginas 165 a 168 do RTCOM – LOTE 1). Além disso, as telas apresentadas às páginas 168 a 178 do relatório mostram apenas as detecções obtidas, de forma isolada, por parte do IPS em modo global e outros *engines* de segurança da amostra (no caso o ATP e *Application Control*), mas cujos resultados não correspondem ao que foi solicitado.

Tendo em vista as evidências verificadas, as limitações apresentadas pelo equipamento e confirmadas pelo fabricante e os resultados observados, o grupo técnico conclui, então, que a amostra em questão, diante dos fluxos apresentados, não é capaz de inspecionar todos os pacotes de dados, independente do seu tamanho ou da direção de fluxo, o que viola o disposto no item 5.1.3 do ANEXO E do edital. Portanto, a afirmação apresentada à página 178 do relatório entregue pela LICITANTE é falsa e não procede (“*AS COMPROVAÇÕES QUE O BLOCKBIT CONSEGUIU ATENDER AO CENÁRIO PROPOSTO PELO CLIENTE ESTÃO LOCALIZADOS NOS SEGUINTE ARQUIVOS: (...)*”).

Ainda buscando dirimir as dúvidas acerca da capacidade do equipamento em atender ao disposto no item 5.1.3, buscou-se compreender o fluxo de funcionamento da amostra no tocante à inspeção do tráfego criptografado em HTTPS, requisito obrigatório conforme disposto no item 2.1.39 do edital, *in verbis*:

“*2.1.39 Possuir inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPN e HTTPS)*”

Pela análise do fluxo de inspeção do equipamento (fig. 6), o grupo técnico constatou que, em tese, existiria tratamento e inspeção de tráfego criptografado apenas no grupo de *engines* correspondentes à funcionalidade de proxy (*Proxy-Based inspection engine*). O proxy, por sua vez, segundo o referido fluxo, utiliza a função de *SSL Inspection* para decifrar tráfego HTTPS e SMTP e, então, encaminhar tal tráfego para inspeção apenas das *engines* de *Web Filtering* (filtragem de conteúdo web), *Web Application Control* (controle de aplicações, em tese restrito a aplicações web), *Surf Control* e *Antimalware*, não sendo executada, em sequência, a inspeção pelos *engines* de inspeção profunda – *Deep Inspection engines (Intrusion Prevention, Threat Protection e Application Control)*.

Não havia clareza, portanto, se o equipamento era capaz de inspecionar todo o tráfego criptografado, conforme reza o item editalício supracitado, principalmente no tocante a ataques web tanto via HTTP quanto, sobretudo, encapsulados no protocolo HTTPS, os quais trazem grandes riscos às redes da Administração Pública Federal. Ressalta-se que a preocupação com a necessidade dessa inspeção é crítica para a aplicação com sucesso deste tipo de equipamento e é clara desde a publicação do edital, tanto por força do item 2.1.39 (que é parte dos requisitos comuns e estruturais a todos os lotes da presente aquisição) quanto pelo padrão de tráfego que seria utilizado como base para todos os testes de conformidade, o qual busca garantir que tais ataques sejam também testados e seus resultados auditados, conforme detalhado no item 5.1.12 do ANEXO E, especificamente nos subitens 5.1.12.1 e 5.1.12.2:

“5.1.12.1 HTTP = 55% (conteúdo variável com imagens e textos, tamanho variável, de 100 bytes a 500 Kbytes, sendo uma reserva de 5% para arquivos com malwares e 1% para ataques);

5.1.12.2 HTTPS a sercriptografado e inspecionado = 25% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 bytes, sendo uma reserva de 5% para arquivos com malware e 1% para ataques, utilizando-se criptografia AES e SHA - 256 ou superior).”

Nesse sentido e de forma complementar, o grupo técnico propôs realizar um teste de assertividade para os protocolos HTTP e HTTPS. A empresa concordou e realizou o teste proposto com a coleta das evidências. O grupo técnico verificou que, nos resultados dos testes de assertividade, foram apresentados nas telas do equipamento (a partir da página 63) e nos *logs* resultantes relativos ao tráfego HTTPS apenas resultados para arquivos em URL's com *malware* e categorizações de sítios *web*, constatado pelo relatório do equipamento gerador de tráfego Spirent Avalanche (*“report_5.1.1.3.pdf”*). Detecções de tráfego HTTPS ocorreram na *engine* de filtragem WEB, conforme esperado, mas não foram submetidos à inspeção da amostra quaisquer ataques de rede em tráfego HTTPS, capazes de sensibilizar as *engines* de *Deep Inspection* (IPS e ATP/*Application Control*).

Dentro do teste proposto, foi solicitado, então, a geração de ataque WEB típico de injeção SQL, disponível a partir do gerador de tráfego Spirent (conforme relatório *“report_2.1.39.pdf”*, página 11, com trecho reproduzido na fig. 9) e que, comumente, acomete as redes da Administração Pública Federal. Ademais, o ataque faz parte do conjunto mínimo de proteções que a *engine* IPS deve detectar e bloquear, conforme especifica o item 2.3.7 do edital:

“2.3.7 Possuir proteção contra os ataques como, mas não se restringindo aos mesmos: 1) Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS, Spywares, Botnets e malwares em geral; 2) Ataques e utilização de tecnologia P2P; 3) Ataques de estouro de pilha (buffer overflow); 4) Tráfego mal formado; 5) Cabeçalhos inválidos de protocolo; 6) Ataques de injeção (SQL Injection, LDAP Injection) e de Cross-Site Scripting; 7) Elevação de privilégio e 8) Exploits - Web Server, Web Browser, ActiveX, Javascript, Browser Plugins/Add-ons.”

Foi solicitado que o ataque fosse realizado tanto em uma URL no protocolo HTTP quanto por meio da mesma URL no protocolo HTTPS, destinadas a dois alvos distintos,

submetidas em um total de 4 ataques (portanto, ambos os protocolos para cada um dos destinos), de forma a verificar o comportamento do equipamento em sua inspeção. Foi solicitado também que a amostra fosse configurada apenas para a detecção, e não bloqueio, do ataque selecionado, para simplificação dos testes.

Page (Black)/ URL (Blue)	Method	Attempted Transactions	Successful Transactions	UnSuccessful Transactions	Aborted Transactions	Minimum Response Time	Maximum Response Time	Average Response Time
"https://172.17.2.19/miniuke/pages.asp?id=3%20union+select+0,kul_adi,sifre_0,0+from+members+where+uye_id=2"	GET	1	1	0	0	8506.0	8506.0	8506.0
"https://172.17.2.19/miniuke/pages.asp?id=3%20union+select+0,kul_adi,sifre_0,0+from+members+where+uye_id=2"	GET	1	1	0	0	8495.0	8495.0	8495.0
"http://172.17.1.200/miniuke/pages.asp?id=3%20union+select+0,kul_adi,sifre_0,0+from+members+where+uye_id=2"	GET	1	1	0	0	1260.0	1260.0	1260.0
"http://172.17.1.200/miniuke/pages.asp?id=3%20union+select+0,kul_adi,sifre_0,0+from+members+where+uye_id=2"	GET	1	1	0	0	1258.0	1258.0	1258.0

Fig. 9 – Ataques de injeção SQL solicitados, disponível no relatório “report_2.1.39.pdf” do equipamento gerador Spirent Avalanche, página 11.

A tela resumo do equipamento com o resultado do teste (pág. 209 do RTCOM – LOTE 1), bem como os logs associados fornecidos pela LICITANTE, mostram que foram detectados apenas os ataques de injeção SQL realizados por meio do protocolo HTTP, mas não existiu nenhuma referência, evento ou sinal de inspeção, por parte dos engines de *Deep Inspection*, do ataque realizado por meio do protocolo HTTPS. Conforme inferiu o grupo técnico a partir das informações prestadas pela LICITANTE sobre o fluxo de inspeção da amostra e das evidências previamente coletadas, apenas o engine de filtragem web (*Web Filter*) foi capaz de identificar, embora sem sequer categorizar o tráfego como um ataque, as quatro requisições realizadas em HTTP e HTTPS (telas apresentadas nas páginas 207 e 208), não se tratando, portanto, do efeito requerido ou da comprovação necessária.

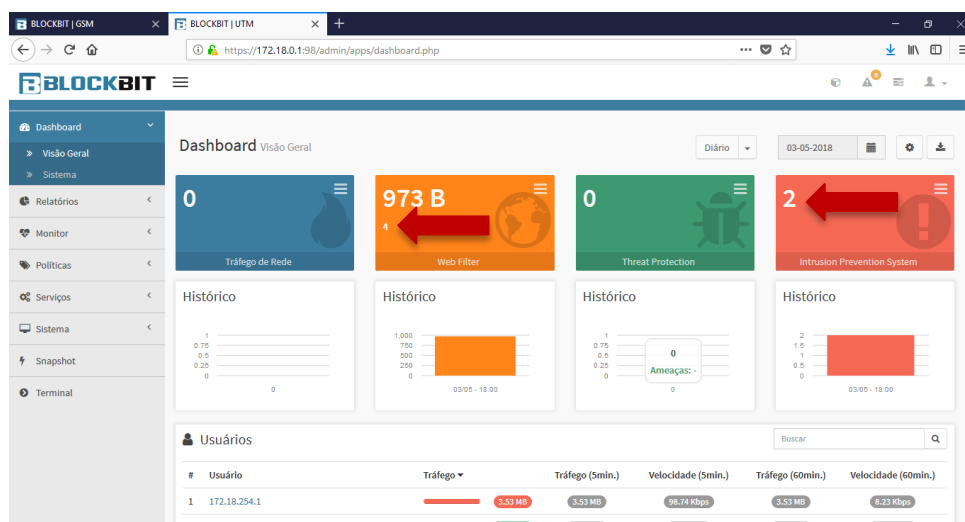


Fig. 10 – Tela resumo com os resultados das detecções efetuadas pela amostra, com destaque para o número de detecções dos módulos de filtragem web (4) e IPS (2), informado no RTCOM – LOTE 1, pág. 209.

Data	Usuário/IP	Origem	Destino	Impacto	Detecção	Ação
03-05-2018 18:54	172.17.1.200	172.18.3.10:17861	172.17.1.200:80	alto	WEB_SERVER Possible SQL Injection Attempt SELECT FROM	
03-05-2018 18:54	172.17.1.200	172.18.3.10:17861	172.17.1.200:80	alto	WEB_SERVER Possible SQL Injection Attempt UNION SELECT	

Fig. 11 – Detalhamento das detecções do módulo IPS (inspecionado apenas tráfego HTTP) – RTCOM – LOTE 1, pág 209

Tendo em vista as evidências coletadas, o grupo técnico constatou explícita e inequívoca violação do disposto no item 2.1.39 do edital e, conseqüentemente, não atendimento do disposto no item 5.1.3 do ANEXO E, dada a incapacidade do equipamento de inspecionar totalmente o tráfego criptografado no protocolo HTTPS.

Ressalta-se, também, que as afirmações realizadas por parte da LICITANTE, na página 207 do relatório apresentado, são falsas e não procedem, conforme expõe-se:

i) Afirmação 1: *“FOI SOLICITADO PARA EXECUTAR O TESTE DE INSPEÇÃO DA FUNCIONALIDADE DE IPS COM DESCRIPTOGRAFIA DO TRÁFEGO. VALE RESSALTAR QUE NA ESPECIFICAÇÃO DO EDITAL DO MÓDULO DE IPS QUANDO É DETALHADO OS REQUISITOS MÍNIMO DE FUNCIONALIDADES NÃO É SOLICITADO A DECRYPTOGRAFIA DO TRÁFEGO.”*

i.1) Resposta: a LICITANTE mostra desentendimento do disposto no edital do pregão eletrônico n ° 05/2017, sobretudo no que se refere à especificação mínima do LOTE 1 (itens 3.1 a 3.7), o qual deve atender, de forma simultânea e total, todos os requisitos mínimos comuns a todos os lotes (item 2.1, e por sua vez, sub-item 2.1.39), bem como todas as funcionalidades de segurança especificadas nos itens 2.3 a 2.6 (incluindo, portanto, o conjunto de funcionalidades IPS, especificado no item 2.3). Tal atendimento simultâneo e total constitui, inclusive, objeto de verificação durante os testes, conforme reza o item 5.1.1.1 do ANEXO E:

“5.1.1.1 Destaca-se que, durante a realização dos testes, a amostra será avaliada com as funcionalidades dos itens 2.1, 2.3, 2.4, 2.5 e 2.6 habilitadas, salvo quando houver

indicação explícita contrária neste documento, permitindo sempre que possível inspeção por fluxo."

Ademais, em que pese eventuais diferenças tecnológicas ou formas diferentes de implementação das funcionalidades entre fabricantes, a inspeção profunda de tráfego, sobretudo do tráfego criptografado (objeto do referido item 2.1.39), é conceito e condição basilar para que se torne viável e possível o funcionamento completo das *engines* de segurança dos equipamentos ora licitados de forma a atender, no que couber, ao disposto nos itens 2.3, 2.4, 2.5 e 2.6. Em nenhum momento da presente licitação, seja durante a fase de análise das propostas ou durante os testes de conformidade, a LICITANTE apresentou informações, indícios ou comprovações de que o equipamento fosse capaz de, por meio de alguma tecnologia específica, realizar inspeção profunda sem a necessária decifração de tráfego HTTPS.

ii) Afirmação 2: *"O ATAQUE SOLICITADO PELO CLIENTE COM O TRÁFEGO CRIPTOGRAFADO NÃO É SUPORTADO PELA FERRAMENTA DE INJEÇÃO DE TRÁFEGO (AVALANCHE)."*

ii.1) Resposta: o equipamento de geração de tráfego Spirent Avalanche mostrou-se capaz e habilitado para gerar o ataque WEB de injeção SQL baseado em protocolo HTTPS. Tal informação é evidente e clara no relatório "*report_2.1.39.pdf*" e configurações associadas, extraídos diretamente da ferramenta Spirent Avalanche e disponíveis para consulta pública, caso necessário. Ademais, não existiu quaisquer manifestações em contrário, por parte da equipe técnica responsável pelo equipamento gerador de tráfego, acerca de quaisquer limitações de configuração e geração do ataque solicitado. Ainda, a LICITANTE se contradiz em seu próprio relatório, dado que o ataque de injeção SQL foi gerado pela mesma funcionalidade ou módulo do equipamento gerador, por meio do mesmo tipo de requisição (GET) utilizado para gerar o tráfego *web* HTTPS detectado pela amostra na ocasião dos testes de filtragem de conteúdo *web* e detecção de *malwares web*. Tal informação pode ser depreendida de diversas telas apresentadas no próprio documento, a exemplo das imagens nas páginas 205 e 284, dentre outras.

iii) Afirmação 3: *"O TESTE FOI REALIZADO ATRAVÉS DO MÓDULO DE TESTE DE NAVEGAÇÃO WEB DA FERRAMENTA AVALANCHE, ONDE NÃO SENDO POSSÍVEL EXTRAIR O RELATÓRIO COMPROBATÓRIO QUE O ATAQUE FOI REALIZADO, DETECTADO OU BLOQUEADO."*

iii.1) Resposta: conforme item ii.1, o relatório “report_2.1.39.pdf” pode ser extraído com sucesso e sem problemas do equipamento, o qual mostra o sucesso da geração do ataque por parte do equipamento gerador Spirent Avalanche. A tela resumo do resultado dos testes é apresentada na figura 12, sendo o equipamento gerador, portanto, capaz de informar que o ataque foi gerado e submetido à amostra, tendo seu resultado coletado com sucesso.

Top Level Summary

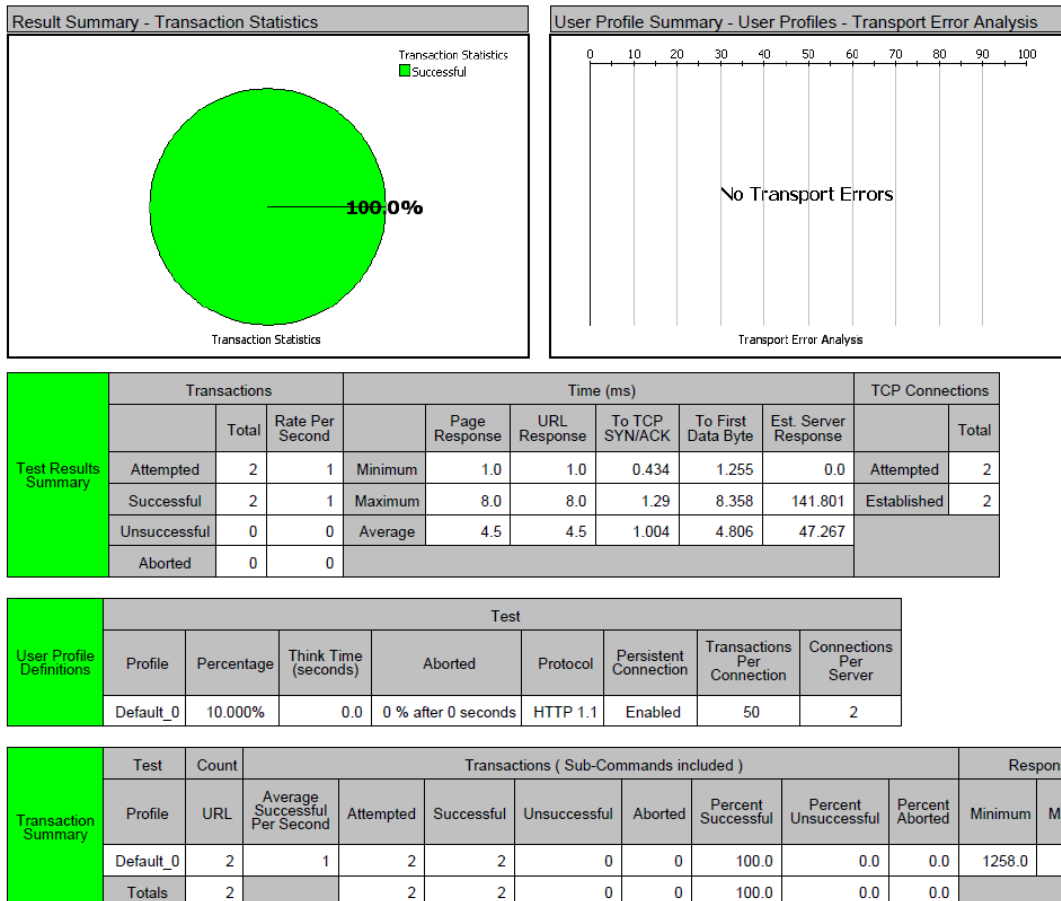


Fig. 12 – Sumário da execução do teste de injeção SQL, disponível no relatório “report_2.1.39.pdf” do equipamento gerador Spirent Avalanche, página 2.

5. TESTES DE DESEMPENHO E TESTES ADICIONAIS

Conforme exposto na conclusão do TAM - LOTE 1, o não atendimento ao item 5.1.3 traria prejuízo à avaliação do desempenho da amostra:

“O não atendimento do requisito anterior traz impacto negativo direto ao previsto no item “3.1.1.2. Possuir, no mínimo, o throughput de inspeção de 100 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”, prejudicando a avaliação do atendimento do Teste de Desempenho, uma vez que a inspeção, independentemente da direção do fluxo, é pressuposto necessário para a execução dos testes de desempenho. Em outras palavras, não há como garantir que a vazão mínima apresentada na página 597 (121 Mbps) do Relatório de Testes da Amostra se manteria com os mesmos valores, caso houvesse a inspeção integral, uma vez que tal ação consome mais processamento do equipamento avaliado, o que possui reflexo direto na redução da vazão entregue pela solução e que é ponto relevante de avaliação na vertical de desempenho dos testes de conformidade do Anexo E do Termo de Referência.”

Ainda que persistindo a impossibilidade de avaliação do desempenho da amostra - dada a não comprovação do item 5.1.3 do ANEXO E e consequente prejuízo à verificação efetiva do item 3.1.12, a equipe técnica da LICITANTE prosseguiu ao teste de desempenho, tendo seus registros apresentados a partir da página 209 do relatório. As evidências referentes à parametrização estão apresentadas até a página 269 e a partir da página 270 são apresentadas as evidências referentes ao teste de desempenho. Na página 283 é apresentada a comparação entre os resultados da parametrização e os testes de desempenho, conforme solicitado no item 5.3.8.3.

Durante as configurações e após a execução do referido teste, entretanto, o grupo técnico observou que as detecções relacionadas a *malwares* submetidos via tráfego SMTP se concentravam apenas nos resultados do *engine* IPS, que funcionava em modo detecção, e que a funcionalidade de detecção e eventual bloqueio por parte do módulo de proteção *antimalware* estava desabilitada para o protocolo SMTP. Segundo o fluxo de inspeção do equipamento (fig. 6 anterior) e informações prestadas pela LICITANTE, era esperado que o tratamento de tráfego SMTP fosse realizado pelo *Proxy-based inspection engine* e pelo módulo específico *antimalware*. Foi solicitada à equipe técnica da LICITANTE esclarecimentos adicionais acerca do módulo de *antimalware* e da razão de estar desabilitado, informações as quais o grupo técnico não considerou suficientes para esclarecer, de forma objetiva, o seu funcionamento.

Ressalta-se que as funcionalidades *antimalware* da amostra devem estar em conformidade ao disposto no item 2.4 do edital, que especifica o conjunto de funcionalidades anti-vírus e *antimalware*, em especial destaque aos itens 2.4.1, 2.4.2 e 2.4.7:

"2.4.1 Possuir módulo de proteção de antivírus, anti-malware e anti-bot no mesmo equipamento do firewall;

2.4.2 Possuir funcionalidades de varredura contra vírus e malwares em tráfego nos seguintes protocolos: HTTPS, HTTP e pelo menos dois dos seguintes: FTP, POP3, IMAP e SMTP;

2.4.7 Identificação, classificação e bloqueio de malwares, contemplando no mínimo, Trojan, Spywares, Backdoors, Worms e Vírus."

Da mesma forma, vale ressaltar que, similarmente ao já exposto sobre a criticidade de inspeção integral para proteção contra ataques via HTTPS, a inspeção de *malwares* que trafegam via protocolo de e-mail SMTP é igualmente crítica para as redes da Administração Pública Federal. Pelos motivos já expostos, a preocupação com a inspeção de segurança de tráfego de e-mail é também objeto de análise e comprovação dos testes de conformidade, tendo em vista o padrão de tráfego que seria utilizado como base para todos os testes, conforme detalhado no item 5.1.12 do ANEXO E, especificamente nos subitens 5.1.12.3 e 5.1.12.3.2:

"5.1.12.3 Aplicações, outros ataques, outras ameaças e outros protocolos = 20%, a ser acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes.

5.1.12.3.2 E-mail (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos)"

O grupo técnico solicitou, então, teste específico para esclarecimento e comprovação do funcionamento do módulo *antimalware* da amostra, que não se encontrava habilitado nos testes prévios para tráfego SMTP. O serviço de *malware scanning* do *proxy* foi habilitado para o protocolo SMTP e na regra que trata o fluxo de teste foi selecionada a função *Email Protection - SMTP* (páginas 295 e 294 do RTCOM – LOTE 1, respectivamente). Para este teste isolado, o equipamento gerador Spirent Avalanche foi configurado com o mesmo *malware* via SMTP utilizado nos testes de desempenho (constante às páginas 21 do relatório "*performance.pdf*" e 14 do relatório "*Spirent_smtp_malware_detect.pdf*", respectivamente).

A tela resumo do equipamento com o resultado do teste (fig. 13), bem como o extrato do resultado descrito em "*Spirent_sntp_malware_detect.pdf*", apresentado na página 293 do relatório da LICITANTE, mostram haver bloqueio do *malware* submetido via SMTP.

Top Level Summary

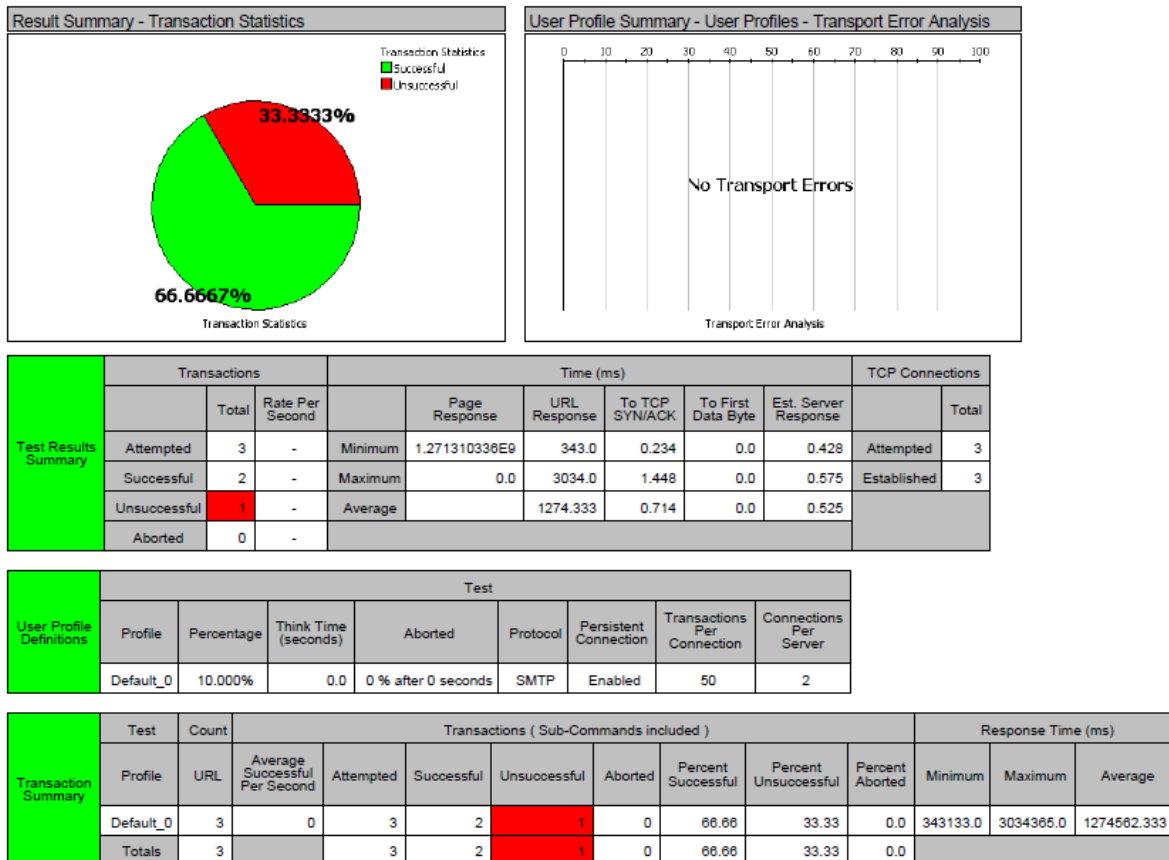


Fig. 13 – Sumário da execução do teste de inspeção de *malware* via SMTP, disponível no relatório "*Spirent_sntp_malware_detect.pdf*", pág. 2.

Entretanto, verificando-se os demais resultados e as evidências geradas pela amostra, constatou-se que apenas o módulo IPS foi capaz de detectar a ameaça em questão (telas nas páginas 297 e 298), inexistindo quaisquer sinais, eventos ou registros de identificação e classificação por parte do módulo *antimalware*, ou mesmo confirmação ou evidências de que, de fato, o bloqueio observado foi realizado pelo módulo em questão (conforme tela de resultados do referido módulo, que está vazia, apresentada na página 296 do relatório da LICITANTE).

Tendo em vista tais resultados, conclui-se que as observações do LICITANTE constantes na página 293 do relatório apresentado são apenas parcialmente verdadeiras, a saber:

iv) Afirmação 1: "*MALWARE DETECTADO PELO MÓDULO IPS;*"

iv.1) Resposta: De fato o módulo IPS foi capaz de detectar a ameaça no *malware* via SMTP, o que está alinhado ao esperado de seu funcionamento mínimo, haja vista o disposto no item 2.3.7 do edital, já abordado anteriormente.

v) Afirmação 2: "*MALWARE DETECTADO PELO MÓDULO DE PROXY SMTP;*"

v.1) Resposta: não é possível afirmar tal comportamento, dado que não foram detectados, conforme exposto, quaisquer evidências de que o módulo *antimalware* da amostra funciona como o informado. Ainda seguindo o resultado apresentado, o módulo não foi capaz de detectar, inspecionar, identificar e classificar o *malware* utilizado no teste;

vi) Afirmação 3: "*COMPROVAÇÃO (ARQUIVO: Spirent_smtp_malware_detect.pdf, PÁGINA 14), ONDE EMAIL BLOQUEADO É O ÚNICO QUE CONTÉM VÍRUS.*"

vi.1) Resposta: o relatório do teste mostra, de fato, o bloqueio do *malware* infectado após a tráfego ser submetido à amostra. Entretanto, dado que o *engine* IPS foi configurado em modo detecção (sem bloqueio) e dado que não existem evidências de que, de fato, o módulo *antimalware* foi o responsável pelo referido bloqueio, a comprovação de atendimento ao teste requerido não foi evidenciada.

Diante das evidências acima coletadas, o grupo técnico constatou explícita e inequívoca violação do disposto no item 2.4.7 do edital e, conseqüentemente, não atendimento do disposto no item 5.1.3 do ANEXO E, dada a incapacidade do equipamento de inspecionar totalmente os fluxos de dados em protocolo SMTP.

6. CONCLUSÃO

O grupo técnico de apoio ao pregoeiro, tendo em vista os dados, as informações, os registros, as evidências coletadas durante os testes complementares da amostra e os fatos previamente expostos nesse TAM dos testes complementares, conclui, sem margem de incertezas, que o equipamento ofertado pela LICITANTE BLOCKBIT para o LOTE 1 **não atende ao especificado nos itens 5.1.3 (ANEXO E), 2.1.39 e 2.4.7 do edital de pregão eletrônico nº 05/2017**, dado que não existe, para a amostra apresentada, configuração possível que seja capaz de "*realizar a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo*". A conclusão é fundamentada pela comprovação de que:

1. o funcionamento das *engines Deep Inspection* (IPS e ATP) não permite a inspeção e análise de todos os fluxos de dados;
2. o equipamento não é capaz de inspecionar, detectar e proteger contra ataques *web* realizados via HTTPS;
3. o equipamento não é capaz de inspecionar completamente o tráfego SMTP e não identifica e nem classifica *malware* que é enviado por este protocolo.

Considerando-se o exposto no TAM-LOTE 1 inicial; nos testes complementares realizados no período de 2 a 4 de maio de 2018; no respectivo relatório sobre tais testes complementares entregue pela empresa BLOCKBIT; neste TAM dos Testes Complementares -LOTE 1 e, ainda, levando-se em conta o desafio encontrado, desde os testes iniciais, para a obtenção de informações claras, precisas, suficientes e inequívocas acerca do funcionamento da solução ofertada pela fabricante em questão, para a confirmação do completo atendimento das especificações plasmadas nas exigências técnicas do Termo de Referência do Pregão Eletrônico nº 5/2017, o grupo técnico recomenda ao pregoeiro a REPROVAÇÃO da amostra do LOTE 1 e consequente desclassificação da empresa BLOCKBIT. Além disso, em vista de todos os recursos e esforços dispendidos pela Administração Pública com a realização dos testes iniciais e complementares, bem como das evidências indicadas, ao longo dos testes, de que a solução ofertada pela BLOCKBIT não atenderia ao disposto nas exigências técnicas do pregão em epígrafe, o grupo técnico sugere também ao pregoeiro que avalie possíveis aplicações de sanções à LICITANTE, em função de todo o exposto no presente documento e no TAM – LOTE 1.