ESTADO DE GOIÁS
SECRETARIA DE ESTADO DA EDUCAÇÃO
GERÊNCIA DE SUPORTE DE REDES

Nota Técnica nº: 1/2023 - SEDUC/GESRCD-12035

Assunto: QUESTIONAMENTOS PROVA DE CONCEITO LOTE 01

Preparado por HUGO AUGUSTO AGUIAR COBRA **Data: 08/08/2023**

Identificação do Projeto

Processo 202000006045301

Etapa: Teste de Conformidade PREGÃO ELETRÔNICO Nº001/2023

Coordenador do Projeto: Marcus Paulo Magalhães Barbosa **E-mail: marcus.barbosa@seduc.go.gov.br**

Gerente de Suporte de Rede: Marcus Paulo Magalhães Barbosa

Superintendente de Tecnologia da Informação: Bruno Marques Correia

Interessado: COMPWIRE INFORMATICA LTDA **CNPJ: 01.181.242/0006-04**

1 **QUESTIONAMENTOS:**

Item 5.1.5.1 - Possuir throughput de no mínimo 9 (Nove) Gbps de tráfego real por nó do cluster com as funcionalidades de segurança habilitadas (Firewall,IPS, Logging, Controle de Aplicação, Proteção contra Malware):
Baseado no teste de performance, apontamos os seguintes tópicos que não são coerentes com o item solicitado:

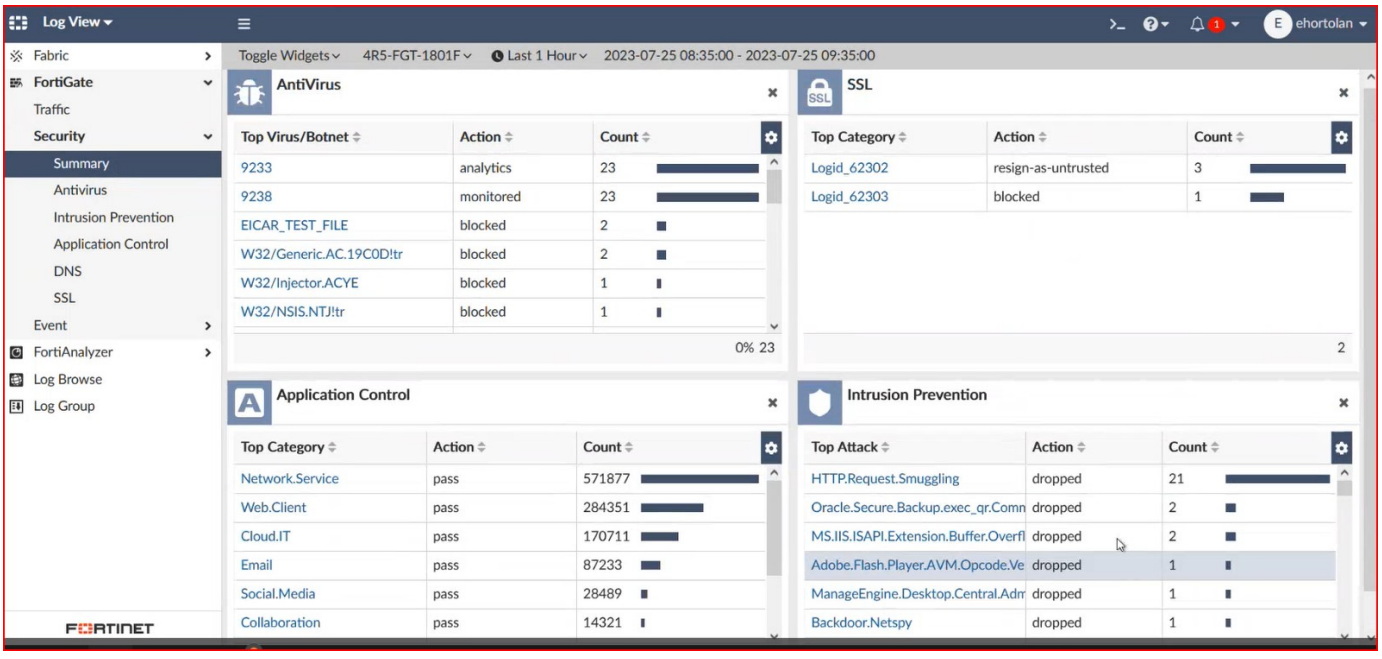
Para cada teste foi utilizado um policy. No caso de performance, foram usados os "***Teste TP***" e "***Teste TP Malware***".
Deve ser apresentado toda a base de dados contendo as assinaturas que estão sendo utilizadas na inspeção, assim como o perfil de SSL inspection deve ser o mesmo para as duas regras, pois é evidente que o Deep inspection que é o recomendado não foi habilitado na primeira regra na qual teve maior quantidade de match de conexões.

RESPOSTA: Quanto ao teste de Troughput, no TERMO DE REFERÊNCIA não é solicitado DEEP Inspection/SSL Inspections como fator para calculo de troughput, conforme ITEM 5.1.5.1: Possuir throughput de no mínimo 9 (Nove) Gbps de tráfego real por nó do cluster com,no mínimo, as funcionalidades de segurança habilitadas (Firewall,IPS, Logging, Controle de Aplicação,Proteção contra Malware);
Mesmo assim, os teste realizados foram feitos com SSL Inspections habilitado.

No print abaixo, não mostra nenhuma evidência de tráfego com malware:

Na comprovação, não foi apresentado log minuto a minuto da parte de Security, apenas de "Traffic". Mostraram apenas no FortiAnalyzer, precisa ser apresentado no próprio equipamento.
Ou seja, seria interessante gerar um novo teste e mostrar tráfego, aplicações, malwares conhecidos e desconhecidos (dia/zero) baseado em cada funcionalidade de segurança que foi solicitado no itens de capacidade.

RESPOSTA: Informamos que o LOG de Malware foi apresentado em outra tela.



Outro ponto, quando foi realizado o teste com as funcionalidades de segurança ativadas, percebe que a quantidade de sessões (Conexões concorrentes e Simultâneas) está bem abaixo do que foi solicitado pelo edital, sendo assim, invalidaria os itens posteriores de Conexões concorrentes e novas conexões por segundo.
Dentro do equipamento FG-1801F não foi apresentado o nível de processamento da NPs, sendo assim, não é possível visualizar o consumo de CPU das NPs.

RESPOSTA: O teste apresentado foi de TROUGHPUT e não de Conexões concorrentes e Simultâneas.

Outro ponto de destaque é que o teste deveria ser realizado com um cluster habilitado conforme aludido no referido item que deve ser por "**NÓ**" do cluster. Sabemos que as soluções em composição de cluster, podem ter uma carga de processamento maior devido a tarefas de sincronização de sessões, tabelas de FIB e etc e isso iria afetar o seu desempenho real.

Também não foi apresentado se todas as assinaturas da solução estavam habilitadas e atuantes com seus bancos de assinatura em modo extended.

RESPOSTA: Nas regras constam todas as assinaturas solicitadas habilitadas, também foi reforçado ao final da reunião.
Não é solicitado montagem de cluster no laboratório.

5.1.6.1 - Permitir no mínimo 150.000 (cento e cinquenta mil) novas conexões por segundo por
nó do cluster;
O teste foi realizado com uma regra exclusiva para novas conexões por segundo, ou seja, em nenhum momento foi realizado envio de tráfego, somente abriu uma conexão sem tráfego de rede.

Outro ponto de destaque é que o teste deveria ser realizado com um cluster habilitado conforme aludido no referido item que deve ser por **"NÓ"** do cluster. Sabemos que as soluções em composição de cluster, podem ter uma carga de processamento maior devido a tarefas de sincronização de sessões, tabelas de FIB e etc e isso iria afetar o seu desempenho real.

RESPOSTA: Envio de tráfego foi realizado no teste de TROUGHPUT.
Não é solicitado montagem de cluster no laboratório.

5.1.6.2 - Permitir no mínimo 4.000.000 (quatro milhões) conexões simultâneas por nó do cluster;
Cada teste está sendo realizado HTTP 64Kb de payload, porém sem nenhum tráfego de rede que mostre algo próximo ao mundo real que terá bastante tráfego web nas escolas.
Outro ponto de destaque é que o teste deveria ser realizado com um cluster habilitado conforme aludido no referido item que deve ser por **"NÓ"** do cluster. Sabemos que as soluções em composição de cluster, podem ter uma carga de processamento maior devido a tarefas de sincronização de sessões, tabelas de FIB e etc e isso iria afetar o seu desempenho real..
O equipamento FG-1801F apresentou mais de 50% de utilização de memória. Somente gerou uma sessão, porém sem nenhuma transação de tráfego para mostrar a capacidade do equipamento. Podemos dizer que no caso de envio de tráfego (mínimo) web, o consumo de memória seria elevado.

Conforme a configuração do FG-1801F, é notado que a funcionalidade de Web Filter está desabilitada, assim como o SSL Inspection não possui nada de deep inspection habilitado para trazer mais segurança à infraestrutura.

Basta observar no teste de capacidade da Miercom que comparou throughput e outros dos appliances da Fortinet e Palo Alto:
https://miercom.com/wp-content/uploads/2022/07/Miercom-Report-Palo-Alto-NGFW-Competitiv
e-Performance-DR220527E.pdf
Pode notar no link que o perfil de funcionalidades está diferente do que foi apresentado na homologação:

RESPOSTA: Envio de tráfego foi realizado no teste de TROUGHPUT.
Não é solicitado Filtro WEB e SSL inspection em no teste de conexões simultâneas, isso é feito no teste de TROUGHPUT. O qual é solicitado web filter e não ssl inspection.
Não é solicitado montagem de cluster no laboratório.
Não é solicitado quantidade de memória.

Itens de capacidade do FG-81F

5.2.3 TROUGHPUT
5.2.3.1 Possuir no mínimo 900 (novecentos) Mbps de tráfego real com as funcionalidades de segurança habilitadas (Firewall, IPS, Logging, Controle de Aplicação, Proteção contra Malware);
Conforme a configuração do FG-81F, é notado que a funcionalidade de SSL Inspection possui perfis diferentes na qual o deep inspection deveria trazer mais segurança para o ambiente das escolas. Assim, como é notado que o fluxo de conexões da primeira regra é muito superior à
segunda, assim concluímos que todas as funcionalidades não foram habilitadas corretamente uma vez que o tráfego da regra 1 "***Teste TP***" teve mais de 38 Gb comparado a regra 2 "***Teste TP Malware***" que foi apenas de 32Mb.
Conforme o item 5.2.3.1, a solução deve performar 900 Mbps de tráfego real com as funcionalidades de segurança habilitadas (Firewall, IPS, Logging, Controle de Aplicação, Proteção contra Malware) simultaneamente. Ou seja, as regras 1 e 2, deverão ser resumida a uma única regra ou ter o mesmo perfil de configuração em especial da engine SSL "Deep Inspection".

Baseado nos relatório da Miercom conforme (público) do link abaixo, é possível perceber a degradação do equipamento quando é habilitada as funcionalidades de segurança, ou seja, espelhando o mais próximo do mundo real como é solicitado no item. Segue abaixo:
https://miercom.com/pdf/reports/DR210617G.pdf

RESPOSTA: Quanto ao teste de Troughput, no TERMO DE REFERÊNCIA não é solicitado DEEP Inspection/SSL Inspections como fator para calculo de troughput, conforme ITEM 5.1.5.1: Possuir throughput de no mínimo 9 (Nove) Gbps de tráfego real por nó do cluster com,no mínimo, as funcionalidades de segurança habilitadas (Firewall,IPS, Logging, Controle de Aplicação,Proteção contra Malware);
Mesmo assim, os teste realizados foram feitos com SSL Inspections habilitado.

Também não foi apresentado se todas as assinaturas da solução estavam habilitadas e atuantes com seus bancos de assinatura em modo extended.

RESPOSTA: Nas regras constam todas as assinaturas solicitadas habilitadas, também foi reforçado ao final da reunião.

5.2.4.2 Permitir no mínimo 200.000 (duzentas mil) conexões simultâneas;
Foi realizado o teste de conexões simultâneas, porém nenhum tráfego é transferido, apenas abrem as conexões e encerram. Sendo assim, como esse teste pode ser aplicado no mundo real, uma vez que o item do projeto solicita que o equipamento deve possuir funcionalidades de segurança.
É notado que nenhum erro é apresentado, pq nenhum tráfego foi apresentado.
Na comprovação de "Hits" que contém Match na regra, é notado que nenhum tráfego de rede passou pelas regras 1 e 2.

Apenas na regra 3 "Teste CPS e CC", teve conexões, pois não existe nenhuma aplicação atrelada a regra, assim, impossível determinar o quanto o equipamento vai suportar em ambiente educacional.

RESPOSTA: As regras 1 e 2 foram aplicadas para o teste de TROUGHPUT, não cabendo cita-las no teste de conexões simultâneas.

5.2.5.2 Possuir unidade de armazenamento interna de no mínimo 120 GB, capaz de armazenar todo o software, configuração e logs;
De acordo com o item de capacidade mínima de armazenamento, é solicitado 120 Gb de espaço em disco. Durante a comprovação do item, foi realizado o procedimento do comando:
● diagnose hardware deviceinfo disk
Conforme print abaixo, é evidente que o equipamento possui apenas (Total HD Logging Space):
● 94517 MB / 1024 = Corresponde a **92 GB para log.**
Outro ponto a se considerar é que o equipamento proposto possui um armazenamento flash de 4GB para o sistema operacional e arquivos de configuração. Assim como um disco adicional para as demais funções.
Isto mostra que a unidade de armazenamento exibida não é capaz de armazenar todos os arquivos conforme solicitado pelo item.

RESPOSTA: ITEM 5.2.5.2: Possuir unidade de armazenamento interna de no mínimo 120 GB, capaz de armazenar todo o software, configuração e logs;

Não é solicitado 120 exclusivo para LOGS, o equipamento apresentou disco interno de 120GB conforme solicitado.

2	CONCLUSÃO
2.1	Quanto aos questionamentos realizados pelo representante da empresa COMPWIRE INFORMÁTICA durante a POC do LOTE 01, entendemos que os testes apresentados foram realizados respeitando o solicitado em Termo de Referência.

GERÊNCIA DE SUPORTE DE REDES, em GOIANIA - GO, aos 08 dias do mês de agosto de 2023.

Documento assinado eletronicamente por **MARCUS PAULO MAGALHAES BARBOSA**, **Gerente**, em 28/08/2023, às 17:31, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **50485543** e o código CRC **0FAECDCB**.