

# CADERNO DE TESTES



## Tracenet IT Solutions

CNPJ/MF: 10.242.293/0001-77

Matriz: Av. Presidente Vargas, 541 – Centro –  
Rio de Janeiro – RJ – CEP: 20071-000

Filial: Av. Santo Amaro, 3432 Cj 35 – Santo  
Amaro – São Paulo – SP – CEP 04556-300

Tels. +55 21 2223-1412 / 11 2306-2122

Contato: Francesco Pollola – Diretor Executivo

<http://www.tracenetsolutions.com>

[comercial@tracenetsolutions.com](mailto:comercial@tracenetsolutions.com)

**PREGÃO ELETRÔNICO Nº 05/2017**

**PROCESSO Nº 04300.0204177/2015-44**

**UASG: 201057 - CENTRAL DE COMPRAS**

**LOTE 5 – FIREWALL MULTIFUNCIONAL**

AO MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
CENTRAL DE COMPRAS

## CADERNO DE TESTES

### TESTES DE CONFORMIDADE CONFORME ANEXO E

### LOTE 5 FIREWALL MULTIFUNCIONAL

# CADERNO DE TESTES

Prezados Senhores,

Apresentamos a V.S<sup>a</sup>, nosso Caderno de Testes para o Lote 5 – Firewall Multifuncional, conforme exigido no item 16.11 seguido padrão exigido no Anexo E

## TESTES DE CONFORMIDADE

### 1 - Definição

O teste de conformidade da amostra visa à aferição da real capacidade técnica dos equipamentos ofertados pela Tracenet . Busca-se comprovar, juntamente com a documentação do fabricante, que os equipamentos de fato atendem aos requisitos constantes da especificação técnica do Anexo B. Nesse sentido, os testes serão efetuados em todos os itens de hardware e software da solução do Lote 5.

### 2. Disposições gerais

**2.1.** O Teste de Conformidade será realizado em laboratório a ser disponibilizado pelo Ministério do Planejamento na cidade de Brasília-DF ou em local indicado pelo grupo técnico de apoio ao pregoeiro, na cidade de Brasília-DF.

**2.8.** A amostra que será utilizada na execução do Teste de Conformidade deverá ser disponibilizada no laboratório em que se realizarão os testes no prazo de até 30 dias corridos, contados a partir da solicitação do pregoeiro.

**2.12.** O Teste de Conformidade será executado em dia útil, de segunda-feira à sexta-feira, das 08:00 horas às 18:00 horas, com previsão de até 2 horas de almoço.

**2.13.** Segue indicação da Tracenet sobre a composição da equipe Técnica da Tracenet junto com fabricante e representante da solução de gerador de tráfego:

- Bruno Guedes - Tracenet
- Felipe Pollola - Tracenet
- Francesco Pollola - Tracenet
- Yan Zhou - Hillstone
- Romulo Melo - IXIA

**2.17.** Ficaremos à disposição para que 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, possa 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.

**2.20 .** A Tracenet proverá integralmente, às suas custas, toda a infraestrutura necessária (equipamentos e cabos de conectividade de rede, equipamentos de geração de tráfego e ameaças, *appliances*, servidores de virtualização, desktops, todos os *softwares* e licenças de utilização, etc.) para a completa instalação e execução do Teste de Conformidade.

**2.22.** A solução ofertada, bem como os demais equipamentos necessários à execução do Teste de Conformidade serão instalados, configurados, operados e acessados pela Equipe Técnica da Tracenet, sempre acompanhada e supervisionada pelo grupo técnico de apoio ao pregoeiro.

**2.23.** Não caberá ao Ministério do Planejamento, Desenvolvimento e Gestão, sob nenhuma hipótese, o pagamento de nenhum tipo de indenização, em virtude da realização do Teste de Conformidade, seja a solução ofertada aprovada ou reprovada.

**2.24.** A Tracenet disponibilizará em até 5 dias úteis contados da data da finalização dos testes o

# CADERNO DE TESTES

Relatório dos Testes da Amostra, o qual deverá conter todas as informações e resultados apurados durante os testes.

**2.25.** No Relatório dos Testes de Amostra constará, no mínimo: informações da topologia do ambiente de teste utilizado, arquivos, impressões de telas, scripts de configuração, versões de software utilizadas e registros de logs com evidências capturadas e quaisquer informações que a equipe de apoio ao pregoeiro ache pertinente, seguindo a estrutura estabelecida no Caderno de Teste.

O relatório será fornecido de maneira impressa e digital, com a mesma sequência do Caderno de Teste as respectivas comprovações e ou evidências.

**2.28.1.** Caso a Tracenet seja convocada para Testes Complementares de Amostra, será disponibilizado em até 3 dias úteis contados da data da finalização dos testes complementares o Relatório dos Testes Complementares da Amostra, o qual conterá todas as informações e resultados, apurados durante os testes.

## 3. Amostra

**3.1.** Para o Teste de Conformidade, a Tracenet apresentará uma AMOSTRA da solução ofertada no Grupo 5, composta por:

### MODELOS

- (i) 1 (um) equipamento firewall multifuncional; (SG-6000-T5860)
- (ii) 1 (uma) solução de gerenciamento centralizado; (HSM-200)
- (iii) demais equipamentos que compõem a solução apresentada na proposta; Servidores de Geração de Tráfego IXIA IxChariot e Ixia BreakingPoint
- (iv) todas as licenças e softwares necessários ao funcionamento da solução;
- (v) cabos, conectores, kits de fixação, trilhos, fibras óticas, patchcords, transceivers e demais acessórios necessários à sua instalação e operação.

**3.2.** A solução de gerenciamento centralizado será instalada, executada e acessada em equipamentos providos pela própria Tracenet (servidor de virtualização, desktops, notebooks, etc.)

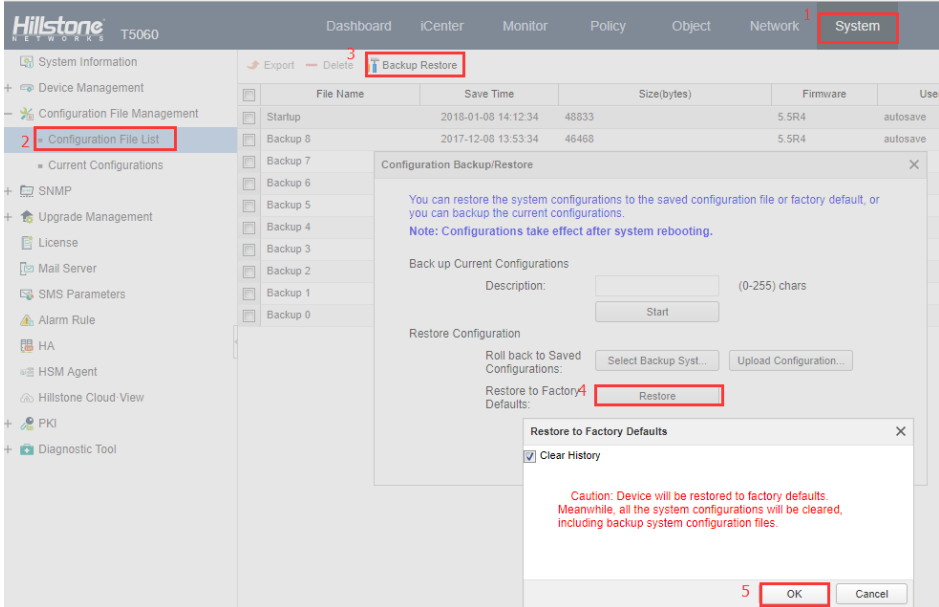
**3.3.** Todos os equipamentos e produtos que compõe a amostra da solução ofertada estarão acompanhados de seus respectivos programas, CDs, manuais, guias de instalação e demais documentos necessários para dirimir quaisquer dúvidas, a fim de que possam ser realizados procedimentos de verificação de conformidade com as especificações técnicas.

## 4. Preparação Inicial

**4.1.** Todos os componentes da solução ofertada serão, antes de iniciado o Teste de Conformidade, submetidos a procedimento de limpeza e exclusão dos dados de forma a zerar quaisquer configurações.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Limpeza e exclusão de dados   |
| <b>Objetivo do Teste</b>     | Limpar e excluir dados de forma a zerar quaisquer configurações.  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br><br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | C LI:<br>1. Faça o login no dispositivo via SSH.  |

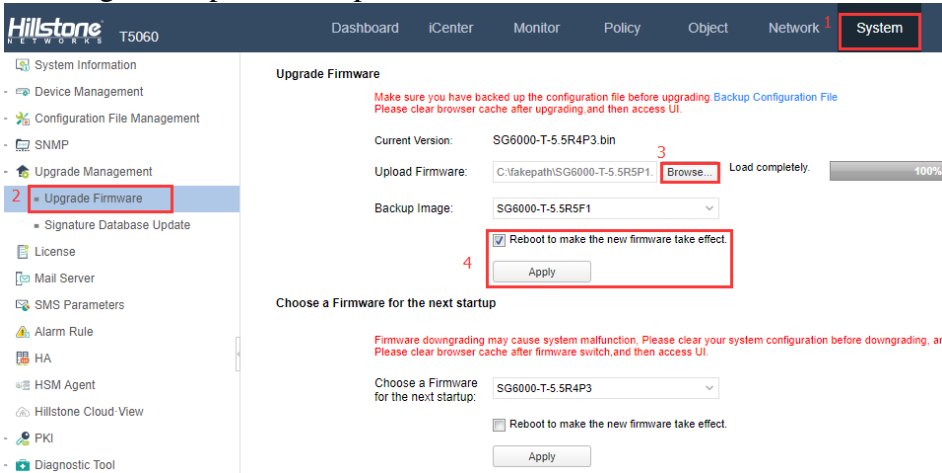
## CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              | <p>2. Siga as etapas abaixo para redefinir o dispositivo para o padrão de fábrica:</p> <p>SG-6000 # unset all</p> <p>a. Remover todas as configurações</p> <p>b. Remover todos os dados de configuração e histórico</p> <p>c. Exit</p> <p>Remova toda a configuração (de volta ao padrão de fábrica), você tem certeza? [a] / b / c: b</p> <p>Notificação: você deve reiniciar o sistema para remover todos os efeitos imediatamente</p> <p>Reinicialização do sistema, você tem certeza? [y] / n: y</p> <p>WebUI:</p> <ol style="list-style-type: none"> <li>1. Faça o login no dispositivo via HTTP / HTTPS</li> <li>2. Siga as etapas abaixo para restaurar o dispositivo</li> </ol>  |
| <b>Resultado esperado</b>    | Todos os dados de configuração e históricos serão removidos após a reinicialização.   |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

**4.2.** A solução ofertada será então atualizada para a versão mais recente de *firmware*, *software*, listas de assinaturas e afins, disponíveis pelos canais oficiais de suporte técnico do fabricante da solução com mais de 3 meses de liberação.

|                          |   |
|--------------------------|---|
| <b>Item Testado</b>      | Atualização de Firmware                             |
| <b>Objetivo do Teste</b> | Realizar a atualização para o firmware mais recente |

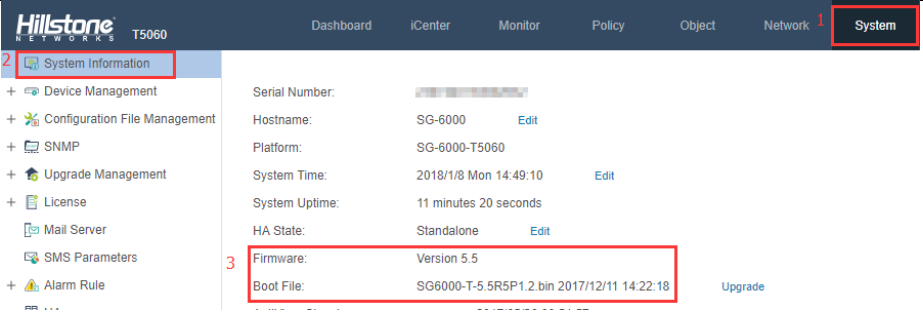
## CADERNO DE TESTES

|                              |   |
|------------------------------|---|
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <ul style="list-style-type: none"> <li>- conforme topologia no item 5.1.6</li> </ul> <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol>  |
| <b>Procedimento de Teste</b> | <ol style="list-style-type: none"> <li>1. Carregar para baixo o mais recente firmware para o seu desktop PC</li> <li>2. Faça login no dispositivo WebUI</li> <li>3. Siga as etapas abaixo para atualizar o firmware</li> </ol>  |
| <b>Resultado esperado</b>    | Após a reinicialização, o dispositivo será atualizado para a versão mais recente do firmware  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

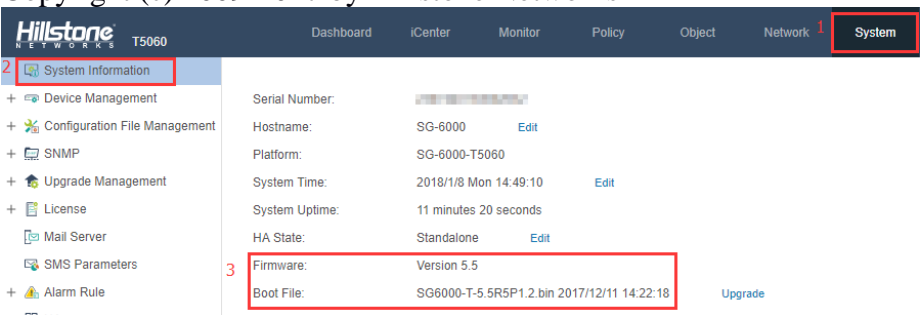
**4.3.** A versão utilizada do *firmware* terá a comprovação de sua integridade realizada por meio da comparação dos *hashes* da versão de firmware utilizada nos testes e a disponibilizada no sítio oficial do fabricante.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Versão atualizada do firmware  |
| <b>Objetivo do Teste</b>     | Verificar se firmware foi atualizado para versão mais recente  |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <ul style="list-style-type: none"> <li>- conforme topologia no item 5.1.6</li> </ul> <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol> |
| <b>Procedimento de Teste</b> | <p>Siga as etapas abaixo para verificar as informações da firmware do dispositivo:</p> <p>Use abaixo o comando para verificar a versão do firmware:</p> <pre>SG-6000 # show version</pre> <p>Software Hillstone Stone Stone, versão 5.5</p> <p>Copyright (c) 2009-2017 by Hillstone Networks</p>                 |

# CADERNO DE TESTES

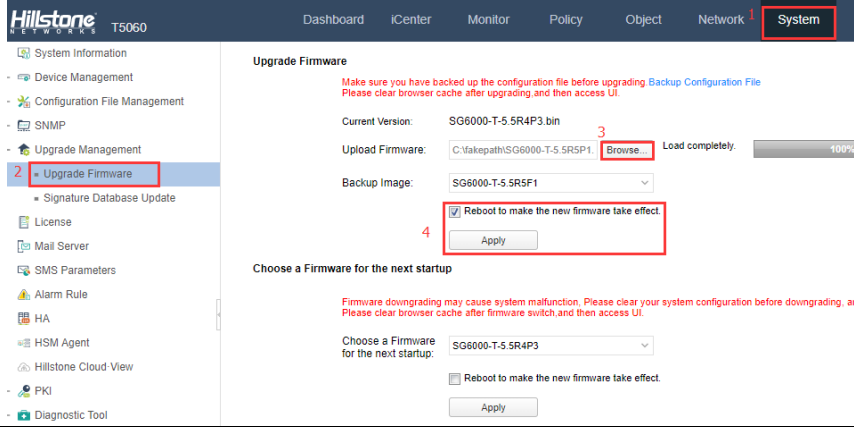
|                              |  |
|------------------------------|--|
|                              |  <p>O arquivo de inicialização é SG6000-T-5.5R5P1.2.bin de flash<br/>Construído por buildmaster8 2017/12/11 14:22:18</p> |
| <b>Resultado esperado</b>    | O firmware da versão usado no dispositivo é consistente comparando com o site oficial.   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

## 4.3.1. Não serão instalados firmwares pré-instalados.

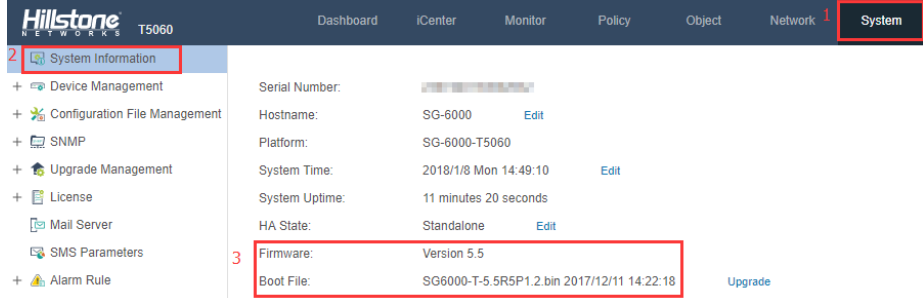
|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Versão de firmware  |
| <b>Objetivo do Teste</b>     | Demonstrar que não foi pré-instalado versão de firmware anterior  |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <p>- conforme topologia no item 5.1.6</p> <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol>   |
| <b>Procedimento de Teste</b> | <p>O mesmo que 4.3 verifica a informação do firmware.</p> <p>Use abaixo o comando para verificar a versão do firmware:</p> <pre>SG-6000 # show version</pre> <p>Software Hillstone Stone Stone, versão 5.5<br/>Copyright (c) 2009-2017 by Hillstone Networks</p>  <p>O arquivo de inicialização é SG6000-T-5.5R5P1.2.bin de flash<br/>Construído por buildmaster8 2017/12/11 14:22:18</p> |
| <b>Resultado esperado</b>    | Sem firmware pré-instalado no dispositivo   |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

## CADERNO DE TESTES

**4.3.2.** Serão ser aplicadas todas as correções, *patches*, *fixes* e afins recomendados pelo fabricante da solução em seus canais oficiais de suporte técnico.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Aplicar correções e atualizações  |
| <b>Objetivo do Teste</b>     | Atualizar o equipamento com todas atualizações, patches e fixes   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | Mesmo procedimento que 4.2, aplicar atualizações, patches e fixes:<br>  |
| <b>Resultado esperado</b>    | Atualizar o equipamento com correções de patches e fixes  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

**4.3.3.** Não serão fornecidos versões, correções ou afins em estágios de testes (versões alfa e beta, *release candidates*, *early availability*, etc.).

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Versão de firmware   |
| <b>Objetivo do Teste</b>     | Demonstrar que não existe versão beta instalada  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.  |
| <b>Procedimento de Teste</b> | O mesmo que 4.3 verifica a informação do firmware.<br>Use abaixo o comando para verificar a versão do firmware:<br>SG-6000 # show version<br>Software Hillstone Stone Stone, versão 5.5<br>Copyright (c) 2009-2017 by Hillstone Networks<br> |

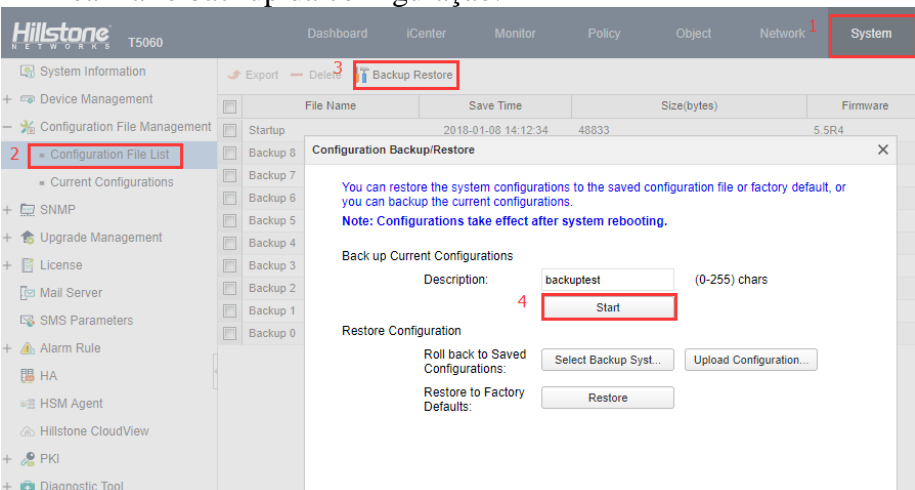
## CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              | O arquivo de inicialização é SG6000-T-5.5R5P1.2.bin de flash<br>Construído por buildmaster8 2017/12/11 14:22:18 |
| <b>Resultado esperado</b>    | Sem firmware beta pré-instalado no dispositivo  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

4.4. Toda configuração da amostra será feita item a item, em linha de comando ou interface gráfica, de forma que se permita o acompanhamento inequívoco por parte da equipe técnica.

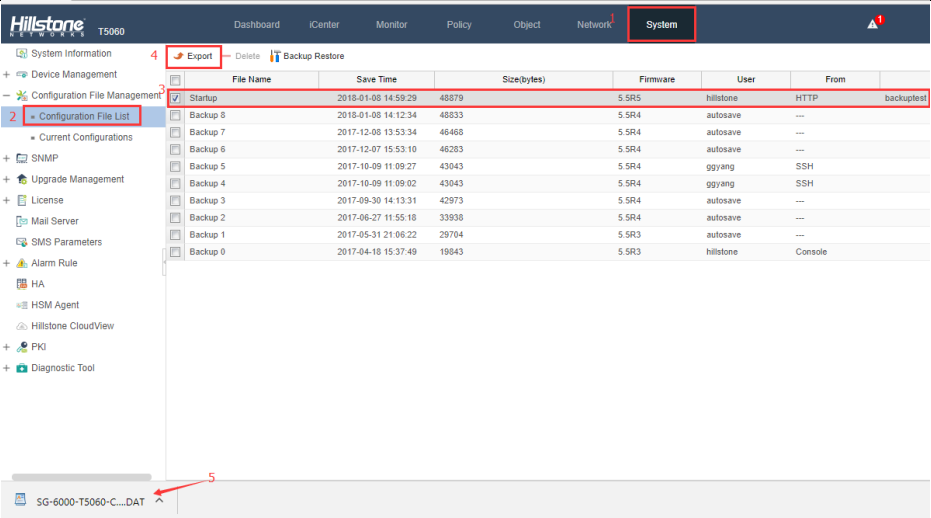
| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

4.5. Ao final de todo o procedimento de configuração inicial será realizado backup em DVD ou pendrive ou drive externo com a geração de *hash* do(s) arquivo(s), sendo uma cópia entregue ao grupo técnico de apoio ao pregoeiro. Este *backup* poderá ser restaurado no início de cada teste para agilizar os procedimentos.

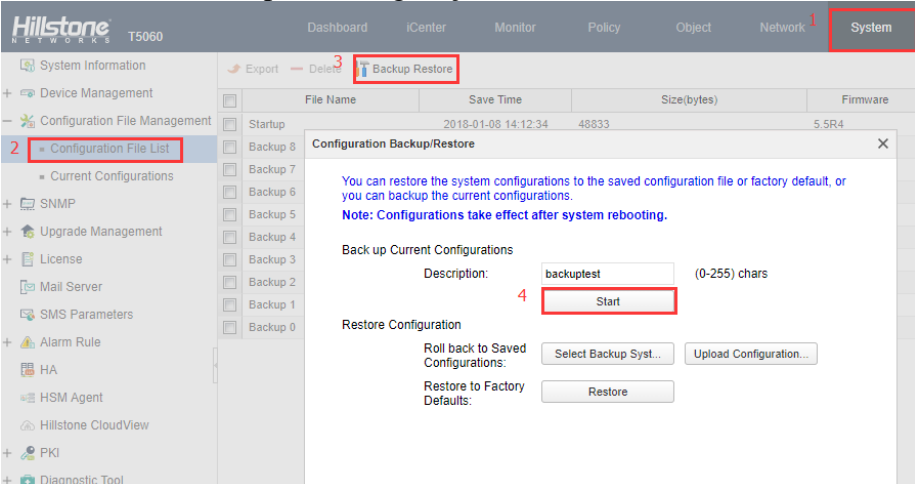
|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Backup das configurações  |
| <b>Objetivo do Teste</b>     | Realizar o backup das configurações realizadas para mídia externa   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | <p>1. Realizar o backup da configuração:</p>  <p>2. Exportar as configurações salvas para o computador:</p>   |



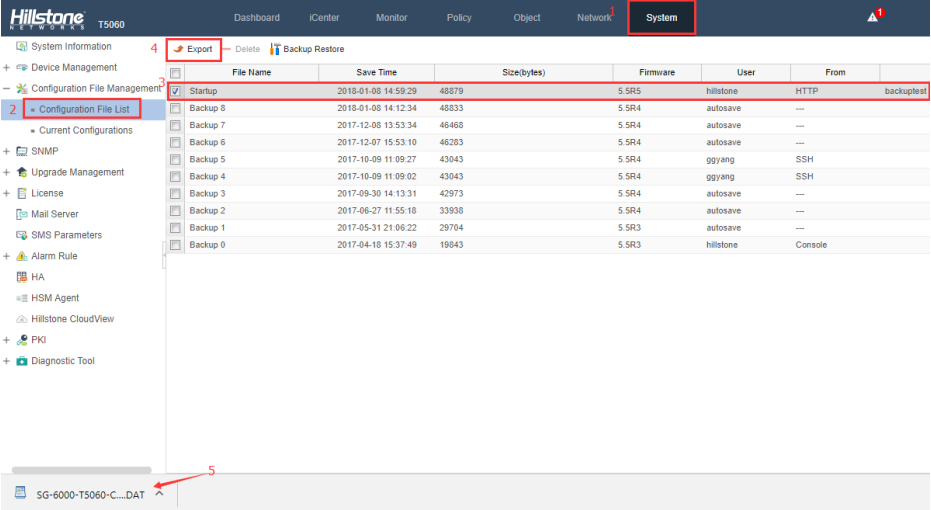
# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              |  <p>3 - Salvar o arquivo de configurações para pendrive ou CD</p> |
| <b>Resultado esperado</b>    | A configuração será exportada para mídia externa  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

4.6 . Uma vez que a solução ofertada tenha sido atualizada na forma do item 4.5, não será mais permitida nenhuma atualização adicional durante a execução de todo o Teste de conformidade.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Backup das configurações   |
| <b>Objetivo do Teste</b>     | Realizar o backup das configurações realizadas para mídia externa  |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <p>- conforme topologia no item 5.1.6</p> <p>Pré-condições:</p> <p>1) Todos os dispositivos funcionam normalmente.</p> <p>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</p> |
| <b>Procedimento de Teste</b> | <p>3. Realizar o backup da configuração:</p>  <p>4. Exportar as configurações salvas para o computador:</p>                          |

# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              |  <p>3 - Salvar o arquivo de configurações para pendrive ou CD</p> |
| <b>Resultado esperado</b>    | A configuração será exportada para mídia externa  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

**4.7.** A Tracenet providenciará equipamentos especializados de geração de tráfego e ameaças, observado, ou seja, sem custos adicionais aos ofertados.

**4.8.** O conjunto de equipamentos especializados de geração de tráfego e ameaças, a ser utilizado no testes em comento, será capaz de gerar, no mínimo, 100 (cem) aplicações e 5.000 (cinco mil) ameaças ou ataques de tipos variados, *stateful* e *stateless*, encapsuladas em protocolos diversos, incluindo HTTP, HTTPS, protocolos de e-mail, vídeo conferência, VoIP, FTP, VPN e métodos de ofuscação.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**4.9** Antes da execução dos testes, será realizada uma aferição do gerador de tráfego da seguinte forma: as portas geradoras e receptoras deverão estar em *loop*, no qual serão gerados os tráfegos com os respectivos percentuais solicitados, bem como as ameaças. A mesma quantidade de tráfego, com as mesmas características, serão então, equivalentes entre as portas geradoras e receptoras. A documentação do processo gerará, como insumos, arquivos do tipo PCAP, estatísticas do gerador ou similares.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**4.10.** A aferição de *throughput* de tráfego durante os testes terá por base os dados gerados e obtidos pelo gerador de tráfego.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

## 5. Teste de Conformidade

(i) Configurações de Testes e Topologia: tem como objetivo, definir um catálogo de configurações da amostra, a topologia e o tráfego para os testes. Os itens desse catálogo serão demandados no início de cada teste.

# CADERNO DE TESTES

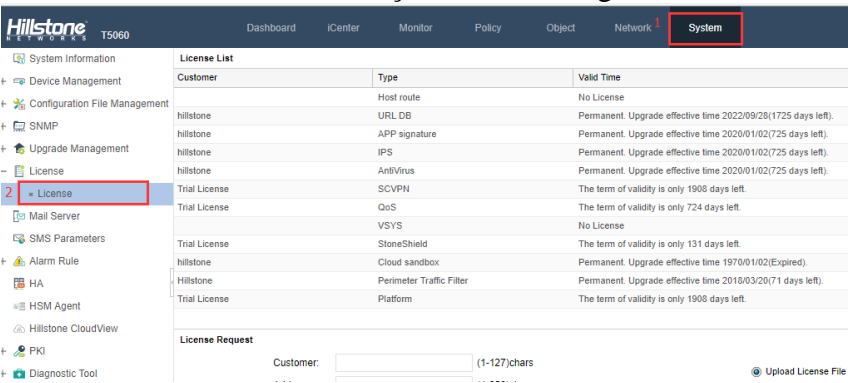
(ii) Teste de assertividade: tem como objetivo, mensurar a eficácia das funcionalidades da amostra, em relação às categorizações, os bloqueios e às detecções de ameaças, ataques, URLs e aplicações.

(iii) Teste de desempenho: tem como objetivo, mesurar o desempenho da amostra em consonância com os requisitos técnicos exigidos no Anexo “B” do Termo de Referência, em relação à taxa de transferência (*throughput*) e performance.

(iv) Teste de sessões: tem como objetivo, mensurar o desempenho da amostra em consonância com os requisitos técnicos exigidos no anexo “B” do TR, em relação às novas sessões por segundo e sessões simultâneas.

## 5.1. Configurações de Testes e Topologia

5.1.1. A amostra será configurada com as funcionalidades de *firewall*, tal como previstas na especificação técnica do Anexo B do TR, 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.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Ativar funcionalidades do Firewall para IDS, IPS, geolocalização, filtro URL, Antivírus e anti-malware, QoS, descriptografia, inspeção SSL e VPN IPSec  |
| <b>Objetivo do Teste</b>     | Comprovar que todas funcionalidades foram habilitadas no equipamento  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.   |
| <b>Procedimento de Teste</b> | <ol style="list-style-type: none"> <li>1. Instalar todas as licenças requeridas</li> <li>2. Verificar o status das licenças na interface gráfica:</li> </ol>  |
| <b>Resultado esperado</b>    | Instalação de todas licenças e habilitação de todas funcionalidades   |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

5.1.1.1. 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.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

## CADERNO DE TESTES

**5.1.2.** A amostra será configurada com seus módulos de sistema de detecção/prevenção à intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e *Anti-malware*) e controle de acesso (controle de aplicações e filtragem de URL's) habilitados pelo fabricante para ambientes empresariais ou *enterprise* em modo de detecção. Sendo submetida a:

- (i) ataques de, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS;
- (ii) ameaças de, no mínimo 2.000 (duas mil) assinaturas de *malwares* distintas;
- (iii) acessos de, no mínimo, 5.000 (cinco mil) sites distintos de internet, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias distintas;
- (iv) um mínimo de 100 (cem) aplicações.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Provar que a solução atende aos itens 5.1.2 i ii iii e iv  |
| <b>Objetivo do Teste</b>     | Comprovar que a solução atende na íntegra os itens   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.  |
| <b>Procedimento de Teste</b> | 1. Realize o login por SSH e abra a linha de comando CLI<br>2. Use os commands abaixo para verificar as informações de IPS, AV, URL, APP<br><br>(i)<br>SG-6000# show ips signature info<br>Signature vendor: Hillstone Networks<br>Current version: 2.1.188<br>Release date: 2017-05-17 09:29:39<br>Total signature count: 7824<br>(ii)<br>SG-6000# show av signature info<br>Current version: 2.1.180106<br>Release date: 2018-01-06 00:52:12<br>Total signature count: 3565194<br>(iii)<br>SG-6000# show url-category<br>Total 69 category<br>(iv)<br>SG-6000# show application predefined<br>Total configured: 3427 |
| <b>Resultado esperado</b>    | Demonstração de todas funcionalidades habilitadas conforme itens i, ii, iii e iv   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

# CADERNO DE TESTES

**5.1.2.1.** Os ataques, ameaças, sites e aplicações acima serão previamente apresentados no caderno de teste.

Informamos que a lista de ameaças é superior à 37000 ataques portanto inviável enviar em formato de planilha excel, para tanto, estamos encaminhando junto com o caderno de testes catálogo do fabricante com informações técnicas das ameaças suportadas, nos arquivos com nome:

915-6728-01-S-DS-BreakingPoint.pdf  
915-1602-01-T-DS-IxChariot

Ataques e ameaças suportadas na plataforma de geração de tráfego IXIA:

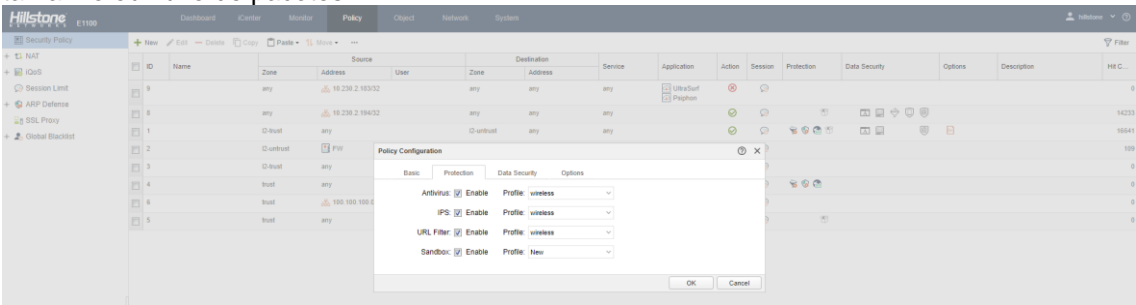
- 37,000+ total attacks
- 7,000+ exploits
- 30,000+ malware
- 100+ evasion classes

Informamos que dentre os mais de 37000 ataques suportados para teste, estarão inclusos também os mandatórios exigidos no item 5.1.2.1:

Youtube, Livestream, Skype, Viber, Whatsapp, Google+, Google Talk, Google Docs, Google Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex, Facebook-chat, Facebookvídeo, 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.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

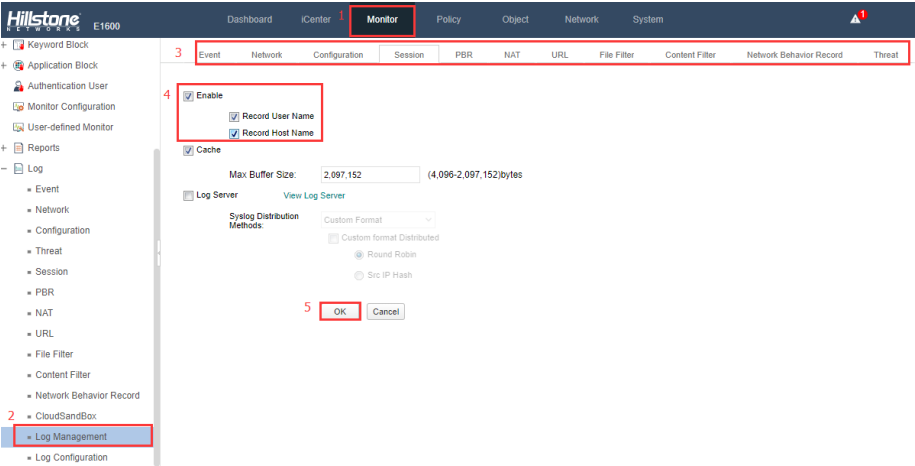
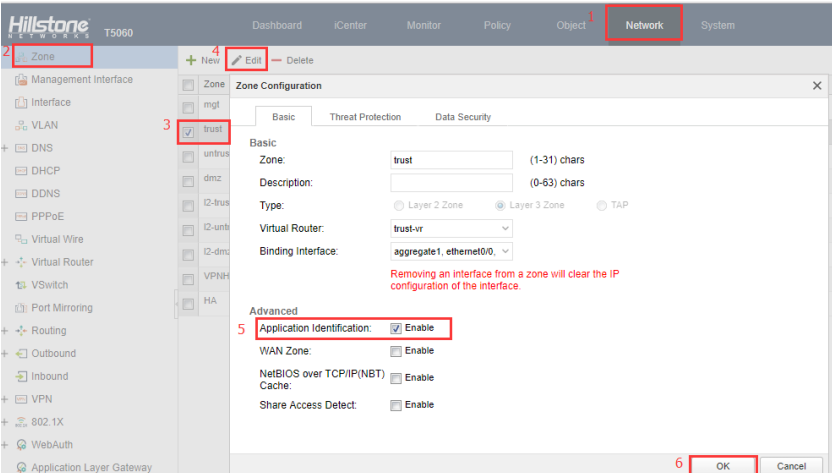
**5.1.3.** A amostra será configurada de forma a realizar a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Inspeção integral de pacotes  |
| <b>Objetivo do Teste</b>     | Demonstrar a inspeção integral dos pacotes independente de tamanho ou fluxo   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.               |
| <b>Procedimento de Teste</b> | Inspeção integral dos pacotes com perfil de proteção vinculado à política, independente de tamanho ou fluxo de pacotes:<br> |
| <b>Resultado esperado</b>    | Demonstração de análise integral de pacotes independente de tamanho, direção ou fluxo   |
| <b>Teste OK</b>              |   |

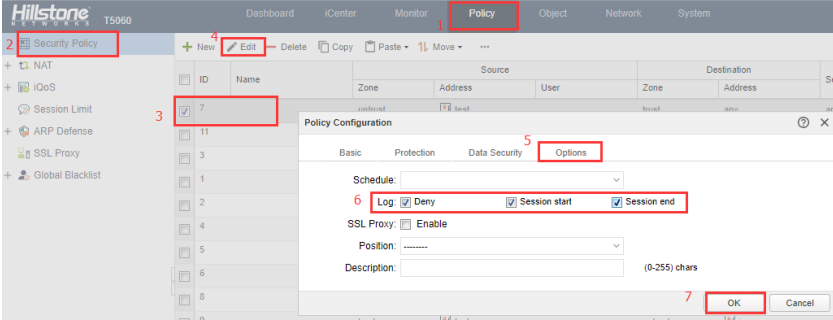
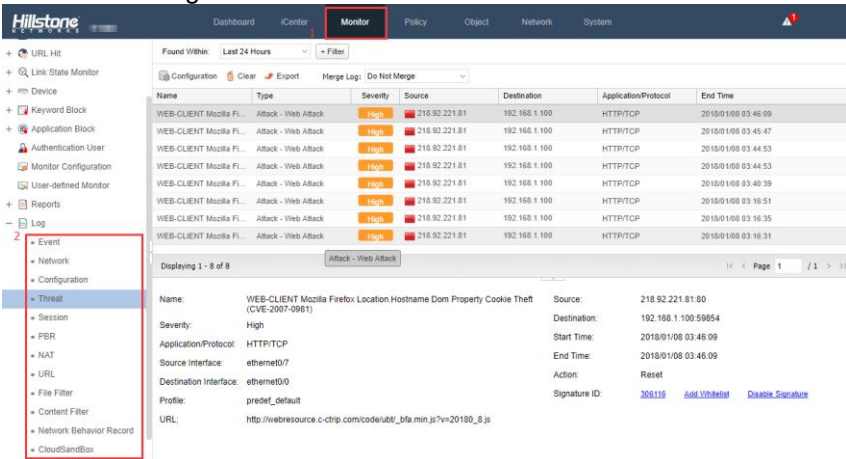
# CADERNO DE TESTES

|                       |  |
|-----------------------|--|
| Teste com Falha       |  |
| Observação            |  |
| Assinatura do cliente |  |
| Assinatura Tracenet   |  |

5.1.4 . A amostra será configurada de forma a registrar todos os tráfegos autorizados ou bloqueados, bem como todas as aplicações e ameaças detectadas pelo *Firewall* Multifuncional.

|                       |  |
|-----------------------|--|
| Item Testado          | Registro de tráfego autorizado ou bloqueado  |
| Objetivo do Teste     | Demonstrar o registro de tráfego autorizado ou bloqueado   |
| Configuração de Teste | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.  |
| Procedimento de Teste | <p>1. Habilite as funções de log correspondentes</p>  <p>2. Ative as funções correspondentes em política ou zona, como proteção contra ameaças, identificação de aplicativos, etc.</p>  |

# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              |  <p>3. Verificar Logs</p>  |
| <b>Resultado esperado</b>    | O FW pode gravar todo o tráfego permitido ou bloqueado, bem como todos os aplicativos e ameaças detectados  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

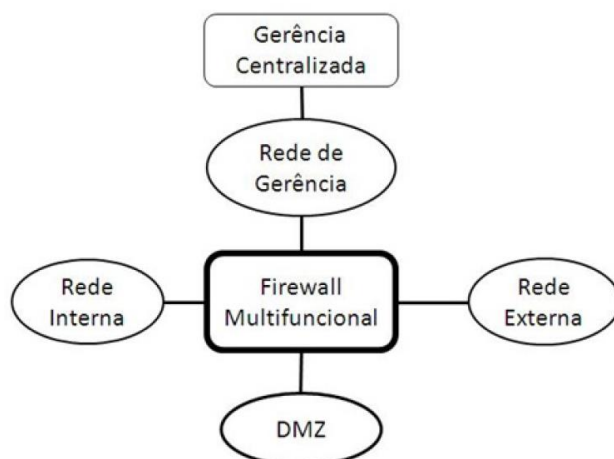
**5.1.5.** Durante a realização dos testes, ficará disponível para avaliação a solução de gerência local e centralizada, que permanecerão acessíveis, possibilitando a modificação e aplicação de políticas de segurança, bem como a visualização dos logs de acesso e de detecção de ameaças e aplicações, por CLI e/ou por GUI (interface gráfica).

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.1.6.** A amostra e demais equipamentos serão instalados e configurados de forma a simular uma arquitetura de rede básica conforme a figura abaixo:

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

## CADERNO DE TESTES



**5.1.7.** O firewall multifuncional e a solução de Gerência Centralizada irão se comunicar por meio de Rede de Gerência dedicada. O Firewall será conectado à Rede de Gerência por meio de interface utilizada para este fim, conforme o item 2.1.45 das especificações técnicas presentes no Anexo B do Termo de Referência.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.1.8.** A Rede Interna possuirá clientes, considerando 1 (um) IP para cada cliente, que acessarão a DMZ e a Rede Externa, a qual será acessada por meio de NAT N-1 a seguir:

v) Lote 5, pelo menos 2.500 clientes.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | NAT N-1 para mais de 2500 clientes   |
| <b>Objetivo do Teste</b>     | Comprovar que a solução comporta mais de 2500 clientes por meio de NAT N-1   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.  |
| <b>Procedimento de Teste</b> | 1. Realize o Login no equipamento por CLI,<br>2. Use o comando abaixo:<br>SG-6000# show capacity all   include scvpn<br>system :scvpn feature 1;<br>scvpn :Max num of scvpn host security check profile 64;<br>scvpn :Max num of scvpn host security check entry 1000;<br>scvpn :Max num of scvpn tunnels 128;<br>scvpn :Limit of scvpn user 10000;<br>scvpn :Max num of scvpn bind table 20000;<br>scvpn :Max Concurrent Users 128; |
| <b>Resultado esperado</b>    | Comprovação que a solução suporta mais de 2500 clientes NAT N-1  |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

**5.1.9.** A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que serão acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores será de:

v) Lote 5, pelo menos 400 servidores.



## CADERNO DE TESTES

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | NAT 1-1 para mais de 400 servidores   |
| <b>Objetivo do Teste</b>     | Comprovar que a solução comporta mais de 400 servidores por NAT 1-1   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.   |
| <b>Procedimento de Teste</b> | 3. Realize o Login no equipamento por CLI,<br>4. Use o comando abaixo:<br>Show capacity all   in dnat<br><br><pre> SG-6000-E1100# show capacity all   in dnat dnat/server          :Max dnat server          512; dnat/server          :Max slb server pool      512; nat/pat              :Max dnat rule entries    128; nat/pat              :Max dnat rule entries of non-root vsys 1024; nat/pat              :Max dnat rule entries of non-root vsys 1024; nat/pat              :Max address used for dnat 16777216; nat/pat              :Max address used for dnat with track 256; SG-6000-E1100# █ </pre> |
| <b>Resultado esperado</b>    | Comprovação que a solução suporta mais de 400 Servidores em NAT 1-1   |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

**5.1.10.** A Rede Externa possuirá clientes, considerando 1 IP para cada cliente, que farão acesso aos servidores da DMZ, e mais servidores, que serão acessados pelos clientes da Rede Interna.

A quantidade de clientes e servidores será de:

v) Lote 5, pelo menos 2.500 clientes e 400 servidores.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | DMZ 2500 clientes e 400 Servidores  |
| <b>Objetivo do Teste</b>     | Comprovar que a solução comporta na DMZ mais de 2500 clientes e mais de 400 servidores  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | 1 - Realize o Login no equipamento por CLI,<br>2 - Use o comando abaixo:<br>Show capacity all   in dnat<br>Show session generic   |

## CADERNO DE TESTES

|                              |  |
|------------------------------|--|
|                              | <pre> SG-6000-E1100# show capacity all   in dnat dnat/server      :Max dnat server      512; dnat/server      :Max slb server pool   512; nat/pat          :Max dnat rule entries 128; nat/pat          :Max dnat rule entries of non-root vsys 1024; nat/pat          :Max dnat rule entries of non-root vsys 1024; nat/pat          :Max address used for dnat 16777216; nat/pat          :Max address used for dnat with track 256; SG-6000-E1100# show sess SG-6000-E1100# show session g SG-6000-E1100# show session generic Device: max 25000, alloc 256, deny session 0, free 24744, tunnel 0, alloc failed 0 SG-6000-E1100# </pre> |
| <b>Resultado esperado</b>    | Comprovação que a solução comporta na DMZ mais de 2500 clientes e mais de 400 servidores   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

**5.1.11.** Cada servidor da Rede Externa e da DMZ corresponderá a pelo menos 1 (uma) regra específica de acesso no Firewall.

No mínimo 60% dos hits devem ocorrer nas últimas regras, baseando-se na análise *top-down*, conforme especificado a seguir:

v) Lote 5, pelo menos 1.000 regras.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Comprovar no mínimo 1000 regras suportadas   |
| <b>Objetivo do Teste</b>     | Demonstrar que a solução suporta mais de 1000 regras   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.              |
| <b>Procedimento de Teste</b> | Abrir a linha de de comando CLI e digitar:<br><br><pre> SG-6000# show capacity all   include policy stateful-firewall :Max policy entries      40000; stateful-firewall :Max policy group entries 1000; </pre> |
| <b>Resultado esperado</b>    | Comprovação que a solução suporta mais de 1000 regras de firewall  |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

**5.1.12.** A amostra será submetida à padrão de tráfego de dados, baseado na metodologia do NSS Labs, estudos de perfil de tráfego de órgãos do SISP, adaptações das RFCs 2544, 3511 e

# CADERNO DE TESTES

diretrizes e políticas de Firewalls do NIST, com a seguinte distribuição média, permitindo-se variações em até 10%:

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**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).

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

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

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

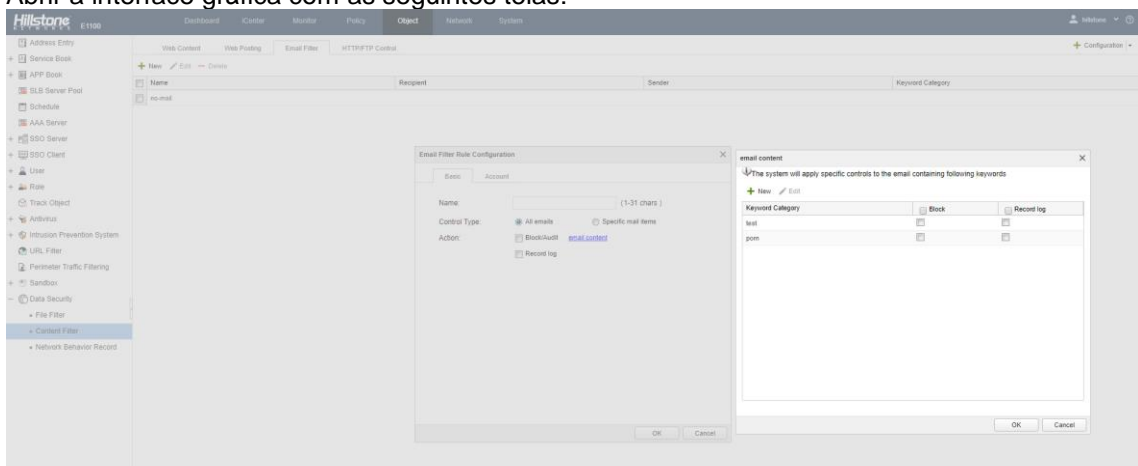
**5.1.12.3. Aplicações, outros ataques, outras ameaças e outros protocolos = 20%** que será acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.1.12.3.1. 5% VPN (PiSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes)**

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

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

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          |   |
| <b>Objetivo do Teste</b>     |   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | <p>Abrir a interface gráfica com as seguintes telas:</p>    |

## CADERNO DE TESTES

|                              |  |
|------------------------------|--|
|                              | <div> <div> <div>Antivirus Rule Configuration</div> <div> <div>Rule Name: <input type="text"/> (1-31) chars</div> <div> <div>File Types:</div> <div> <input checked="" type="checkbox"/> GZIP <input checked="" type="checkbox"/> PE <input type="checkbox"/> RAR <input type="checkbox"/> TAR <input type="checkbox"/> MS OFFICE </div> <div> <input checked="" type="checkbox"/> HTML <input checked="" type="checkbox"/> MAIL <input type="checkbox"/> RIFF <input checked="" type="checkbox"/> ELF <input type="checkbox"/> Raw data </div> <div> <input type="checkbox"/> JPEG <input type="checkbox"/> BZIP2 <input type="checkbox"/> ZIP <input type="checkbox"/> PDF <input type="checkbox"/> Others </div> </div> <div> <div>Protocol Types:</div> <div> <input checked="" type="checkbox"/> HTTP Reset Connection </div> <div> <input checked="" type="checkbox"/> SMTP Log Only </div> <div> <input checked="" type="checkbox"/> POP3 Log Only </div> <div> <input checked="" type="checkbox"/> IMAP4 Log Only </div> <div> <input checked="" type="checkbox"/> FTP Reset Connection </div> </div> </div> <div> <input checked="" type="checkbox"/> Malicious Website Access Control <div>Action: Log Only</div> </div> <div> <input type="checkbox"/> Enable Label E-mail <div>Checked by Hillstone Network AntiVirus (1-128)chars</div> </div> <div> <div>OK</div> <div>Cancel</div> </div> </div> <div> <div>Sandbox</div> <div> <div>Name: <input type="text"/> (1 - 31) chars</div> <div> <div>White list: <input type="checkbox"/> Enable</div> <div>Certificate verify: <input type="checkbox"/> Enable</div> <div> <div>Action:</div> <div> <input checked="" type="radio"/> Log Only <input type="radio"/> Reset </div> </div> <div> <div>File filter</div> <div> <div>File type: <input type="text"/></div> <div> <div>Protocol:</div> <div> <input type="checkbox"/> HTTP Upload </div> <div> <input type="checkbox"/> SMTP Upload </div> <div> <input type="checkbox"/> POP3 Download </div> <div> <input type="checkbox"/> IMAP4 Download </div> <div> <input type="checkbox"/> FTP Upload </div> </div> </div> </div> <div> <div>OK</div> <div>Cancel</div> </div> </div> </div> </div></div> |
| <b>Resultado esperado</b>    | Comprovar que a solução detecta o fluxo de reconhecimento de email   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |

# CADERNO DE TESTES

|                                |  |
|--------------------------------|--|
| <b>Assinatura<br/>Tracenet</b> |  |
|--------------------------------|--|

**5.1.12.3.3.** 5% UDP (distribuição de tamanho: 56% 72 bytes, 17% 512 bytes e 27% 1518 bytes).

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.1.12.3.4.** 4% de aplicações (qualquer protocolo e com tamanho variável).

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.1.12.3.5.** Outros (distribuição de tamanho variável)

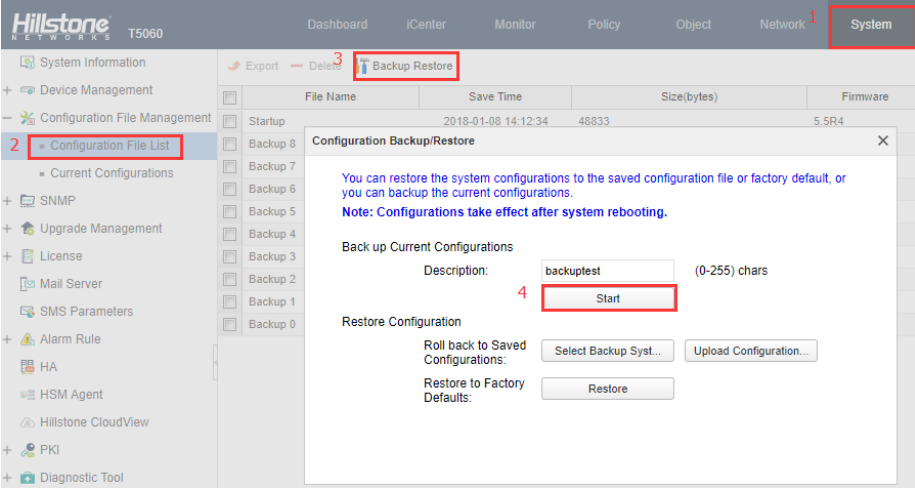
| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

## 5.2. Teste de Assertividade

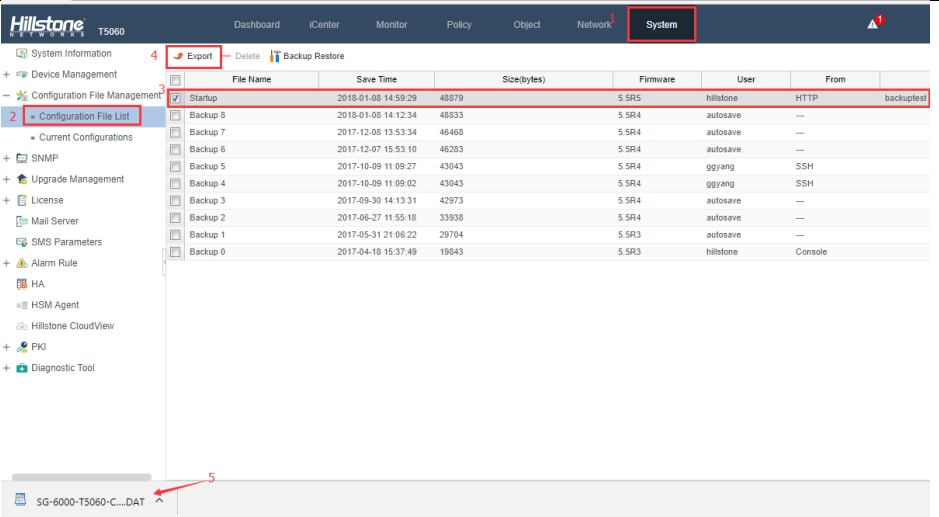
**5.2.1.** Será utilizada a configuração de testes descritos nos itens 5.1.1 a 5.1.5 do Anexo E do TR.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.2.2.** Após as configurações do item acima, será ser realizado o *backup* das configurações da Amostra, sendo calculado seu *hash*.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Backup das configurações e cálculo do hash  |
| <b>Objetivo do Teste</b>     | Realizar o backup das configurações e informação de hash do arquivo   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | <p>5. Realizar o backup da configuração:</p>  <p>6. Exportar as configurações salvas para o computador:</p>   |

# CADERNO DE TESTES

|                              |  |
|------------------------------|--|
|                              |  <p>3 - Salvar o arquivo de configurações para pendrive ou CD</p> <p>4 - rodar o seguinte commando:<br/>SG-6000 # show version</p> <p>Software Hillstone Stone Stone, versão 5.5</p> <p>Copyright (c) 2009-2017 by Hillstone Networks</p> <p>O arquivo de inicialização é SG6000-T-5.5R5P1.2.bin de flash</p> <p>Construído por buildmaster8 2017/12/11 14:22:18</p> |
| <b>Resultado esperado</b>    | A configuração será exportada para mídia externa e hash do arquivo demonstrado   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

5.2.3. Da distribuição do item 5.1.2, o grupo técnico modificará durante os testes, em até 25%, os ataques, ameaças, sites e aplicações apresentados no caderno de teste.

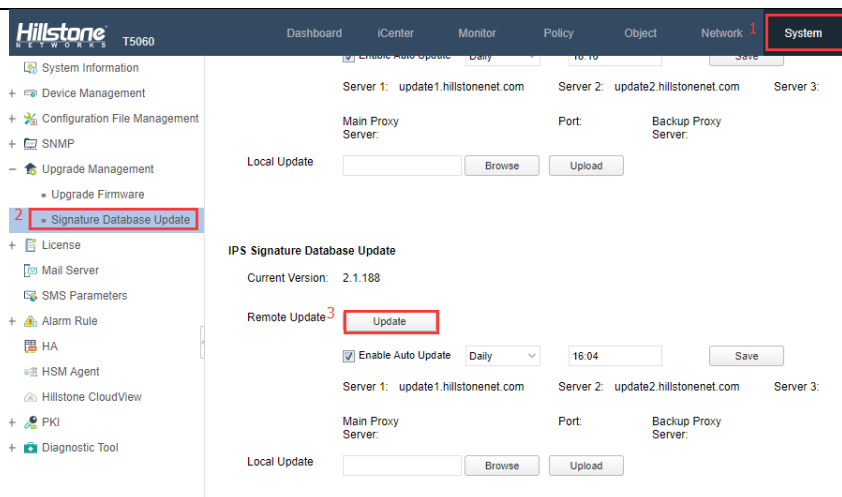
| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

5.2.4. No teste de assertividade, a solução apresentará:

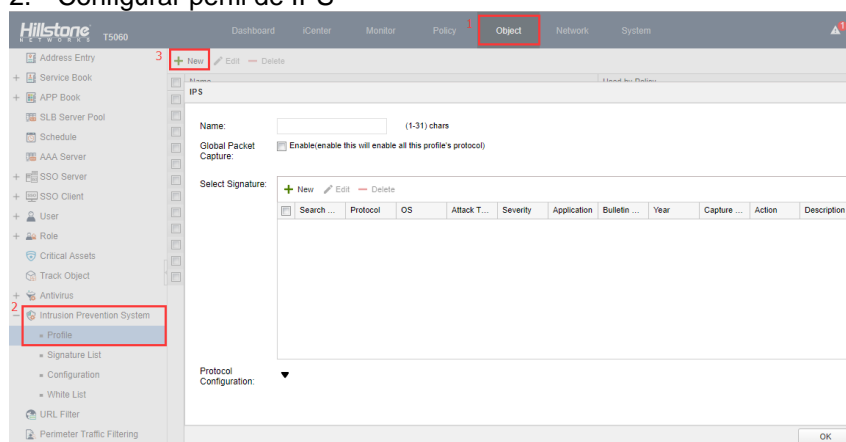
i) Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS;

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | No mínimo 2000 assinaturas distintas de IPS/IDS  |
| <b>Objetivo do Teste</b>     | Demonstrar assertividade da solução para no mínimo 2000 assinaturas IPS e IDS  |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <p>- conforme topologia no item 5.1.6</p> <p>Pré-condições:</p> <p>1) Todos os dispositivos funcionam normalmente.</p> <p>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</p> |
| <b>Procedimento de Teste</b> | 1. Atualiza a assinatura de IPS:   |

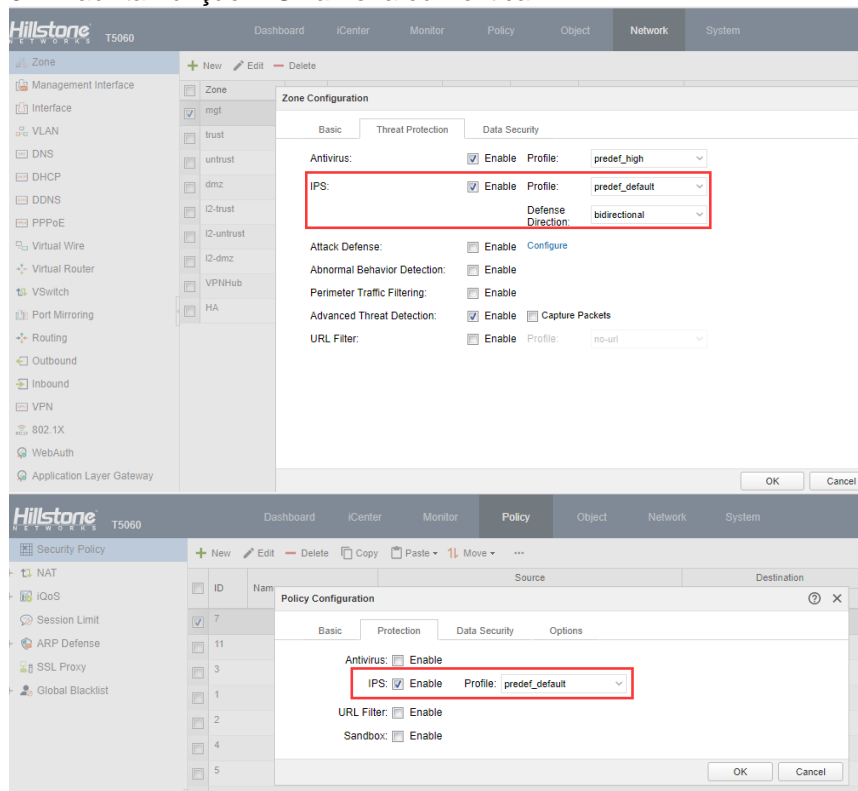
# CADERNO DE TESTES



## 2. Configurar perfil de IPS



## 3. Habilitar função IPS na Zona ou Política

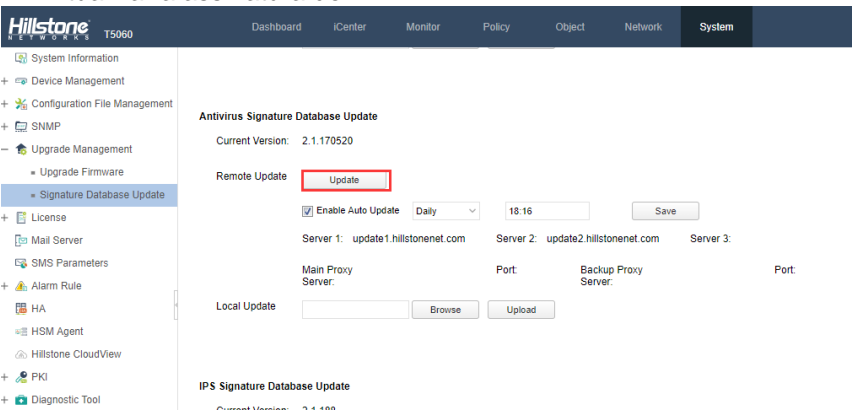
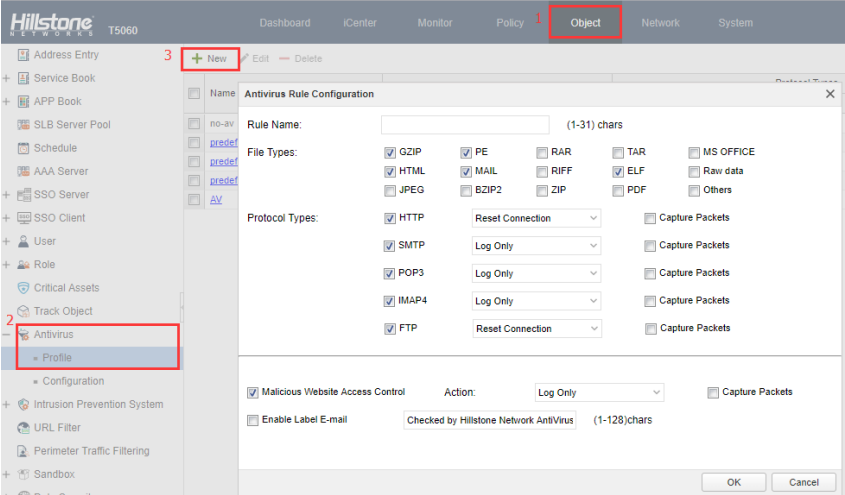


## 4. Testar o resultado

## CADERNO DE TESTES

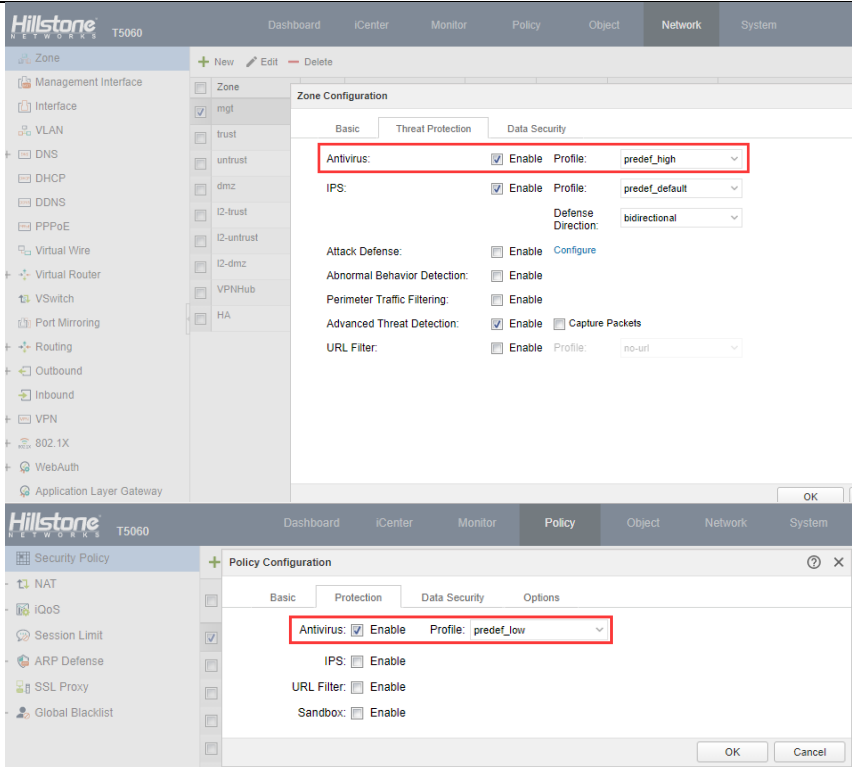
|                              |  |
|------------------------------|--|
| <b>Resultado esperado</b>    | Comprovar que a solução consegue reconhecer ao menos 2000 assinaturas distintas de IPS/IDS |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

ii) Categorizar e bloquear as ameaças em, no mínimo 2.000 (duas mil) assinaturas de *malwares* distintas;

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Categorizar e bloquear no mínimo 2000 assinaturas de malware   |
| <b>Objetivo do Teste</b>     | Comprovar que a solução bloqueia mais de 2000 assinaturas de malware   |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <p>- conforme topologia no item 5.1.6</p> <p>Pré-condições:</p> <p>1) Todos os dispositivos funcionam normalmente.</p> <p>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</p>   |
| <b>Procedimento de Teste</b> | <p>1. Atualizar a assinatura de AV</p>  <p>2. Configure AV profile</p>  <p>3. Habilitar a função AV na Zona ou Política</p> |



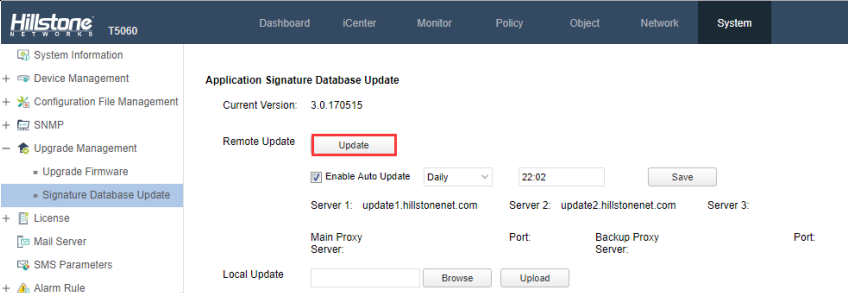
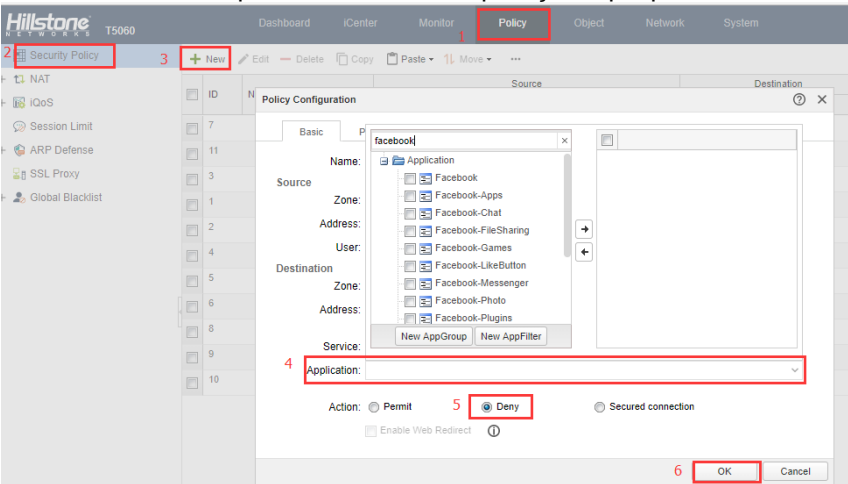
# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              |  <p>4. Testar os resultados</p> |
| <b>Resultado esperado</b>    | Comprovar que a solução consegue reconhecer e bloquear ao menos 2000 assinaturas de malware                       |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

iii) Categorizar e bloquear, pelo menos, 100 (cem) aplicações distintas;

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Categorizar e bloquear pelo menos 100 aplicações distintas  |
| <b>Objetivo do Teste</b>     | Comprovar que a solução bloqueia ao menos 100 aplicações  |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <p>- conforme topologia no item 5.1.6</p> <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol> |
| <b>Procedimento de Teste</b> | 1. Atualize a base de assinaturas de APP  |

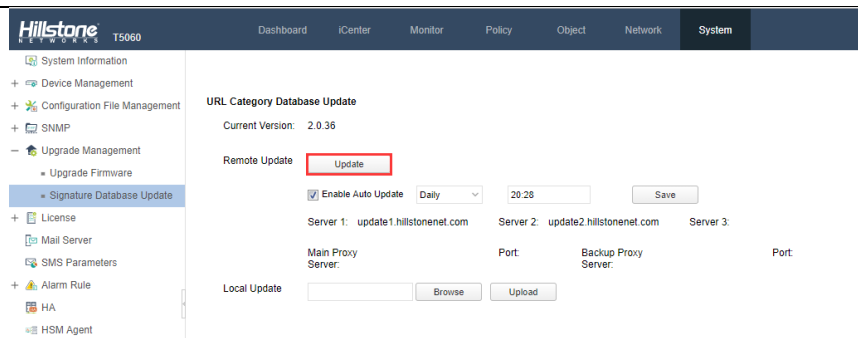
# CADERNO DE TESTES

|                              |  |
|------------------------------|--|
|                              |  <p>2. Criar uma nova política e adicionar aplicações que precisam ser bloqueadas</p>  <p>3. Testar o resultado</p> |
| <b>Resultado esperado</b>    | Comprovar que a solução bloqueia ao menos 100 aplicações   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

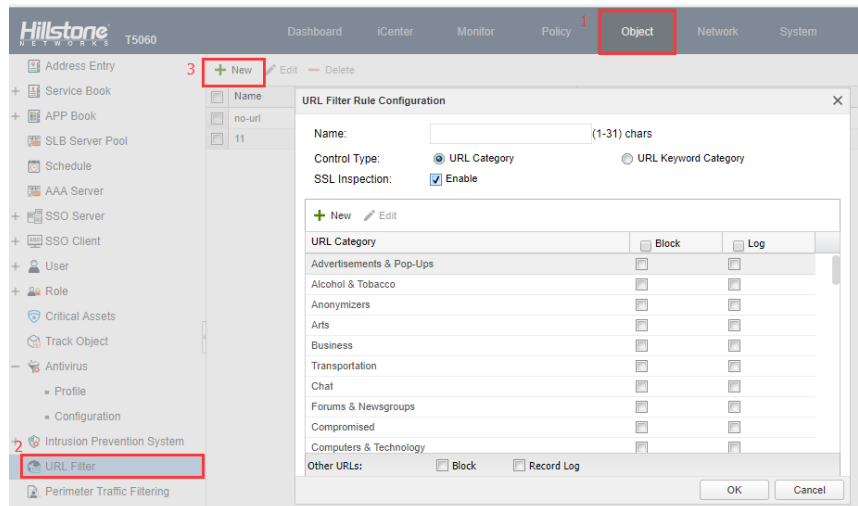
iv) Classificar os acessos em, no mínimo, 5.000 (cinco mil) sites distintos de internet, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias distintas sendo bloqueados 25% deste total escolhidos por categorias específicas definidas pelo grupo técnico de apoio ao pregoeiro no momento do teste.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Classificar no mínimo 5000 sites distintos em 40 categorias   |
| <b>Objetivo do Teste</b>     | Bloquear 25% do total de sites escolhidos por categorias específicas  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | 1. Atualize a base de Sites para a mais atual   |

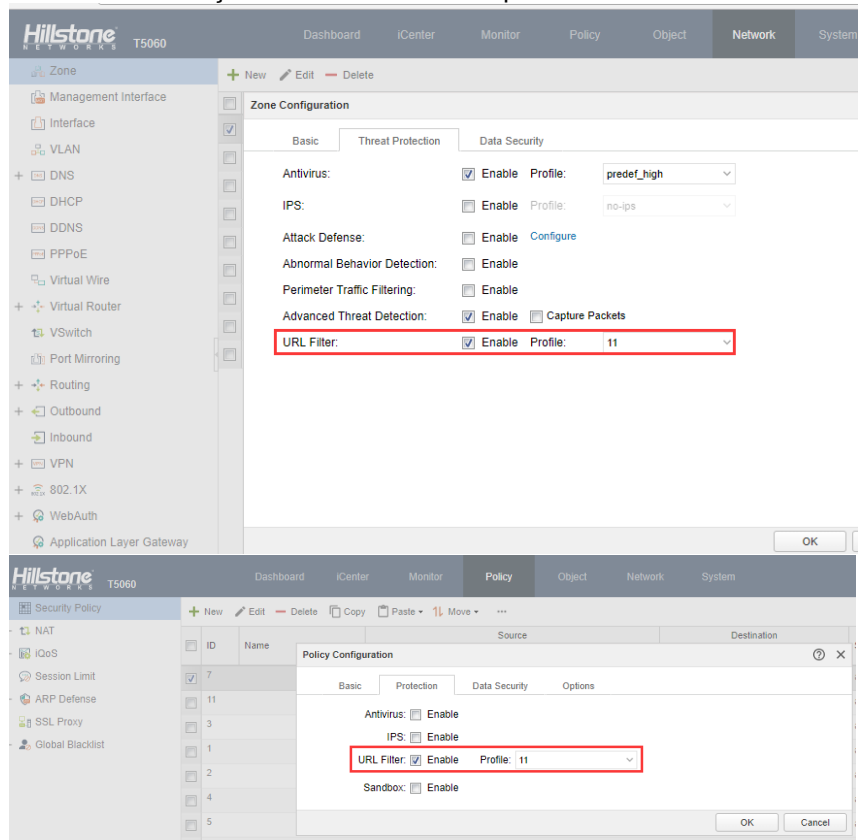
# CADERNO DE TESTES



## 2. Crie um filtro de URL



## 3. Habilite a função de URL na Zona ou política



## 4. Testar o resultado

**Resultado esperado**

Comprovar que a solução consegue categorizar mais de 5000 sites, dividir em ao menos 40 categorias e bloquear ao menos 25%

## CADERNO DE TESTES

|                              |  |
|------------------------------|--|
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

**5.2.5.** Serão coletados parâmetros que indiquem o índice de assertividade das funcionalidades dos lotes descritas nos itens 2.1, 2.3, 2.4, 2.5 e 2.6 do anexo B do TR.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5 . 2 . 5 . 1 .** Serão contabilizados apenas os bloqueios e categorizações de(as) ameaças/ataques/aplicações/URLs corretos(as), devendo, portanto, ser excluídos(as) da contabilização aqueles(as) que correspondem aos falsos positivos (inexistentes, mas bloqueados(as) pela solução) e categorizados como mal formados, não identificados, desconhecidos ou similares.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.2.5.2.** 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.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.2.5.3.** A auditoria da contabilidade será feita por amostragem

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.2.6.** A amostra apresentará no teste de assertividade o valor de acerto de pelo menos 80% para cada funcionalidade testada dos itens 2.1, 2.3, 2.4, 2.5 e 2.6 do anexo B.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5 . 2 . 6 . 1 .** A referida taxa de 80% (oitenta por cento) significa que de cada 100 ameaças/ataques/aplicações/URLs distintas(os) trafegadas através da solução, esta deverá categorizar e bloquear, de forma assertiva, pelo menos 80 deles(as).

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.2.7.** Após a realização do teste de assertividade, o *firewall* da Amostra terá todos os seus contadores zerados e configurações apagadas.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Zerar os contadores e configurações   |
| <b>Objetivo do Teste</b>     | Zerar os contadores e configurações   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | 1. Login via HTTP/HTTPS<br>2. Siga os passos abaixo para restaurar o equipamento  |

# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              |   |
| <b>Resultado esperado</b>    | Todas configurações e histórico serão perdidos após o equipamento ser reiniciado. |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

## 5.3. Teste de Desempenho

5.3.1. Para os testes serão utilizadas todas as configurações de testes e topologia descritas no item 5.1 do Anexo E do TR.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

5.3.2. Será considerado como taxa de transferência (*throughput*) o somatório das interfaces de entrada do gerador de tráfego, após passagem do tráfego no equipamento testado.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

5.3.3. Durante os testes, não será habilitado o modo de conservação, ou desligar funcionalidades automaticamente da amostra.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

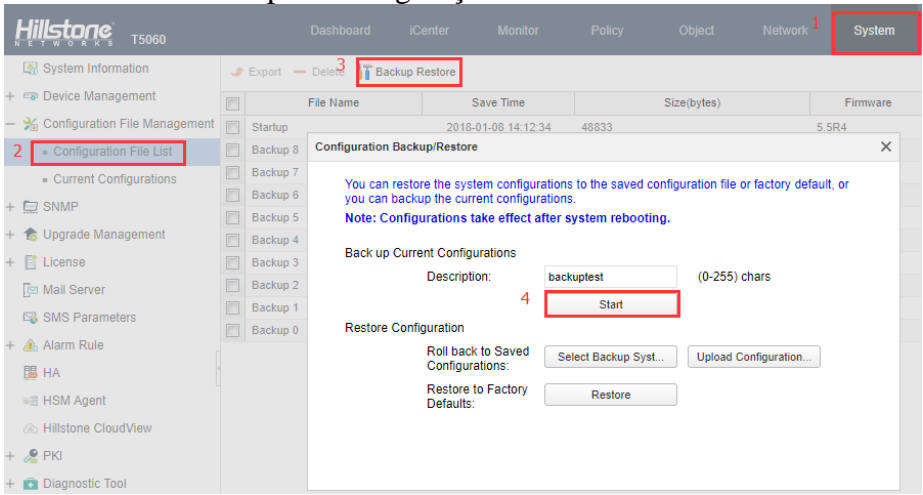
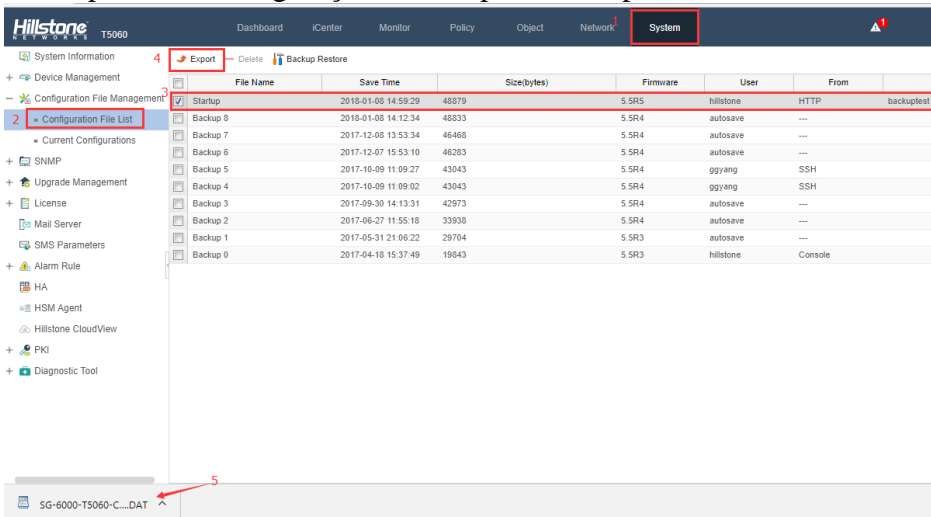
5.3.4. Durante os testes de desempenho minimamente serão gerados(as) as ameaças, ataques, aplicações e URLs, bem como ativadas as assinatura e perfis de antivírus, *anti-malware*, IDS/IPS, aplicações e URLs, em modo de detecção, que foram homologadas no teste de assertividade.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

5.3.5. Após os ajustes para os testes, será realizado o backup das configurações da Amostra, sendo calculado seu *hash*.

|                          |   |
|--------------------------|---|
| <b>Item Testado</b>      | Backup das configurações e cálculo do hash                          |
| <b>Objetivo do Teste</b> | Realizar o backup das configurações e informação de hash do arquivo |

# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <ul style="list-style-type: none"> <li>- conforme topologia no item 5.1.6</li> </ul> <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol>  |
| <b>Procedimento de Teste</b> | <p>7. Realizar o backup da configuração:</p>  <p>8. Exportar as configurações salvas para o computador:</p>  <p>3 - Salvar o arquivo de configurações para pendrive ou CD</p> <p>4 – rodar o seguinte comando:</p> <pre>SG-6000 # show version</pre> <p>Software Hillstone Stone Stone, versão 5.5</p> <p>Copyright (c) 2009-2017 by Hillstone Networks</p> <p>O arquivo de inicialização é SG6000-T-5.5R5P1.2.bin de flash</p> <p>Construído por buildmaster8 2017/12/11 14:22:18</p> |
| <b>Resultado esperado</b>    | <p>A configuração será exportada para mídia externa e hash do arquivo demonstrado</p>   |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

## CADERNO DE TESTES

**5.3.6.** As configurações da Amostra serão as mesmas, tanto para o item 5.3.7 quanto para o item 5.3.8 do Anexo E do TR.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.3.7. Parametrização:** A amostra será inicialmente submetida a uma taxa de transferência do tamanho de 25% do *throughput* do lote, no padrão de tráfego descrito no item 5.1, sendo testado por 30 (trinta) minutos contínuos e ininterruptos com o objetivo de coleta de parâmetros que serão utilizados para verificação da performance do equipamento. A contagem poderá ser iniciada após o período de estabilização do tráfego.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.3.7.1.** Após a realização da parametrização descrita no *caput*, o *firewall* da Amostra terá todos os seus contadores zerados.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Zerar os contadores  |
| <b>Objetivo do Teste</b>     | Contadores serão zerados após execução de comando  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.  |
| <b>Procedimento de Teste</b> | 1 – rodar o seguinte parâmetro da linha de commando CLI<br>SG-6000# clear logging ?<br>anti-defacement Anti-defacement logging messages<br>configuration Configuration logging messages<br>data-security Data-security logging messages<br>debug Debug logging messages<br>event Event logging messages<br>network Network logging messages<br>operation Operation logging messages<br>sandbox Sandbox logging messages<br>statistics Clear current logging statistics<br>threat Threat logging messages<br>traffic Traffic logging messages<br>web-security Web-security logging messages<br>SG-6000# clear logging traffic |
| <b>Resultado esperado</b>    | Todos contadores serão apagados  |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

**5.3.7.2.** Serão coletados os parâmetros que indiquem a taxa de transferência, latência média e variação média de latência (*jitter*) do equipamento, erros absolutos irreversíveis de transações TCP/layer-7 e a detecção de ameaças, aplicações, ataques e URLs;

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

## CADERNO DE TESTES

**5.3.8. Teste:** A amostra será então submetida a uma taxa de transferência de 85% do *throughput* do lote, no padrão de tráfego do item 5.1, sendo testado, por 30 minutos contínuos e ininterruptos e não apresentará prejuízo em sua performance. A contagem poderá ser iniciada após o período de estabilização do tráfego.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.3.8.1.** O Lote 5, deverá ter uma amostra submetida a uma taxa de transferência de 80% do respectivo *throughput*, no padrão de tráfego do item 5.1, sendo testado por 30 minutos contínuos e ininterruptos e não apresentará prejuízo em sua performance. A contagem poderá ser iniciada após o período de estabilização do tráfego.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.3.8.2.** Serão coletados os parâmetros que indiquem a taxa de transferência, latência média e variação média de latência (*jitter*) do equipamento, erros absolutos irrecuperáveis de transações TCP/layer-7 e a detecção de ameaças, aplicações, ataques e URLs;

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.3.8.3.** Serão comparados os parâmetros coletados nos itens 5.3.7.1 e 5.3.8.2, sendo considerado prejuízo na performance do equipamento a ocorrência de quaisquer dos eventos a seguir:

i) Perda absoluta de pacotes superior a 1%.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

ii) Erros absolutos irrecuperáveis de transações TCP/layer-7 superior a 0,5%.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

iii) Valores de latência média ou de variação média de latência (*jitter*) acima de 10 x (vezes) dos valores coletados no item 5.3.2 do Anexo E.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

iv ) A não observância de detecções por amostragem de ameaças, ataques, aplicações e URLs presentes no item 5.2.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.3.8.4.** A amostra não apresentará prejuízos na performance no teste de desempenho, conforme exigido item 5.3.8.3 do Anexo E.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.3.8.5.** Após a realização do teste do item 5.3.2, o firewall da Amostra terá todos os seus contadores zerados e configurações apagadas.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Zerar os contadores e configurações  |
| <b>Objetivo do Teste</b>     | Apagar todos contadores e configurações  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente. |



## CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              | 2) Estabeleça o ambiente de teste de acordo com o diagrama acima.   |
| <b>Procedimento de Teste</b> | 1. Login no equipamento via SSH.<br>2. Rodar os seguintes comandos para apagar o equipamento para configurações de fábrica:<br>SG-6000# unset all<br>a.Remove all configuration<br>b.Remove all configuration and history data<br>c.Exit<br>Remove all the configuration(back to factory default), are you sure?<br>[a]/b/c: b<br>Notification: you must reboot system to take unset all effect immediately<br>System reboot, are you sure? [y]/n:y |
| <b>Resultado esperado</b>    | Apagar os contadores e todas configurações  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

### 5.4. Teste de Sessões

**5.4.1.** Para a mensuração de novas sessões por segundo e sessões simultâneas, a amostra será submetida a dois testes. Esses testes serão realizados na ordem descrita abaixo, devendo ser a amostra aprovada em no mínimo em um deles.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

#### 5.4.2. Primeiro teste

**5.4.2.1.** Para o teste deverá ser utilizada a configuração de testes descritos nos itens 5.1, 5.3.2 a 5.3.5 do Anexo E, sendo a amostra submetida a taxa de *throughput* do item 5.3.8.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.4.2.2.** Mensuração de novas sessões por segundo: para tal aferição, será utilizada a distribuição de tráfego descrita no item 5.1.12 do Anexo E, incluindo tráfego *stateless* UDP e VPN.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.4.2.2.1.** A amostra comprovará no mínimo 50% do número de novas sessões por segundo TCP, que é estabelecido no Anexo B por no mínimo 5 minutos contínuos e ininterruptos.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.4.2.3.** Mensuração de sessões simultâneas: para tal aferição, deverá obrigatoriamente ser utilizada a distribuição de tráfego descrita no item 5.1.12 do Anexo E.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.4.2.3.1.** A amostra apresentará mensuração de novas sessões simultâneas TCP estabelecido no Anexo B, por no mínimo 5 minutos contínuos e ininterruptos.

## CADERNO DE TESTES

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.4.2.4.** A mensuração de novas sessões por segundo e a de sessões simultâneas serão realizadas em momentos distintos.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.4.2.5.** A amostra apresentará no primeiro teste de sessões as mensurações dos itens 5.4.2.2 e 5.4.2.3.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

**5.4.2.6.** Após a realização do teste do item 5.4.2 deste anexo, o firewall da amostra terá todos os seus contadores zerados e configurações apagadas.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Zerar os contadores e configurações   |
| <b>Objetivo do Teste</b>     | Apagar todos contadores e configurações   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.   |
| <b>Procedimento de Teste</b> | 3. Login no equipamento via SSH.<br>4. Rodar os seguintes comandos para apagar o equipamento para configurações de fábrica:<br>SG-6000# unset all<br>a.Remove all configuration<br>b.Remove all configuration and history data<br>c.Exit<br>Remove all the configuration(back to factory default), are you sure?<br>[a]/b/c: b<br>Notification: you must reboot system to take unset all effect immediately<br>System reboot, are you sure? [y]/n:y |
| <b>Resultado esperado</b>    | Apagar os contadores e todas configurações  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

### 5.4.3. Segundo teste

**5.4.3.1.** Mensuração de novas sessões por segundo: para tal aferição, será utilizado tráfego HTTP puro e, no mínimo, objeto de 64 bytes, ativando apenas a funcionalidade de firewall *statefull*, não sendo necessário seguir as especificações do item 5.1 e seus subitens.

|          |                 |            |
|----------|-----------------|------------|
| Teste OK | Teste com falha | Observação |
|          |                 |            |

## CADERNO DE TESTES

**5.4.3.1.1.** A amostra comprovará o número de novas sessões por segundo, que são estabelecidos no Anexo B, por pelo menos, 5 (cinco) minutos contínuos e ininterruptos.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.4.3.2.** Mensuração de sessões simultâneas: para tal aferição, deve ser utilizado tráfego HTTP puro e, no mínimo, objeto de 64 bytes, ativando apenas a funcionalidade de firewall *statefull*, não sendo necessário seguir as especificações do item 5.1 e seus subitens.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.4.3.2.1.** A amostra comprovará o número de sessões simultâneas, que são estabelecidos no Anexo B, por pelo menos, 5 (cinco) minutos contínuos e ininterruptos.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.4.3.3.** As mensurações de novas sessões por segundo e sessões simultâneas serão realizadas em momentos distintos.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

**5.4.3.4.** Para mensurar novas sessões, cada uma será estabelecida, minimamente, por meio de *handshake* de três vias (*three-way handshake*).

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

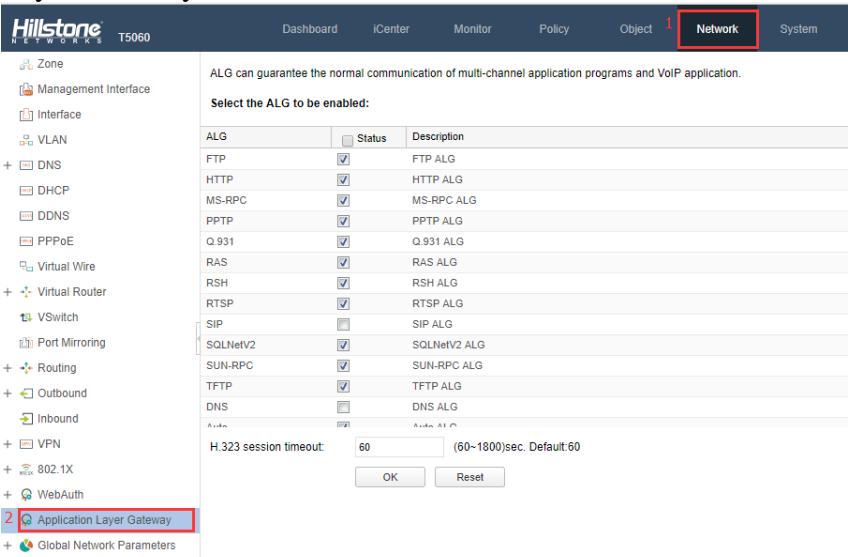
**5.4.3.5.** A amostra apresentará no segundo teste de sessões as mensurações dos itens 5.4.3.1 e 5.4.3.2.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

# CADERNO DE TESTES

## Testes complementares:

i. 2.1.29. Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), H323 e SIP sobre os protocolos IPV4 ou IPV6.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | RTP, H323 e SIP sobre IPV4 e IPV6   |
| <b>Objetivo do Teste</b>     | Comprovar que os protocolos são suportados e possuem proteção   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | <p>Protocolos suportados e protegidos pela camada de ALG, Application Layer Gateway:</p>                       |
| <b>Resultado esperado</b>    | Comprovar que a solução suporta os protocolos e consegue proteger em IPV4 e IPV6  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

ii. 2.3.3. Decodificar múltiplos formatos de Unicode

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Decodificar múltiplos formatos Unicode  |
| <b>Objetivo do Teste</b>     | Comprovar múltiplos formatos de Unicode   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |

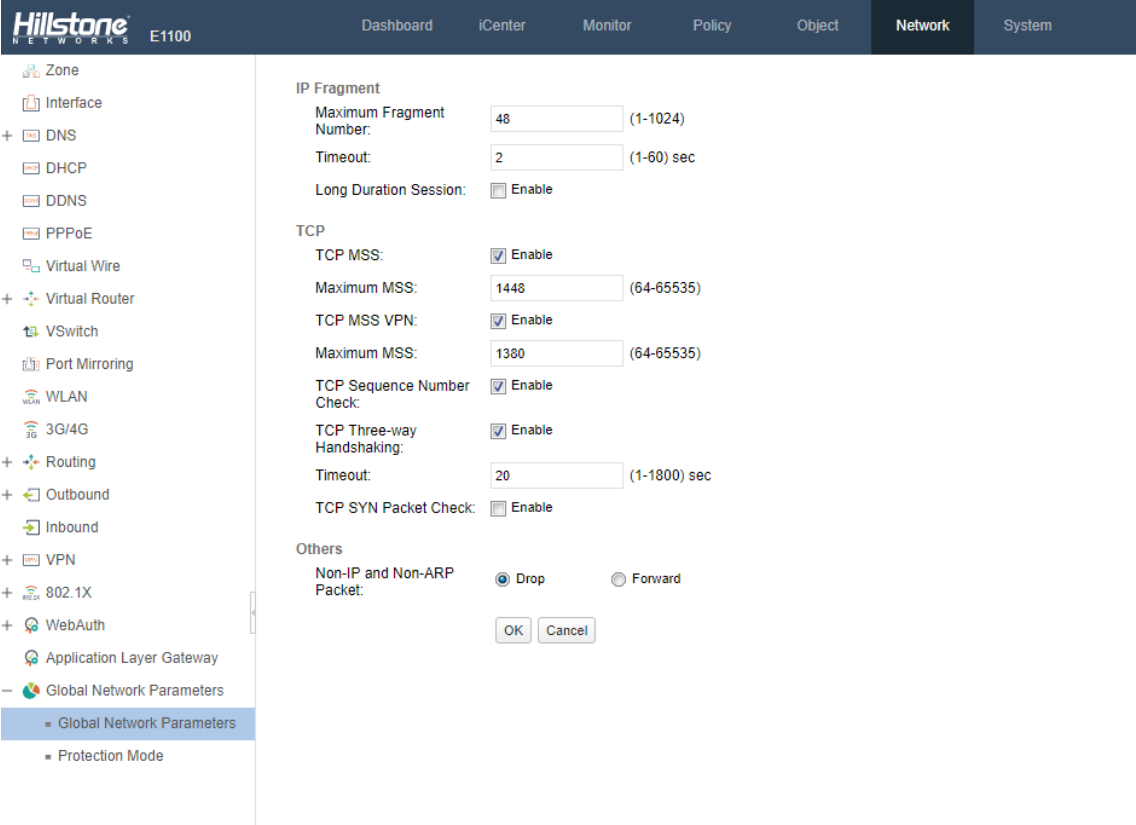
## CADERNO DE TESTES

|                              |  |
|------------------------------|--|
| <b>Procedimento de Teste</b> | <p>Vários formatos podem ser comprovados através de utilização de navegadores com linguagens distintas configuradas (inglês, português, chinês, entre outras), realizando testes em tempo real para prova de múltiplos formatos Unicode.</p> <p>Informações também disponíveis de múltiplos formatos Unicode suportados para proteção em vulnerabilidades Unicode:</p> <p><a href="http://www.hillstonenet.com/support/IPS_Help/en/HTTP/301838.html">http://www.hillstonenet.com/support/IPS_Help/en/HTTP/301838.html</a><br/> <a href="http://www.hillstonenet.com/support/IPS_Help/en/HTTP/301863.html">http://www.hillstonenet.com/support/IPS_Help/en/HTTP/301863.html</a></p> <p><a href="http://www.hillstonenet.com/subscription-security-services/ips-update-service/2_0_19.html">http://www.hillstonenet.com/subscription-security-services/ips-update-service/2_0_19.html</a><br/> <a href="http://www.hillstonenet.com/support/IPS_Help/en/MSSQL/1600035.html">http://www.hillstonenet.com/support/IPS_Help/en/MSSQL/1600035.html</a></p> |
| <b>Resultado esperado</b>    | Comprovar atendimento à múltiplos formatos Unicode   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

### iii. 3.3.4 Suportar fragmentação e desfragmentação IP

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Fragmentação e desfragmentação IP  |
| <b>Objetivo do Teste</b>     | Comprovar que a solução suporta fragmentação e desfragmentação de IP   |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:<br/>         - conforme topologia no item 5.1.6</p> <p>Pré-condições:<br/>         1) Todos os dispositivos funcionam normalmente.<br/>         2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</p> |
| <b>Procedimento de Teste</b> | Tela de comprovação de fragmentação e defragmentação de IP:  |

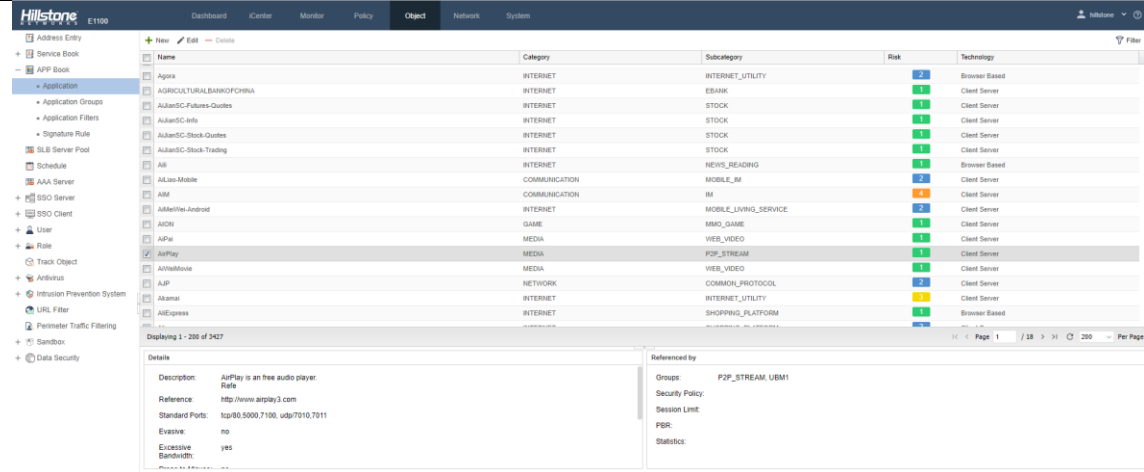
# CADERNO DE TESTES

|                              |  |
|------------------------------|--|
|                              |  <p>The screenshot shows the Hillstone E1100 Network Configuration Interface. The left sidebar contains a tree view with categories like Zone, Interface, DNS, DHCP, DDNS, PPPoE, Virtual Wire, Virtual Router, VSwitch, Port Mirroring, WLAN, 3G/4G, Routing, Outbound, Inbound, VPN, 802.1X, WebAuth, Application Layer Gateway, and Global Network Parameters. The main area displays configuration settings for IP Fragment, TCP, and Others. IP Fragment settings include Maximum Fragment Number (48), Timeout (2), and Long Duration Session (Enable). TCP settings include TCP MSS (Enable), Maximum MSS (1448), TCP MSS VPN (Enable), Maximum MSS (1380), TCP Sequence Number Check (Enable), TCP Three-way Handshaking (Enable), Timeout (20), and TCP SYN Packet Check (Enable). Others settings include Non-IP and Non-ARP Packet (Drop/Forward) and OK/Cancel buttons.</p> |
| <b>Resultado esperado</b>    | Comprovar que a solução suporta fragmentação e defragmentação de IP  |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

iv. 3.3.5 Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Aplicações conhecidas em porta não padrão  |
| <b>Objetivo do Teste</b>     | Detectar protocolos independentemente da porta utilizada   |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <ul style="list-style-type: none"> <li>- conforme topologia no item 5.1.6</li> </ul> <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol> |
| <b>Procedimento de Teste</b> | Tela comprovando detecção de protocolo independente de porta:  |

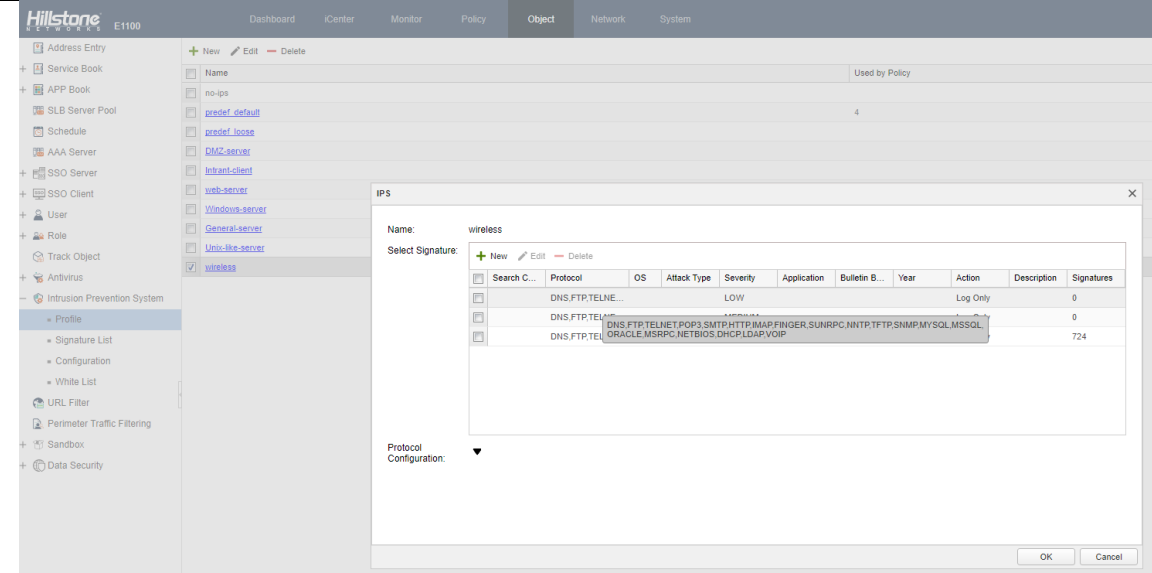
# CADERNO DE TESTES

|                              |  |
|------------------------------|--|
|                              |  |
| <b>Resultado esperado</b>    | Comprovar que a solução detecta protocolos independente da porta                   |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

v. 3.3.6 Detectar e Proteger contra, no mínimo, ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol), DNS (Domain Name System), FTP, SSH, Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP ou CHARGEN, RDP (Remote Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | RPC SMTP IMAP POP SIP SNMP SSDP RDP DoS   |
| <b>Objetivo do Teste</b>     | Provar detecção e proteção em todos ataques relacionados do item 3.3.6  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | Tela comprovando todos tipos de ataques suportados:   |

# CADERNO DE TESTES

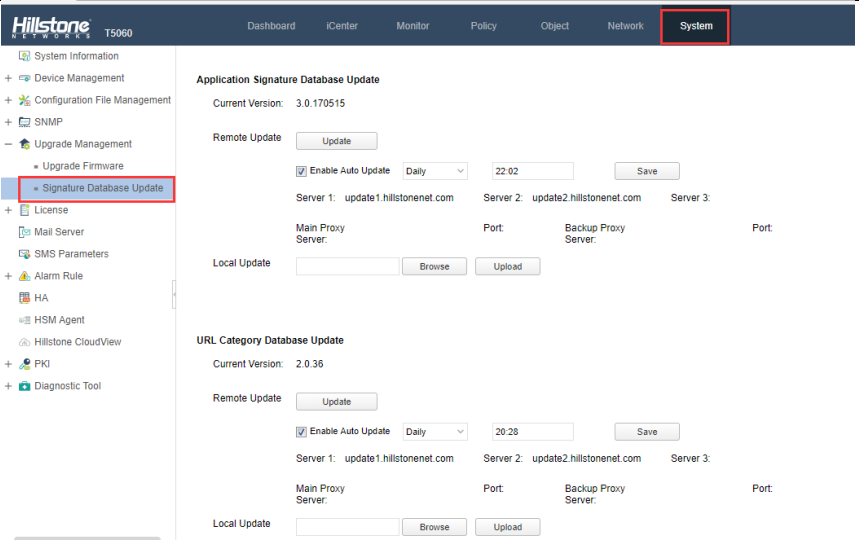
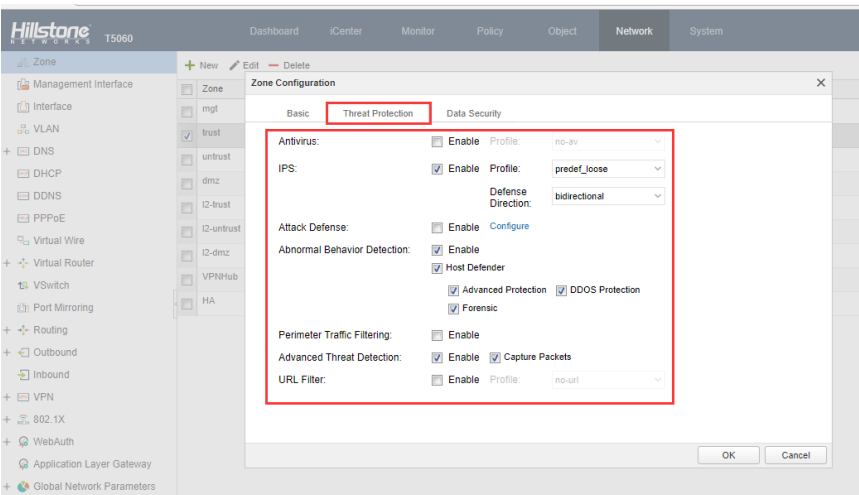
|                              |  |
|------------------------------|--|
|                              |                |
| <b>Resultado esperado</b>    | Comprovar que a solução detecta e protege contra ataques RPC SMTP IMAP POP SIP SNMP SSDP RDP DoS |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

vi. 3.3.7 Possuir proteção contra os ataques como, mas não restringindo-se 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); 5) Tráfego mal formado; 6) 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 Plug-ins/Add-ons.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Proteção contra ataques Worm, Trojan, backdoors, portscan, IP Spoofing, DoS, Spywares, Botnets, malwares  |
| <b>Objetivo do Teste</b>     | Comprovar proteção aos ataques do item 3.3.7  |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima. |
| <b>Procedimento de Teste</b> | 1. Atualizar as assinaturas para a mais recente:  |



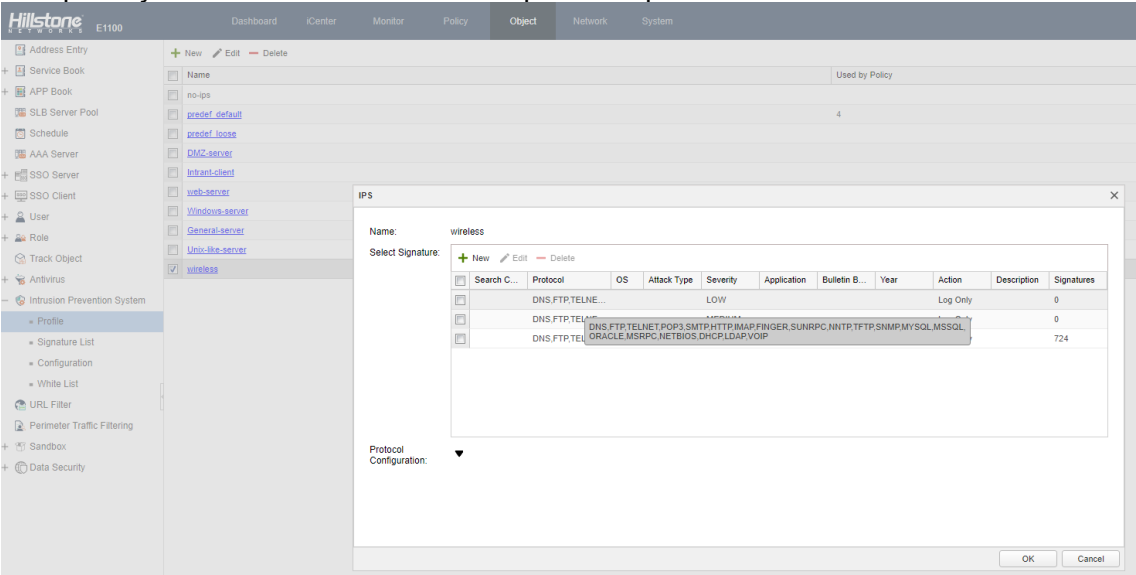
# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              |  <p>2. Habilitar as funcionalidades na Zona:</p>  <p>3. Testar os resultados</p> |
| <b>Resultado esperado</b>    | Comprovar atendimento de proteção aos ataques listados no item 3.3.7  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

vii. 2.3.13 . Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, suportando, no mínimo, as técnicas: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.

|                              |   |
|------------------------------|---|
| <b>Item Testado</b>          | Ip Packet fragmentation, stream segmentation, RPC fragmentation, URL obfuscation, HTML obfuscation, Payload encoding, FTP evasion layered evasion |
| <b>Objetivo do Teste</b>     | Resistir as técnicas de evasão ou ataques listados no item 2.3.13   |
| <b>Configuração de Teste</b> | Diagrama de rede:<br>- conforme topologia no item 5.1.6   |

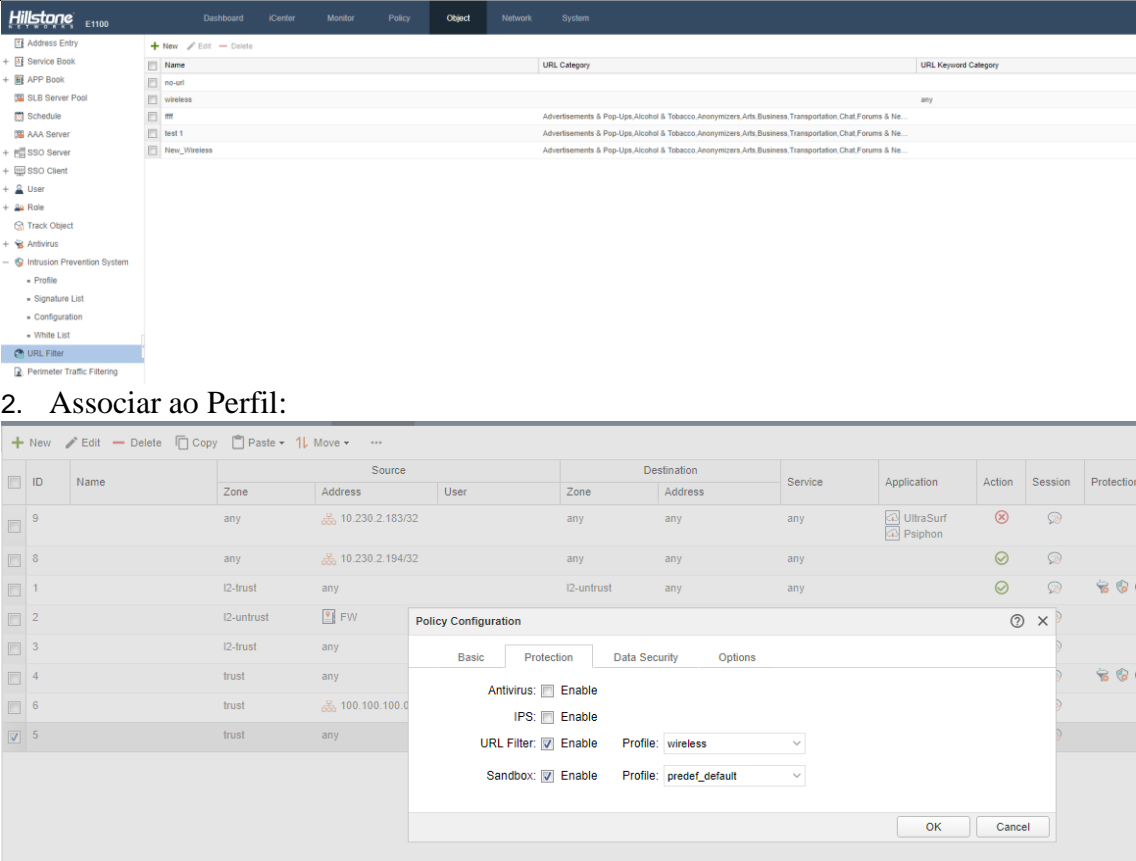
## CADERNO DE TESTES

|                              |  |
|------------------------------|--|
|                              | <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol> |
| <b>Procedimento de Teste</b> | <p>Comprovação de técnicas de evasão suportadas para defesa:</p>   |
| <b>Resultado esperado</b>    | Resistir as técnicas de evasão ou ataques listados no item 2.3.13  |
| <b>Teste OK</b>              |  |
| <b>Teste com Falha</b>       |  |
| <b>Observação</b>            |  |
| <b>Assinatura do cliente</b> |  |
| <b>Assinatura Tracenet</b>   |  |

viii. 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.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Categorizar ao menos 80% dos sites   |
| <b>Objetivo do Teste</b>     | Categorizar sem reconhecimento de categoria como genérica ou similar   |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <ul style="list-style-type: none"> <li>- conforme topologia no item 5.1.6</li> </ul> <p>Pré-condições:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionam normalmente.</li> <li>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</li> </ol> |
| <b>Procedimento de Teste</b> | 1. Configurar o URL profile  |

# CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              |  <p>2. Associar ao Perfil:</p> <p>3 – Testar os resultados</p> |
| <b>Resultado esperado</b>    | Categorizar os sites com ao menos 80% do resultado não sendo genérico ou similar  |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

ix. 2.5.16. Suportar e forçar pesquisas seguras em pelo menos dois sistemas de buscas, contemplando Google e/ou Bing e/ou Yahoo.

|                              |  |
|------------------------------|--|
| <b>Item Testado</b>          | Suportar pesquisas seguras   |
| <b>Objetivo do Teste</b>     | Testar pesquisa segura em ao menos dois mecanismos Google, Bing e Yahoo  |
| <b>Configuração de Teste</b> | <p>Diagrama de rede:</p> <p>- conforme topologia no item 5.1.6</p> <p>Pré-condições:</p> <p>1) Todos os dispositivos funcionam normalmente.</p> <p>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.</p> |
| <b>Procedimento de Teste</b> | 1 - Habilitar a funcionalidade safe-search por linha de comando CLI:<br>enable safe-search   |

## CADERNO DE TESTES

|                              |   |
|------------------------------|---|
|                              | <pre> SG-6000[DBG]# configure SG-6000[DBG](config)# url-profile test SG-6000[DBG](config-url-profile)# ?   keyword-category  Configure Keyword Category   safe-search       Enable safe search enforcement for Google, Yahoo!, Bing, Yandex   ssl-inspection    Enable SSL-inspection for URL-category   url-category      Configure URL Category   urlfilter         Enable Http url filter -   auxswitch        Switch aux port to subcard   clear            Reset functions or clear the screen   debug            Debugging functions   delete           Delete a file   end              Exit from configure mode   exec             Perform command operation   exit            Exit from URL Filter Profile configuration mode   help            CLI help   no              Negate a command or reset to default   ping            Test network connectivity   remove          Remove nbc database   rollback        Rollback startup with one backup   save            Save configuration   show            Show running system information   terminal        Configure terminal line parameters   traceroute      Trace route to destination   undebg         Negate debugging functions   unset          Back to the default configuration SG-6000[DBG](config-url-profile)# safe-search ?   block          Block search results that are not using strict safe search setti   enforce        Transparently enforce safe search SG-6000[DBG](config-url-profile)# safe-search enforce SG-6000[DBG](config-url-profile)# show url-profile test url-profile "test" (ID 1)     safe-search: enable, action: enforce  SG-6000[DBG](config-url-profile)# end </pre> |
| <b>Resultado esperado</b>    | Pesquisas seguras em ao menos dois sites de pesquisa entre Google, Bing e Yahoo   |
| <b>Teste OK</b>              |   |
| <b>Teste com Falha</b>       |   |
| <b>Observação</b>            |   |
| <b>Assinatura do cliente</b> |   |
| <b>Assinatura Tracenet</b>   |   |

x. 3.29.1.2 Possuir, no mínimo, o throughput de 10 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.

| Teste OK | Teste com falha | Observação |
|----------|-----------------|------------|
|          |                 |            |

xi. 3.29.1.5 Possuir a capacidade mínima de 2 (dois) discos, sendo rígidos ou SSD de 240 GB em RAID 1 para armazenamento de logs:

# CADERNO DE TESTES

| Item Testado                            | 2 discos de no mínimo 240GB em RAID  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
|---|--|---------------------|---------|---------|---------------|---------|--------|--------------------------|--------|--------|------------------|----|----|-----------------|------|------|-------------|--------|--------|--------------|------------------|-------------|----------------------------|---------------------|---------------------|---|-------|--------|--------|---------|------------------|---|---|----|----|--------------------|-----|------|------|------|------------------|---------|---------|---------|---------|-----------------------|-------|----|----|----|---------------------------------|--------------------------------|--|--|--|
| Objetivo do Teste                       | Comprovar que a solução faz RAID 1 em 2 discos com capacidade mínima de 240GB  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Configuração de Teste                   | Diagrama de rede:<br>- conforme topologia no item 5.1.6<br>Pré-condições:<br>1) Todos os dispositivos funcionam normalmente.<br>2) Estabeleça o ambiente de teste de acordo com o diagrama acima.  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Procedimento de Teste                   | <div>Especificação da solução de armazenamento de logs:</div> <div><div><div>Product Specification</div><div>HSM Appliance Specification</div><table><tr><th>Specification</th><th>HSM-200</th><th>HSM-50</th></tr><tr><td>Devices Supported (max.)</td><td>15/500</td><td>15/100</td></tr><tr><td>Storage Capacity</td><td>4T</td><td>2T</td></tr><tr><td>Fixed I/O Ports</td><td>2xGE</td><td>2xGE</td></tr><tr><td>RAID Levels</td><td>RAID 5</td><td>RAID 0</td></tr><tr><td>Power Supply</td><td>Single/Dual 750W</td><td>Single 750W</td></tr><tr><td>Dimensions (W x D x H, mm)</td><td>2U (440 x 520 x 88)</td><td>1U (434 x 394 x 43)</td></tr></table></div><div><div>Virtual Appliance (vHSM) Specification</div><table><tr><th>Management Capability (Default/Maximum)</th><th>15/25</th><th>15/100</th><th>15/500</th><th>15/1000</th></tr><tr><td>vCPU Requirement</td><td>4</td><td>8</td><td>18</td><td>24</td></tr><tr><td>Memory Requirement</td><td>4GB</td><td>16GB</td><td>32GB</td><td>64GB</td></tr><tr><td>Port Requirement</td><td>2 ports</td><td>2 ports</td><td>2 ports</td><td>2 ports</td></tr><tr><td>Hard Disk Requirement</td><td>100GB</td><td>2T</td><td>4T</td><td>8T</td></tr><tr><td>Virtual Environment Requirement</td><td colspan="4">Vmware Workstation/EXSi or KVM</td></tr></table></div></div> <div><a href="http://www.hillstonenet.com/wp-content/uploads/Hillstone_HSM_2.5R4P2_EN.pdf">http://www.hillstonenet.com/wp-content/uploads/Hillstone_HSM_2.5R4P2_EN.pdf</a></div> |                     |         |         | Specification | HSM-200 | HSM-50 | Devices Supported (max.) | 15/500 | 15/100 | Storage Capacity | 4T | 2T | Fixed I/O Ports | 2xGE | 2xGE | RAID Levels | RAID 5 | RAID 0 | Power Supply | Single/Dual 750W | Single 750W | Dimensions (W x D x H, mm) | 2U (440 x 520 x 88) | 1U (434 x 394 x 43) | Management Capability (Default/Maximum) | 15/25 | 15/100 | 15/500 | 15/1000 | vCPU Requirement | 4 | 8 | 18 | 24 | Memory Requirement | 4GB | 16GB | 32GB | 64GB | Port Requirement | 2 ports | 2 ports | 2 ports | 2 ports | Hard Disk Requirement | 100GB | 2T | 4T | 8T | Virtual Environment Requirement | Vmware Workstation/EXSi or KVM |  |  |  |
| Specification                           | HSM-200  | HSM-50              |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Devices Supported (max.)                | 15/500   | 15/100              |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Storage Capacity                        | 4T   | 2T                  |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Fixed I/O Ports                         | 2xGE   | 2xGE                |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| RAID Levels                             | RAID 5   | RAID 0              |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Power Supply                            | Single/Dual 750W   | Single 750W         |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Dimensions (W x D x H, mm)              | 2U (440 x 520 x 88)  | 1U (434 x 394 x 43) |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Management Capability (Default/Maximum) | 15/25  | 15/100              | 15/500  | 15/1000 |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| vCPU Requirement                        | 4  | 8                   | 18      | 24      |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Memory Requirement                      | 4GB  | 16GB                | 32GB    | 64GB    |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Port Requirement                        | 2 ports  | 2 ports             | 2 ports | 2 ports |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Hard Disk Requirement                   | 100GB  | 2T                  | 4T      | 8T      |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Virtual Environment Requirement         | Vmware Workstation/EXSi or KVM   |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Resultado esperado                      | Comprovar que a solução de armazenamento de logs HSM support ao menos 2 disks de pelo menos 240GB em RAID 1  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Teste OK                                |  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Teste com Falha                         |  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Observação                              |  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Assinatura do cliente                   |  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |
| Assinatura Tracenet                     |  |                     |         |         |               |         |        |                          |        |        |                  |    |    |                 |      |      |             |        |        |              |                  |             |                            |                     |                     |   |       |        |        |         |                  |   |   |    |    |                    |     |      |      |      |                  |         |         |         |         |                       |       |    |    |    |                                 |                                |  |  |  |

Razão Social: Tracenet Treinamento e Comércio em Informática Ltda  
CNPJ/MF: 10.242.293/0001-77

Endereço: Avenida Presidente Vargas, 542 – Grupo 415 – Centro

Tel./Fax: (21) 2223-1412 - CEP: 20071-000 - Cidade: Rio de Janeiro UF: Rio de Janeiro

Rio de Janeiro, 09 de janeiro de 2018.