Caderno de Testes

Homologação de Firewall para o cliente MPOG

Cliente:	**MPOG**
Responsável:	**Ronaldo de Melo**
Documento:	**Huawei_Firewall_Test_Cases_Huawe_MPOGv2.docx**
Processo:	**PREGÃO ELETRÔNICO N.º 05/2017 (Lote 4)**
Versão do produto:	
Total de páginas:	**125**
Elaboração:	**23/11/2017**
Atualização:	
Responsável:	**Ronaldo de Melo | ronaldo.melo@vert.com.br**

Controle de Revisão

Date	Revision Version	Change Description	Author
22/11/2017	1.0		Ronaldo de Melo ronaldo.melo@vert.com.br (M) +55 61 99966-1082
08/01/2018	2.0		Ronaldo de Melo ronaldo.melo@vert.com.br (M) +55 61 99966-1082

CONTEUDO

CONTEUDO **2**

1 CONFIDENCIALIDADE **5**

2 EQUIPAMENTOS HUAWEI EM UTILIZAÇÃO **5**

3 EQUIPE TÉCNICA **7**

4 TOPOLOGIA DE TESTES: **8**

5 PREPARAÇÃO INICIAL **8**

5.1.1 Realizar a inspeção integral de todos os pacotes de dados e registar tudo 8

5.1.2 Zerar contadores 10

5.1.3 Zerar o equipamento 11

5.1.4 Atualização do Equipamento 12

5.1.5 Atualização listas de assinaturas e afins. 13

5.1.6 Criação do backup da Configuração. 16

6 SECURITY CONTROL **17**

6.1 SECURITY POLICY 17

6.1.1 Based on Quintuple 17

6.1.2 Based on User 19

6.1.3 Based on Application 22

7 NAT **24**

7.1 SOURCE NAT 24

7.1.1 NAT NO-PAT 24

7.1.2 NAPT 26

7.1.3 Easy-IP 27

7.1.4 Destinaton NAT 29

8 CONTENT SECURITY **30**

8.1 INTRUSION PREVENTION 30

8.2 ANTI VIRUS 33

8.3 CONTENT SECURITY DETECTION BASED ON SSL ENCRYPTED TRAFFIC 36

8.4 URL FILTERING 38

8.4.1 HTTP Filtering 38

8.4.2 HTTPS Filtering 41

9 TRAFFIC MANAGEMENT 44

9.1 BANDWIDTH MANAGEMENT 44

9.1.1 Bandwidth Limitation 44

9.1.2 Concurrent Limitation 45

9.1.3 New Connections Limitation 47

10 VPN 48

10.1 IPSEC VPN 48

10.2 LOGS&REPORTS 52

10.2.1 Traffic Log 52

10.2.2 Threat Log 53

10.2.3 URL Log 54

10.2.4 Traffic Report 55

10.2.5 Threat Report 57

10.2.6 Packet Capture 59

10.3 CENTRALIZED MANAGEMENT 61

10.3.1 CPU、Memory Usage&Performance Status Monitoring 61

11 PERFORMANCE 64

11.1 IMIX THROUGHPUT 64

11.2 HTTP NEW CONNECTIONS 80

11.3 HTTP CONCURRENT 84

12 CONFIGURAÇÕES DE TESTES E TOPOLOGIA 86

13 DETECÇÃO/PREVENÇÃO À INTRUSÃO/ATAQUES (IDS/IPS) 89

14 PROTEÇÃO CONTRA AMEAÇAS (ANTIVÍRUS E ANTI-MALWARE) 92

15 CONTROLE DE ACESSO (CONTROLE DE APLICAÇÕES E FILTRAGEM DE URL'S) 94

16 TESTE DE ASSERTIVIDADE 97

17 TESTE DE DESEMPENHO 99

18 TESTE DE SESSÕES 101

19 TESTES COMPLEMENTARES 103

19.1 ITEM 2.1.29 103

19.2 ITEM 2.1.39 104

19.3 ITEM 2.1.45.6 105

19.4 ITEM 2.1.45.9 105

19.5 ITEM 2.1.45.12 109

19.6 ITEM 2.1.63 110

19.7 ITEM 2.1.68 111

19.8 ITEM 2.2.7 111

19.9 ITEM 2.2.8 112

19.10 ITEM 2.3.3 112

19.11 ITEM 2.3.6 114

19.12 ITEM 2.3.7 114

19.13 ITEM 2.3.12 115

19.14 ITEM 2.3.13 116

19.15 ITEM 2.5.1 117

19.16 ITEM 2.5.9 118

19.17 ITEM 2.5.10 E 2.5.10.1 119

19.18 ITEM 2.5.11 119

19.19 ITEM 2.5.14 120

19.20 ITEM 2.5.15 121

19.21 ITEM 2.6.12 121

19.22 ITEM 2.6.13 122

19.23 ITEM 3.22.1.4 E 3.22.1.4.1 123

19.24 ITEM 3.24.1.2 E 3.24.1.3 124

I. CONCLUSÃO DO TESTE 125

1 Confidencialidade

O conteúdo deste documento é estritamente confidencial e não poderá ser acessado por pessoas, dentro ou fora do Cliente, que não estejam diretamente autorizadas pelo mesmo e ligadas ao processo de avaliação ou ser utilizado para outros fins que não a própria avaliação.

Deste modo, este documento contém o entendimento da Huawei e Vert pautado pelo trabalho conjunto de esclarecimentos sobre o processo, necessidades e outras informações pertinentes, ressalvando-se que as informações aqui constantes têm caráter confidencial e não poderão ser usadas para outras finalidades que não as aqui propostas.

2 Equipamentos Huawei em utilização

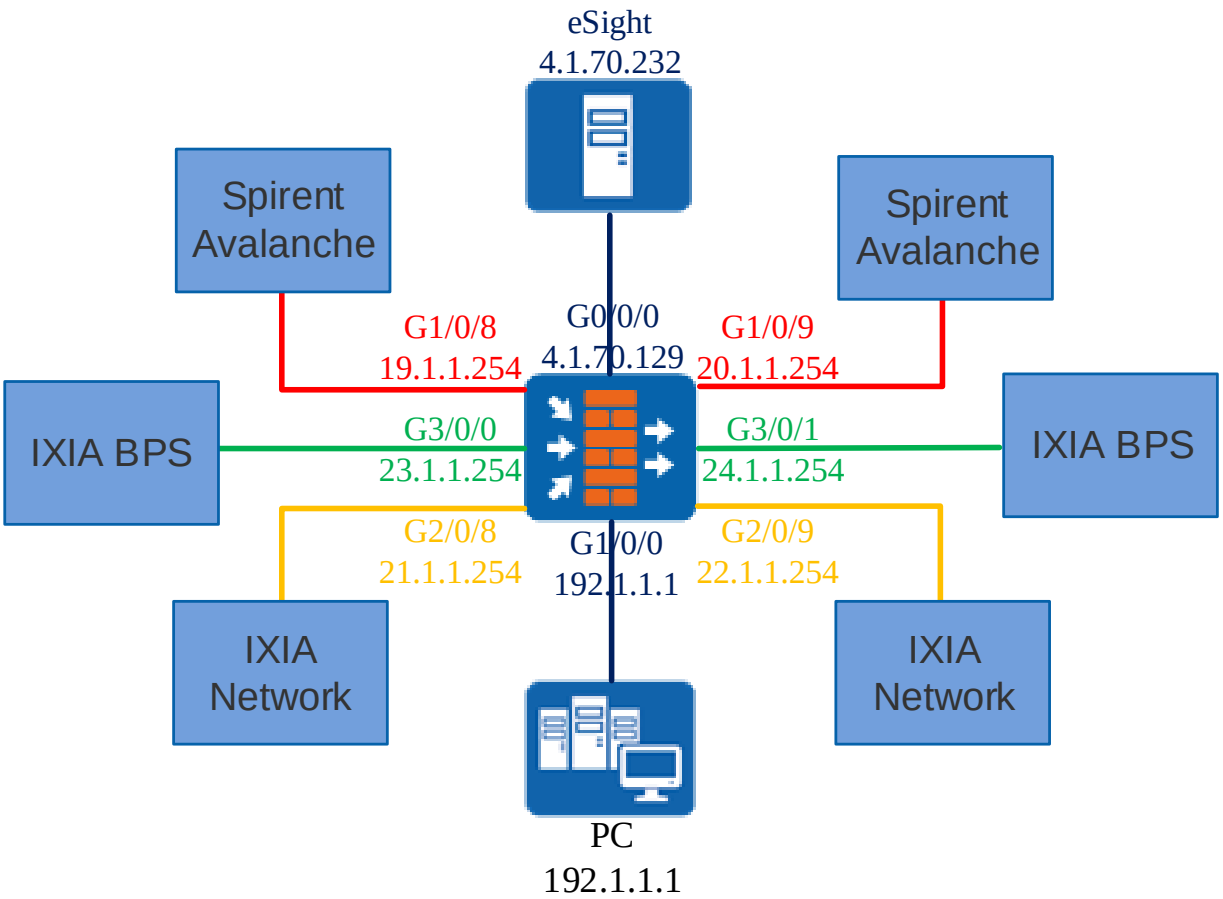
Part Number	Model	Description
LogCenter		
Log Event Management Center		
Auxiliary Equipment		
05200219	SC1GSUSE1101	Novell SuSE Linux Enterprise Server 11,1Y7*24 Service
05331608	WM5GLADMVE56	System Application Software,Light Application Data Management Software Package(5.6 S), 1 Year Standard Product Services
Software License		
Function License		

88033ADW	LIC-LC-BAS	Log Manager Basic Package (including LogCenter Basic Function and Small-scale Management License)
eSight Network		
eSight,Enterprise Operation System		
Self-made Software		
eSight Standard Edition		
88032VEW	NSHSPLTSTD01	eSight Platform,Standard
USG6680		
USG6600		
Main Equipment		
Basic Configuration		
02358057	USG6680-BDL-AC	USG6680 AC Host(16GE(RJ45)+8GE(SFP)+4*10GE(SFP+),16G Memory,2 AC Power, with IPS-AV-URL Function
Harddisk		
0235G7GC	SM-HDD-SAS300G-A	300GB 10K RPM SAS Hard Disk Unit
Optical Transmitter Module Collection		
02315204	eSFP-GE-SX-MM850	Optical Transceiver,eSFP,GE,Multi-mode Module(850nm,0.55km,LC)
02318169	OMXD30000	Optical Transceiver,SFP+,10G,Multi-mode Module(850nm,0.3km,LC)

3 Equipe Técnica

NOME	E-MAIL	EMPRESA
Ronaldo de Melo	Ronaldo.melo@vert.com.br	VERT
Willian Zanardi	Willian.zanardi@vert.com.br	VERT
Rubens Karklin	Rubens.karklin@huawei.com	HUAWEI
Wilian Mainarte	Wmainarte@latin-telecom.com	Latin Telecom do Brasil

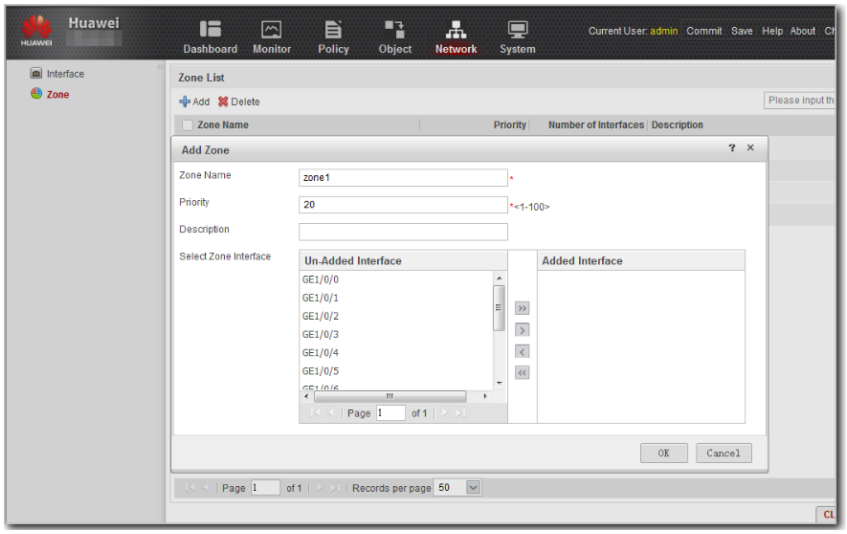
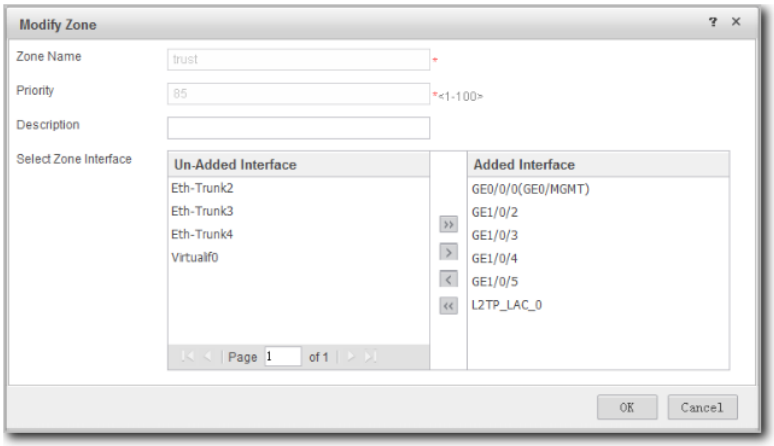
4 Topologia de Testes:



5 Preparação Inicial

5.1.1 Realizar a inspeção integral de todos os pacotes de dados e registrar tudo

Objetivo de teste	Configurar o equipamento de forma a realizar a inspeção integral de todos os pacotes de dados e registrar todos os tráfegos autorizados ou bloqueados
Especificação de teste	O equipamento deve ser configurado de forma a realizar a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo de forma a registrar todos os tráfegos autorizados ou bloqueados, bem como todas as aplicações e ameaças detectadas pelo Firewall Multifuncional.
Ambiente de teste	Test TOPO: Pré-condição:

	1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Criar duas zonas (Trust/Untrust) com uma regra "any -> any" nos dois sentidos; 1. Choose **Network** > **Zone**. 2. Click **Add**. 3. Set the following security zone parameters.  1. Choose **Network** > **Zone**. 2. Perform either of the following methods to enter the operation page before adding interfaces to security zones: • After a security zone is created, perform operations on the **Add Zone** page. • Click of the line where the entry to be modified resides and enter the **Modify Zone** operation page.  3. In **Select Zone Interface**, perform one of the following operations: • On the **Un-Added Interface** page, double-click a desired interface. This interface appears in the **Added Interface** window. • On the **Un-Added Interface** page, select a desired interface and click . This interface appears in the **Added Interface** window. • Click to assign all interfaces to the current security zone. 4. Click **OK**. 2. Configurar os logs de todo tipo de trafego:

<table>
<tr><td></td><td colspan="4">

Procedure

1. Choose **Monitor** > **Log** > **Traffic Log**.
2. Choose **Customize** and select/deselect conditions for traffic log display.
3. **Optional:** Click **Export** to export traffic logs in CSV format to the management PC.

The following table lists the fields in a traffic log.

Field	Description
View	Click . In View **Traffic Log Details**, the details of each field in a traffic log are displayed. In View **Traffic Log Details**, click the **Source Address**/**Destination Address**/**Source User**/**Application**/**Security Policy**/**Traffic Policy** field value. You can view and operate the existing field settings. For details on how to view and operate the settings, see Table 1.
Time	Time when a traffic log is generated
Source Zone	Source security zone of traffic
Destination Zone	Destination security zone of traffic
Source Region	Source region of the traffic
Destination Region	Destination region of the traffic
Source Address	Source IP address of traffic
Source User	User who generates traffic
Destination Address	Destination IP address of traffic
Source Port	Source port of traffic
Destination Port	Destination port of traffic
Application	Application type of traffic
Protocol	Protocol type of traffic
Security Policy	Security policy that traffic matches
Traffic Policy	Traffic policy that traffic matches
Total Traffic	Traffic volume
Inbound Interface	Inbound interface of traffic
Outbound Interface	Outbound interface of traffic
Virtual System	Virtual system that generates the traffic

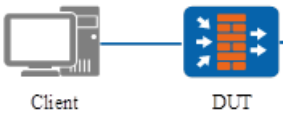
During the traffic log analysis, you can click **Advanced Query** and enter a value into **Total Traffic** to query the logs of traffic that exceeds the value. Based on the displayed logs, you can take measures as follows if necessary.

Table 1 Traffic log field settings

Field	Setting
Source Address/Destination Address	Click the **Source Address**/**Destination Address** field value of a specific traffic log. **Add Blacklist Entry** is displayed. The parameters in **Add Blacklist Entry** are as follows: • Type: The source/destination address is automatically blacklisted. • Source IP/Destination IP: The source/destination IP address is automatically blacklisted. • Protocol: The protocol type is automatically blacklisted. • Source Port/Destination Port: The source/destination port is automatically blacklisted. • Timeout: You can use either of the following methods to set a timeout period for a blacklist entry: • Select **Unlimited** to permanently blacklist the source/destination address. • Enter a timeout period.
Source Region/Destination Region	Click the **Source Region**/**Destination Region** across the **Edit** page and change the region configuration as required. For details, see Changing Predefined Regions and Customizing Regions.
Source User	Click the **Source User** field value of a specific traffic log. **Modify User** is displayed. For details on how to modify user configuration, see Configuring Users, User Groups or Security Groups.
Application	Click the **Application** field value of a specific traffic log. **Application Details** is displayed. You can view application details and configure port mappings. For details on how to configure port mappings, see Configuring Port Mapping.
Security Policy	Click the **Security Policy** field value of a specific traffic log. **Modify Security Policy** is displayed. You can change the settings of the source address, destination address, user, application, time range, action, and security profile. For details on how to change the settings, see Configuring a Security Policy.
Traffic Policy	Click the **Traffic Policy** field value of a specific traffic log. **Modify Traffic Policy** is displayed. You can change the settings of the source address, destination address, user, application, time range, and action. For details on how to change the settings, see Configuring Bandwidth Management Using the Web UI.

</td></tr>
<tr><td>Resultado Esperado</td><td colspan="4">1. Atender aos requisitos do item 5.13 e 5.14 do Anexo E.</td></tr>
<tr><td>Resultado do Teste</td><td colspan="4">☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA</td></tr>
<tr><td>Observação</td><td colspan="4"></td></tr>
<tr><td>Assinatura</td><td>Cliente</td><td></td><td>Huawei</td><td></td></tr>
</table>

5.1.2 Zerar contadores

Objetivo de teste	Limpeza e exclusão dos dados de forma a zerar os contadores do equipamento.
Especificação de teste	Após a realização do teste de assertividade, o firewall da Amostra deverá ter todos os seus contadores zerados.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente;

	4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).

Procedimento de Teste	3. Zerar os "counters" existentes no dispositivo;
	# Clear GTP ACL rule counter.
	`<sysname> system-view`
	`[sysname] gtp policy policy1`
	`[sysname-gtp-policy1] acl`
	`[sysname-gtp-policy1-acl] reset rule counter`
	# Clear statistics about ACL 2001.
	`<sysname> reset acl counter 2001`
	# Clear counter information about a traffic policy rule named **traffic_rule**.
	`<sysname> reset traffic-policy counter rule traffic_rule`
	# Clear statistics on authentication policy rule **auth_rule**.
	`<sysname> reset auth-policy counter rule auth_rule`
	# Clear the match count of security policy rule **policy_sec**.
	`<sysname> reset security-policy counter rule policy_sec`
	# Clear the matching counts of all PBR rules.
	`<sysname> reset policy-based-route counter all`

Resultado Esperado	2. Resetar os counters do equipamento.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

5.1.3 Zerar o equipamento

Objetivo de teste	Limpeza e exclusão dos dados de forma a zerar quaisquer configurações.
Especificação de teste	Todos os componentes da solução ofertada deverão ser, antes de iniciado o Teste de Conformidade, submetidos a procedimento de limpeza e exclusão dos dados de forma a zerar quaisquer configurações.
Ambiente de teste	Test TOPO:

	 Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).

Procedimento de Teste	4. Deletar as configurações existentes no dispositivo;
	`<sysname> reset saved-configuration`
	`The action will delete the saved configuration in the NGFW.`
	`The configuration will be erased to reconfigure.`
	`Are you sure?[Y/N]y`

Resultado Esperado	3. Restaurar as configurações de fábrica do dispositvo.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

5.1.4 Atualização do Equipamento

Objetivo de teste	Atualizar para a versão mais recente de firmware e software
Especificação de teste	A solução ofertada deverá então ser 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.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente;

<table>
<tr><td></td><td colspan="4">4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).</td></tr>
<tr><td>Procedimento de Teste</td><td colspan="4">1. Obter a ultima versão disponível no site da Huawei e coloca-lo em uma unidade USB, neste exemplo o arquivo é chamado system-software.bin;
2. Inserir a unidade USB no equipamento;
3. Realizar o upgrade, conforme abaixo:

<pre><NGFW> upgrade system-software udisk0:/system-software.bin
Upgrade system software ?[Y/N]:Y
Info: Check system software begin, it will take a long time, please don't power down or pull out disk.....
.....
Info:Udisk0:Successful upgrade, ready to restart.</pre>
4. Verificar o resultado do upgrade

<pre><NGFW> display startup
MainBoard:
Configed startup system software: hda1:/SUP.bin
Startup system software: hda1:/system-software.bin
Next startup system software: hda1:/SUP51.bin
Startup saved-configuration file: hda1:/system-config.zip
Next startup saved-configuration file: hda1:/system-cfg.zip</pre>

<pre><NGFW> display version
HUAWEI Versatile Routing Platform Software
Software Version: V100R001C30SPC900 (VRP (R) Software, Version 5.30)
Copyright (C) 2014-2017 Huawei Technologies Co., Ltd.
sysname uptime is 0 week, 0 day, 15 hours, 20 minutes
Patch: V100R001C20SPH001</pre></td></tr>
<tr><td>Resultado Esperado</td><td colspan="4">4. Atualizar o equipamento para a versão que será utilizada na homologação.</td></tr>
<tr><td>Resultado do Teste</td><td colspan="4">☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA</td></tr>
<tr><td>Observação</td><td colspan="4"></td></tr>
<tr><td>Assinatura</td><td>Cliente</td><td></td><td>Huawei</td><td></td></tr>
</table>

5.1.5 Atualização listas de assinaturas e afins.

Objetivo de teste	Atualizar para a versão mais recente de listas de assinaturas e afins.
Especificação de teste	A solução ofertada deverá então ser 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.
Ambiente de teste	Test TOPO:

<table>
<tr>
<td></td>
<td>

Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;
4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
</td>
</tr>
<tr>
<td>Procedimento de Teste</td>
<td>
1. Obter a ultima versão disponível no site da Huawei (sec.huawei.com) dos arquivos AV-SDB (Antivirus Assinatura database), SA-SDB (Application Assinatura database) e IPS-SDB (IPS Assinatura database) e coloca-lo em uma unidade USB (site : http://sec.huawei.com/sec/web/freesignature.do)
2.
3. Inserir a unidade USB no equipamento;
4. Realizar o upgrade para cada arquivo, conforme abaixo:

```
<sysname> system-view
[sysname] update local sa-sdb file hda1:/sa_h20010000_2012051800.sdb
```

5. Verificar a quantidade de assinaturas Anti-virus (5 milhões):

```
[MPOG]disp av-signature  database
 ---------------------------------------------------------------------------

  Total Virus Family     :  11172
  Total Virus Signature :  5000000
 ---------------------------------------------------------------------------
    Packed.Win32.Krap
    Packed.Win32.InstallCore
    Packed.Win32.TDSS
    Packed.Win32.Refroso
    Packed.Win32.PolyCrypt
    Packed.Win32.Katusha
    Packed.Win32.Agent
    Packed.Win32.FakeAV
    Packed.Win32.Tibs
    Packed.Win32.Klone
    Packed.Win32.Black
    Packed.Win32.Pasta
    Packed.Win32.PePatch
    Packed.Win32.Injector
    Packed.Win32.Shiz
    Packed.Win32.Hrup
    Packed.Win32.CPEX-based
    Packed.Win32.Bancos
    Packed.Win32.Salpack
  ---- More ----
```

6. Verificar a quantidade de assinaturas IPS (7.945):
</td>
</tr>
</table>

```
[MPOG]disp ips-signature
 ---------------------------------------------------------------------------
 *                          All Searched Signature                         *
 *                             (Counts: 7945)                              *
 ---------------------------------------------------------------------------
 Sig-ID   Protocol   Target  Severity OS        Category         Event Counts
 ---------------------------------------------------------------------------
 1030     FILE       both    high     windows   Overflow                   0
 1040     HTTP       client  high     windows   Overflow                   0
 1050     TCP        server  high     windows   Dos                        0
 1060     HTTP       server  high     windows   Overflow                   0
 1070     TCP        server  high     all       Overflow                   0
 1080     TCP        server  high     windows   Overflow                   0
 1090     UDP        server  high     all       Code-execution             0
 1100     MSRPC      server  high     windows   Overflow                   0
 1101     TCP        server  high     windows   Overflow                   0
 1102     MSRPC      server  high     windows   Overflow                   0
 1110     TCP        server  high     all       Overflow                   0
 1120     TCP        server  high     all       Overflow                   0
 1140     IMAP4      server  high     unix-like Code-execution             0
 1150     MSRPC      server  high     windows   Overflow                   0
 1160     MSRPC      server  medium   windows   Dos                        0
 1170     MSRPC      server  medium   windows   Code-execution             0
 1189     TCP        server  medium   windows   Dos                        0
 1190     FILE       both    high     all       Overflow                   0
  ---- More ----
```

7. Verificar a quantidade de aplicações (6.309):

```
<MPOG>disp application  pre-defined
Service Awareness Signature Database Information:
Total Applications: 6309
-----------------------------------------------------------------------------------------------
 AppID Name                                Category                 Sub-category
 1     BT                                  General_Internet         FileShare_P2P
 2     PPLive                              Entertainment            Peercasting
 3     Thunder                             General_Internet         FileShare_P2P
 5     FTP                                 Network                  Infrastructure
 6     FTPS                                Network                  Infrastructure
 7     eDonkey_eMule                       General_Internet         FileShare_P2P
 9     QQLive                              Entertainment            Peercasting
 11    Fasttrack                           General_Internet         FileShare_P2P
 12    PPStream                            Entertainment            Peercasting
 14    DirectConnect                       General_Internet         FileShare_P2P
 15    KuGoo                               Entertainment            Peercasting
 16    Fring_VoIP                          Entertainment            VoIP
 18    POCO                                General_Internet         FileShare_P2P
 20    Maze                                General_Internet         FileShare_P2P
 22    UUSee                               Entertainment            Peercasting
 23    Vagaa                               General_Internet         FileShare_P2P
 25    QQDownLoad                          General_Internet         FileShare_P2P
 27    Filetopia                           General_Internet         FileShare_P2P
 28    Soulseek                            General_Internet         FileShare_P2P
 29    Sopcast                             Entertainment            Peercasting
 31    KooWo                               Entertainment            Peercasting
 32    FengXing                            Entertainment            Peercasting
 33    PPFilm                              Entertainment            Peercasting
 34    DoPool                              Entertainment            Peercasting
  ---- More ----
```

Resultado Esperado	1. Atualizar as assinaturas de IPS , Antivirus e aplicações do equipamento que será utilizada na homologação.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	A lista conforme Atendimento ao item 5.1.2.1 do Anexo E se divide da seguinte forma: Lista das ameaças IPS/IDS link : http://sec.huawei.com/sec/web/ipsVulnerability.do Obs: Devido ao tamanho temos essa informação apenas on-line. Lista das aplicações enviada em anexo com o arquivo : SA-SDB_Protocol_Identification.pdf Lista de URL´s: http://sec.huawei.com/sec/web/urlClassification.do

Assinatura	**Cliente**		**Huawei**	

5.1.6 Criação do backup da Configuração.

Objetivo de teste	Criar uma cópia em pendrive das configurações realizadas.			
Especificação de teste	Ao final de todo o procedimento de configuração inicial deverá ser 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..			
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			

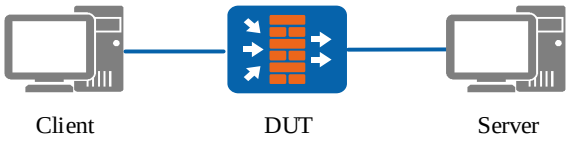
Procedimento de Teste	1. Copiar as configurações para um dispositivo externo “pendrive”:
	`<sysname> copy vrpcfg.cfg hda1:/vrpcfg-bak.cfg`
	`Copy hda1:/vrpcfg.cfg to hda1:/vrpcfg-bak.cfg?[Y/N]:y`
	`When deciding whether to copy file hda1:/vrpcfg.cfg to hda1:/vrpcfg-bak.cfg, the user chose Y.`
	`100% complete`
	`Info:Copied file hda1:/vrpcfg.cfg to hda1:/vrpcfg-bak.cfg...Done`
	2. Restaurar backup:
	`<sysname> copy hda1:/vrpcfg-bak.cfg vrpcfg.cfg`
	`Copy hda1:/vrpcfg-bak.cfg to hda1:/vrpcfg.cfg?[Y/N]:y`
	`The file hda1:/vrpcfg.cfg exists. Overwrite it?[Y/N]:y`
	`Deleting file permanently from hda1:/ will take a long time if needed...Done.`
	`100% complete`
	`Info:Copied file hda1:/vrpcfg-bak.cfg to hda1:/vrpcfg.cfg...Done`			

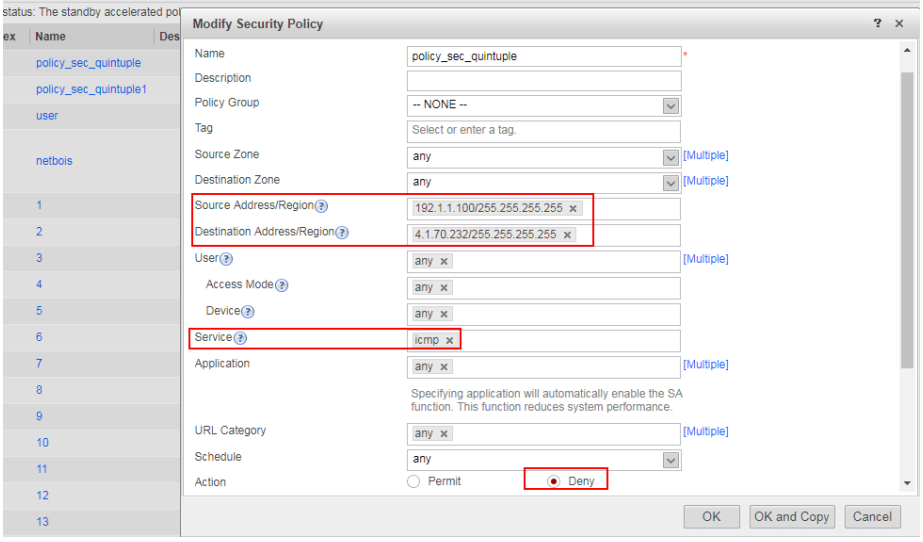
Resultado Esperado	1. Realizar o backup das configurações e restaurar.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

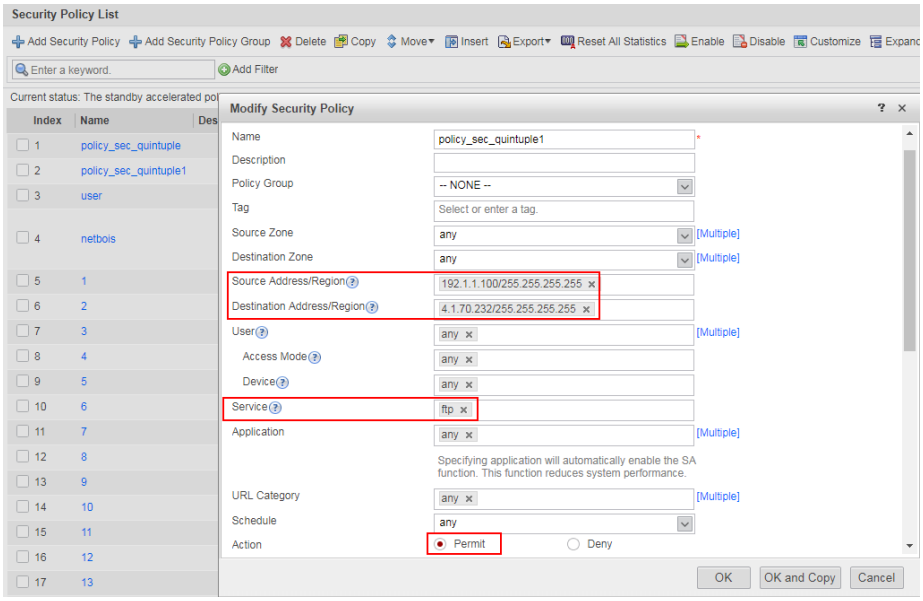
6 Security Control

6.1 Security Policy

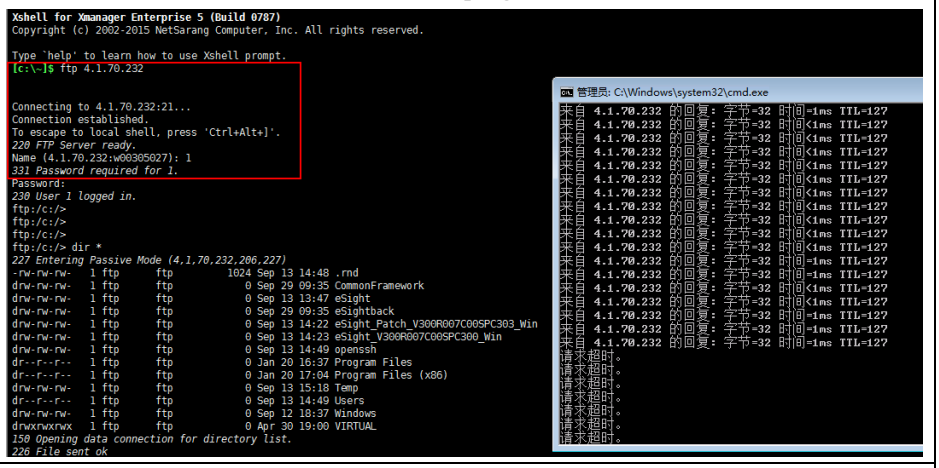
6.1.1 Based on Quintuple

Objetivo de teste	Verificar se o equipamento oferece suporte à diretiva de segurança com base em cinco fatores.
Especificação de teste	Cinco vezes: Incluindo o endereço IP de origem, endereço IP de destino, porta origem, porta de destino e protocolo.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Set the responding action of default policy as deny; 2. Configure security policy ***policy_sec_quintuple*** based on quintuple group, in which the source address is the network of Client, the destination address is the network of Server, the service is ICMP, and the responding action is deny; 3. Configure security policy ***policy_sec_quintuple1*** based on quintuple group, in which the source address is the network of Client, the destination address is the network of Server, the service is FTP, and the responding action is allow;





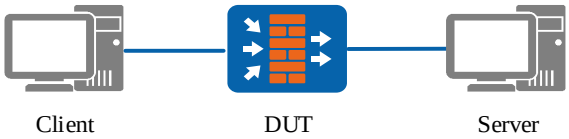
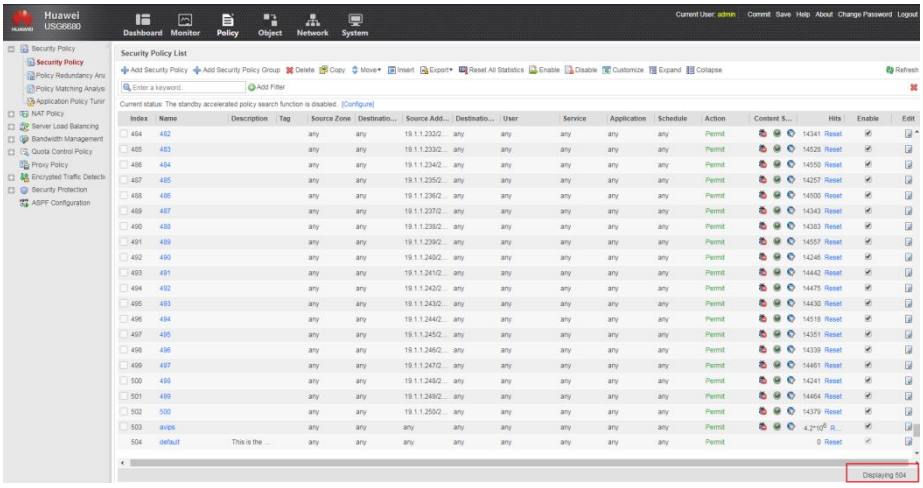
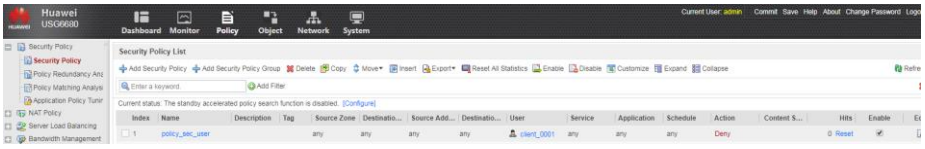
4. Let Client visit the Server side with ping and FTP;

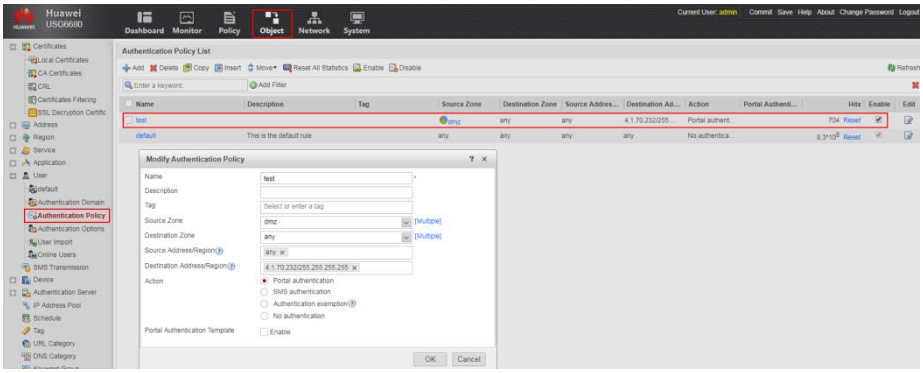


Resultado Esperado	2. The visit from Client to Server with ping fails; while the visit from Client to Server with FTP successes.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA

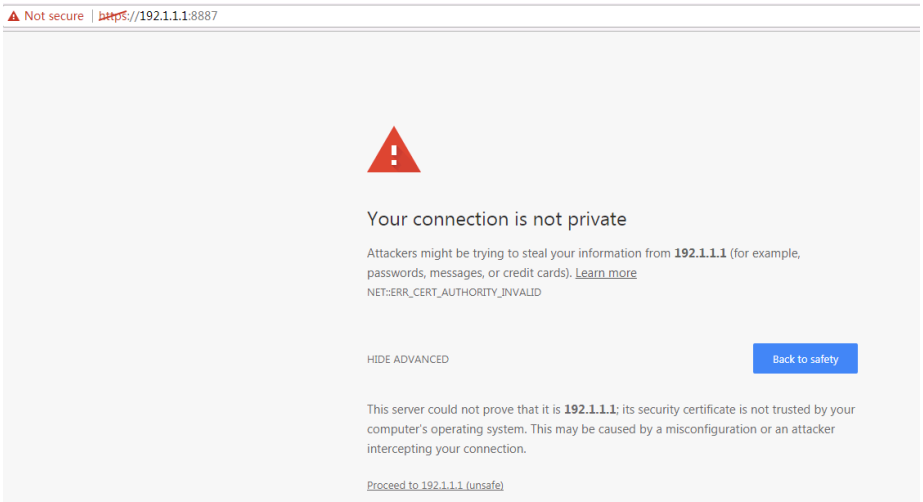
Observação				
Assinatura	**Cliente**		**Huawei**	

6.1.2 Based on User

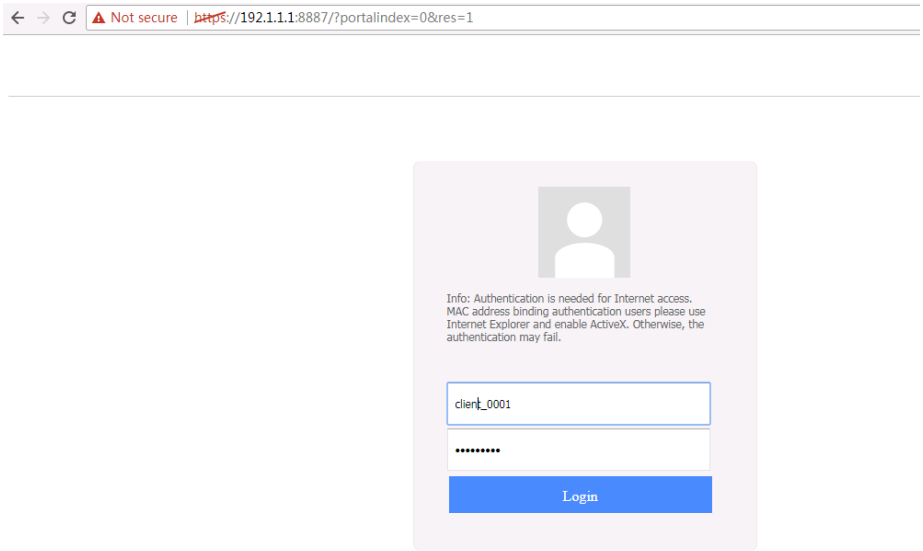
Objetivo de teste	Verify whether the equipment supports security policy based on user.
Especificação de teste	You can reference local users, user groups, or security groups or create new ones. Also allow importing and referencing users, user groups, and security groups.
Ambiente de teste	Test TOPO:  Client DUT Server Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Set the responding action of default policy as permit, which allows the message of user authentication;  2. Configure security policy ***policy_sec_user*** based on user, in which the user is ***Client_0001*** and the responding action is deny;  3. Create an authentication policy with action of portal authentication;

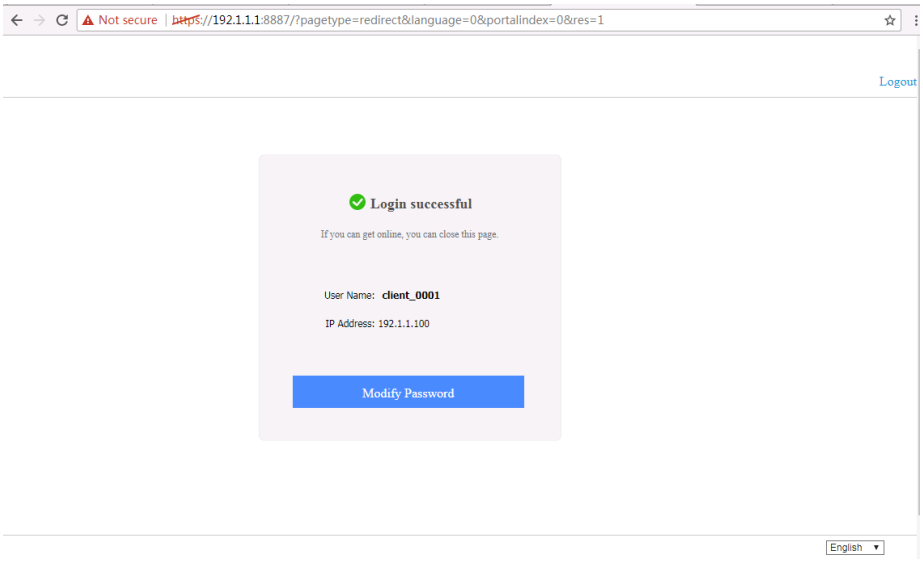


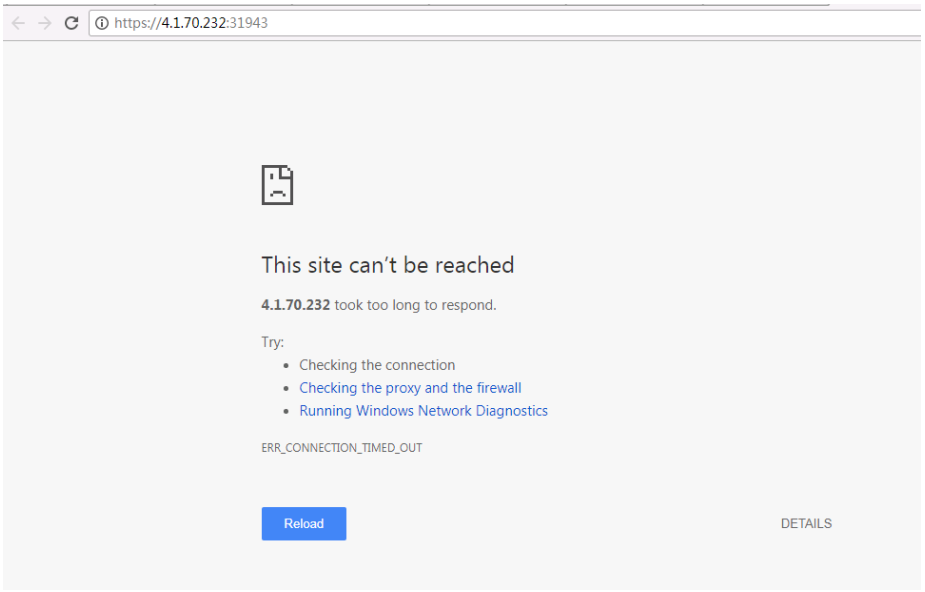
4. Let Client make HTTP visit to the Web server in the Server side;

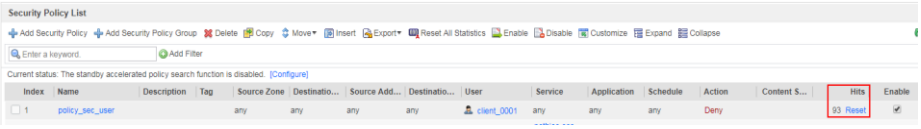


Input username and password:

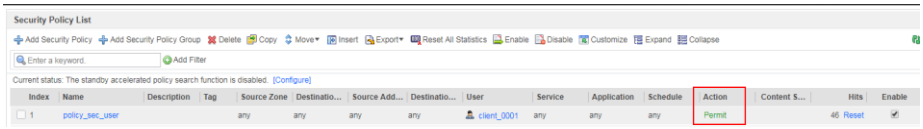




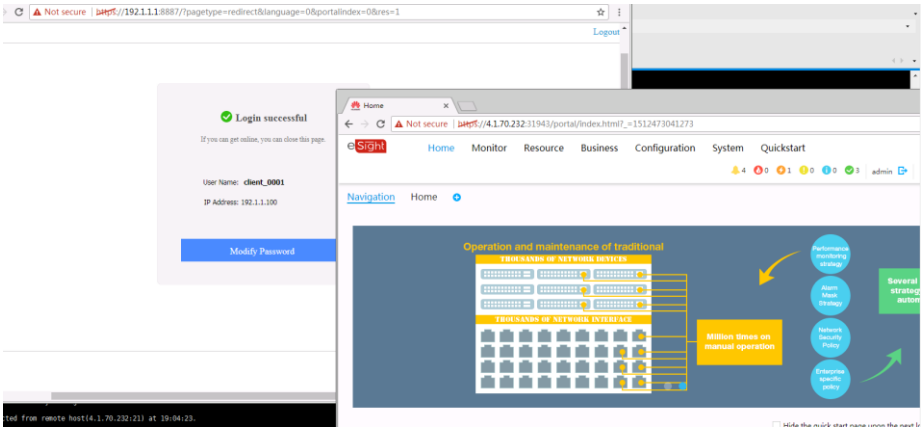




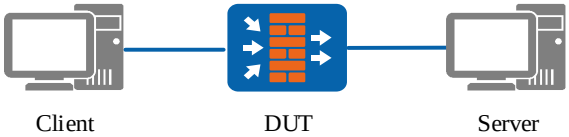
5. Set the responding action of security policy ***policy_sec_user*** as permit instead;

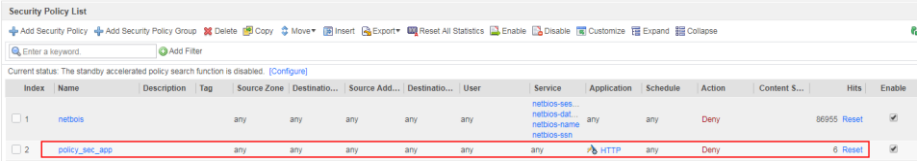
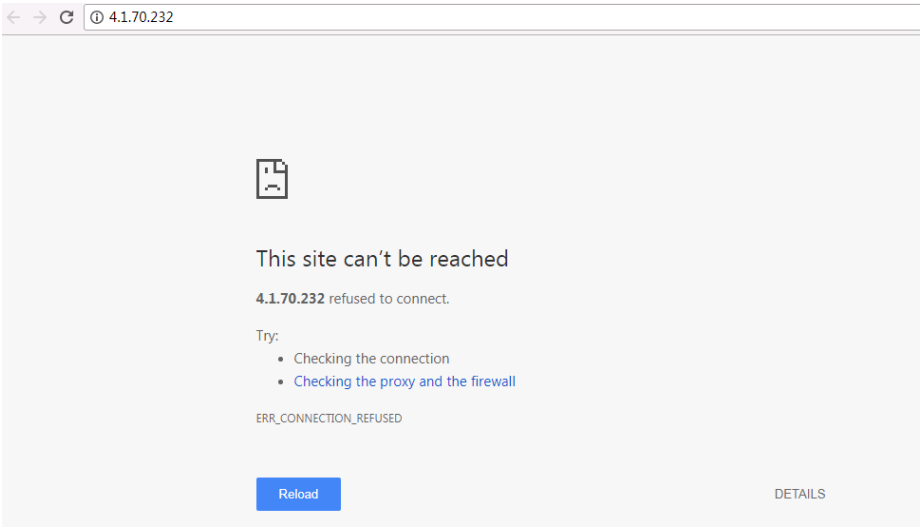
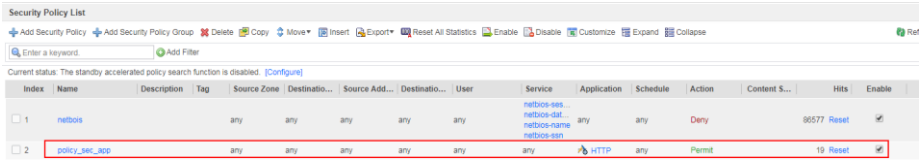
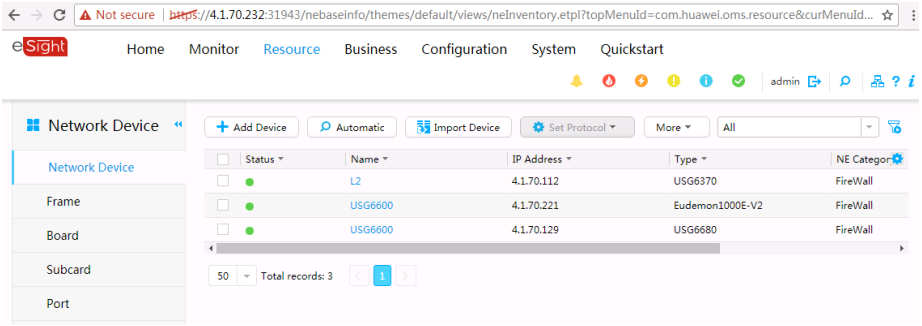


After authenticated, server webpages can be successfully accessed:

	 6. Let Client make HTTP visit to the Web server in the Server side again.			
Resultado Esperado	1. The HTTP visit from Client to Server leads to user authentication, and the visit of ***Client_0001*** fails when the responding action of security policy ***policy_sec_user*** is deny; 2. The HTTP visit from Client to Server succeeds when the responding action of security policy ***policy_sec_user*** is permit, which proves that the equipment support security policy based on user.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

6.1.3 Based on Application

Objetivo de teste	Verify whether the equipment supports security policy based on application.
Especificação de teste	Application identification mode: • Intelligent Identification: Identifies the applications of matching traffic only when the application identification policy or content security detection function is configured; • Full Identification: in this mode, identifies the applications of all traffic.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente;

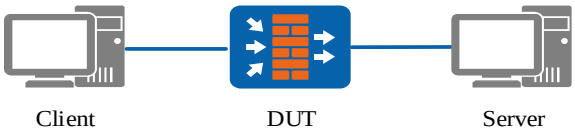
	4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Set the responding action of default policy as deny; 2. Configure security policy ***policy_sec_app*** based on application, in which the application is HTTP and the responding action is deny;  3. Let Client make HTTP visit to the Web server in Server side;  4. Set the responding action of security policy ***policy_sec_app*** as permit instead;  5. Let Client make HTTP visit to the Web server in Server side again. 
Resultado Esperado	1. The HTTP visit from Client to Server fails when the responding action of security policy ***policy_sec_app*** is deny; 2. The HTTP visit from Client to Server succeeds when the responding action of security policy ***policy_sec_app*** is permit, which proves that the equipment support security policy based on application.

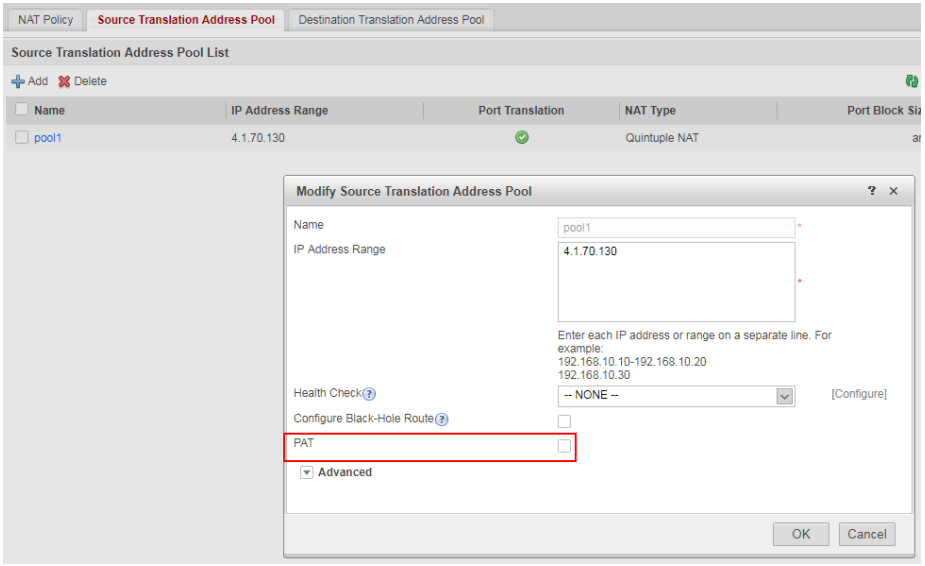
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

7 NAT

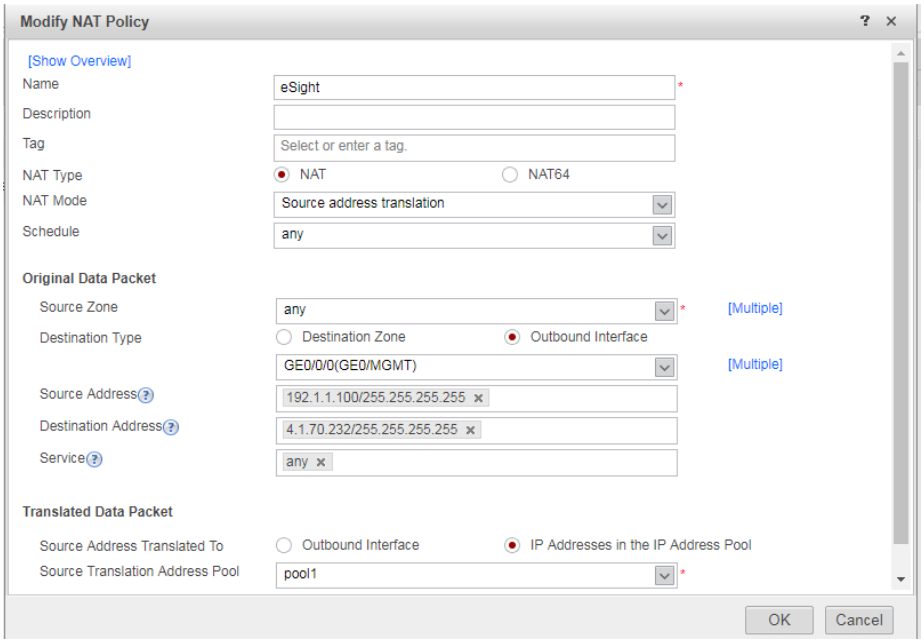
7.1 Source NAT

7.1.1 NAT NO-PAT

Objetivo de teste	Verify whether the equipment supports NAT NO-PAT function.
Especificação de teste	NAT No-PAT is one-to-one network address translation. The IP address will be translated and the port does not.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Configure the NAT Address Pool, and don’t select “PAT”;



2. Configure the NAT Policy, and reference the NAT Address Pool;



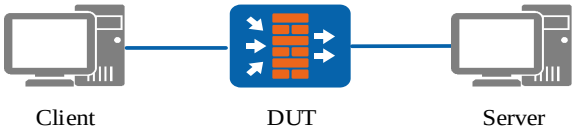
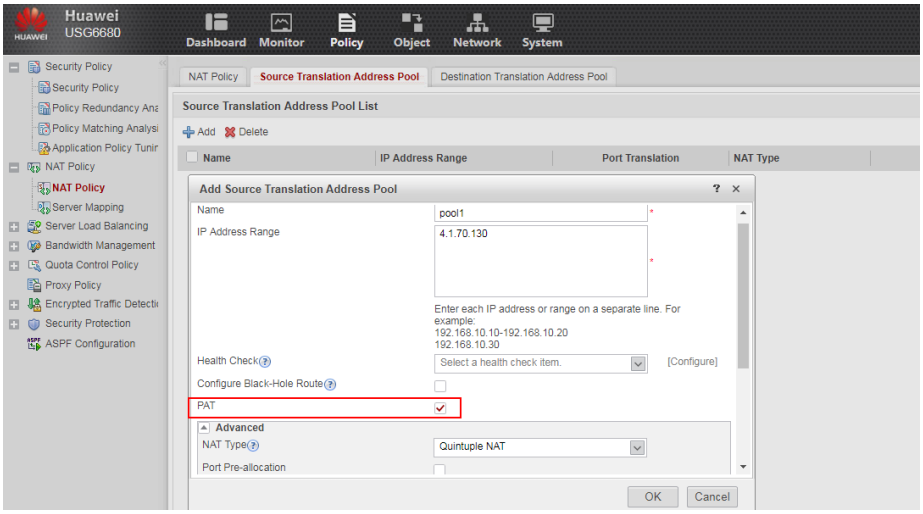
3. The Client visit the Server.

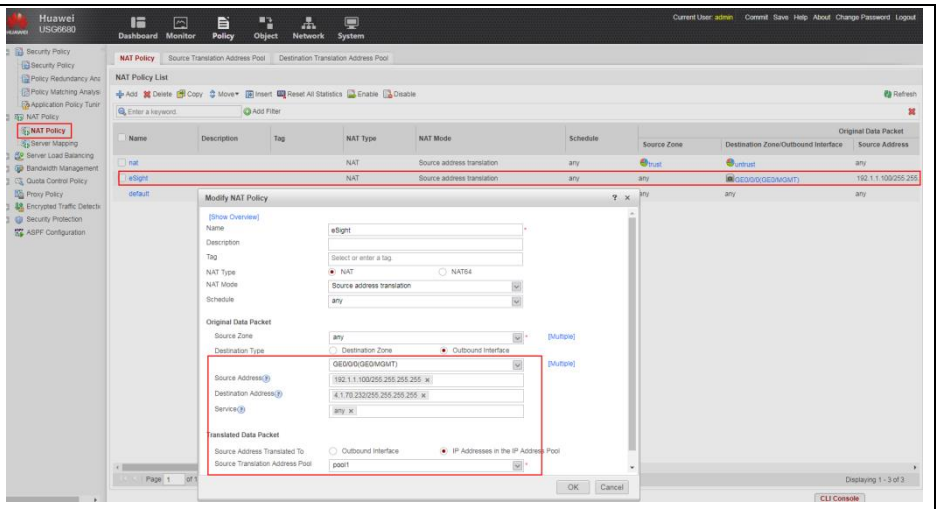
```
<USG6600>disp firewall  session table  source inside 192.1.1.100
2017-12-05 19:46:28.200 +08:00
 Current Total Sessions : 12
 HTTP  VPN: public --> public  192.1.1.100:49694[4.1.70.130:49694] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49691[4.1.70.130:49691] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49697[4.1.70.130:49697] --> 4.1.70.232:31942
 icmp  VPN: public --> public  192.1.1.100:19[4.1.70.130:19] --> 4.1.70.232:2048
 HTTP  VPN: public --> public  192.1.1.100:49695[4.1.70.130:49695] --> 4.1.70.232:31942
 SSL  VPN: public --> public  192.1.1.100:49680[4.1.70.130:49680] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49681[4.1.70.130:49681] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49692[4.1.70.130:49692] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49698[4.1.70.130:49698] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49699[4.1.70.130:49699] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49696[4.1.70.130:49696] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49693[4.1.70.130:49693] --> 4.1.70.232:31942
<USG6600>
```

Resultado Esperado	1. The Client can visit the Server; 2. Check the session on DUT. The source IP translate to the pool IP but the port does not.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA

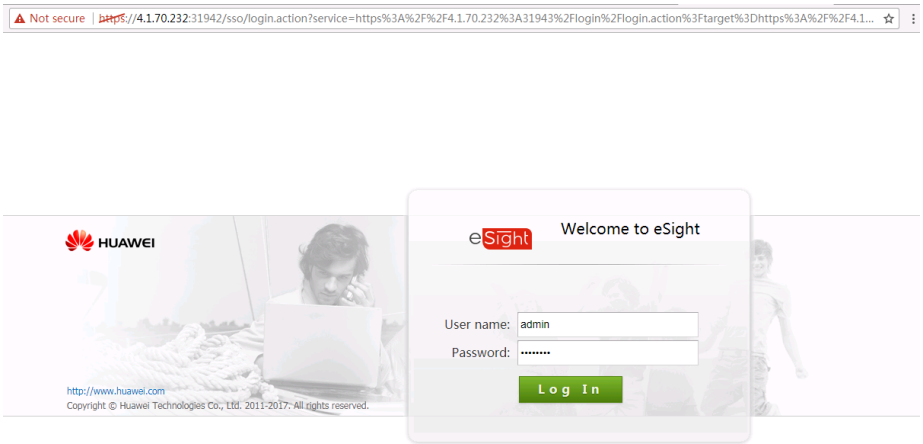
Observação				
Assinatura	**Cliente**		**Huawei**	

7.1.2 NAPT

Objetivo de teste	Verify whether the equipment supports NAPT function.
Especificação de teste	NAPT is many-to-one address translation and translates both IP addresses and port numbers.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Configure the NAT Address Pool, and select “PAT”;  2. Configure the NAT Policy, and reference the NAT Address Pool;



3. The Client visit the Server.




```
<USG6600>disp firewall  session table  source inside 192.1.1.100
2017-12-05 19:44:19.970 +08:00
 Current Total Sessions : 4
 HTTP  VPN: public --> public  192.1.1.100:49540[4.1.70.130:2090] --> 4.1.70.232:31942
 icmp  VPN: public --> public  192.1.1.100:19[4.1.70.130:2074] --> 4.1.70.232:2048
 HTTP  VPN: public --> public  192.1.1.100:49545[4.1.70.130:2095] --> 4.1.70.232:31942
 HTTP  VPN: public --> public  192.1.1.100:49544[4.1.70.130:2094] --> 4.1.70.232:31942
<USG6600>
```

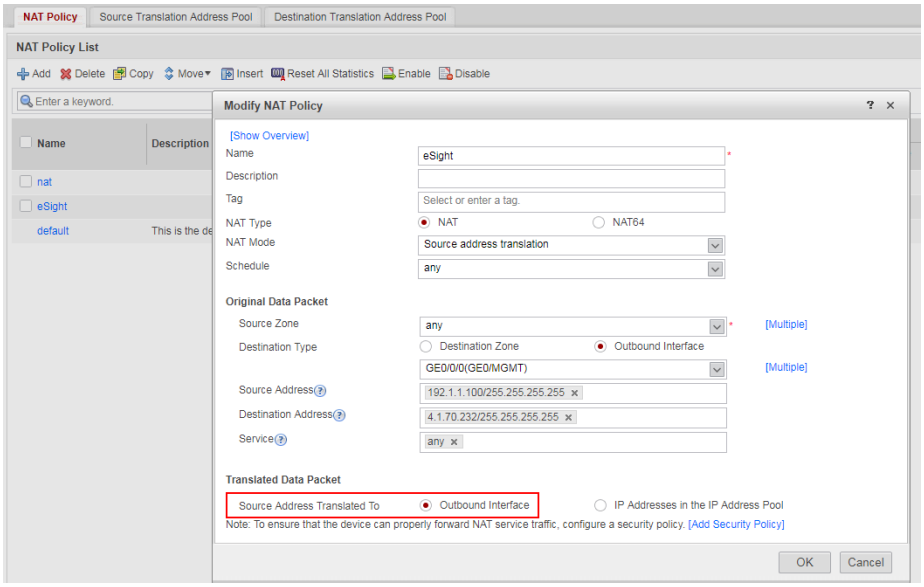
Resultado Esperado	1. The Client can visit the Server; 2. Check the session on DUT. The source IP translates to the pool IP and the port changes also.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

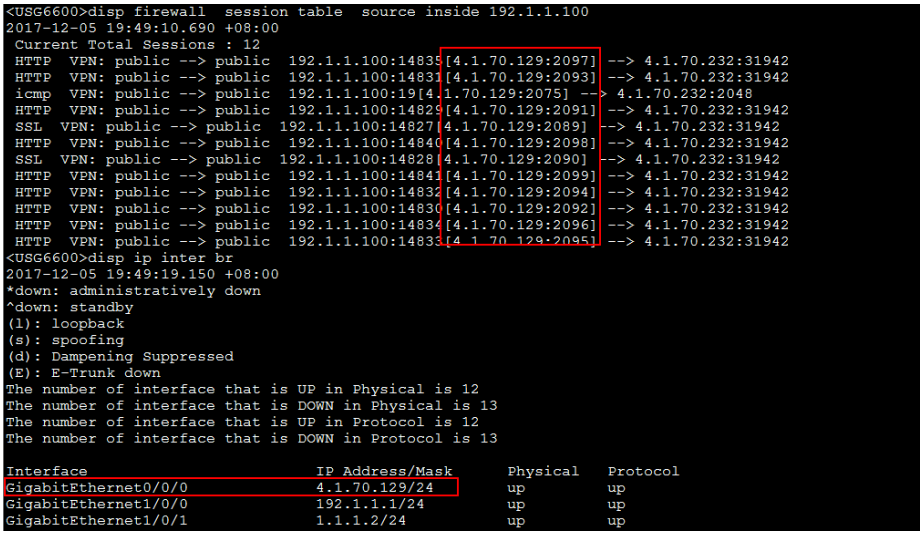
7.1.3 Easy-IP

Objetivo de teste	Verify whether the equipment supports Easy-IP function.
Especificação de teste	Easy IP mode translates private addresses into an IP address of a WAN interface, and does not require a NAT address pool. Easy IP translates both IP addresses and port numbers of packets. Source NAT in this mode translates both private

<table>
<tr><td></td><td>addresses and port numbers. Intranet users can share a single public IP address of a specific WAN interface.</td></tr>
<tr><td>Ambiente de teste</td><td>Test TOPO:

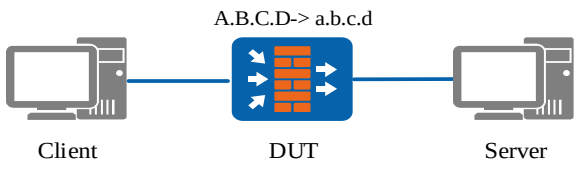
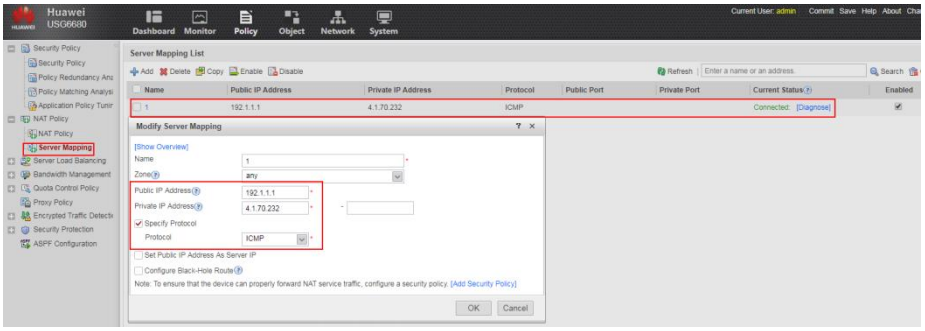
Client DUT Server

Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;
4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).</td></tr>
<tr><td>Procedimento de Teste</td><td>1. Configure the NAT Policy, and select the outbound interface IP address mode;
 

2. The Client visit the Server.

</td></tr>
</table>

Resultado Esperado	1. The Client can visit the Server; 2. Check the session on DUT. The source IP translates to the interface IP and the port change also.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

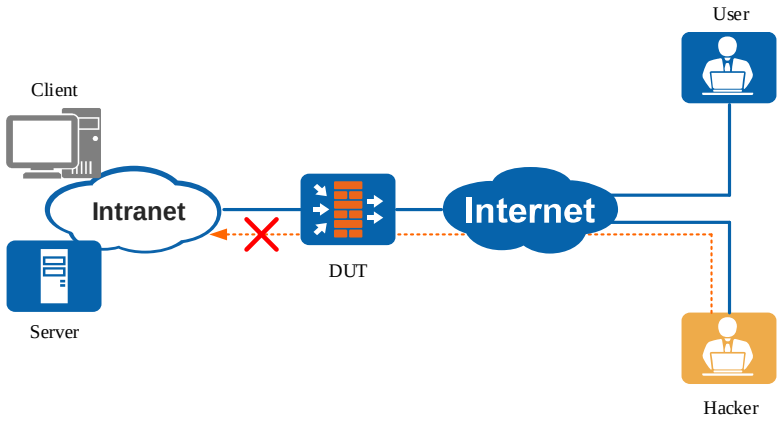
7.1.4 Destinaton NAT

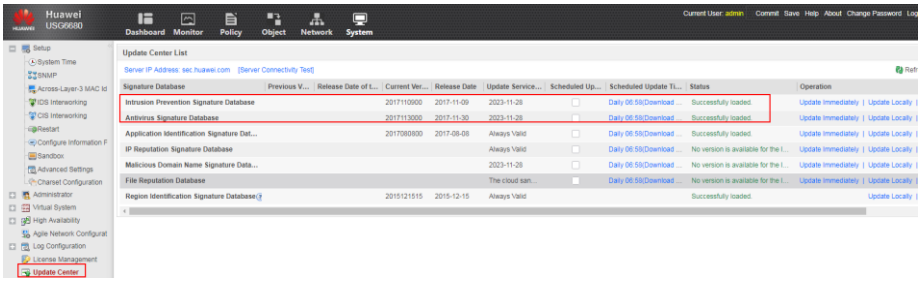
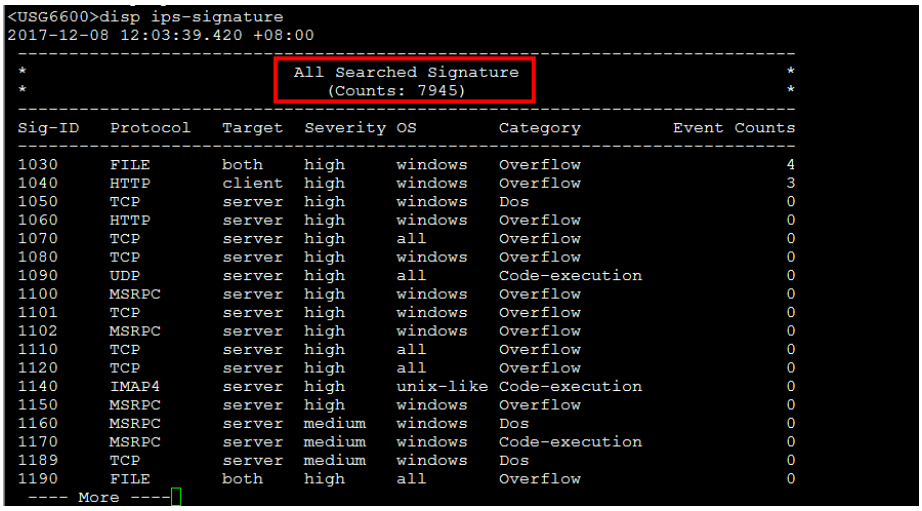
Objetivo de teste	Verify whether the equipment supports NAT server function.
Especificação de teste	NAT Server translates destination IP addresses for packets. The NAT Server function maps a public IP address to a single private address.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Configure the Server-Mapping policy. The virtual public IP A.B.C.D map in the real private IP a.b.c.d;  2. Client visit the public IP A.B.C.D;

	[c:\~]$ ping 192.1.1.1 正在 Ping 192.1.1.1 具有 32 字节的数据: 来自 192.1.1.1 的回复: 字节=32 时间=1ms TTL=127 来自 192.1.1.1 的回复: 字节=32 时间=1ms TTL=127 来自 192.1.1.1 的回复: 字节=32 时间=1ms TTL=127 来自 192.1.1.1 的回复: 字节=32 时间=1ms TTL=127 192.1.1.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 1ms, 最长 = 1ms, 平均 = 1ms [c:\~]$ <USG6600> <USG6600>disp firewall session table destination global 192.1.1.1 2017-12-05 20:13:59.000 +08:00 Current Total Sessions : 1 icmp VPN: public --> public 192.1.1.100:19 --> 192.1.1.1:2048[4.1.70.232:2048] <USG6600>
Resultado Esperado	1. The client visits the server successfully. Check the session table and the destination IP A.B.C.D translated the private IP a.b.c.d;
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

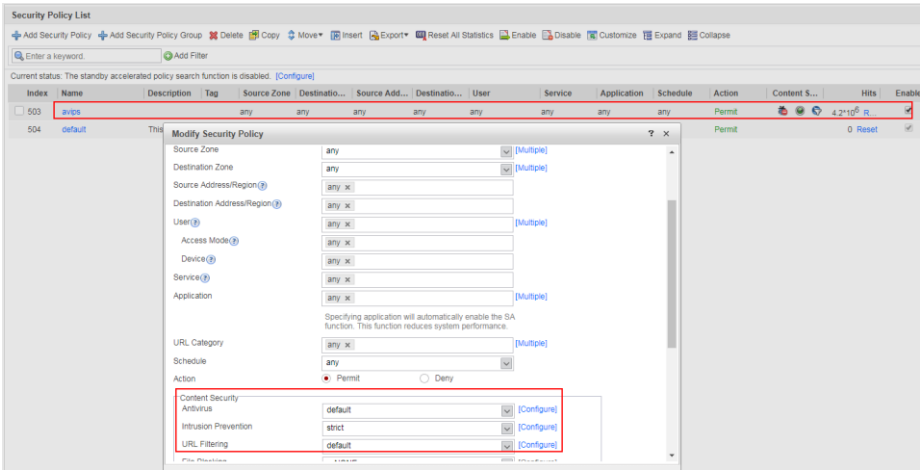
8 Content Security

8.1 Intrusion Prevention

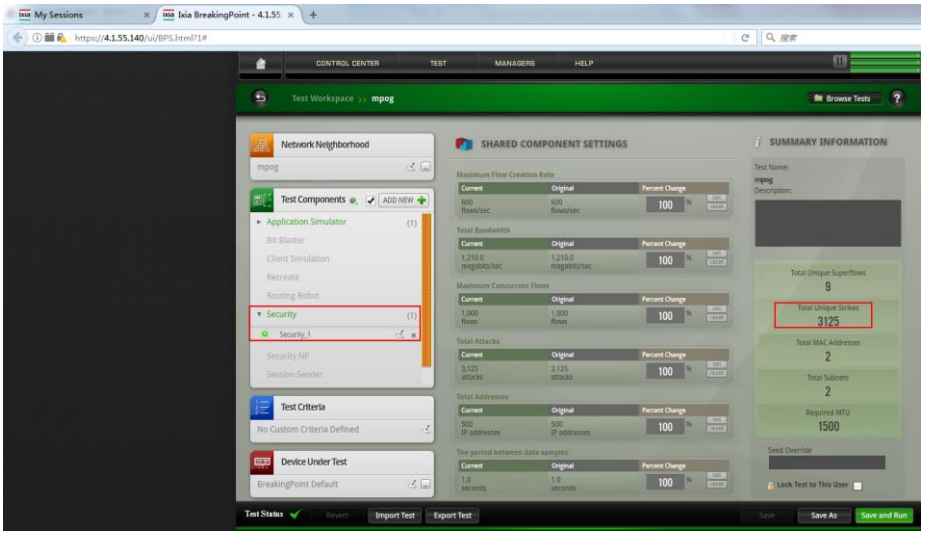
Objetivo de teste	Verify whether the equipment supports intrusion prevention.
Especificação de teste	Intrusion prevention detects intrusions, such as buffer overflow attacks, Trojan horses, and worms, by analyzing network traffic and takes actions to quickly terminate the intrusions.
Ambiente de teste	Test TOPO:  Pré-condição:

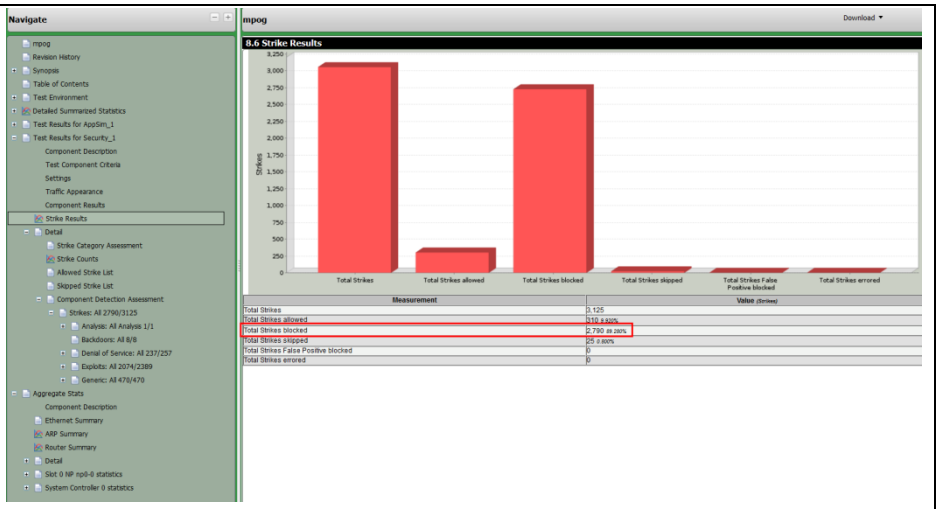
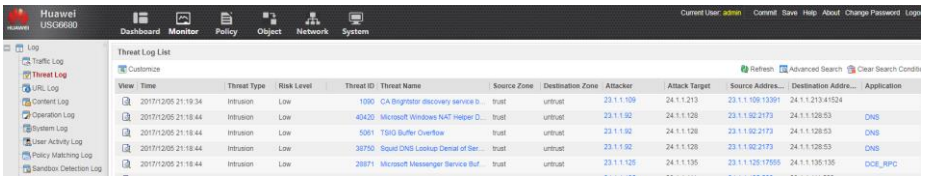
	1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Create intrusion prevention configuration file ***profile_ips_pc***, and configure the corresponding Assinatura filter (the configuration file will take effect after being committed); 2. Create intrusion prevention configuration file ***profile_ips_server***, and configure the corresponding Assinatura filter (the configuration file will take effect after being committed); 3. To make the intranet users immune to the attacks from the internet, configure security policy ***policy_sec_1*** and cite the intrusion prevention configuration file ***profile_ips_pc***; 4. To make the intranet server immune to the attacks from the internet or intranet users, configure security policy ***policy_sec_2*** and cite the intrusion prevention configuration file ***profile_ips_server***; 5. Construct intrusion attacks, and examine the threat log of the DUT. Update the IPS and AV Assinaturas:  Check the IPS Assinatura nums installed on FW: 

```
<USG6600>disp ips-signature
2017-12-08 12:03:39.420 +08:00
 ------------------------------------------------------------------------------
 *                        All Searched Signature                              *
 *                            (Counts: 7945)                                  *
 ------------------------------------------------------------------------------
 Sig-ID   Protocol   Target  Severity OS        Category         Event Counts
 ------------------------------------------------------------------------------
 1030     FILE       both    high     windows   Overflow                    4
 1040     HTTP       client  high     windows   Overflow                    3
 1050     TCP        server  high     windows   Dos                         0
 1060     HTTP       server  high     windows   Overflow                    0
 1070     TCP        server  high     all       Overflow                    0
 1080     TCP        server  high     windows   Overflow                    0
 1090     UDP        server  high     all       Code-execution              0
 1100     MSRPC      server  high     windows   Overflow                    0
 1101     TCP        server  high     windows   Overflow                    0
 1102     MSRPC      server  high     windows   Overflow                    0
 1110     TCP        server  high     all       Overflow                    0
 1120     TCP        server  high     all       Overflow                    0
 1140     IMAP4      server  high     unix-like Code-execution              0
 1150     MSRPC      server  high     windows   Overflow                    0
 1160     MSRPC      server  medium   windows   Dos                         0
 1170     MSRPC      server  medium   windows   Code-execution              0
 1189     TCP        server  medium   windows   Dos                         0
 1190     FILE       both    high     all       Overflow                    0
  ---- More ----
```

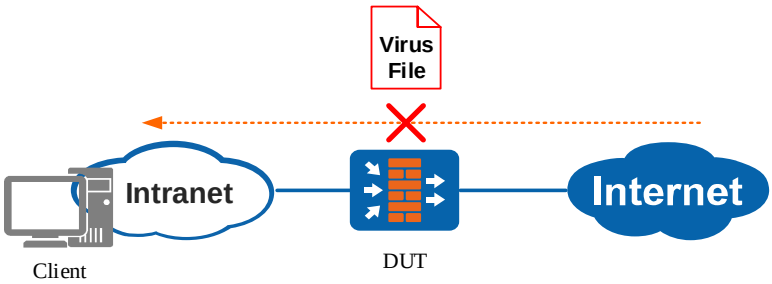


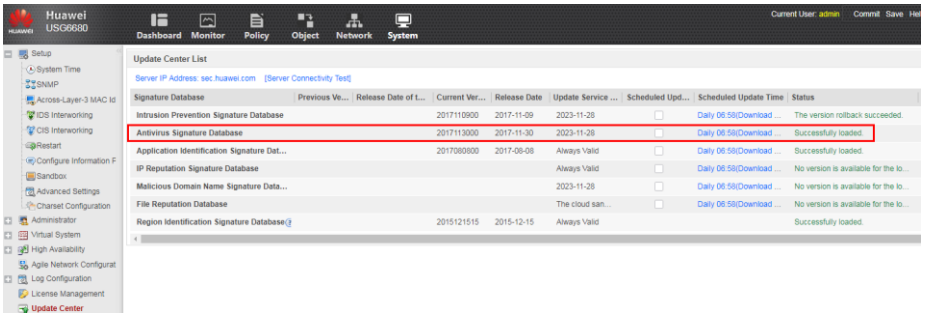
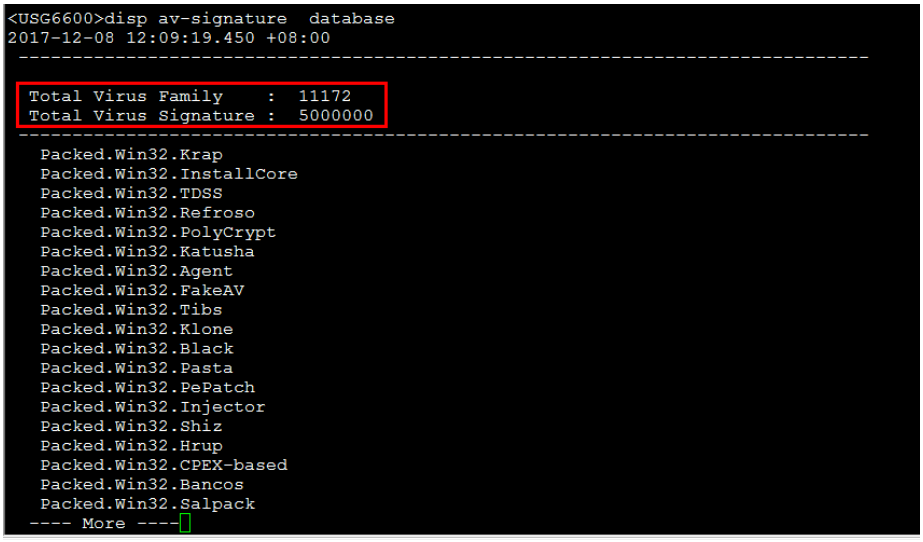
Use the tester to generate attacks towards firewall:

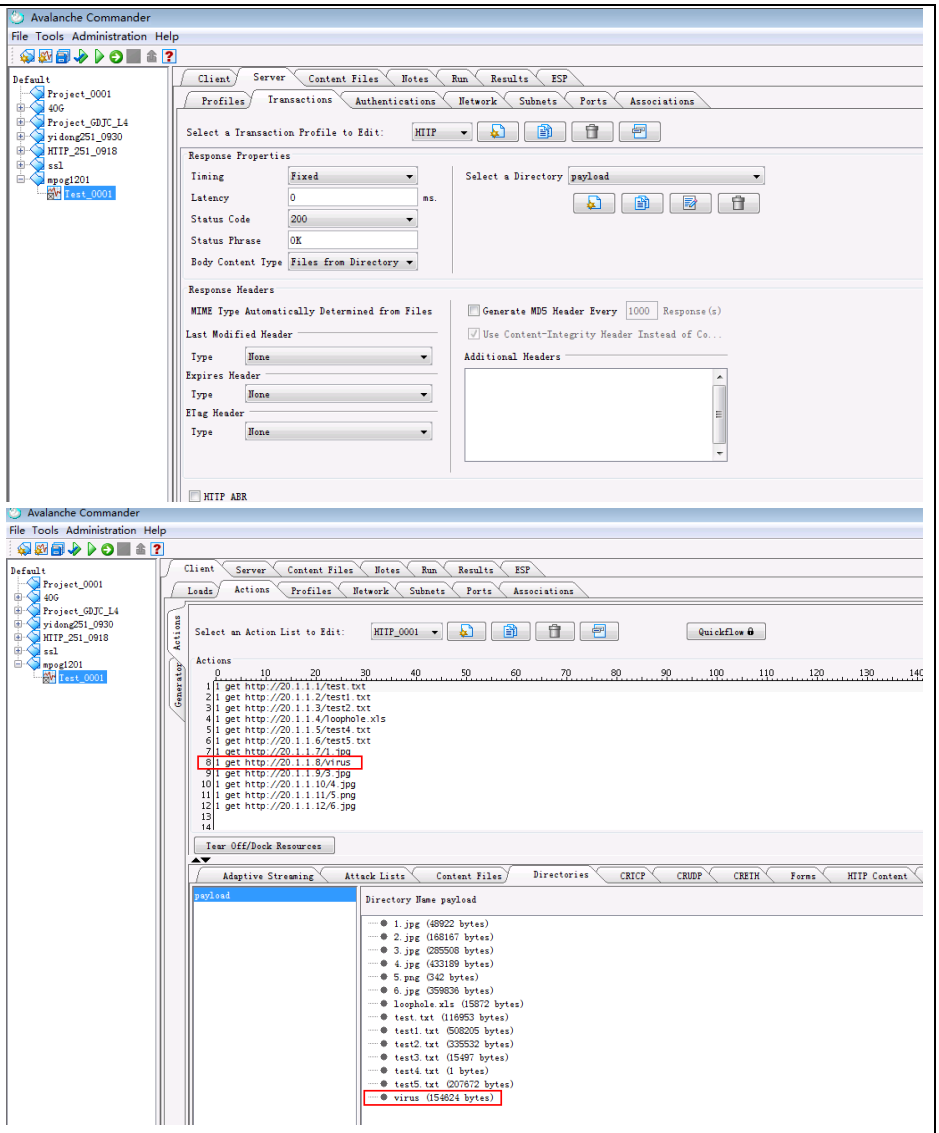


	 Check the logs: 
Resultado Esperado	1. After activating the intrusion prevention, the intrusion attacks will be blocked and DUT threat log will record the corresponding attacks, which proves that the equipment supports intrusion prevention.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

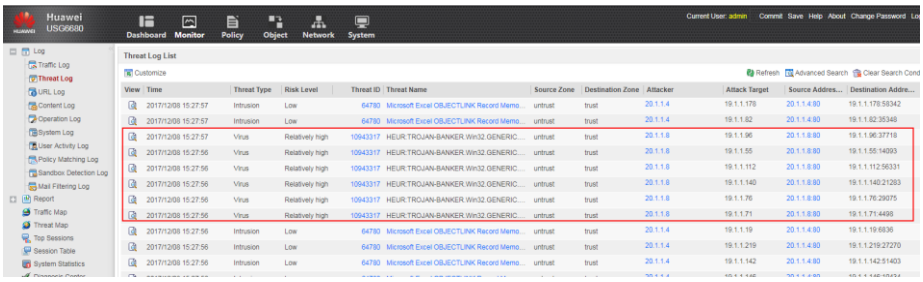
8.2 Anti Virus

Objetivo de teste	Verify whether the equipment supports antivirus.
Especificação de teste	Antivirus is a security mechanism that identifies and removes viruses to secure the network and prevent such problems as data corruption, permission escalation, and system crash.
Ambiente de teste	Test TOPO:  Pré-condição:

	1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Create antivirus configuration file ***profile_av_pc***, and configure the matching condition and responding action (the configuration file will take effect after being committed); 2. To make the intranet users immune to the attacks from the internet, configure security policy ***policy_sec_1*** and cite the antivirus configuration file ***profile_av_pc***; 3. Check interception situation on the DUT when intranet users download virus file, and examine the threat log of the DUT.  Check the AV Assinatura nums installed on FW:  Use the tester to generate virus files going across FW:



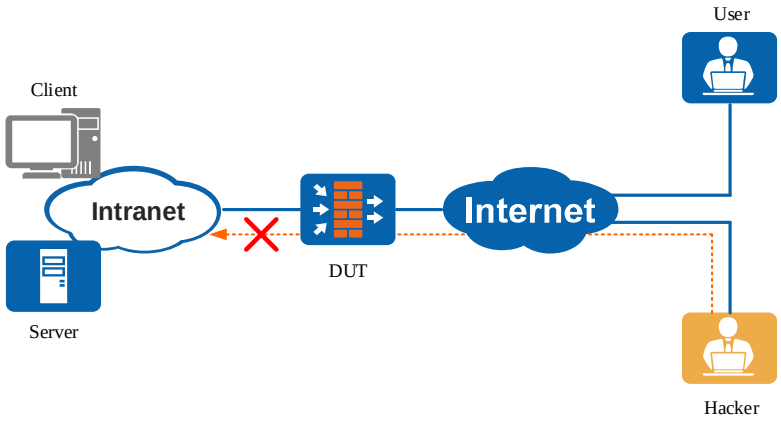
Check the anti-virus logs:



Resultado Esperado	1. After activating the antivirus, the virus file will be blocked and DUT threat log will record the corresponding attacks, which proves that the equipment supports antivirus.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

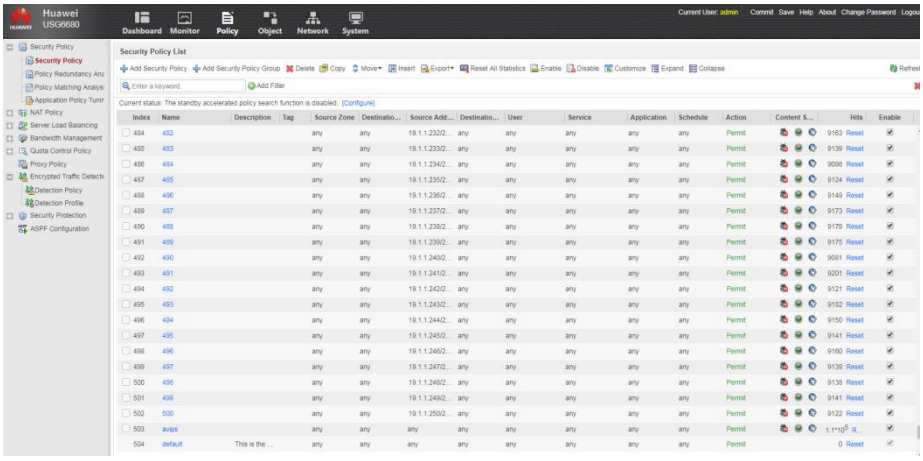
Assinatura	**Cliente**		**Huawei**	

8.3 Content Security Detection Based on SSL Encrypted Traffic

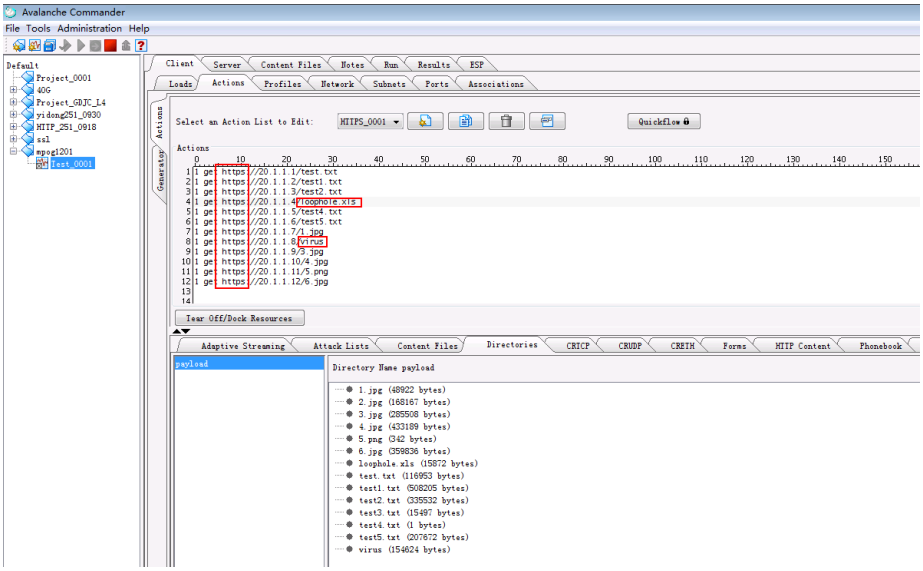
Objetivo de teste	Verify whether the equipment supports content security detection based on SSL encrypted traffic.
Especificação de teste	Security and privacy issues driving more and more network traffic began to use SSL encryption transmission equipment, if the device don't check and audit content security of encrypt SSL traffic (content security check including anti-virus, intrusion prevention, URL remote query, content filtering, file filtering and email filtering and auditing, etc.) , the encrypted SSL traffic will become a blind spot of security defense, it also provides an opportunity for illegal users to use the encryption characteristics of SSL for malicious network attacks. SSL encrypted traffic detection function is to decrypt the SSL encrypted traffic, and then to decrypt the traffic to do content security checks and audits.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Import server certificates and its private keys; 2. Configure the detection configuration file and select bi-directional detection; 3. Configure sophisticated SSL encryption traffic detection policies, which allow devices to decrypt traffic that needs to be checked for content security; 4. Configure proxy policy, citing TCP services and SSL decryption operations, to achieve the HTTPS traffic decryption; 5. Configure the security policy and cite the content security profile, then it can do a content security check on the decrypted traffic;

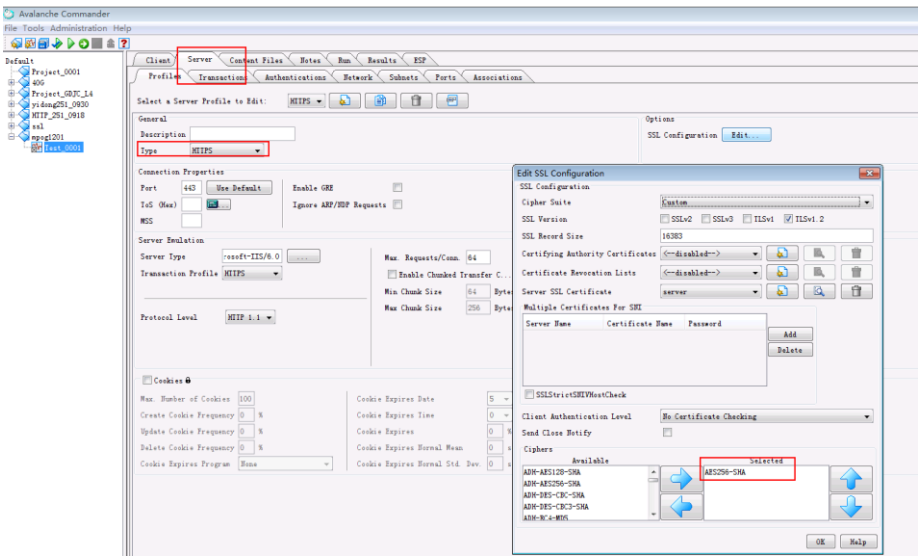
6. Transmit attack traffic by HTTPS between Client and Server, and then check the threat logs.

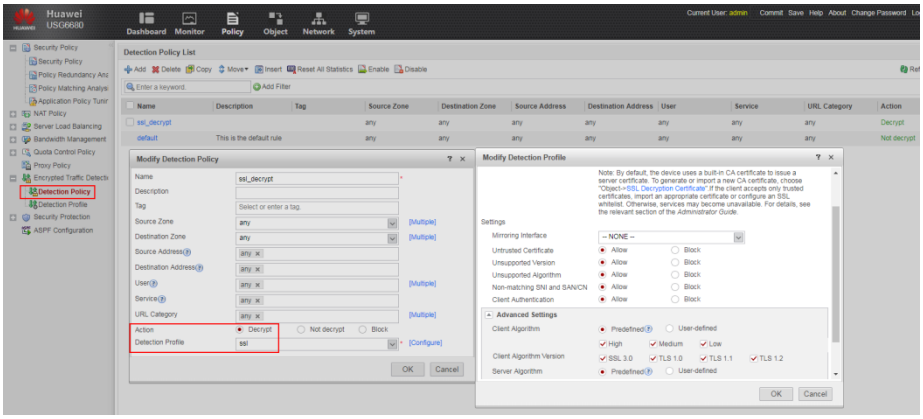
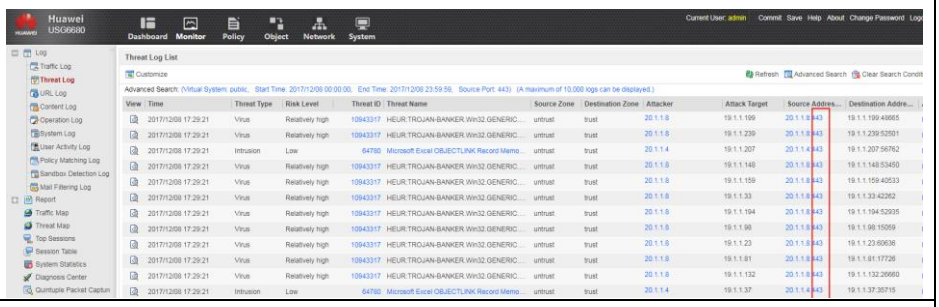
Configure security policy with IPS&AV function enabled:



Using https to transfer IPS and AV accrossing FW:



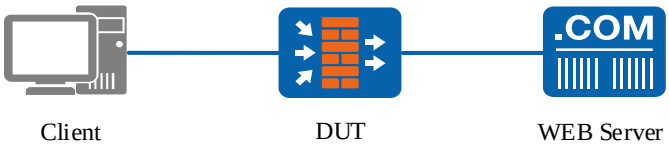


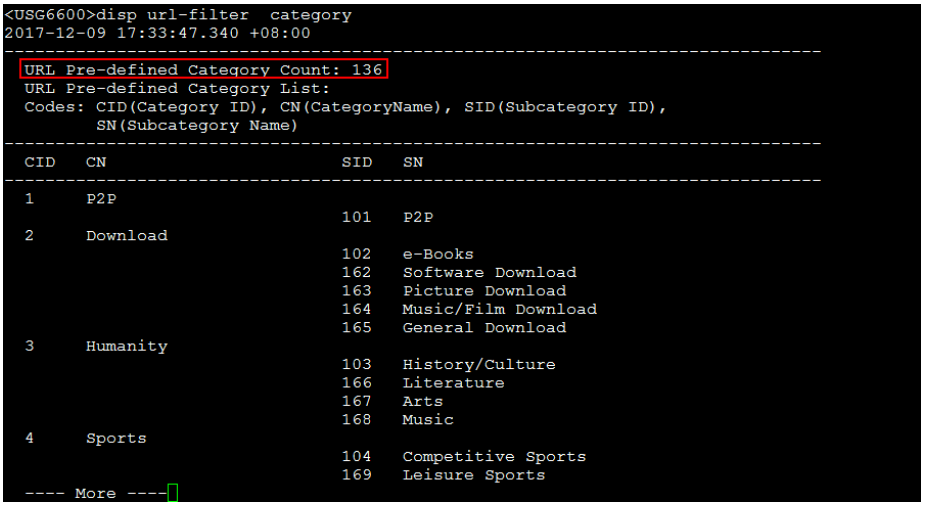
	Configure the SSL decryption policy:  After the HTTPS traffic was decrypted ,the IPS&AV can be detected and blocked by FW: 
Resultado Esperado	1. Through the SSL proxy, the Cliente can decrypt the HTTPS traffic, and then does the content security check and audit of the traffic after the decryption, corresponding attack logs come out.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

8.4 URL Filtering

8.4.1 HTTP Filtering

Objetivo de teste	Verify whether the equipment supports to filter HTTP URL.

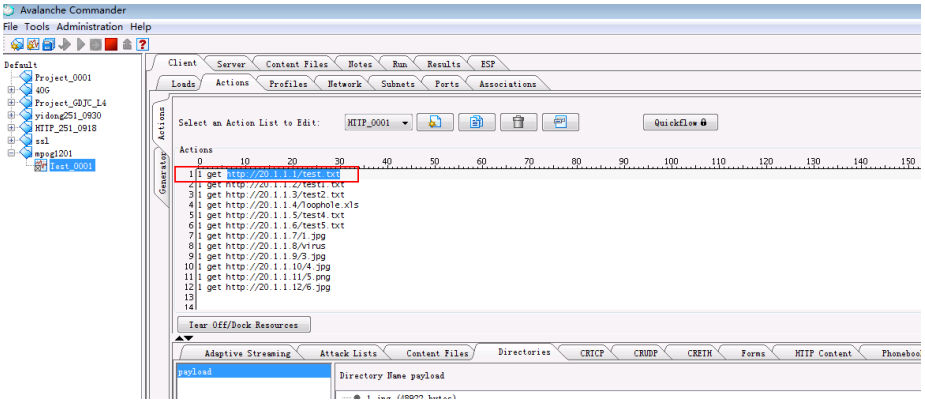
<table>
<tr><td>Especificação de teste</td><td>URL filtering regulates online behavior by controlling which URLs users can access.</td></tr>
<tr><td>Ambiente de teste</td><td>Test TOPO:
 

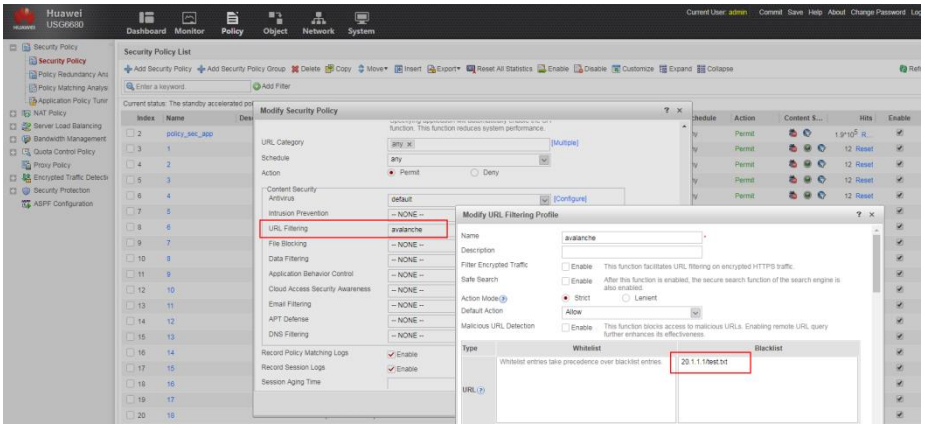
Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;
4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).</td></tr>
<tr><td>Procedimento de Teste</td><td>1. Create URL filtering configuration file profile_url_intrauser, configure the default action as blocking, add white list URL http://IP/news and black list URL http://IP/sports, and set the responding action of the pre-defined categories as blocking (the configuration file will take effect after being committed);
2. To realize the URL visiting control for intranet users, configure security policy policy_sec_1 and cite the URL filtering configuration file profile_url_intrauser;
3. Let intranet user make HTTP visits, and examine the URL log of the DUT.
Check the URL category nums:
 

Check the URL nums:</td></tr>
</table>

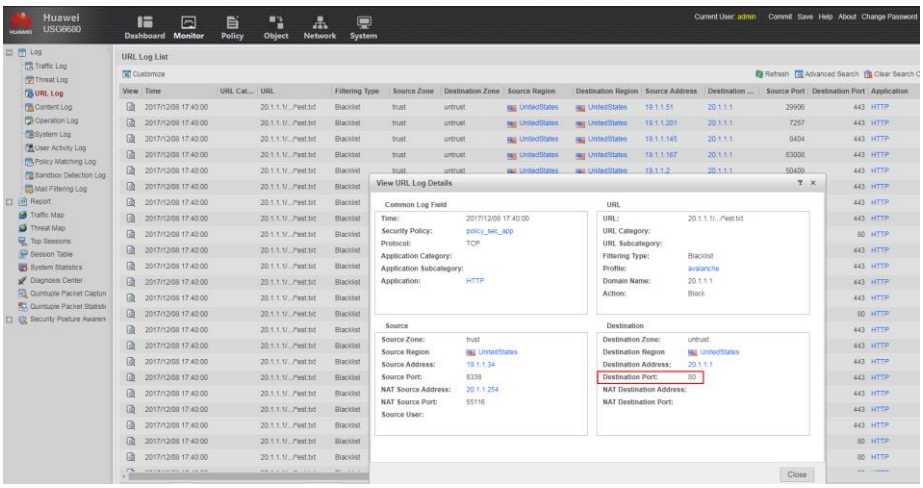
```
<USG6600>disp url-filter  statistics
2017-12-09 17:32:12.850 +08:00
  Statistics Information on slot 11 cpu 0:
-----------------------------------------------------------------------------
  Statistics Information:
-----------------------------------------------------------------------------
  Total HTTP Requests              : 908534
  Total Permitted HTTP Requests    : 781091
  Total Denied HTTP Requests       : 127443
  Matched Blacklist                : 127443
  Matched Whitelist                : 0
  Matched User-defined Category    : 0
  Matched Malicious URL            : 0
  Matched Pre-defined Category     : 0
  Matched Timeout Action           : 0
  Matched Default Action           : 781091
  Exception Packets Numbers        : 0
  Malicious URL Numbers            : 2
  Pre-defined Cache Hit Rate(%)    : 0
  Pre-defined URL Numbers          : 282359
-----------------------------------------------------------------------------
  Statistics Information on slot 12 cpu 0:
-----------------------------------------------------------------------------
  Statistics Information:
-----------------------------------------------------------------------------
  Total HTTP Requests              : 1603861
  Total Permitted HTTP Requests    : 1383383
  Total Denied HTTP Requests       : 220478
  Matched Blacklist                : 220478
  Matched Whitelist                : 0
  Matched User-defined Category    : 0
  Matched Malicious URL            : 0
  Matched Pre-defined Category     : 1
  Matched Timeout Action           : 0
  Matched Default Action           : 1383382
  Exception Packets Numbers        : 0
  Malicious URL Numbers            : 2
  Pre-defined Cache Hit Rate(%)    : 0
  Pre-defined URL Numbers          : 282359
-----------------------------------------------------------------------------
<USG6600>
```

Specitfy a URL to be blocked by URL filtering function on FW:



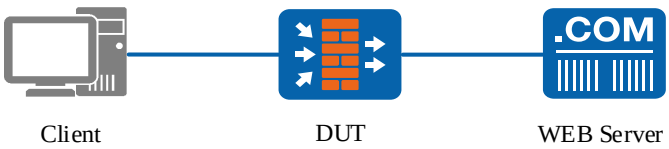


Check the URL blocking logs:

	
Resultado Esperado	1. After activating the HTTP filtering, the HTTP visits of white list URL is allowed and the ones of blacklist URL is blocked and DUT URL log will record the corresponding visits, which proves that the equipment supports HTTP filtering.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

Assinatura	**Cliente**		**Huawei**	

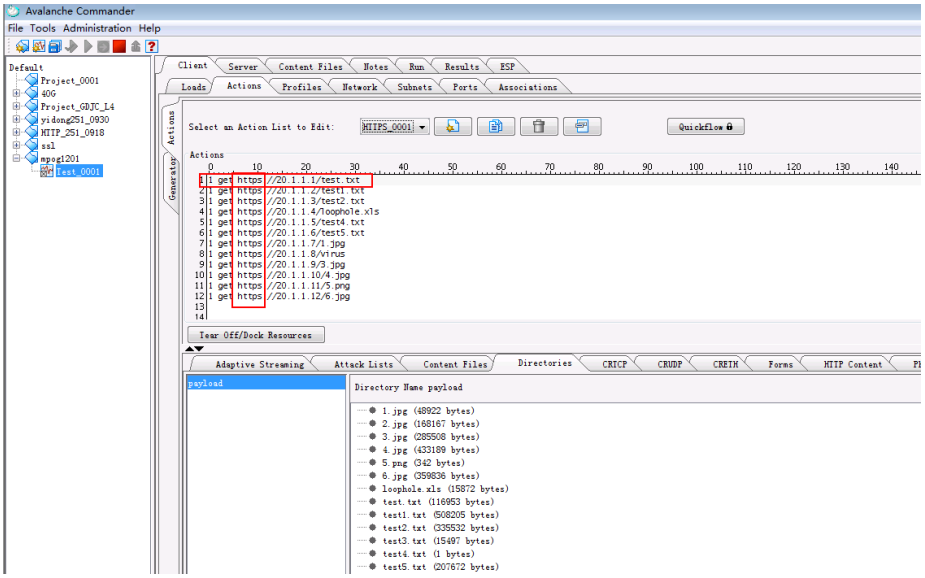
8.4.2 HTTPS Filtering

Objetivo de teste	Verify whether the equipment supports to filter HTTPS URL.
Especificação de teste	For HTTPS traffic, a proxy policy with the action of SSL decryption is required. URL filtering is performed for decrypted HTTPS traffic.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Create URL filtering configuration file ***profile_url_intrauser***, configure the default action as blocking, add white list URL ***https://IP/news*** and blacklist URL ***https://IP/sports***, and set the responding action of the pre-defined

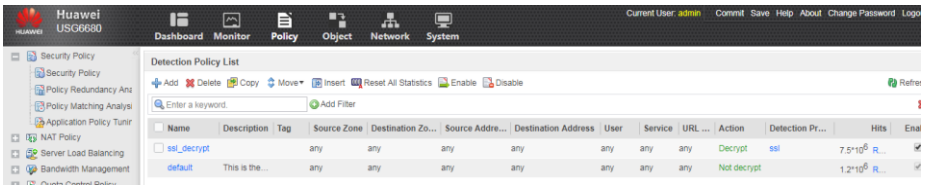
categories as blocking (the configuration file will take effect after being committed);

2. To realize the URL visiting control for intranet users, configure security policy ***policy_sec_1*** and cite the URL filtering configuration file ***profile_url_intrauser***;
3. Configure SSL decryption certificate, and install the trusted certificate into the intranet PC;
4. To realize the decryption of HTTPS visiting flow, configure proxy policy which cites TCP service and activates SSL decryption;
5. Let intranet user make HTTPS visits, and examine the URL log of the DUT.

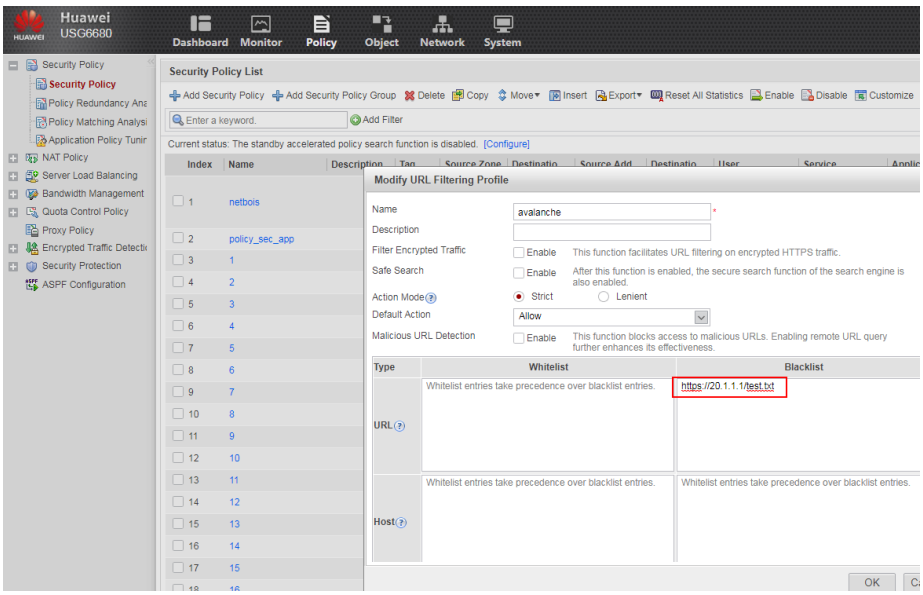
Generate HTTPS traffic by tester and specify a URL to be blocked by FW:



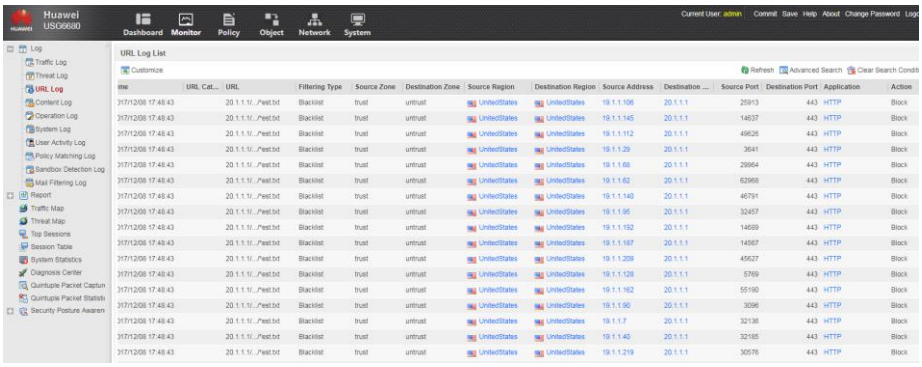
Configure SSL decryption policy:



Configure security policy with URL filtering function enabled:

<table>
<tr><td></td><td colspan="4">


After HTTPS traffic was decrypted, the specified URL can be blocked by FW:

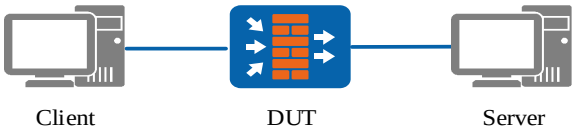
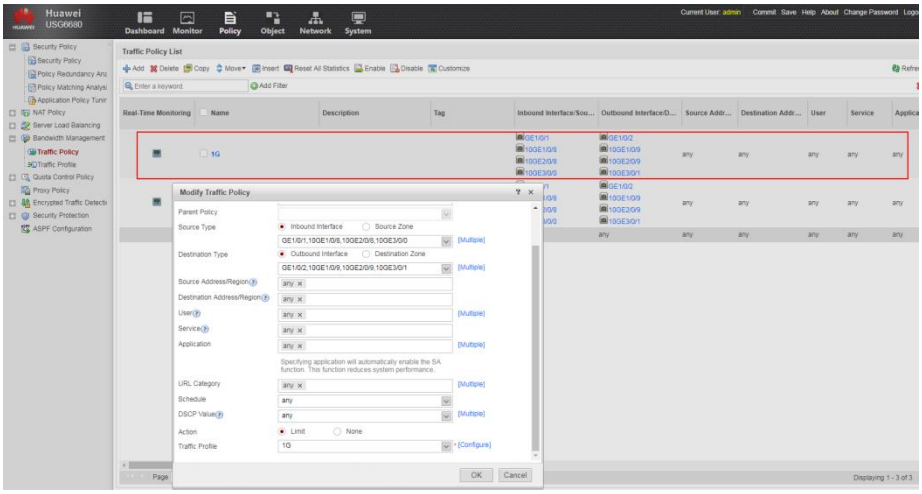


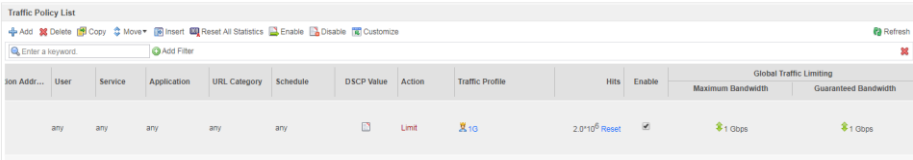
</td></tr>
<tr><td>Resultado Esperado</td><td colspan="4">1. After activating the HTTPS filtering, the HTTPS visits of white list URL is allowed and the ones of blacklist URL is blocked, and DUT URL log will record the corresponding visits, which proves that the equipment supports HTTPS filtering.</td></tr>
<tr><td>Resultado do Teste</td><td colspan="4">☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA</td></tr>
<tr><td>Observação</td><td colspan="4"></td></tr>
<tr><td>Assinatura</td><td>Cliente</td><td></td><td>Huawei</td><td></td></tr>
</table>

9 Traffic Management

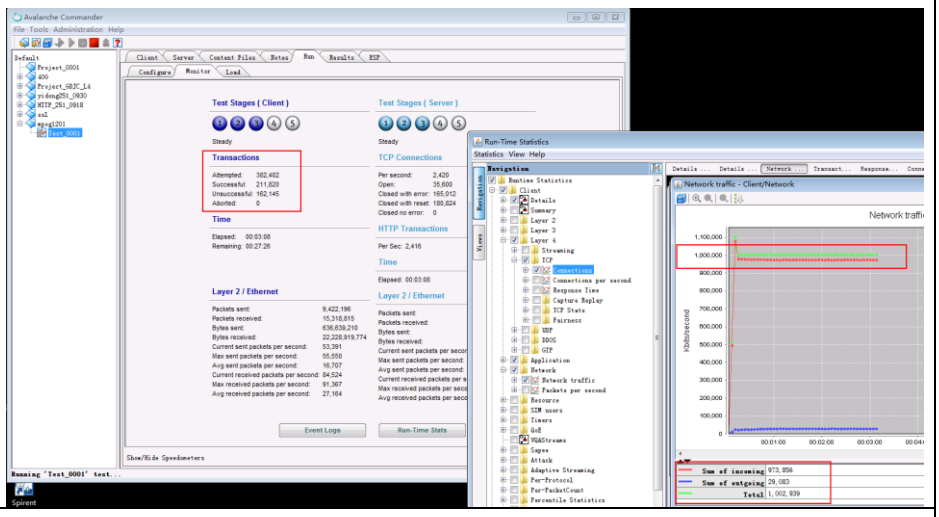
9.1 Bandwidth Management

9.1.1 Bandwidth Limitation

Objetivo de teste	Verify whether the equipment supports bandwidth management.
Especificação de teste	Limit the bandwidth of non-key services, in order to avoid these services which take up too much resource.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Add a new traffic profile, limit the max of uplink and downlink bandwidth as 1Gbps; 2. Add a new traffic policy, and quote the newly added traffic profile; 3. Visit the server through PC and download file form server, and view the speed of download. 

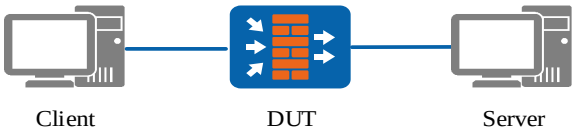
<table>
<tr><td></td><td colspan="4">


Using tester to generate more than 1Gbps traffic and check the bandwidth limitation effect:



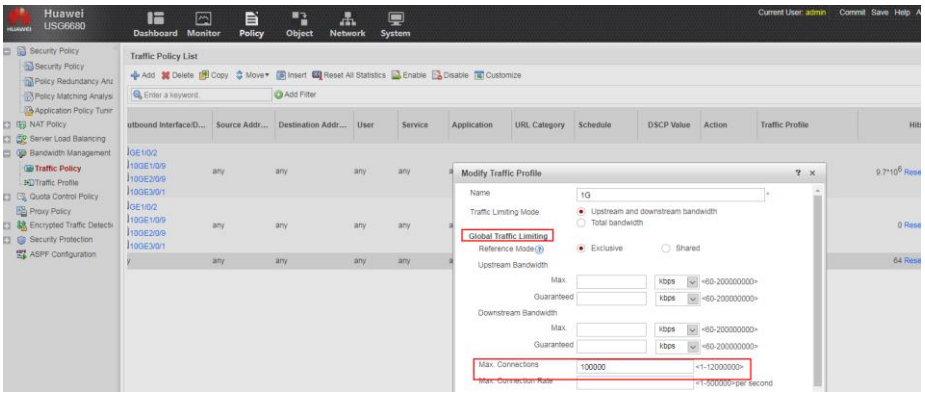
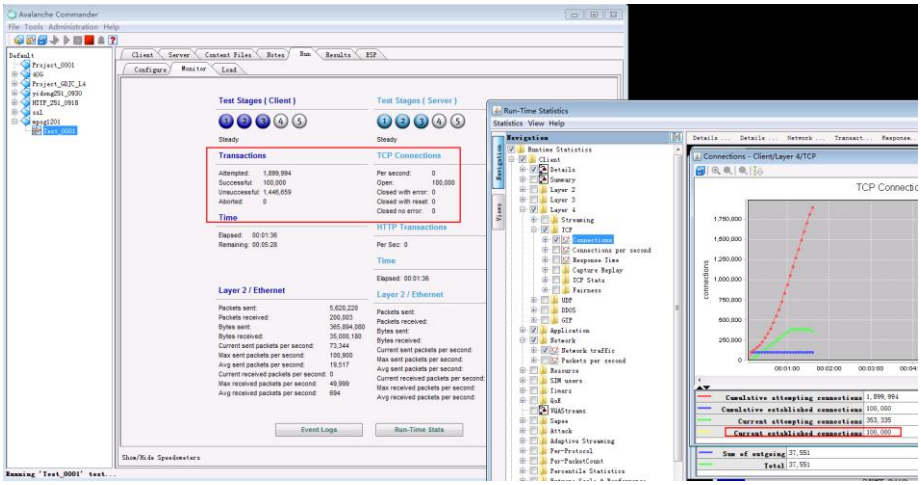
</td></tr>
<tr><td>Resultado Esperado</td><td colspan="4">1. The download rate is limited to 1Gbps and device supports the function of bandwidth limitation.</td></tr>
<tr><td>Resultado do Teste</td><td colspan="4">☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA</td></tr>
<tr><td>Observação</td><td colspan="4"></td></tr>
<tr><td>Assinatura</td><td>Cliente</td><td></td><td>Huawei</td><td></td></tr>
</table>

9.1.2 Concurrent Limitation

<table>
<tr><td>Objetivo de teste</td><td>Verify whether the equipment supports concurrent limitation.</td></tr>
<tr><td>Especificação de teste</td><td>The maximum number of all connections and the maximum number of source-IP-address-specific or user-specific connections can be set in a traffic profile.</td></tr>
<tr><td>Ambiente de teste</td><td>Test TOPO:
 

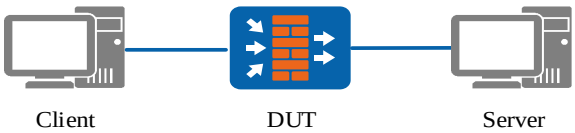
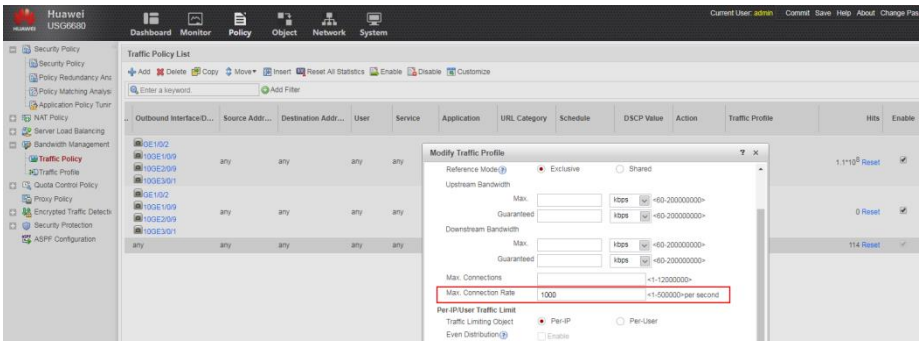
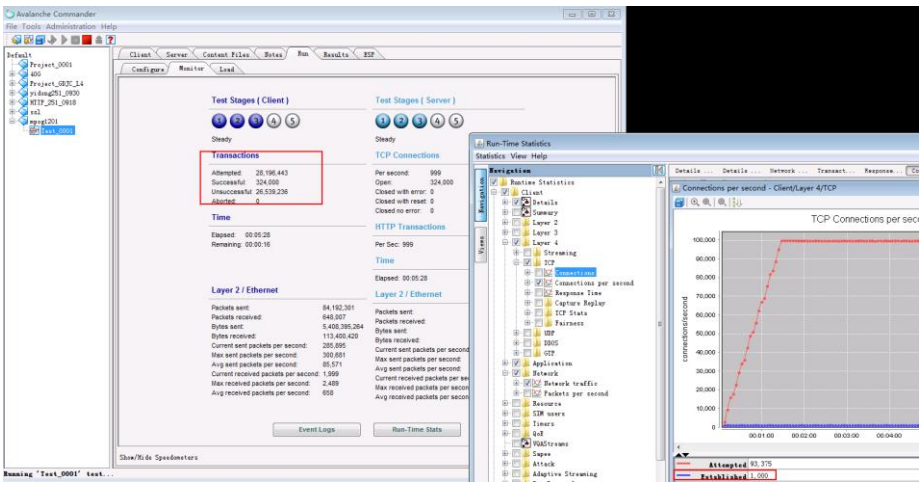
Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;</td></tr>
</table>

	4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).

Procedimento de Teste	1. Set the concurrent session number is 100,000 in bandwidth policy;
	2. The client sends more than 100,000 sessions to the server. Check the session on DUT.
	 
	 
	`<USG6600>d f s s a`
	`Session Statistics:`
	`Slot 11 cpu 0:  100000`
	`Total 100000 [0.83%] session(s) on all slots.`
	
	`Session Creation Rate(num/s):`
	`Slot 11 cpu 0:  0`
	`Total session(s) creation rate on all slots is 0.`
	
	`Max Session Statistics:`
	`Slot 11 cpu 0: 2400017, time:2017/12/11 12:07:58`
	`Total max session(s) on all slot is 2400017, time is 2017/12/11 12:07:58.`
	
	`Max Session Creation Rate(num/s):`
	`Slot 11 cpu 0:  130585, time:2017/12/11 09:29:40`
	`Total max session(s) creation rate on all slot is 130585, time is 2017/12/11 09:29:40.`
	
	`<USG6600>`

Resultado Esperado	1. The concurrent number of specific user is same as the configuration value 10.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
>	**Cliente** | | **Huawei** |

9.1.3 New Connections Limitation

Objetivo de teste	Verify whether the equipment supports new connection limitation.
Especificação de teste	The maximum number of service connections can be set to ensure efficient use of session resources and prevent a specific service from overusing bandwidth resources.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Set the connect rate number is 1000/s in bandwidth policy; 2. The client sends traffic to the server. Check the session connect rate on DUT.  

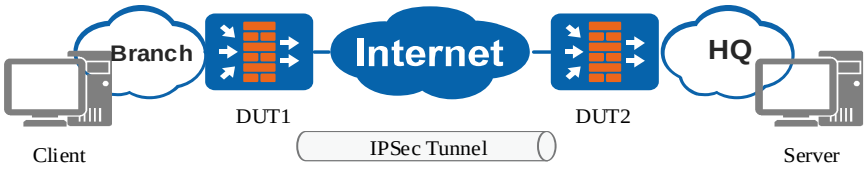
```
[USG6600]disp firewall session statistics all
 Session Statistics:
 Slot 11 cpu 0:  308015
 Total 308015 [2.57%] session(s) on all slots.

 Session Creation Rate(num/s):
 Slot 11 cpu 0:    1000
 Total session(s) creation rate on all slots is 1000.

 Max Session Statistics:
 Slot 11 cpu 0: 2400017, time:2017/12/11 12:07:58
 Total max session(s) on all slot is 2400017, time is 2017/12/11 12:07:58.

 Max Session Creation Rate(num/s):
 Slot 11 cpu 0:  130585, time:2017/12/11 09:29:40
 Total max session(s) creation rate on all slot is 130585, time is 2017/12/11 09:29:40.

[USG6600]disp fire sess ta
 Current Total Sessions : 310000
 HTTP  VPN: public --> public  19.1.1.237:1130[20.1.1.132:19156] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.247:60569[20.1.1.112:10379] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.198:53463[20.1.1.125:29084] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.201:3377[20.1.1.119:34024] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.176:25833[20.1.1.145:32333] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.169:37150[20.1.1.143:52237] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.25:49958[20.1.1.119:42018] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.77:13020[20.1.1.143:25006] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.155:41356[20.1.1.139:44778] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.198:24404[20.1.1.125:40947] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.236:64294[20.1.1.102:23865] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.159:39259[20.1.1.101:30996] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.78:35067[20.1.1.149:64560] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.87:21803[20.1.1.126:18211] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.15:37845[20.1.1.100:59387] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.188:25752[20.1.1.121:51214] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.38:20505[20.1.1.111:42789] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.53:48193[20.1.1.110:52090] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.213:39288[20.1.1.137:23021] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.227:20279[20.1.1.136:61427] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.56:20069[20.1.1.122:61953] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.250:11925[20.1.1.107:51781] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.10:56519[20.1.1.111:29241] --> 20.1.1.4:80
  ---- More ----
```

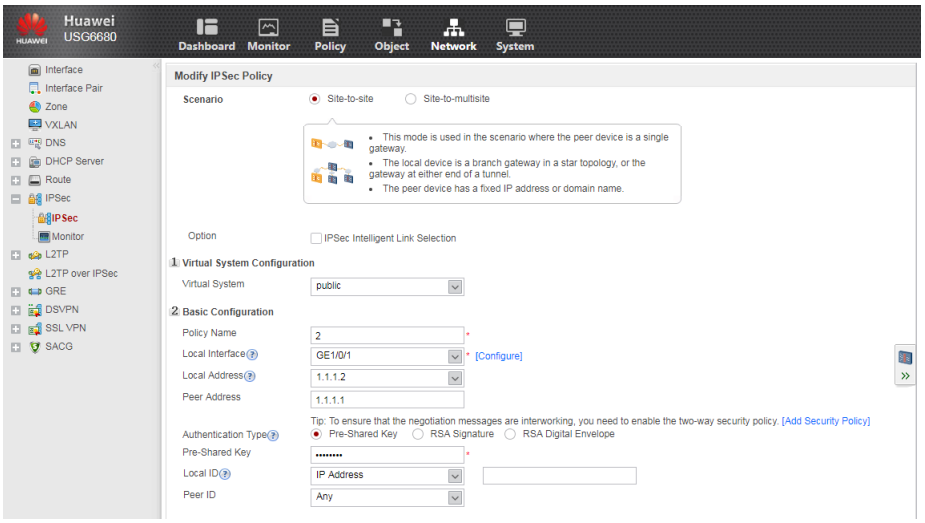
Resultado Esperado	1. The connect rate number of specific user is same as the configuration value 100/s.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

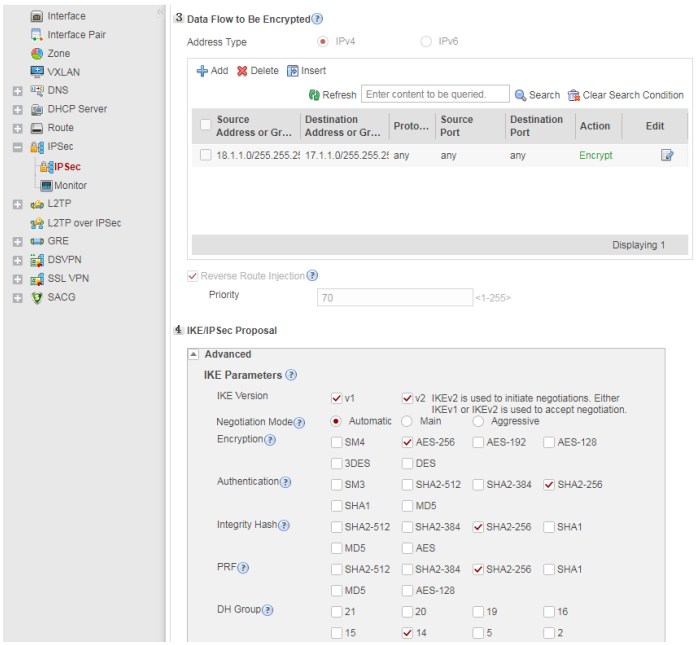
Assinatura	**Cliente**		**Huawei**	

10 VPN

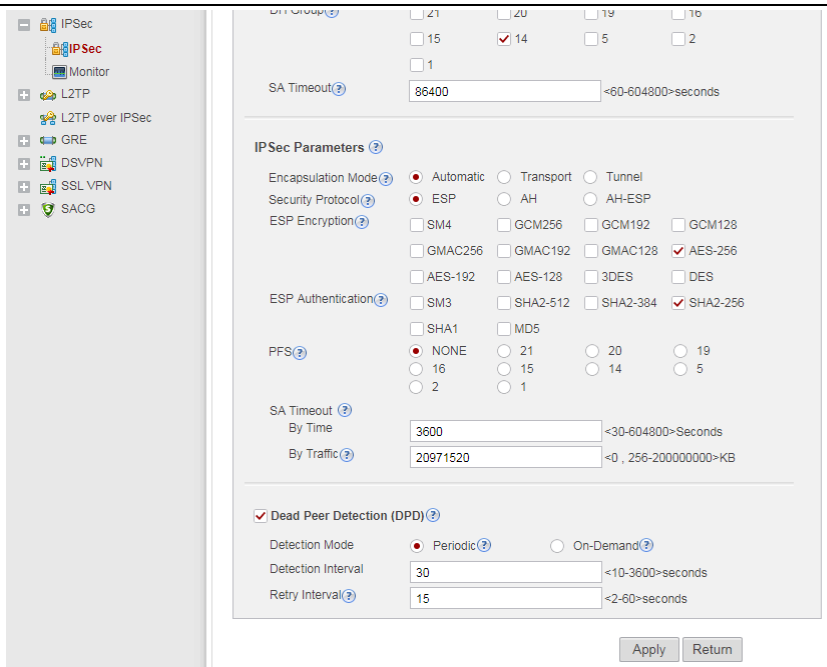
10.1 IPSec VPN

Objetivo de teste	Verify whether the equipment supports IPSec pre-share key mode.
Especificação de teste	Pre-shared key (PSK) authentication: An authentication key is used to generate a key. The two peers compute the hash value of packets using a shared key and check whether they obtain the same hash value. If they obtain the same hash value, the authentication succeeds. Otherwise, the authentication fails.
Ambiente de teste	Test TOPO: 

<table>
<tr>
<td></td>
<td>Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;
4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).</td>
</tr>
<tr>
<td>Procedimento de Teste</td>
<td>1. Set the IPSec application circumstance as site to site access;
2. Finish the basic configuration of IPSec, in which, choose the pre-share key authentication mode;
 

3. Define the corresponding ACL rules for the flow to be encrypted;
 

4. Configure the IKE and IPSec negotiation parameters of the security proposal, and it is preferable to use the default configuration;</td>
</tr>
</table>

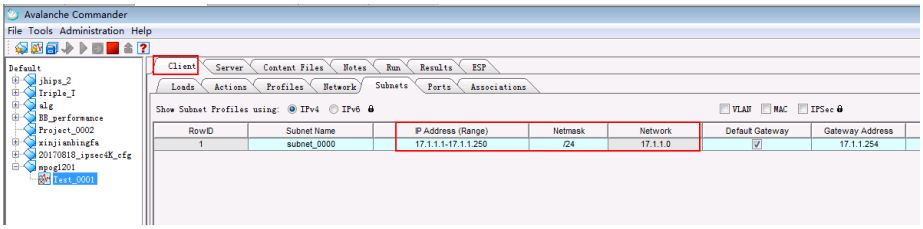


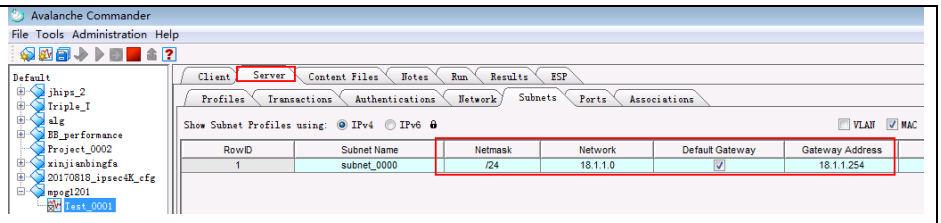
5. Client side visits the Server side.

```
<USG6600>disp ike sa
2017-12-08 12:27:58.980 +08:00

IKE SA information :
   Conn-ID    Peer                                        VPN                          Flag(s)              Phase
  -----------------------------------------------------------------------------------------------------------------
   150994982  1.1.1.1:500                                                               RD|A                 v2:2
   150994949  1.1.1.1:500                                                               RD|A                 v2:1

  Number of IKE SA : 2
  -----------------------------------------------------------------------------------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

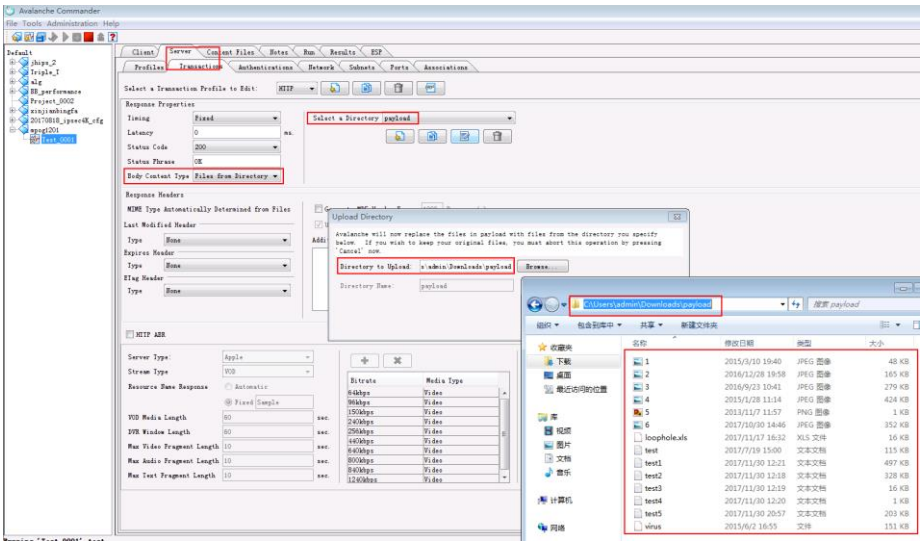
```
<USG6600>disp ipsec sa
2017-12-08 12:19:44.010 +08:00

ipsec sa information:

===============================
Interface: GigabitEthernet1/0/1
===============================

  ----------------------------
  IPSec policy name: "ipsec5121018198"
  Sequence number  : 1
  Acl group        : 3002
  Acl rule         : 5
  Mode             : ISAKMP
  ----------------------------
    Connection ID     : 150994976
    Encapsulation mode: Tunnel
    Holding time      : 0d 2h 14m 52s
    Tunnel local      : 1.1.1.2:500
    Tunnel remote     : 1.1.1.1:500
    Flow source       : 18.1.1.0/255.255.255.0 0/0
    Flow destination  : 17.1.1.0/255.255.255.0 0/0

    [Outbound ESP SAs]
      SPI: 196843124 (0xbbb9674)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
      SA remaining key duration (kilobytes/sec): 20891670/3596
  ---- More ----
```

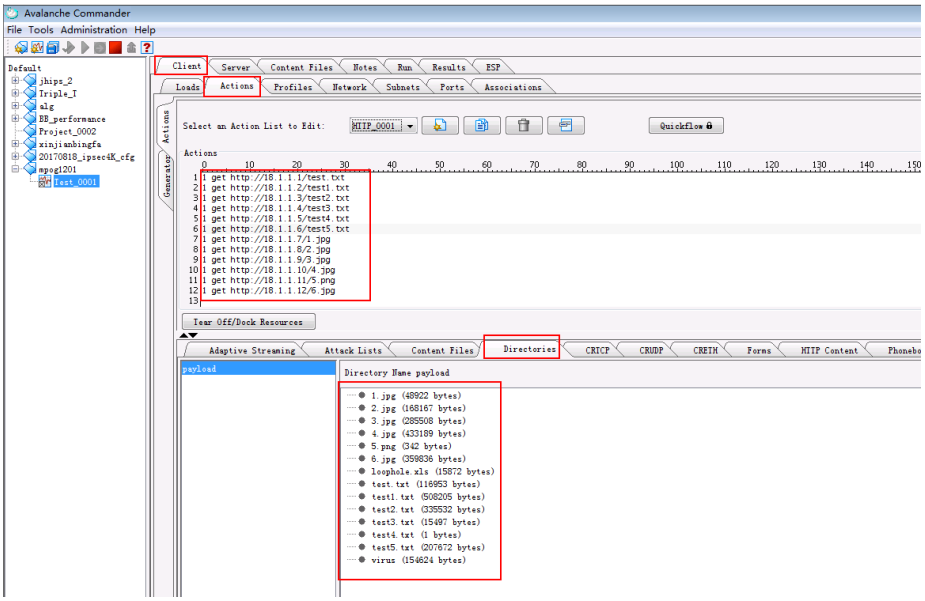
Using tester to generate traffic to be encrypted according to IPSec ACL rules:

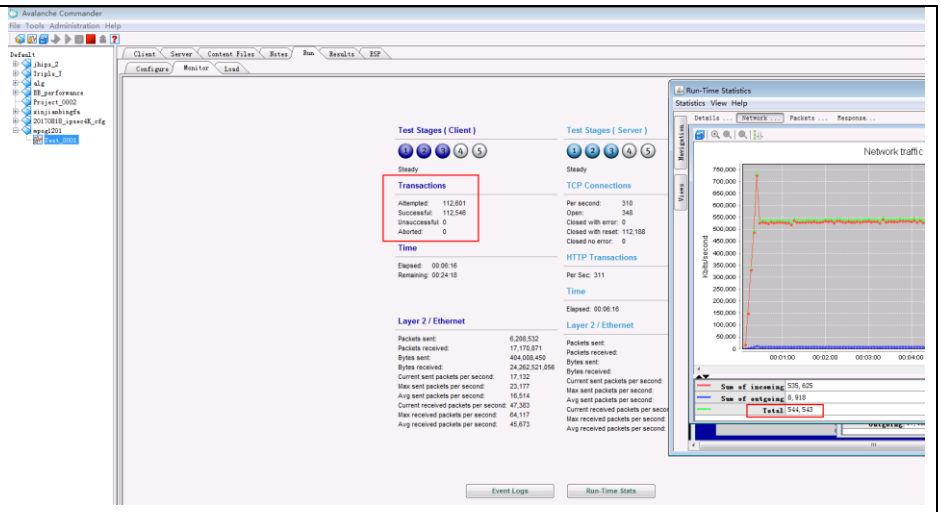
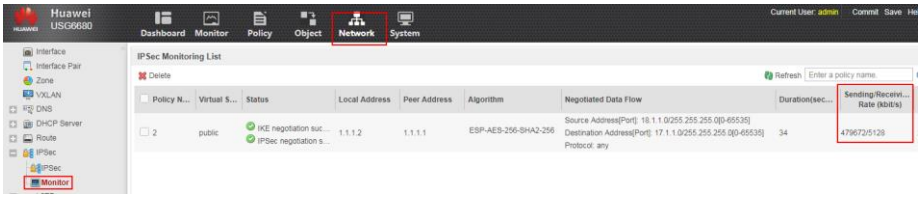




Configure variable content with images and texts, variable size 100 bytes to 500 Kbytes:



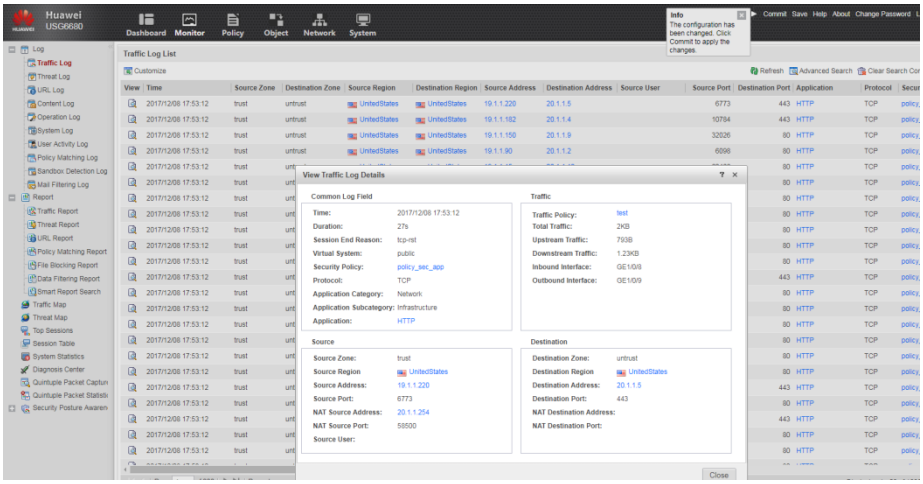


	 Check the IPSec traffic on FW: 
Resultado Esperado	1. The IPSec tunnel is negotiated successfully and the Client is able to visit the Server across the established tunnel, which proves that the equipment support IPSec tunnel negotiation via pre-share key authentication.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

10.2 Logs&Reports

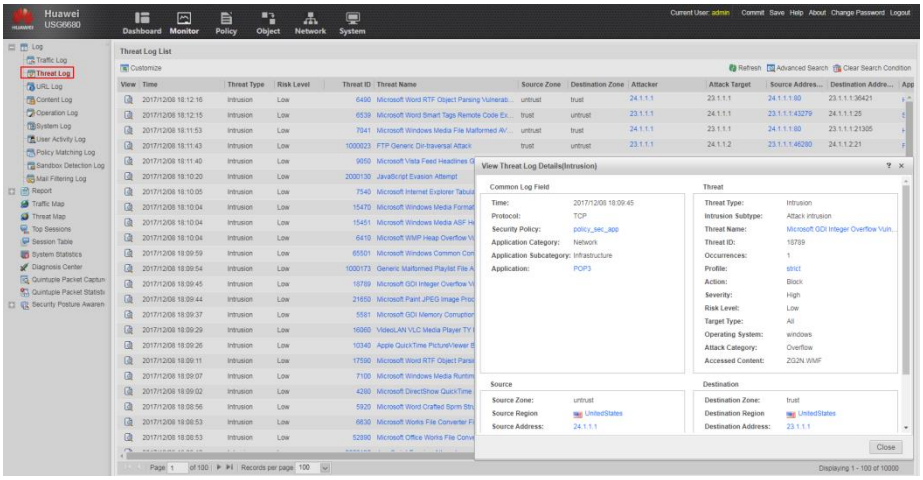
10.2.1 Traffic Log

Objetivo de teste	Verify whether the equipment supports to check traffic log.
Especificação de teste	Traffic logs provide visibility into traffic Assinaturas, bandwidth usage, and how the configured security and bandwidth policies have been applied.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar

	todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Login the device via WEB to view the traffic log. 
Resultado Esperado	1. Device supports the function of traffic log.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

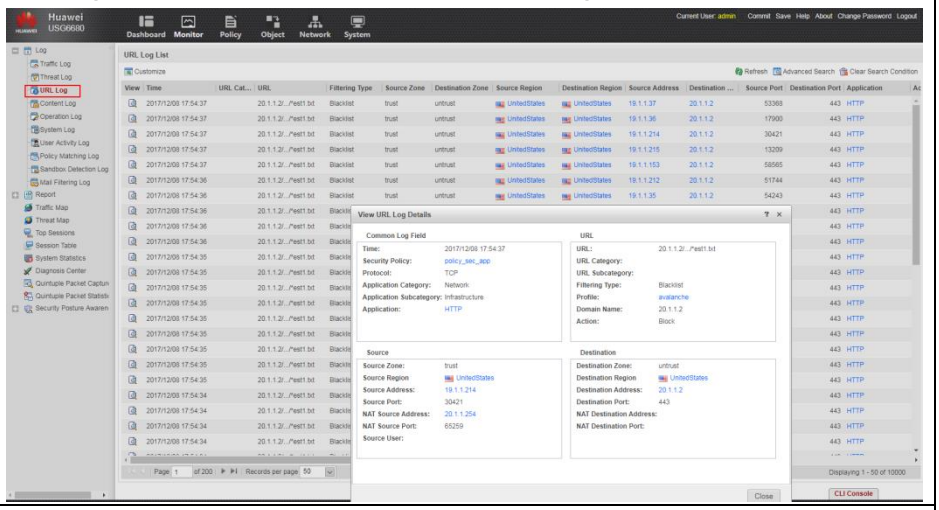
10.2.2 Threat Log

Objetivo de teste	Verify whether the equipment supports to check threat log.
Especificação de teste	Threat logs provide statistics on network threats (such as viruses, intrusion behaviors, DDoS, Trojan horses, Botnets, worms, and APT). Threat logs help you learn what threats have occurred or are occurring, and adjust the security policies for better attack defense.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente;

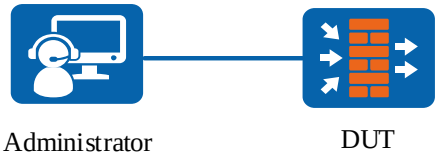
	4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Login the device via WEB to view the threat log. 
Resultado Esperado	1. Device supports the function of threat log.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

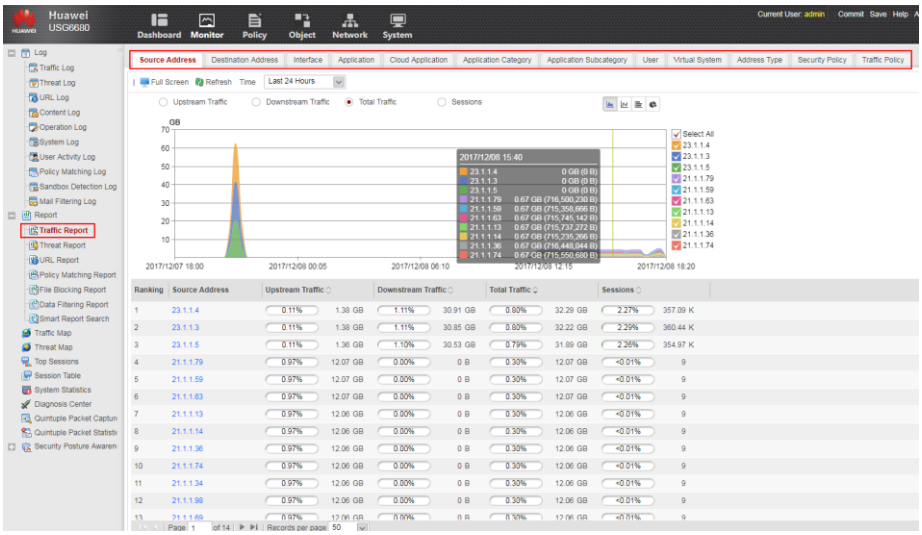
10.2.3 URL Log

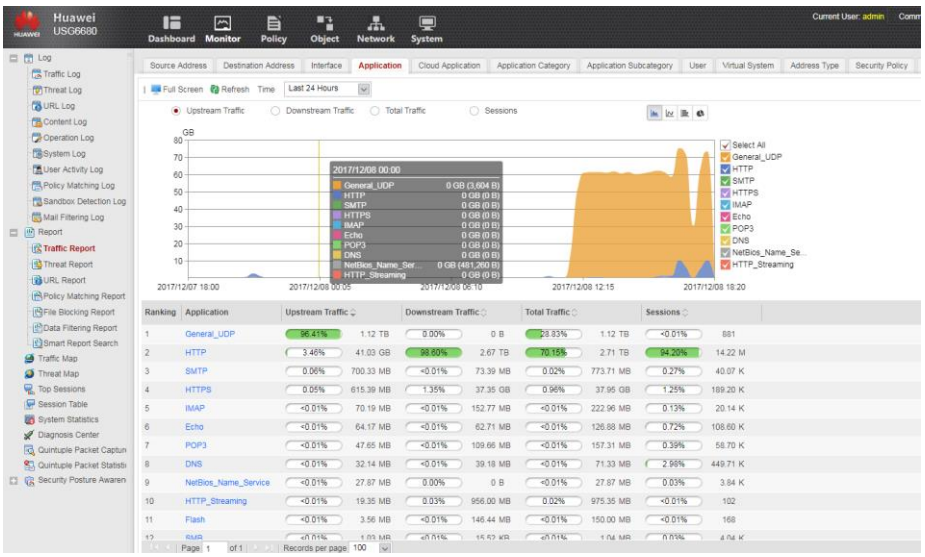
Objetivo de teste	Verify whether the equipment supports to check URL log.
Especificação de teste	URL logs provide statistics on requested URLs. You can view URL logs to check why access to some URLs is allowed, blocked or allowed with an alert record.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).

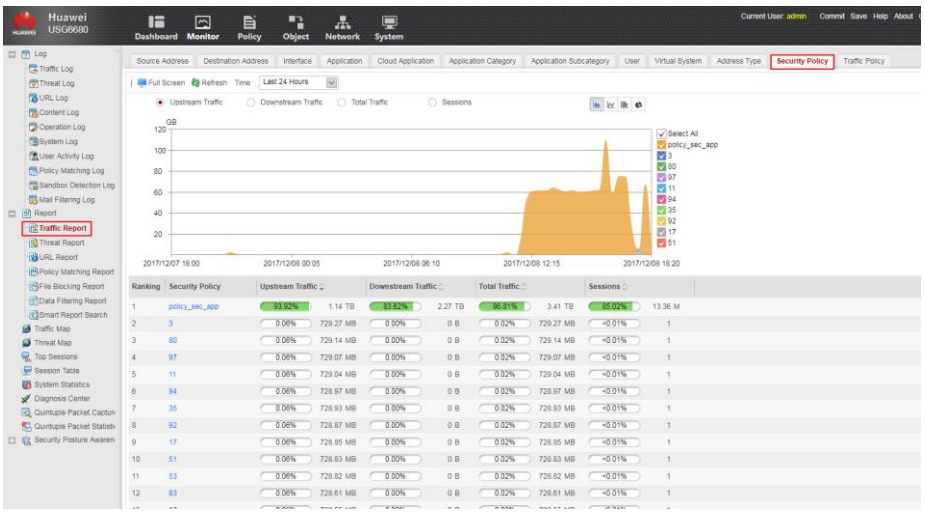
Procedimento de Teste	1. Login the device via WEB to view the URL log. 			
Resultado Esperado	1. Device supports the function of URL log.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

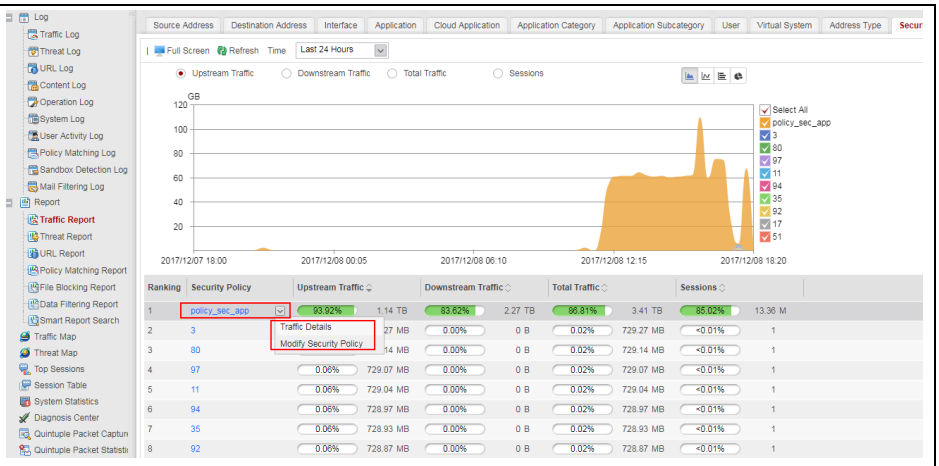
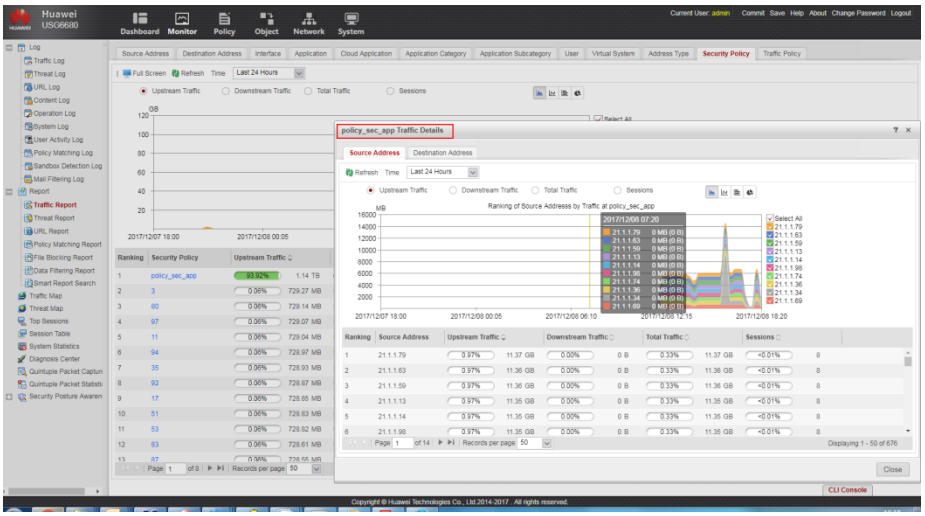
10.2.4 Traffic Report

Objetivo de teste	Verify whether the equipment supports to view traffic report.
Especificação de teste	Traffic reports display traffic trends and top rankings in various dimensions. You can effectively learn the traffic status of the current network based on traffic reports and therefore formulate the corresponding traffic measurement measures.
Ambiente de teste	Test TOPO:  Administrator DUT Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Create traffic through the device, and login to view the traffic report.


Huawei
USG6680
Dashboard
Monitor
Policy
Object
Network
System
Source Address
Destination Address
Interface
Application
Cloud Application
Application Category
Application Subcategory
User
Virtual System
Address Type
Security Policy
Traffic Policy
Full Screen
Refresh
Time
Last 24 Hours
Upstream Traffic
Downstream Traffic
Total Traffic
Sessions
Traffic Report
Ranking
Source Address
Upstream Traffic
Downstream Traffic
Total Traffic
Sessions


Huawei
USG6680
Dashboard
Monitor
Policy
Object
Network
System
Source Address
Destination Address
Interface
Application
Cloud Application
Application Category
Application Subcategory
User
Virtual System
Address Type
Security Policy
Full Screen
Refresh
Time
Last 24 Hours
Upstream Traffic
Downstream Traffic
Total Traffic
Sessions
Traffic Report
Ranking
Application
Upstream Traffic
Downstream Traffic
Total Traffic
Sessions


Huawei
USG6680
Dashboard
Monitor
Policy
Object
Network
System
Source Address
Destination Address
Interface
Application
Cloud Application
Application Category
Application Subcategory
User
Virtual System
Address Type
Security Policy
Traffic Policy
Full Screen
Refresh
Time
Last 24 Hours
Upstream Traffic
Downstream Traffic
Total Traffic
Sessions
Traffic Report
Ranking
Security Policy
Upstream Traffic
Downstream Traffic
Total Traffic
Sessions

	 			
Resultado Esperado	1. Traffic report shows the traffic trend and top ranking based on source IP, destination IP, application, and user and so on. The device supports the function of traffic report.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

10.2.5 Threat Report

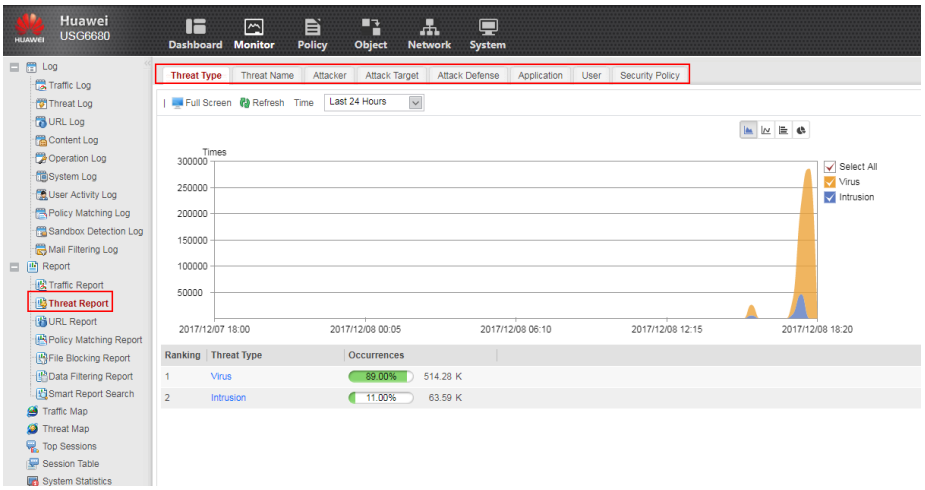
Objetivo de teste	Verify whether the equipment supports to view threat report.
Especificação de teste	Threat reports show the number of threats in each dimension and top rankings. You can effectively learn common threat types, active attackers, and victims that frequently suffer attacks based on threat reports, and therefore formulate the corresponding security protection measures.
Ambiente de teste	Test TOPO:

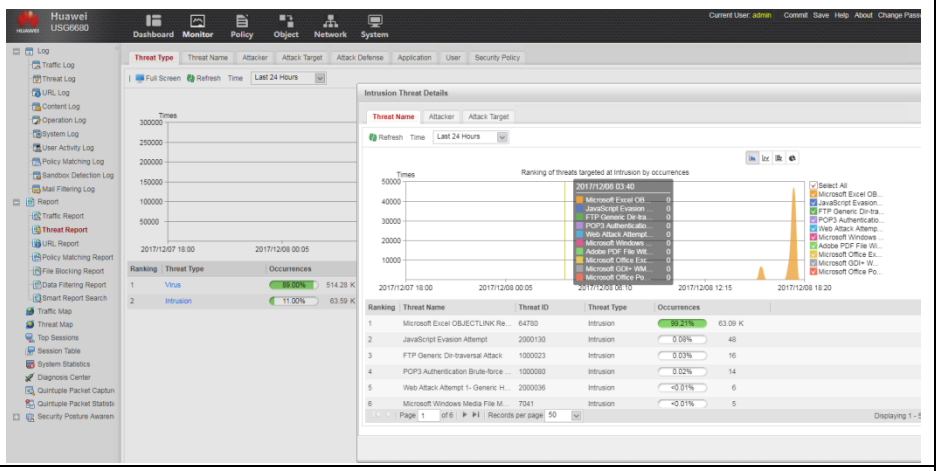
<table>
<tr><td></td><td>

Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;
4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).

</td></tr>
<tr><td>Procedimento de Teste</td><td>

1. Create threat traffic through the device, and login to view the threat report.



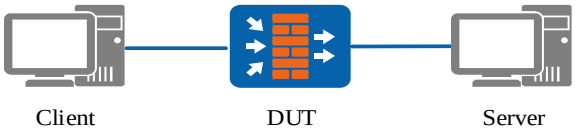
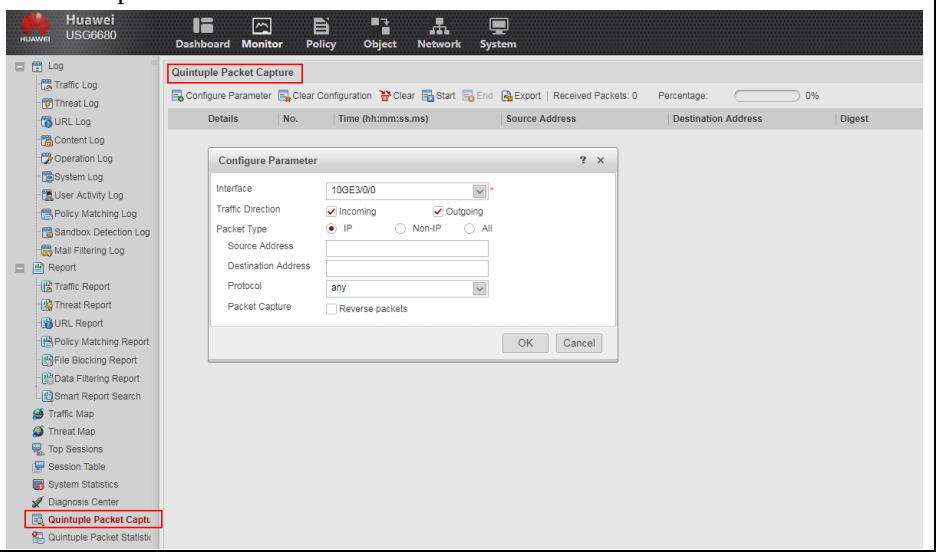


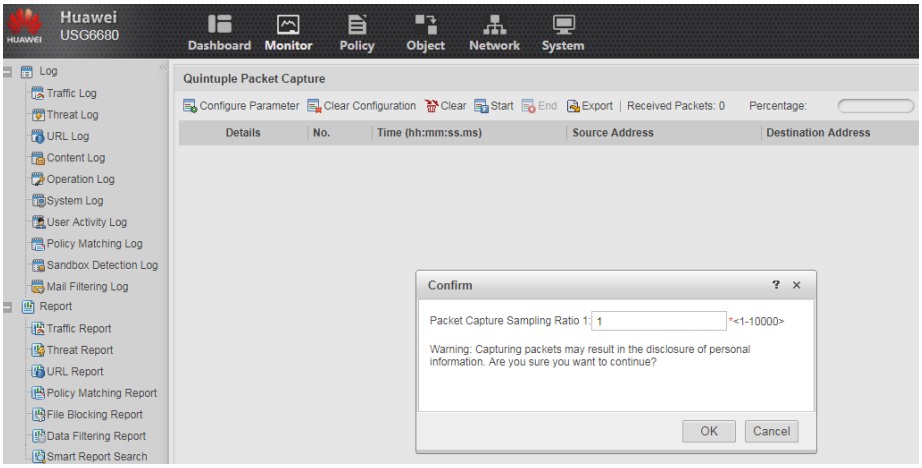
</td></tr>
<tr><td>Resultado Esperado</td><td>

1. Threat report shows the threat trend and top ranking based on threat type, attacker, and victim and so on. The device supports the function of threat report.

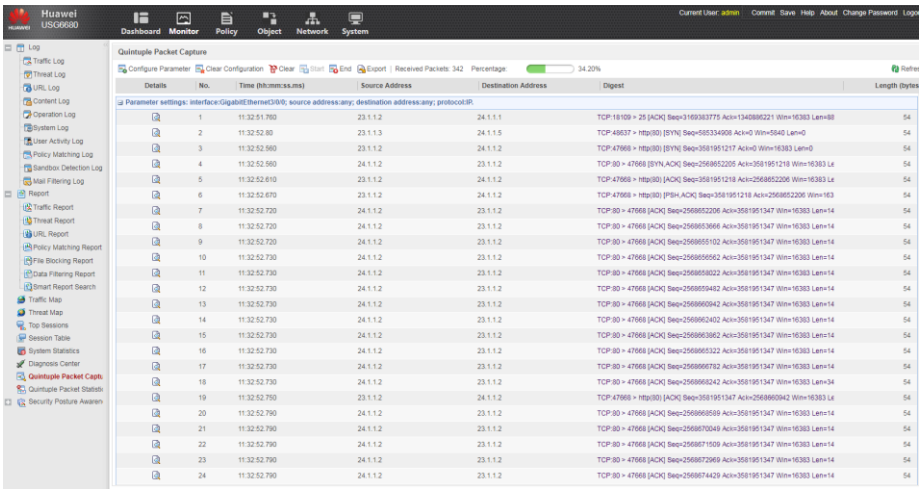
</td></tr>
<tr><td>Resultado do Teste</td><td>☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA</td></tr>
<tr><td>Observação</td><td></td></tr>
<tr><td>Assinatura</td><td>Cliente</td><td></td><td>Huawei</td><td></td></tr>
</table>

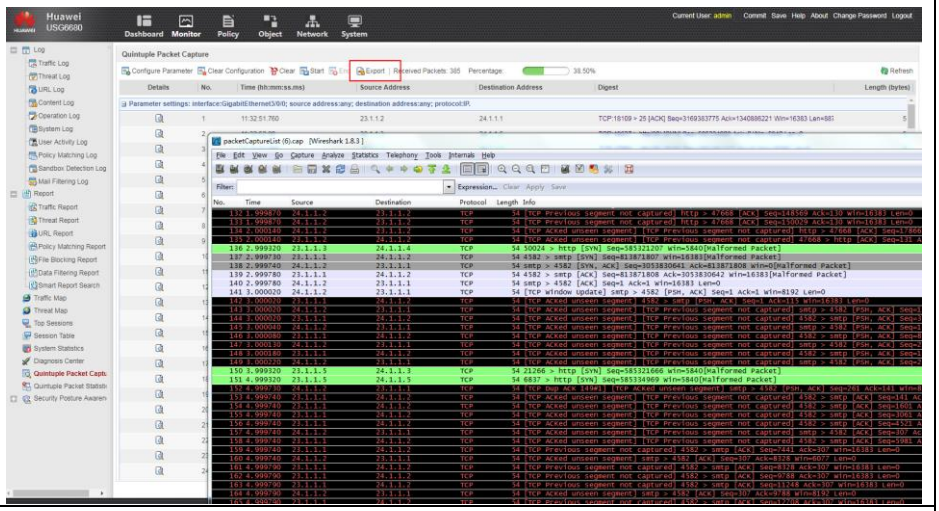
10.2.6 Packet Capture

Objetivo de teste	Verify whether the equipment supports packet capture function.
Especificação de teste	Quituple packet capture function enables the FW to copy the passing packets and save or export them in a certain format on the FW .
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Login the device via WEB, enter into the “Monitor” tag and select “Quintuple packet capture”.Configure the parameters for traffic need to be captured then click start. 



2. Generate the traffic and check the packets been captured.



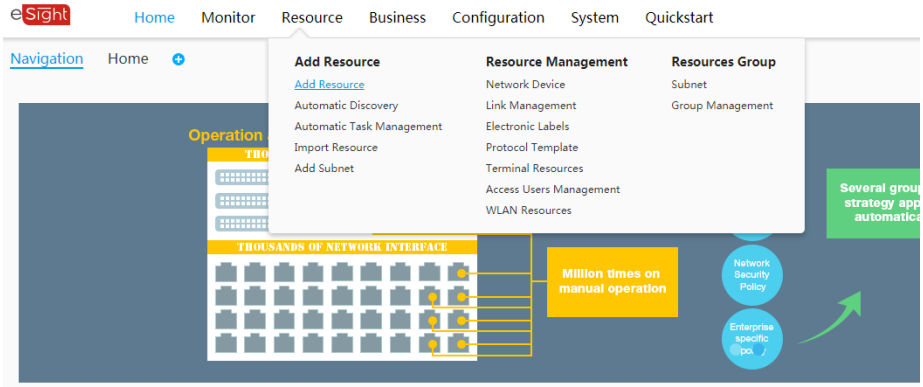
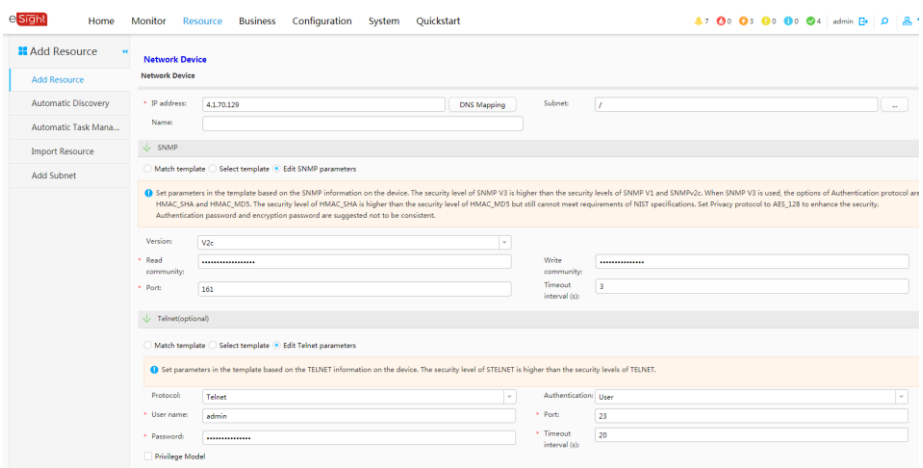


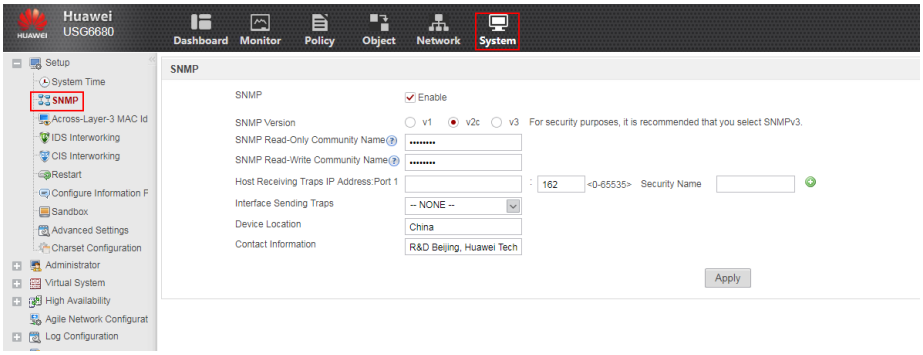
Resultado Esperado	2. Device supports packet capture function.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

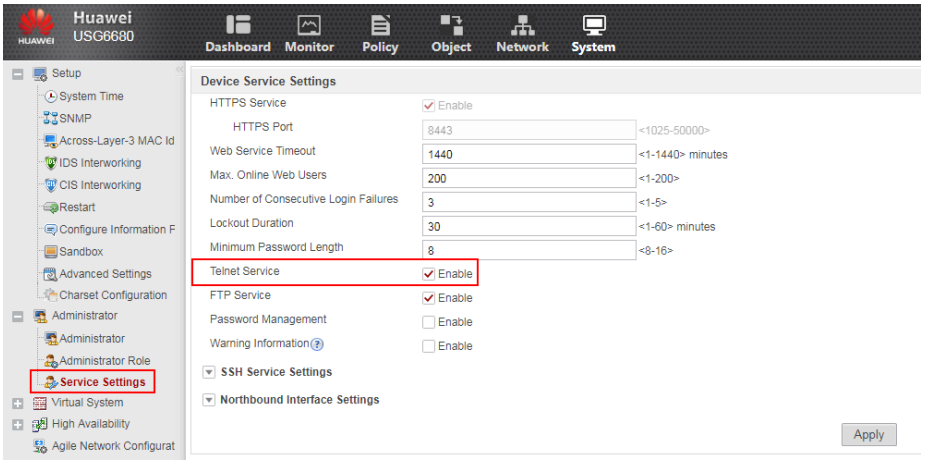
Assinatura	**Cliente**		**Huawei**	

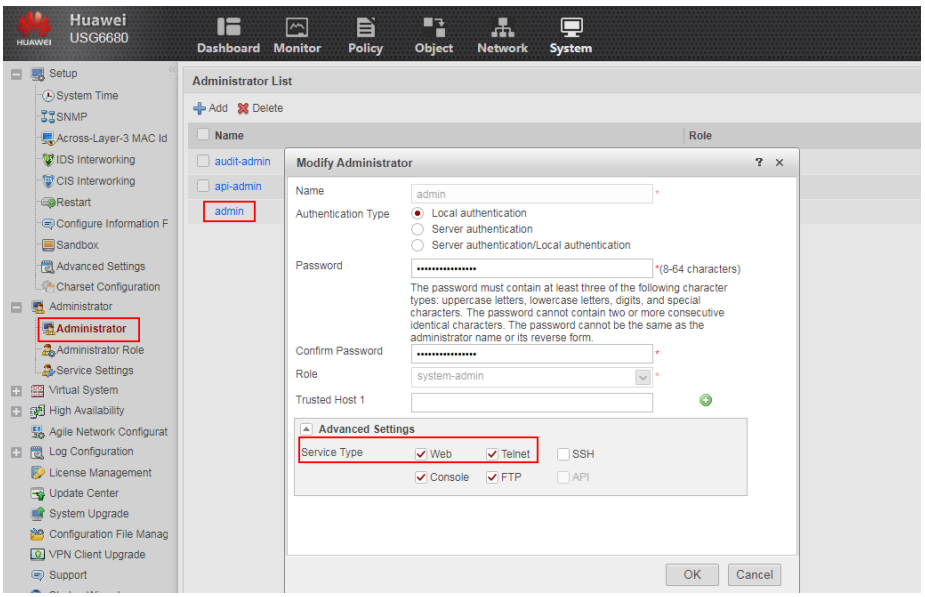
10.3 Centralized Management

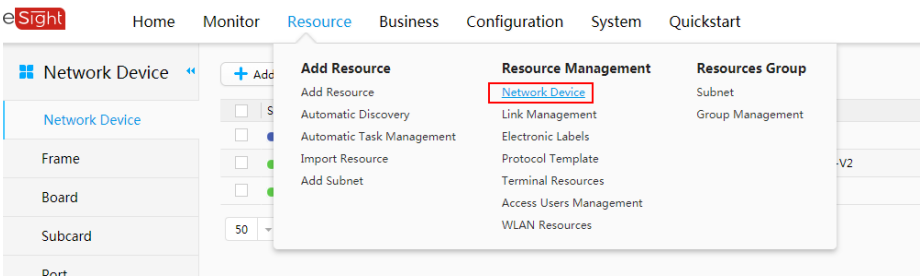
10.3.1 CPU、Memory Usage&Performance Status Monitoring

Objetivo de teste	Verify whether the equipment supports to monitor CPU and memory usage.
Especificação de teste	CPU Usage: Percentage of CPU resources used by the device at a time point; Memory Usage: Percentage of memory resources used.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Add the device to eSight;  

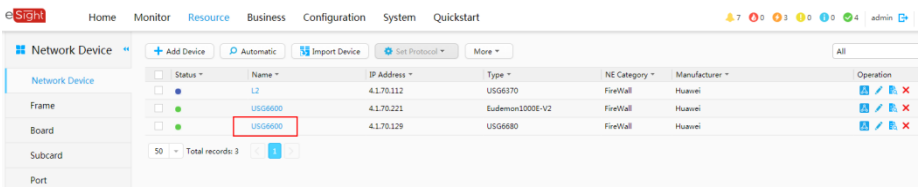




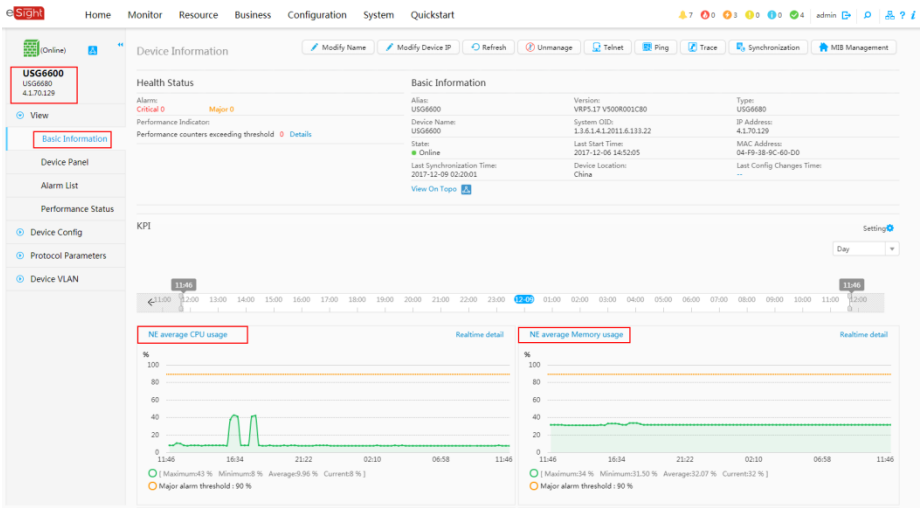




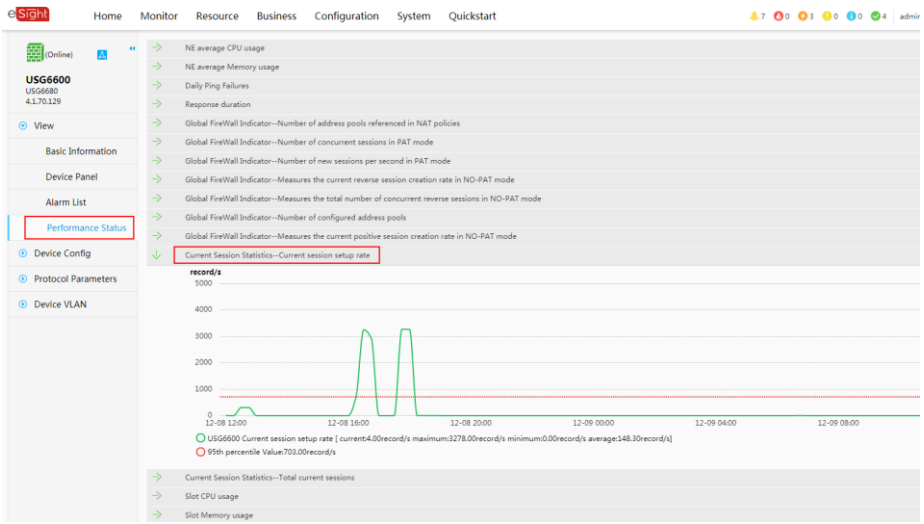
2. Check the data of device collected on eSight.



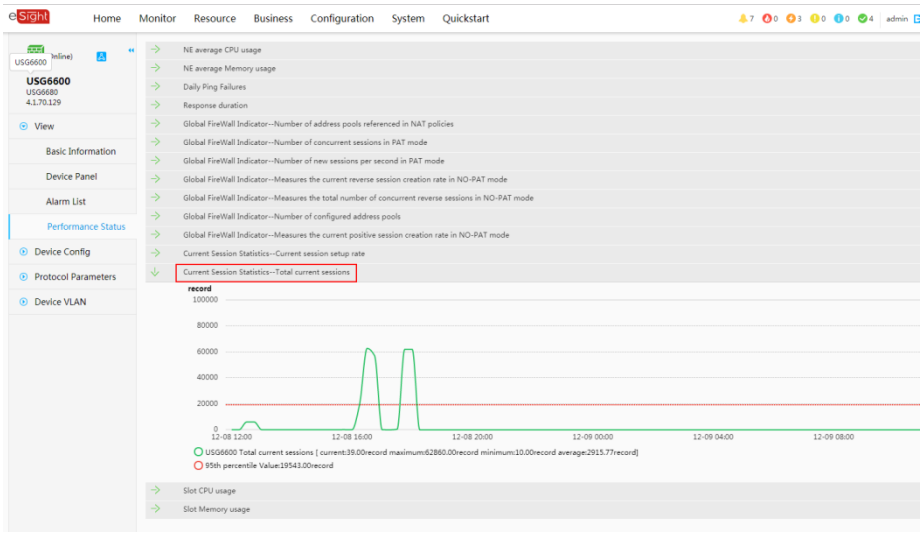
CPU、Memory:



Session create rate:



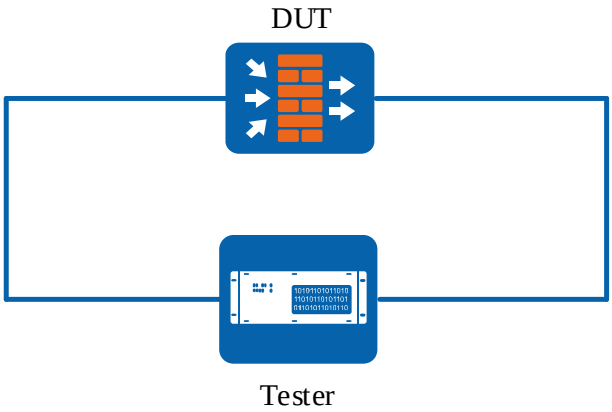
Concurrent sessions:

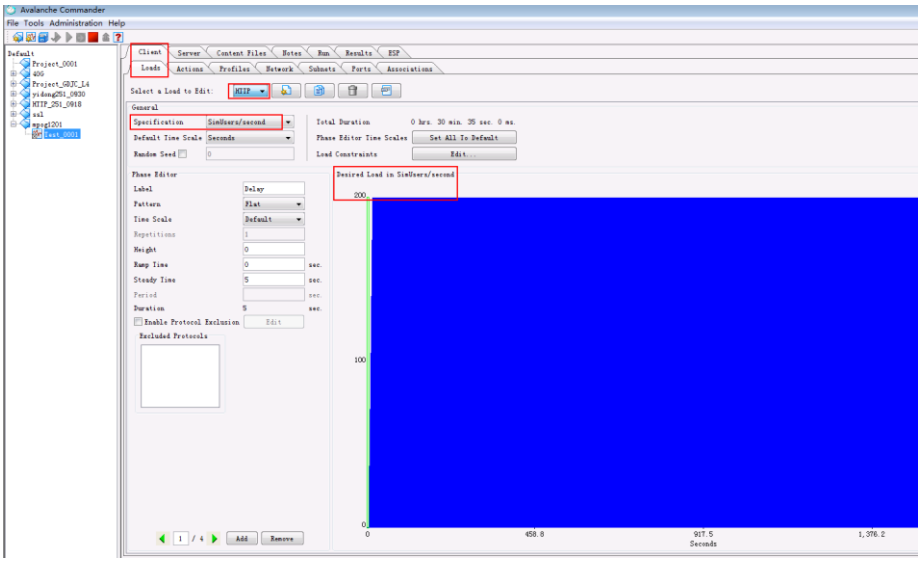
				
Resultado Esperado	1. CPU usage and memory usage can be monitored on eSight, and the date is no difference with which is shown on the device.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

11 Performance

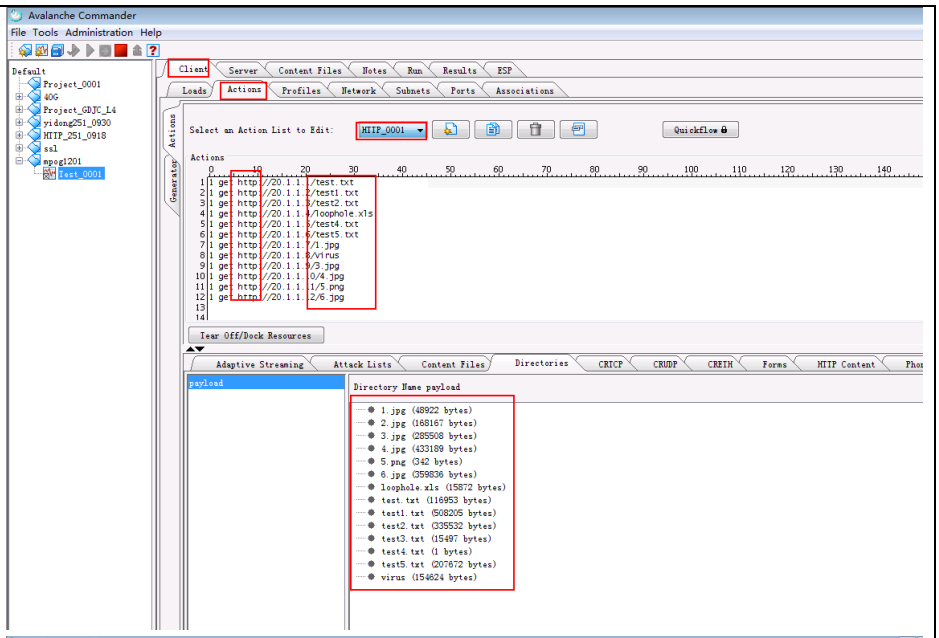
11.1 IMIX Throughput

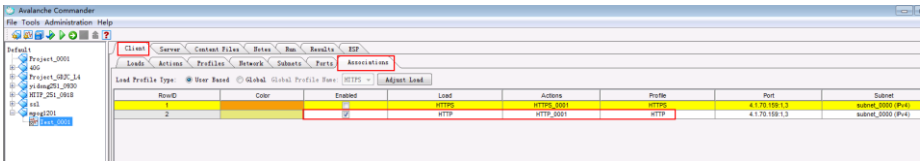
Objetivo de teste	Verify the equipment capability of HTTP throughput.
Especificação de teste	Throughput is the maximum ability that a device handles data packets. It determines how much traffic or how many packets a device can handle in a second. The higher throughput is the larger bandwidth we can provide to Cliente. HTTP throughput means usin vqg HTTP traffic to test device's throughput. Test tools generally use Avalanche or BPS.
Ambiente de teste	Test TOPO:

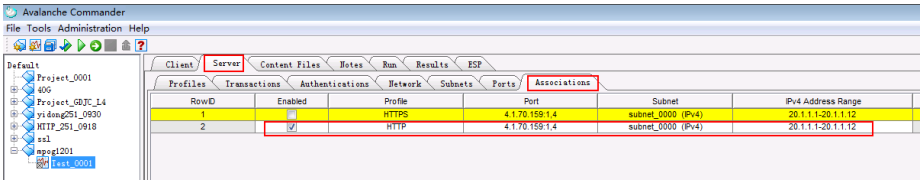
<table>
<tr>
<td></td>
<td>


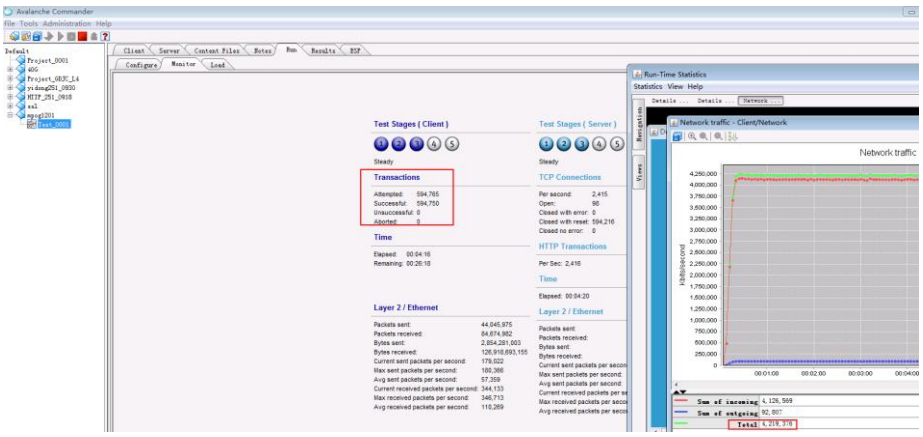
Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;
4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
</td>
</tr>
<tr>
<td>Procedimento de Teste</td>
<td>
Traffic Model:
5.1.12.1. HTTP = 55% (variable content with images and texts, variable size from 100 bytes to 500 Kbytes, being a reserve of 5% for files with malware and 1% for attacks).


</td>
</tr>
</table>



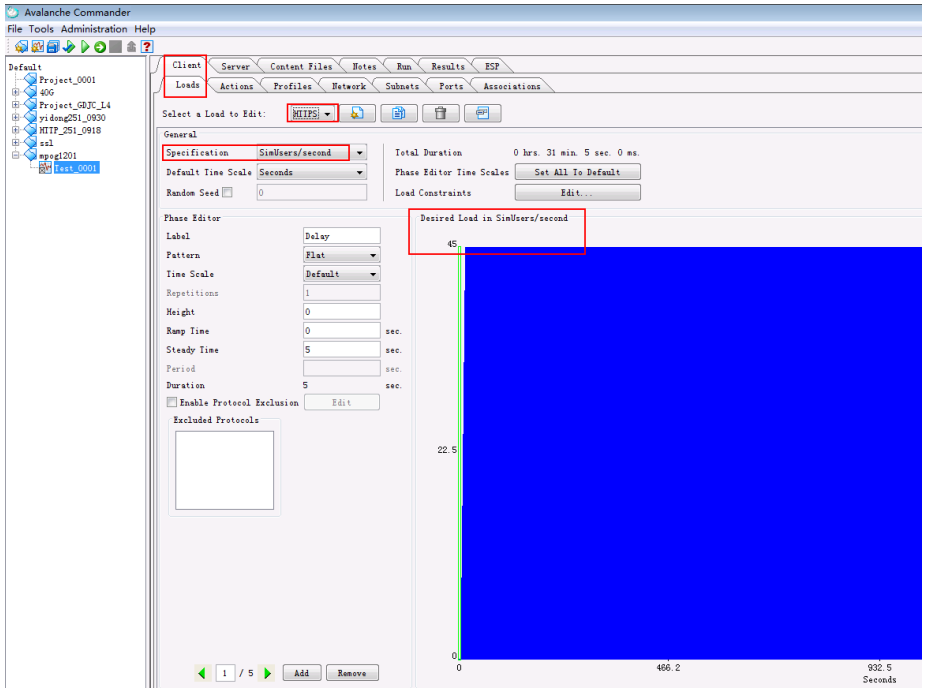


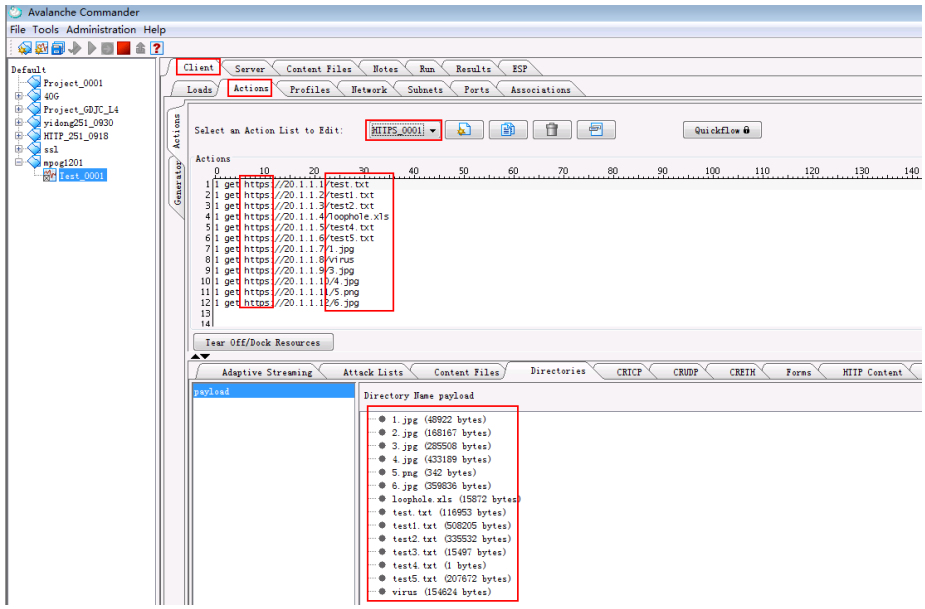


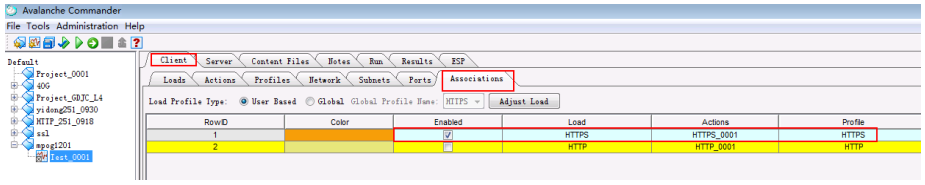


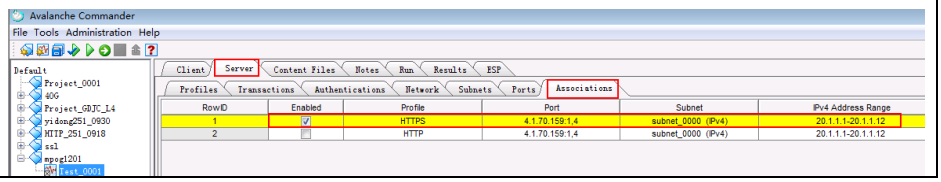
HTTP throughput 4.2G >80%*5G

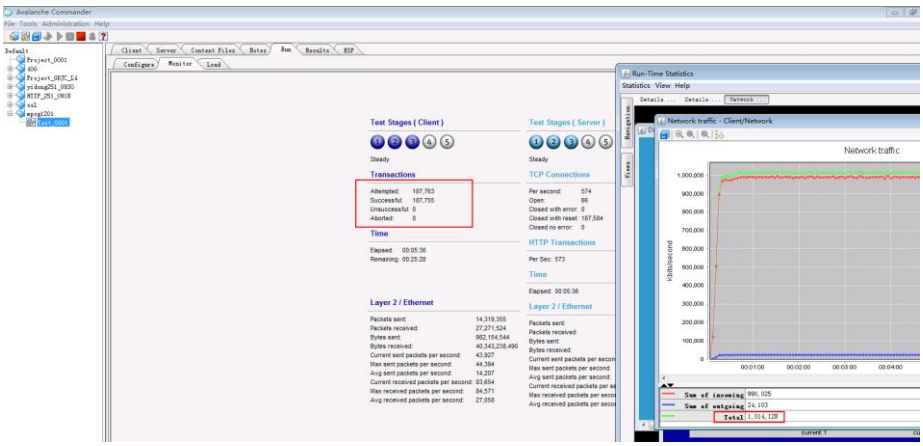
5.1.12.2. HTTPS to be decrypted and inspected = 25% (variable content with images and texts, variable size from 100 bytes to 500 Kbytes, with a reserve of 5% for files with malware and 1% for attacks using AES and SHA-256 encryption or higher).


Avalanche Commander
File Tools Administration Help
Client Server Content Files Notes Run Results ESP
Loads Actions Profiles Network Subnets Ports Associations
Select a Load to Edit: HTTPS
General
Specification SimUsers/second
Total Duration 0 hrs. 31 min. 5 sec. 0 ms.
Phase Editor Time Scales Set All To Default
Load Constraints Edit...
Phase Editor
Desired Load in SimUsers/second
Seconds


Avalanche Commander
File Tools Administration Help
Client Server Content Files Notes Run Results ESP
Loads Actions Profiles Network Subnets Ports Associations
Select an Action List to Edit: HTTPS_0001
Quickflow
Actions
Tear Off/Dock Resources
Adaptive Streaming Attack Lists Content Files Directories CRTCP CRUDP CRETM Forms HTTP Content
payload
Directory Name payload


Avalanche Commander
File Tools Administration Help
Client Server Content Files Notes Run Results ESP
Loads Actions Profiles Network Subnets Ports Associations
Load Profile Type: User Based Global
Adjust Load
RowID Color Enabled Load Actions Profile
1 HTTPS HTTPS_0001 HTTPS
2 HTTP HTTP_0001 HTTP

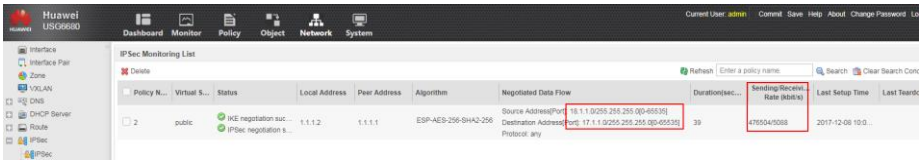

Avalanche Commander
File Tools Administration Help
Client Server Content Files Notes Run Results ESP
Profiles Transactions Authentications Network Subnets Ports Associations
RowID Enabled Profile Port Subnet IPv4 Address Range
1 HTTPS 4.1.70.159:1,4 subnet_0000 (IPv4) 20.1.1.1-20.1.1.12
2 HTTP 4.1.70.159:1,4 subnet_0000 (IPv4) 20.1.1.1-20.1.1.12

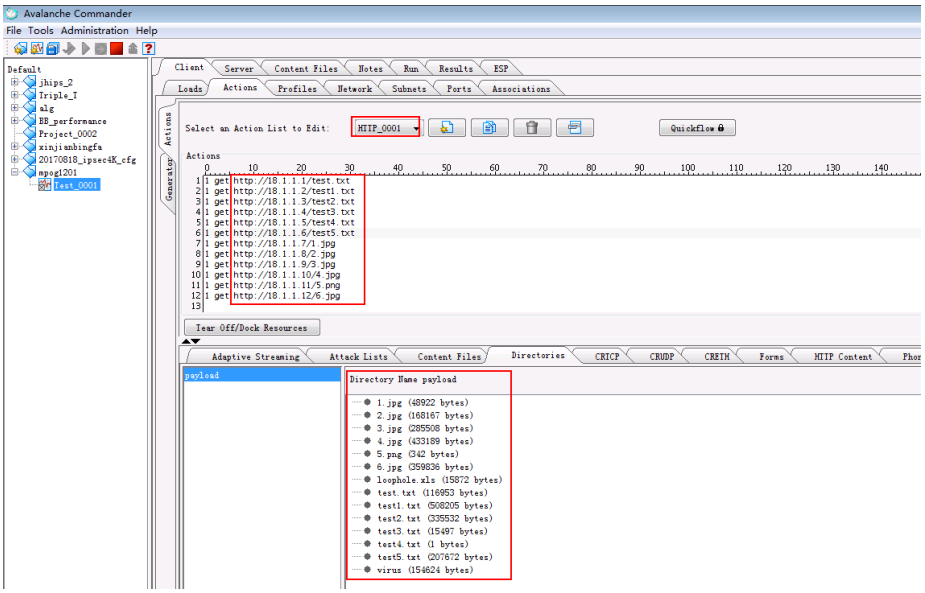


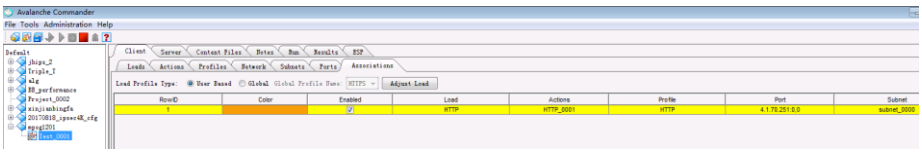
HTTPS throughput 1G=20%*5G

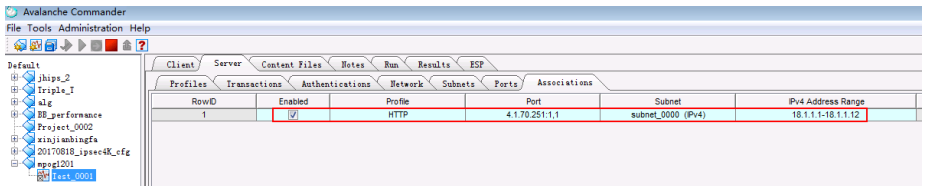
5.1.12.3. Applications, other attacks, other threats and other protocols = 20%, to be agreed with the technical group of support to the crier and approved in the Caderno de Tests.

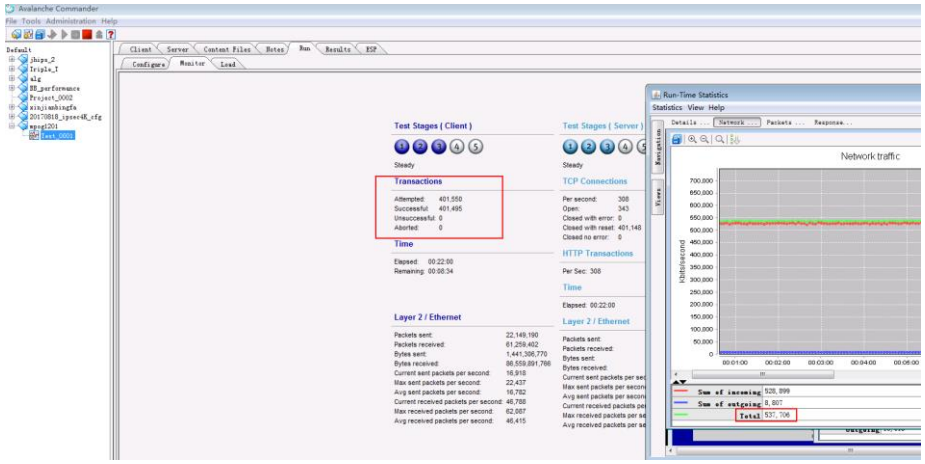
5.1.12.3.1. 5% VPN (PiSec, variable content with images and texts, variable size 100 bytes to 500 Kbytes)





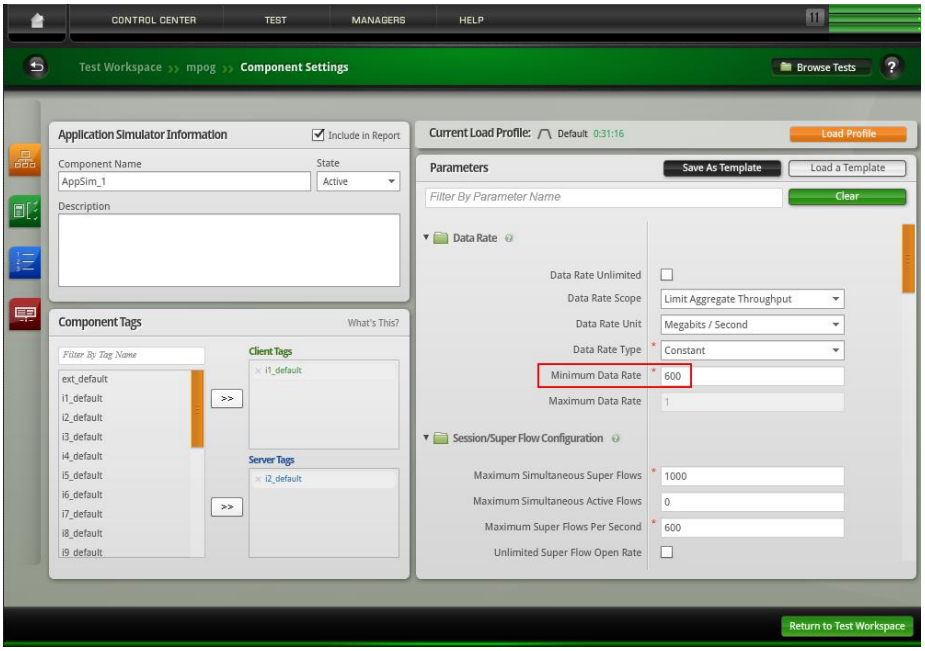


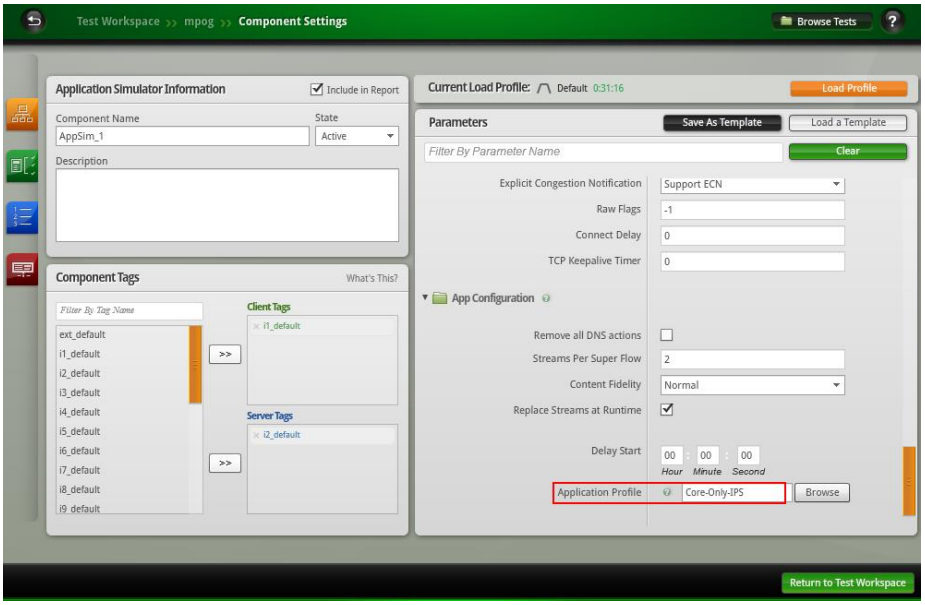


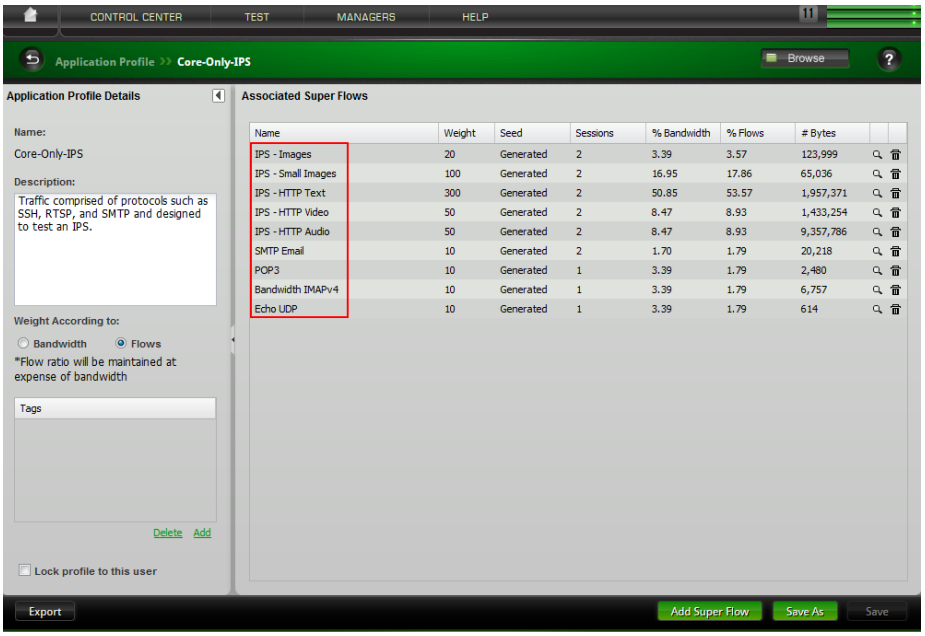


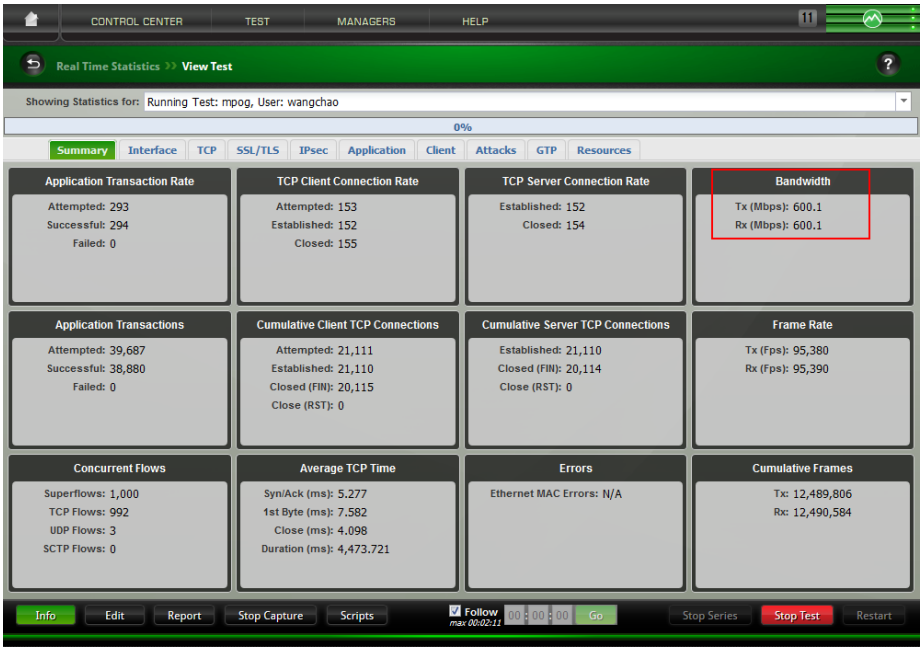
IPSec VPN throughput: 530Mbps>5%*5G

5.1.12.3.2. E-mail (POP, SMTP and IMAP with variable content, including attached files).



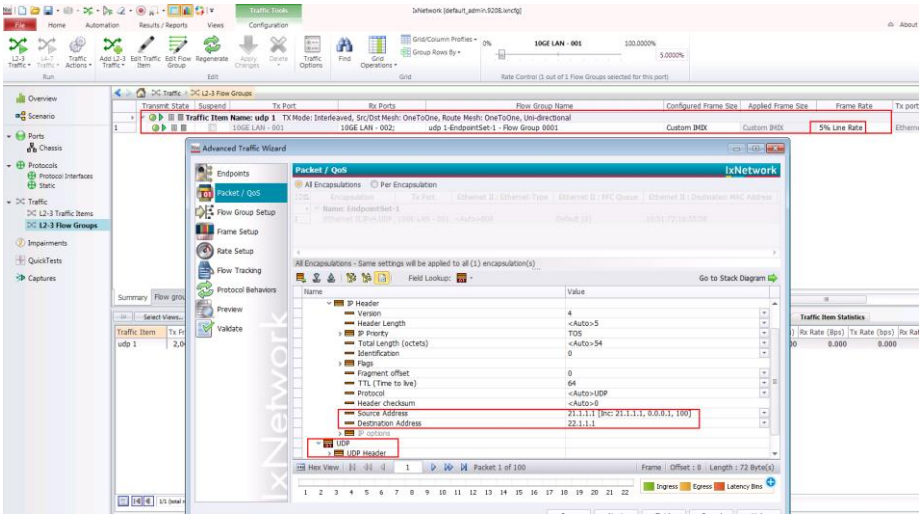

Test Workspace >> mpog >> Component Settings
Browse Tests
Application Simulator Information
Include in Report
Component Name
AppSim_1
State
Active
Description
Current Load Profile: Default 0:31:16
Load Profile
Parameters
Save As Template
Load a Template
Filter By Parameter Name
Clear
Explicit Congestion Notification
Support ECN
Raw Flags
-1
Connect Delay
0
TCP Keepalive Timer
0
App Configuration
Remove all DNS actions
Streams Per Super Flow
2
Content Fidelity
Normal
Replace Streams at Runtime
Delay Start
00 : 00 : 00
Hour Minute Second
Application Profile
Core-Only-IPS
Browse
Component Tags
What's This?
Filter By Tag Name
ext_default
i1_default
i2_default
i3_default
i4_default
i5_default
i6_default
i7_default
i8_default
i9_default
Client Tags
i1_default
Server Tags
i2_default
Return to Test Workspace

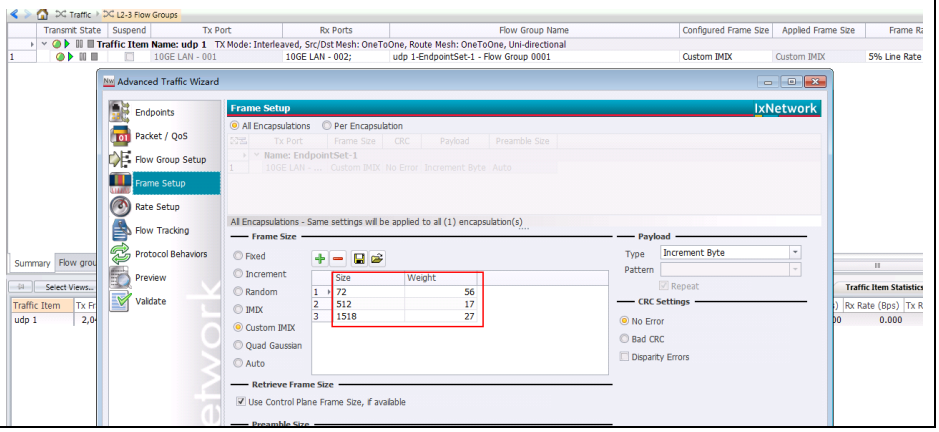

CONTROL CENTER
TEST
MANAGERS
HELP
Application Profile >> Core-Only-IPS
Browse
Application Profile Details
Name:
Core-Only-IPS
Description:
Traffic comprised of protocols such as SSH, RTSP, and SMTP and designed to test an IPS.
Weight According to:
Bandwidth
Flows
*Flow ratio will be maintained at expense of bandwidth
Tags
Delete
Add
Lock profile to this user
Associated Super Flows
Name | Weight | Seed | Sessions | % Bandwidth | % Flows | # Bytes
IPS - Images | 20 | Generated | 2 | 3.39 | 3.57 | 123,999
IPS - Small Images | 100 | Generated | 2 | 16.95 | 17.86 | 65,036
IPS - HTTP Text | 300 | Generated | 2 | 50.85 | 53.57 | 1,957,371
IPS - HTTP Video | 50 | Generated | 2 | 8.47 | 8.93 | 1,433,254
IPS - HTTP Audio | 50 | Generated | 2 | 8.47 | 8.93 | 9,357,786
SMTP Email | 10 | Generated | 2 | 1.70 | 1.79 | 20,218
POP3 | 10 | Generated | 1 | 3.39 | 1.79 | 2,480
Bandwidth IMAPv4 | 10 | Generated | 1 | 3.39 | 1.79 | 6,757
Echo UDP | 10 | Generated | 1 | 3.39 | 1.79 | 614
Export
Add Super Flow
Save As
Save

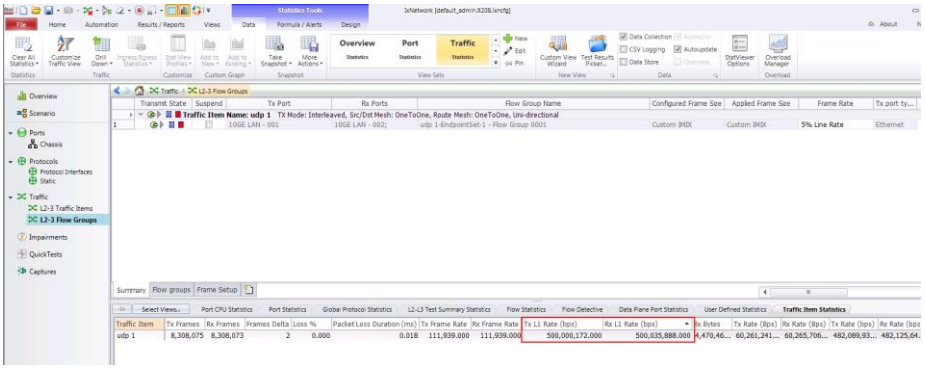


Email+other Applications: 600Mbps>10%*5G

5.1.12.3.3. 5% UDP (size distribution: 56% 72 bytes, 17% 512 bytes and 27% 1518 bytes).







UDP throughput: 500Mbps=10%*5G

5.1.12.3.4. 4% of applications (any protocol and with variable size).

5.1.12.3.5. Other (variable size distribution)

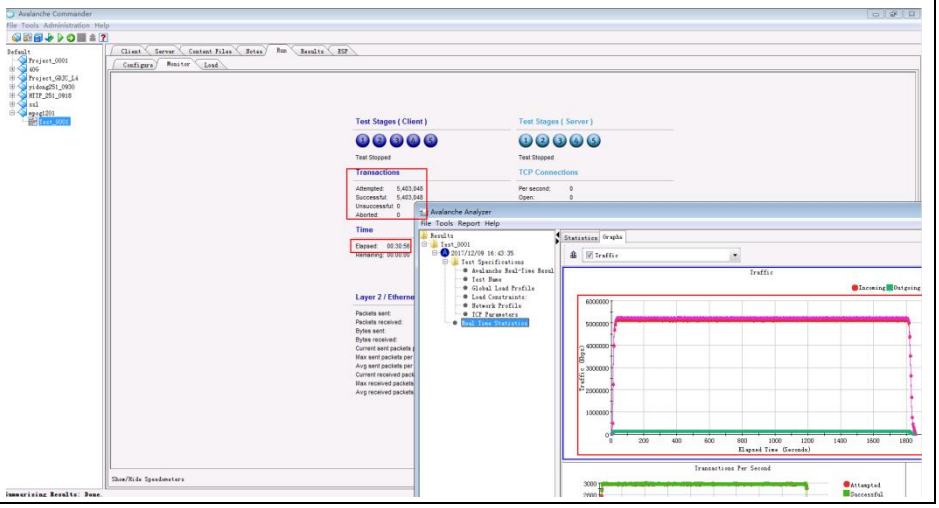
Procedimento de Teste:

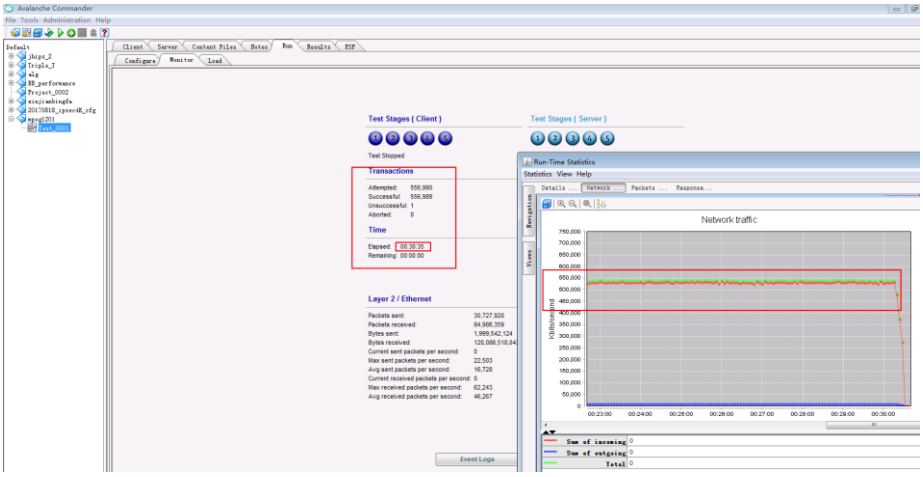
1. Open the tester and generate required IMIX traffic for an uninterrupted 30 minutes;

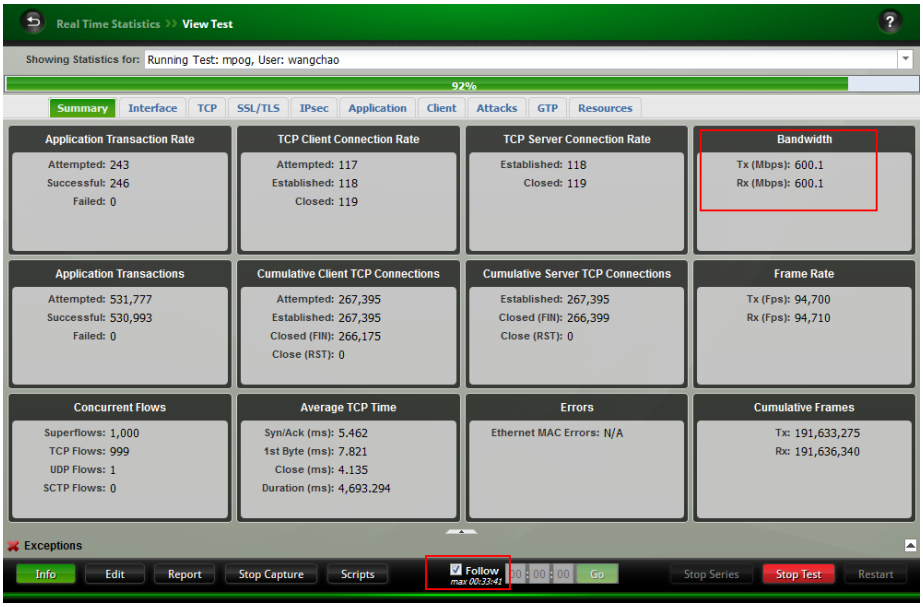
```
[USG6600]disp firewall  session table
2017-12-09 16:38:34.770 +08:00
 Current Total Sessions : 15159
 udp  VPN: public --> public  21.1.1.16:63[22.1.1.254:2563] --> 22.1.1.1:63
 DNS  VPN: public --> public  23.1.1.4:15638[24.1.1.254:26210] --> 24.1.1.5:53
 HTTP  VPN: public --> public  23.1.1.3:7175[24.1.1.254:23585] --> 24.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.38:14499[20.1.1.254:41031] --> 20.1.1.11:443
 HTTP  VPN: public --> public  23.1.1.4:25714[24.1.1.254:29531] --> 24.1.1.3:80
 HTTP  VPN: public --> public  17.1.1.143:54285[18.1.1.254:20943] --> 18.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.129:48485[20.1.1.254:46464] --> 20.1.1.5:443
 DNS  VPN: public --> public  23.1.1.4:31288[24.1.1.254:32548] --> 24.1.1.3:53
 HTTP  VPN: public --> public  17.1.1.93:41537[18.1.1.254:20893] --> 18.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.60:18514[20.1.1.254:43317] --> 20.1.1.8:443
 HTTP  VPN: public --> public  23.1.1.3:10144[24.1.1.254:25629] --> 24.1.1.4:80
 smtp  VPN: public --> public  23.1.1.4:3796[24.1.1.254:20664] --> 24.1.1.4:25
 HTTP  VPN: public --> public  23.1.1.5:37769[24.1.1.254:25635] --> 24.1.1.4:80
 DNS  VPN: public --> public  23.1.1.5:51759[24.1.1.254:32774] --> 24.1.1.3:53
 HTTP  VPN: public --> public  23.1.1.5:20417[24.1.1.254:25811] --> 24.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.33:64500[20.1.1.254:47913] --> 20.1.1.3:443
 HTTP  VPN: public --> public  19.1.1.56:27804[20.1.1.254:49771] --> 20.1.1.1:443
 DNS  VPN: public --> public  23.1.1.4:54118[24.1.1.254:31942] --> 24.1.1.3:53
 HTTP  VPN: public --> public  17.1.1.99:37472[18.1.1.254:20910] --> 18.1.1.3:80
 HTTP  VPN: public --> public  17.1.1.8:46241[18.1.1.254:20830] --> 18.1.1.1:80
 HTTP  VPN: public --> public  17.1.1.211:27139[18.1.1.254:21011] --> 18.1.1.6:80
 HTTP  VPN: public --> public  19.1.1.119:4436[20.1.1.254:41641] --> 20.1.1.10:443
 HTTP  VPN: public --> public  23.1.1.4:42210[24.1.1.254:25827] --> 24.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.133:58251[20.1.1.254:42634] --> 20.1.1.9:443
 HTTP  VPN: public --> public  19.1.1.199:37989[20.1.1.254:48026] --> 20.1.1.3:443
 HTTP  VPN: public --> public  23.1.1.4:59325[24.1.1.254:24189] --> 24.1.1.5:80
 DNS  VPN: public --> public  23.1.1.3:42707[24.1.1.254:26209] --> 24.1.1.5:53
 HTTP  VPN: public --> public  23.1.1.5:16290[24.1.1.254:24202] --> 24.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.202:49234[20.1.1.254:46422] --> 20.1.1.5:443
 HTTP  VPN: public --> public  23.1.1.5:50396[24.1.1.254:29425] --> 24.1.1.3:80
 HTTP  VPN: public --> public  23.1.1.4:4521[24.1.1.254:25101] --> 24.1.1.4:80
 HTTP  VPN: public --> public  17.1.1.247:51561[18.1.1.254:21019] --> 18.1.1.11:80
 HTTP  VPN: public --> public  19.1.1.42:45493[20.1.1.254:40357] --> 20.1.1.12:443
 HTTP  VPN: public --> public  19.1.1.228:59785[20.1.1.254:43867] --> 20.1.1.7:443
 DNS  VPN: public --> public  23.1.1.3:59355[24.1.1.254:24204] --> 24.1.1.4:53
 HTTP  VPN: public --> public  17.1.1.195:24144[18.1.1.254:20990] --> 18.1.1.7:80
 HTTP  VPN: public --> public  17.1.1.36:36085[18.1.1.254:20831] --> 18.1.1.7:80
 DNS  VPN: public --> public  23.1.1.4:53598[24.1.1.254:25577] --> 24.1.1.5:53
 HTTP  VPN: public --> public  19.1.1.137:30104[20.1.1.254:43137] --> 20.1.1.8:443
 HTTP  VPN: public --> public  19.1.1.42:45487[20.1.1.254:42572] --> 20.1.1.9:443
 DNS  VPN: public --> public  23.1.1.5:10657[24.1.1.254:32291] --> 24.1.1.3:53
 HTTP  VPN: public --> public  17.1.1.207:25907[18.1.1.254:21018] --> 18.1.1.3:80
 HTTP  VPN: public --> public  23.1.1.5:33867[24.1.1.254:23732] --> 24.1.1.5:80
```

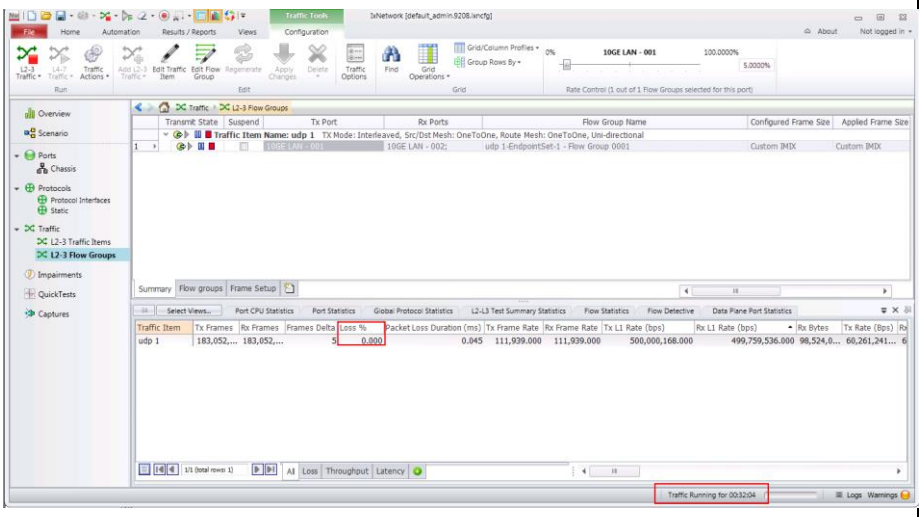
```
[USG6600]disp cpu-usage
2017-12-09 16:51:34.100 +08:00
CPU Usage Stat. Cycle: 10 (Second)
CPU Usage            :  51.1%  Max:  52.1%
Management-plane CPU Usage:  16.6%   Data-plane CPU Usage :  52.2%
CPU utilization for ten seconds:  51.1% : one minute:  51.2% : five minutes:  48.2%

PID   ProcessName         CPU       Runtime     State
1067  fpath.out         26.1%      114997220   S
1226  https.out         19.9%      3091843     S
1086  nge.out            3.3%      1475376     S
1069  nlog.out           0.6%      271022      S
635   vrp                0.5%      4005526     S
1016  vrpio_s            0.3%      366743      S
1088  slb_proxy.out      0.0%      217444      S
1082  ssa.out            0.0%      3515        S
1076  mail_proxy.out     0.0%      11225       S
1078  ike.out            0.0%      44268       S
1023  procmgmt.out       0.0%      8633        S
1081  auth.out           0.0%      53718       S
1079  am.out             0.0%      29483       S
1074  mail_send.out      0.0%      3739        S
1070  svn.out            0.0%      3710        S
1083  xmpp.out           0.0%      14781       S
1087  netopeer-server.out  0.0%     3496        S
1085  disk_smart.out     0.0%      2301        S
  ---- More ----
```

```
[USG6600]disp inter br
2017-12-09 16:57:19.380 +08:00
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                     PHY    Protocol  InUti OutUti   inErrors  outErrors
GigabitEthernet0/0/0          up     up           0%     0%          0          0
GigabitEthernet1/0/0          down   down         0%     0%          0          0
GigabitEthernet1/0/1          up     up        1.89% 53.72%          0          0
GigabitEthernet1/0/2          up     up       51.01%  1.09%          0          0
GigabitEthernet1/0/3          down   down         0%     0%          0          0
GigabitEthernet1/0/4          down   down         0%     0%          0          0
GigabitEthernet1/0/5          down   down         0%     0%          0          0
GigabitEthernet1/0/6          down   down         0%     0%          0          0
GigabitEthernet1/0/7          down   down         0%     0%          0          0
GigabitEthernet1/0/8(10G)     up     up        1.56% 52.93%          0          0
GigabitEthernet1/0/9(10G)     up     up       52.54%  1.35%          2          0
GigabitEthernet2/0/0          down   down         0%     0%          0          0
GigabitEthernet2/0/1          down   down         0%     0%          0          0
GigabitEthernet2/0/2          down   down         0%     0%          0          0
GigabitEthernet2/0/3          down   down         0%     0%          0          0
GigabitEthernet2/0/4          down   down         0%     0%          0          0
GigabitEthernet2/0/5          down   down         0%     0%          0          0
GigabitEthernet2/0/6          down   down         0%     0%          0          0
GigabitEthernet2/0/7          down   down         0%     0%          0          0
GigabitEthernet2/0/8(10G)     up     up        5.01%     0%          0          0
GigabitEthernet2/0/9(10G)     up     up           0%  5.01%          0          0
GigabitEthernet3/0/0(10G)     up     up        0.28%  5.63%          0          0
GigabitEthernet3/0/1(10G)     up     up        5.63%  0.28%          0          0
NULL0                         up     up(s)        0%     0%          0          0
Virtual-if0                   up     up(s)        --     --          0          0
[USG6600]
```



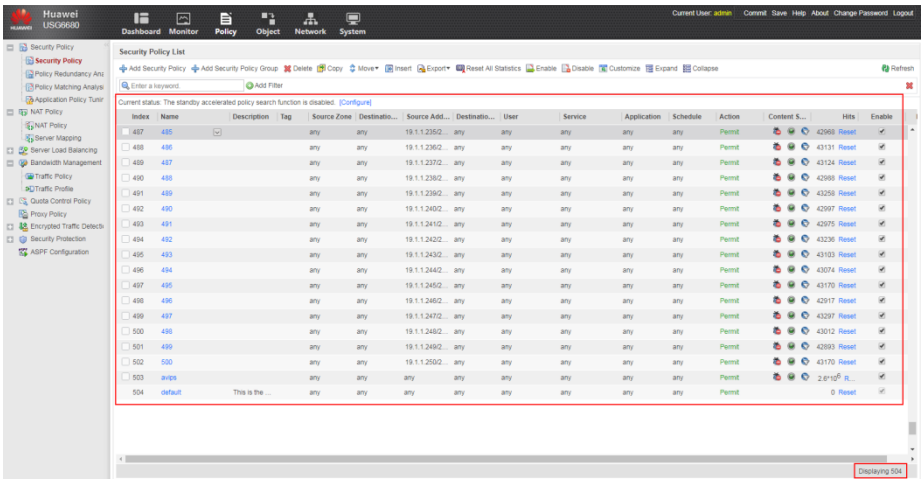




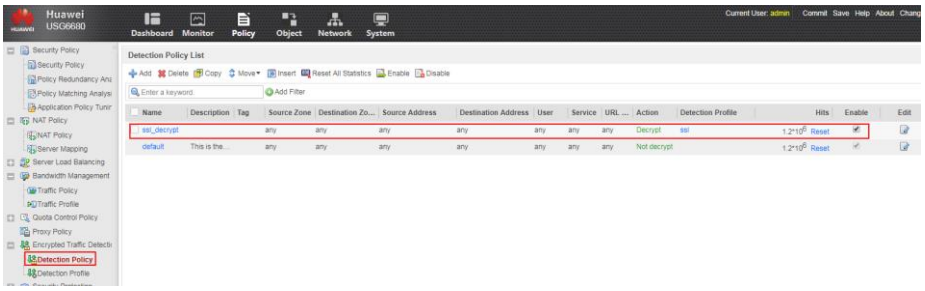


Configurations with all required functions enabled on FW：

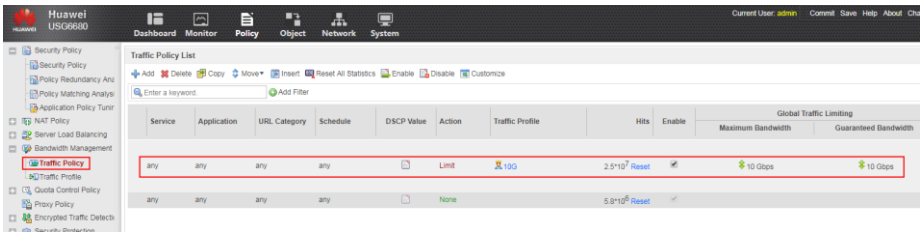
500 security policies:

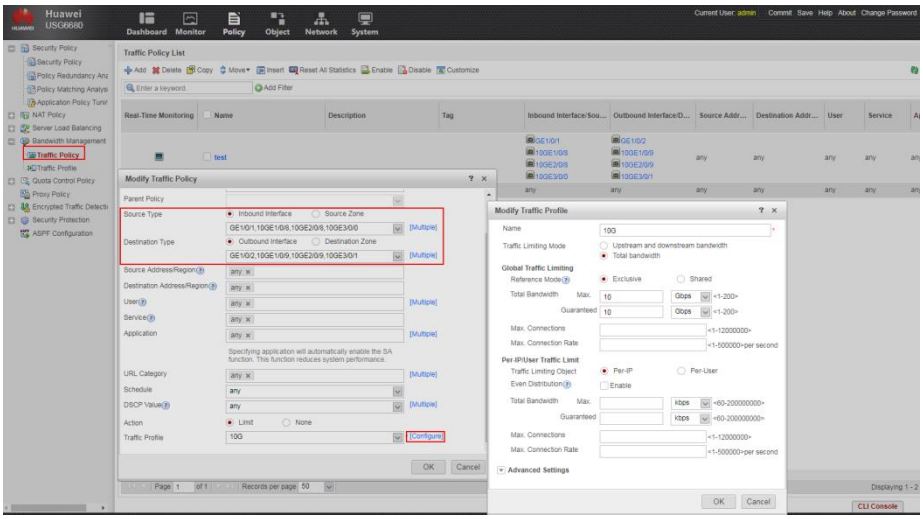


SSL decryption policy:

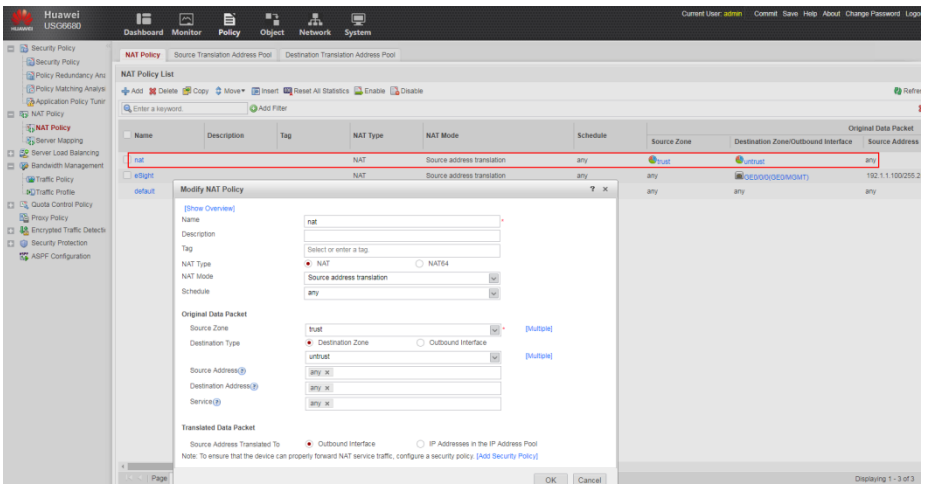


Traffic policy:



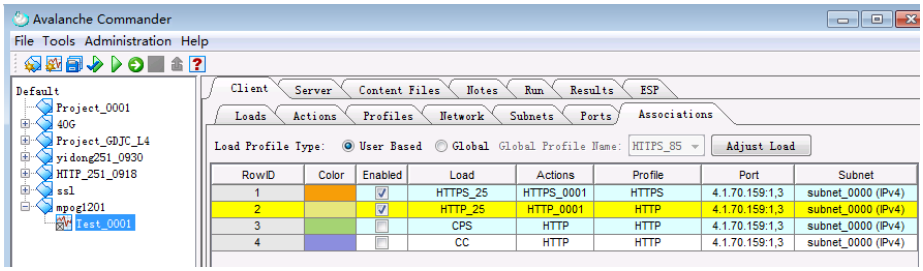


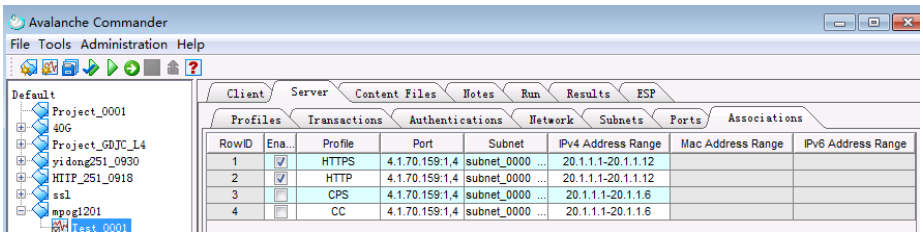
NAT policy:

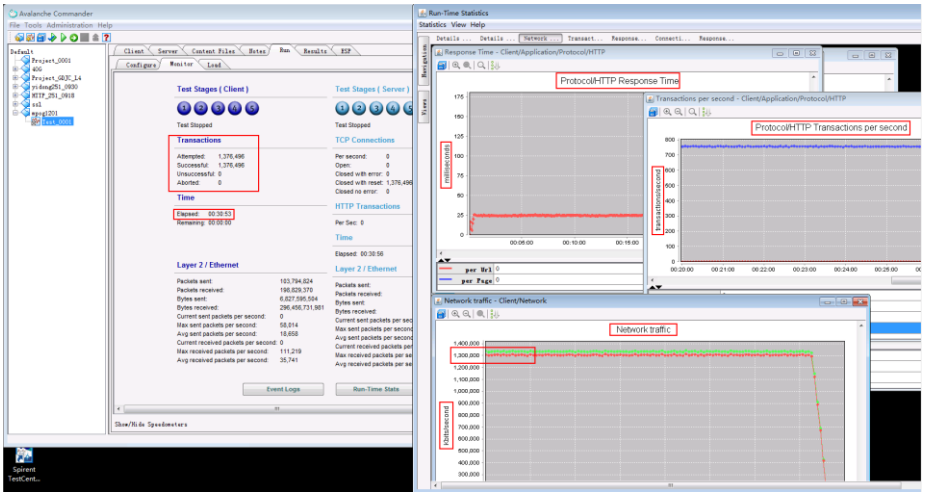


25% IMIX traffic of the lot required throughput:

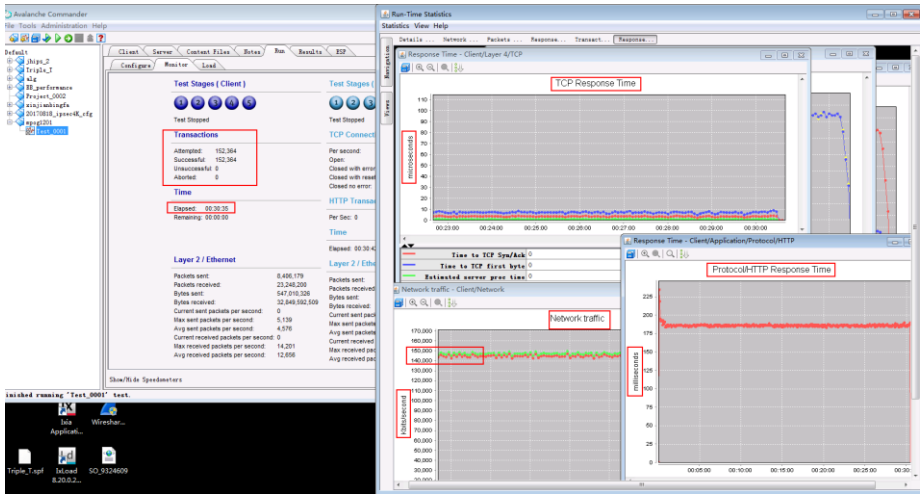
(80% HTTP+20% HTTPS)*25%=1.3G：
4.2G + 1G



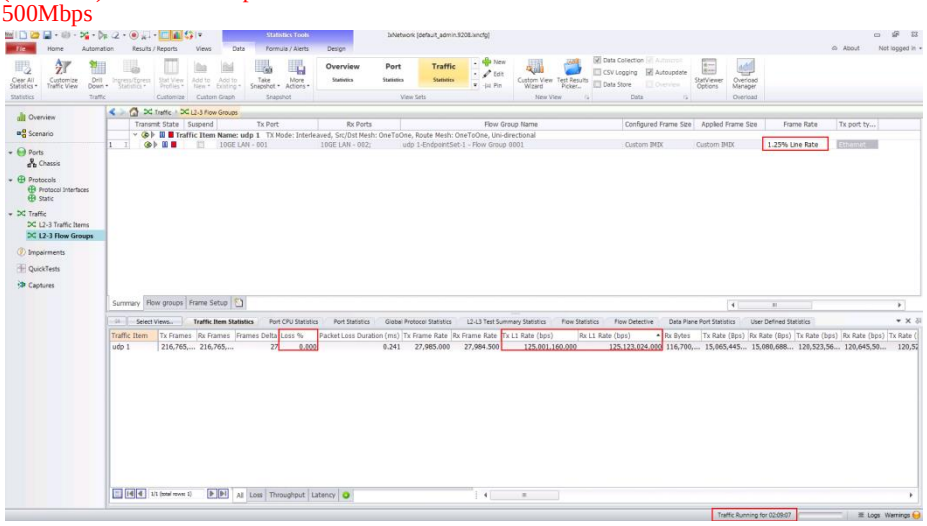


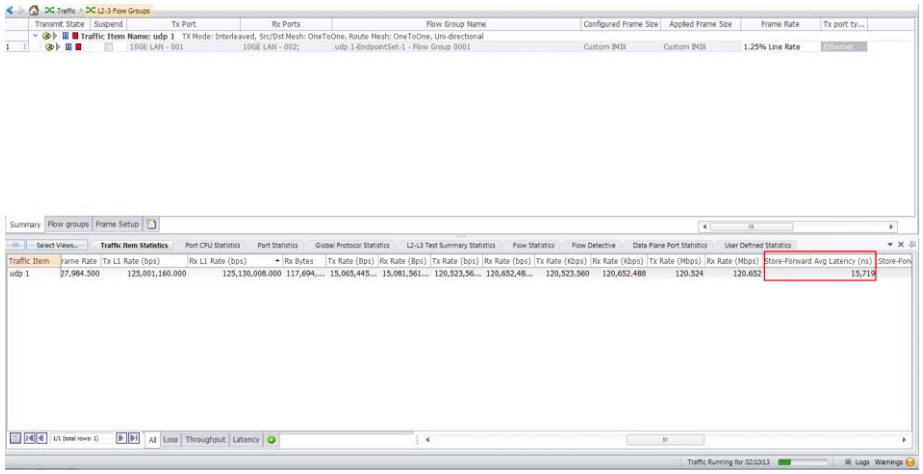


(5% IPSec VPN)*25%=140Mbps：
530Mbps

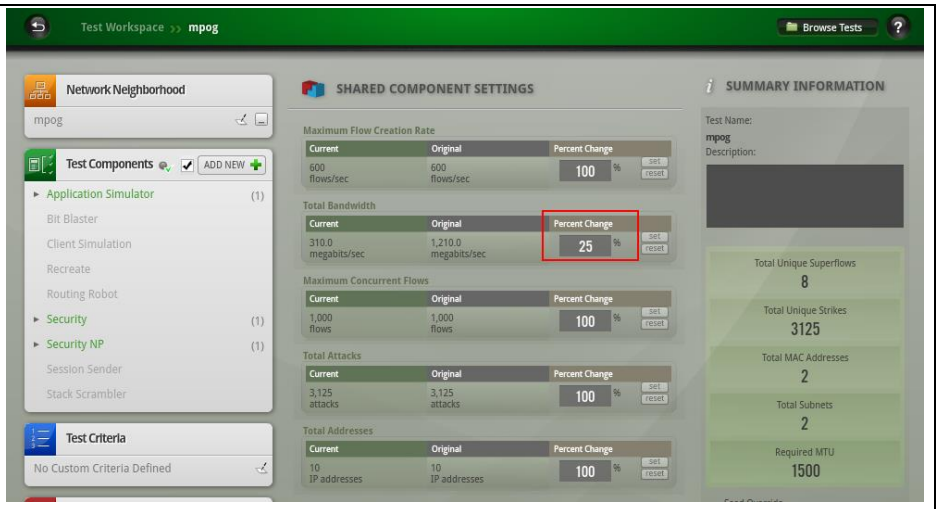


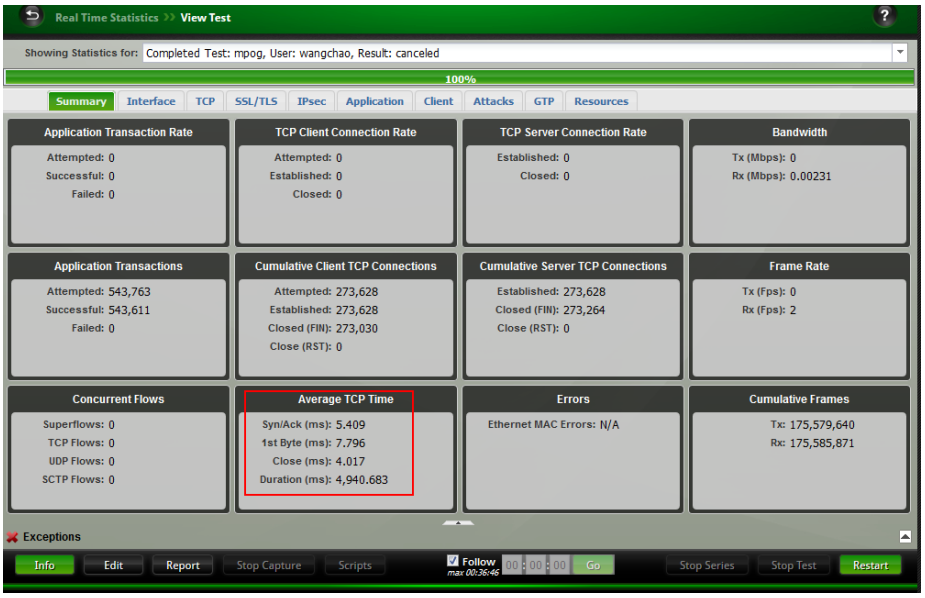
(5% UDP)*25%=125Mbps：
500Mbps





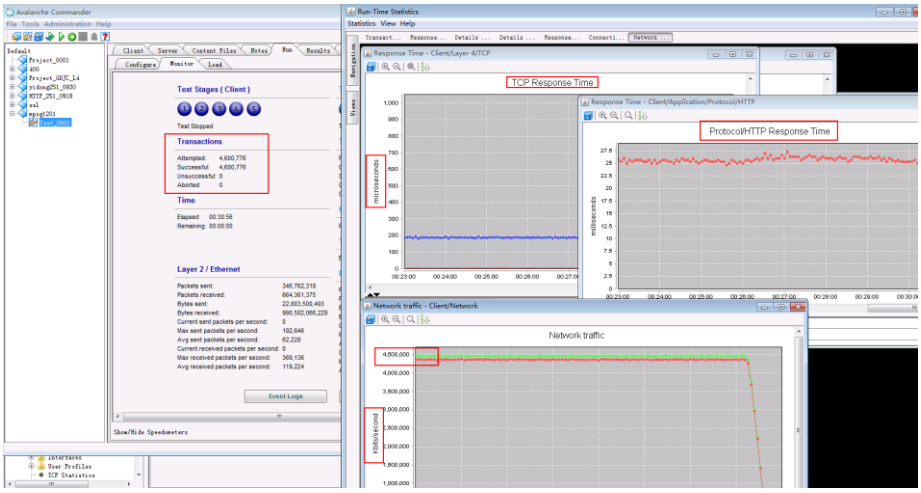
(5%Email+5%other Applications)*25%=150Mbps
600Mbps



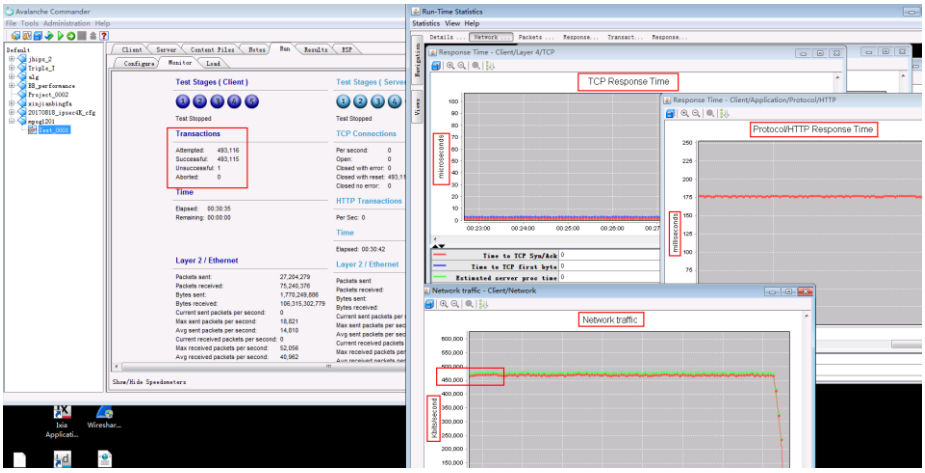


85% IMIX traffic of the lot required throughput:

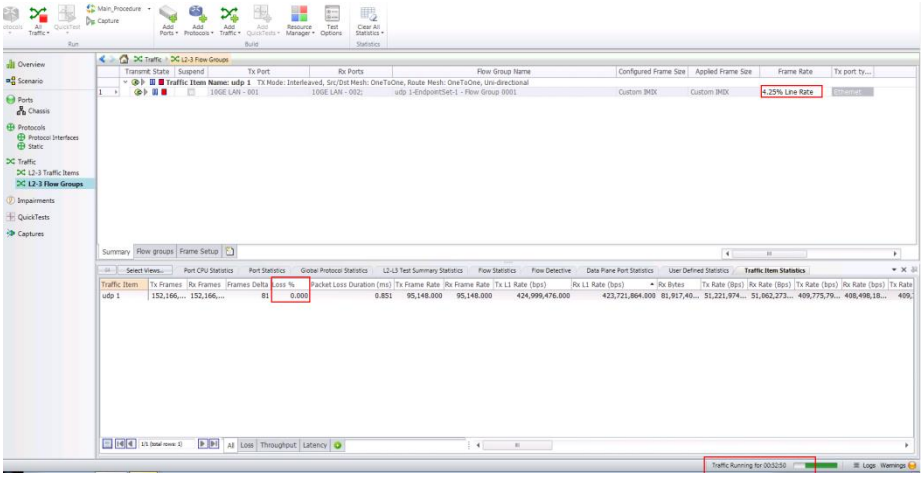
(80% HTTP+20% HTTPS)*85%=4.42G：
4.2G + 1G

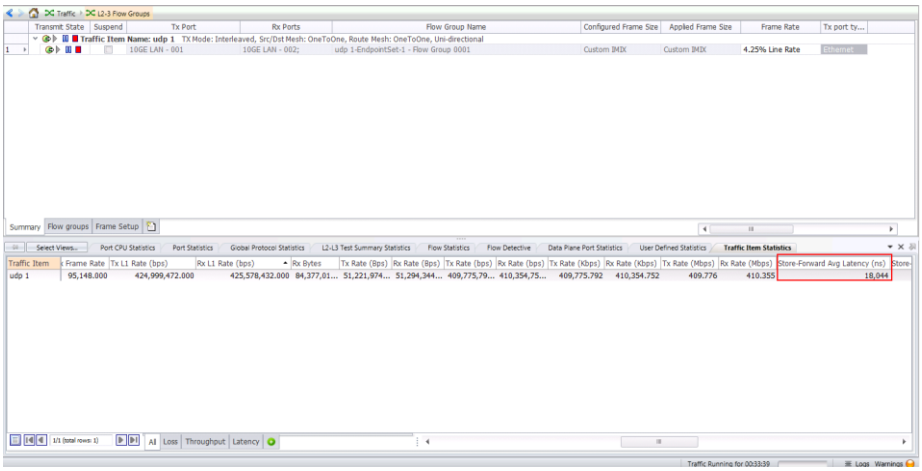


(5% IPSec VPN)*85%=450Mbps：
530Mbps



(5% UDP)*85%=425Mbps：
500Mbps

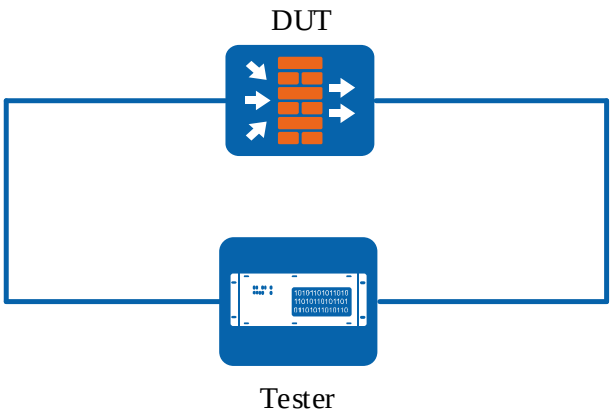


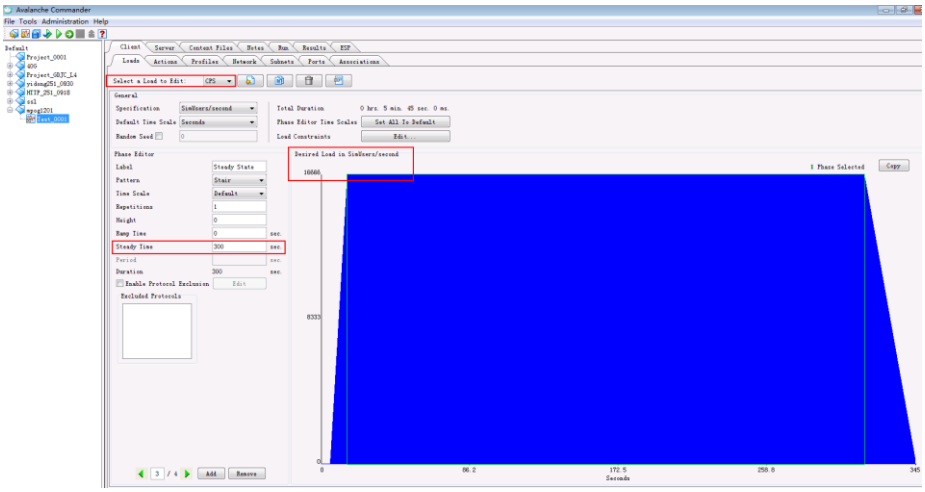
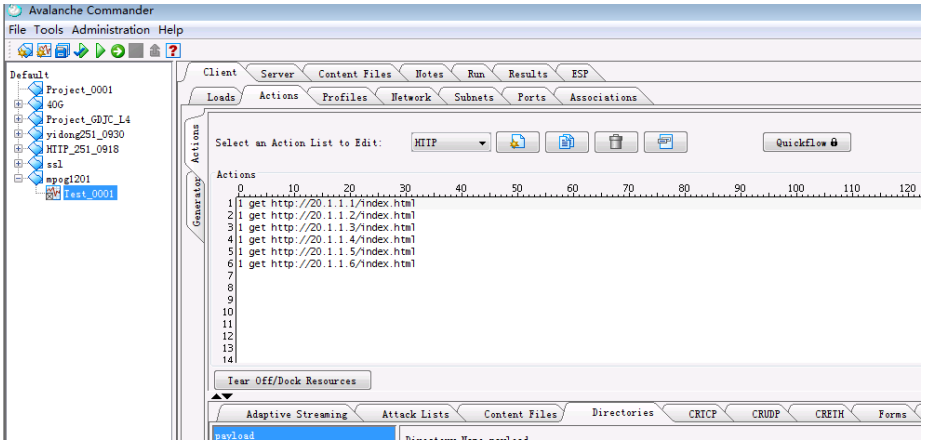


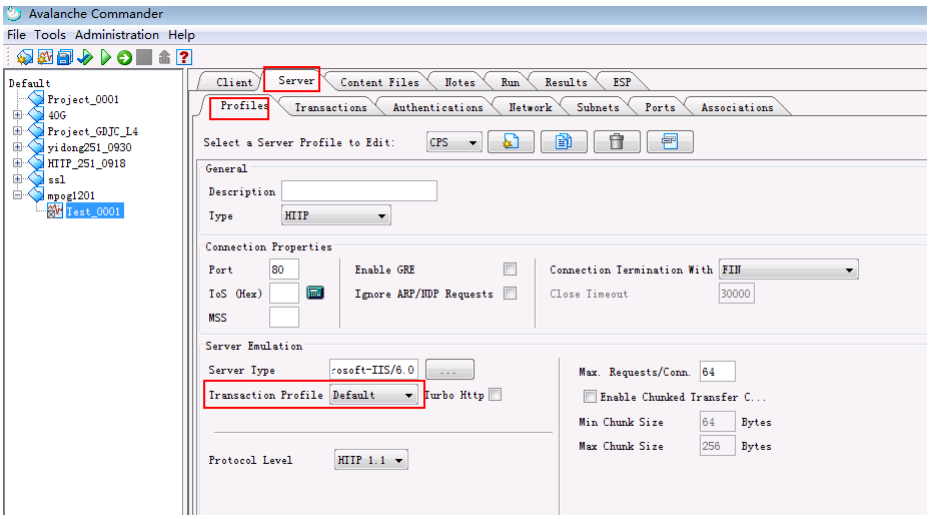
(5%Email+5%other Applications)*85%=510Mbps:
600Mbps

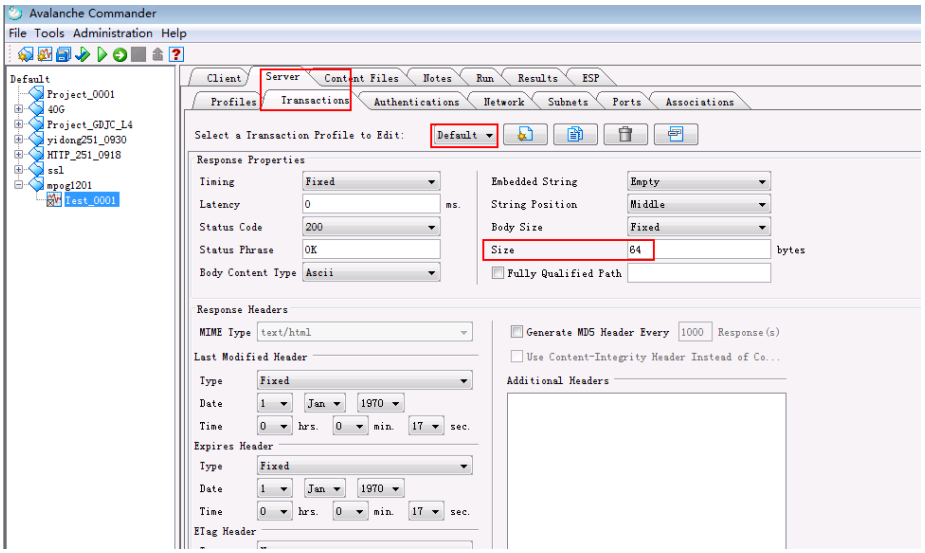
Resultado Esperado	1. Throughput can meet expectations.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

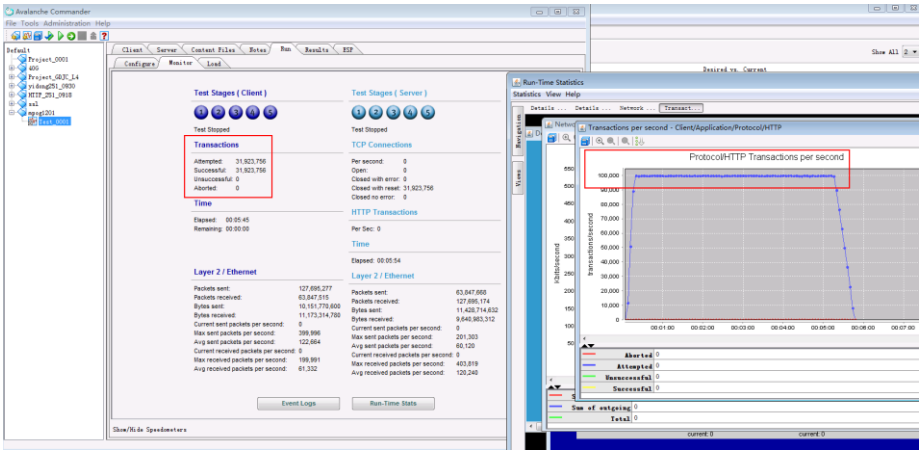
11.2 HTTP New Connections

Objetivo de teste	Verify the equipment capability of new connections.
Especificação de teste	The new connection rate refers to the number of HTTP new connection requests that a device can handle within a second. Every time a user opens a WEB page, or visits a server, it will establish one or more new connections on the device. And the higher the new connection rate is, the more users we can provide network access for. Test tools generally use Avalanche or IXIA.
Ambiente de teste	Test TOPO:  Pré-condição:

	1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Open the tester and structure the required flow; 1. Run HTTP new connections test. Modify parameters to get the maximal connections without failure.  


Avalanche Commander
File Tools Administration Help
Default
Project_0001
40G
Project_GDJC_L4
yidong251_0930
HTTP_251_0918
ssl
mpog1201
Test_0001
Client
Server
Content Files
Notes
Run
Results
ESP
Profiles
Transactions
Authentications
Network
Subnets
Ports
Associations
Select a Server Profile to Edit:
CPS
General
Description
Type
HTTP
Connection Properties
Port
80
ToS (Hex)
MSS
Enable GRE
Ignore ARP/NDP Requests
Connection Termination With
FIN
Close Timeout
30000
Server Emulation
Server Type
Transaction Profile
Default
Turbo Http
Protocol Level
HTTP 1.1
Max. Requests/Conn.
64
Enable Chunked Transfer C...
Min Chunk Size
Max Chunk Size
Bytes


Avalanche Commander
File Tools Administration Help
Default
Project_0001
40G
Project_GDJC_L4
yidong251_0930
HTTP_251_0918
ssl
mpog1201
Test_0001
Client
Server
Content Files
Notes
Run
Results
ESP
Profiles
Transactions
Authentications
Network
Subnets
Ports
Associations
Select a Transaction Profile to Edit:
Default
Response Properties
Timing
Fixed
Latency
0
ms.
Status Code
200
Status Phrase
OK
Body Content Type
Ascii
Embedded String
Empty
String Position
Middle
Body Size
Fixed
Size
64
bytes
Fully Qualified Path
Response Headers
MIME Type
text/html
Generate MD5 Header Every
1000
Response(s)
Use Content-Integrity Header Instead of Co...
Last Modified Header
Type
Fixed
Date
1
Jan
1970
Time
0
hrs.
0
min.
17
sec.
Expires Header
Type
Fixed
Date
1
Jan
1970
Time
0
hrs.
0
min.
17
sec.
ETag Header
Additional Headers


Test Stages (Client)
Test Stages (Server)
Transactions
TCP Connections
HTTP Transactions
Time
Layer 2 / Ethernet
Run-Time Statistics
Transactions per second - Client/Application/Protocol/HTTP
Protocol/HTTP Transactions per second

```
<USG6600>d f s s a
2017-12-11 09:16:51.340 +08:00
 Session Statistics:
 Slot 11 cpu 0: 1801854
 Total 1801854 [15.02%] session(s) on all slots.

 Session Creation Rate(num/s):
 Slot 11 cpu 0:  100048
 Total session(s) creation rate on all slots is 100048.

 Max Session Statistics:
 Slot 11 cpu 0: 2269457, time:2017/12/09 18:05:58
 Total max session(s) on all slot is 2269457, time is 2017/12/09 18:05:58.

 Max Session Creation Rate(num/s):
 Slot 11 cpu 0:  125404, time:2017/12/11 09:05:40
 Total max session(s) creation rate on all slot is 125404, time is 2017/12/11 09:05:40.
```

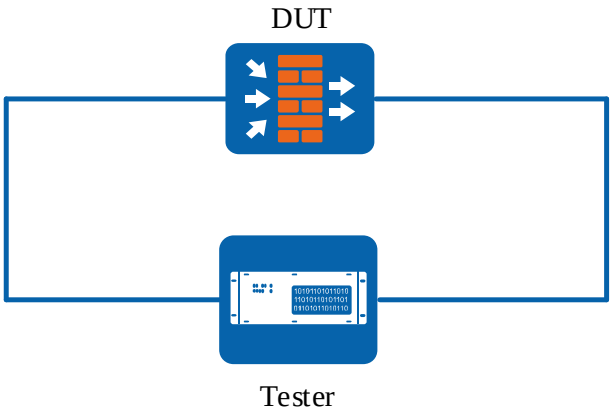
```
 HTTP  VPN: public --> public  19.1.1.188:3457[20.1.1.121:30207] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.110:17759[20.1.1.137:31321] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.136:51737[20.1.1.135:38538] --> 20.1.1.6:80
 HTTP  VPN: public --> public  19.1.1.142:34377[20.1.1.145:53728] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.139:32539[20.1.1.113:27485] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.217:42193[20.1.1.108:7947] --> 20.1.1.6:80
 HTTP  VPN: public --> public  19.1.1.20:43070[20.1.1.149:20909] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.163:8228[20.1.1.103:38276] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.39:62933[20.1.1.150:26972] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.98:42293[20.1.1.113:25857] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.65:37237[20.1.1.112:41958] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.242:52733[20.1.1.133:26274] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.160:13331[20.1.1.102:61870] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.126:5891[20.1.1.133:24840] --> 20.1.1.6:80
 HTTP  VPN: public --> public  19.1.1.126:6320[20.1.1.133:26615] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.78:20099[20.1.1.149:19438] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.170:13658[20.1.1.144:29490] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.98:43303[20.1.1.113:26355] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.165:52356[20.1.1.118:53686] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.121:5702[20.1.1.138:29795] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.190:36653[20.1.1.143:41757] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.141:25298[20.1.1.131:28600] --> 20.1.1.5:80
```

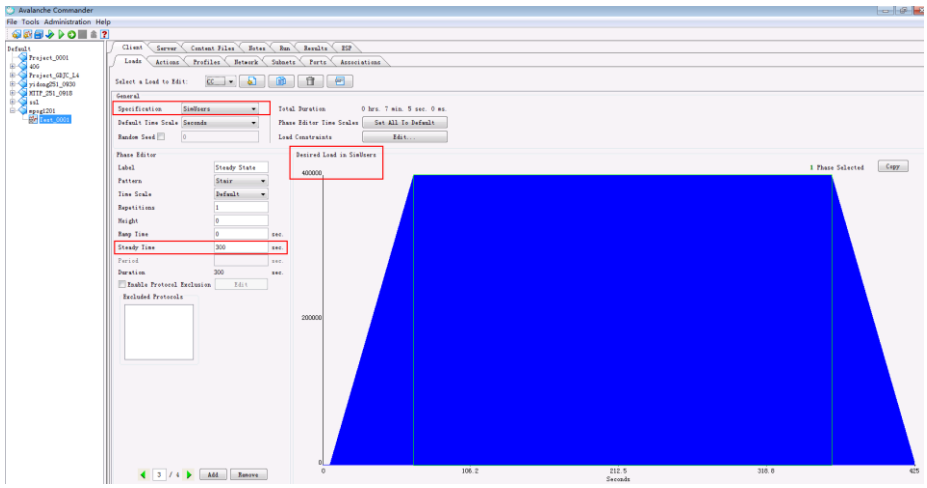
CPU usage is 74.9%:

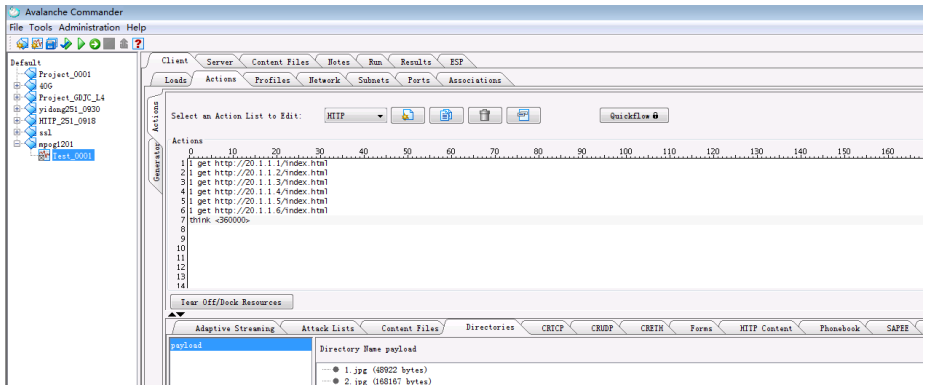
```
<USG6600>disp cpu-usage
2017-12-11 09:10:16.540 +08:00
CPU Usage Stat. Cycle: 10 (Second)
CPU Usage             :  74.9%  Max:  90.6%
Management-plane CPU Usage:  12.6%   Data-plane CPU Usage :  76.9%
CPU utilization for ten seconds:  74.9% : one minute:  75.1% : five minutes:  70.3%

PID   ProcessName          CPU       Runtime     State
1067  fpath.out          54.6%      179804269   S
1086  nge.out            18.0%      3160520     S
1069  nlog.out            1.6%      448800      S
635   vrp                 0.3%      6000940     S
1016  vrpio_s             0.0%      550951      S
1088  slb_proxy.out       0.0%      333612      S
1078  ike.out             0.0%      68832       S
1079  am.out              0.0%      45008       S
1074  mail_send.out       0.0%      5668        S
1081  auth.out            0.0%      82927       S
1023  procmgmt.out        0.0%      18785       S
1070  svn.out             0.0%      5635        S
1226  https.out           0.0%      3775112     S
1083  xmpp.out            0.0%      22731       S
1076  mail_proxy.out      0.0%      15543       S
1082  ssa.out             0.0%      5137        S
1087  netopeer-server.out  0.0%      3998        S
1085  disk_smart.out      0.0%      3532        S
```

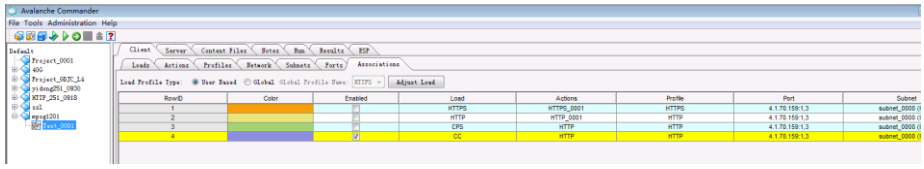
Resultado Esperado	1. New connections rate can meet expectations.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

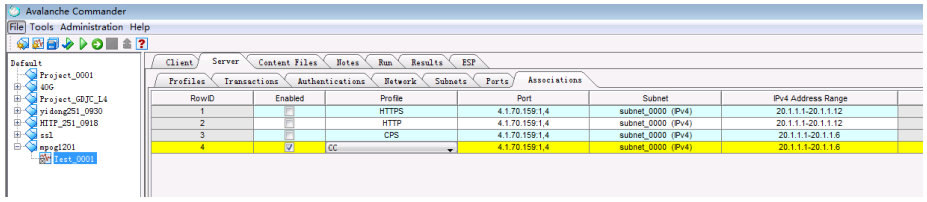
11.3 HTTP Concurrent

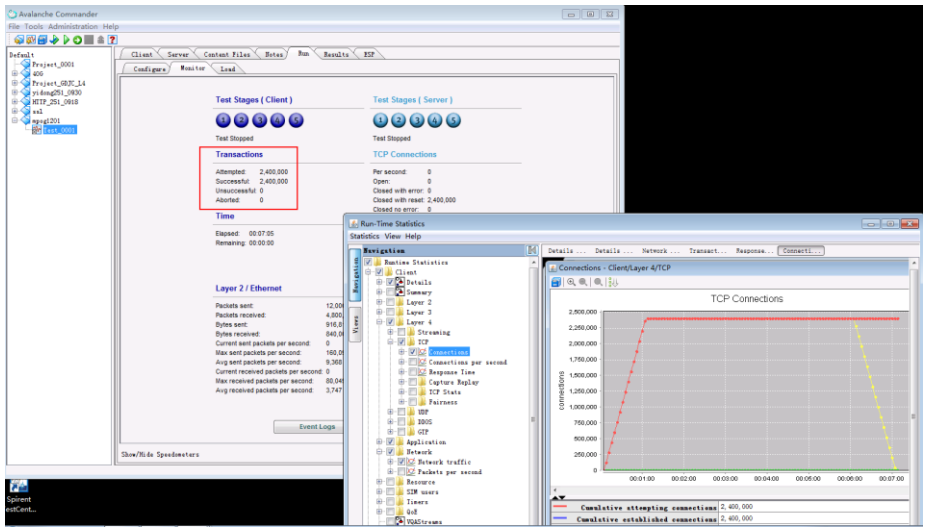
Objetivo de teste	Verify the equipment capability of concurrent.
Especificação de teste	The number of concurrent connections refers to the number of connections that a device can maintain at the same time. With the increasing complexity of WEB applications and the wide use of P2P programs, each user generated more and more connections, or even a user's number of connections may be thousands, so the larger HTTP concurrent is, the more users can have access to the Internet at the same time. Test tools generally use Avalanche or IXIA.
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Open the tester and structure the required flow; 2. Run HTTP concurrent test. Modify parameters to get the maximal concurrent connections.


Avalanche Commander
File Tools Administration Help
Desired Load in SimUsers
Seconds


Avalanche Commander
File Tools Administration Help
Select an Action List to Edit:
HTTP
Quickflow
Actions
1 get http://20.1.1.1/index.html
1 get http://20.1.1.2/index.html
1 get http://20.1.1.3/index.html
1 get http://20.1.1.4/index.html
1 get http://20.1.1.5/index.html
1 get http://20.1.1.6/index.html
think <360000>
Tear Off/Dock Resources
Directory Name payload
1.jpg (48922 bytes)
2.jpg (168167 bytes)


Avalanche Commander
File Tools Administration Help


Avalanche Commander
File Tools Administration Help
RowID
Enabled
Profile
Port
Subnet
IPv4 Address Range
1 HTTPS 4.1.70.159:1,4 subnet_0000 (IPv4) 20.1.1.1-20.1.1.12
2 HTTP 4.1.70.159:1,4 subnet_0000 (IPv4) 20.1.1.1-20.1.1.12
3 CPS 4.1.70.159:1,4 subnet_0000 (IPv4) 20.1.1.1-20.1.1.6
4 CC 4.1.70.159:1,4 subnet_0000 (IPv4) 20.1.1.1-20.1.1.6


Avalanche Commander
Test Stages (Client)
Test Stages (Server)
Transactions
TCP Connections
Layer 2 / Ethernet
Run-Time Statistics
TCP Connections

Memory usage is 73%:

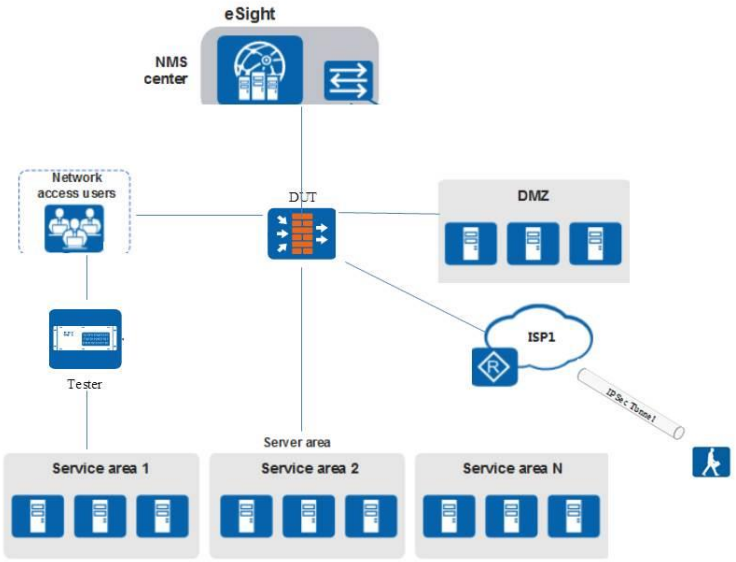
```
<USG6600>disp memory-usage
 Memory utilization statistics at 2017-12-11 11:00:34+08:00
 System Total Memory Is: 616562688 bytes
 Total Memory Used Is: 452813908 bytes
 Memory Using Percentage Is: 73%
 (The statistics count only management-plane memory resources.)
 --------------------------slot 11----------------------------------
 Device Total Memory Is: 16750108672 bytes
 Total Memory Used Is: 9943308288 bytes
 Memory Using Percentage Is: 59%
 --------------------------slot 12----------------------------------
 Device Total Memory Is: 16483516416 bytes
 Total Memory Used Is: 13328149504 bytes
 Memory Using Percentage Is: 80%
<USG6600>disp firewall session statistics all
 Session Statistics:
 Slot 11 cpu 0: 2400001
 Total 2400001 [20.00%] session(s) on all slots.

 Session Creation Rate(num/s):
 Slot 11 cpu 0:       0
 Total session(s) creation rate on all slots is 0.

 Max Session Statistics:
 Slot 11 cpu 0: 2400001, time:2017/12/11 11:00:59
 Total max session(s) on all slot is 2400001, time is 2017/12/11 11:00:59.

 Max Session Creation Rate(num/s):
 Slot 11 cpu 0:  130585, time:2017/12/11 09:29:40
 Total max session(s) creation rate on all slot is 130585, time is 2017/12/11 09:29:40.
```

```
[USG6600]disp firewall  session table
 Current Total Sessions : 2400001
 HTTP  VPN: public --> public  19.1.1.55:6998[20.1.1.101:40955] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.124:2464[20.1.1.115:40170] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.135:12459[20.1.1.128:58733] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.72:25439[20.1.1.123:47591] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.119:45156[20.1.1.132:57386] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.61:41314[20.1.1.116:23460] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.81:31439[20.1.1.103:32555] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.244:31612[20.1.1.125:33368] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.32:13695[20.1.1.147:9372] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.250:3379[20.1.1.107:58335] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.20:63569[20.1.1.149:57438] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.23:21216[20.1.1.126:29637] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.182:54091[20.1.1.117:51578] --> 20.1.1.3:80
 HTTP  VPN: public --> public  19.1.1.55:6082[20.1.1.101:38554] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.120:35929[20.1.1.132:53532] --> 20.1.1.6:80
 HTTP  VPN: public --> public  19.1.1.224:60409[20.1.1.150:51876] --> 20.1.1.6:80
 HTTP  VPN: public --> public  19.1.1.177:30484[20.1.1.144:33933] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.17:32478[20.1.1.117:57918] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.114:7884[20.1.1.137:57957] --> 20.1.1.4:80
 HTTP  VPN: public --> public  19.1.1.62:37540[20.1.1.101:42580] --> 20.1.1.1:80
 HTTP  VPN: public --> public  19.1.1.197:29563[20.1.1.146:45416] --> 20.1.1.5:80
 HTTP  VPN: public --> public  19.1.1.213:11621[20.1.1.137:61872] --> 20.1.1.2:80
 HTTP  VPN: public --> public  19.1.1.152:48607[20.1.1.125:39955] --> 20.1.1.2:80
  ---- More ----
```

Resultado Esperado	1. Concurrent number can meet expectations.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

12 Configurações de Testes e Topologia

Teste objetivo	Definir um catálogo de configurações da amostra, a topologia e o tráfego para os testes.
Especificação de	Configurar as funcionalidades de firewall, tal como previstas na especificação

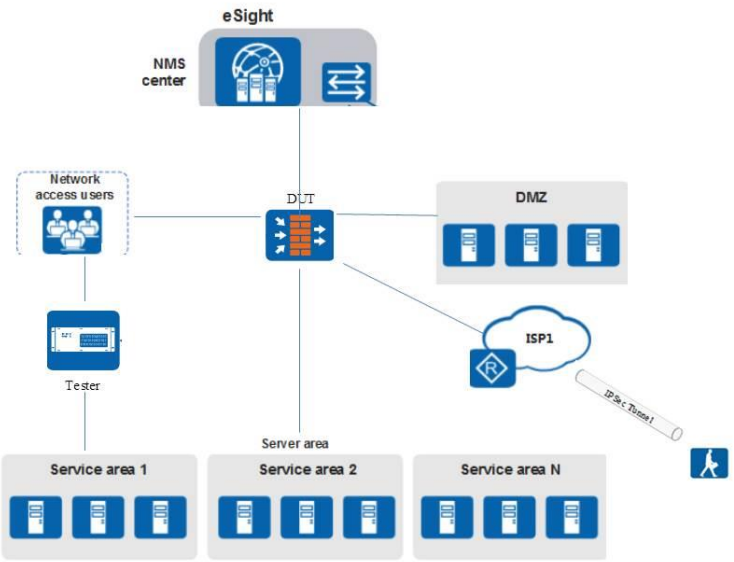
teste	técnica do Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso (controle de aplicações e filtragem de URL's), sistema de detecção/prevenção a intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e Anti-malware), administração de largura de banda de serviço (QoS), descriptografia, inspeção de tráfego SSL e suporte para conexões VPN IPSec.
Ambiente de teste	Teste de TOPO:  Pré-condição: 1. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de 1.500 clientes; 2. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores é de 200. 3. A Rede Externa deverá possuir 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 é de 1.500 e 200 servidores; 4. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1

	(uma) regra específica de acesso no Firewall. A quantidade de 500 regras; 5. Percentual de trafego configurado conforme abaixo: 5.1. A amostra deve ser 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 diretrizes e políticas de Firewalls do NIST, com a seguinte distribuição média, permitindo-se variações em até 10%: 5.2. HTTP = 55% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes, sendo uma reserva de 5% para arquivos com malwares e 1% para ataques). 5.3. 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). 5.4. Aplicações, outros ataques, outras ameaças e outros protocolos = 20%, a ser acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes. 5.5. 5% VPN (PiSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes) 5.6. E-mail (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos). 5.7. 5% UDP (distribuição de tamanho: 56% 72 bytes, 17% 512 bytes e 27% 1518 bytes). 5.8. 4% de aplicações (qualquer protocolo e com tamanho variável). 5.9. Outros (distribuição de tamanho variável)
Procedimento de teste	1. Testar bloqueio do acesso pela ISP utilizando IP´s por “geolocalização”; 2. Testar acesso às aplicações pelos usuários aos serviços na área de servidores; 3. Testar acesso a URL´s através de filtragem pelo DUT; 4. Habilitar IDS e IPS com assinaturas atualizadas no DUT;

	5. Habilitar Antivírus e Anti-malware com assinaturas atualizadas no DUT; 6. Criação de QoS para aplicações especificas na Server Area; 7. Testar “SSL inspection”; 8. Testar acesso externo pelo ISP1 para usuários utilizando IPSec VPN.			
Resultado esperado	1. Homologar ambiente para inicio dos testes.			
Resultado do teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Ao cliente**		**Huawei**	

13 Detecção/prevenção à intrusão/ataques (IDS/IPS)

Teste objetivo	Comprovar detecção/prevenção à intrusão/ataques (IDS/IPS) conforme requisitos.
Especificação de teste	Configurar as funcionalidades de firewall, tal como previstas na especificação técnica do Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso (controle de aplicações e filtragem de URL’s), sistema de detecção/prevenção a intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e Anti-malware), administração de largura de banda de serviço (QoS), descriptografia, inspeção de tráfego SSL e suporte para conexões VPN IPSec.
Ambiente de teste	Teste de TOPO:



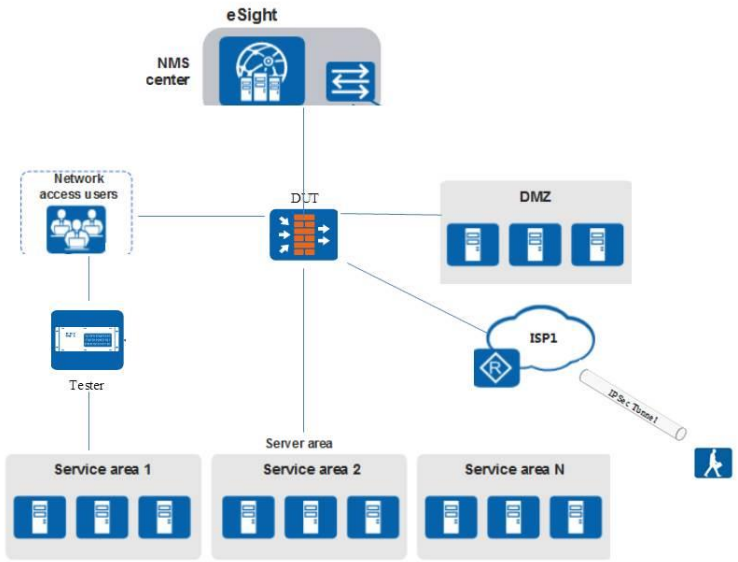
Pré-condição:

1. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de 1.500 clientes;
2. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores é de 200.
3. A Rede Externa deverá possuir 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 é de 1.500 e 200 servidores;
4. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1 (uma) regra específica de acesso no Firewall. A quantidade de 500 regras;
5. Percentual de trafego configurado conforme abaixo:

5.1. A amostra deve ser 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 diretrizes e políticas de Firewalls do NIST, com a seguinte distribuição média, permitindo-se variações em até 10%:

	5.2. HTTP = 55% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes, sendo uma reserva de 5% para arquivos com malwares e 1% para ataques). 5.3. 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). 5.4. Aplicações, outros ataques, outras ameaças e outros protocolos = 20%, a ser acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes. 5.5. 5% VPN (PiSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes) 5.6. E-mail (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos). 5.7. 5% UDP (distribuição de tamanho: 56% 72 bytes, 17% 512 bytes e 27% 1518 bytes). 5.8. 4% de aplicações (qualquer protocolo e com tamanho variável). 5.9. Outros (distribuição de tamanho variável)			
Procedimento de teste	1. Testar ataques de, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS;			
Resultado esperado	1. Bloqueio do trafego malicioso.			
Resultado do teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Ao cliente**		**Huawei**	

14 Proteção contra ameaças (Antivírus e Anti-malware)

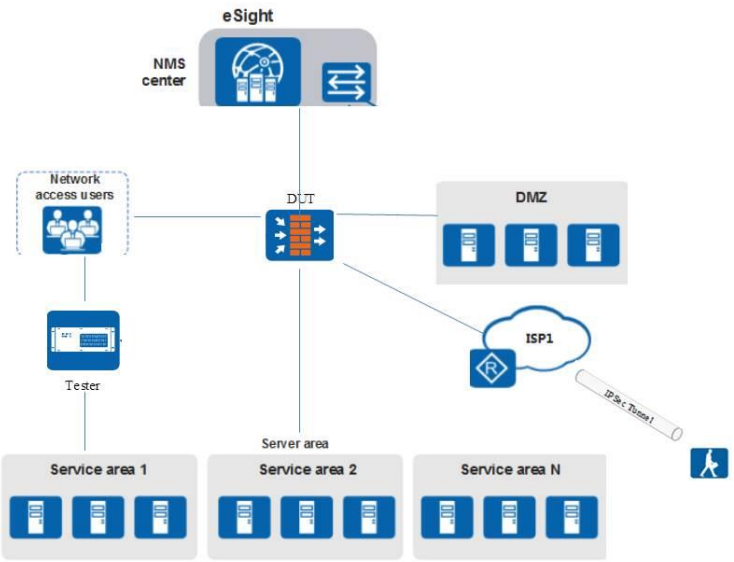
Teste objetivo	Comprovar proteção contra ameaças (Antivírus e Anti-malware) conforme requisitos.
Especificação de teste	Configurar as funcionalidades de firewall, tal como previstas na especificação técnica do Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso (controle de aplicações e filtragem de URL's), sistema de detecção/prevenção a intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e Anti-malware), administração de largura de banda de serviço (QoS), descriptografia, inspeção de tráfego SSL e suporte para conexões VPN IPSec.
Ambiente de teste	Teste de TOPO:  Pré-condição: 1. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de 1.500 clientes; 2. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores é de 200. 3. A Rede Externa deverá possuir 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 é de 1.500 e 200 servidores; 4. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1 (uma) regra específica de acesso no Firewall. A quantidade de 500 regras; 5. Percentual de trafego configurado conforme abaixo: 5.1. A amostra deve ser 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 diretrizes e políticas de Firewalls do NIST, com a seguinte distribuição média, permitindo-se variações em até 10%: 5.2. HTTP = 55% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes, sendo uma reserva de 5% para arquivos com malwares e 1% para ataques). 5.3. 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). 5.4. Aplicações, outros ataques, outras ameaças e outros protocolos = 20%, a ser acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes. 5.5. 5% VPN (PiSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes) 5.6. E-mail (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos). 5.7. 5% UDP (distribuição de tamanho: 56% 72 bytes, 17% 512 bytes e 27% 1518 bytes). 5.8. 4% de aplicações (qualquer protocolo e com tamanho variável). 5.9. Outros (distribuição de tamanho variável)

Procedimento de teste	1. Testar ameaças de, no mínimo 2.000 (duas mil) assinaturas de malwares distintas;			
Resultado esperado	1. Bloqueio do trafego malicioso.			
Resultado do teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Ao cliente**		**Huawei**	

15 Controle de acesso (controle de aplicações e filtragem de URL's)

Teste objetivo	Comprovar controle de aplicações e filtragem de URL's conforme requisitos.
Especificação de teste	Configurar as funcionalidades de firewall, tal como previstas na especificação técnica do Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso (controle de aplicações e filtragem de URL's), sistema de detecção/prevenção a intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e Anti-malware), administração de largura de banda de serviço (QoS), descriptografia, inspeção de tráfego SSL e suporte para conexões VPN IPSec.
Ambiente de teste	Teste de TOPO:

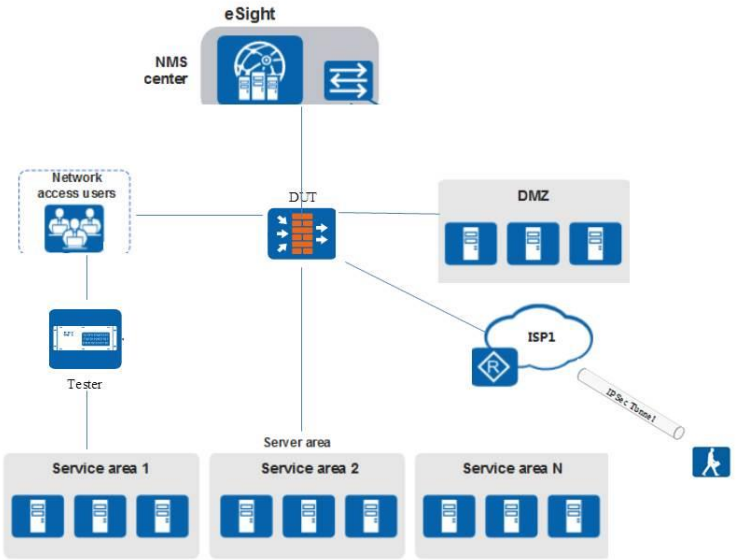


1. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de 1.500 clientes;
2. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores é de 200.
3. A Rede Externa deverá possuir 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 é de 1.500 e 200 servidores;
4. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1 (uma) regra específica de acesso no Firewall. A quantidade de 500 regras;
5. Percentual de trafego configurado conforme abaixo:

5.1. A amostra deve ser 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 diretrizes e políticas de Firewalls do NIST, com a seguinte distribuição média, permitindo-se variações em até 10%:

	5.2. HTTP = 55% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes, sendo uma reserva de 5% para arquivos com malwares e 1% para ataques). 5.3. 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). 5.4. Aplicações, outros ataques, outras ameaças e outros protocolos = 20%, a ser acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes. 5.5. 5% VPN (PiSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes) 5.6. E-mail (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos). 5.7. 5% UDP (distribuição de tamanho: 56% 72 bytes, 17% 512 bytes e 27% 1518 bytes). 5.8. 4% de aplicações (qualquer protocolo e com tamanho variável). 5.9. Outros (distribuição de tamanho variável)			
Procedimento de teste	1. Testar acessos de, no mínimo, 5.000 (cinco mil) sites distintos de internet, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias distintas; 2. Testar para um mínimo de 100 (cem) aplicações.			
Resultado esperado	1. Bloqueio das URL´s conforme aplicação.			
Resultado do teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Ao cliente**		**Huawei**	

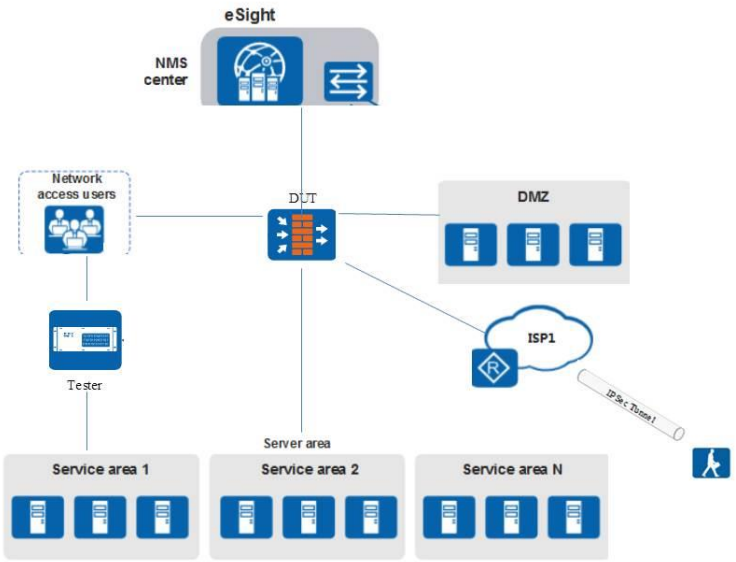
16 Teste de assertividade

Teste objetivo	Mensurar a eficácia das funcionalidades da amostra, em relação às categorizações, os bloqueios e às detecções de ameaças, ataques, URLs e aplicações.
Especificação de teste	Verificação da eficácia das funcionalidades da amostra.
Ambiente de teste	Teste de TOPO:  1. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de 1.500 clientes; 2. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores é de 200. 3. A Rede Externa deverá possuir 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 é de 1.500 e 200 servidores; 4. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1 (uma) regra específica de acesso no Firewall. A quantidade de 500 regras; 5. Percentual de trafego configurado conforme abaixo:

	5.1. A amostra deve ser 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 diretrizes e políticas de Firewalls do NIST, com a seguinte distribuição média, permitindo-se variações em até 10%: 5.2. HTTP = 55% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes, sendo uma reserva de 5% para arquivos com malwares e 1% para ataques). 5.3. 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). 5.4. Aplicações, outros ataques, outras ameaças e outros protocolos = 20%, a ser acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes. 5.5. 5% VPN (PiSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes) 5.6. E-mail (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos). 5.7. 5% UDP (distribuição de tamanho: 56% 72 bytes, 17% 512 bytes e 27% 1518 bytes). 5.8. 4% de aplicações (qualquer protocolo e com tamanho variável). 5.9. Outros (distribuição de tamanho variável)
Procedimento de teste	1.Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS; 2. Categorizar e bloquear as ameaças em, no mínimo 2.000 (duas mil) assinaturas de malwares distintas; 3. Categorizar e bloquear, pelo menos, 100 (cem) aplicações distintas; 4.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.			
Resultado esperado	1. Atender às expectativas acima.			
Resultado do teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Ao cliente**		**Huawei**	

17 Teste de Desempenho

Teste objetivo	Mesurar o desempenho da amostra em consonância com os requisitos técnicos exigidos no anexo "B", em relação à taxa de transferência (throughtput) e performance. **(throughput de 5 Gbps)**
Especificação de teste	Durante os testes de desempenho minimamente deverão ser 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.
Ambiente de teste	Teste de TOPO:  Pré-condição:

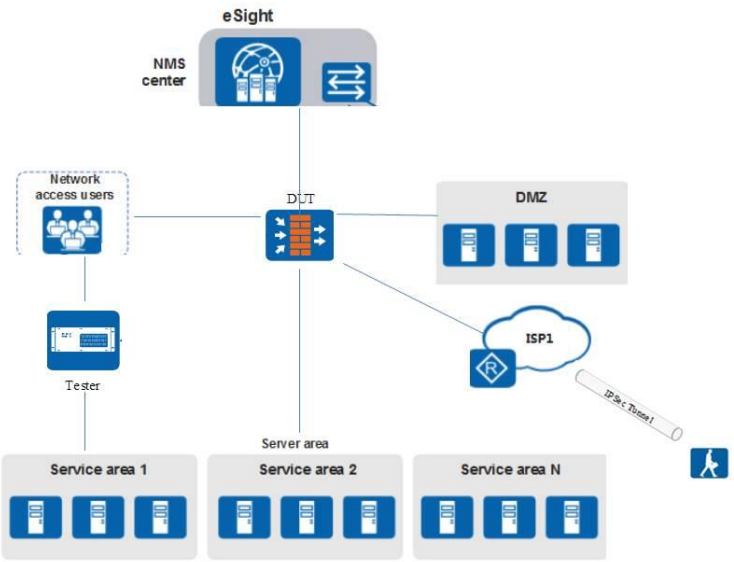
	1. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de 1.500 clientes; 2. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores é de 200. 3. A Rede Externa deverá possuir 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 é de 1.500 e 200 servidores; 4. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1 (uma) regra específica de acesso no Firewall. A quantidade de 500 regras; 5. Percentual de trafego configurado conforme item 5.1.12 do termo de referencia.
Procedimento de teste	1. A amostra deverá ser 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; 2. Após a realização da parametrização descrita no caput, o firewall da Amostra deverá ter todos os seus contadores zerados; 3. 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; 4. A amostra deverá ser então submetida a uma taxa de transferência de 85% do throughput do lote, no padrão de tráfego conforme já estabelecida, sendo testado, por 30 minutos contínuos e ininterruptos e não poderá apresentar prejuízo em sua performance;

	5. 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;
Resultado esperado	1. Serão comparados os parâmetros coletados nos itens 3 e 5 acima, sendo considerado prejuízo na performance do equipamento a ocorrência de quaisquer dos eventos a seguir: 1.1 Perdas absolutas de pacotes superiores a 1%. 1.2 Erros absolutos irrecuperáveis de transações TCP/layer-7 superior a 0,5%. 1.3 Valores de latência média ou de variação média de latência (jitter) acima de 10 x (vezes) dos valores coletados da taxa de transferência (throughtput) ou seja o somatório das interfaces de entrada do gerador de tráfego, após passagem do tráfego no equipamento testado.
Resultado do teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

Assinatura	**Ao cliente**		**Huawei**	

18 Teste de Sessões

Teste objetivo	Mensurar o desempenho da amostra em consonância com os requisitos técnicos exigidos no anexo “B”, em relação às novas sessões por segundo e sessões simultâneas**. (sessões simultâneas 2.000.000)**
Especificação de teste	Mensuração de novas sessões simultâneas do número de sessões simultâneas TCP, que é estabelecido no Anexo B, por no mínimo 5 minutos contínuos e ininterruptos.
Ambiente de teste	Teste de TOPO:



Pré-condição:

1. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de 1.500 clientes;
2. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores é de 200.
3. A Rede Externa deverá possuir 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 é de 1.500 e 200 servidores;
4. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1 (uma) regra específica de acesso no Firewall. A quantidade de 500 regras;
5. Percentual de trafego configurado conforme já especificado do termo de referencia.

Procedimento de teste	1. Mensuração de sessões simultâneas, deve ser utilizado tráfego HTTP puro e, no mínimo, objeto de 64 bytes; 2. Mensuração de novas sessões por segundo, cada uma deverá ser estabelecida,

	minimamente, por meio de handshake de três vias (three-way handshake).			
Resultado esperado	1. A amostra será considerada aprovada no segundo teste de sessões se for considerada aprovada nas mensurações dos itens 5.4.3.1 e 5.4.3.2.			
Resultado do teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Ao cliente**		**Huawei**	

19 Testes Complementares

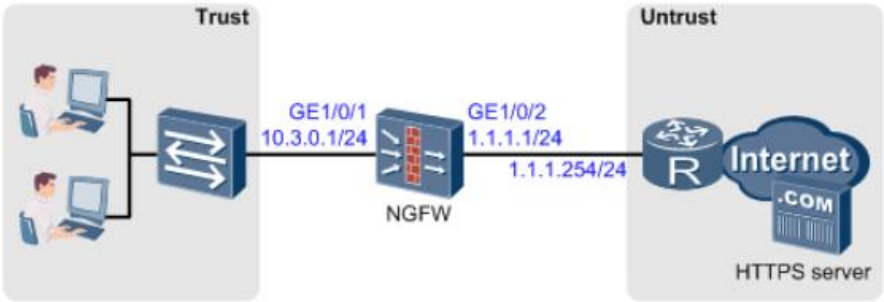
19.1 Item 2.1.29

Objetivo de teste	Possuir proteção e suporte a protocolos de Real Time.
Especificação de teste	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.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).

Procedimento de Teste	1. Logar via CLI e verificar os serviços pre-definidos.
	`<sysname> display predefined-service`
	`h323 udp/1719`
	`h323-rtcp h323-rtcp protocol ( dynamic port )`
	`h323-rtp h323-rtp protocol ( dynamic port )`
	`h323-t120 h323-t120 protocol ( dynamic port )`
	`sip-rtp sip-rtp protocol ( dynamic port )`

Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.1.29.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.2 Item 2.1.39

Objetivo de teste	Possuir inspeção profunda de pacotes para tráfego criptografado.
Especificação de teste	Possuir inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPN e HTTPS).
Ambiente de teste	Test TOPO:  Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Configurar os certificados para descriptografar o SSL. Será necessário dois certificados, um é confiável e o outro não é confiável; 2. O certificado confiável é o certificado que todos os clientes da intranet devem instalar e confiar. Você pode importar um para o NGFW ou usar o CA incorporado no NGFW para gerar um.
Resultado Esperado	2. Verificar o suporte as funcionalidades do item 2.1.39.

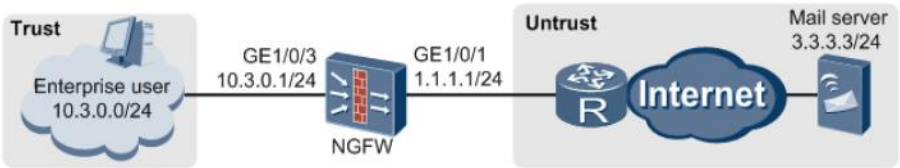
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.3 Item 2.1.45.6

Objetivo de teste	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede.
Especificação de teste	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Pode ser verificado no item 6 “Security Control” desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.1.45.6.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

19.4 Item 2.1.45.9

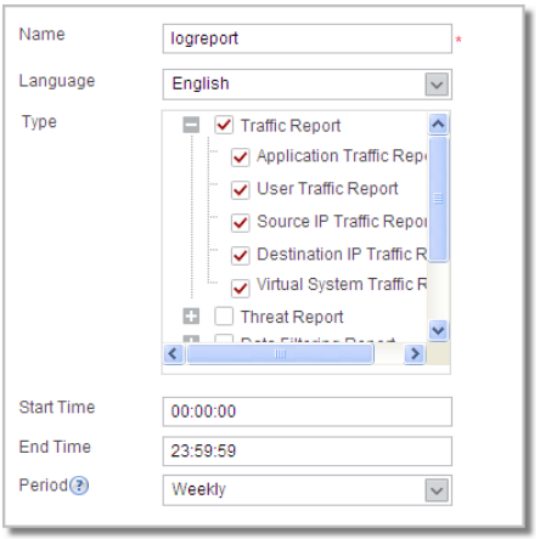
12.4.1 Envio de email.

<table>
<tr><td>Objetivo de teste</td><td>Deve suportar a geração de alertas automáticos via email, SNMP e Syslog.</td></tr>
<tr><td>Especificação de teste</td><td>Deve suportar a geração de alertas automáticos via email.</td></tr>
<tr><td>Ambiente de teste</td><td>Test TOPO:
 

Pré-condição:
1. Equipamentos operacionais e com acesso pelo console.
2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos;
3. Atribuir a interface para a zona de segurança correspondente;
4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).</td></tr>
<tr><td>Procedimento de Teste</td><td>1. Configurar as interfaces IP , zonas de segurança e politicas de segurança interzonas;
<table>
<tr><td>Name</td><td>policy_security_0</td></tr>
<tr><td>Source Zone</td><td>local</td></tr>
<tr><td>Destination Zone</td><td>Untrust</td></tr>
<tr><td>Destination Address/Region</td><td>3.3.3.0/24</td></tr>
<tr><td>Action</td><td>Permit</td></tr>
</table>
<table>
<tr><td>Name</td><td>policy_security_1</td></tr>
<tr><td>Source Zone</td><td>trust</td></tr>
<tr><td>Destination Zone</td><td>Untrust</td></tr>
<tr><td>Source Address/Region</td><td>10.3.0.0/24</td></tr>
<tr><td>Action</td><td>Permit</td></tr>
</table>
2. Criar um “report” para que o Firewall envie alertas customizados para um determinado e-mail;</td></tr>
</table>

a. Choose **Monitor** > **Report** > **Customized Report**.

b. Click **Add** in **Customized Report List**, and set the parameters as follows.

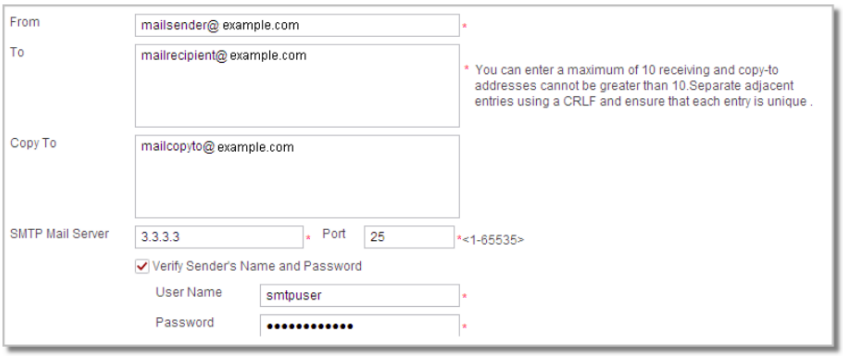


c. Click **OK**.

3. Configurar o email para serem enviados automaticamente.

a. Choose **System** > **Set Mail Service**.

b. In **Set Mail Service**, set the parameters as follows.



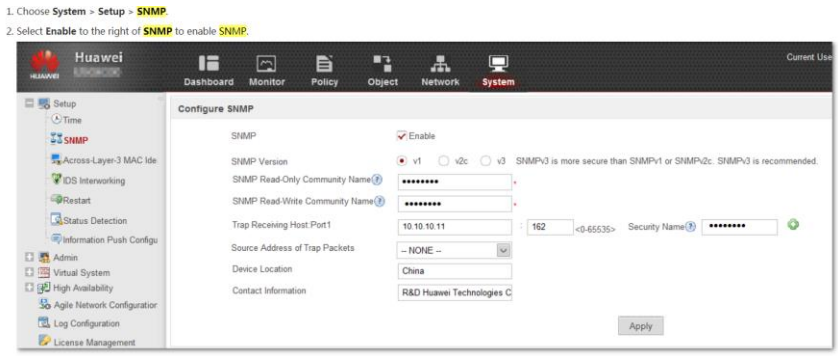
c. Click **Apply**.

d. Click **Send Test Email** and check whether the recipient email box receives the report.

Resultado Esperado	2. Verificar o suporte as funcionalidades do item 2.1.45.9 envio de email.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

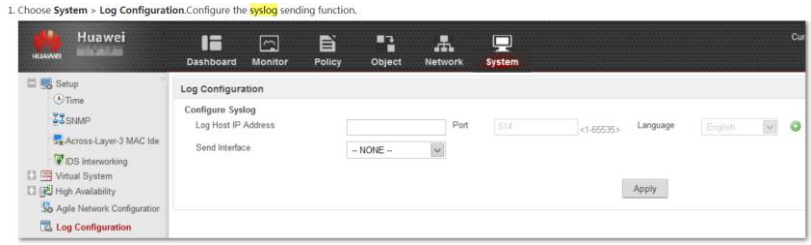
12.4.2 Envio de SNMP.

Objetivo de teste	Deve suportar a geração de alertas automáticos via email, SNMP e Syslog.
Especificação de teste	Deve suportar a geração de alertas automáticos via SNMP.

Ambiente de teste	Test TOPO: Pre-condition: 1. All test devices start normally; 2. Set up the testing environment according to test TOPO and configure all the devices IP addresses; 3. Assign interface into the corresponding security zone; 4. Configure the routings, make sure the devices can ping each other.			
Procedimento de Teste	1. Configurar o SNMP e o TRAP Receiver:  			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.1.45.9 envio SNMP.			
Resultado do Teste	☐Pass ☐Partial Pass ☐Fail ☐Not test or NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

12.4.3 Envio de Syslog.

Objetivo de teste	Deve suportar a geração de alertas automáticos via email, SNMP e Syslog.
Especificação de teste	Deve suportar a geração de alertas automáticos via Syslog.
Ambiente de teste	Test TOPO: Pre-condition: 5. All test devices start normally; 6. Set up the testing environment according to test TOPO and configure all the devices IP addresses;

	7. Assign interface into the corresponding security zone; 8. Configure the routings, make sure the devices can ping each other.
Procedimento de Teste	1. Configurar o Syslog: 
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.1.45.9 envio Syslog.
Resultado do Teste	☐Pass ☐Partial Pass ☐Fail ☐Not test or NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

19.5 Item 2.1.45.12

Objetivo de teste	Deve informar o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.
Especificação de teste	Deve informar o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Verificar o numero de sessões simultâneas e de novas sessões por segundo ;

<table>
<tr><td></td><td colspan="4">Procedure
1. Choose Monitor > Session Table.
2. View information about session entries on the Session Table page.
Example
The session table of a specified time range is displayed as follows:
<table>
<tr><th>Details</th><th>Proto...</th><th>Source ...</th><th>Desti...</th><th>Source Address</th><th>Destination Addr...</th><th>Source P...</th><th>Destination ...</th><th>Left Time</th><th>Outbound In...</th><th>Next Hop</th></tr>
<tr><td></td><td>https</td><td>trust</td><td>local</td><td>172.16.10.178</td><td>10.18.74.29</td><td>62001</td><td>8443</td><td>00:10:00</td><td>InLoopBack0</td><td>127.0.0.1</td></tr>
<tr><td></td><td>https</td><td>trust</td><td>local</td><td>172.16.10.133</td><td>10.18.74.29</td><td>51513</td><td>8443</td><td>00:10:00</td><td>InLoopBack0</td><td>127.0.0.1</td></tr>
<tr><td></td><td>https</td><td>trust</td><td>local</td><td>172.16.10.134</td><td>10.18.74.29</td><td>59740</td><td>8443</td><td>00:09:56</td><td>InLoopBack0</td><td>127.0.0.1</td></tr>
<tr><td></td><td>https</td><td>trust</td><td>local</td><td>172.16.10.134</td><td>10.18.74.29</td><td>59723</td><td>8443</td><td>00:08:24</td><td>InLoopBack0</td><td>127.0.0.1</td></tr>
</table></td></tr>
<tr><td>Resultado Esperado</td><td colspan="4">1. Verificar o suporte as funcionalidades do item 2.1.45.12.</td></tr>
<tr><td>Resultado do Teste</td><td colspan="4">☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA</td></tr>
<tr><td>Observação</td><td colspan="4"></td></tr>
<tr><td>Assinatura</td><td>Cliente</td><td></td><td>Huawei</td><td></td></tr>
</table>

19.6 Item 2.1.63

Objetivo de teste	Suportar os protocolos de roteamento RIPv2, OSPFv2 ou OSPFv3 para as funcionalidades de VPN.
Especificação de teste	Suportar os protocolos de roteamento RIPv2, OSPFv2 ou OSPFv3 para as funcionalidades de VPN.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será adicionado as configurações conforme o Item 10 VPN desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.1.63.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

Assinatura	**Cliente**		**Huawei**	

19.7 Item 2.1.68

Objetivo de teste	Possuir gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência local do equipamento ou do cluster quanto com a gerência centralizada da solução.
Especificação de teste	Possuir gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência local do equipamento ou do cluster quanto com a gerência centralizada da solução.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será verificado no Item 10 VPN desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.1.68.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

19.8 Item 2.2.7

Objetivo de teste	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.
Especificação de teste	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.
Ambiente de teste	Test TOPO:

	 Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			
Procedimento de Teste	1. Será verificado no Item 10.2 Logs & Reports desde caderno de testes.			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.2.7.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.9 Item 2.2.8

Objetivo de teste	Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de sessões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectadas com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários que consumem mais banda de Internet, os sítios na Internet mais visitados.
Especificação de teste	Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de sessões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectadas com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários que consumem mais banda de Internet, os sítios na Internet mais visitados.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console.

	2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			
Procedimento de Teste	1. Será verificado no Item 10.2 Logs & Reports desde caderno de testes.			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.2.8.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.10 Item 2.3.3

Objetivo de teste	Decodificar múltiplos formatos de Unicode;
Especificação de teste	Decodificar múltiplos formatos de Unicode;
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Verificar localmente a funcionalidade.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.3.3.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

Assinatura	**Cliente**		**Huawei**	

19.11 Item 2.3.6

Objetivo de teste	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.
Especificação de teste	Detectar e Proteger contra, no mínimo, ataques.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será verificado no Item 8 Content Security desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.3.6.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

Assinatura	**Cliente**		**Huawei**	

19.12 Item 2.3.7

Objetivo de teste	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 Plugins/ Add-nos.
Especificação de teste	Possuir proteção contra os ataques.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será verificado no Item 8 Content Security desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.3.7.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

19.13 Item 2.3.12

Objetivo de teste	Permitir filtros de anomalias de protocolos, inclusive protocolos de aplicação (ex.: HTTP, SMTP, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, RPC, SSH e Telnet);
Especificação de teste	Permitir filtros de anomalias de protocolos.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console.

	2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			
Procedimento de Teste	1. Será verificado no Item 6 Security Control desde caderno de testes.			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.3.12.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.14 Item 2.3.13

Objetivo de teste	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.
Especificação de teste	Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será verificado no Item 8 Content Security desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.3.12.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA

Observação				
Assinatura	**Cliente**		**Huawei**	

19.15 tem 2.5.1

Objetivo de teste	Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;
Especificação de teste	Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipame Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Abaixo pode ser verificado as categorias e subcategorias: 2. Devido a grande quantidade de sites 100.000.000 segue o valor total:

```
<MPOG>disp url category
-------------------------------------------------------------------------------
  URL Pre-defined Category Count: 136
  URL Pre-defined Category List:
  Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID),
         SN(Subcategory Name)
-------------------------------------------------------------------------------
  CID   CN                        SID   SN
-------------------------------------------------------------------------------
  1     P2P
                                  101   P2P
  2     Download
                                  102   e-Books
                                  162   Software Download
                                  163   Picture Download
                                  164   Music/Film Download
                                  165   General Download
  3     Humanity
                                  103   History/Culture
                                  166   Literature
                                  167   Arts
                                  168   Music
  4     Sports
                                  104   Competitive Sports
                                  169   Leisure Sports
  ---- More ----
```

	[urlhadoop@y04 full_base]$ ls -l 20180105_132941.full_base -rw-rw-r--. 1 urlhadoop urlhadoop 8067996212 Jan 5 14:32 20180105_132941 [urlhadoop@y04 full_base]$ wc -l 20180105_132941.full_base 116658874 20180105_132941.full_base
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.5.1.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

Assinatura	**Cliente**		**Huawei**	

19.16 Item 2.5.9

Objetivo de teste	Deve ser capaz de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;
Especificação de teste	Deve ser capaz de exibir mensagem de bloqueio customizável.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será verificado no Item 8 Content Security desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.5.9.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	

Assinatura	**Cliente**		**Huawei**	

19.17 Item 2.5.10 e 2.5.10.1

Objetivo de teste	Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual. Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual			
Especificação de teste	Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual.			
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			
Procedimento de Teste	1. Será verificado no Item 8 Content Security desde caderno de testes.			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.5.10 e 2.5.10.1.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.18 Item 2.5.11

Objetivo de teste	Permitir o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certificado SSL.
Especificação de teste	Permitir o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certificado SSL.
Ambiente de teste	Test TOPO: Pré-condição:

	1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			
Procedimento de Teste	1. Será verificado no Item 8 Content Security desde caderno de testes.			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.5.11.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.19 Item 2.5.14

Objetivo de teste	Possuir categorização de sites governamentais nacionais, mesmo não tendo domínio “gov” ou “.gov.br.”
Especificação de teste	Possuir categorização de sites governamentais nacionais.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será verificado no Item 8 Content Security desde caderno de testes.
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.5.14.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA

Observação				
Assinatura	**Cliente**		**Huawei**	

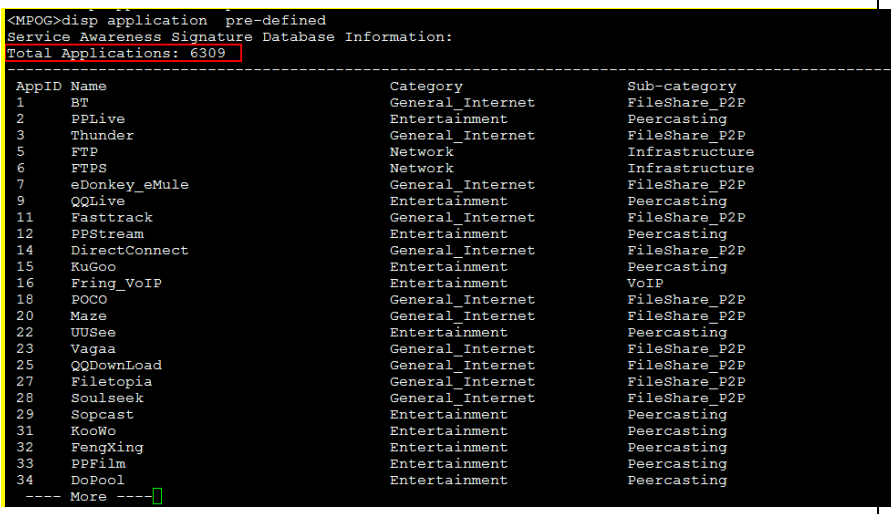
19.20 Item 2.5.15

Objetivo de teste	Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo consideradas neste percentual categorização genérica ou similar.
Especificação de teste	Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento).
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	2. Será verificado no Item 11 Performance desde caderno de testes.
Resultado Esperado	2. Verificar o suporte as funcionalidades do item 2.5.15.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | **Huawei**

19.21 Item 2.6.12

Objetivo de teste	Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email..
Especificação de teste	Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações.

Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).

Procedimento de Teste	1. Executar o comando abaixo:
	 
	`<MPOG>disp application pre-defined`
	`Service Awareness Signature Database Information:`
	`Total Applications: 6309`
	`AppID Name Category Sub-category`
	`1 BT General_Internet FileShare_P2P`
	`2 PPLive Entertainment Peercasting`
	`3 Thunder General_Internet FileShare_P2P`
	`5 FTP Network Infrastructure`
	`6 FTPS Network Infrastructure`
	`7 eDonkey_eMule General_Internet FileShare_P2P`
	`9 QQLive Entertainment Peercasting`
	`11 Fasttrack General_Internet FileShare_P2P`
	`12 PPStream Entertainment Peercasting`
	`14 DirectConnect General_Internet FileShare_P2P`
	`15 KuGoo Entertainment Peercasting`
	`16 Fring_VoIP Entertainment VoIP`
	`18 POCO General_Internet FileShare_P2P`
	`20 Maze General_Internet FileShare_P2P`
	`22 UUSee Entertainment Peercasting`
	`23 Vagaa General_Internet FileShare_P2P`
	`25 QQDownLoad General_Internet FileShare_P2P`
	`27 Filetopia General_Internet FileShare_P2P`
	`28 Soulseek General_Internet FileShare_P2P`
	`29 Sopcast Entertainment Peercasting`
	`31 KooWo Entertainment Peercasting`
	`32 FengXing Entertainment Peercasting`
	`33 PPFilm Entertainment Peercasting`
	`34 DoPool Entertainment Peercasting`
	`---- More ----`

Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.6.12.
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA
Observação	
Assinatura	**Cliente** | | **Huawei** |

19.22 Item 2.6.13

Objetivo de teste	Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Instagram, Twitter, LinkedIn, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR e Webex.

Especificação de teste	Identificação, bloqueio e restrição em profundidade e granularidade de aplicações.			
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			
Procedimento de Teste	1. Será verificado no Item 6 Security Control desde caderno de testes.			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 2.6.13.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.23 Item 3.22.1.4 e 3.22.1.4.1

Objetivo de teste	Possuir no mínimo 6 (seis) portas 10/100/1000 BASE-T, podendo 01 (uma) delas ser utilizada para gerência, 4 (quatro) portas 1GE SFP, com os respectivos transceivers 1000BASE-SX e padrão IEEE802.3z, e 2 (duas) portas 10GE SFP+ ou XFP, com os respectivos transceivers 10GBASE-SR e padrão IEEE802.3ae.
Especificação de teste	Verificar visualmente as especificações de Hardware.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente;

	4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).			
Procedimento de Teste	1. Verificar visualmente.			
Resultado Esperado	1. Verificar o suporte as funcionalidades do item 3.22.1.4 e 3.22.1.4.1.			
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA			
Observação				
Assinatura	**Cliente**		**Huawei**	

19.24 Item 3.24.1.2 e 3.24.1.3

Objetivo de teste	Possuir suporte para a integração com equipamentos ou serviços com a funcionalidade de APT (Advanced Persistent Threat) e Zero Day.
Especificação de teste	funcionalidade de APT (Advanced Persistent Threat) e Zero Day deve possuir capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, tais como: Windows XP e Windows 7, assim como documentos do Windows Office. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.
Ambiente de teste	Test TOPO: Pré-condição: 1. Equipamentos operacionais e com acesso pelo console. 2. Configurar o ambiente de testes de acordo com teste de TOPO e configurar todos os endereços IP de dispositivos; 3. Atribuir a interface para a zona de segurança correspondente; 4. Executar roteiro de configuração e os dispositivos deve possuir comunicação uns aos outros (ping).
Procedimento de Teste	1. Será verificado no Item Content Security desde caderno de testes.
Resultado Esperado	2. Verificar o suporte as funcionalidades do item 3.24.1.2 e 3.24.1.3
Resultado do Teste	☐ OK ☐ OK parcial ☐ Falhou ☐ Não testado ou NA

Observação				
Assinatura	**Cliente**		**Huawei**	

i. Conclusão do Teste

Localização do Teste		Dia / Hora:
Conclusão do Teste		
Observações Adicionais	（）Nenhuma. （）Sim. Segue:	
Assinatura	**Representante Cliente**	
	Representante Vert/ Huawei	