

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 1/126



**Procuradoria Geral do
Distrito Federal**

CADERNO DE TESTES

Solução de Segurança de Rede-Firewalls Appliances

**Homologação do Pregão Eletrônico Nº.04/2015
Processo No. 020.003.077/2013**

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 2/126

Sumário

1.	OBJETIVO DO CADERNO DE TESTE	3
2.	ESTRUTURA FÍSICA	3
3.	TABELA DE EQUIPAMENTOS	4
4.	CABEAMENTO ESTRUTURADO	7
5.	DEMAIS EQUIPAMENTOS.....	7
6.	PERFIL DE TRÁFEGO TESTE	8
7.	AMBIENTE DE TESTE.....	9
8.	RELATÓRIO FINAL.....	10

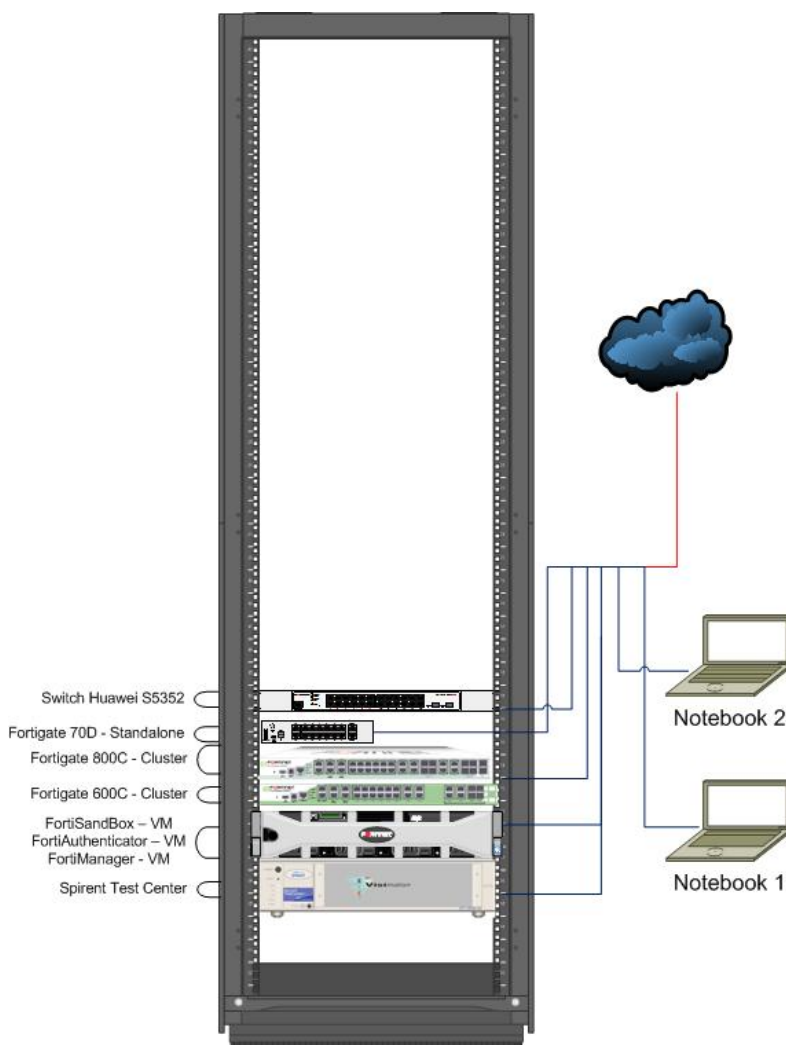
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 3/126

1. OBJETIVO DO CADERNO DE TESTE

Este caderno de testes refere-se ao item 10 do termo de referência do certame Nº 04/2015, que visa comprovar as funcionalidades e requisitos técnicos da solução de NGFW firewall appliances (equipamento, licenças e software) para conclusão de prova de conceito dos produtos ofertados da marca Fortinet. Serão demonstradas as funcionalidades específicas aos itens pontualmente indicados no subtópico 9.1.2 e demais que a PGDF considerar relevantes para homologação dos testes.

Os testes foram realizados nas instalações da NCT Informática, localizado no Centro Empresarial João Carlos Saad no SBS Quadra - 02, Lt - 03, Bl - Q, 8º andar Brasília/DF CEP 70070-120, a partir da data do dia 19/11/2015 horário comercial das 08:00 as 18:00 com intervalo das 12:00 as 14:00 até o seu final no dia 26/11/2015.

2. ESTRUTURA FÍSICA



	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 4/126

3. TABELA DE EQUIPAMENTOS

Equipamentos entregues, conforme edital.

Quantidade	Modelo Equipamento	Descrição
2	Fortigate 800C	NGFW + Web Filter
2	Fortigate 600C	NGFW
1	Fortigate 70D	NGFW
1	Huawei S5352	Switch para conectorização de ativos.
1	Fortimanager VM	Gerência Centralizada + Fortianalyzer
1	Fortiauthenticator VM	Fortiauthenticator
1	FortiSandBox VM	FortiSandBox



Fortigate 800C

Firewall Throughput 1518 Bytes	Firewall Throughput 512 Bytes	Firewall Throughput 64 Bytes	Firewall Max Concurrent Session	Firewall New Sessions per second	IPS Throughput	Firmware Instalado
20 Gbps	20 Gbps	20 Gbps	7 Million	190,000	6 Gbps	FortiOS 5.2.4 ou mais atual



Fortigate 600C

Firewall Throughput 1518 Bytes	Firewall Throughput 512 Bytes	Firewall Throughput 64 Bytes	Firewall Max Concurrent Session	Firewall New Sessions per second	IPS Throughput	Firmware Instalado
16 Gbps	16 Gbps	16 Gbps	3 Million	70,000	4 Gbps	FortiOS 5.2.4 ou mais atual

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 5/126



Fortigate 70D

Firewall Throughput 1518 Bytes	Firewall Throughput 512 Bytes	Firewall Throughput 64 Bytes	Firewall Max Concurrent Session	Firewall New Sessions per second	IPS Throughput	Firmware Instalado
3.5 Gbps	3.5 Gbps	3.5 Gbps	2 Million	4,000	275 Mbps	FortiOS 5.2.4 ou mais atual



Spirent Test Center

Feature	Ports per module	Connector type	Min/max frame size (w/CRC)	Min/max tx rates	Firmware Instalado
CV-10G-S8	8 x ports -10G (tráfego IMIX stateless)	10/100/1000 Base-T copper	58-16384	1 packet per 3.43 seconds to 101% of line rate	4.44
CPU-5003	2x 10G (tráfego statefull)	SFP+, 10GBASE-SR/SW	58-16384	58-16384	4.44

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 6/126



Switch Huawei 5352

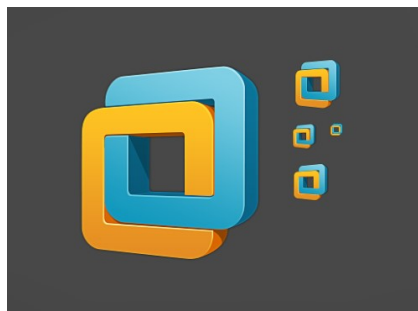
Interfaces	Performance	Firmware
Fourty-eight 10/100/1000Base-T ports and four 10GE Base-X SFP+ports	Forwarding performance:130.94Mpps	V200R003 ou mais atual



Servidor para teste do ambiente de Virtualização

PowerEdge M620
2x Intel Xeon E5-2650 2.00GHz, 20 M Cache, 8.0GT/s QPI, Turbo, 8 C, 95W
256GB RDIMM, 1333 MT/s, Low Vol t, Dual Rank, x4 Data Width
Serial-Attach SCSI Backplane f or M620
2x 300GB 10K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive
1x Controller H310 SCSI Hardware RAID 1
1x Intel x520-k Dual Port 10Gb KR Blade Network Daughter Card
1x Intel 10GbE -x/k, Dual Port I/ O Card for M-Series Blades
12G iDRAC7 Enterprise for Blades
VMware® vSphere® ESXi™ 5.5

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 7/126



Ambiente Virtualizado

FortiManager-VM				
Devices/ADOMs/VDOMs Supported (Max)	Max Number of Web Portals	Total Network Interfaces	Total Storage Capacity	Firmware Instalado
Up to 10,000	Up to 10,000	1 to 4 network card supported	80 GB (minimum)	FortiOS 5.2.4 ou mais atual
FortiAuthenticator-VM				
Recommended Max Number of End-users	Firmware Instalado			
Up to 1M	4.0.1 ou mais atual			
FortiSandBox - VM				
Virtual CPUs (Minimum / Maximum)	Memory Support (Minimum / Maximum)	Virtual Storage (Minimum / Maximum)	Number of VMs	Firmware Instalado
4 / Unlimited	8 GB / Unlimited	30 GB / 16 TB	4 to 54 (Upgrade via appropriate licenses)	2.1.0 ou mais atual

4. CABEAMENTO ESTRUTURADO

A infraestrutura montada para os testes deste caderno em determinadas situações podem ser alteradas, inclusive para uma melhor demonstração ou sanar dúvidas, os laboratórios serão interligados com:

- Cabos UTP cat. 6
- Transceivers FG-TRAN-SX - SFP 1.25 Gbps
- Cordões fibras ópticas OM3

5. DEMAIS EQUIPAMENTOS

Demais equipamentos que compõem o ambiente de testes:

- Notebooks – com o sistema operacional Microsoft Windows Professional - responsáveis por salvar todas as evidências dos testes.
- Power Distribution Unit para energização dos equipamentos.

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 8/126

6. PERFIL DE TRÁFEGO TESTE

Os padrões de testes adotados os quais visam à validação de desempenho dos equipamentos dos equipamentos ofertados para o pregão eletrônico 04/2015 estarão com todas as funcionalidades habilitadas requisitadas no certame conforme cada tipo, respectivamente *Tipo 1, Tipo 2 e Tipo 3*, isto é, o tráfego gerado será distribuído e ajustado de forma a alcançar as regras.

Será utilizando o método de teste de avaliação de acordo com a RFC-3511, metodologia padrão e reconhecida pelo mercado com modificações para refletir o ambiente no qual o dispositivo irá realmente ser avaliado.

O tráfego de teste utilizado na avaliação deverá possuir a seguinte distribuição aproximada de protocolos:

- a) HTTP = 35% (conteúdo variável com imagens, textos, tipo e tamanho de 100bytes a 500kbytes)
- b) HTTPS = 5% (conteúdo variável com imagens, textos, tipo e tamanho de 100bytes a 500kbytes)
- c) RTP UDP = 30% (distribuição de tamanho: 56% 64bytes, 17% 512bytes e 23% 1518bytes)
- d) FTP = 5% (imagens, textos, tipo e tamanho de 100bytes a 1Mbytes)
- e) VPN = 5% (IPSec, conteúdo variável com imagens e textos)
- f) DNS = 5% (queries de tamanho variável: 10bytes a 1kbytes)
- g) Email = 2% (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos)
- h) Multicast = 3% (streaming com tráfego de pacotes UDP 64bytes)
- i) Ataques = 5% (Ataques stateful/stateless, variados, no mínimo 100 tipos diferentes, encapsulados nos protocolos http, https, ftp, ftps, sftp, cifs, nfs, POP3, SMTP e IMAP sendo que 10% destes ataques devem utilizar algum método de ofuscação)
- j) Aplicações = 5% (uTorrent, Skype, Exchange, SQL, RDP)

Poderá haver uma variação de na distribuição de cada protocolo indicado acima e incrementar a taxa de tráfego UDP/RTP.

Todo o volume de tráfego mencionado tem por objetivo obter os resultados de cada equipamento NGFW firewall appliance através dos testes gerados pelos equipamentos Spirent baseados em suas respectivas na folha de dados, para cada um dos tipos de equipamentos ofertados.

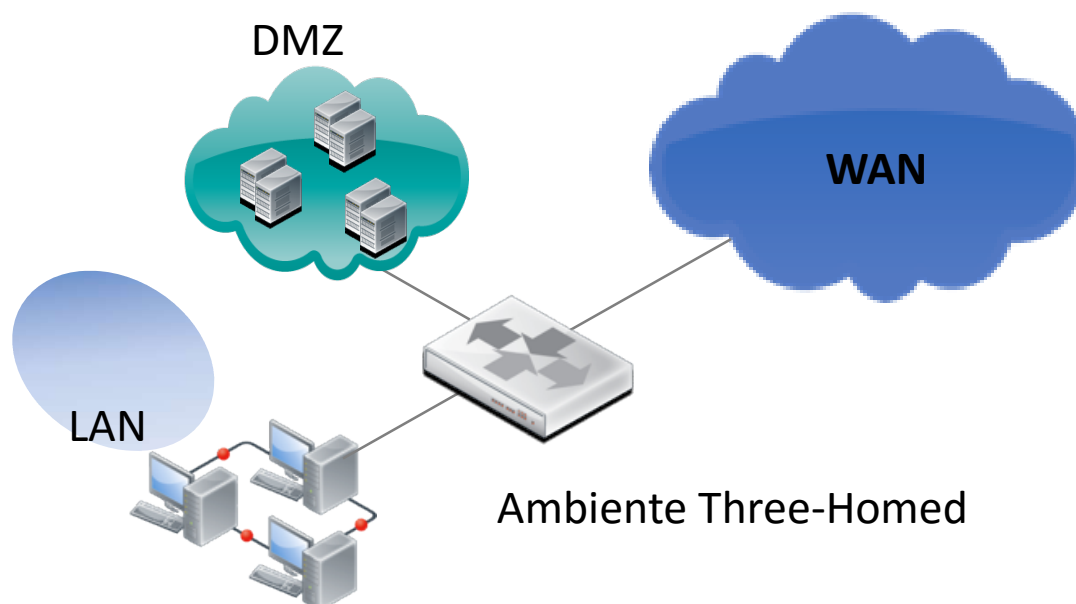
Parâmetro	Definição
CPS	Connections per Second - Este parâmetro indica quantas novas conexões/sessões TCP por Segundo o sistema sob teste está consegue tratar. Neste teste as conexões/sessões TCP estabelecem com o "triple handshake" e são encerradas imediatamente com "Reset"
CC	Concurrent Connections – Este parâmetro indica quantas conexões/sessões TCP simultâneas o sistema consegue sustentar. No teste de Concurrent Connections a conexão TCP é estabelecida com o "triple handshake", mas não é encerrada por um período programável, ao final do teste todas as conexões estabelecidas devem ser encerradas.

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 9/126

Throughput	É a quantidade de bits por Segundo recebidos, que passaram pelo sistema sob teste.
Túneis VPN	Quantidade de túneis VPN IPSec estabelecidos com tráfego

7. AMBIENTE DE TESTE

Para execução dos testes será utilizado uma estrutura de ambiente em formato "Three-Homed", composta por uma LAN (local Area Network), WAN (Wide Area Network) e DMZ (Demilitarized Zone), aplicando esta para todos os modelos de equipamento.



Serão criados objetos de demonstração de teste tais como: Regras de Firewall, endereços de nós de rede, NAT/PAT, IPS/IDS, controle de aplicação, antivírus/anti-spyware, DLP, VPN Ipsec, Filtro URL e QoS, e geração de Logs dos registros de eventos.

Adoção de nomenclatura e a quantidades de objetos seguiram um padrão de script base em todos os testes da seguinte maneira:

Objeto	Descrição	Quantidade
Address/IP Range	Servidor_X	1-128
VIP	VIP_IP	1-100
IPS	Default	1 (4000 Assinaturas)
Regras de firewall	N/A	1-128

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 10/126

8. RELATÓRIO FINAL

Ao final da execução do caderno de teste da prova de conceito, conforme item 10 do anexo I - Termo de Referência, apresentamos o relatório final com todas as evidências:

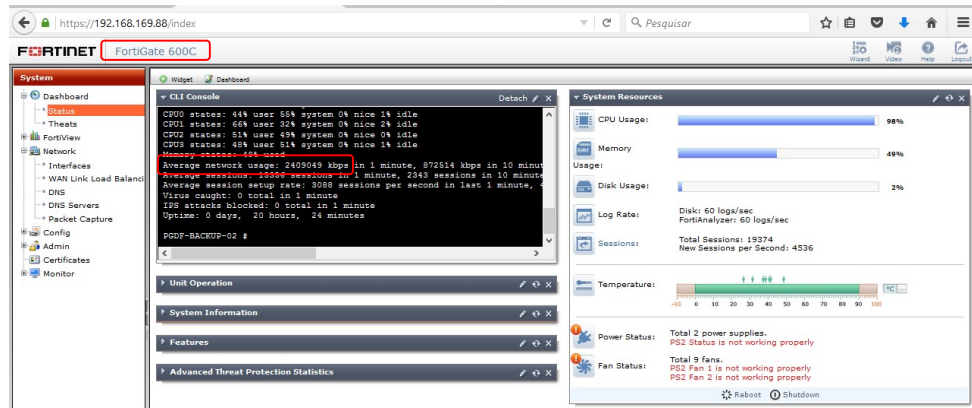
8.1. QUANTO AO DESEMPENHO

Todos os equipamentos NGFW Firewall appliance dos Tipo 1,2 e 3 submetidos nesta prova de conceito foram testados com todas as funcionalidades ativas, tais como: IPS, Antivírus e Anti-spyware ativados em caráter simultâneo, para ser aferida a capacidade de throughput.

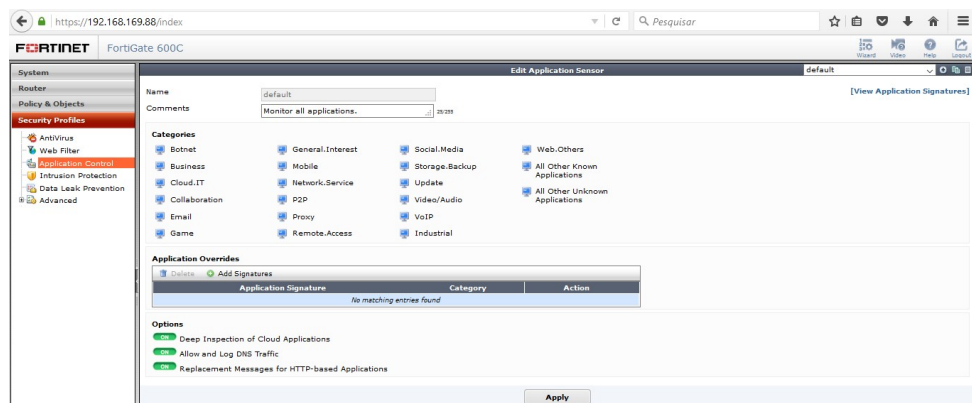
Item 1.6 - CARACTERÍSTICAS ESPECÍFICAS PARA OS 4 (QUATROS) APPLIANCES QUE COMPORÃO O CLUSTER DO SITE PRINCIPAL E DO SITE BACKUP:

Site Backup

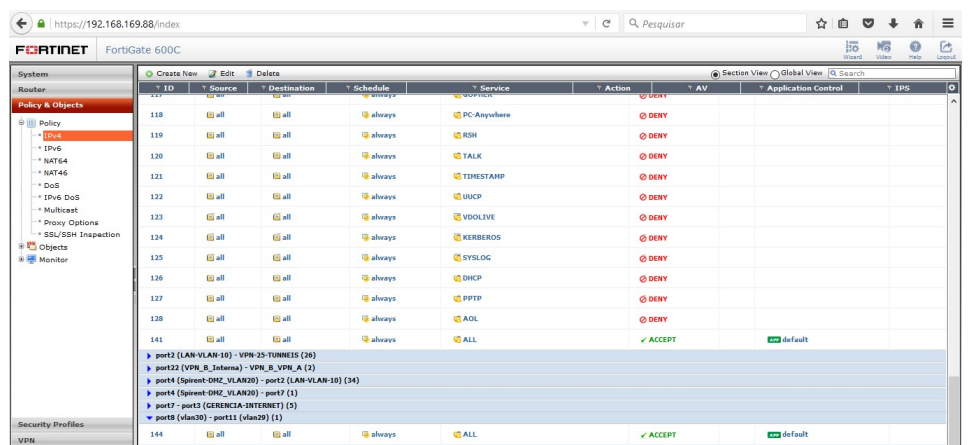
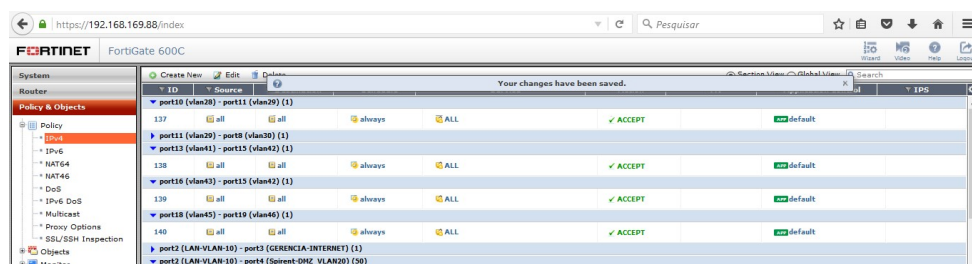
Item de Teste - 1.6.1.1	Os equipamentos que comporão o cluster do Site Backup (Firewall Appliance Tipo 2) deverão possuir um throughput mínimo de 2 (dois) Gbps para as funcionalidades de firewall com controle de aplicação habilitado e throughput mínimo de 1 (um) Gbps para controle de aplicativos, IPS, antivírus e anti-spyware habilitados e atuantes simultaneamente para todas as assinaturas que o fabricante possuir;
Objetivo do Teste	Aferir os índices de throughput com as features solicitadas
Configuração do Teste	Foram configurados sensores de IPS, APP control e Antivírus com as configurações de base e assinaturas default: -Sensor de IPS : todas as assinaturas disponíveis no dia do teste. -Sensor de AV : habilitado a monitoração de todos os protocolos. -Sensor de APP control: habilitado com todas as categorias de aplicações disponíveis no dia do teste. Os sensores foram habilitados em todas as regras onde o tráfego foi gerado. O gerador de tráfego (spirent) foi configurado com os parâmetros de tráfego já descritos nesse caderno de testes.
Procedimento do Teste	O tráfego é gerado a partir do Spirent, e pode ser observado que os números solicitados neste edital foram alcançados no equipamento FGT 600C
Evidências	- Teste com APPControl habilitado.



Equipamento alcançando throughput solicitado.

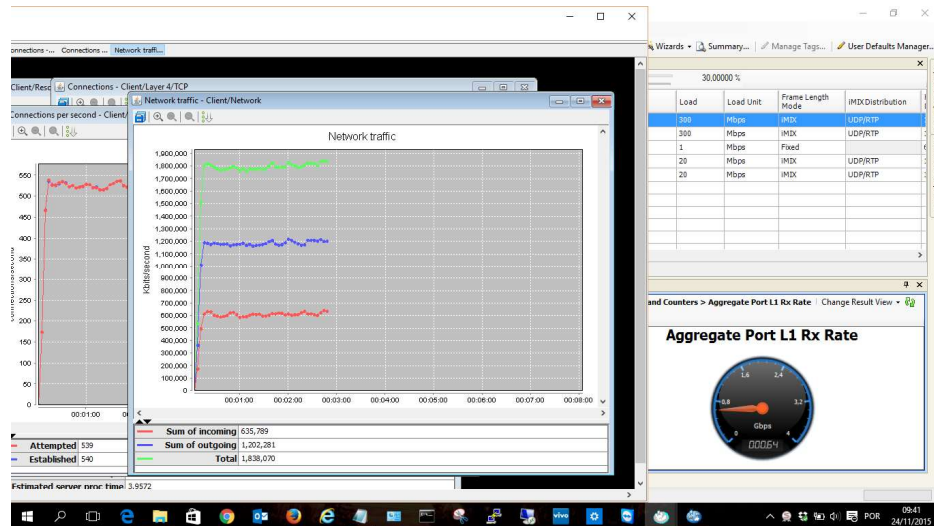


Sensor de APPControl configurado

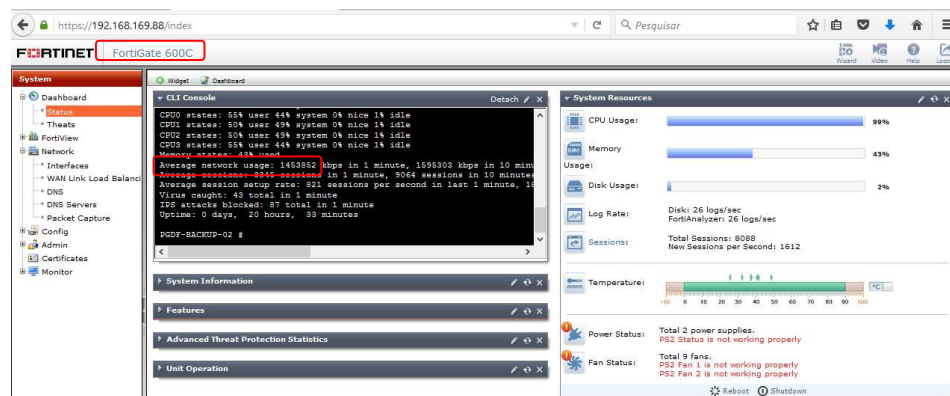


Regras de firewall.

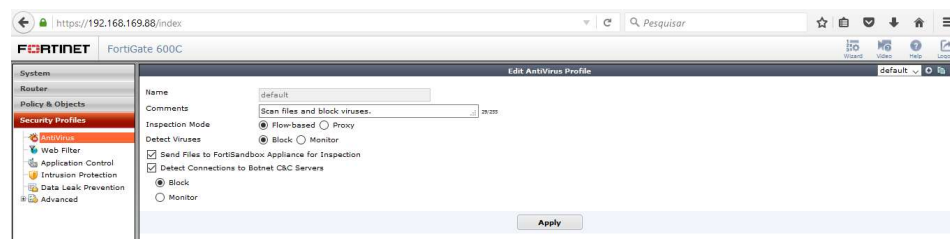
- Spirent



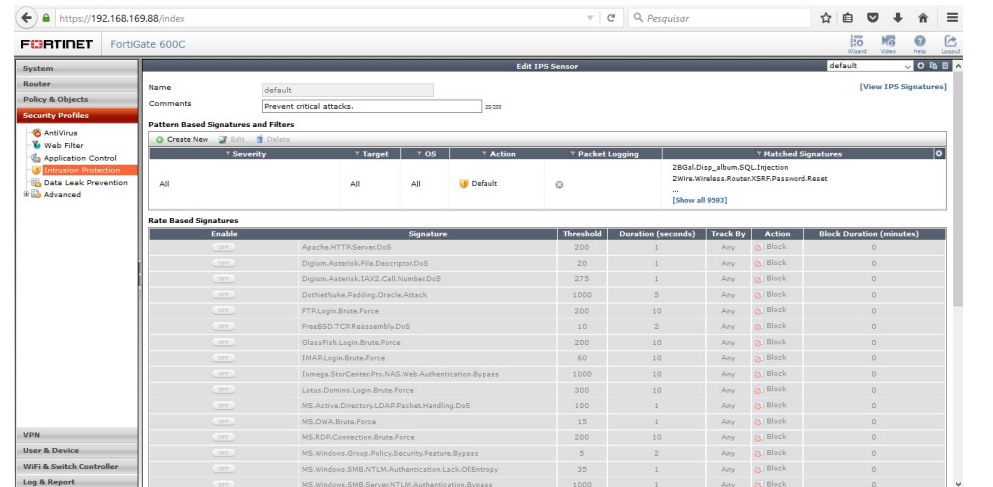
- Teste com APPContrl + AV + IPS



Equipamento alcançando throughput solicitado.



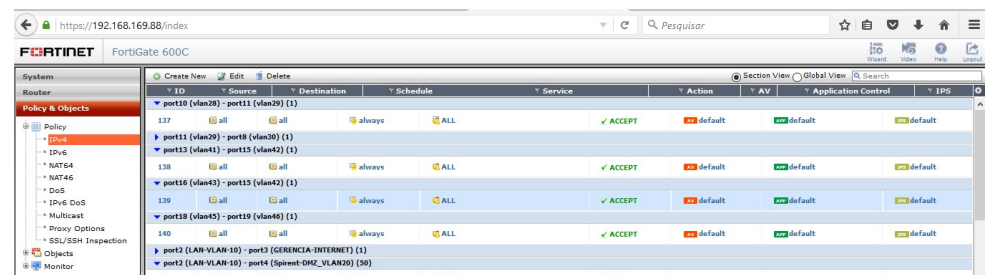
Sensor de AV



The screenshot shows the FortiGate 600C web interface for configuring an IPS Sensor. The left sidebar shows the navigation menu with 'Security Profiles' selected. The main area is titled 'Edit IPS Sensor' and shows a table of 'Pattern Based Signatures and Filters'. Below this, there is a table of 'Rate Based Signatures'.

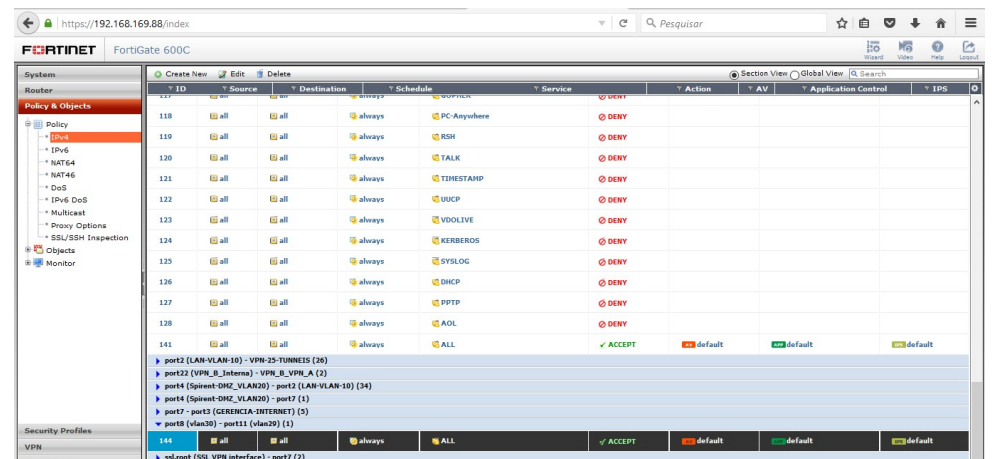
Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
☐	Apache HTTP Server DoS	200	1	Any	☐ Block	0
☐	Digum Asterisk File Description DoS	25	1	Any	☐ Block	0
☐	Digum Asterisk IAX2 Call Number DoS	275	1	Any	☐ Block	0
☐	DosWithNoPacking Oracle Attack	1000	5	Any	☐ Block	0
☐	FTP Login Brute Force	200	10	Any	☐ Block	0
☐	FreeBSD TCP Reassembly DoS	10	2	Any	☐ Block	0
☐	GlassFish Login Brute Force	200	10	Any	☐ Block	0
☐	IMAP Login Brute Force	60	10	Any	☐ Block	0
☐	Isomaps StorCenter Pro NAS Web Authentication Bypass	1000	10	Any	☐ Block	0
☐	Lotus Domino Login Brute Force	300	10	Any	☐ Block	0
☐	MS Active Directory LDAP Packet Handling DoS	100	1	Any	☐ Block	0
☐	MS DWA Brute Force	15	1	Any	☐ Block	0
☐	MS RDR Connection Brute Force	200	10	Any	☐ Block	0
☐	MS Windows Group Policy Security Feature Bypass	5	2	Any	☐ Block	0
☐	MS Windows SMB NTLM Authentication Lack Of Entropy	35	1	Any	☐ Block	0
☐	MS Windows SMB Server NTLM Authentication Bypass	1000	1	Any	☐ Block	0

Sensor de IPS



The screenshot shows the FortiGate 600C web interface for configuring Policy Objects. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main area is titled 'Create New' and shows a table of policy objects.

ID	Source	Destination	Schedule	Service	Action	AV	Application Control	IPS
137	port10 (vlan29) - port11 (vlan29) (1)	all	always	ALL	ACCEPT	default	default	default
138	port11 (vlan29) - port8 (vlan30) (1)	all	always	ALL	ACCEPT	default	default	default
139	port12 (vlan41) - port15 (vlan42) (1)	all	always	ALL	ACCEPT	default	default	default
140	port16 (vlan43) - port15 (vlan42) (1)	all	always	ALL	ACCEPT	default	default	default
141	port18 (vlan45) - port19 (vlan46) (1)	all	always	ALL	ACCEPT	default	default	default
142	port2 (LAN-VLAN-10) - port3 (CERENCIA-INTERNET) (1)	all	always	ALL	ACCEPT	default	default	default
143	port2 (LAN-VLAN-10) - port4 (Spirent-DMZ_VLAN20) (50)	all	always	ALL	ACCEPT	default	default	default



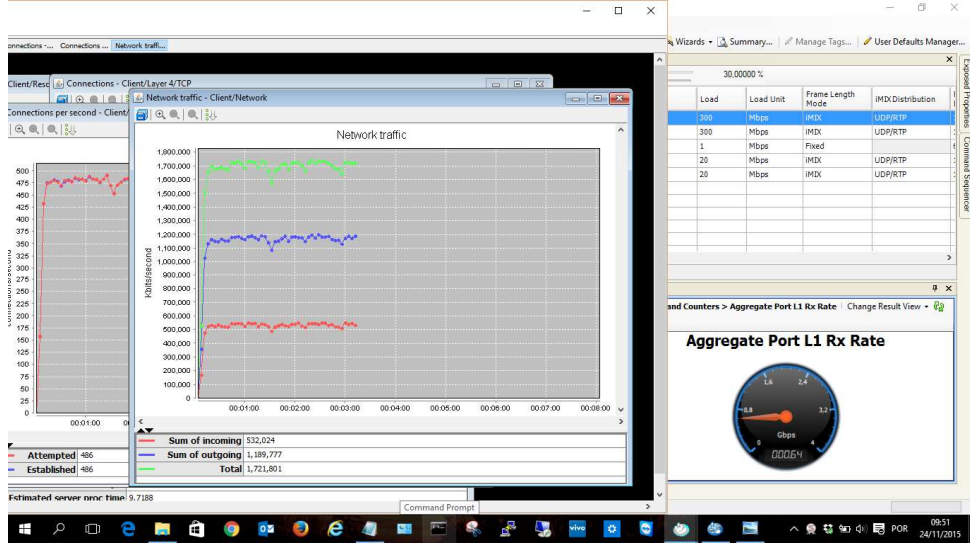
The screenshot shows the FortiGate 600C web interface for configuring Policy Rules. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main area is titled 'Create New' and shows a table of policy rules.

ID	Source	Destination	Schedule	Service	Action	AV	Application Control	IPS
118	all	all	always	PC-Anywhere	DENY			
119	all	all	always	RSH	DENY			
120	all	all	always	TALK	DENY			
121	all	all	always	TIMESTAMP	DENY			
122	all	all	always	UUCP	DENY			
123	all	all	always	VDOFILE	DENY			
124	all	all	always	KERBEROS	DENY			
125	all	all	always	SYSLLOG	DENY			
126	all	all	always	DHCP	DENY			
127	all	all	always	PPTP	DENY			
128	all	all	always	AOL	DENY			
141	all	all	always	ALL	ACCEPT	default	default	default
144	port2 (LAN-VLAN-10) - VPN-25-TUNNELS (26)	all	always	ALL	ACCEPT	default	default	default
145	port22 (VPN_B_Interna) - VPN_B_VPN_A (2)	all	always	ALL	ACCEPT	default	default	default
146	port4 (Spirent-DMZ_VLAN20) - port2 (LAN-VLAN-10) (34)	all	always	ALL	ACCEPT	default	default	default
147	port4 (Spirent-DMZ_VLAN20) - port7 (1)	all	always	ALL	ACCEPT	default	default	default
148	port7 - port3 (CERENCIA-INTERNET) (5)	all	always	ALL	ACCEPT	default	default	default
149	port8 (vlan30) - port11 (vlan29) (1)	all	always	ALL	ACCEPT	default	default	default
150	sslroot (SSL VPN interface) - port7 (2)	all	always	ALL	ACCEPT	default	default	default

Regras de firewall

- Spirent

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 14/126

		
Comentário	Todas as configurações tanto do FGT 600C como do Spirent foram apresentadas/explicadas a todos os presentes na sala de homologação. Maiores detalhes sobre o relatório de tráfego gerado pelo spirent, podem ser encontrados no CD anexo a este caderno.	
Assinatura do Cliente	Assinatura NCT	

Site principal

Item de Teste - 1.6.1.2	Os equipamentos que comporão o cluster do Site Principal (Firewall Appliance Tipo 1) deverão possuir um throughput mínimo de 4 (quatro) Gbps para as funcionalidades de firewall com controle de aplicação habilitado e throughput mínimo de 2 (dois) Gbps para controle de aplicativos, IPS, antivírus e anti-spyware habilitados e atuantes simultaneamente para todas as assinaturas que o fabricante possuir;
Objetivo do Teste	Aferir os índices de throughput das features solicitadas
Configuração do Teste	Foram configurados sensores de IPS, APP control e Antivírus com as configurações de base e assinaturas default: -Sensor de IPS : todas as assinaturas disponíveis no dia do teste. -Sensor de AV : habilitado a monitoração de todos os protocolos. -Sensor de APP control : habilitado com todas as categorias de aplicações disponíveis no dia do teste. Os sensores foram habilitados em todas as regras onde o tráfego foi gerado. O spirent foi configurado com os parâmetros de tráfego já descritos nesse caderno de testes.
Procedimento	O tráfego é gerado a partir de Spirent e pode ser observado que os números

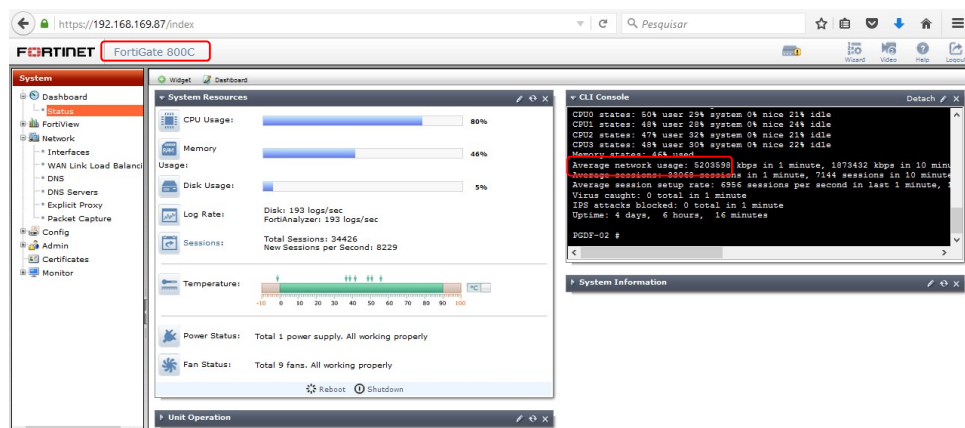
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 15/126

do Teste

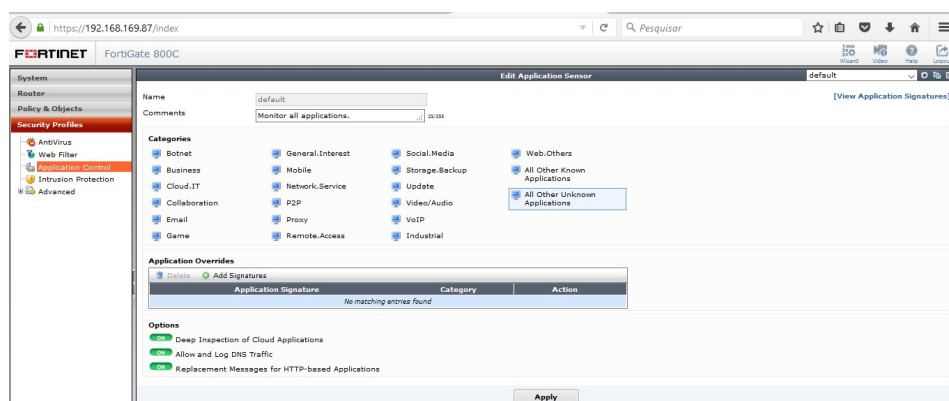
solicitados neste edital foram alcançados no equipamento FGT 800C

Evidências

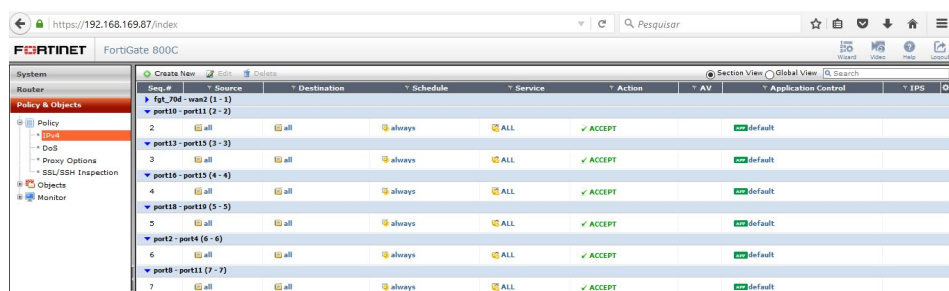
- 800C com APPControl



Equipamento alcançando throughput solicitado.



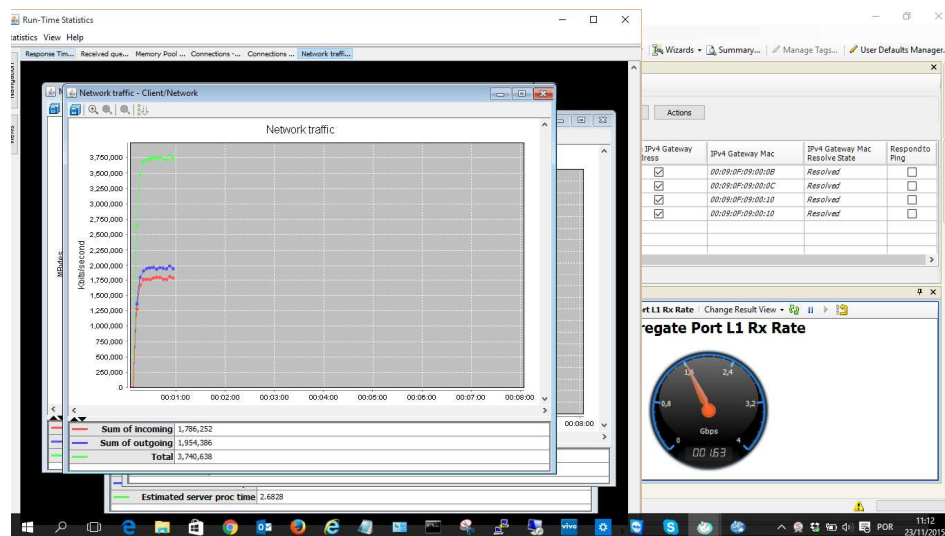
Sensor de AppControl



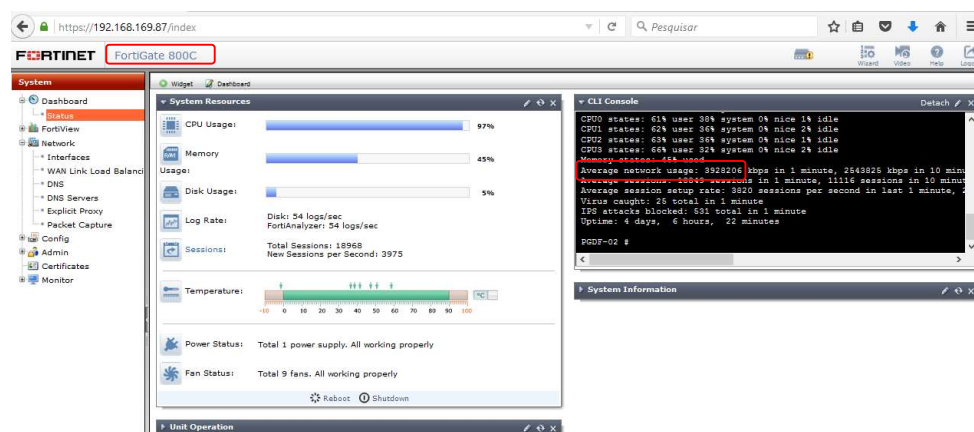
Policy	Source	Destination	Schedule	Service	Action	AV	Application Control	IPS
1	fgt794 - vwan2 (1-13)	port10 - port11 (2-2)	always	ALL	ACCEPT	default		
2	all	all	always	ALL	ACCEPT	default		
3	port13 - port15 (3-3)	all	always	ALL	ACCEPT	default		
4	port16 - port15 (4-4)	all	always	ALL	ACCEPT	default		
5	port18 - port19 (5-5)	all	always	ALL	ACCEPT	default		
6	port12 - port14 (6-6)	all	always	ALL	ACCEPT	default		
7	port8 - port11 (7-7)	all	always	ALL	ACCEPT	default		

Regras de firewall

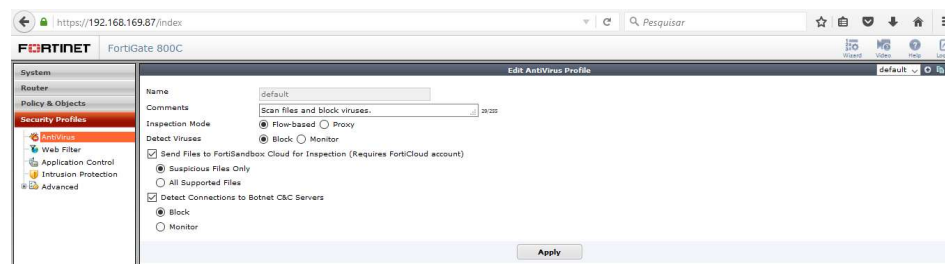
- Spirent



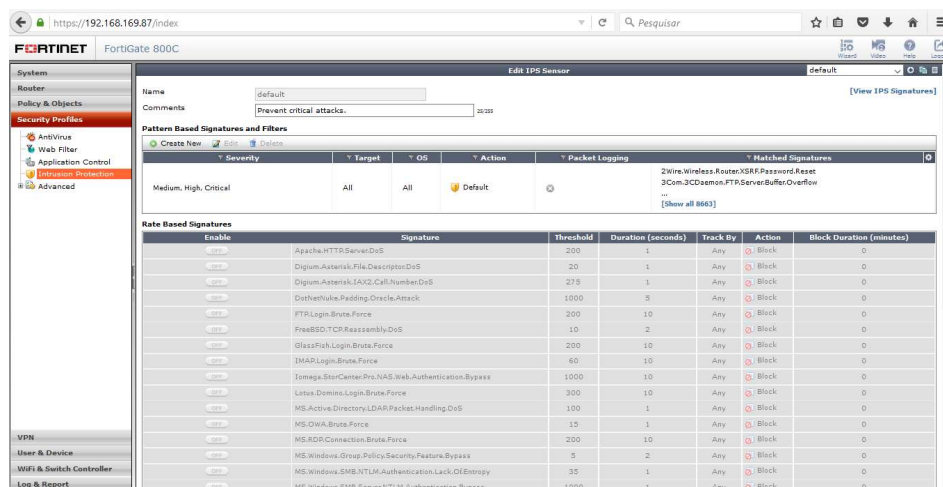
- 800C com AppControl + AV + IPS



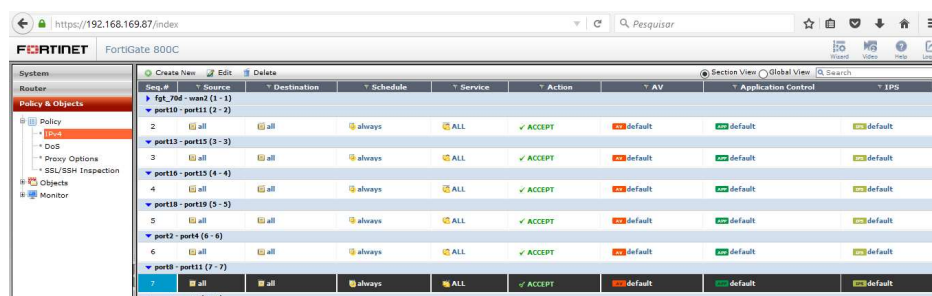
Equipamento alcançando throughput solicitado.



Sensor de AV

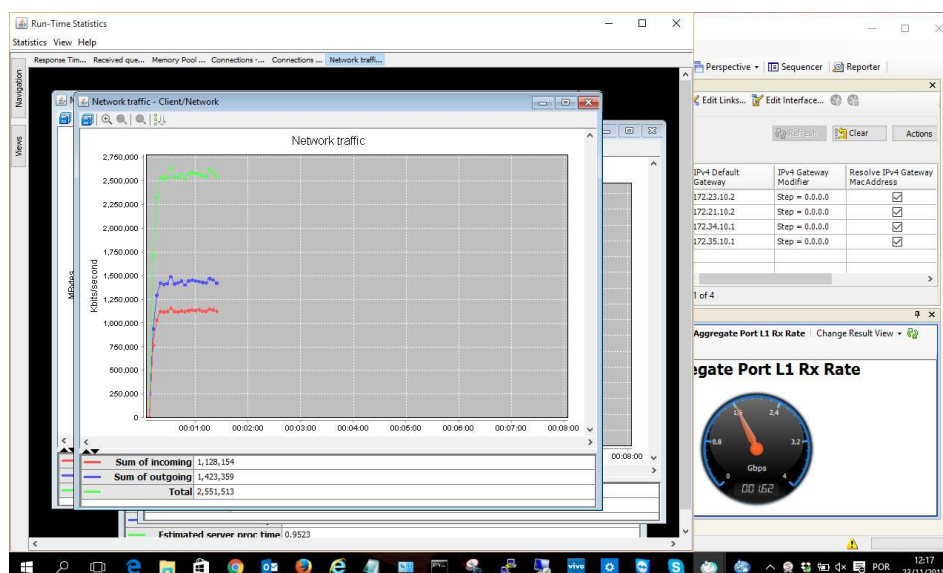


Sensor de IPS



Regras de firewall

- Spirent

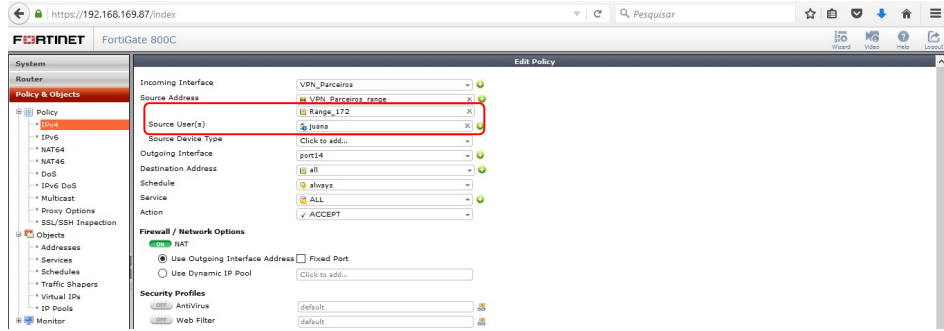
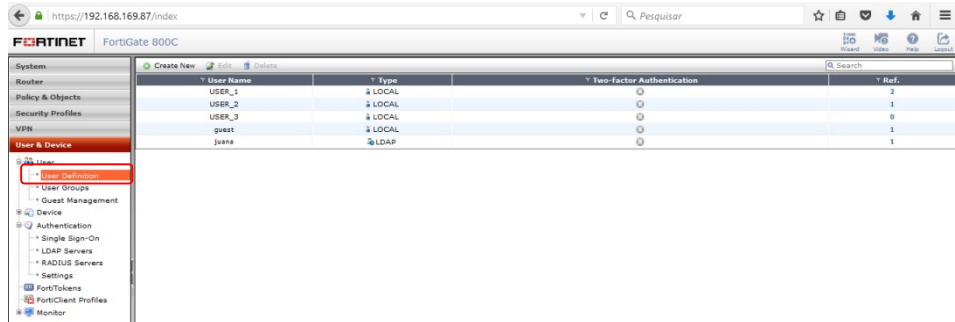


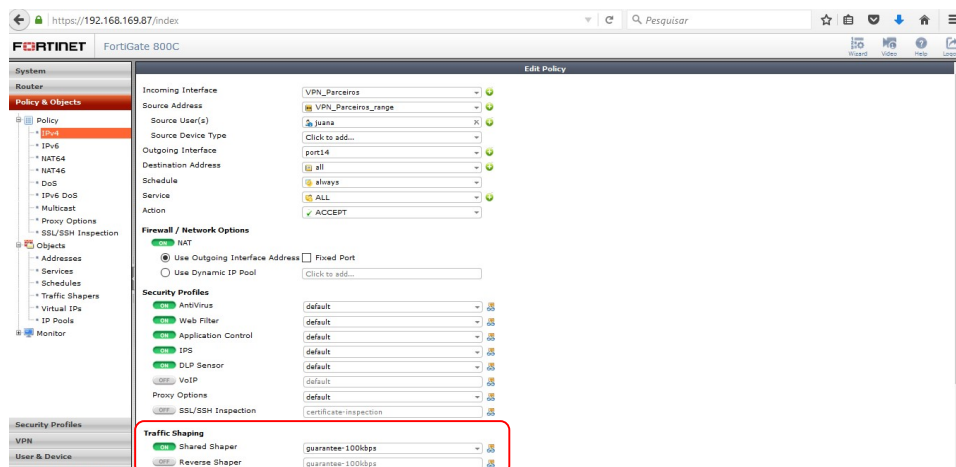
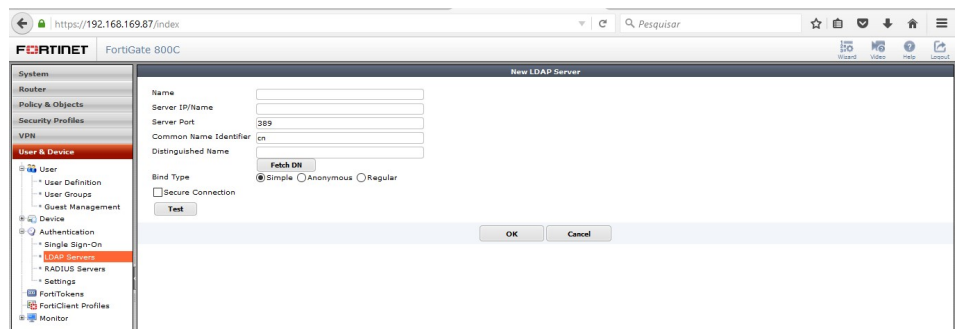
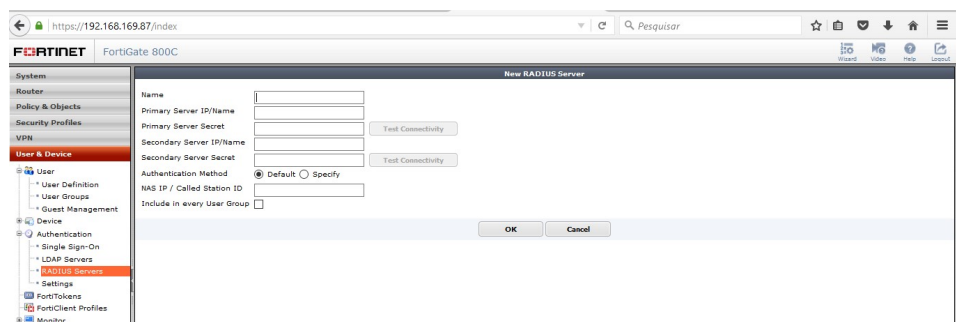
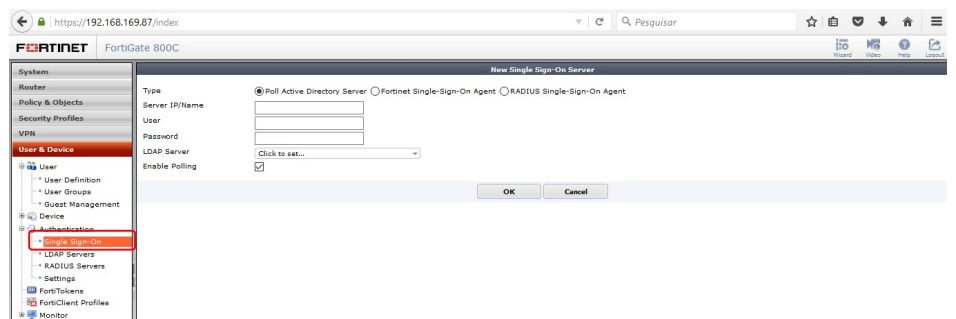
Comentário

Todas as configurações tanto do FGT 800C como do Spirent foram apresentadas/explicadas a todos os presentes na sala de homologação. Maiores detalhes sobre o relatório de tráfego gerado pelo spirent, podem ser

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 18/126

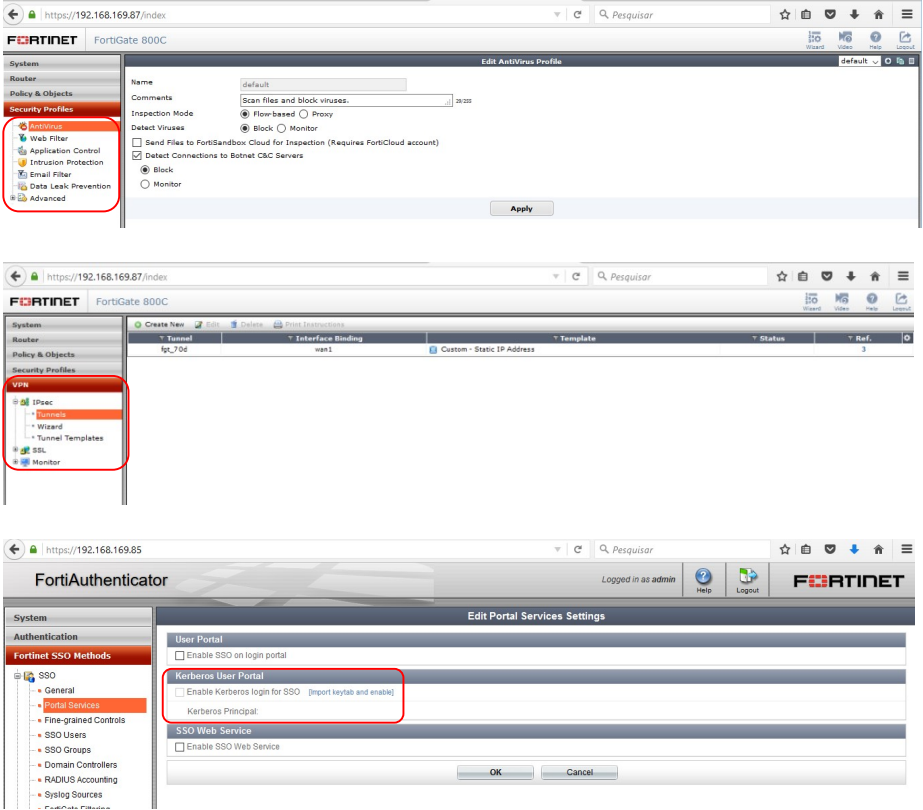
	encontrados no CD anexo a este caderno.	
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.1.21	Identificar e controlar o acesso dos usuários às aplicações utilizando: endereço IP, LDAP, Microsoft Active Directory, RADIUS, Kerberos, eDirectory. Os esquemas de autenticação deverão ser suportados pelos módulos de firewall (incluindo o controle de aplicações, DLP, filtros de conteúdo, IPS, antivírus, anti-spyware, QoS, roteamento baseado em políticas PBF ou PBR) e VPN. Deverá também possuir uma base de dados local para permitir a autenticação de usuários sem a necessidade de um dispositivo externo;
Objetivo do Teste	Demonstrar funcionalidades solicitadas
Configuração do Teste	Configurado os tipos de controle de autenticação às aplicações utilizando os métodos solicitados , e configurar em regra de firewall.
Procedimento do Teste	Validar autenticação do usuário à aplicação
Evidências	 Regra de firewall com aplicação  Base local de usuários

O acesso a microsoft active directory e eDirectory é realizado com a configuração de "single sign-on"

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 20/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.1.22	As funcionalidades de SSL decryption, VPN IPsec e SSL, controle de aplicações, QoS e roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante em vigência.
Objetivo do Teste	Conforme proposta comercial
Configuração do Teste	Demonstrar as funcionalidades solicitadas presentes nos equipamentos
Procedimento do Teste	Os Fortigates não necessitam de licenças para que os módulos de " SSL decryption, VPN IPsec e SSL, controle de aplicações, QoS e roteamento dinâmico "
Evidências	



https://192.168.169.83/index

FortiGate 600C

System

- Dashboard
- Status
- Threat
- FortView
- Network
- Config
- HA
- SNMP
- Replacement Message
- FortiGuard
- FortiSandBox
- Advanced
- Features
- Admin
- Administrators
- Admin Profiles
- Settings
- Certificates
- Monitor

Router

Policy & Objects

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

FortiGuard Distribution Network

Next Generation Firewall	Licensed (Expires 2017-03-28)	6.00738 (Updated 2015-11-26 via Scheduled Update) [Update]	2015-11-26
IPS Definitions	3.00079 (Updated 2015-07-02 via Manual Update)		
ATP Services	Licensed (Expires 2017-03-28)	30.00754 (Updated 2015-11-26 via Scheduled Update) [Update]	2015-11-26
Antivirus	5.00174 (Updated 2015-09-08 via Manual Update)		
AV Engine	Licensed (Expires 2017-03-28)		
Web Filtering			
Other Services	Licensed (Expires 2017-03-28)	1.00384 (Updated 2015-10-03 via Manual Update) [Update]	
Vulnerability Scan	Licensed (Expires 2017-03-28)		
VCM Plugins	Registered (Expires 2015-12-18)		
Email Filtering	4 Allowed (0 Used)		
Messaging Services			
SMS Messages			
FortiClient Information			
FortiGuard Availability	Reachable		
FortiClient Version (Mac)	5.4.0 (Updated 2015-11-26)		
FortiClient Version (Windows)	5.4.0 (Updated 2015-11-26)		
SSL-VPN Package Information			
SSL-VPN Package Version	4.0.2300 (Updated 2014-12-23) [Update]		
FortiToken Seed Server			
Registration	Reachable (0 Tokens Registered)		
AV & IPS Download Options			
Web Filtering and Email Filtering Options			

Apply

https://192.168.169.82/index

FortiGate 70D

System

- Dashboard
- Status
- FortView
- Network
- Config
- HA
- SNMP
- Replacement Message
- FortiGuard
- FortiSandBox
- Advanced
- Features
- Admin
- Administrators
- Admin Profiles
- Settings
- Certificates
- Monitor

Router

Policy & Objects

Security Profiles

VPN

User & Device

WiFi Controller

www.fortinet.com

FortiGuard Distribution Network

Registration	Registered (Login ID: gpimonta@nct.com.br) [Login Now]		
Firmware	8 x 3 support (Expires: 2016-11-11)		
Enhanced Support	8 x 3 support (Expires: 2016-11-11)		
8 x 5 support (Expires: 2016-11-11)			
FortiGuard Services			
Next Generation Firewall	Licensed (Expires 2016-11-11)	6.00738 (Updated 2015-11-26 via Scheduled Update) [Update]	2015-11-26
IPS & Application Control	3.00079 (Updated 2015-07-02 via Manual Update)		
IPS Definitions			
IPS Engine			
ATP Services	Licensed (Expires 2016-11-11)	30.00755 (Updated 2015-11-26 via Scheduled Update) [Update]	2015-11-26
Antivirus	5.00174 (Updated 2015-09-08 via Manual Update)		
AV Definitions	Licensed (Expires 2016-11-11)		
AV Engine			
Web Filtering			
Other Services	Licensed (Expires 2016-11-11)	1.00384 (Updated 2015-11-19 via Manual Update) [Update]	
Vulnerability Scan	Licensed (Expires 2016-11-11)		
VCM Plugins	Registered (Expires 2016-11-18)		
Email Filtering	4 Allowed (0 Used)		
Messaging Services			
SMS Messages			
FortiClient Information			
FortiGuard Availability	Reachable		
FortiClient Version (Mac)	5.4.0 (Updated 2015-11-26)		
FortiClient Version (Windows)	5.4.0 (Updated 2015-11-26)		
SSL-VPN Package Information			
SSL-VPN Package Version	4.0.2300 (Updated 2015-11-26) [Update]		
FortiToken Seed Server			
Registration	Reachable (0 Tokens Registered)		
AV & IPS Download Options			
Web Filtering and Email Filtering Options			

https://192.169.87/index

FortiGate 800C

System

- Dashboard
- FortView
- Network
- Config
- HA
- SNMP
- Replacement Message
- FortiGuard
- FortiSandBox
- Advanced
- Features
- Admin
- Certificates
- Monitor

Router

Policy & Objects

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

FortiGuard Distribution Network

Support Contract	Registered (Login ID: gpimonta@nct.com.br) [Login Now]		
Registration			
FortiGuard Services			
Next Generation Firewall	Licensed (Expires 2015-12-19)	6.00738 (Updated 2015-11-26 via Scheduled Update) [Update]	2015-11-26
IPS & Application Control	3.00079 (Updated 2015-07-02 via Manual Update)		
IPS Definitions			
IPS Engine			
ATP Services	Licensed (Expires 2015-12-19)	30.00754 (Updated 2015-11-26 via Scheduled Update) [Update]	2015-11-26
Antivirus	5.00174 (Updated 2015-09-08 via Manual Update)		
AV Definitions	Licensed (Expires 2015-12-19)		
AV Engine			
Web Filtering			
Other Services	Not Registered Subscribe	1.00297-L (Updated 2015-11-10 via Manual Update) [Update]	
Vulnerability Scan	Licensed (Expires 2015-12-19)		
VCM Plugins	Unreachable		
Email Filtering			
Messaging Services			
FortiClient Information			
FortiGuard Availability	Reachable		
FortiClient Version (Mac)	5.4.0 (Updated 2015-11-26)		
FortiClient Version (Windows)	5.4.0 (Updated 2015-11-26)		
SSL-VPN Package Information			
SSL-VPN Package Version	Unreachable [Update]		
FortiToken Seed Server			
Registration	Reachable (0 Tokens Registered)		
AV & IPS Download Options			
Web Filtering and Email Filtering Options			

Apply

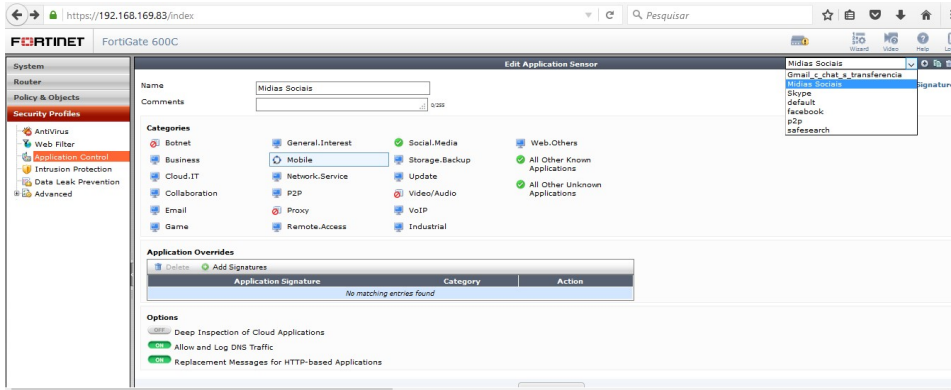
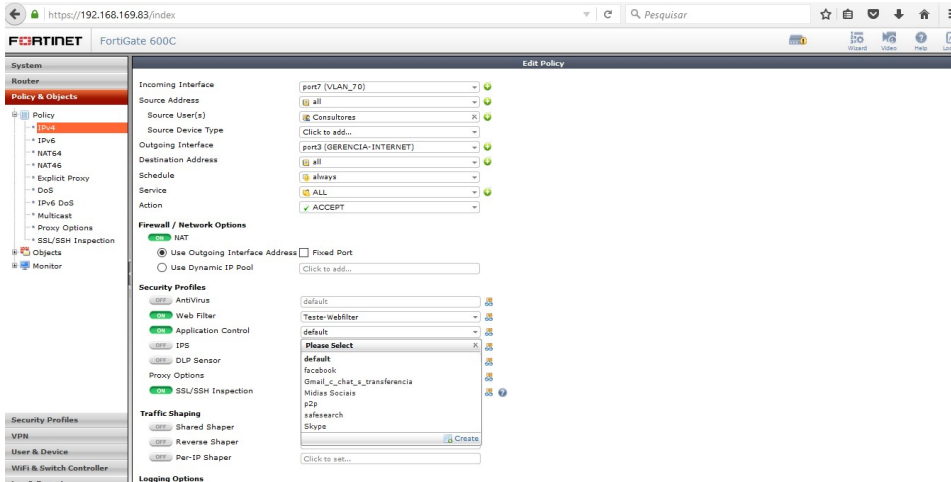
Comentário

Assinatura
do Cliente

Assinatura NCT

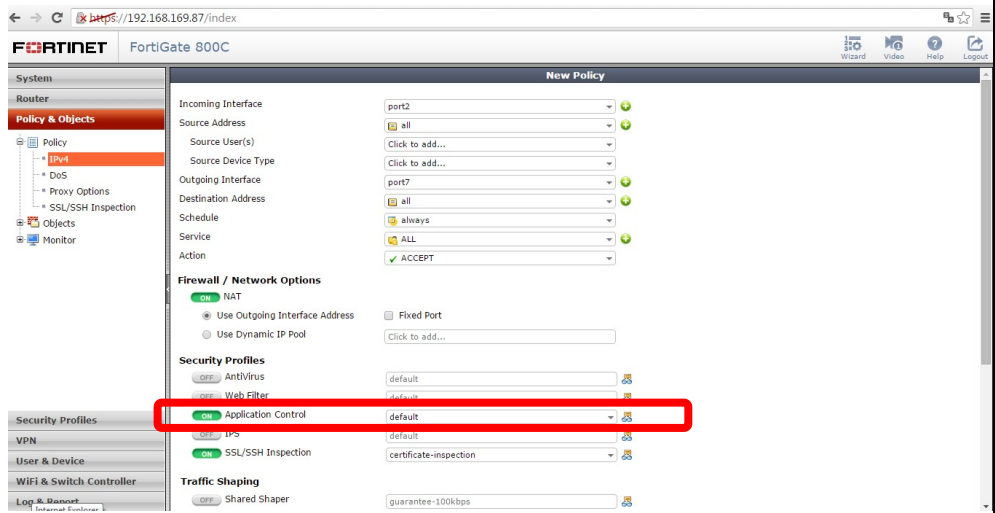
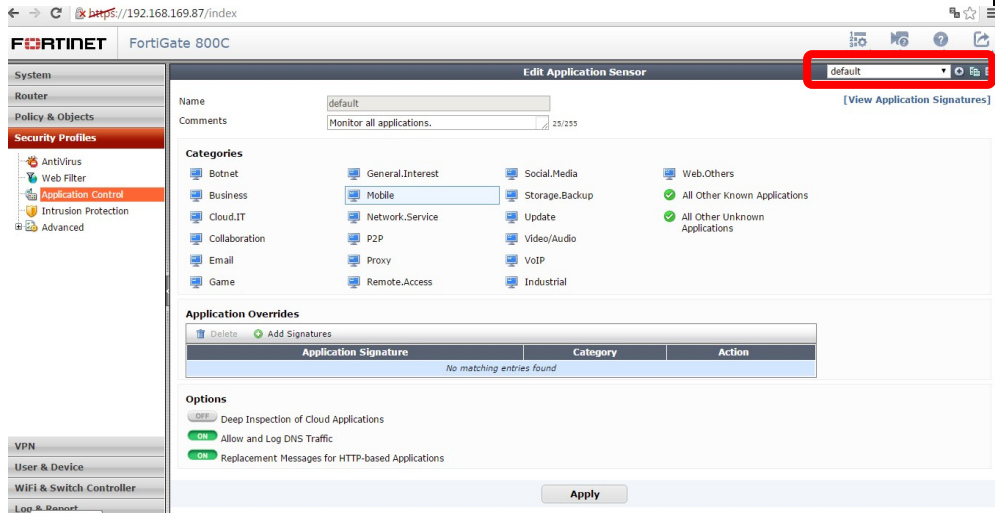
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 22/126

CONTROLE POR POLÍTICA DE FIREWALL

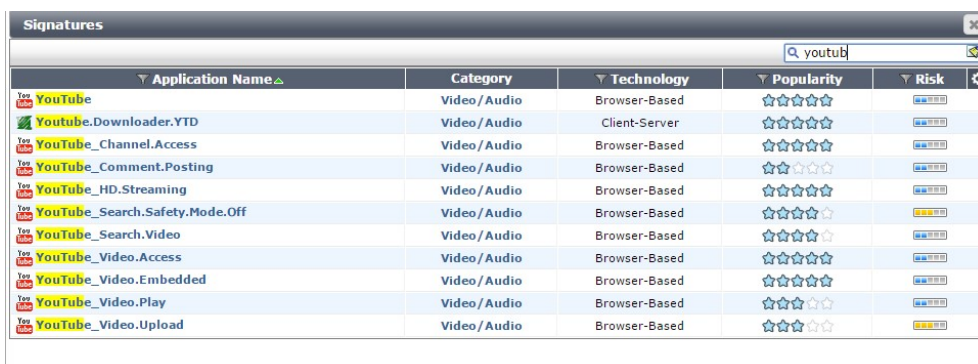
Item de Teste - 1.6.2.2	Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento) e categorias de aplicações;		
Objetivo do Teste	Demonstrar funcionalidade solicitada		
Configuração do Teste	Configurado profiles de app control conforme os grupos solicitados e ativado em regra de firewall.		
Procedimento do Teste	Demonstrar que é possível a criação de diferentes configurações de sensores visando a proteção das aplicações.		
Evidências	 Possibilidade de criação de diversos sensores com diferentes configurações  Aplicação de sensor em regra de firewall.		
Comentário			
Assinatura do Cliente	Assinatura NCT		

CONTROLE DE APLICAÇÕES

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 23/126

Item de Teste - 1.6.3.1.1	Deve ser possível liberar e bloquear aplicações sem a necessidade de liberar portas e/ou protocolos;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurado um profile de APP control especificando as aplicações tais como Youtube assim como a categoria P2P, em uma regra de firewall onde um usuários cujo o gateway de saída de internet é o Fortigate.
Procedimento do Teste	Usuário no IP 10.60.70.222 acessou o Youtube e não efetivar o acesso apos a configuração do perfil de aplicação bloqueando o youtube assim como a aplicação Utorrent.
Evidências	Configurado uma regra de firewall sem especificação de porta, apenas habilitando o perfil de segurança de controle de aplicação neste caso o default:  Configurado o perfil default liberando o youtube e todos os demais categorias:  Em seguida selecionado as aplicações correspondente ao youtube para habilitar o

bloqueio apenas para estes:



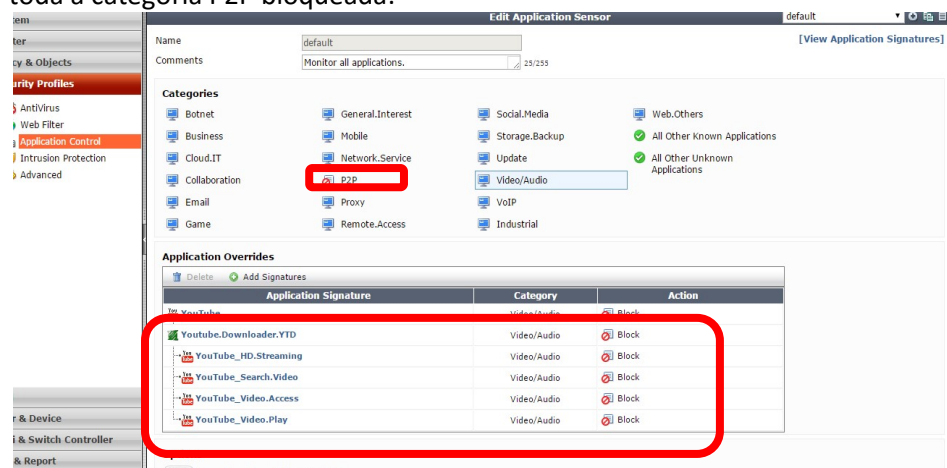
Application Name	Category	Technology	Popularity	Risk
YouTube	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Downloader.YTD	Video/Audio	Client-Server	★★★★★	Low
YouTube.Channel.Access	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Comment.Posting	Video/Audio	Browser-Based	★★★★★	Low
YouTube.HD.Streaming	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Search.Safety.Mode.Off	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Search.Video	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Video.Access	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Video.Embedded	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Video.Play	Video/Audio	Browser-Based	★★★★★	Low
YouTube.Video.Upload	Video/Audio	Browser-Based	★★★★★	Low

Selecionado o bloqueio de P2P tais como aplicações Bittorrent, que tem também instalado na máquina do cliente:



Application Name	Category	Technology	Popularity	Risk
Arctic.Torrent	P2P	Peer-to-Peer	★★★★★	High
BitTorrent	P2P	Peer-to-Peer	★★★★★	High
BitTorrent.Sync	P2P	Peer-to-Peer	★★★★★	High
C.Torrent	P2P	Peer-to-Peer	★★★★★	High
ExtraTorrent	P2P	Peer-to-Peer	★★★★★	High
G3.Torrent	P2P	Peer-to-Peer	★★★★★	High
HTTP.Torrent	P2P	Browser-Based	★★★★★	High
Pirate.Bay.Torrent	P2P	Browser-Based	★★★★★	High
TorrentSpy	P2P	Peer-to-Peer	★★★★★	High
Torrentz	P2P	Browser-Based	★★★★★	High

Perfil de controle de aplicação pronto com aplicações de youtube assim como toda a categoria P2P bloqueada:

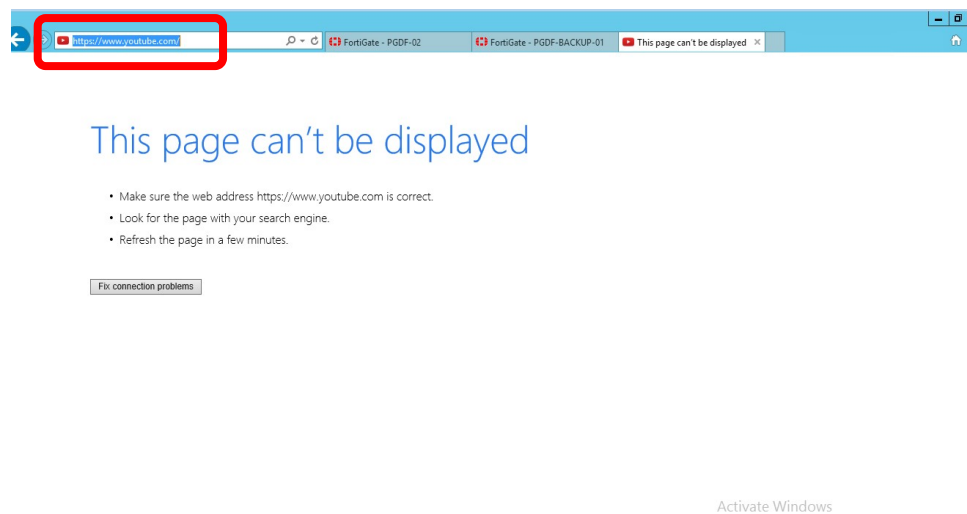


Category	Action
General.Interest	Block
Mobile	Block
Network.Service	Block
P2P	Block
Proxy	Block
Remote.Access	Block
Social.Media	Block
Storage.Backup	Block
Update	Block
VoIP	Block
Industrial	Block
Web.Others	Block
All Other Known Applications	Block
All Other Unknown Applications	Block

Application Signature	Category	Action
Youtube.Downloader.YTD	Video/Audio	Block
Youtube.HD.Streaming	Video/Audio	Block
Youtube.Search.Video	Video/Audio	Block
Youtube.Video.Access	Video/Audio	Block
Youtube.Video.Play	Video/Audio	Block

Em seguida a tela de tentativa de um acesso de um usuário que passa pelo Firewall na regra de acesso a qual contem o bloqueio do youtube:

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 25/126



No Log a tela de bloqueio da aplicação do youtube assim como alguns logs de BitTorrent que também foi bloqueado no perfil:

Router	#	Date/Time	Source	Destination	Application Name	Action	Destination Port	Application User	Application Details
Policy & Objects	1	17:09:47	10.69.70.222	216.58.222.14	YouTube	block	443		
Security Profiles	2	17:09:22	10.69.70.222	107.20.217.71	BitTorrent	block	80		
VPN	3	17:09:22	10.69.70.222	107.20.217.71	HTTP.BROWSER	pass	80		
User & Device	4	17:09:21	10.69.70.222	174.129.255.167	BitTorrent	block	80		
WiFi & Switch Controller	5	17:09:21	10.69.70.222	174.129.255.167	HTTP.BROWSER	pass	80		
Log & Report	6	17:09:21	10.69.70.222	107.20.217.71	BitTorrent	block	80		
	7	17:09:21	10.69.70.222	107.20.217.71	HTTP.BROWSER	pass	80		
Traffic Log	8	17:09:20	10.69.70.222	200.84.180.42	BitTorrent	block	60405		
Forward Traffic	9	17:09:19	10.69.70.222	66.150.48.45	HTTP.BROWSER_IE	pass	80		IE
Local Traffic	10	17:09:19	10.69.70.222	66.150.48.45	HTTP.BROWSER_IE	pass	80		IE
Multicast Traffic	11	17:09:19	10.69.70.222	23.21.139.158	BitTorrent	block	80		
Sniffer Traffic	12	17:09:19	10.69.70.222	184.26.136.98	HTTP.BROWSER_IE	pass	80		IE
	13	17:09:19	10.69.70.222	23.21.139.158	HTTP.BROWSER_IE	pass	80		IE
Event Log	14	17:09:19	10.69.70.222	50.19.123.159	HTTP.BROWSER_IE	pass	80		IE
Security Log	15	17:09:19	10.69.70.222	184.26.136.98	HTTP.BROWSER_IE	pass	80		IE
Antivirus	16	17:09:19	10.69.70.222	23.21.139.158	BitTorrent	block	80		

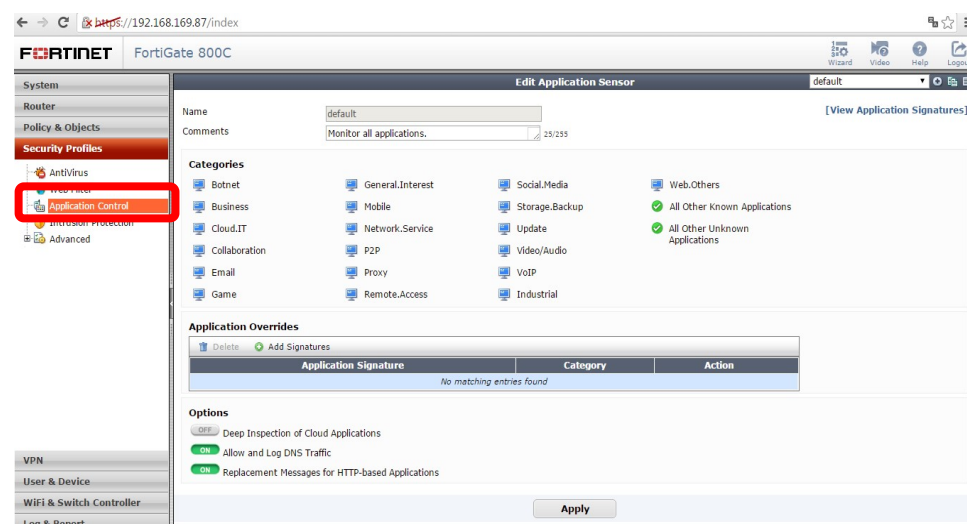
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.3.1.2	Reconhecer, no mínimo, 1.500 (um mil e quinhentas) aplicações diferentes, incluindo, mas não limitado: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualizações de software, protocolos de rede, VOIP, áudio, vídeo, proxies, mensageiros instantâneos, compartilhamento de arquivos e e-mail;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Listar a relação de todas as aplicações a partir de um profile default.
Procedimento do Teste	

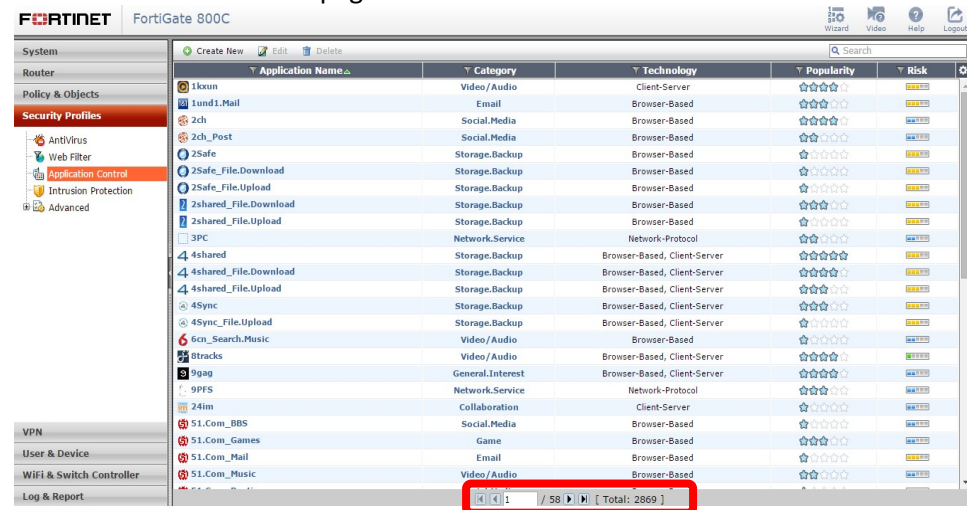
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 26/126

Evidências

Tela do Firewall referente a parte de configuração de controle de aplicação contendo todas as categorias conforme solitado



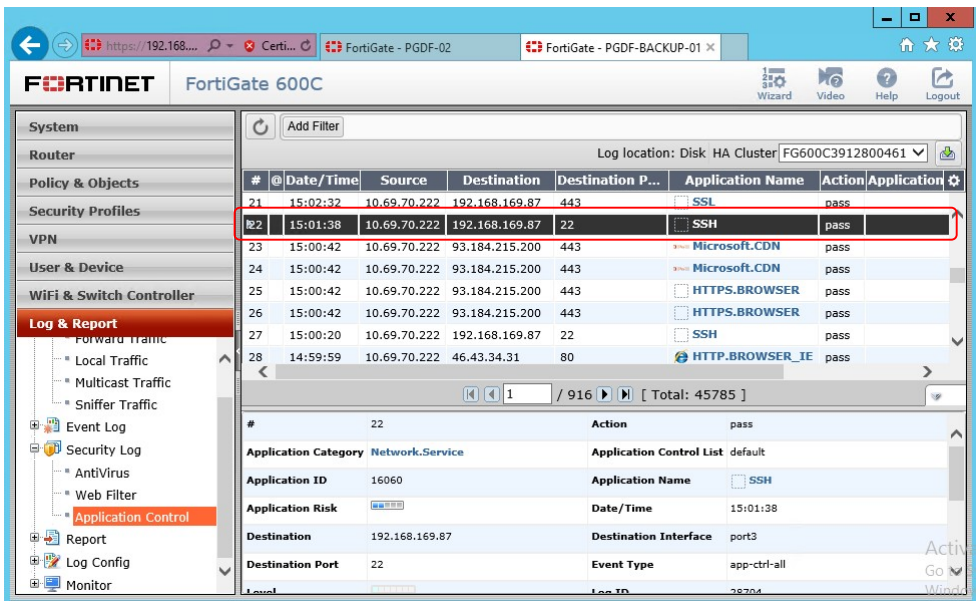
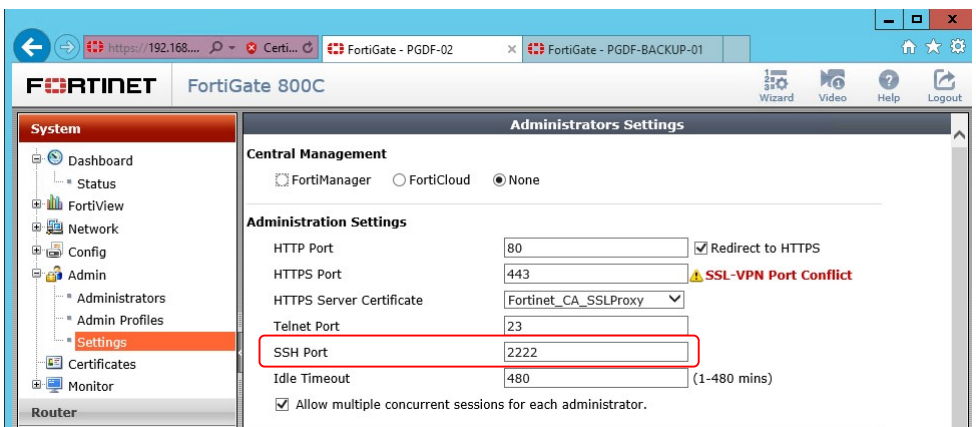
Segue abaixo a tela contendo uma demonstração do "View Application Signatures", o qual é possível observar que há mais de 2000 aplicações no database divididos em 58 páginas:

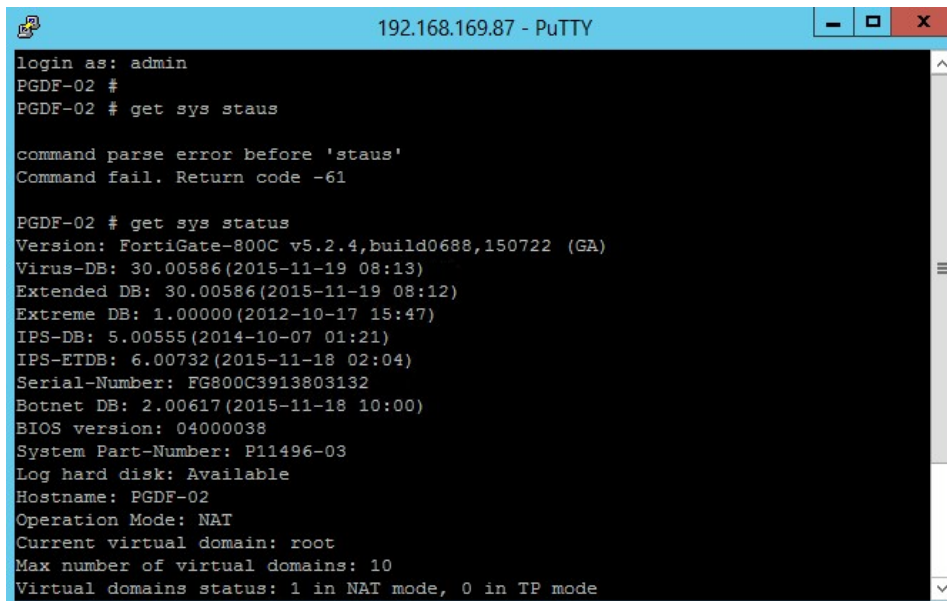


Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.3.1.4	Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares e assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A inspeção deve determinar se uma aplicação está utilizando a porta padrão ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 389;
---------------------------	--

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 27/126

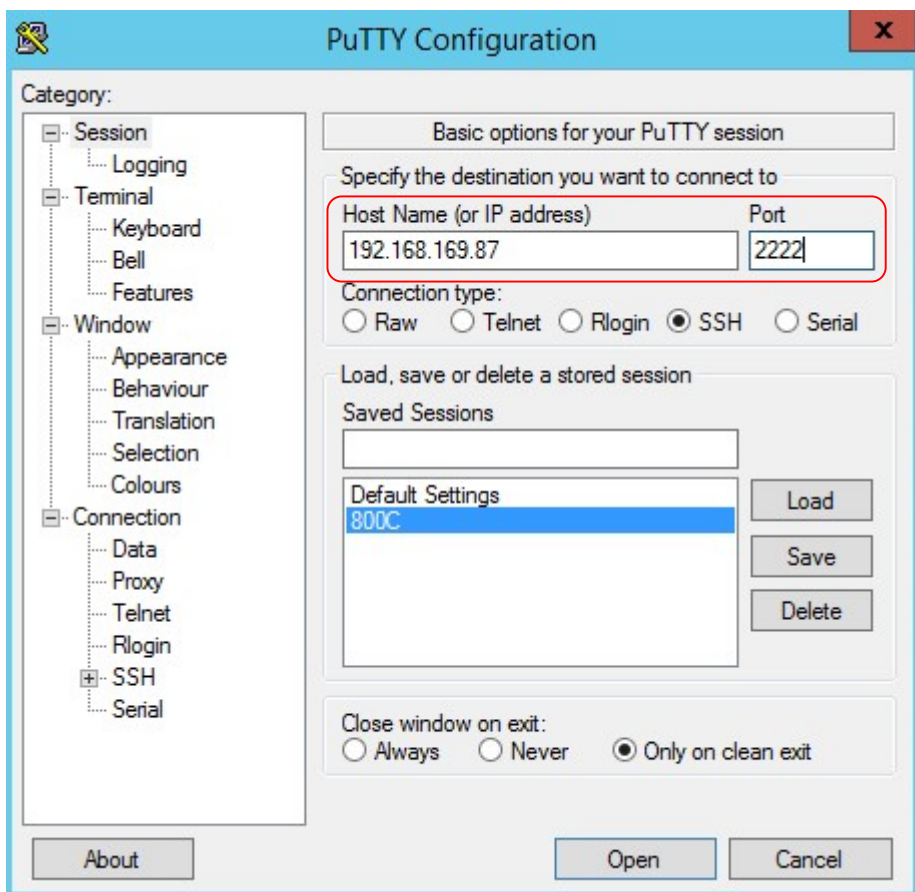
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Foi utilizado um teste onde a porta padrão do SSH foi alterada para demonstrar que mesmo em outra porta o equipamento consegue identificar corretamente a aplicação.
Procedimento do Teste	Usar o putty para logar na porta padrão e logar novamente após a porta ter sido alterada.
Evidências	 Log com porta padrão  Porta padrão de SSH sendo alterada para 2222



```
192.168.169.87 - PuTTY
login as: admin
PGDF-02 #
PGDF-02 # get sys staus

command parse error before 'staus'
Command fail. Return code -61

PGDF-02 # get sys status
Version: FortiGate-800C v5.2.4,build0688,150722 (GA)
Virus-DB: 30.00586(2015-11-19 08:13)
Extended DB: 30.00586(2015-11-19 08:12)
Extreme DB: 1.00000(2012-10-17 15:47)
IPS-DB: 5.00555(2014-10-07 01:21)
IPS-ETDB: 6.00732(2015-11-18 02:04)
Serial-Number: FG800C3913803132
Botnet DB: 2.00617(2015-11-18 10:00)
BIOS version: 04000038
System Part-Number: P11496-03
Log hard disk: Available
Hostname: PGDF-02
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
```



PuTTY Configuration

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH**
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.169.87 Port: 2222

Connection type:
☐ Raw ☐ Telnet ☐ Rlogin ☒ SSH ☐ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings	Load
800C	

Save Delete

Close window on exit:
☐ Always ☐ Never ☒ Only on clean exit

About Open Cancel

```

192.168.169.87 - PuTTY
login as: admin
PGDF-02 # get system status
Version: FortiGate-800C v5.2.4,build0688,150722 (GA)
Virus-DB: 30.00586(2015-11-19 08:13)
Extended DB: 30.00586(2015-11-19 08:12)
Extreme DB: 1.00000(2012-10-17 15:47)
IPS-DB: 5.00555(2014-10-07 01:21)
IPS-ETDB: 6.00732(2015-11-18 02:04)
Serial-Number: FG800C3913803132
Botnet DB: 2.00617(2015-11-18 10:00)
BIOS version: 04000038
System Part-Number: P11496-03
Log hard disk: Available
Hostname: PGDF-02
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
License Status: Low-Encryption (LENC)
Branch point: 688
Release Version Information: GA
--More--

```

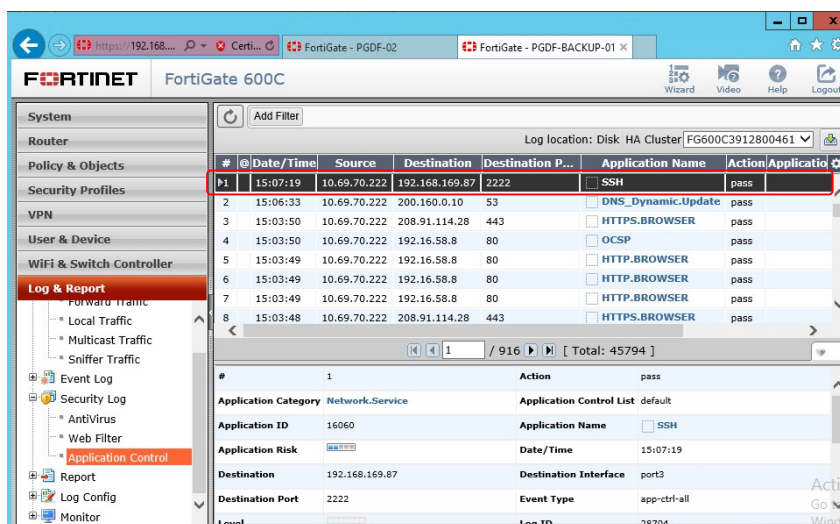
Acessado pela porta 2222

```

Administrator: Command Prompt
TCP 0.0.0.0:49162 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49163 0.0.0.0:0 LISTENING
TCP 10.69.70.222:139 0.0.0.0:0 LISTENING
TCP 10.69.70.222:3389 10.61.3.16:64639 ESTABLISHED
TCP 10.69.70.222:49828 192.168.169.87:22 TIME_WAIT
TCP 10.69.70.222:49873 192.168.169.87:2222 ESTABLISHED
TCP 1::1:80 1::1:0 LISTENING
TCP 1::1:135 1::1:0 LISTENING

```

Conexão estabelecida pela porta 2222



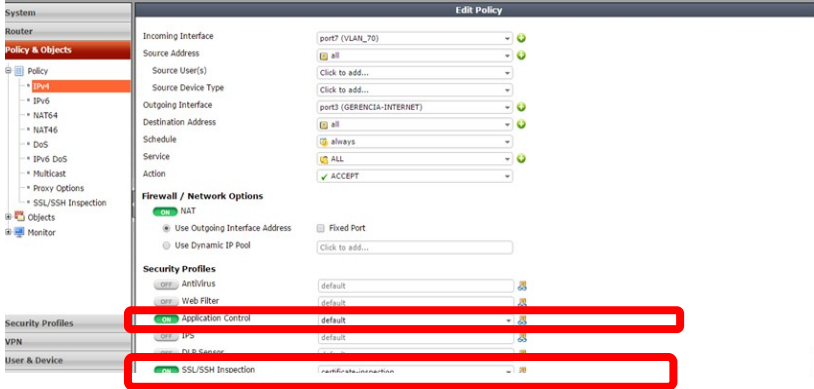
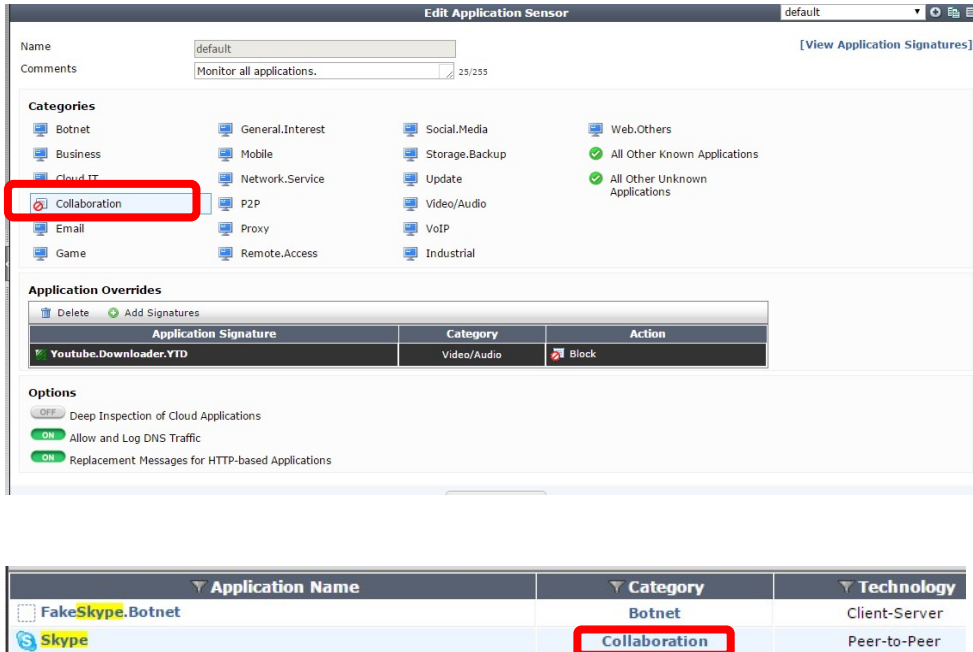
#	@/Date/Time	Source	Destination	Destination P...	Application Name	Action/Applicatio
1	15:07:19	10.69.70.222	192.168.169.87	2222	SSH	pass
2	15:06:33	10.69.70.222	200.160.0.10	53	DNS_Dynamic.Update	pass
3	15:03:50	10.69.70.222	208.91.114.28	443	HTTPS.BROWSER	pass
4	15:03:50	10.69.70.222	192.16.58.8	80	OCSP	pass
5	15:03:49	10.69.70.222	192.16.58.8	80	HTTP.BROWSER	pass
6	15:03:49	10.69.70.222	192.16.58.8	80	HTTP.BROWSER	pass
7	15:03:49	10.69.70.222	192.16.58.8	80	HTTP.BROWSER	pass
8	15:03:48	10.69.70.222	208.91.114.28	443	HTTPS.BROWSER	pass

Comentário

Assinatura
do Cliente

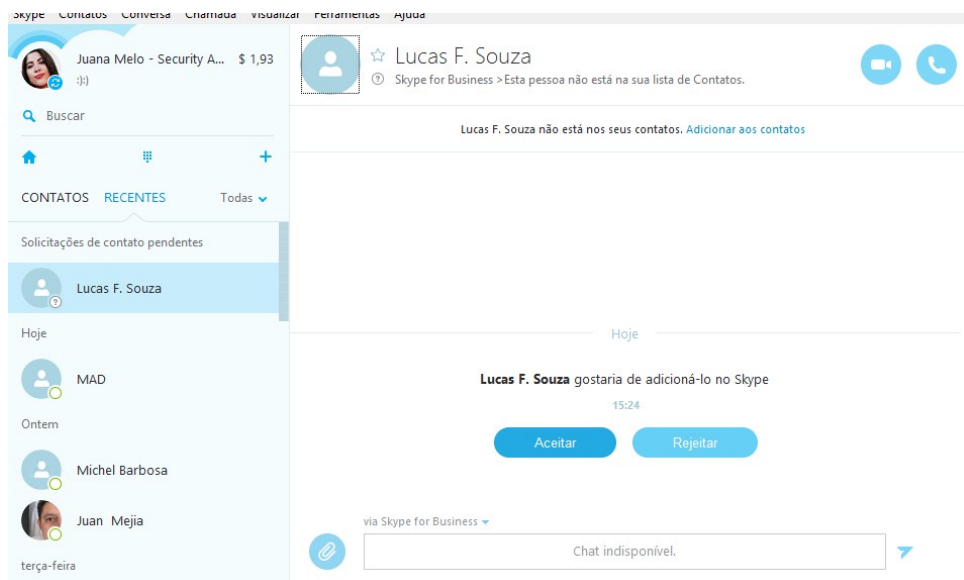
Assinatura NCT

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 30/126

Item de Teste - 1.6.3.1.7	Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurado profile de APP control em adicional na regra de firewall habilitado o SSL inspection, bloqueando neste caso o acesso do Skype via 443.
Procedimento do Teste	Executar um acesso seguro ao Skype verificar no Log o match no tráfego das aplicações bloqueando aplicação do usuário.
Evidências	Configurado uma regra de firewall especificando o perfil de controle de aplicação default assim como o perfil de SSL/SSH inspection :  O perfil inserido na regra correspondente ao default onde foi configurado o bloqueio de toda a categoria "collaboration" a qual o Skype esta inserido: 

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 31/126

Apos a configuração de acesso o usuário conectado na estação de teste que passa pelo firewall no IP 10.69.70.222 tenta acessar o Skype, e o mesmo na consegue efetivar o acesso:



No Log mostra vários eventos de bloqueio do Skype do usuário pela porta 443:

System									
#	Date/Time	Source	Destination	Application Name	Action	Destination Port	Application User	Application Details	
1	16:54:21	10.69.70.222	157.55.130.147	Skype	block	80			
2	16:54:20	10.69.70.222	157.55.130.148	Skype	block	80			
3	16:54:19	10.69.70.222	157.55.130.147	Skype	block	443			
4	16:54:18	10.69.70.222	65.52.108.74	Skype	block	443			
5	16:54:18	10.69.70.222	157.55.130.148	Skype	block	80			
6	16:54:18	10.69.70.222	157.55.130.162	Skype	block	33033			
7	16:54:17	10.69.70.222	157.55.130.147	Skype	block	443			
8	16:54:16	10.69.70.222	157.55.130.148	Skype	block	33033			
9	16:54:16	10.69.70.222	157.55.130.162	Skype	block	443			
10	16:54:16	10.69.70.222	157.55.235.147	Skype	block	33033			
11	16:54:14	10.69.70.222	157.55.130.162	Skype	block	33033			
12	16:54:14	10.69.70.222	157.56.52.15	Skype	block	33033			
13	16:54:13	10.69.70.222	111.221.77.144	Skype	block	40018			
14	16:54:08	10.69.70.222	157.55.56.173	Skype	block	40004			
15	16:54:07	10.69.70.222	157.56.52.15	Skype	block	33033			
16	16:54:04	10.69.70.222	111.221.77.174	Skype	block	40031			

Comentário

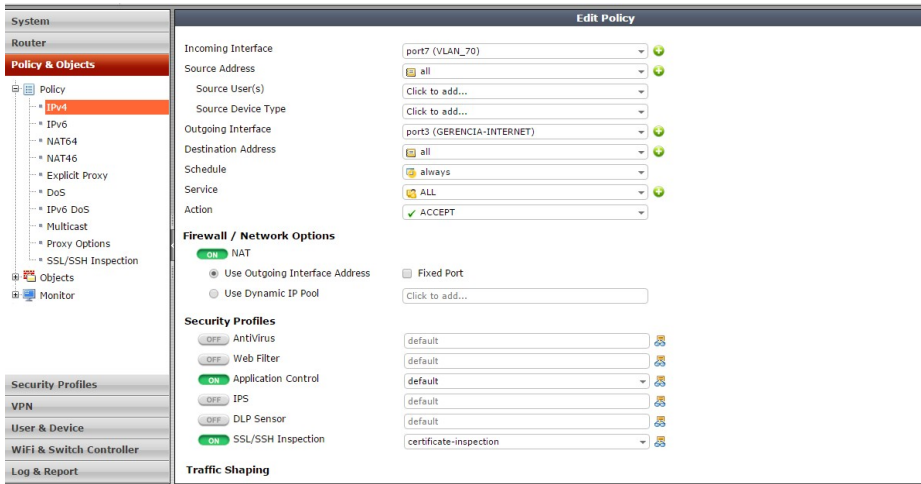
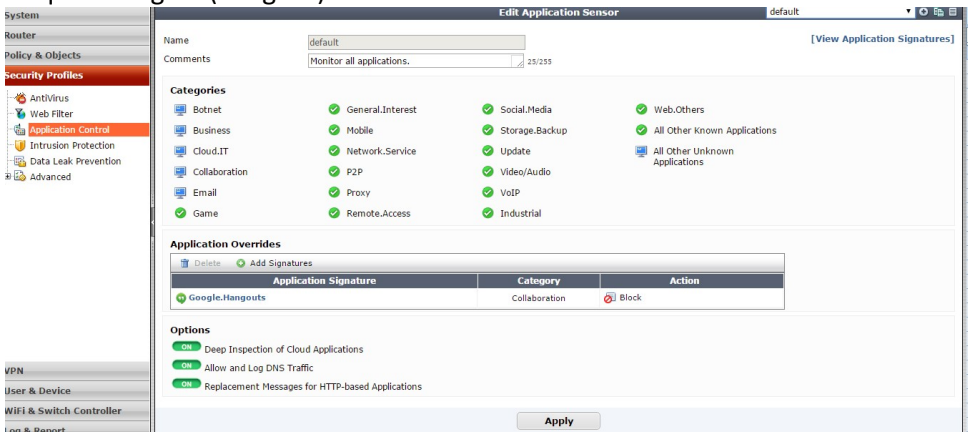
Assinatura do Cliente

Assinatura NCT

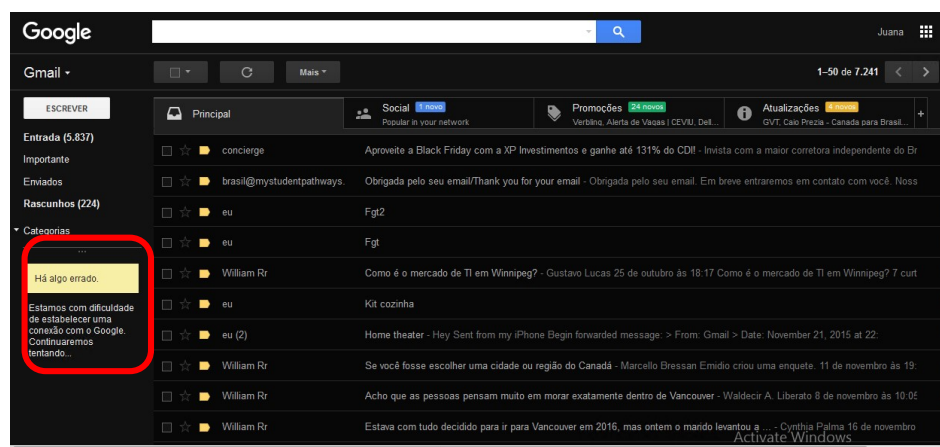
Item de Teste - 1.6.3.1.8

Deve realizar a decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do mesmo, validando se o tráfego corresponde à sua especificação, incluindo, mas não limitado a: Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 32/126

	deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a: compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurado o profile de APP control contendo as aplicações conforme mencionado, assim como ativando na política o SSL inspection, onde o cliente da maquina 10.69.70.222 acessou o gmailn todavia sendo bloqueado via controle de aplicação o bloqueio referente ao chat hangout.
Procedimento do Teste	Efetivar um acesso correspondente a aplicação conforme mencionado verificar no Log o match no trafego das aplicações
Evidências	Feito uma regra de firewall habilitando o perfil de segurança de controle de aplicação default e perfil de SSL/SSH inspection:  Configuração do perfil de segurança de controle de aplicação selecionando o bloqueio do gtalk(hangout):  Cliente conseguiu acessar o gmail mais o gtalk (hangout) foi bloqueado, todos conexão segura SSL:

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 33/126



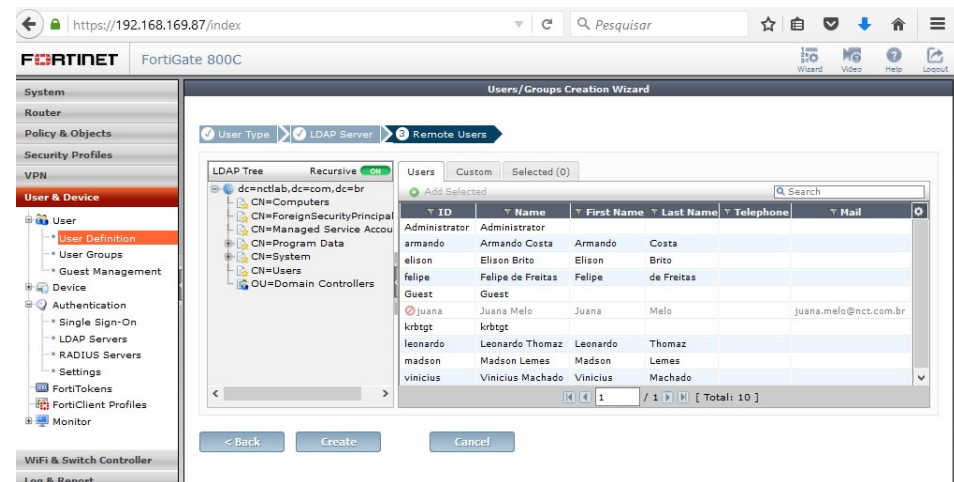
Log no firewall mostrando o acesso normal ao gmail e o block ao hangout na porta 443:

#	Date/Time	Source	Destination	Application Name	Action	Destination Port	Application User
1	14:20:31	10.69.70.222	173.194.42.199	Google.Hangouts	block	443	
2	14:20:28	10.69.70.222	216.58.222.5	Gmail	pass	443	
3	14:20:01	10.69.70.222	192.168.169.182	Unknown Application	pass	137	
4	14:18:01	10.69.70.222	192.168.169.182	Unknown Application	pass	137	
5	14:16:40	10.69.70.222	173.194.42.199	Google.Hangouts	pass	443	
6	14:16:01	10.69.70.222	192.168.169.182	Unknown Application	pass	137	
7	14:15:58	10.69.70.222	173.194.42.199	Google.Hangouts	pass	443	
8	14:14:45	10.69.70.222	216.58.222.14	HTTP.BROWSER_Firefox	pass	80	
9	14:14:44	10.69.70.222	173.194.42.192	HTTP.BROWSER_Firefox	pass	80	
10	14:14:02	10.69.70.222	192.168.169.182	NetBIOS.Name.Service	pass	137	
11	14:11:49	10.69.70.222	200.123.194.11	Facebook	pass	443	
12	14:11:49	10.69.70.222	200.123.194.11	Facebook	pass	443	
13	14:11:47	10.69.70.222	173.252.89.132	Facebook	pass	443	
14	14:11:32	10.69.70.222	200.123.194.11	Facebook	pass	443	
15	14:11:32	10.69.70.222	200.123.194.11	Facebook	pass	443	
16	14:11:26	10.69.70.222	173.252.89.132	Facebook	pass	443	
17	14:11:14	10.69.70.222	200.182.35.138	Root.Certificate.URL	pass	80	
18	14:11:08	10.69.70.222	200.123.194.11	Facebook	pass	443	
19	14:11:08	10.69.70.222	200.123.194.11	Facebook	pass	443	

Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.3.1.13	Os appliances devem possuir a capacidade de identificar o usuário com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar o modo Polling mode Active Directory Server
Procedimento do Teste	Demonstrar integração com Fortigate com AD, sem a necessidade de instalação de agente.
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 34/126

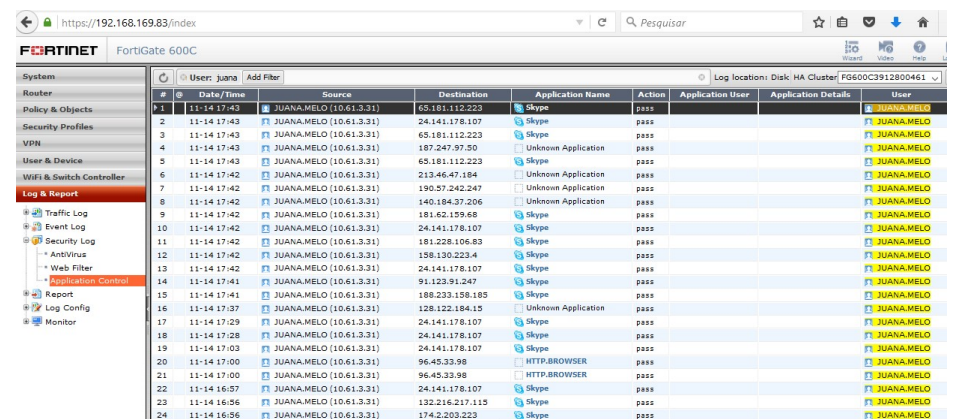


The screenshot shows the FortiGate 800C web interface. The left sidebar has 'User & Device' selected, with 'User' and 'User Definition' highlighted. The main area is the 'Users/Groups Creation Wizard' in the 'Remote Users' step. It shows an LDAP tree on the left with 'OU=Domain Controllers' selected. On the right, a table lists users from the LDAP server:

ID	Name	First Name	Last Name	Telephone	Mail
Administrator	Administrator				
armando	Armando Costa	Armando	Costa		
elison	Elison Brito	Elison	Brto		
felipe	Felipe de Freitas	Felipe	de Freitas		
Guest	Guest				
juana	Juana Melo	Juana	Melo		juana.melo@nct.com.br
krbtgt	krbtgt				
leonardo	Leonardo Thomaz	Leonardo	Thomaz		
madson	Madson Lemes	Madson	Lemes		
vinicius	Vinicius Machado	Vinicius	Machado		

Buttons at the bottom include '< Back', 'Create', and 'Cancel'.

Fortigate integrado com servidor Microsoft AD

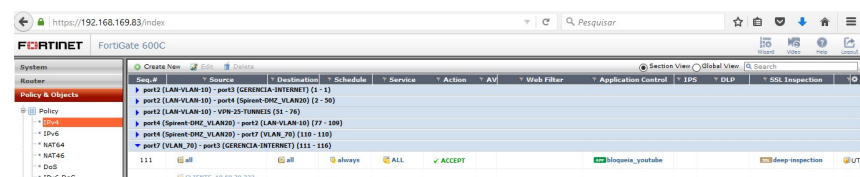


The screenshot shows the FortiGate 600C web interface. The left sidebar has 'Log & Report' selected. The main area displays a table of user activity logs:

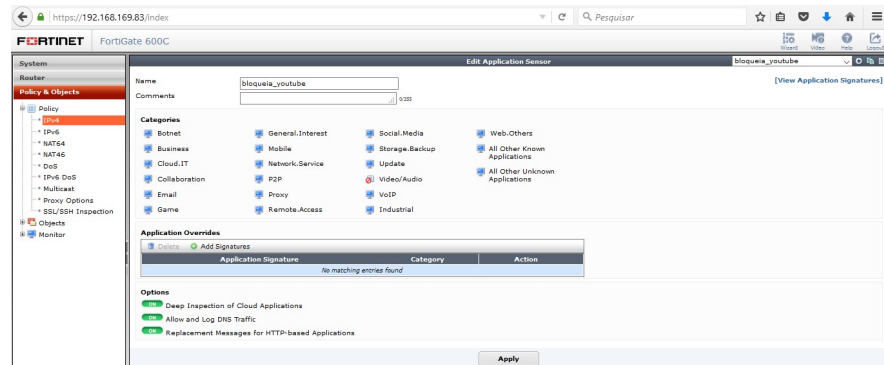
#	Date/Time	Source	Destination	Application Name	Action	Application User	Application Details	User
1	11-14 17:43	JUANA.MELO (10.61.3.31)	65.181.112.223	Skype	pass			JUANA.MELO
2	11-14 17:43	JUANA.MELO (10.61.3.31)	24.141.178.107	Skype	pass			JUANA.MELO
3	11-14 17:43	JUANA.MELO (10.61.3.31)	65.181.112.223	Skype	pass			JUANA.MELO
4	11-14 17:43	JUANA.MELO (10.61.3.31)	187.247.97.50	Unknown Application	pass			JUANA.MELO
5	11-14 17:43	JUANA.MELO (10.61.3.31)	65.181.112.223	Skype	pass			JUANA.MELO
6	11-14 17:42	JUANA.MELO (10.61.3.31)	213.46.47.184	Unknown Application	pass			JUANA.MELO
7	11-14 17:42	JUANA.MELO (10.61.3.31)	190.57.242.247	Unknown Application	pass			JUANA.MELO
8	11-14 17:42	JUANA.MELO (10.61.3.31)	140.184.37.206	Unknown Application	pass			JUANA.MELO
9	11-14 17:42	JUANA.MELO (10.61.3.31)	181.62.159.68	Skype	pass			JUANA.MELO
10	11-14 17:42	JUANA.MELO (10.61.3.31)	24.141.178.107	Skype	pass			JUANA.MELO
11	11-14 17:42	JUANA.MELO (10.61.3.31)	181.228.106.83	Skype	pass			JUANA.MELO
12	11-14 17:42	JUANA.MELO (10.61.3.31)	158.130.223.4	Skype	pass			JUANA.MELO
13	11-14 17:42	JUANA.MELO (10.61.3.31)	24.141.178.107	Skype	pass			JUANA.MELO
14	11-14 17:41	JUANA.MELO (10.61.3.31)	91.122.91.247	Skype	pass			JUANA.MELO
15	11-14 17:41	JUANA.MELO (10.61.3.31)	188.233.158.185	Skype	pass			JUANA.MELO
16	11-14 17:37	JUANA.MELO (10.61.3.31)	128.122.184.15	Unknown Application	pass			JUANA.MELO
17	11-14 17:29	JUANA.MELO (10.61.3.31)	24.141.178.107	Skype	pass			JUANA.MELO
18	11-14 17:28	JUANA.MELO (10.61.3.31)	24.141.178.107	Skype	pass			JUANA.MELO
19	11-14 17:03	JUANA.MELO (10.61.3.31)	24.141.178.107	Skype	pass			JUANA.MELO
20	11-14 17:00	JUANA.MELO (10.61.3.31)	96.45.33.98	HTTP.BROWSER	pass			JUANA.MELO
21	11-14 17:00	JUANA.MELO (10.61.3.31)	96.45.33.98	HTTP.BROWSER	pass			JUANA.MELO
22	11-14 16:57	JUANA.MELO (10.61.3.31)	24.141.178.107	Skype	pass			JUANA.MELO
23	11-14 16:56	JUANA.MELO (10.61.3.31)	132.216.217.115	Skype	pass			JUANA.MELO
24	11-14 16:56	JUANA.MELO (10.61.3.31)	174.2.203.223	Skype	pass			JUANA.MELO

Log de atividade de usuário identificado do Microsoft AD sem agente.

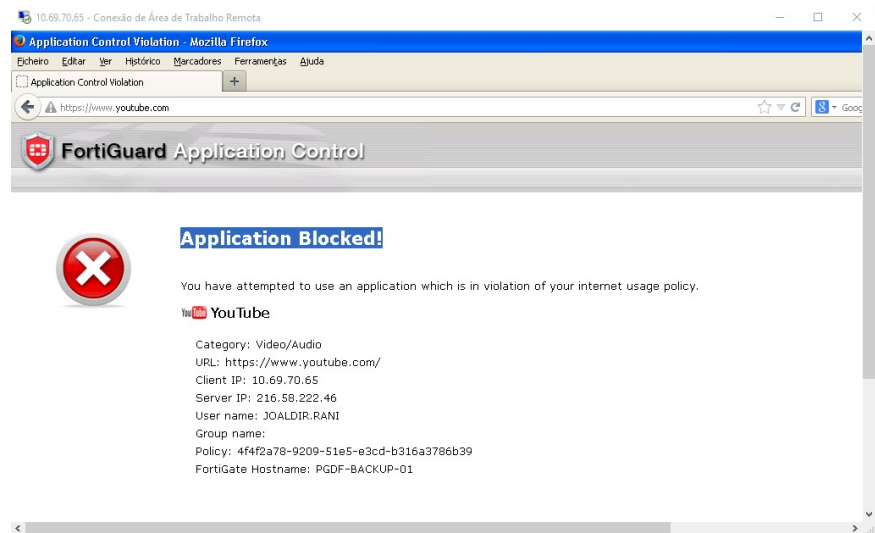
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.3.1.18	Deve alertar o usuário quando uma aplicação for bloqueada																																																																																				
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado																																																																																				
Configuração do Teste	Configurar replacement messages para " Application Control Block Page"																																																																																				
Procedimento do Teste	Validar a mensagem de bloqueio por um usuário ao acessa uma aplicação bloqueada e homologar a replacement messages.																																																																																				
Evidências	 The screenshot shows the FortiGate 600C web interface. The left sidebar has 'Policy & Objects' selected. The main area displays a table of firewall policies: <table><thead><tr><th>Seq.#</th><th>Source</th><th>Destination</th><th>Schedule</th><th>Service</th><th>Action</th><th>AV</th><th>Web Filter</th><th>Application Control</th><th>IPS</th><th>DLP</th><th>SSL Inspection</th></tr></thead><tbody><tr><td>1</td><td>port2 (LAN-VLAN-10)</td><td>port3 (CERENCIA-INTERNET) (1 - 1)</td><td></td><td>any</td><td>deny</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>2</td><td>port2 (LAN-VLAN-10)</td><td>port4 (Spine1-DMZ_VLAN20) (2 - 50)</td><td></td><td>any</td><td>deny</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>3</td><td>port2 (LAN-VLAN-10)</td><td>VLAN-25-TUNNELS (51 - 76)</td><td></td><td>any</td><td>deny</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>4</td><td>port4 (Spine1-DMZ_VLAN20)</td><td>port2 (LAN-VLAN-10) (77 - 100)</td><td></td><td>any</td><td>deny</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>5</td><td>port4 (Spine1-DMZ_VLAN20)</td><td>port7 (VLAN_70) (110 - 110)</td><td></td><td>any</td><td>deny</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>6</td><td>port7 (VLAN_70)</td><td>port3 (CERENCIA-INTERNET) (111 - 110)</td><td></td><td>any</td><td>deny</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table> Buttons at the bottom include 'Create New', 'Edit', 'Delete', 'Add Filter', and 'Monitor'. Regra de firewall	Seq.#	Source	Destination	Schedule	Service	Action	AV	Web Filter	Application Control	IPS	DLP	SSL Inspection	1	port2 (LAN-VLAN-10)	port3 (CERENCIA-INTERNET) (1 - 1)		any	deny							2	port2 (LAN-VLAN-10)	port4 (Spine1-DMZ_VLAN20) (2 - 50)		any	deny							3	port2 (LAN-VLAN-10)	VLAN-25-TUNNELS (51 - 76)		any	deny							4	port4 (Spine1-DMZ_VLAN20)	port2 (LAN-VLAN-10) (77 - 100)		any	deny							5	port4 (Spine1-DMZ_VLAN20)	port7 (VLAN_70) (110 - 110)		any	deny							6	port7 (VLAN_70)	port3 (CERENCIA-INTERNET) (111 - 110)		any	deny						
Seq.#	Source	Destination	Schedule	Service	Action	AV	Web Filter	Application Control	IPS	DLP	SSL Inspection																																																																										
1	port2 (LAN-VLAN-10)	port3 (CERENCIA-INTERNET) (1 - 1)		any	deny																																																																																
2	port2 (LAN-VLAN-10)	port4 (Spine1-DMZ_VLAN20) (2 - 50)		any	deny																																																																																
3	port2 (LAN-VLAN-10)	VLAN-25-TUNNELS (51 - 76)		any	deny																																																																																
4	port4 (Spine1-DMZ_VLAN20)	port2 (LAN-VLAN-10) (77 - 100)		any	deny																																																																																
5	port4 (Spine1-DMZ_VLAN20)	port7 (VLAN_70) (110 - 110)		any	deny																																																																																
6	port7 (VLAN_70)	port3 (CERENCIA-INTERNET) (111 - 110)		any	deny																																																																																

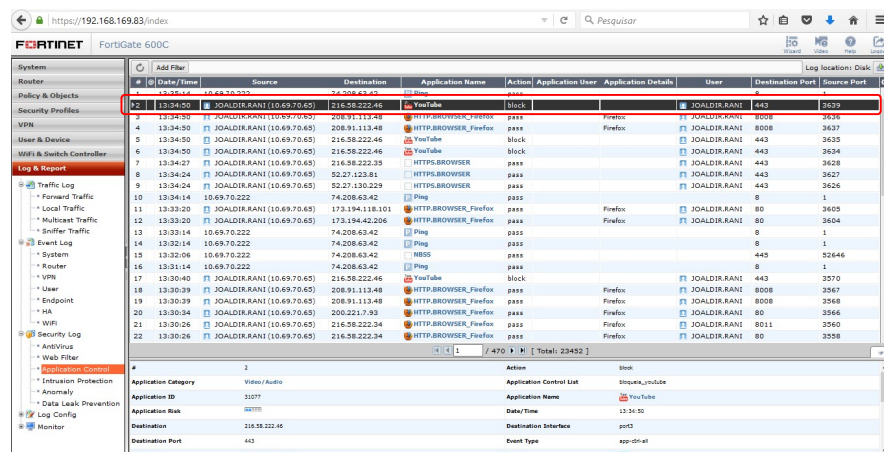
Regra de firewall



Sensor de AppControl



Tela de bloqueio ao acessar aplicação bloqueada.



Comentário

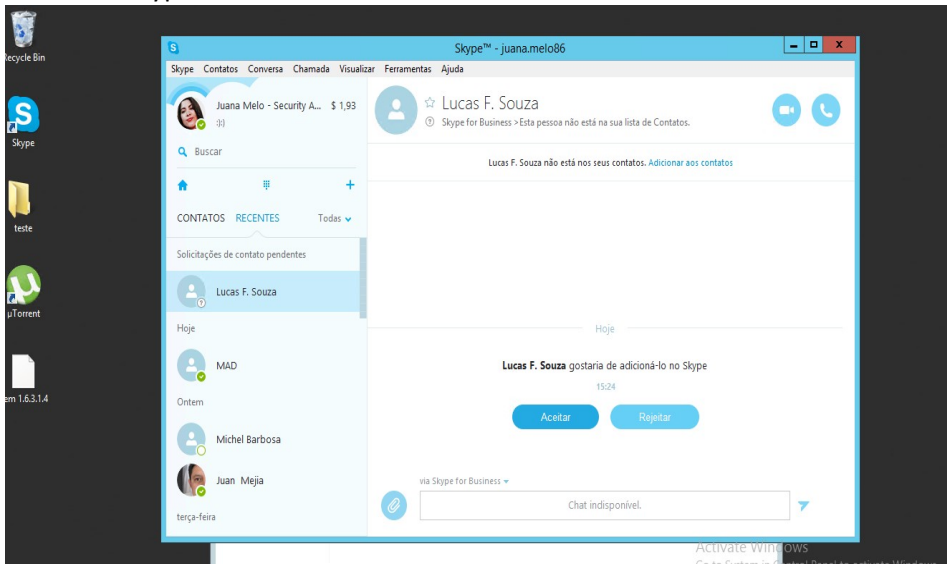
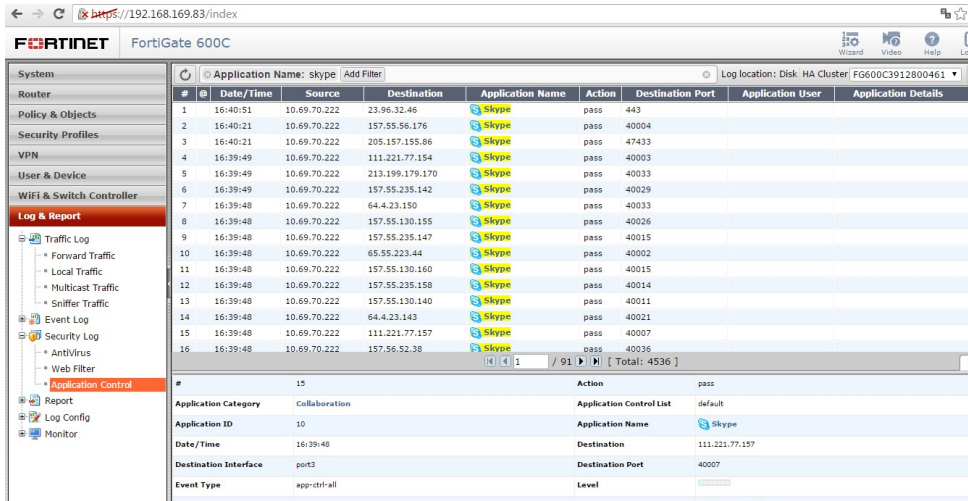
Assinatura
do Cliente

Assinatura NCT

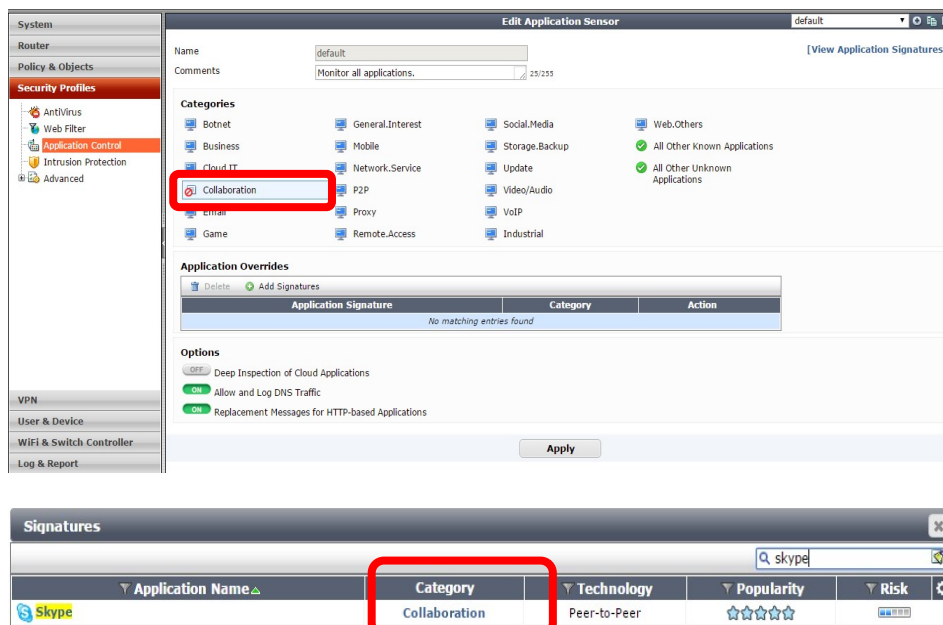
Item de Teste

Deve possibilitar que o controle de portas seja aplicado para todas as

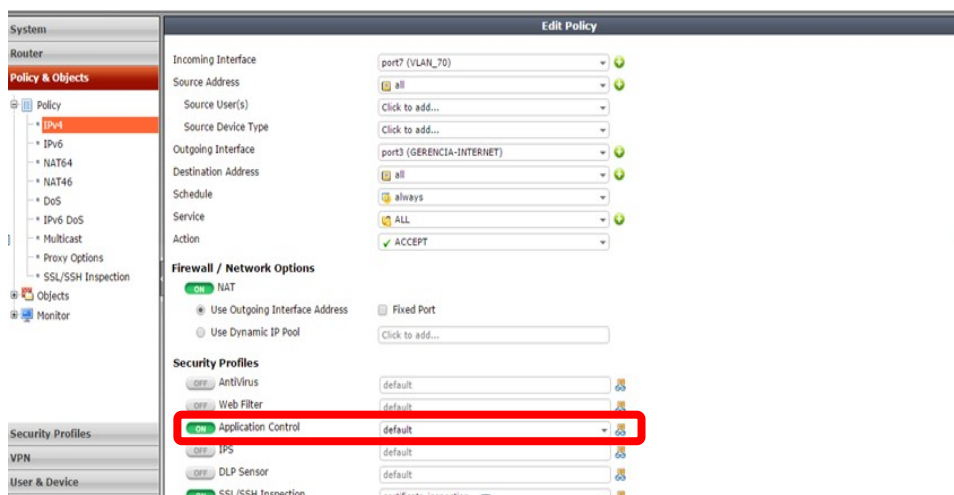
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 36/126

- 1.6.3.1.19	aplicações;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar profile de APP control assim como criar uma regra de firewall habilitando este profile.
Procedimento do Teste	Foi criado uma regra de firewall indicando um perfil de segurança de controle de aplicação "default" o qual contém a lista completa de todas as aplicações, onde foi demonstrado o controle de acesso por aplicações , onde o usuário efetuou o acesso ao Skype que estava com sua categoria bloqueada.
Evidências	Inicialmente o usuário acessou da estação de estes o IP 10.69.70.222 onde o acesso ao Skype estava liberado:  O log demonstra que o acesso do usuário passou normalmente sem nenhum bloqueio: 

Configurando o perfil de controle de aplicação bloqueando a categoria Collaboration a qual o Skype está inserido:

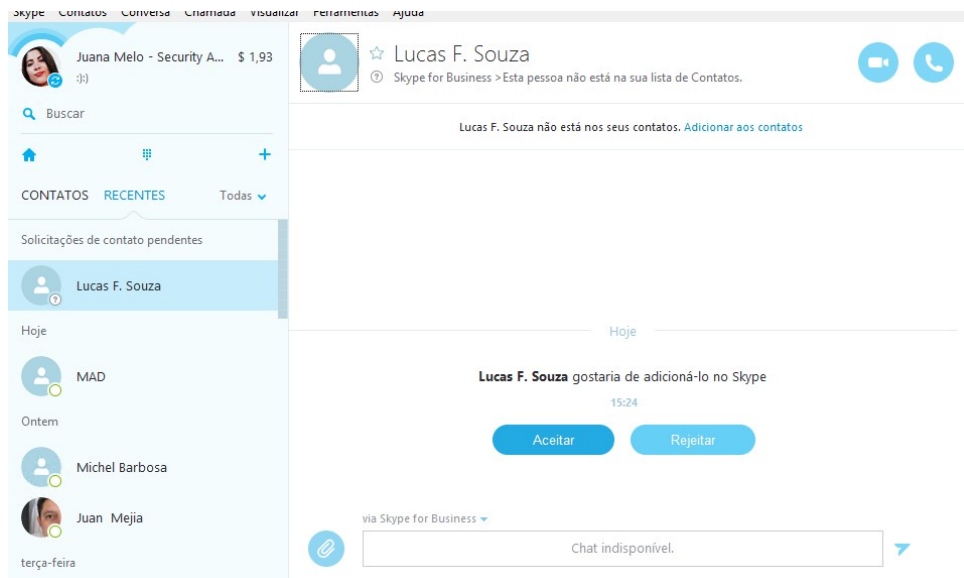


Na regra de Firewall foi inserido o perfil de default de controle de aplicação contendo as especificas configurações conforme executado acima:



Apos habilitado a política de acesso o cliente tenta novamente acessar o Skype, e o mesmo é bloqueado:

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 38/126



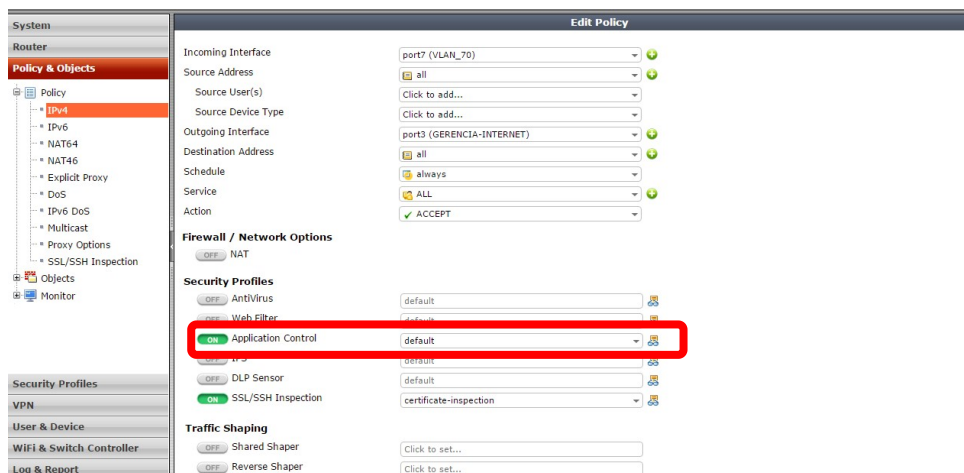
No Log é possível observar que o usuário está sendo bloqueado pelo filtro de controle de aplicação pelo fato do sensor tem habilitado a categoria do Skype:

Router	#	Date/Time	Source	Destination	Application Name	Action	Destination Port	Application User	Application Details
Policy & Objects	1	16:54:21	10.69.70.222	157.55.130.147	Skype	block	80		
Security Profiles	2	16:54:20	10.69.70.222	157.55.130.148	Skype	block	80		
VPN	3	16:54:19	10.69.70.222	157.55.130.147	Skype	block	443		
User & Device	4	16:54:18	10.69.70.222	65.52.108.74	Skype	block	443		
WiFi & Switch Controller	5	16:54:18	10.69.70.222	157.55.130.148	Skype	block	443		
Log & Report	6	16:54:18	10.69.70.222	157.55.130.162	Skype	block	80		
	7	16:54:17	10.69.70.222	157.55.130.147	Skype	block	33033		
	8	16:54:16	10.69.70.222	157.55.130.148	Skype	block	33033		
	9	16:54:16	10.69.70.222	157.55.130.162	Skype	block	443		
	10	16:54:16	10.69.70.222	157.55.235.147	Skype	block	33033		
	11	16:54:14	10.69.70.222	157.55.130.162	Skype	block	33033		
	12	16:54:14	10.69.70.222	157.56.52.15	Skype	block	33033		
	13	16:54:13	10.69.70.222	111.221.77.144	Skype	block	40018		
	14	16:54:08	10.69.70.222	157.55.56.173	Skype	block	40004		
	15	16:54:07	10.69.70.222	157.56.52.15	Skype	block	33033		
	16	16:54:04	10.69.70.222	111.221.77.174	Skype	block	40031		

#	1	Action	block
Application Category	Collaboration	Application Control List	default
Application ID	10	Application Name	Skype
Date/Time	16:54:21	Destination	157.55.130.147
Destination Interface	port2	Destination Port	80
Event Type	app-ctrl-all	Level	deny

Comentário	
Assinatura do Cliente	Assinatura NCT

Item de Teste - 1.6.3.1.20	Deve possibilitar a diferenciação de tráfego peer-to-peer (bittorrent, emule, neonet e etc.), proxies (ghostsurf, freegate, ultrasurf e etc.) e Instant Messaging (AIM, Gtalk, Facebook Chat, etc.), permitindo controle granular nas políticas definidas para ambos;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar profile de APP control, especificando ações específicas para cada categoria de aplicações, neste caso habilitando o perfil default.
Procedimento do Teste	Configurado uma regra de firewall com o perfil de segurança de controle de aplicação ativado, apenas em caráter de monitoração para que apareça no log os diferentes tipos de aplicações conforme solicitado, utilizando o usuário autenticado Joaldir e a máquina 10.69.70.222.
Evidências	Regra de firewall com o perfil de segurança de controle de aplicação ativado:



System
Router
Policy & Objects
Policy
IPv4
IPv6
NAT64
NAT46
Explicit Proxy
DoS
IPv6 DoS
Multicast
Proxy Options
SSL/SSH Inspection
Objects
Monitor
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report

Edit Policy

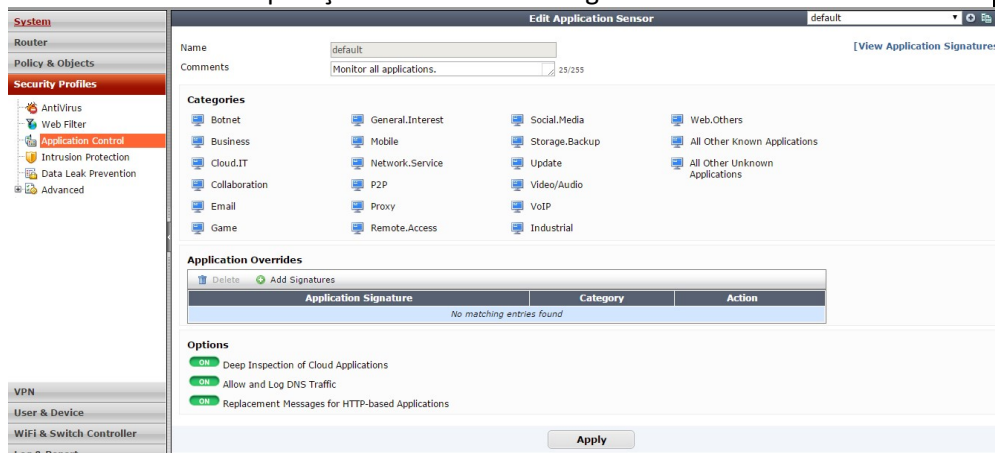
Incoming Interface: port7 (VLAN_70)
Source Address: all
Source User(s): Click to add...
Source Device Type: Click to add...
Outgoing Interface: port3 (GERENCIA-INTERNET)
Destination Address: all
Schedule: always
Service: ALL
Action: ACCEPT

Firewall / Network Options
NAT: OFF

Security Profiles
Antivirus: OFF
Web Filter: OFF
Application Control: ON
DLP Sensor: OFF
SSL/SSH Inspection: ON (certificate-inspection)

Traffic Shaping
Shared Shaper: OFF
Reverse Shaper: OFF

Perfil de controle de aplicação com todas as categorias habilitadas :



System
Router
Policy & Objects
Security Profiles
Antivirus
Web Filter
Application Control
Intrusion Protection
Data Leak Prevention
Advanced
VPN
User & Device
WiFi & Switch Controller
Log & Report

Edit Application Sensor default

Name: default
Comments: Monitor all applications. 25/255

Categories
Botnet, General.Interest, Social.Media, Web.Others, Business, Mobile, Storage.Backup, All Other Known Applications, Cloud.IT, Network.Service, Update, All Other Unknown Applications, Collaboration, P2P, Video/Audio, Email, Proxy, VoIP, Game, Remote.Access, Industrial

Application Overrides
Delete, Add Signatures
Application Signature, Category, Action
No matching entries found

Options
Deep Inspection of Cloud Applications: ON
Allow and Log DNS Traffic: ON
Replacement Messages for HTTP-based Applications: ON

Apply

Este é o log do firewall correspondente aos acessos do cliente 10.69.70.222:

#	Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
11	13:28:52	10.69.70.222	64.182.240.181	UltraSurf_9.6+	pass		9.6+
12	13:28:05	10.69.70.222	23.4.43.27	Root.Certificate.URL	pass		
13	13:28:04	10.69.70.222	23.4.43.27	Root.Certificate.URL	pass		
14	13:28:03	10.69.70.222	52.5.113.206	HTTP.BROWSER	pass		
15	13:28:03	10.69.70.222	198.41.215.68	HTTP.BROWSER	pass		
16	13:28:03	10.69.70.222	54.232.239.156	HTTP.BROWSER_Firefox	pass		Firefox
17	13:28:03	10.69.70.222	216.58.222.38	HTTP.BROWSER	pass		
18	13:28:03	10.69.70.222	72.30.2.182	HTTP.BROWSER_Firefox	pass		Firefox
19	13:28:02	10.69.70.222	63.250.200.37	HTTP.BROWSER	pass		
20	13:28:01	10.69.70.222	98.139.225.168	HTTP.BROWSER_Firefox	pass		Firefox
21	13:28:01	10.69.70.222	216.58.222.34	HTTP.BROWSER_Firefox	pass		Firefox
22	13:28:01	10.69.70.222	72.167.239.239	Godaddy	pass		
23	13:28:01	10.69.70.222	206.190.56.190	HTTP.BROWSER	pass		
24	13:28:01	10.69.70.222	216.58.222.38	HTTP.BROWSER	pass		
25	13:28:01	10.69.70.222	98.139.225.168	HTTP.BROWSER_Firefox	pass		Firefox
26	13:28:01	10.69.70.222	54.210.81.50	HTTP.BROWSER	pass		
27	13:28:00	10.69.70.222	23.4.43.27	Root.Certificate.URL	pass		
28	13:28:00	10.69.70.222	199.38.164.54	HTTP.BROWSER	pass		
29	13:28:00	10.69.70.222	54.164.201.243	HTTP.BROWSER_Firefox	pass		Firefox
30	13:28:00	10.69.70.222	200.174.107.10	HTTP.BROWSER_Firefox	pass		Firefox
31	13:28:00	10.69.70.222	200.174.107.10	HTTP.BROWSER_Firefox	pass		Firefox
32	13:28:00	10.69.70.222	54.230.59.57	HTTP.BROWSER_Firefox	pass		Firefox
33	13:28:00	10.69.70.222	23.212.53.164	Facebook	pass		



Router	#	@	Source	Destination	Application Name	Action	Destination Port	Application User
Policy & Objects	1		joaldir (10.69.70.65)	107.22.221.32	BitTorrent	pass	80	
Security Profiles	2		joaldir (10.69.70.65)	54.225.194.96	BitTorrent	pass	80	
VPN	3		joaldir (10.69.70.65)	54.225.194.96	BitTorrent	pass	80	
User & Device	4		joaldir (10.69.70.65)	173.254.195.58	BitTorrent	pass	80	
WiFi & Switch Controller	5		joaldir (10.69.70.65)	177.16.236.45	BitTorrent	pass	17775	
Log & Report	6		joaldir (10.69.70.65)	54.225.194.96	BitTorrent	pass	80	
Traffic Log	7		joaldir (10.69.70.65)	54.225.194.96	BitTorrent	pass	80	
Forward Traffic	8		joaldir (10.69.70.65)	107.20.217.71	BitTorrent	pass	80	
Local Traffic	9		joaldir (10.69.70.65)	52.84.27.118	BitTorrent	pass	80	
Multicast Traffic	10		joaldir (10.69.70.65)	107.20.217.71	BitTorrent	pass	80	
Sniffer Traffic	11		joaldir (10.69.70.65)	187.11.114.84	BitTorrent	pass	51413	
Event Log	12		joaldir (10.69.70.65)	201.43.50.13	BitTorrent	pass	6881	
Security Log	13		joaldir (10.69.70.65)	186.203.232.110	BitTorrent	pass	31438	
Antivirus	14		joaldir (10.69.70.65)	191.242.106.246	BitTorrent	pass	12286	
Web Filter	15		joaldir (10.69.70.65)	201.47.68.114	BitTorrent	pass	13031	
Application Control	16		joaldir (10.69.70.65)	177.148.208.35	BitTorrent	pass	15064	
Intrusion Protection	17		joaldir (10.69.70.65)	177.18.134.190	BitTorrent	pass	8080	
Anomaly	18		joaldir (10.69.70.65)	191.54.61.135	BitTorrent	pass	19200	
Data Leak Prevention	19		joaldir (10.69.70.65)	179.183.79.18	BitTorrent	pass	45682	
Log Config	20		joaldir (10.69.70.65)	177.100.218.117	BitTorrent	pass	38351	
Monitor	21		joaldir (10.69.70.65)	179.209.232.212	BitTorrent	pass	51413	
	22		joaldir (10.69.70.65)	179.154.43.50	BitTorrent	pass	51413	
	23		joaldir (10.69.70.65)	186.203.239.223	BitTorrent	pass	58884	
	24		joaldir (10.69.70.65)	92.244.28.27	BitTorrent	pass	6881	

System	#	Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
Router	171	13:26:22	10.69.70.222	64.233.186.132	Google.Accounts	pass		
Policy & Objects	172	13:26:22	10.69.70.222	64.233.186.132	Google.Accounts	pass		
Security Profiles	173	13:26:22	10.69.70.222	173.194.119.6	HTTPS.BROWSER	pass		
VPN	174	13:26:21	10.69.70.222	173.194.42.137	HTTPS.BROWSER	pass		
User & Device	175	13:26:19	10.69.70.222	173.194.119.1	Google.Hangouts	pass		
WiFi & Switch Controller	176	13:26:19	10.69.70.222	173.194.42.160	HTTPS.BROWSER	pass		
Log & Report	177	13:26:19	10.69.70.222	173.194.42.174	OCSF	pass		
Traffic Log	178	13:26:19	10.69.70.222	64.233.186.132	Google.Accounts	pass		
Forward Traffic	179	13:26:19	10.69.70.222	173.194.118.77	HTTPS.BROWSER	pass		
Local Traffic	180	13:26:19	10.69.70.222	173.194.118.77	HTTPS.BROWSER	pass		
Multicast Traffic	181	13:26:19	10.69.70.222	173.194.42.137	HTTPS.BROWSER	pass		
Sniffer Traffic	182	13:26:19	10.69.70.222	173.194.42.160	HTTPS.BROWSER	pass		
Event Log	183	13:26:18	10.69.70.222	173.194.42.164	Google.Plus	pass		
Security Log	184	13:26:17	10.69.70.222	173.194.119.8	HTTPS.BROWSER	pass		
Antivirus	185	13:26:17	10.69.70.222	173.194.119.14	HTTPS.BROWSER	pass		
Web Filter	186	13:26:16	10.69.70.222	64.233.186.132	Google.Accounts	pass		
Application Control	187	13:26:16	10.69.70.222	64.233.186.132	Google.Accounts	pass		
Intrusion Protection	188	13:26:11	10.69.70.222	216.58.222.35	Google.Accounts	pass		
Anomaly	189	13:26:03	10.69.70.222	173.194.42.174	OCSF	pass		
Data Leak Prevention	190	13:26:03	10.69.70.222	173.194.119.62	HTTPS.BROWSER	pass		
Log Config	191	13:26:02	10.69.70.222	189.55.196.109	HTTPS.BROWSER	pass		
Monitor	192	13:26:02	10.69.70.222	173.194.42.137	HTTP.BROWSER_Firefox	pass		Firefox
	193	13:26:02	10.69.70.222	173.194.118.24	Google.Accounts	pass		

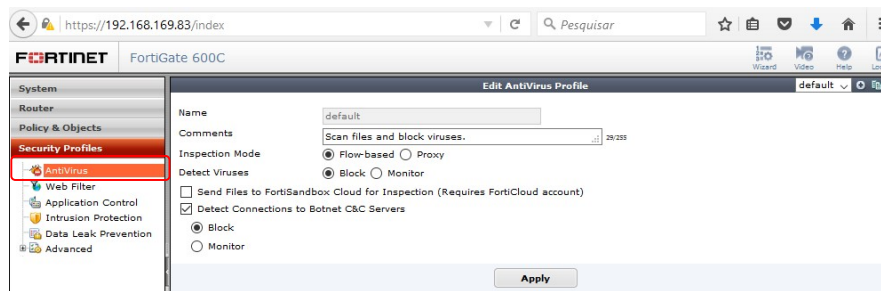
Comentário

Assinatura
do Cliente

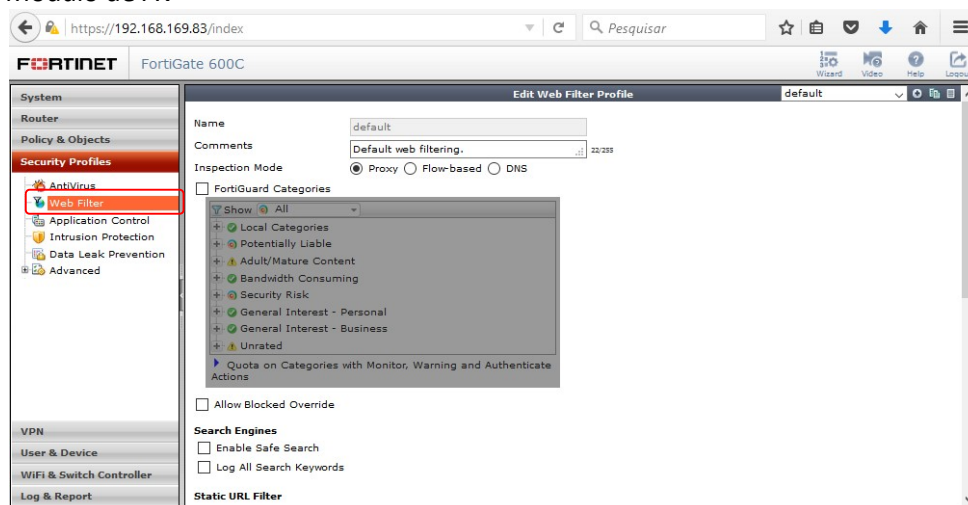
Assinatura NCT

PREVENÇÃO DE AMEAÇAS

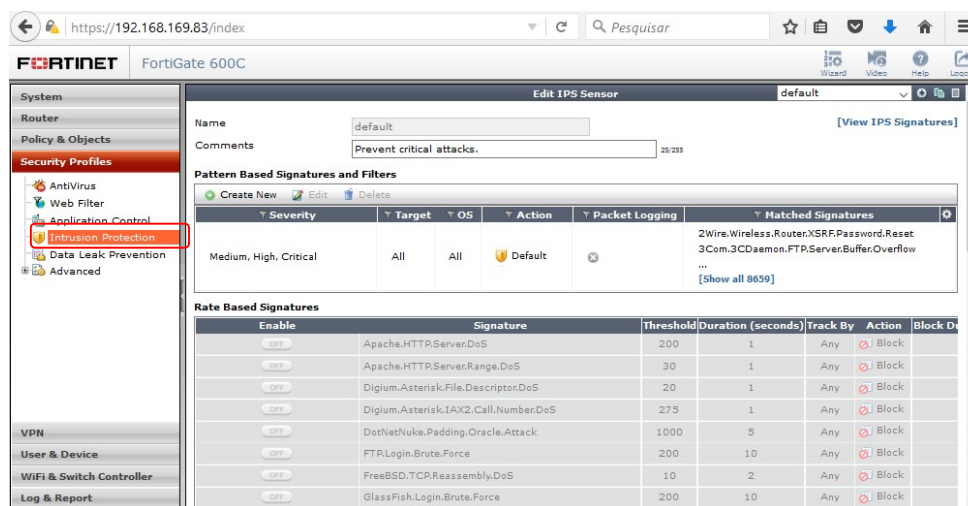
Item de Teste - 1.6.4.1	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulos de IPS, antivírus e anti-spyware integrados no próprio appliance de firewall;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Demonstrar total disponibilidade das funcionalidades solicitadas
Procedimento do Teste	Mostrar os módulos de security profile onde estão disponíveis todos os módulos solicitados.
Evidências	



Módulo de AV



Módulo de web filter



O módulo de anti-spyware esta integrado ao módulo de IPS.

Comentário

Assinatura
do Cliente

Assinatura NCT

Item de Teste -

Quando utilizada as funções de IPS, antivírus e anti spyware, o appliance

1.6.4.5

deve entregar a performance mínima estabelecida no edital entre ter uma única assinatura de IPS ou ter todas as assinaturas de IPS, antivírus e anti spyware habilitadas simultaneamente;

Objetivo do Teste

Demonstrar a funcionalidade conforme solicitado

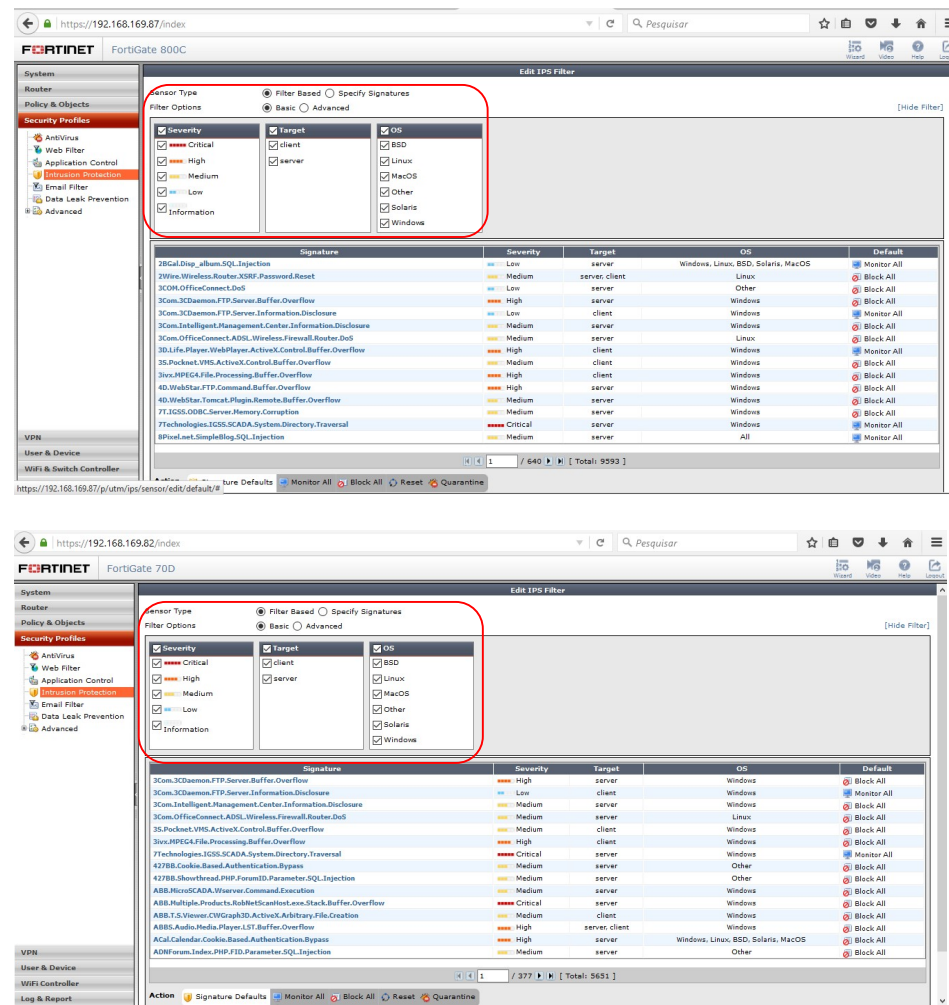
Configuração do Teste

Todos os testes de performance foram realizados com os sensores utilizando todas as assinaturas disponíveis no momento dos testes.

Procedimento do Teste

Marcar todas as assinaturas disponíveis nos equipamentos e testar utilizando o spirent para geração de tráfego.

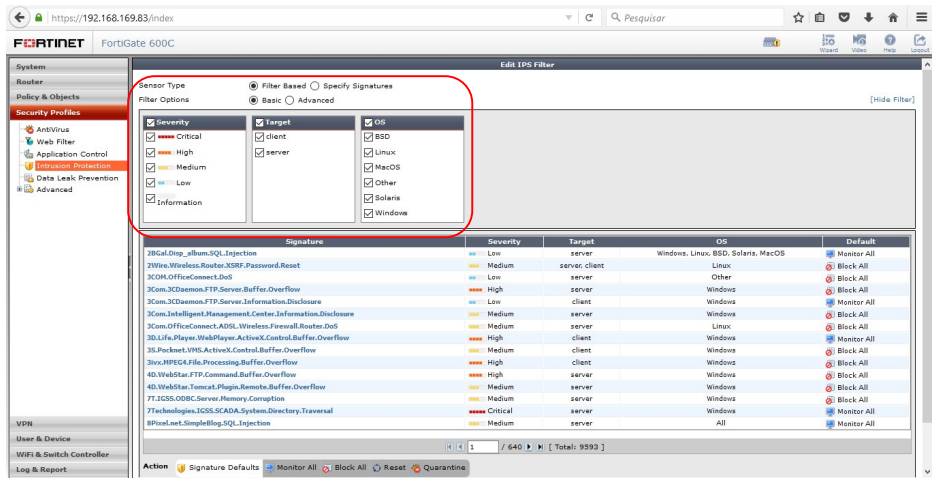
Evidências

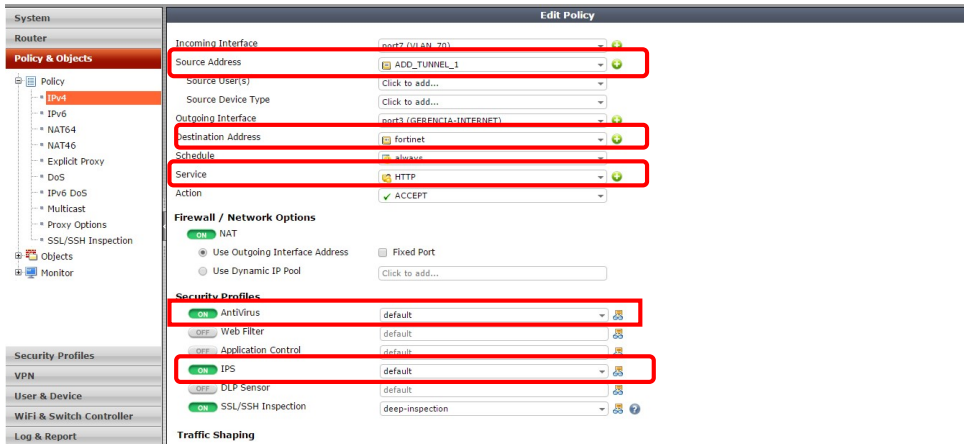


The evidence consists of two screenshots of the FortiGate IPS configuration interface. The top screenshot shows the 'Edit IPS Filter' window for FortiGate 800C, with the 'Severity' tab selected. The bottom screenshot shows the same window for FortiGate 70D, also with the 'Severity' tab selected. Both screenshots show a list of signatures with their severity, target, and OS, and a table of actions (Monitor All, Block All, Reset, Quarantine).

Signature	Severity	Target	OS	Default
3Com.Dmg_album.SQL.Injection	Low	server	Windows, Linux, BSD, Solaris, MacOS	Monitor All
2Wire.Wireless.Router.XSRF.Password.Reset	Medium	server, client	Linux	Block All
3Com.OfficeConnect.DoS	Low	server	Other	Block All
3Com.3Cdaemon.FTP.Server.Buffer.Overflow	High	server	Windows	Block All
3Com.3Cdaemon.FTP.Server.Information.Disclosure	Low	client	Windows	Monitor All
3Com.Intelligent.Management.Center.Information.Disclosure	Medium	server	Windows	Block All
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	Medium	server	Linux	Block All
3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow	High	client	Windows	Monitor All
35.Pocket.VMS.ActiveX.Control.Buffer.Overflow	Medium	client	Windows	Block All
35.NPCC.Fake.Processing.Buffer.Overflow	High	client	Windows	Block All
40.WebStar.FTP.Command.Buffer.Overflow	High	server	Windows	Block All
40.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow	Medium	server	Windows	Block All
71.LOSS.OBRC.Server.Memory.Corruption	Medium	server	Windows	Block All
77.Technologies.IOS.SCADB.System.Directory.Traversal	Critical	server	Windows	Monitor All
8Pwnet.SimpleSQL.SQL.Injection	Medium	server	All	Monitor All

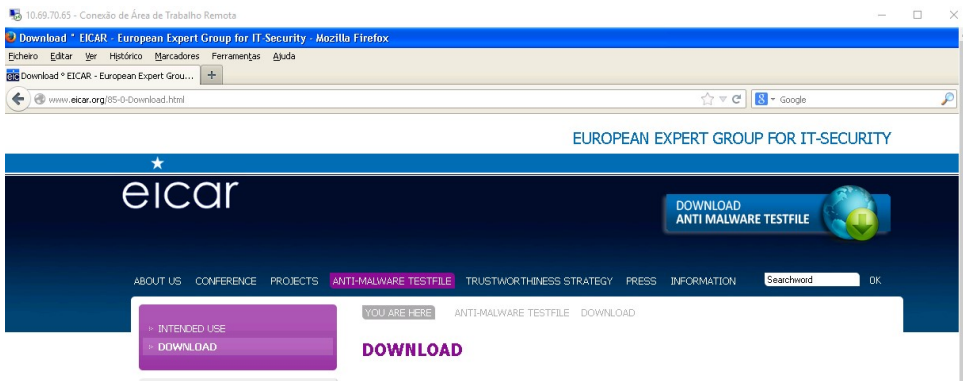
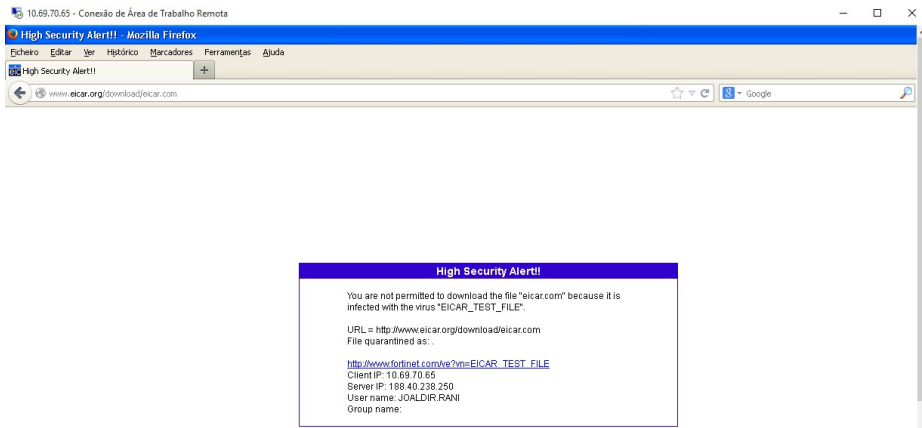
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 43/126

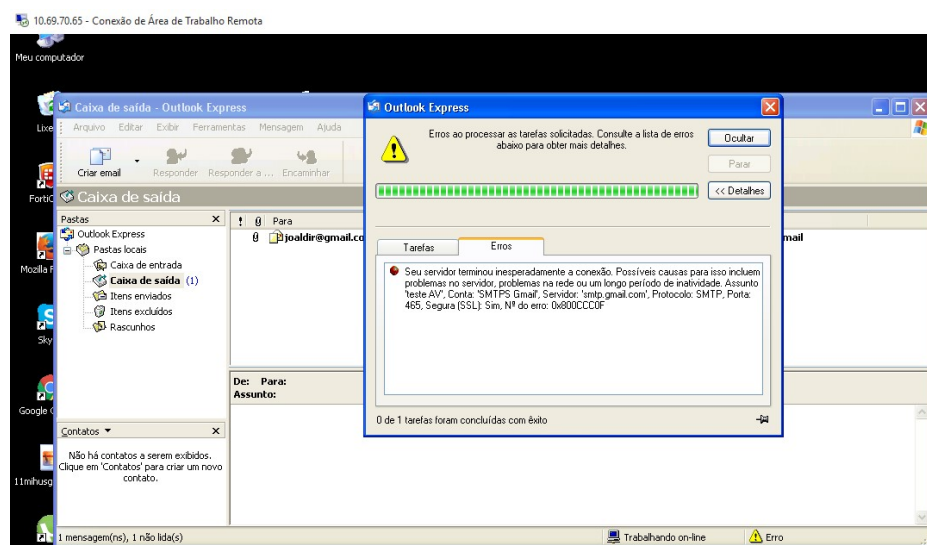
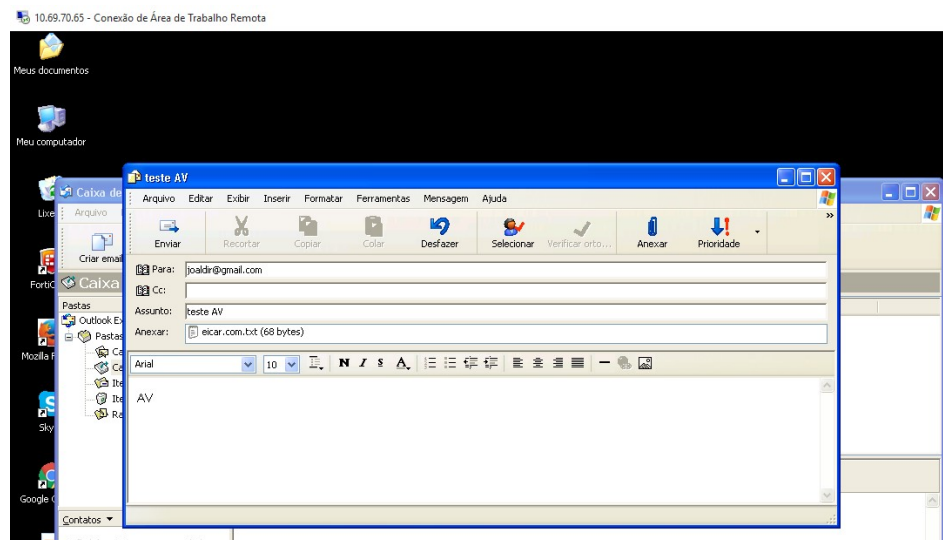
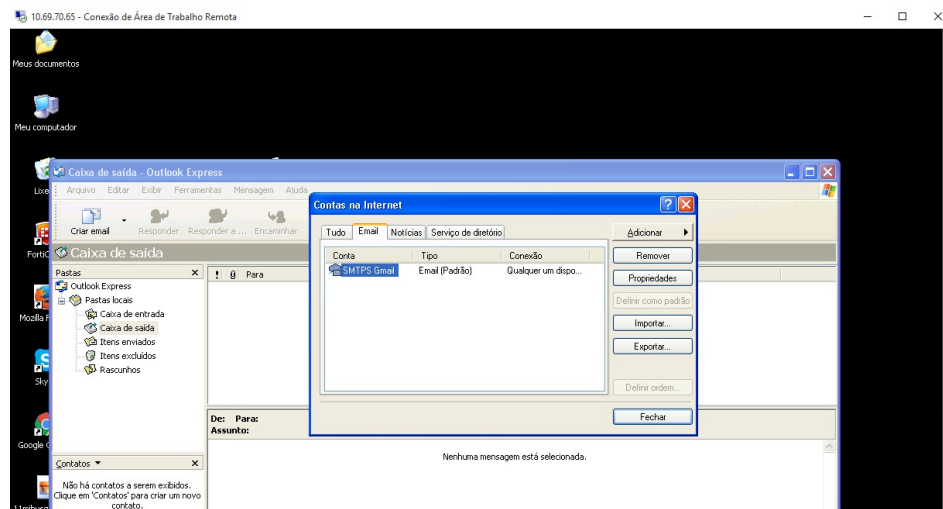
	
Comentário	
Assinatura do Cliente	Assinatura NCT

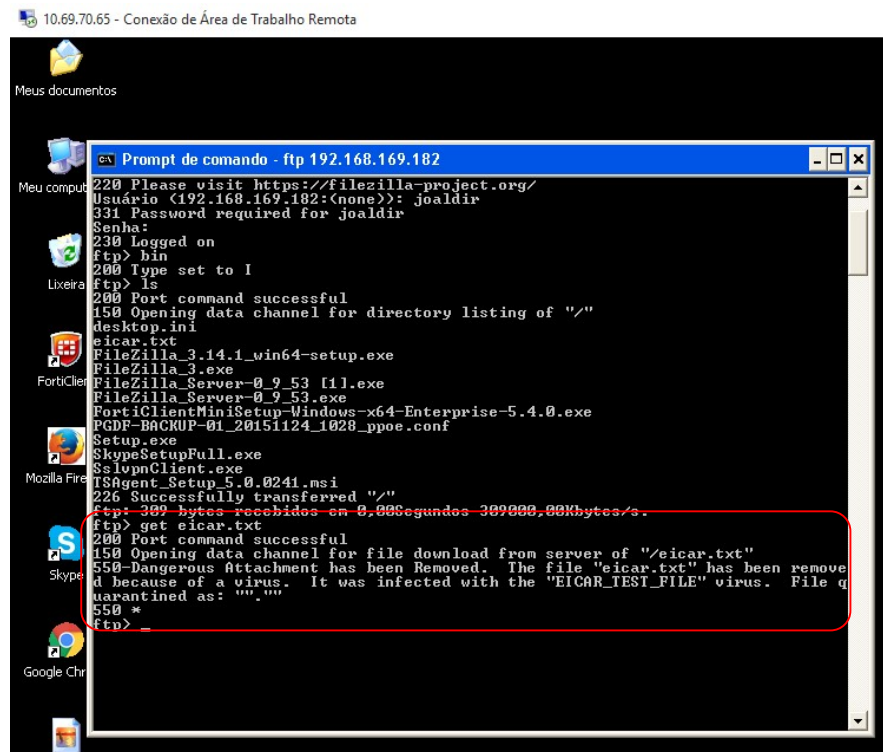
Item de Teste - 1.6.4.8	Deve suportar granularidade nas políticas de IPS, antivírus e anti spyware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar uma política especificando as combinações solicitadas habilitando os perfis de segurança como IPS e Anti-Virus .
Procedimento do Teste	Criado regras especificando perfis de segurança de IPS, e Antivirus/Spyware, especificando perfis de segurança combiandos todos para se obter diferentes instancias de controle de politicas.
Evidências	Regra contendo a combinação de endereço de origem,endereço de destino, serviço e perfil de segurança de Antivirus/spyware e IPS: 
Comentário	O modulo de AntiSpyware correspondente ao mecanismo de Antivirus que já

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 44/126

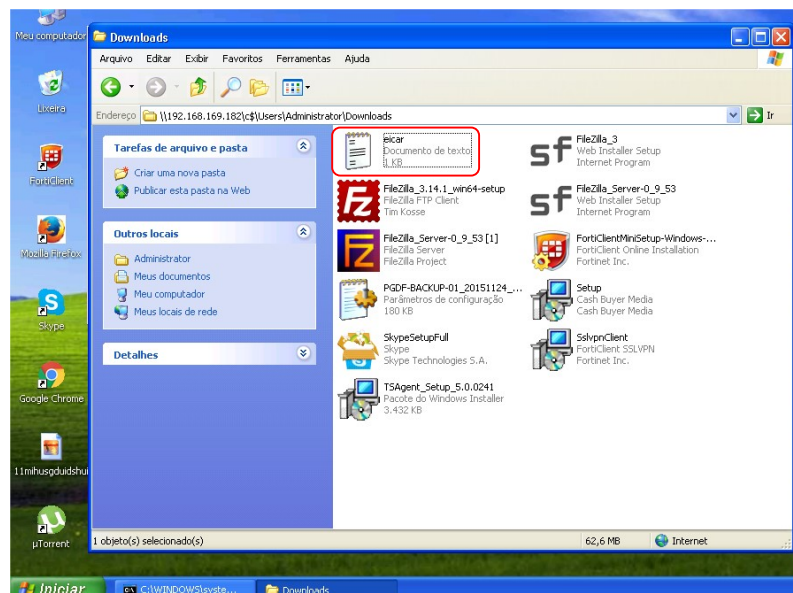
	vem com esta habilidade.		
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.4.18	Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar profiles de Anti-virus selecionado os protocolos mencionado
Procedimento do Teste	Simular trafego dos protocolos mencionado para efetivação dos scans.
Evidências	- HTTP   - SMTP

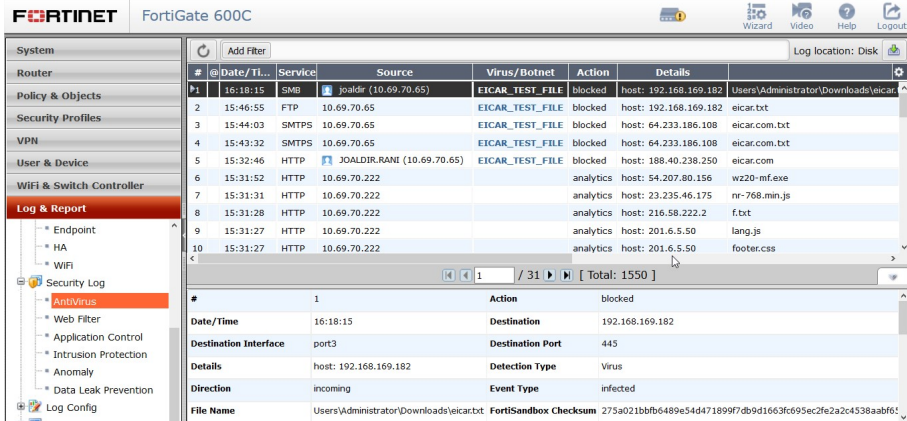


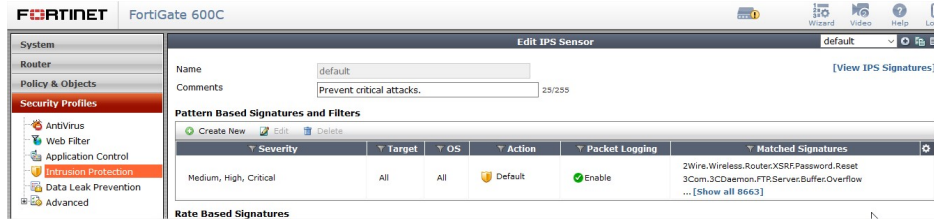
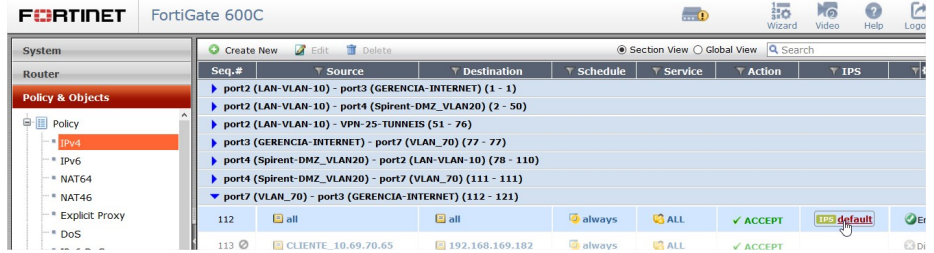


-SMB

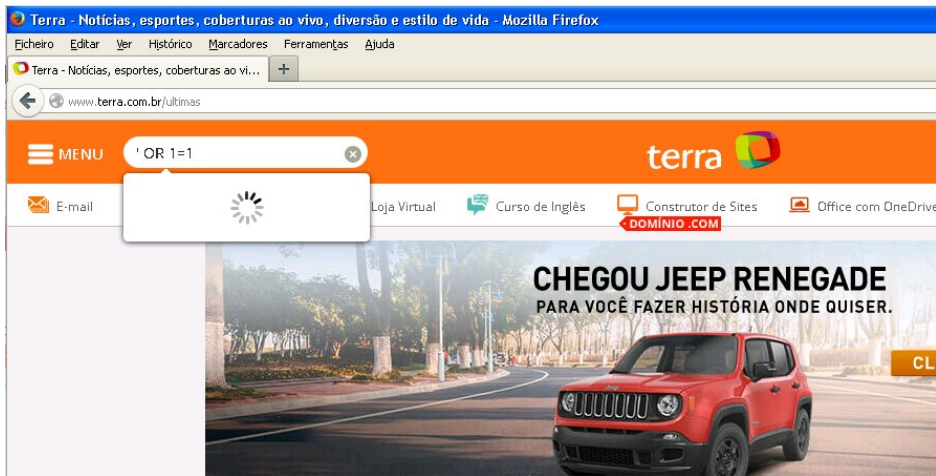
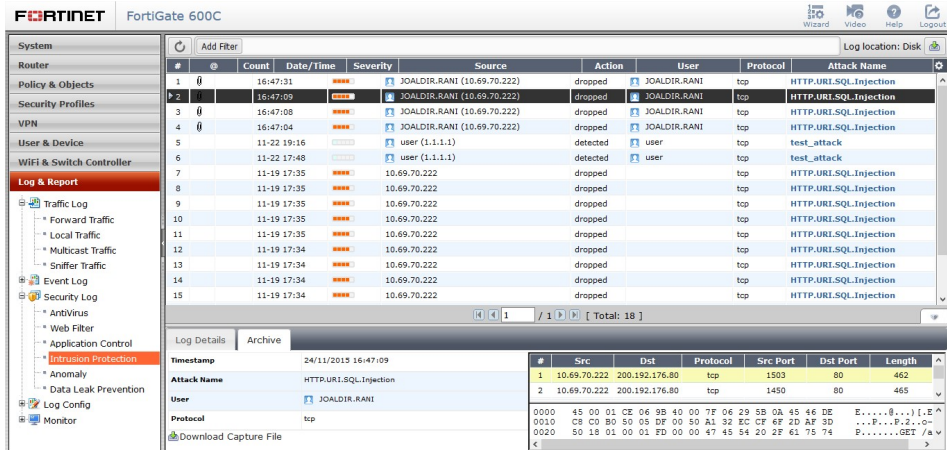


	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 47/126

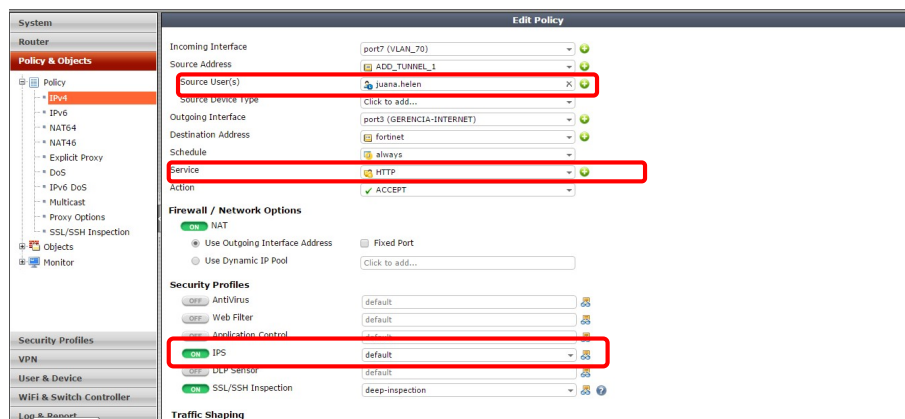
		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.4.23.1	O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Editado o sensor de IPS "default" para capturar os pacotes e bloquear os ataques. Configurado uma regra de firewall e atribuído o sensor. Utilizado windows xp para gerar o ataque.
Procedimento do Teste	A partir do windows xp foi gerado um ataque de sql injection no site do terra com a syntax ' OR 1=1. Foi demonstrado log com as informações e a captura do pacote do ataque.
Evidências	 Sensor IPS  Regra de Firewall

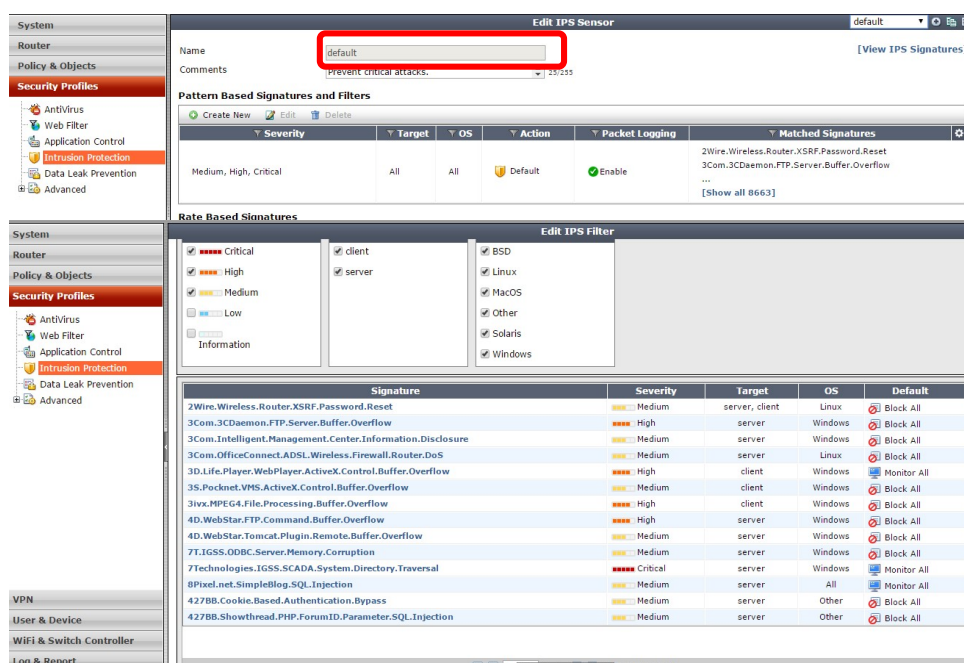
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 48/126

			Browser do atacante
			Informações de captura
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.4.31	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques, baseando-se em políticas de firewall que considere usuários, grupos de usuários, origem e destino;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar políticas de firewall diversas considerando as ponderações citadas no item, associando as profiles de segurança de IPS.
Procedimento do Teste	Configurado uma regra especificando uma restrição de usuário de origem e um destino específico com um perfil de IPS default:

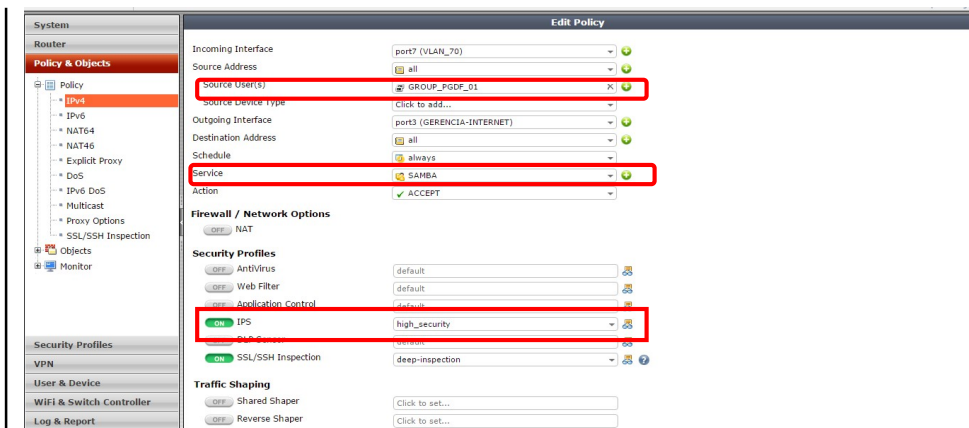


Configuração de perfil default que foi habilitado na regra acima :



Politica com especificação de grupos de usuários de origem, e específico endereço de destino e outro perfil de segurança de IPS:

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 50/126



Configuração de perfil default que foi habilitado na regra acima :

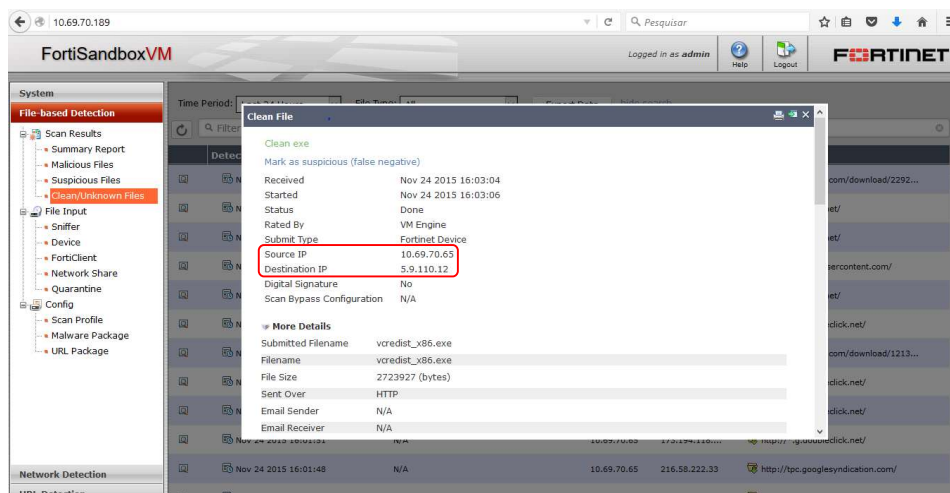


Evidências	
Comentário	
Assinatura do Cliente	Assinatura NCT

Análise de malwares modernos - Sandbox

Item de Teste - 1.6.5.8	O sistema de análise "in cloud" ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar ou propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de antivírus e anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede);
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Acessar o FortiSandbox VM para ter acesso as informações conforme solicitado
Procedimento	

do Teste



FortiSandboxVM

System

File-based Detection

Time Period: Nov 24 2015 16:03:04

Clean File

Mark as suspicious (false negative)

Received: Nov 24 2015 16:03:04

Started: Nov 24 2015 16:03:06

Status: Done

Rated By: VM Engine

Submit Type: Fortinet Device

Source IP: 10.69.70.65

Destination IP: 5.9.110.12

Digital Signature: No

Scan Bypass Configuration: N/A

More Details

Submitted Filename: vcredist_x86.exe

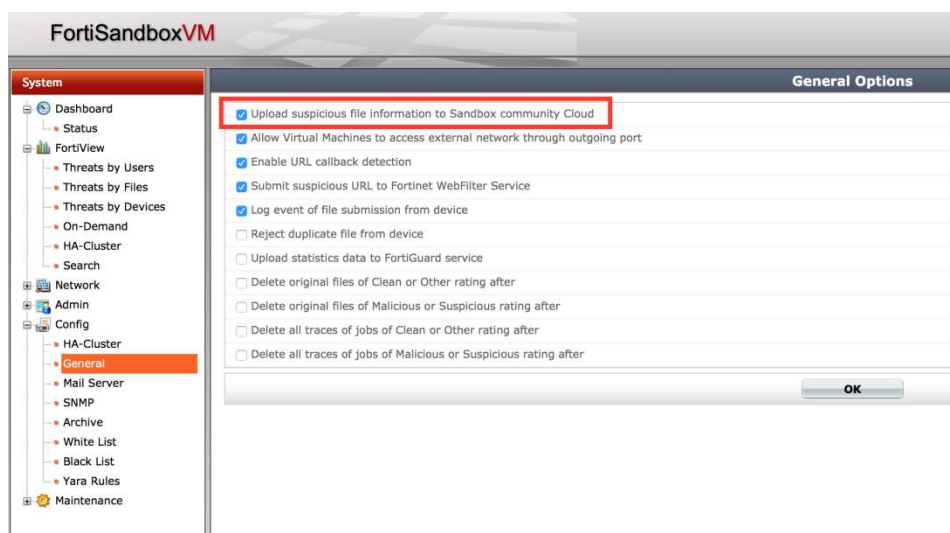
Filename: vcredist_x86.exe

File Size: 2723927 (bytes)

Sent Over: HTTP

Email Sender: N/A

Email Receiver: N/A



FortiSandboxVM

System

General Options

☒ Upload suspicious file information to Sandbox community Cloud

☒ Allow Virtual Machines to access external network through outgoing port

☒ Enable URL callback detection

☒ Submit suspicious URL to Fortinet WebFilter Service

☒ Log event of file submission from device

☐ Reject duplicate file from device

☐ Upload statistics data to FortiGuard service

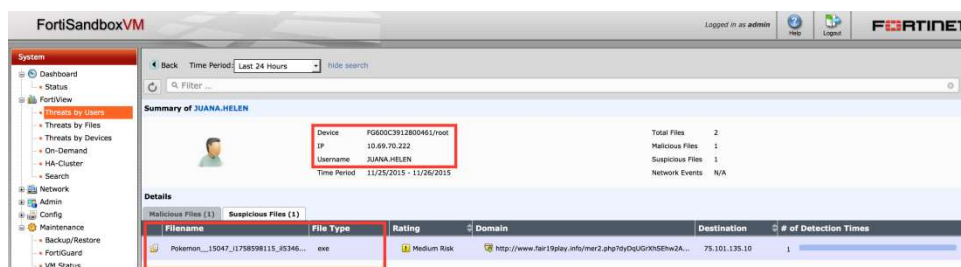
☐ Delete original files of Clean or Other rating after

☐ Delete original files of Malicious or Suspicious rating after

☐ Delete all traces of jobs of Clean or Other rating after

☐ Delete all traces of jobs of Malicious or Suspicious rating after

OK



FortiSandboxVM

System

Summary of JUANA HELEN

Device: FG600C3912800461

IP: 10.69.70.222

Username: JUANA HELEN

Time Period: 11/25/2015 - 11/26/2015

Total Files: 2

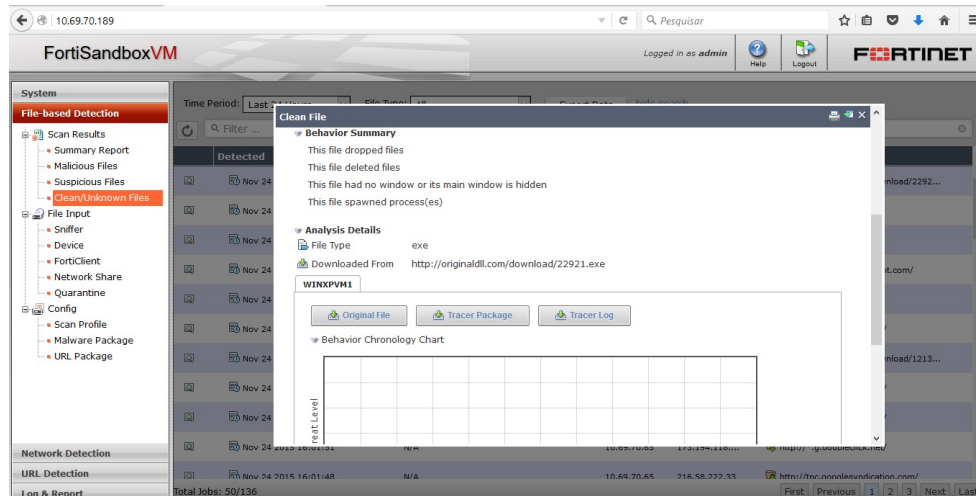
Malicious Files: 1

Suspicious Files: 1

Network Events: N/A

Details

Filename	File Type	Rating	Domain	Destination	# of Detection Times
Pokemon_15047_1758598115_95346..._exe	exe	Medium Risk	http://www.far19play.info/mr2.php?yDpJGrXN5thw24...	75.101.135.10	1



FortiSandboxVM

System: File-based Detection

Time Period: Last 24 hours

Clean File

Behavior Summary

- This file dropped files
- This file deleted files
- This file had no window or its main window is hidden
- This file spawned process(es)

Analysis Details

File Type: exe

Downloaded From: http://originaldll.com/download/22921.exe

WINXPVPM1

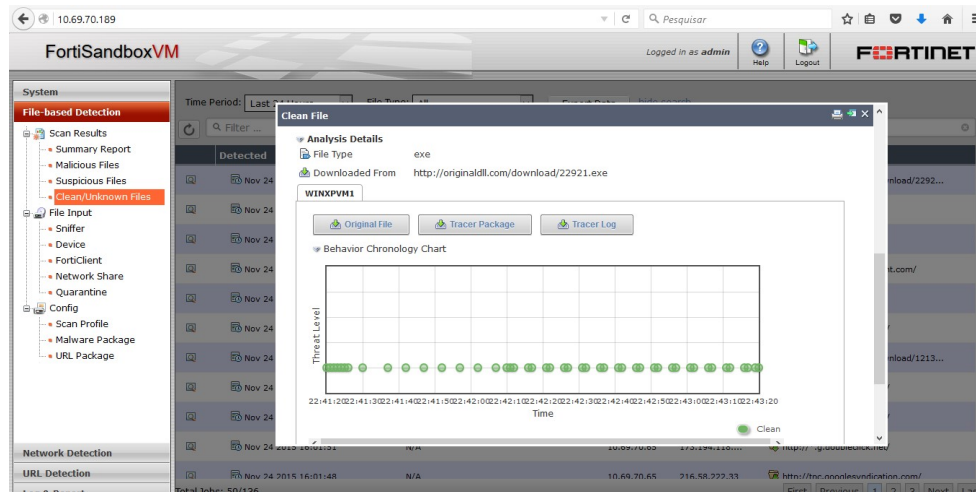
Original File | Tracer Package | Tracer Log

Behavior Chronology Chart

Threat Level

Time

Total Jobs: 50/136



FortiSandboxVM

System: File-based Detection

Time Period: Last 24 hours

Clean File

Analysis Details

File Type: exe

Downloaded From: http://originaldll.com/download/22921.exe

WINXPVPM1

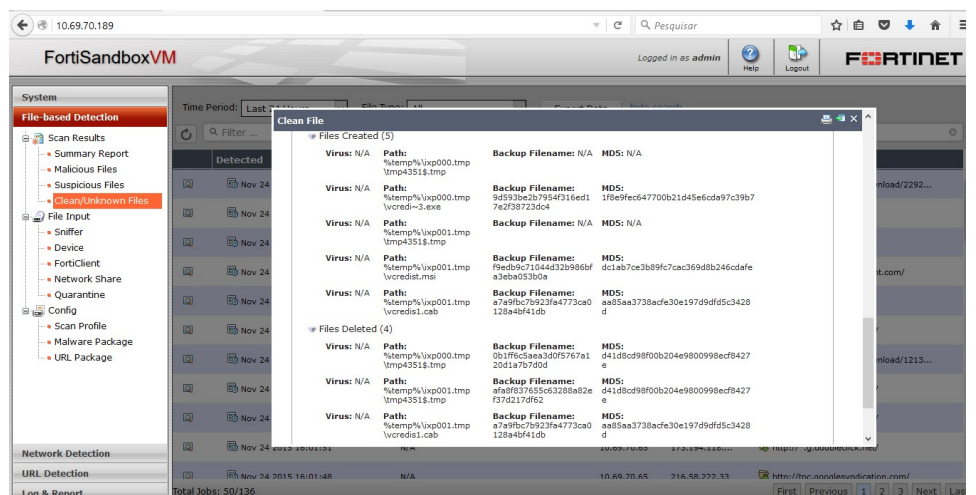
Original File | Tracer Package | Tracer Log

Behavior Chronology Chart

Threat Level

Time

Total Jobs: 50/136



FortiSandboxVM

System: File-based Detection

Time Period: Last 24 hours

Clean File

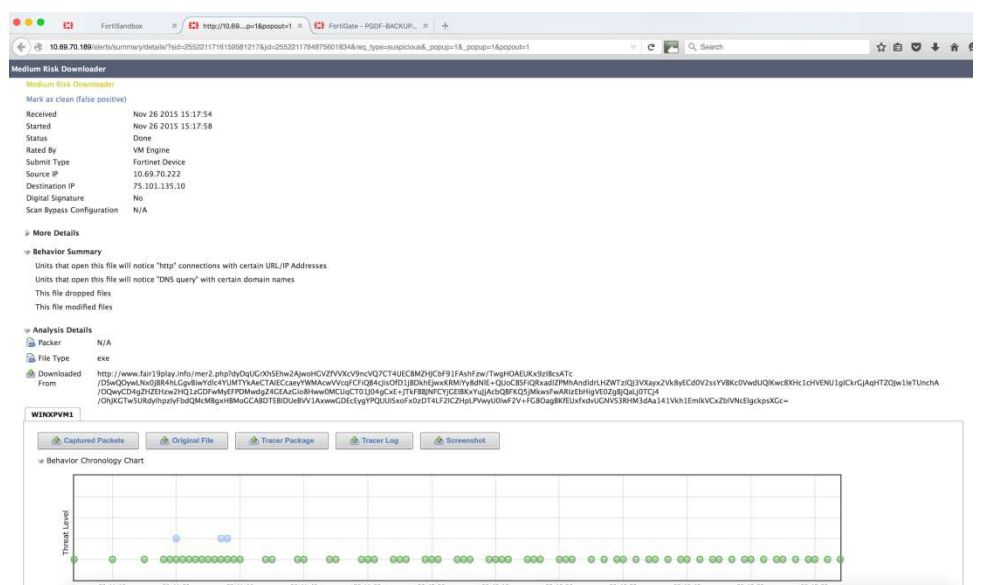
Files Created (5)

Virus	Path	Backup Filename	MD5
N/A	%temp%\ixp000.tmp	N/A	N/A
N/A	%temp%\ixp000.tmp	N/A	N/A
N/A	%temp%\ixp000.tmp	N/A	N/A
N/A	%temp%\ixp001.tmp	N/A	N/A
N/A	%temp%\ixp001.tmp	N/A	N/A

Files Deleted (4)

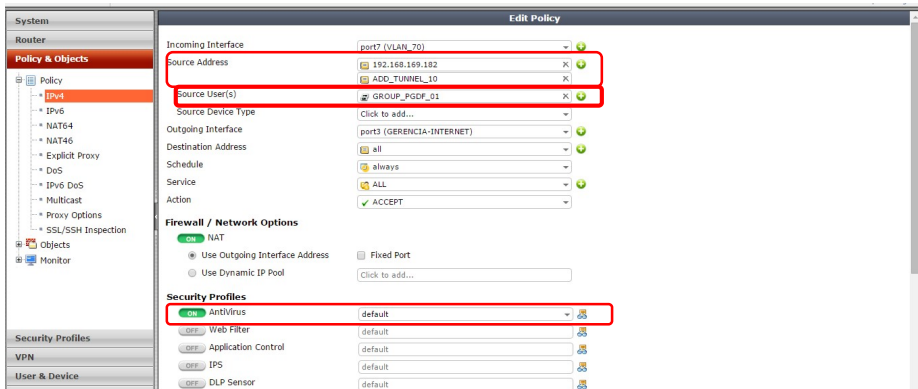
Virus	Path	Backup Filename	MD5
N/A	%temp%\ixp000.tmp	N/A	N/A
N/A	%temp%\ixp001.tmp	N/A	N/A
N/A	%temp%\ixp001.tmp	N/A	N/A
N/A	%temp%\ixp001.tmp	N/A	N/A

Total Jobs: 50/136

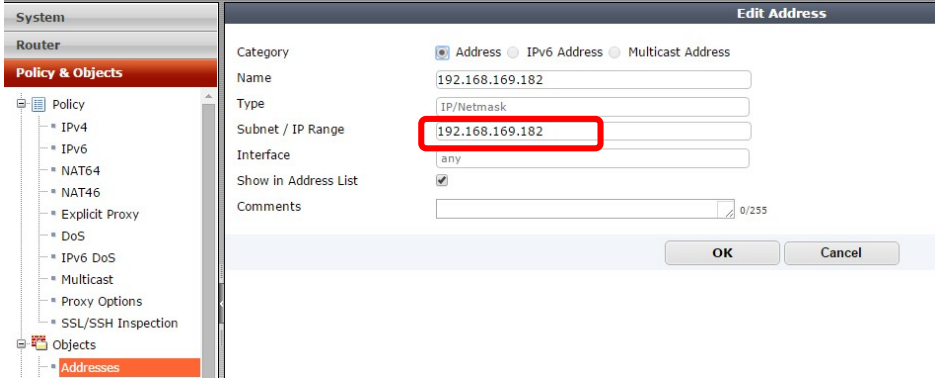
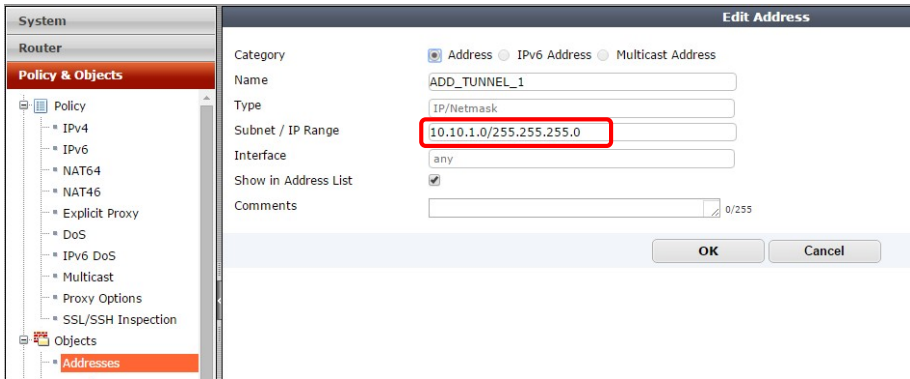


	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 54/126

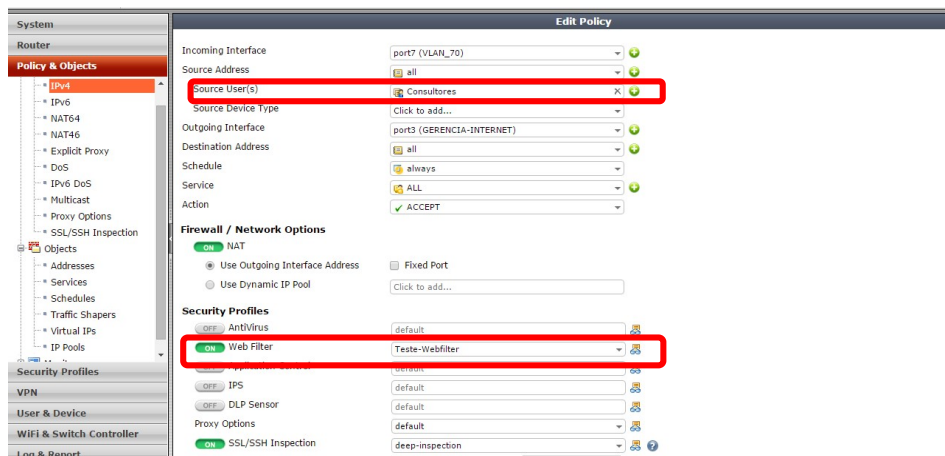
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.6.1.2	Deve ser possível a criação de políticas por usuários, grupos de usuários, IP e redes;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar uma política de firewall especificando os filtros conforme solicitado
Procedimento do Teste	Executar a criação destas politicas conforme solicitado
Evidências	Regra de firewall especificando um grupo de usuários específicos assim como endereços de origem por IP por uma rede com um perfil de segurança de filtro de antivírus :  Grupo de usuário:  Endreços por IP:

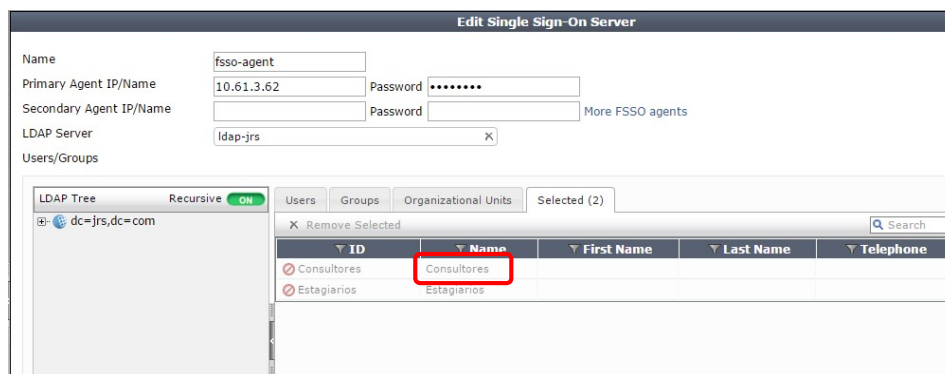
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 55/126

	
Endereço Rede:	
	
Comentário	
Assinatura do Cliente	Assinatura NCT

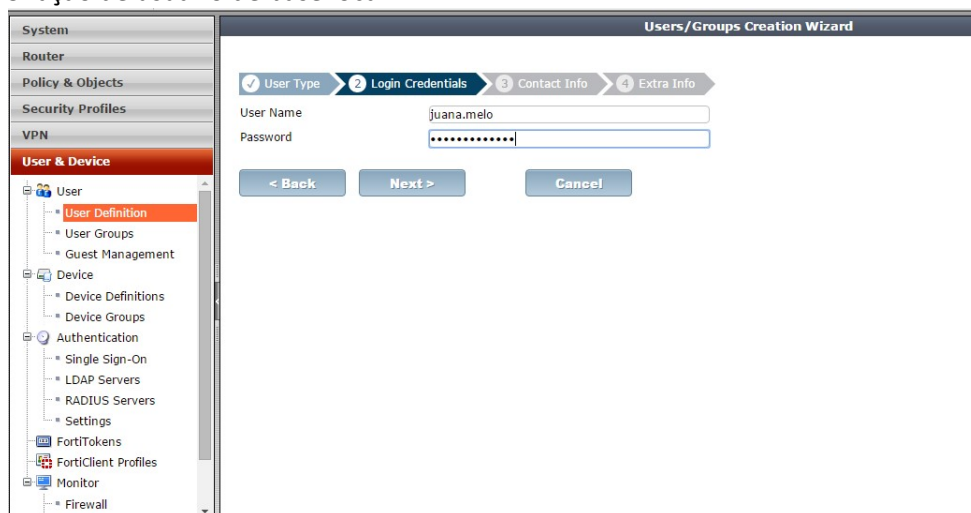
Item de Teste - 1.6.6.1.3	Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-Directory e base de dados local;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurado uma política de firewall selecionando controle de acesso por usuários e grupos através dos serviços de integrações com o Active directory e apontando a capacidade de configuração dos demais métodos.
Procedimento do Teste	Feito um acesso de autenticação do usuário o qual fez match na política de firewall contendo o grupo , e validar nos logs o perfil de web filter acessado por este usuário
Evidências	Configurado a regra de firewall com especificação selecionando um grupo de integração com o AD para que o acesso do mesmos seja autenticado, e habilitando um perfil de segurança de filtro de conteúdo:



Grupo de acesso do usuário foi feito com a integração com o AD fazendo uma consulta LDAP que também é compatível com e-directory:



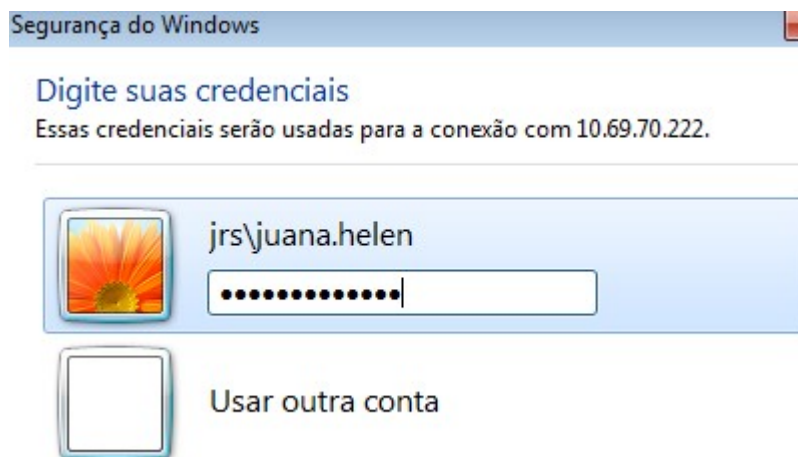
Criação de usuário de base local:



O cliente que acessou no PC RDP 10.69.70.222, autenticou com seu usuário da

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 57/126

rede:



Na tela de monitor do firewall ja foi possível detectar o evento de autenticação do usuário que faz parte do perfil consultores:

JUANA.HELEN	juana.helen, Consultores	0 day(s) 0 hour(s) 0 minute(s)	10.69.70.222	4.44 MB	FSSO
-------------	--------------------------	--------------------------------	--------------	---------	------

Log de acesso web do usuário autenticado o match no perfil Teste-Webfilter :

System	#	Date/Time	User	Source	Action	URL	Category	Description
Router	1	17:21:56	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	tr2.terra.com/broadcast/sub/ch=live.geral.pt-BR.livebar&m[...]/...	Search Engines and Portals	
Policy & Objects	2	17:21:52	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	br06.zopim.com/s/W/ws/sIPTMH0xG2eC3f/c/144856571750	Information Technology	
Security Profiles	3	17:21:52	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	gg.google.com/csi/v=2&s=youtube&action=watch&watch7ads&_sts=ne...	Search Engines and Portals	
VPN	4	17:21:52	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	www.youtube-nocookie.com/gen_2047attributionpartner=SonyBMG	Streaming Media and Down	
User & Device	5	17:21:43	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	beacon.rubiconproject.com/beacon/p/rt/valuation?8p=rubicon&pc=...	Information Technology	
WiFi & Switch Controller	6	17:21:43	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	beacon.rubiconproject.com/beacon/p/rt/valuation?8p=rubicon&pc=...	Information Technology	
Log & Report	7	17:21:42	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	beacon.rubiconproject.com/beacon/p/rt/valuation?8p=rubicon&pc=...	Information Technology	
Traffic Log	8	17:21:40	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	p.mtck.com/an?w=2&cb=0.47858164309084417	Advertising	
Forward Traffic	9	17:21:40	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	rtax.criteo.com/delivery/rtax.js?netId=24208&cookieName=crtg_...	Business	
Local Traffic	10	17:21:25	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	tr2.terra.com/broadcast/sub/ch=live.geral.pt-BR.livebar&m[...]/...	Search Engines and Portals	
Multicast Traffic	11	17:21:12	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	beacon.rubiconproject.com/beacon/p/rt/valuation?8p=rubicon&pc=...	Information Technology	
Sniffer Traffic	12	17:21:12	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	beacon.rubiconproject.com/beacon/p/rt/valuation?8p=rubicon&pc=...	Information Technology	
Event Log	13	17:21:12	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	beacon.rubiconproject.com/beacon/p/rt/valuation?8p=rubicon&pc=...	Information Technology	
Security Log	14	17:21:10	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	p.mtck.com/an?w=2&cb=0.6013573294559369	Advertising	
Antivirus	15	17:21:10	JUANA.HELEN	JUANA.HELEN (10.69.70.222)	passthrough	rtax.criteo.com/delivery/rtax.js?netId=24208&cookieName=crtg_...	Business	

Message	URL belongs to an allowed category in policy	Method	domain
Profile Name	Teste-Webfilter	Protocol	6
Received Bytes	506	Request Type	direct
Sent Bytes	436	Sequence Number	2170810
Service	HTTP	Source	JUANA.HELEN (10.69.70.222)
Source Interface	port7	Source Port	7002

Comentário

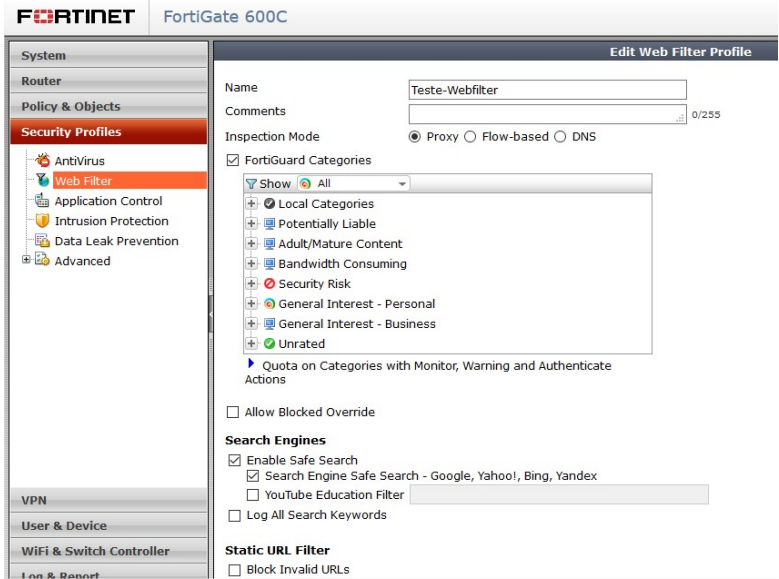
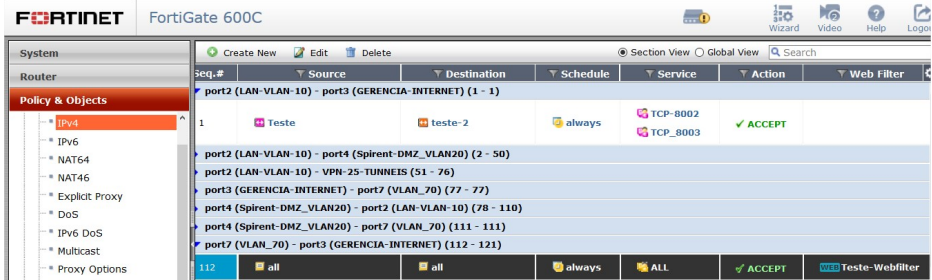
Assinatura do Cliente

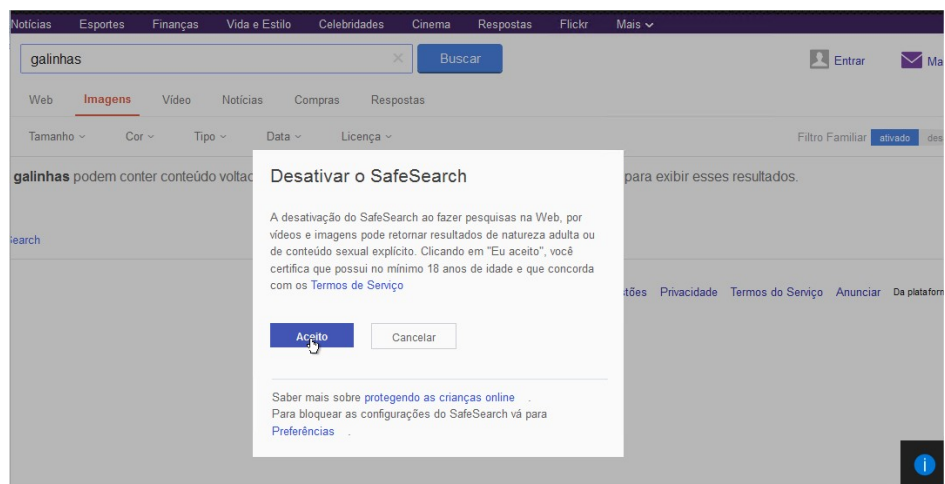
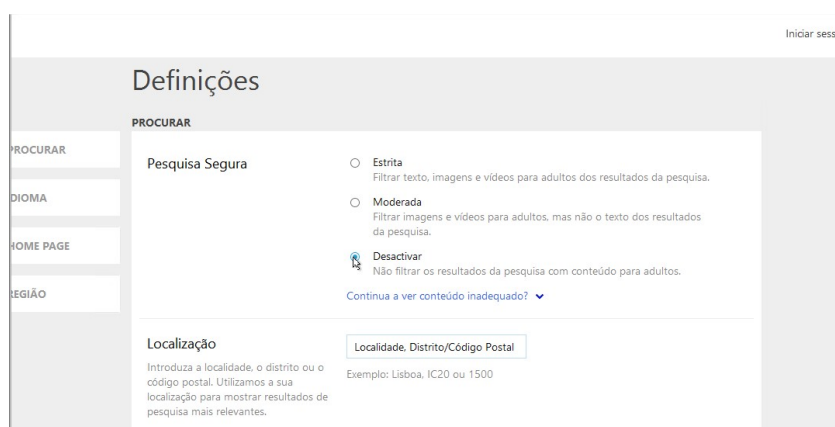
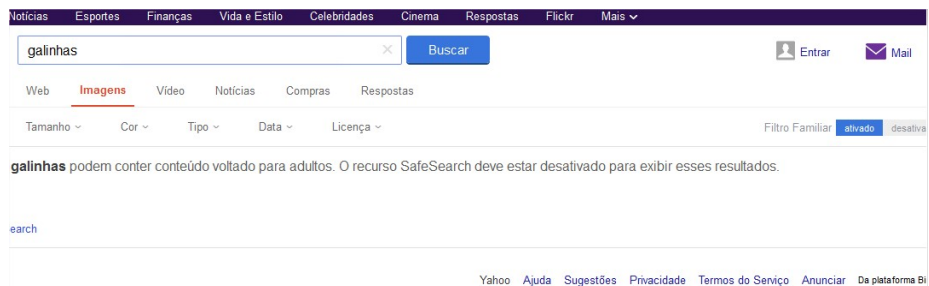
Assinatura NCT

Item de Teste - 1.6.6.1.6

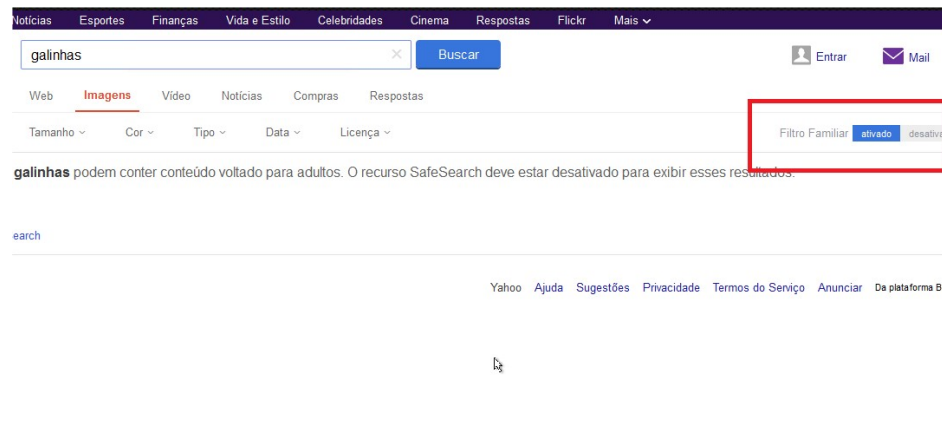
Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 58/126

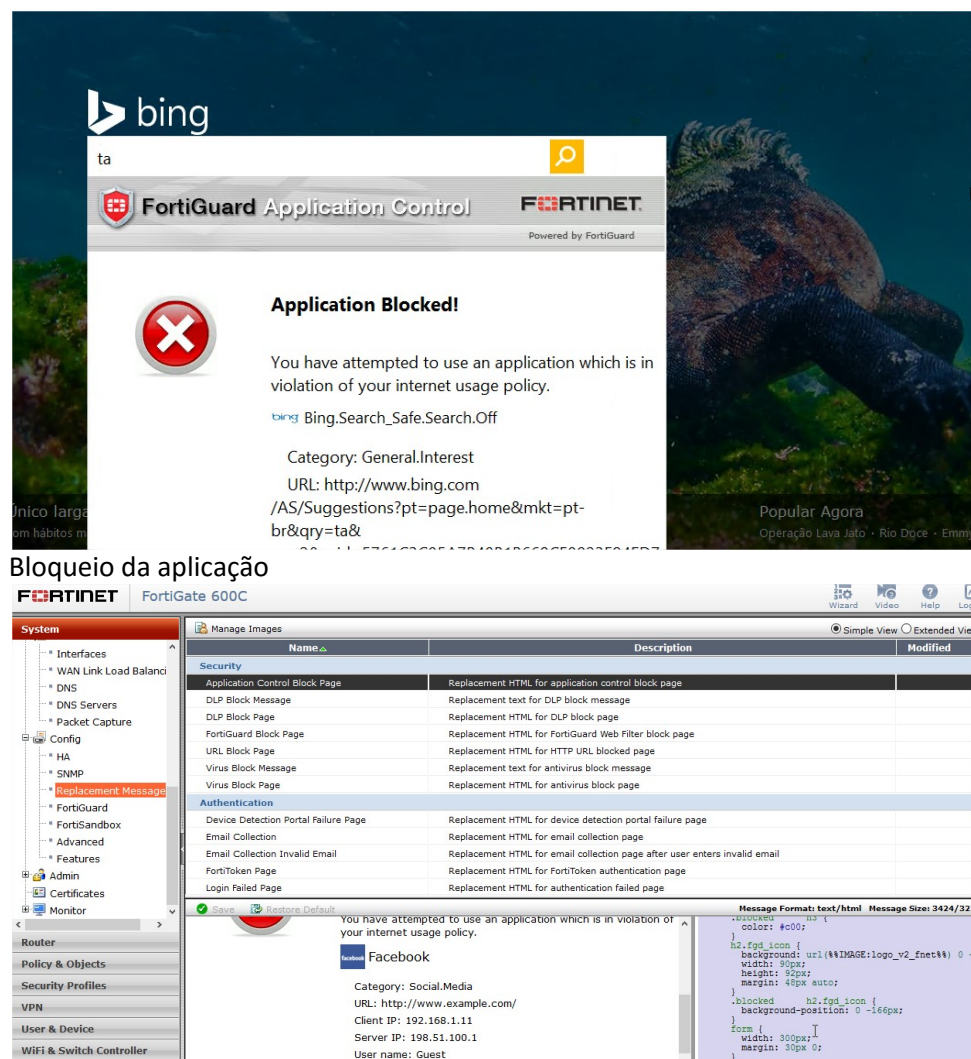
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurado um perfil de filtro de conteúdo Teste-WebFilter com a funcionalidade Enable Safe Search e Search Engine Search. Configurado uma regra e atribuído o perfil web. Criado um perfil de filtro de aplicação para bloqueio de browser caso estiver com o safe search desativado.
Procedimento do Teste	A partir de um browser foi acessado o site de busca do yahoo, nas configurações da pagina modificado a opção para desativar o safe search, ao tentar acesso ao site o fortigate forçava a utilização do safe search não deixando desativar da função. A partir de um browser foi acessado o site de busca Bing, nas configurações da pagina modificado a opção para desativar o safe search, ao tentar acesso ao site o fortigate bloqueia a aplicação mostra pagina de bloqueio. Demonstrado a possibilidade de bloqueio através do filtro de conteúdo bem como a customização de pagina de bloqueio.
Evidências	 Perfil filtro de conteúdo  Regra de firewall com o perfil



Tentativa de desativar o safe search



Falha na tentativa de desabilitar o safe search



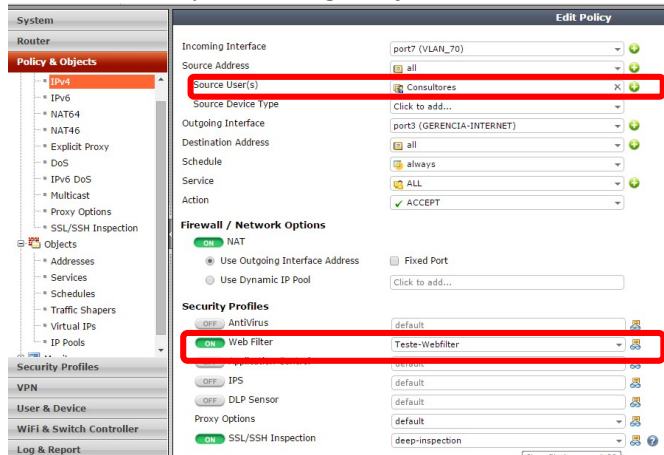
Customização de pagina de bloqueio.

Comentário

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 61/126

Assinatura do Cliente	Assinatura NCT	
--------------------------	----------------	--

Identificação de usuários

Item de Teste - 1.6.7.1	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-Directory e base de dados local;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurado uma política de firewall selecionando controle de acesso por usuários e grupos através dos serviços de integrações com o Active directory e apontando a capacidade de configuração dos demais métodos.
Procedimento do Teste	Feito um acesso de autenticação do usuário o qual fez match na política de firewall contendo o grupo , e validar nos logs o perfil de web filter acessado por este usuário
Evidências	Configurado a regra de firewall com especificação selecionando um grupo de integração com o AD para que o acesso do mesmos seja autenticado, e habilitando um perfil de segurança de filtro de conteúdo:  Grupo de acesso do usuário foi feito com a integração com o AD fazendo uma consulta LDAP que também é compatível com e-directory:

Edit Single Sign-On Server

Name: fssso-agent
 Primary Agent IP/Name: 10.61.3.62 Password: *****
 Secondary Agent IP/Name: Password: More FSSO agents
 LDAP Server: ldap-jrs
 Users/Groups

LDAP Tree Recursive **ON**

dc=jrs,dc=com

Users Groups Organizational Units Selected (2)

X Remove Selected

ID	Name	First Name	Last Name	Telephone
Consultores	Consultores			
Estagiarios	Estagiarios			

Criação de usuário de base local:

Users/Groups Creation Wizard

System Router Policy & Objects Security Profiles VPN **User & Device**

User User Definition User Groups Guest Management Device Device Definitions Device Groups Authentication Single Sign-On LDAP Servers RADIUS Servers Settings FortiTokens FortiClient Profiles Monitor Firewall

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

User Name: juana.melo
 Password: *****

< Back Next > Cancel

O cliente que acessou no PC RDP 10.69.70.222, autenticou com seu usuário da rede:

Segurança do Windows

Digite suas credenciais
 Essas credenciais serão usadas para a conexão com 10.69.70.222.

jrs\juana.helen
 Password: *****

Usar outra conta

Na tela de monitor do firewall ja foi possível detectar o evento de autenticação

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 63/126

do usuário que faz parte do perfil consultores:

JUANA.HELEN	Juana.helen, Consultores	0 day(s) 0 hour(s) 0 minute(s)	10.69.70.222	4.44 MB	FS50
-------------	--------------------------	--------------------------------	--------------	---------	------

Log de acesso web do usuário autenticado o match no perfil Teste-Webfilter :

System	#	Date/Time	User	Source	Action	URL	Category	Description
Router	1	17:21:56	JUANA.HELEN	10.69.70.222	passthrough	tr2.terra.com/broadcast/sub/ch=live.geral.pt-BR.livebar&m[...]	Search Engines and Portals	
Policy & Objects	2	17:21:52	JUANA.HELEN	10.69.70.222	passthrough	br06.zopim.com/s/W/ws/a1P7RH0xG2eC3/c/1440565571750	Information Technology	
Security Profiles	3	17:21:52	JUANA.HELEN	10.69.70.222	passthrough	gg.google.com/csi?v=2&s=youtube&action=watch&watch7ads=ne...	Search Engines and Portals	
VPN	4	17:21:52	JUANA.HELEN	10.69.70.222	passthrough	www.youtube-nocookie.com/gen_204?attributionpartner=SonyBMG	Streaming Media and Down	
User & Device	5	17:21:43	JUANA.HELEN	10.69.70.222	passthrough	beacon.rubiconproject.com/beacon/p/tp/valuation78p=rubicon&pc=...	Information Technology	
WiFi & Switch Controller	6	17:21:43	JUANA.HELEN	10.69.70.222	passthrough	beacon.rubiconproject.com/beacon/p/tp/valuation78p=rubicon&pc=...	Information Technology	
Log & Report	7	17:21:42	JUANA.HELEN	10.69.70.222	passthrough	beacon.rubiconproject.com/beacon/p/tp/valuation78p=rubicon&pc=...	Information Technology	
Traffic Log	8	17:21:40	JUANA.HELEN	10.69.70.222	passthrough	p.mxtck.com/an?a=2&cb=0.47658164309084417	Advertising	
Forward Traffic	9	17:21:40	JUANA.HELEN	10.69.70.222	passthrough	rtax.criteo.com/delivery/rtax.js?netId=24208&cookieName=crtg...	Business	
Local Traffic	10	17:21:25	JUANA.HELEN	10.69.70.222	passthrough	tr2.terra.com/broadcast/sub/ch=live.geral.pt-BR.livebar&m[...]	Search Engines and Portals	
Multicast Traffic	11	17:21:12	JUANA.HELEN	10.69.70.222	passthrough	beacon.rubiconproject.com/beacon/p/tp/valuation78p=rubicon&pc=...	Information Technology	
Sniffer Traffic	12	17:21:12	JUANA.HELEN	10.69.70.222	passthrough	beacon.rubiconproject.com/beacon/p/tp/valuation78p=rubicon&pc=...	Information Technology	
Event Log	13	17:21:12	JUANA.HELEN	10.69.70.222	passthrough	beacon.rubiconproject.com/beacon/p/tp/valuation78p=rubicon&pc=...	Information Technology	
Security Log	14	17:21:10	JUANA.HELEN	10.69.70.222	passthrough	p.mxtck.com/an?a=2&cb=0.6013573294559369	Advertising	
Antivirus	15	17:21:10	JUANA.HELEN	10.69.70.222	passthrough	rtax.criteo.com/delivery/rtax.js?netId=24208&cookieName=crtg...	Business	

Message	URL belongs to an allowed category in policy			Method	domain
Profile Name	Teste-Webfilter			Protocol	6
Received Bytes	506			Request Type	direct
Sent Bytes	436			Sequence Number	2170010
Service	HTTP			Source	JUANA.HELEN (10.69.70.222)
Source Interface	port7			Source Port	7002

Comentário

Assinatura do Cliente

Assinatura NCT

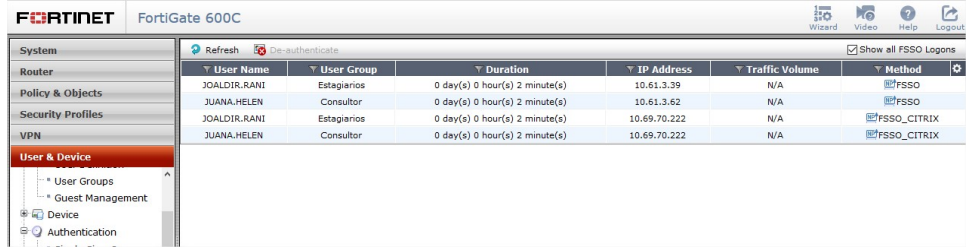
Item de Teste - 1.6.7.3	Deve permitir o controle, sem instalação de software cliente, em equipamentos que solicitem saída à internet, para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Habilitar na configuração da interface a opção de Captive Portal
Procedimento do Teste	Executar o acesso a partir do captive portal autenticando um usuário
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 64/126

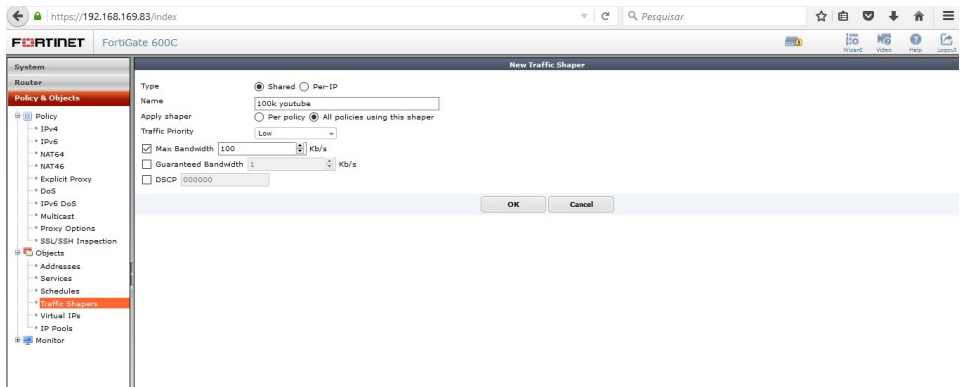
	
	
Comentário	
Assinatura do Cliente	Assinatura NCT

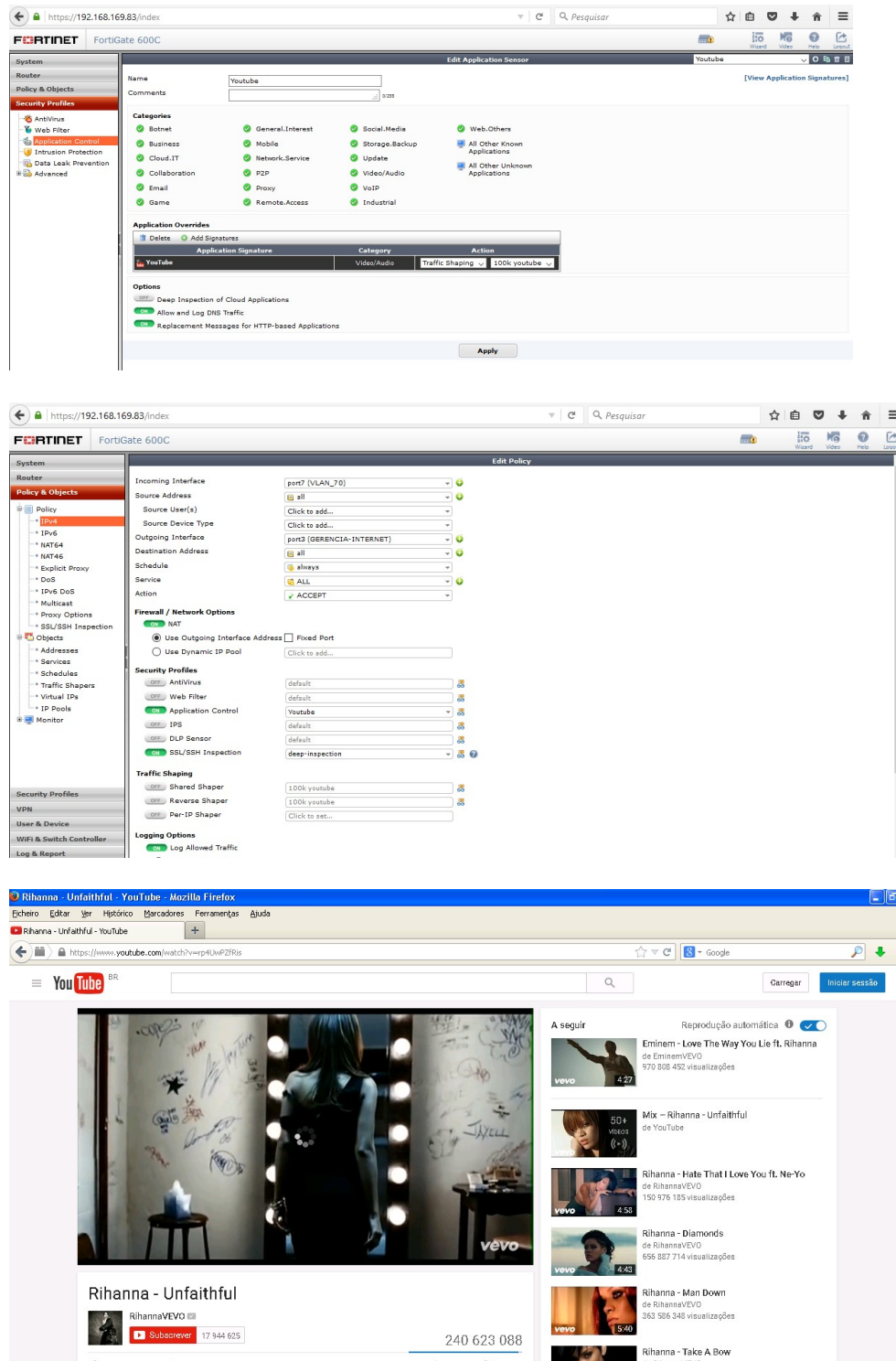
Item de Teste - 1.6.7.5	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Instalado FSSO TS agent para Citrix/Terminal Service no windows, apontado para o FSSO Collector responsável por armazenar as credencias do windows para acesso transparente.
Procedimento do Teste	Demonstrado na tela de monitoria do fortigate dois usuários com o mesmo ip 10.69.70.222
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 65/126

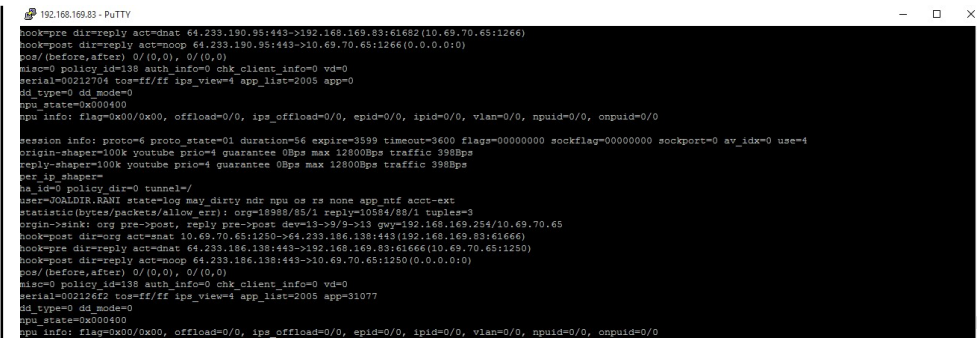
 Tela de usuários com o mesmo ip.	
Comentário	
Assinatura do Cliente	Assinatura NCT

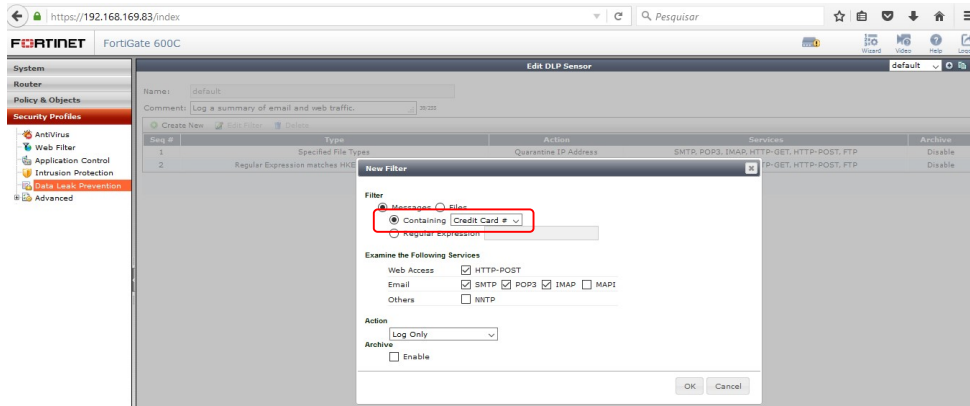
QOS

Item de Teste - 1.6.8.1	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo (youtube, ustream e etc.) e ter um alto consumo de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, tenha a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar profile de traffic shaping executando os filtros e ponderações conforme solicitado neste item
Procedimento do Teste	Acessar o youtube e verificar o shaper sendo utilizado
Evidências	

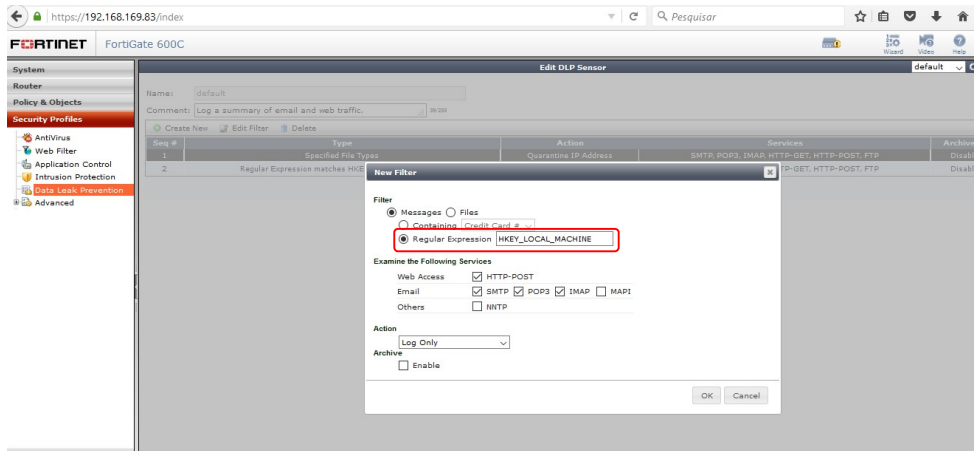
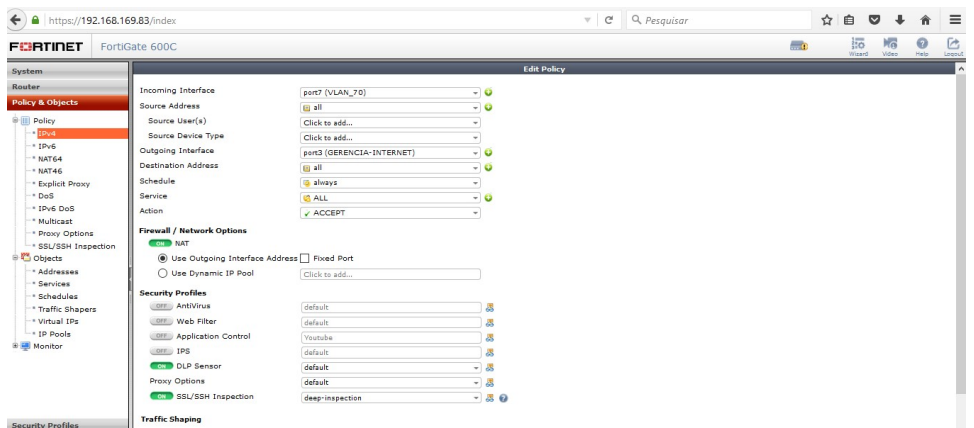


	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 67/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.9.5	Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a: número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar no profile de DLP
Procedimento do Teste	Validar o suporte da funcionalidade de informações sensíveis conforme solicitado neste item
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 68/126

		
		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.11.6.1.2	A funcionalidade de VPN SSL deve ser atendida com ou sem o uso de agente;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Instalar forticlient SSL VPN em uma estação de trabalho de um usuário assim como efetivar um acesso, em seguida relizar um acesso via Web browser.
Procedimento do Teste	Realizar conexão SSL VPN via Forticlient assim como tambem realizar um acesso pela mesma VPN utilizando via web interfece browser
Evidências	

https://192.168.169.83:4433/remote/login?lang=en

Pesquisar

☆

Please Login

Name:

Password:

Login

https://192.168.169.83:4433/sslvpn/portal.html?lang=en

Pesquisar

☆

Welcome to SSL VPN Service

Session Information

Time Logged In: joaldir (0 hours), 0 minute(s), 42 second(s)

HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes

HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes

Login History

Time	Time Logged In	Inbound/Outbound Traffic
26/11/2015 17:55:57	3 Seconds	0 B / 0 B
24/11/2015 11:37:50	21 Seconds	0 B / 0 B
24/11/2015 11:34:17	3 Minutes 19 Seconds	209.75 KB / 10.80 KB
24/11/2015 11:33:37	3 Minutes 59 Seconds	79.58 KB / 1.47 KB
24/11/2015 11:31:51	5 Minutes 3 Seconds	0 B / 0 B

FortiClient Downloaded

FortiClient.Windows

FortiClient.Map

FortiClient.Linux

FortiClient.Android

Tunnel Mode

Connect

Disconnect

Refresh

Link status

Down

Bytes sent:

0

Bytes received:

0

Connection Tool

Type: HTTP/HTTPS

Host:

Go

My Bookmarks

Add

Edit

FortiClient

Arquivo Ajuda



FORTINET

Register Endpoint

Teste SSL

joaldir

••••••••

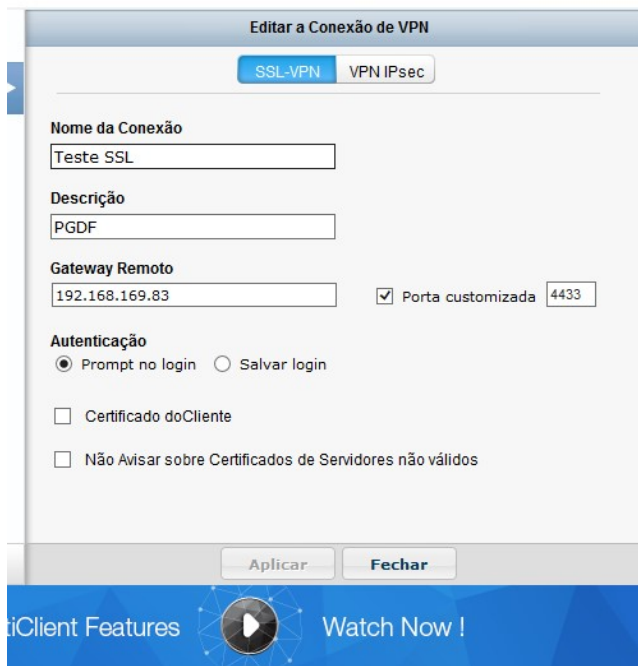
Conectar

Security Features Not Installed

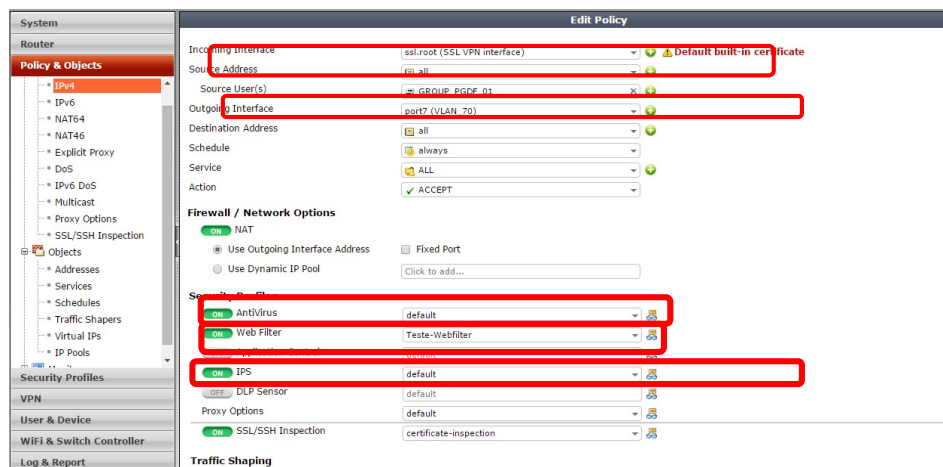


Get Protected

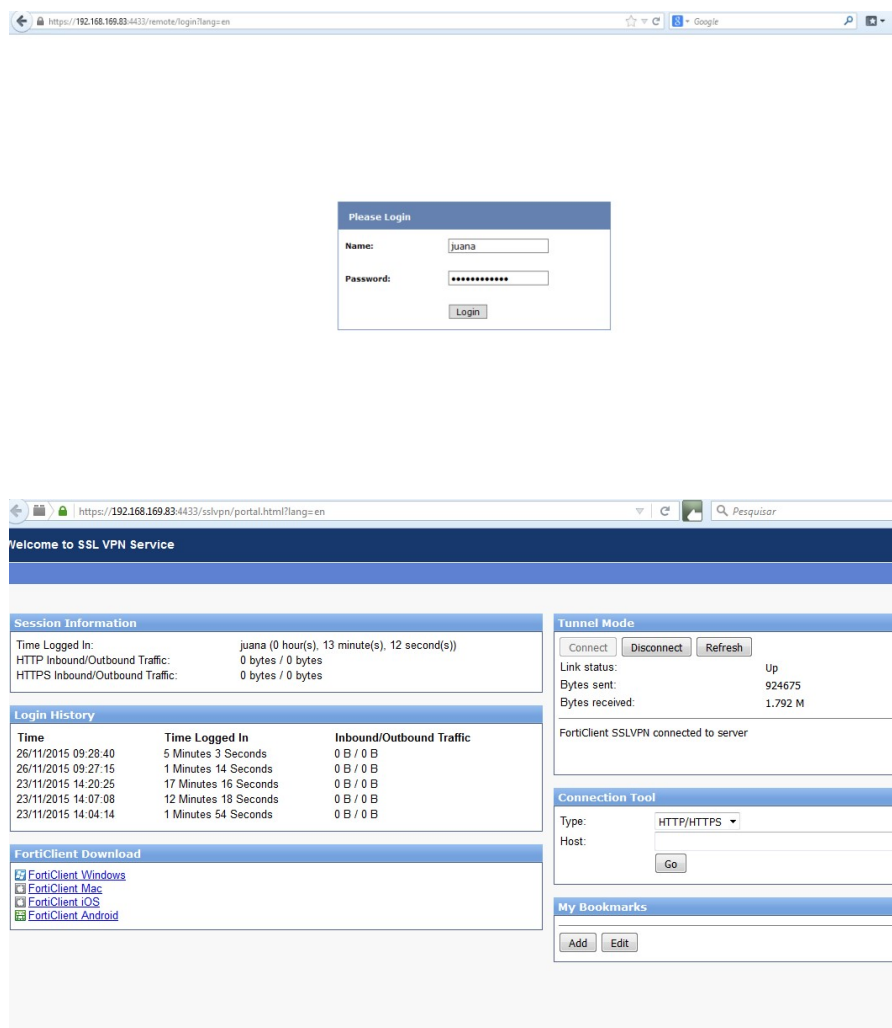
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 70/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.11.6.1.6	Deve permitir criar políticas de controle de aplicações, IPS, antivírus, anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar profiles de segurança nas políticas de acesso SSL VPN
Procedimento do Teste	Validar a criação da inserção das políticas de segurança da regras para o acesso a ssl.root e feito um acesso com um usuário de VPN "juana", onde foi possível gerar vários eventos a partir deste usuário.
Evidências	Regra de firewall correspondente de origem da interface ssl.root que é a interface virtual dos clientes conectados na VPN SSL, a qual consta habilitado perfis de segurança de filtro de IPS, Antivirus/Spyware e filtro de conteúdo:



Usuário conectou-se a VPN com a credencial "juana":



Monitor no firewall dos usuários conectados na VPN, onde é possível observar

que o usuário "juana" se conectou e recebeu o Ip do tunnel ss.root 10.212.134.200:

System	No.	User	Source IP	Begin Time	Description
Router	1	Juana	10.61.3.30	Thu Nov 26 10:29:15 2015	Tunnel IP:10.212.134.200
Policy & Objects					
Security Profiles					
VPN					
IPsec					
Tunnels					
Concentrator					
Wizard					
Tunnel Templates					
SSL					
Portals					
Settings					
Monitor					
IPsec Monitor					
SSL VPN Monitor					

```

Adaptador PPP fortissl:
Sufixo DNS específico de conexão. . . . . : 10.212.134.200
Endereço IPv4. . . . . : 255.255.255.255
Máscara de Sub-rede. . . . . : 0.0.0.0
Gateway Padrão. . . . . :

Adaptador Ethernet Conexão local:
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

Adaptador Ethernet Conexão de Rede Bluetooth:
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

Adaptador Ethernet Conexão local 2:
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

Adaptador Ethernet VMware Network Adapter VMnet1:
Sufixo DNS específico de conexão. . . . . :
Endereço IPv6 de link local . . . . . : fe80::7566:ce25:4154:8e6f%25
Endereço IPv4. . . . . : 192.168.154.1
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . :

Adaptador de Rede sem Fio Conexão de Rede sem Fio:
Sufixo DNS específico de conexão. . . . . : nct.com.br
Endereço IPv6 de link local . . . . . : fe80::51ad:51a:e997:c92d%13
Endereço IPv4. . . . . : 10.61.3.30
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : 10.61.3.254

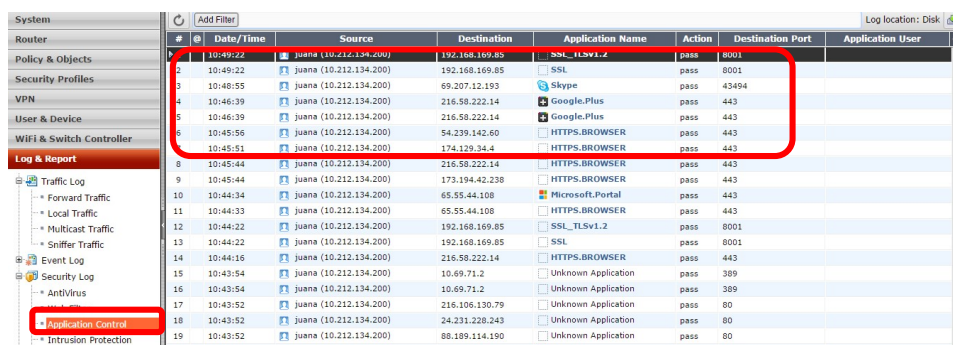
Adaptador de Rede sem Fio Conexão de Rede sem Fio 2:

```

No log do Fortigate é possível observar vários eventos de webfilter :

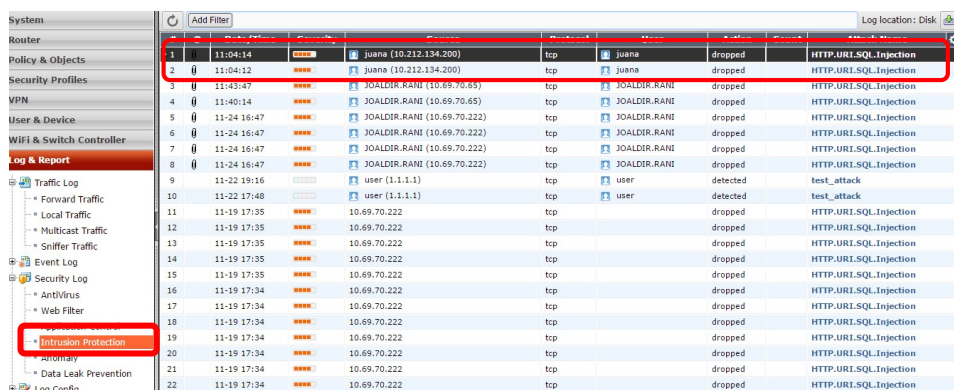
System	#	Date/Time	User	Source	Action	URL	Category	Description
Router	2	10:46:39	Juana	Juana (10.212.134.200)	blocked	plus.google.com/	Social Networking	
Policy & Objects	3	10:45:56	Juana	Juana (10.212.134.200)	passthrough	dynkneymc91ut.cloudfront.net/	Content Servers	
Security Profiles	4	10:45:51	Juana	Juana (10.212.134.200)	passthrough	cupdates.trusteer.com/	Information Technology	
VPN	5	10:45:44	Juana	Juana (10.212.134.200)	passthrough	safebrowsing-cache.google.com/	Search Engines and Portals	
User & Device	6	10:45:44	Juana	Juana (10.212.134.200)	passthrough	safebrowsing.google.com/	Search Engines and Portals	
WiFi & Switch Controller	7	10:44:33	Juana	Juana (10.212.134.200)	passthrough	settings-win.data.microsoft.com/	Information Technology	
Log & Report	8	10:44:16	Juana	Juana (10.212.134.200)	passthrough	clients1.google.com/	Search Engines and Portals	
Traffic Log	9	10:43:19	Juana	Juana (10.212.134.200)	passthrough	pipe.skype.com/	Internet Telephony	
Forward Traffic	10	10:39:59	JUANA-HELEN	JUANA-HELEN (10.69.70.222)	passthrough	safebrowsing-cache.google.com/safebrowsing/rd/CHFnB20nLXBoaYtM...	Search Engines and Portals	
Local Traffic	11	10:39:59	JUANA-HELEN	JUANA-HELEN (10.69.70.222)	passthrough	safebrowsing-cache.google.com/safebrowsing/rd/CHFnB20nLXBoaYtM...	Search Engines and Portals	
Multicast Traffic	12	10:39:59	JUANA-HELEN	JUANA-HELEN (10.69.70.222)	passthrough	safebrowsing-cache.google.com/safebrowsing/rd/CHFnB20nLXBoaYtM...	Search Engines and Portals	
Sniffer Traffic	13	10:39:59	JUANA-HELEN	JUANA-HELEN (10.69.70.222)	passthrough	safebrowsing.clients.google.com/safebrowsing/downloads?client=n...	Search Engines and Portals	
Event Log	14	10:39:57	JUANA-HELEN	JUANA-HELEN (10.69.70.222)	passthrough	www.gstatic.com/generate_204	Information Technology	
Security Log	15	10:38:33	Juana	Juana (10.212.134.200)	passthrough	pipe.skype.com/	Internet Telephony	
Web Filter	16	10:38:21	Juana	Juana (10.212.134.200)	passthrough	prod.registrar.skype.com/	Internet Telephony	
Intrusion Protection	17	10:38:14	Juana	Juana (10.212.134.200)	passthrough	*.dc.trouter.io/	Information Technology	
Anomaly	18	10:38:12	Juana	Juana (10.212.134.200)	passthrough	api.skype.com/	Internet Telephony	
Data Leak Prevention	19	10:38:11	Juana	Juana (10.212.134.200)	passthrough	ocsp.digicert.com/	Information Technology	
Log Config	20	10:37:55	Juana	Juana (10.212.134.200)	passthrough	tiles.services.mozilla.com/	Information Technology	
Monitor	21	10:37:54	Juana	Juana (10.212.134.200)	passthrough	a.config.skype.com/	Internet Telephony	
	22	10:37:45	Juana	Juana (10.212.134.200)	passthrough	pipe.skype.com/	Internet Telephony	
	23	10:37:19	Juana	Juana (10.212.134.200)	passthrough	pipe.skype.com/	Internet Telephony	

No log do Fortigate é possível observar vários eventos de Antivirus/Spyware:



#	Date/Time	Source	Destination	Application Name	Action	Destination Port	Application User
2	10:49:22	juana (10.212.134.200)	192.168.169.85	SSL_TLSv1.2	pass	8001	
3	10:49:55	juana (10.212.134.200)	69.207.12.193	Skype	pass	43494	
4	10:46:39	juana (10.212.134.200)	216.58.222.14	Google.Plus	pass	443	
5	10:46:39	juana (10.212.134.200)	216.58.222.14	Google.Plus	pass	443	
6	10:45:56	juana (10.212.134.200)	54.239.142.60	HTTPS.BROWSER	pass	443	
8	10:45:51	juana (10.212.134.200)	174.129.34.4	HTTPS.BROWSER	pass	443	
9	10:45:44	juana (10.212.134.200)	216.58.222.14	HTTPS.BROWSER	pass	443	
10	10:44:34	juana (10.212.134.200)	65.55.44.108	Microsoft.Portals	pass	443	
11	10:44:33	juana (10.212.134.200)	65.55.44.108	HTTPS.BROWSER	pass	443	
12	10:44:22	juana (10.212.134.200)	192.168.169.85	SSL_TLSv1.2	pass	8001	
13	10:44:22	juana (10.212.134.200)	192.168.169.85	SSL	pass	8001	
14	10:44:16	juana (10.212.134.200)	216.58.222.14	HTTPS.BROWSER	pass	443	
15	10:43:54	juana (10.212.134.200)	10.69.71.2	Unknown Application	pass	389	
16	10:43:54	juana (10.212.134.200)	10.69.71.2	Unknown Application	pass	389	
17	10:43:52	juana (10.212.134.200)	216.106.130.79	Unknown Application	pass	80	
18	10:43:52	juana (10.212.134.200)	24.231.228.243	Unknown Application	pass	80	
19	10:43:52	juana (10.212.134.200)	88.189.114.190	Unknown Application	pass	80	

No log do Fortigate é possível observar vários eventos de IPS :



#	Date/Time	Source	Destination	Protocol	Application	Action	Destination Port	Application User
1	11:04:14	juana (10.212.134.200)	10.69.70.65	tcp	juana	dropped	8001	
2	11:04:12	juana (10.212.134.200)	10.69.70.65	tcp	juana	dropped	8001	
3	11:43:47	JOALDIR.RANI (10.69.70.65)	10.69.70.222	tcp	JOALDIR.RANI	dropped	8001	
4	11:40:14	JOALDIR.RANI (10.69.70.65)	10.69.70.222	tcp	JOALDIR.RANI	dropped	8001	
5	11:24 16:47	JOALDIR.RANI (10.69.70.222)	10.69.70.222	tcp	JOALDIR.RANI	dropped	8001	
6	11:24 16:47	JOALDIR.RANI (10.69.70.222)	10.69.70.222	tcp	JOALDIR.RANI	dropped	8001	
7	11:24 16:47	JOALDIR.RANI (10.69.70.222)	10.69.70.222	tcp	JOALDIR.RANI	dropped	8001	
8	11:24 16:47	JOALDIR.RANI (10.69.70.222)	10.69.70.222	tcp	JOALDIR.RANI	dropped	8001	
9	11:22 17:48	user (1.1.1.1)	10.69.70.222	tcp	user	detected	8001	
10	11:22 17:48	user (1.1.1.1)	10.69.70.222	tcp	user	detected	8001	
11	11:19 17:35	10.69.70.222	10.69.70.222	tcp		dropped	8001	
12	11:19 17:35	10.69.70.222	10.69.70.222	tcp		dropped	8001	
13	11:19 17:35	10.69.70.222	10.69.70.222	tcp		dropped	8001	
14	11:19 17:35	10.69.70.222	10.69.70.222	tcp		dropped	8001	
15	11:19 17:35	10.69.70.222	10.69.70.222	tcp		dropped	8001	
16	11:19 17:34	10.69.70.222	10.69.70.222	tcp		dropped	8001	
17	11:19 17:34	10.69.70.222	10.69.70.222	tcp		dropped	8001	
18	11:19 17:34	10.69.70.222	10.69.70.222	tcp		dropped	8001	
19	11:19 17:34	10.69.70.222	10.69.70.222	tcp		dropped	8001	
20	11:19 17:34	10.69.70.222	10.69.70.222	tcp		dropped	8001	
21	11:19 17:34	10.69.70.222	10.69.70.222	tcp		dropped	8001	
22	11:19 17:34	10.69.70.222	10.69.70.222	tcp		dropped	8001	

Comentário

Assinatura
do Cliente

Assinatura NCT

Item de Teste -
1.6.11.6.1.9

Permitir estabelecer um túnel VPN client-to-site do cliente à plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

Objetivo do
Teste

Demonstrar funcionalidade conforme solicitado

Configuração do
Teste

Foi configurado um cliente sistema operacional windows xp, um servidor de arquivos windows server 2012, vpnssl no fortigate com integração Active Directory em um servidor domínio jrs.com.

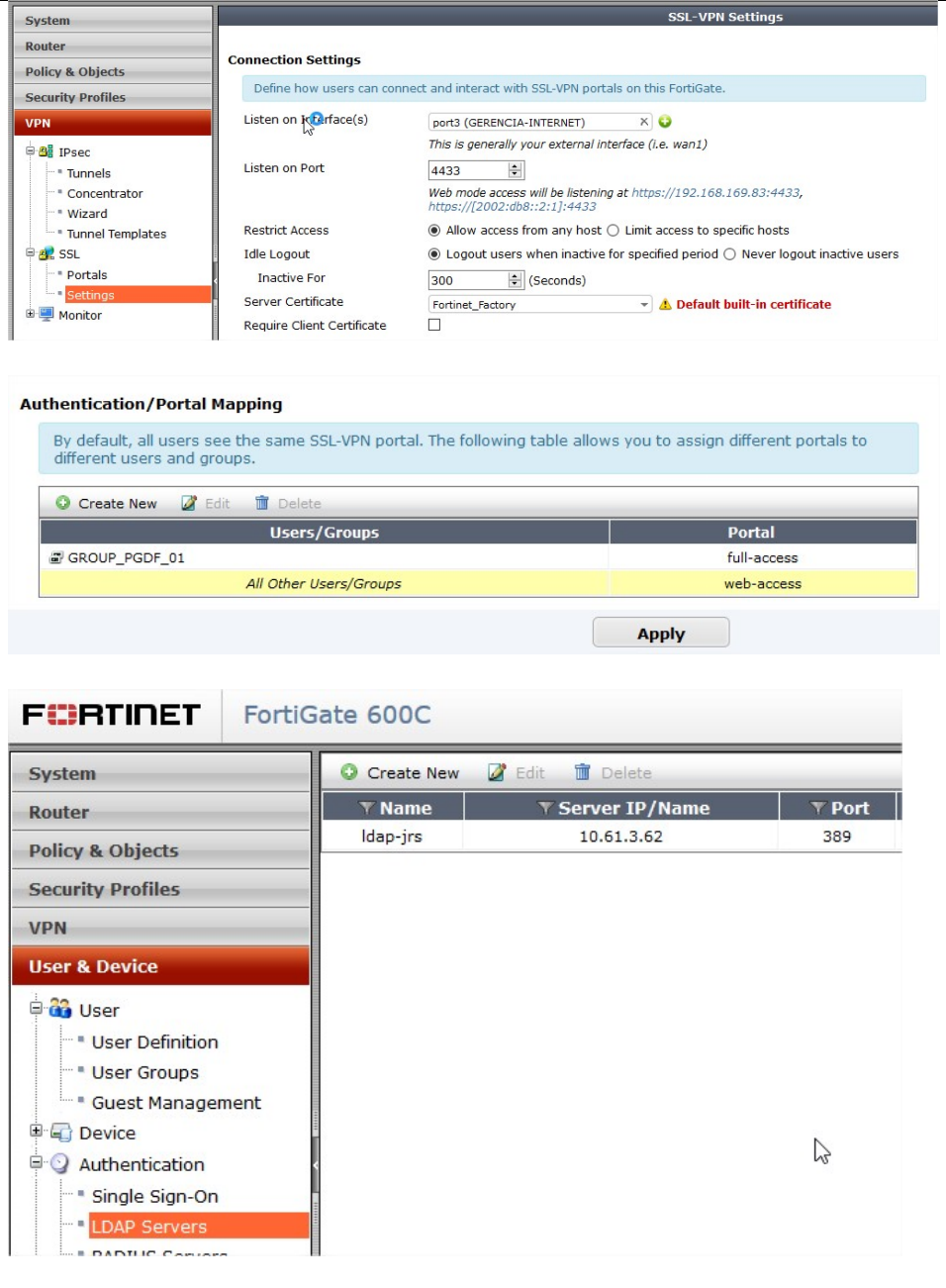
Procedimento
do Teste

Apartir do windows xp o usuário juana.helen pertencente ao domínio JRS escolheu o tunnel VPN pgdf_lab e ativou a opção "minhas credencias são as mesmas credencias do windows" digitou as credencias pertencente a esse domínio e logou.
Após esse evento o tunel foi estabelecido com o equipamento de segurança obtendo o ip 10.212.134.200. Foi utilizado a ferramenta tracert para mostrar o

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 74/126

caminho do cliente ao servidor demonstrando que o tráfego passava pelo tunel. Foi aberto uma sessão de compartilhamento de arquivos no servidor de arquivos 10.61.1.43 para demonstrar acesso as recursos.

Evidências



The image shows two screenshots of the FortiGate 600C web interface. The top screenshot displays the 'SSL-VPN Settings' page under the 'VPN' menu. The 'Connection Settings' section is active, showing options for listening on interfaces and ports. The 'Listen on Interface(s)' is set to 'port3 (GERENCIA-INTERNET)' and 'Listen on Port' is set to '4433'. The 'Restrict Access' section has radio buttons for 'Allow access from any host' (selected) and 'Limit access to specific hosts'. The 'Idle Logout' section has radio buttons for 'Logout users when inactive for specified period' (selected) and 'Never logout inactive users'. The 'Server Certificate' is set to 'Fortinet_Factory' and 'Require Client Certificate' is unchecked.

The bottom screenshot displays the 'Authentication/Portal Mapping' page. It shows a table for mapping users/groups to different SSL-VPN portals. The table has two columns: 'Users/Groups' and 'Portal'. The first row shows 'GROUP_PGDF_01' mapped to 'full-access'. The second row, highlighted in yellow, shows 'All Other Users/Groups' mapped to 'web-access'. An 'Apply' button is visible at the bottom of the table.

Users/Groups	Portal
GROUP_PGDF_01	full-access
All Other Users/Groups	web-access

The bottom screenshot also shows the 'User & Device' section under the 'VPN' menu. The 'User' section is expanded, showing options for 'User Definition', 'User Groups', and 'Guest Management'. The 'Device' section is also expanded, showing options for 'Authentication', 'Single Sign-On', and 'LDAP Servers'.

FORTINET FortiGate 600C

Edit User Group

Name: GROUP_PGDF_01

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: joaldir

Remote groups:

Remote Server	Group Name
ldap-jrs	CN=Consultores,CN=Users,DC=jrs,DC=com

OK Cancel

Logon no Windows

Windows^{XP} Lite 4.0

Nome de usuário: juana.helen

Senha: [obscured]

Fazer logon em: JRS

☐ Fazer logon usando uma conexão dial-up

VPN antes do: pgdf_lab

☒ Minhas credenciais de VPN credenciais são as mesmas cred

Usuário da: [obscured]

Senha da VPN: [obscured]

OK Cancelar Desligar... Opções <<

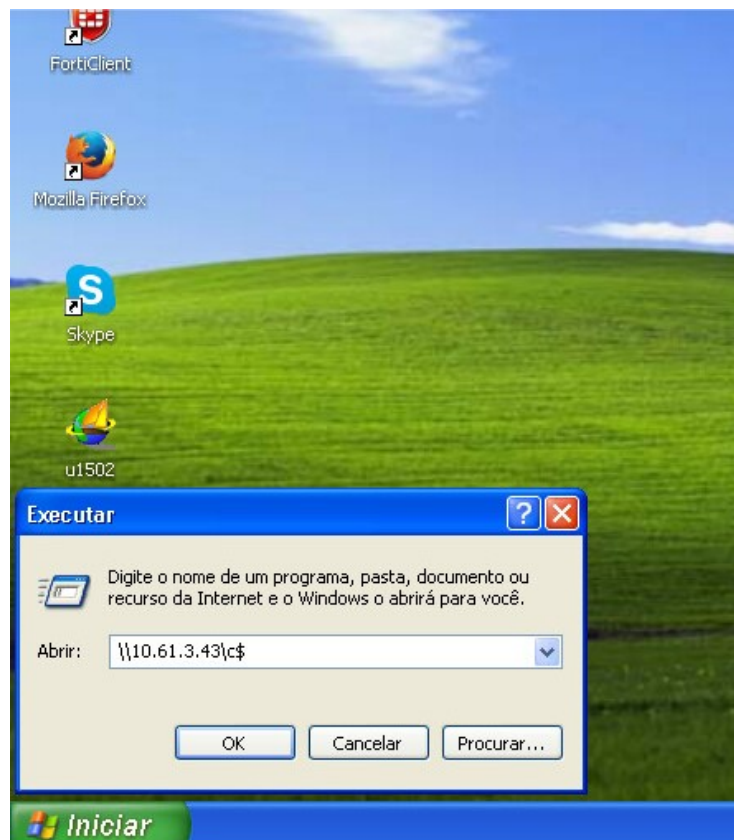
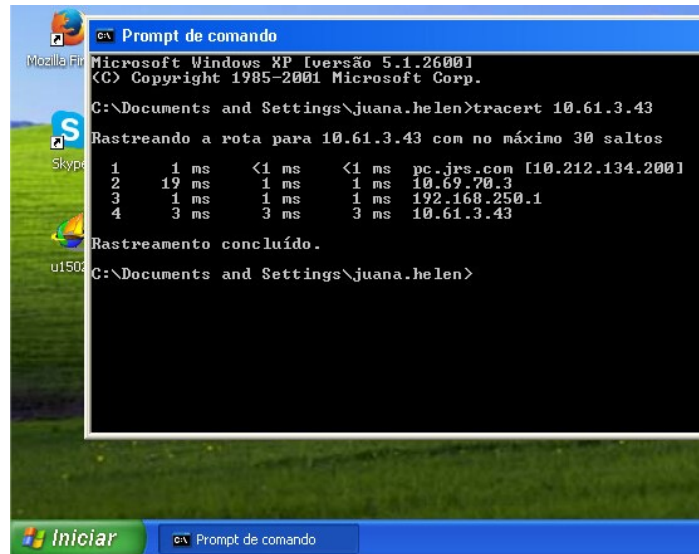
FortiClient

Windows^{XP} Lite 4.0

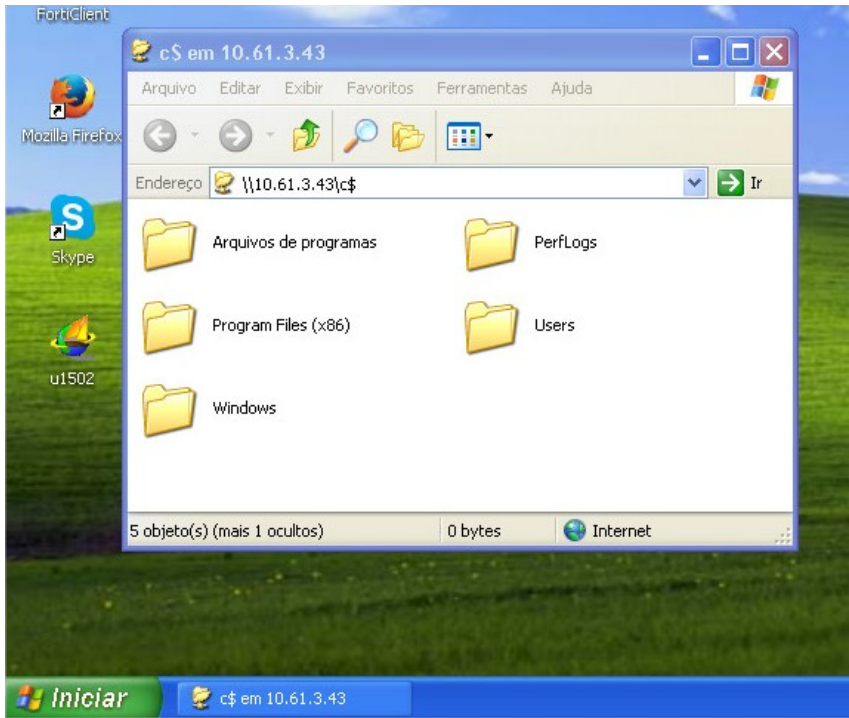
Conectando no tunel VPN (pgdf_lab)...

FORTINET FortiGate 600C

No.	User	Source IP	Begin Time	Description
1	juana.helen	10.69.70.65	Mon Nov 23 15:07:08 2015	Subsession
				Tunnel IP:10.212.134.200



	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 77/126

	
Comentário	
Assinatura do Cliente	Assinatura NCT

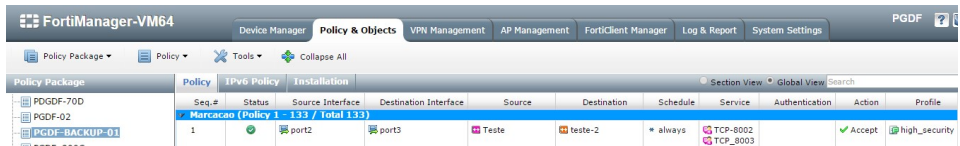
Item de Teste - 1.6.12.5.9	Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Executar o acesso via terminal SSH e digitar a seqüência de comando com o sinal "?"
Procedimento do Teste	Será listado apos digitar o sinal "?" todos os comandos correspondente a linha chave selecionada
Evidências	Ao efetivar o acesso via SSH e digitar no final da linha "?" o mesmo apresenta todas as demais linhas correspondentes:

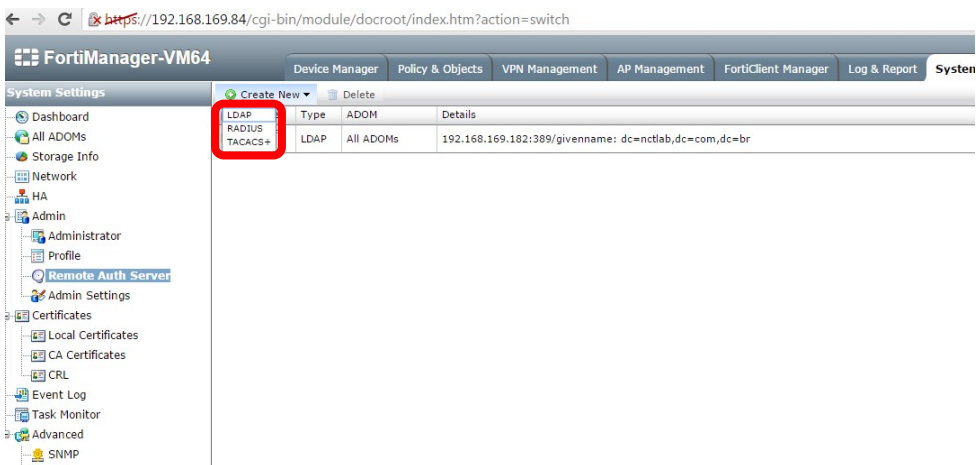
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 78/126

<pre> PGDF-BACKUP-01 # config system 3g-modem Configure 3G modem. accprofile Configure system admin access group. admin Configure admin users. arp-table Configure ARP table. auto-install Configure USB auto installation. autoupdate Configure automatic updates. central-management Configure central management. console Configure console. custom-language Configure custom languages. ddns Configure DDNS. dhcp Configure DHCP. dhcp6 Configure DHCPv6. dns Configure DNS. dns-database Configure DNS database. dns-server Configure DNS servers. dscp-based-priority Configure DSCP based priority table. email-server Configure email server. fips-cc Configure FIPS-CC mode. fortiguard Configure FortiGuard services. fortisandbox Configure FortiSandbox. fsso-polling Configure Fortinet Single Sign On (FSSO) server. geoip-override Configure geographical location mapping for IP address. global Configure global attributes. gre-tunnel Configure GRE tunnel. ha Configure HA. interface Configure interfaces. ipip-tunnel Configure IP in IP Tunneling. ips-urlfilter-dns Configure IPS URL filter DNS servers. ipv6-neighbor-cache Configure IPv6 neighbor cache table. ipv6-tunnel Configure IPv6/IPv4 in IPv6 tunnel. link-monitor Configure Link Health Monitor. lte-modem Configure LTE MODEM. modem Configure MODEM. monitors Configure system monitors. nat64 Configure NAT64. netflow Configure NetFlow. network-visibility Configure network visibility settings. npu Configure NPU attributes. ntp Configure system NTP information. object-tag Configure object tags. password-policy Configure password policy. --More-- </pre>	
Comentário	
Assinatura do Cliente	Assinatura NCT

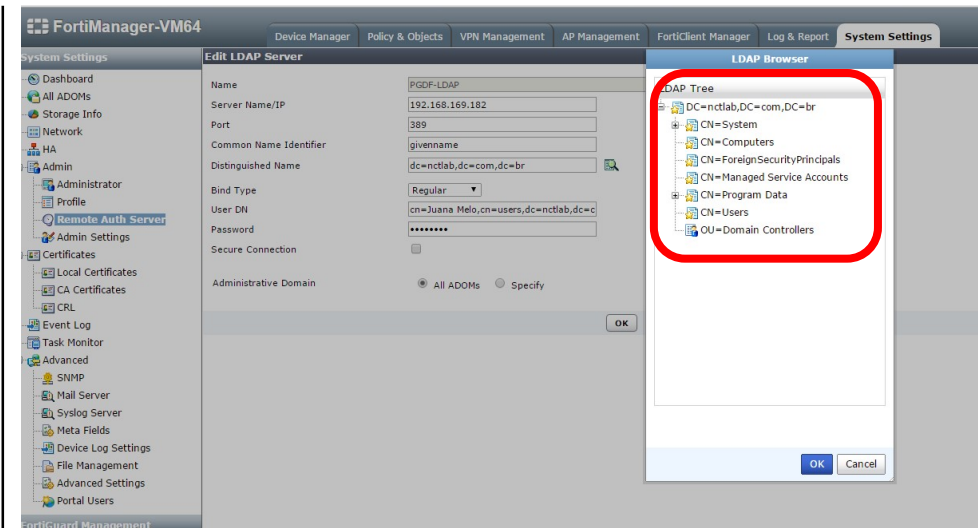
Item de Teste - 1.6.12.5.10	Deve permitir usar palavras-chave e cores para facilitar a identificação de regras;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurado no Fortimanager em uma politica de firewall Cores e tags
Procedimento do Teste	Mostrar a marcação de cores dos objetos diferenciados assim como uma sessão de marcação 'MARCACAO'
Evidências	Marcação de sessão re regras para identificar, e objetos Teste em rosa, objeto teste-2 em laranja, e objetos de serviço personalizados em rosa:

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 79/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

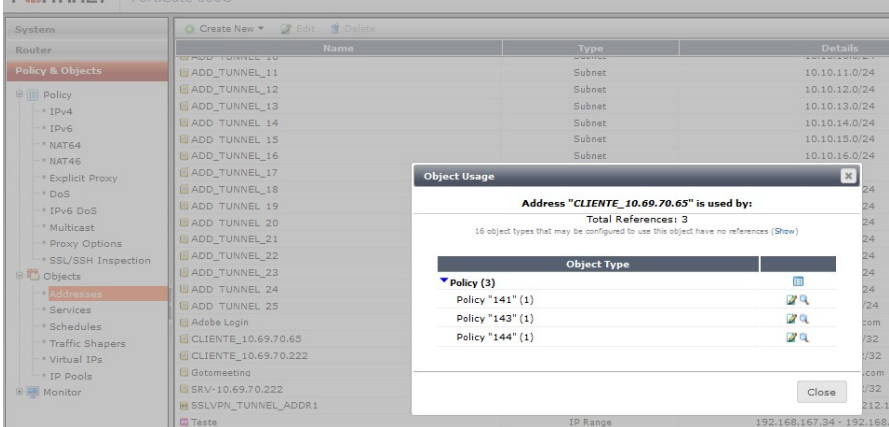
Item de Teste - 1.6.12.5.14	Autenticação integrada ao Microsoft Active Directory e servidor RADIUS;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar servidores de autenticação remoto e integração com o AD conforme solicitado neste item
Procedimento do Teste	Mostrar a integração nos métodos de autenticação mencionados
Evidências	Tela de configuração de servidores remotos para integração de autenticação LDAP, RADIUS e TACACS:  Configurado para teste uma integração com LDAP, neste tela é possível ver a consulta LDAP na árvore do AD:

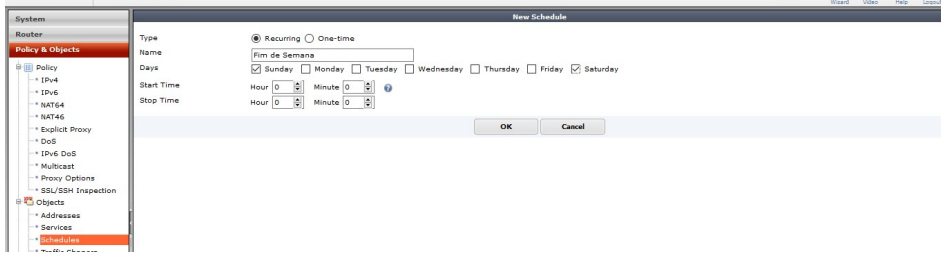
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 80/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

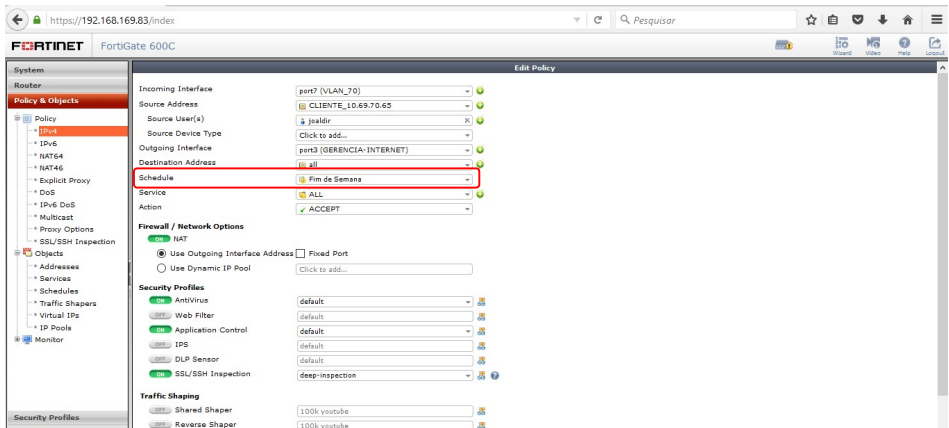
Item de Teste - 1.6.12.5.15	Localização de em quais regras um endereço IP, IP range, subnet ou objetos estão sendo utilizados;																																																																																										
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado																																																																																										
Configuração do Teste	Automaticamente ao configurar um objeto e sendo este inserido em uma regra, perfil ou group, ao lado deste haverá uma referencia "Ref" indicando em quantos objetos ele encontra-se em uso.																																																																																										
Procedimento do Teste	Mostrar a referencias do objeto																																																																																										
Evidências	Objetos address ,Ip range, Subnet os quais contem uma valor abaixo da coluna rafe significa quantas vezes os mesmos estão sendo utilizando em uma regra de firewall: <table><tr><th>Name</th><th>Type</th><th>Details</th><th>Interface</th><th>Visibility</th><th>Ref.</th></tr><tr><td colspan="6">Address (64)</td></tr><tr><td>*.live.com</td><td>FQDN</td><td>*.live.com</td><td>Any</td><td>✓</td><td>1</td></tr><tr><td>192.168.169.182</td><td>Subnet</td><td>192.168.169.182/32</td><td>Any</td><td>✓</td><td>1</td></tr><tr><td>ADD_TUNNEL_1</td><td>Subnet</td><td>10.10.1.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_2</td><td>Subnet</td><td>10.10.2.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_3</td><td>Subnet</td><td>10.10.3.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_4</td><td>Subnet</td><td>10.10.4.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_5</td><td>Subnet</td><td>10.10.5.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_6</td><td>Subnet</td><td>10.10.6.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_7</td><td>Subnet</td><td>10.10.7.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_8</td><td>Subnet</td><td>10.10.8.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_9</td><td>Subnet</td><td>10.10.9.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_10</td><td>Subnet</td><td>10.10.10.0/24</td><td>Any</td><td>✓</td><td>2</td></tr><tr><td>ADD_TUNNEL_11</td><td>Subnet</td><td>10.10.11.0/24</td><td>Any</td><td>✓</td><td>2</td></tr></table>	Name	Type	Details	Interface	Visibility	Ref.	Address (64)						*.live.com	FQDN	*.live.com	Any	✓	1	192.168.169.182	Subnet	192.168.169.182/32	Any	✓	1	ADD_TUNNEL_1	Subnet	10.10.1.0/24	Any	✓	2	ADD_TUNNEL_2	Subnet	10.10.2.0/24	Any	✓	2	ADD_TUNNEL_3	Subnet	10.10.3.0/24	Any	✓	2	ADD_TUNNEL_4	Subnet	10.10.4.0/24	Any	✓	2	ADD_TUNNEL_5	Subnet	10.10.5.0/24	Any	✓	2	ADD_TUNNEL_6	Subnet	10.10.6.0/24	Any	✓	2	ADD_TUNNEL_7	Subnet	10.10.7.0/24	Any	✓	2	ADD_TUNNEL_8	Subnet	10.10.8.0/24	Any	✓	2	ADD_TUNNEL_9	Subnet	10.10.9.0/24	Any	✓	2	ADD_TUNNEL_10	Subnet	10.10.10.0/24	Any	✓	2	ADD_TUNNEL_11	Subnet	10.10.11.0/24	Any	✓	2
Name	Type	Details	Interface	Visibility	Ref.																																																																																						
Address (64)																																																																																											
*.live.com	FQDN	*.live.com	Any	✓	1																																																																																						
192.168.169.182	Subnet	192.168.169.182/32	Any	✓	1																																																																																						
ADD_TUNNEL_1	Subnet	10.10.1.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_2	Subnet	10.10.2.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_3	Subnet	10.10.3.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_4	Subnet	10.10.4.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_5	Subnet	10.10.5.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_6	Subnet	10.10.6.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_7	Subnet	10.10.7.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_8	Subnet	10.10.8.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_9	Subnet	10.10.9.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_10	Subnet	10.10.10.0/24	Any	✓	2																																																																																						
ADD_TUNNEL_11	Subnet	10.10.11.0/24	Any	✓	2																																																																																						

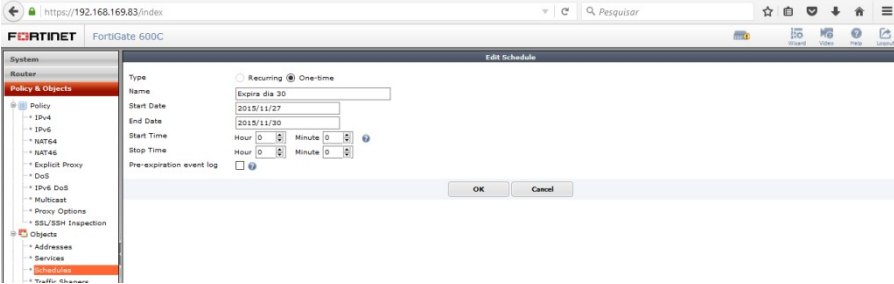
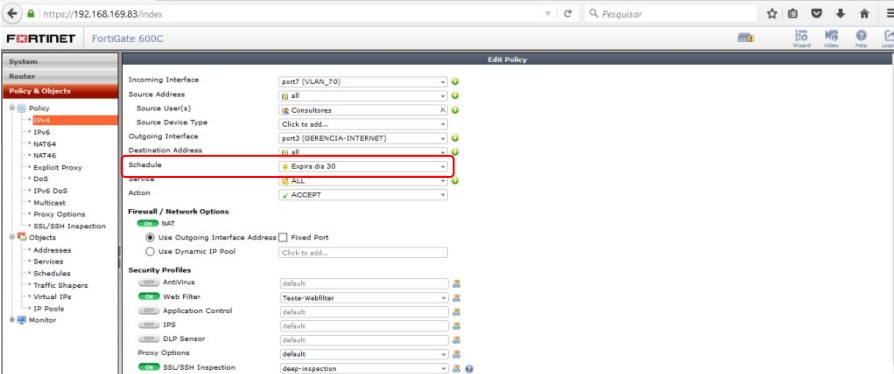
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 81/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

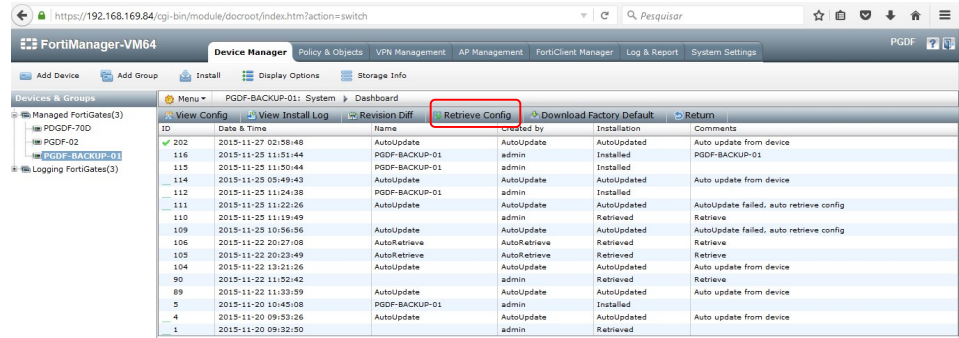
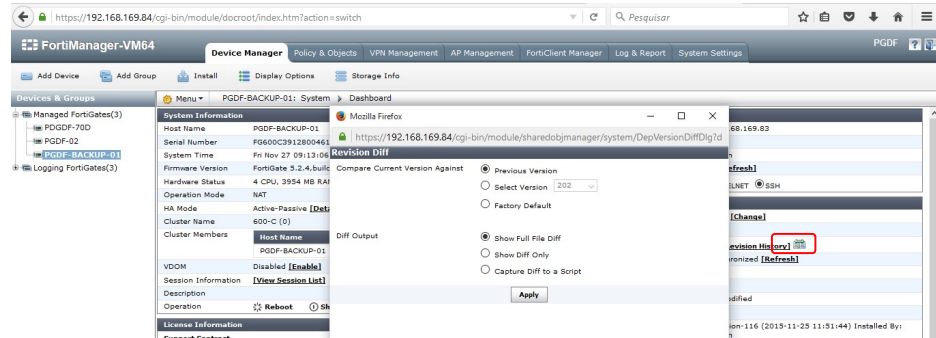
Item de Teste - 1.6.12.5.17	Criação de regras que fiquem ativas em horário definido;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar um schedule para ativação em horários definidos
Procedimento do Teste	Executar teste de validação de funcionamento da regra no horário conforme definido.
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 82/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.12.5.18	Criação de regras com data de expiração;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar um schedule de período de expiração determinado		
Procedimento do Teste	Executar teste de expiração da regra no horário conforme definido.		
Evidências	 		
Comentário			
Assinatura do Cliente	Assinatura NCT		

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 83/126

Item de Teste - 1.6.12.5.19	Backup das configurações e rollback de configuração para a última configuração salva;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar auto-backup, executar retrieve manual de configuração e salvar		
Procedimento do Teste	Executar teste de backup e de rollback		
Evidências	 		
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.12.5.21	Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Iniciar upgrade conforme solicitado		
Procedimento do Teste	Mostrar processo de upgrade pela interface de gerenciamento, CLI e GUI		
Evidências	Via linha de comando é possível executar pelos métodos TFTP, FTP e USB :		

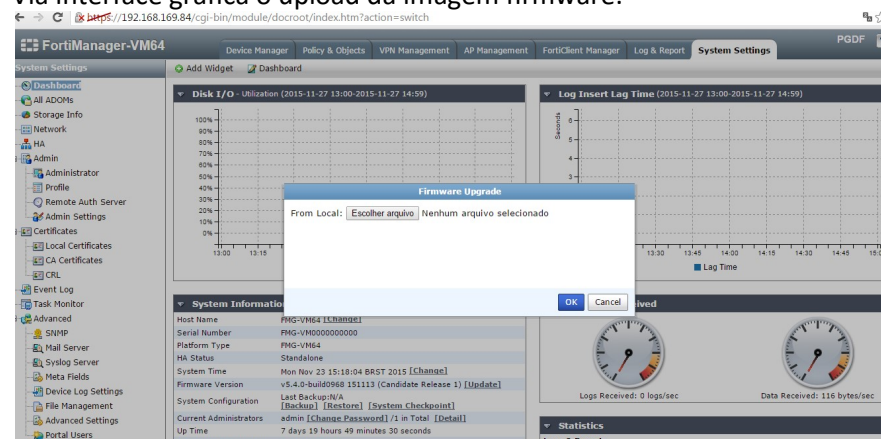
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 84/126

```

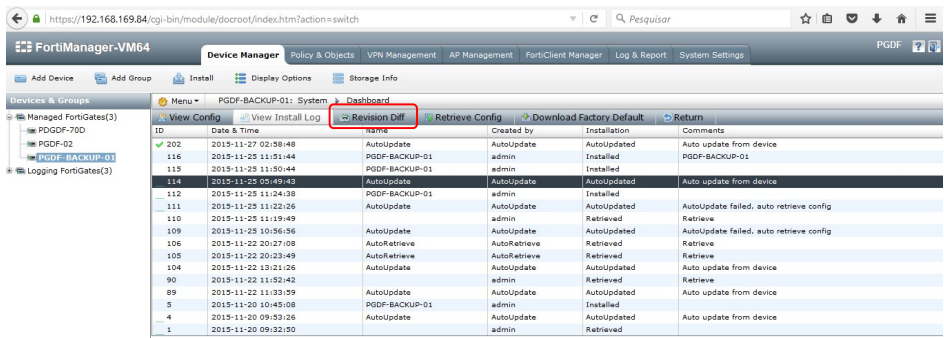
FMG-VM64 # execute upload image
ftp      Load image from FTP server.
tftp     Load image from TFTP server to local disk.
usb      Load image from USB to local disk.

```

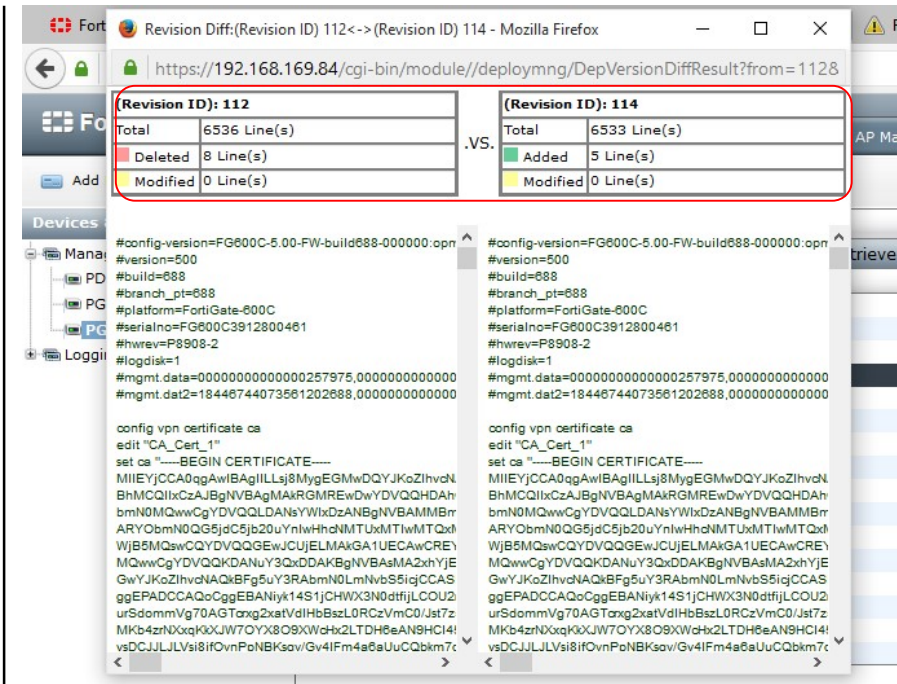
Via interface gráfica o upload da imagem firmware:



Comentário	
Assinatura do Cliente	Assinatura NCT

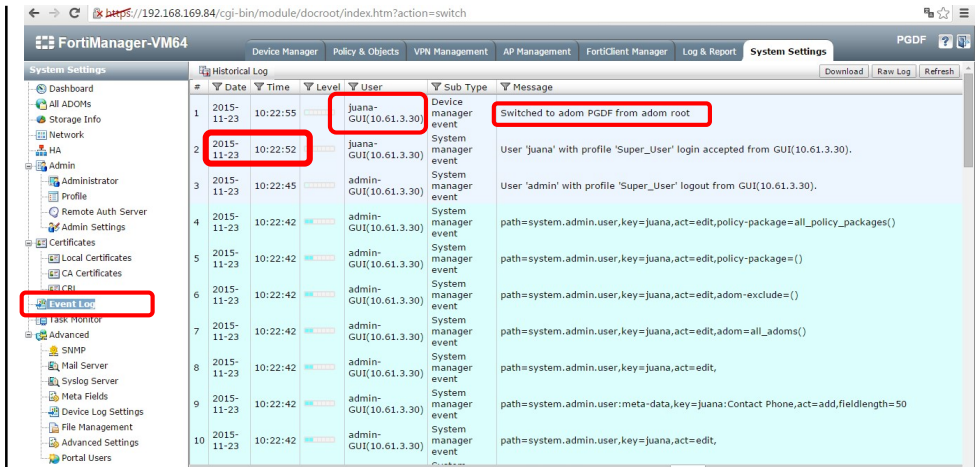
Item de Teste - 1.6.12.5.25	Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Clicar na opção de diff-policy e revision para efetivar um deparar das políticas
Procedimento do Teste	Mostrar a tela de diff-policy e revision , comparando as politicas atuais e anteriores
Evidências	

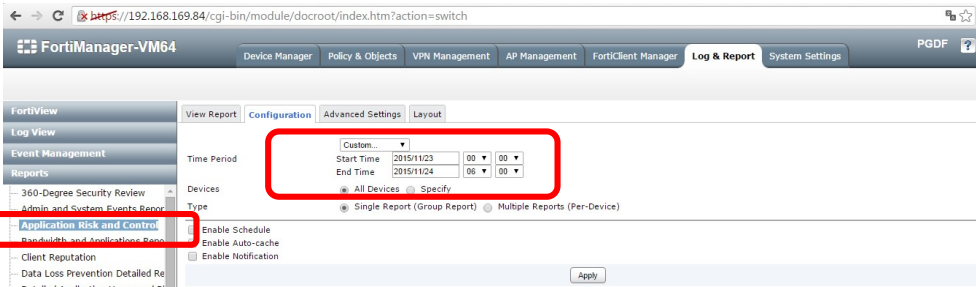
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 85/126

	
Comentário	
Assinatura do Cliente	Assinatura NCT

Item de Teste - 1.6.12.5.27	Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Selecionar aba de Fortiview na opção de logs de event
Procedimento do Teste	Mostrar a categoria de log de event as quais disponibiliza todos os detalhes de auditoria conforme solicitado.
Evidências	Extraído a tela do Fortimanager de event log onde mostrar alterações feita pelo usuário que se logou no equipamento ou mesmo qualquer modificação:

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 86/126

	
Comentário	
Assinatura do Cliente	Assinatura NCT

Item de Teste - 1.6.12.5.28	Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo a comparação dos diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar a geração de relatório com as informações e períodos como solicitado neste item.
Procedimento do Teste	Gerar relatório e executar o download para mostra
Evidências	Tela do Fortimanager onde foi alterado o período de tempo de relatório, sendo possível ter dados de um a variação de período de tempo do passado com a data atual:  Exemplo de um módulo do relatório de aplicação:

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 87/126

Top 30 Applications by Bandwidth and Sessions

#	Application	Bandwidth	Sent	Received Sessions
1	YouTube	163.85 MB		99
2	Skype	36.82 MB		3,674
3	Google.Search	12.51 MB		3
4	Facebook	12.09 MB		30
5	HTTP.BROWSER	10.51 MB		210
6	Google.Accounts	9.68 MB		41
7	SMB	5.66 MB		1
8	Google.Plus	4.94 MB		8
9	BitTorrent	4.82 MB		1,055
10	HTTPS.BROWSER	4.30 MB		119
11	Google.Hangouts	1.96 MB		15
12	SSL	924.28 KB		102
13	Gmail	562.08 KB		2
14	Microsoft.Portals	391.68 KB		21
15	Google	332.37 KB		2
16	HTTP.Video	282.06 KB		3
17	12350/tcp	210.68 KB		1
18	Activsync	130.87 KB		7
19	DNS	53.80 KB		100
20	50004/tcp	27.16 KB		2
21	50005/tcp	20.83 KB		1
22	Root.Certificate.URL	13.11 KB		4
23	NetBIOS.Name.Service	12.84 KB		1
24	OCSP	7.74 KB		3
25	40021/udp	4.75 KB		3
26	40020/udp	4.48 KB		3
27	33033/tcp	4.33 KB		2
28	40015/udp	4.23 KB		1
29	40001/udp	3.38 KB		1
30	40025/udp	3.29 KB		1

Exemplo de modulo do mesmo relatório onde foi capturado as aplicações de alto risco :

High Risk Applications

Top 20 high risk applications are listed below. These applications have the risk rating of 5 (critical risk) or 4 (high risk). Each application is listed with its respective category, technology, number of users, bandwidth and sessions.

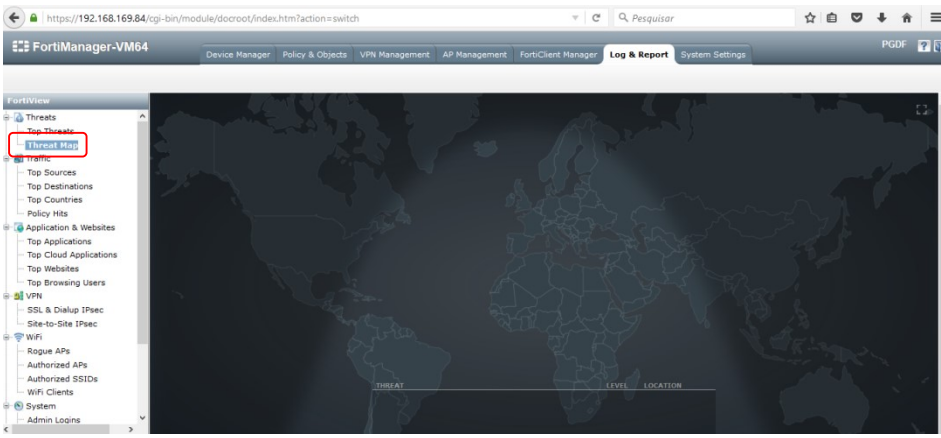
#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	5	Ultrastuf_9.6+	Proxy	Client-Server	1	158.04 KB	13
2	4	BitTorrent	P2P	Peer-to-Peer	2	133.71 KB	539
3	4	Bitcomet.HTTP.Seed	P2P	Peer-to-Peer	1	176 B	8

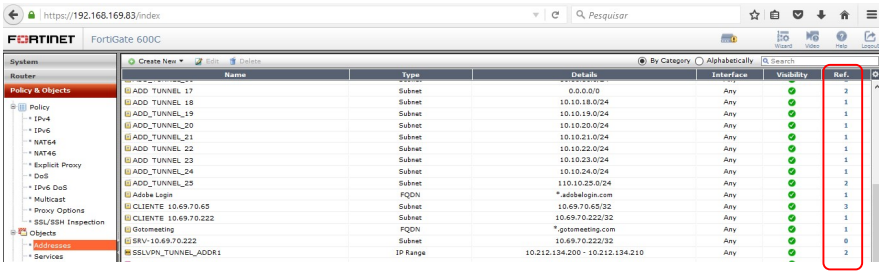
Figure 2: High risk applications (rating of 4 or 5) that are traversing the network.

Comentário		
Assinatura do Cliente	Assinatura NCT	

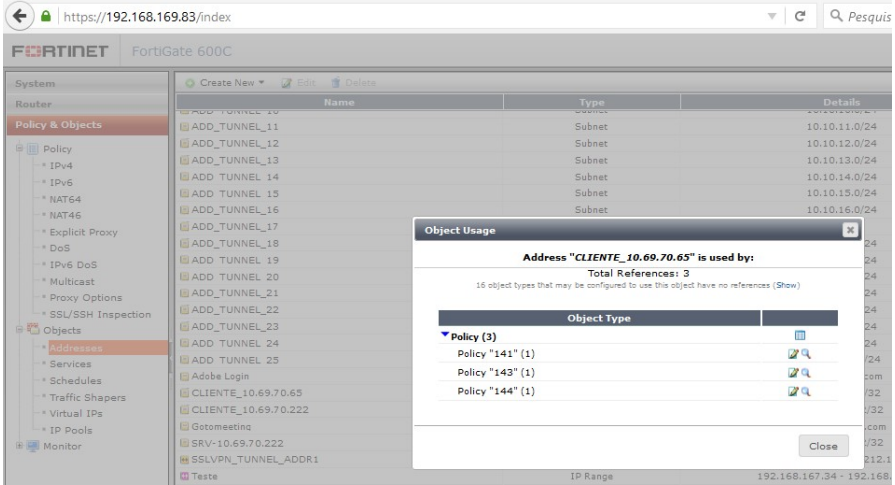
Item de Teste - 1.6.12.5.29	Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar a geração de relatório com as informações e períodos como solicitado neste item.
Procedimento do Teste	Demonstrar opção do Threat Map do FortiView
Evidências	

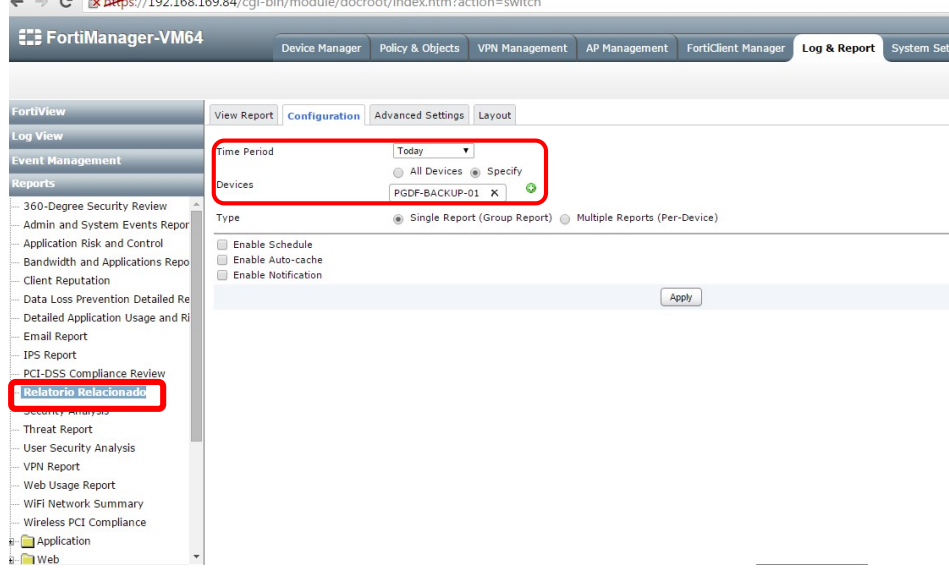
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 88/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.6.12.5.15	Localização de em quais regras um endereço IP, IP range, subnet ou objetos estão sendo utilizados;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Automaticamente ao configurar um objeto e sendo este inserido em uma regra, perfil ou group, ao lado deste haverá uma referencia "Ref" indicando em quantos objetos ele encontra-se em uso.
Procedimento do Teste	Mostrar a referencias do objeto
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 89/126

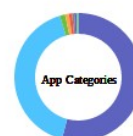
	
Comentário	
Assinatura do Cliente	Assinatura NCT

Item de Teste - 1.6.12.6	Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, antivírus e anti-spyware), URL e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configuração de um relatório de ameaça conforme os filtros de scan solicitados neste item .
Procedimento do Teste	Gerar relatório e executar o download para mostra dos resultados extraídos
Evidências	Executou extração de relatório de um período de tempo da ultima semana: 

Foi criado um relatório específico com os dados mencionando relacionado os resultados conforme solicitado neste item:

App Categories

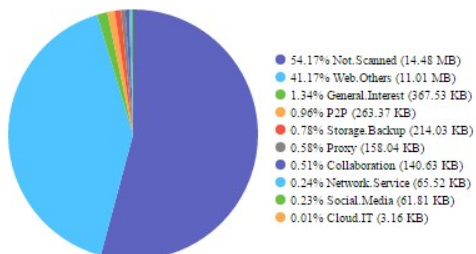
Not.Scanned	54.16%
Web.Others	41.16%
General.Interest	1.34%
P2P	0.96%
Storage.Backup	0.78%
Proxy	0.58%
Collaboration	0.51%
Network.Service	0.24%
Social.Media	0.23%
Cloud.IT	0.01%
Others	0.02%



File Transferred by Applications

No matching log data for this report

Application categories by bandwidth



Top 20 Users by Bandwidth

#	User (or IP)	Source IP	Bandwidth	Sent	Received
1	joaldir	10.69.70.222			26.73 MB

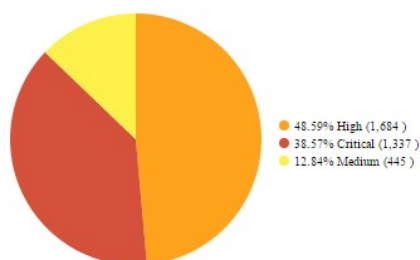
Top 20 Viruses

#	Virus Name	Occurrences
1	Riskware/UltraReach	1

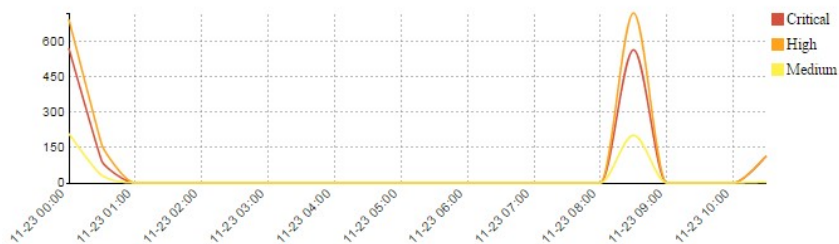
Top 20 Web Domains by Visits

#	Domain	Category	Visits
1	beacon.rubiconproject.com	Information Technology	111
2	hp.imguol.com.br	Content Servers	70
3	www.google.com	Search Engines and Portals	64
4	cf.dropboxstatic.com	File Sharing and Storage	57
5	www.google.com.br	Search Engines and Portals	56
6	imguol.com	Content Servers	51
7	pagead2.googlesyndication.com	Advertising	38
8	tpc.googlesyndication.com	Search Engines and Portals	38
9	bn.imguol.com	Information Technology	35
10	tr2.terra.com	Search Engines and Portals	35
11	rtax.criteo.com	Business	34
12	p.mctck.com	Advertising	34
13	cm.g.doubleclick.net	Advertising	26
14	googleads.g.doubleclick.net	Advertising	19
15	download.cdn.mozilla.net	Information Technology	19
16	www.google.com	Business	19
17	akhtml.nymotion.com	Advertising	18
18	cdn.bitmedianetwork.com	Advertising	16
19	pixel.mathtag.com	Content Servers	15
20	pixel.rubiconproject.com	Advertising	14

Intrusions By Severity

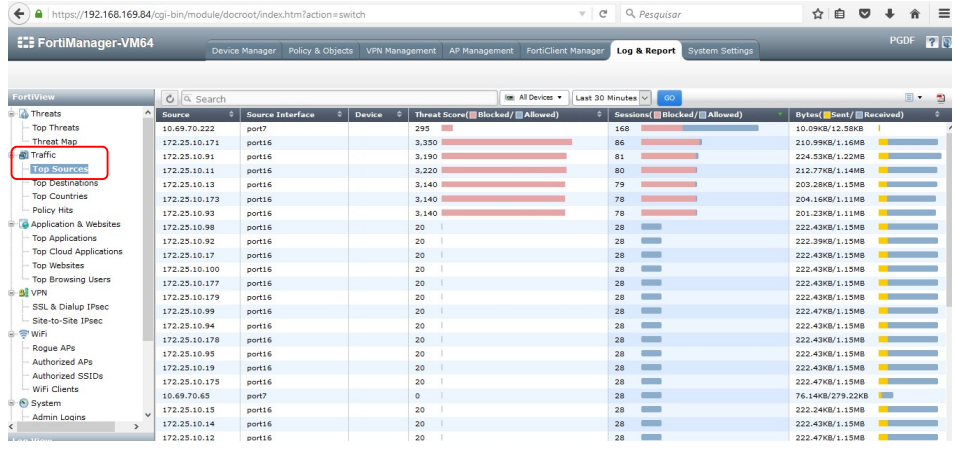


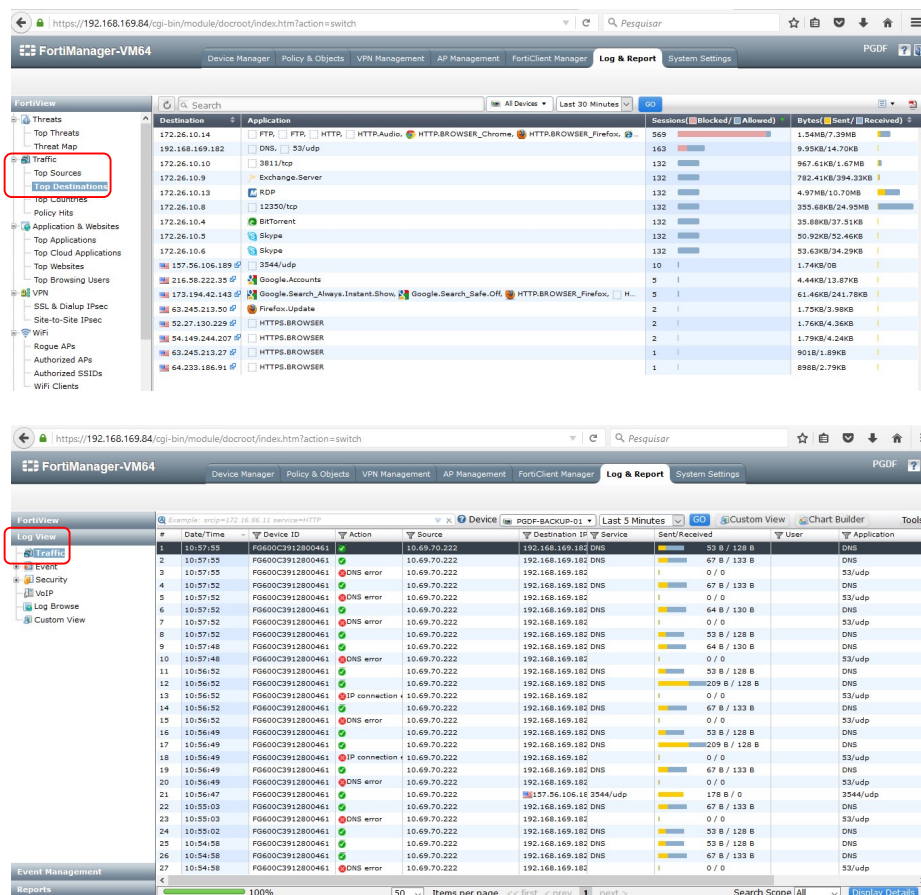
Critical High and Medium Intrusions Timeline



	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 92/126

		Intrusions																																																								
		Intrusions Detected																																																								
		<table><tr><th>#</th><th>Attack Name</th><th>Severity</th><th>CVE-ID</th><th>Counts</th></tr><tr><td>1</td><td>MS.Word.Linked.Objects.Memory.Corrup</td><td>Critical</td><td>CVE-2010-1903</td><td>80</td></tr><tr><td>2</td><td>MS.Publisher.Pubconv.dll.Pointer.Ove</td><td>Critical</td><td>CVE-2011-1508</td><td>40</td></tr><tr><td>3</td><td>MS.Visio.Invalid.Tag.Handling.Remot</td><td>Critical</td><td>CVE-2009-0096</td><td>40</td></tr><tr><td>4</td><td>MS.Windows.MPEG4.Codec.ASF.Par</td><td>Critical</td><td>CVE-2010-0818</td><td>40</td></tr><tr><td>5</td><td>Adobe.Reader.Font.Parsing.Integer.O</td><td>Critical</td><td>CVE-2010-2862</td><td>40</td></tr><tr><td>6</td><td>MS.Office.VBA.Module.Stream.Us</td><td>Critical</td><td></td><td>40</td></tr><tr><td>7</td><td>MS.Excel.Record.Parsing.Memory.Corrup</td><td>Critical</td><td>CVE-2010-3231</td><td>40</td></tr><tr><td>8</td><td>Oracle.Outside.CDR.File.Parser.Integ</td><td>Critical</td><td>CVE-2011-3541</td><td>40</td></tr><tr><td>9</td><td>Apple.QuickTime.JPEG2000.COD.Le</td><td>Critical</td><td>CVE-2011-3250</td><td>32</td></tr><tr><td>10</td><td>Sophos.AV.RAR.VA.SF.RGB.Filter.P</td><td>Critical</td><td></td><td>30</td></tr></table>		#	Attack Name	Severity	CVE-ID	Counts	1	MS.Word.Linked.Objects.Memory.Corrup	Critical	CVE-2010-1903	80	2	MS.Publisher.Pubconv.dll.Pointer.Ove	Critical	CVE-2011-1508	40	3	MS.Visio.Invalid.Tag.Handling.Remot	Critical	CVE-2009-0096	40	4	MS.Windows.MPEG4.Codec.ASF.Par	Critical	CVE-2010-0818	40	5	Adobe.Reader.Font.Parsing.Integer.O	Critical	CVE-2010-2862	40	6	MS.Office.VBA.Module.Stream.Us	Critical		40	7	MS.Excel.Record.Parsing.Memory.Corrup	Critical	CVE-2010-3231	40	8	Oracle.Outside.CDR.File.Parser.Integ	Critical	CVE-2011-3541	40	9	Apple.QuickTime.JPEG2000.COD.Le	Critical	CVE-2011-3250	32	10	Sophos.AV.RAR.VA.SF.RGB.Filter.P	Critical		30
#	Attack Name	Severity	CVE-ID	Counts																																																						
1	MS.Word.Linked.Objects.Memory.Corrup	Critical	CVE-2010-1903	80																																																						
2	MS.Publisher.Pubconv.dll.Pointer.Ove	Critical	CVE-2011-1508	40																																																						
3	MS.Visio.Invalid.Tag.Handling.Remot	Critical	CVE-2009-0096	40																																																						
4	MS.Windows.MPEG4.Codec.ASF.Par	Critical	CVE-2010-0818	40																																																						
5	Adobe.Reader.Font.Parsing.Integer.O	Critical	CVE-2010-2862	40																																																						
6	MS.Office.VBA.Module.Stream.Us	Critical		40																																																						
7	MS.Excel.Record.Parsing.Memory.Corrup	Critical	CVE-2010-3231	40																																																						
8	Oracle.Outside.CDR.File.Parser.Integ	Critical	CVE-2011-3541	40																																																						
9	Apple.QuickTime.JPEG2000.COD.Le	Critical	CVE-2011-3250	32																																																						
10	Sophos.AV.RAR.VA.SF.RGB.Filter.P	Critical		30																																																						
		Malware																																																								
		Malware Detected																																																								
		<table><tr><th>#</th><th>Malware Name</th><th>Malware Type</th><th>Counts</th></tr><tr><td>1</td><td>MSOffice/CVE_2013_3906.B/exploit</td><td>Virus</td><td>60</td></tr><tr><td>2</td><td>MSWord/CVE20103333.A/exploit</td><td>Virus</td><td>40</td></tr><tr><td>3</td><td>PDF/Shellcode.NT/exploit</td><td>Virus</td><td>40</td></tr><tr><td>4</td><td>HTML/CVE_2011_2000.A/exploit</td><td>Virus</td><td>40</td></tr><tr><td>5</td><td>PDF/CVE_2010_2883.A/exploit</td><td>Virus</td><td>40</td></tr><tr><td>6</td><td>PDF/CVE_2011_2462.A/exploit</td><td>Virus</td><td>39</td></tr><tr><td>7</td><td>SWF/Font/exploit.CVE.20121535</td><td>Virus</td><td>30</td></tr><tr><td>8</td><td>virus_test</td><td>Virus</td><td>3</td></tr><tr><td>9</td><td>Riskware/UltraReach</td><td>Spyware</td><td>1</td></tr></table>		#	Malware Name	Malware Type	Counts	1	MSOffice/CVE_2013_3906.B/exploit	Virus	60	2	MSWord/CVE20103333.A/exploit	Virus	40	3	PDF/Shellcode.NT/exploit	Virus	40	4	HTML/CVE_2011_2000.A/exploit	Virus	40	5	PDF/CVE_2010_2883.A/exploit	Virus	40	6	PDF/CVE_2011_2462.A/exploit	Virus	39	7	SWF/Font/exploit.CVE.20121535	Virus	30	8	virus_test	Virus	3	9	Riskware/UltraReach	Spyware	1															
#	Malware Name	Malware Type	Counts																																																							
1	MSOffice/CVE_2013_3906.B/exploit	Virus	60																																																							
2	MSWord/CVE20103333.A/exploit	Virus	40																																																							
3	PDF/Shellcode.NT/exploit	Virus	40																																																							
4	HTML/CVE_2011_2000.A/exploit	Virus	40																																																							
5	PDF/CVE_2010_2883.A/exploit	Virus	40																																																							
6	PDF/CVE_2011_2462.A/exploit	Virus	39																																																							
7	SWF/Font/exploit.CVE.20121535	Virus	30																																																							
8	virus_test	Virus	3																																																							
9	Riskware/UltraReach	Spyware	1																																																							
Comentário																																																										
Assinatura do Cliente		Assinatura NCT																																																								

Item de Teste - 1.6.12.7	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelo dispositivo de segurança;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Apresentar Log & Report
Procedimento do Teste	Demonstrar Log view e FortiView
Evidências	

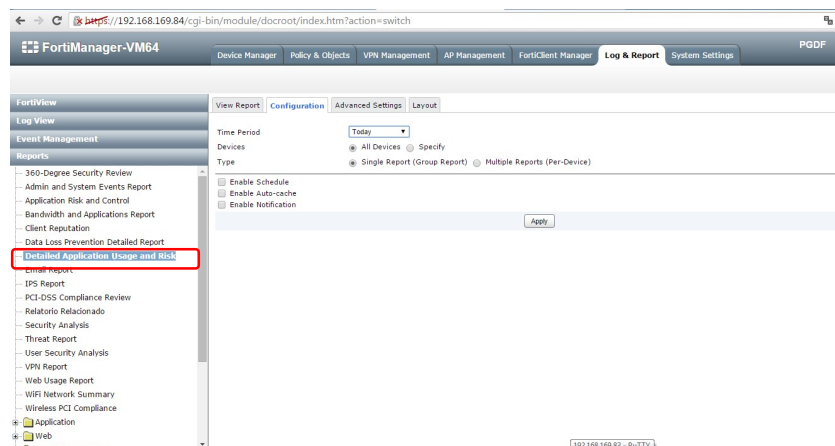


Comentário

Assinatura
do Cliente

Assinatura NCT

Item de Teste - 1.6.12.8	Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, antivírus e anti-spware) e etc.;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar a geração de relatório com as informações como solicitado neste item.
Procedimento do Teste	Gerar relatório e executar o download para mostra
Evidências	Gerado relatório específico para detalhado recurso de aplicações:



Alguns resultados extraídos do relatório de recursos de aplicação:

Application Bandwidth Usage

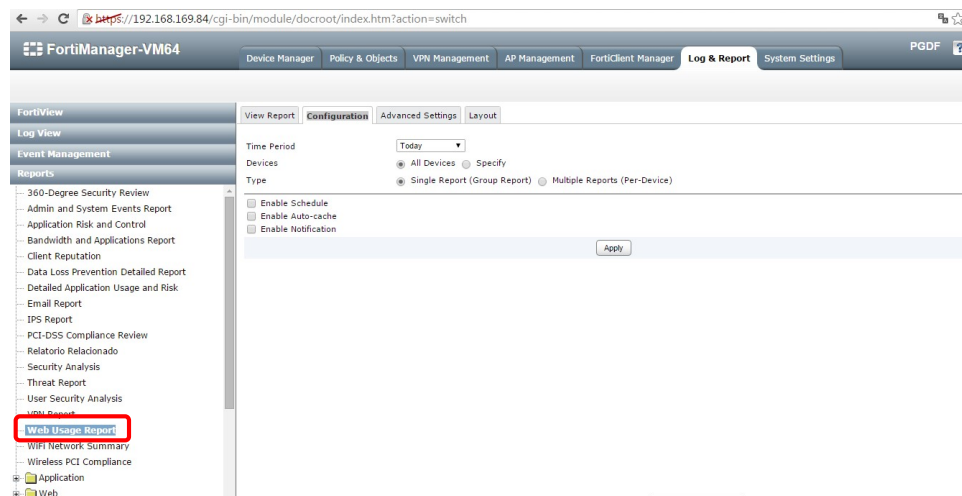
#	Application	Action	Bandwidth	Session Count
1	BitTorrent	Allowed	749.69 KB	1,517
2	BitTorrent	Blocked	260.36 KB	930
3	Bitcomet.HTTP Seed	Blocked	3.91 KB	149
4	Bitcomet.HTTP Seed	Allowed	880 B	6

Note: The above list presents the application combined total usage for the time period of this report.

Application Bandwidth Usage

#	Application	Action	Bandwidth	Session Count
1	HTTP.Download.Accelerator	Allowed	60.09 MB	4
2	Skype	Allowed	50.05 MB	3,663
3	Facebook	Allowed	20.50 MB	570
4	YouTube.Video.Play	Allowed	10.93 MB	4
5	Microsoft.Portals	Allowed	5.79 MB	41
6	Facebook.Chat	Allowed	3.94 MB	26
7	YouTube	Allowed	3.25 MB	34
8	FTP	Allowed	3.09 MB	60
9	Google.Search.Safe.Off	Allowed	2.29 MB	14
10	HTTP.Audio	Blocked	1.93 MB	110
11	Google.Accounts	Allowed	1.43 MB	114
12	Google.Search.Always.Instant.Show	Allowed	914.10 KB	5
13	Google.Hangouts	Allowed	782.64 KB	5
14	Facebook	Blocked	771.82 KB	51
15	Facebook.Chat.Message	Allowed	732.30 KB	1
16	Ping	Allowed	406.77 KB	11
17	Facebook.Chat.File.Upload	Allowed	388.72 KB	3
18	Google.Plus	Allowed	333.29 KB	5
19	Google.Login	Allowed	300.68 KB	2
20	Facebook.Chat	Blocked	288.28 KB	89
21	Google.Hangouts	Blocked	270.14 KB	13
22	Microsoft.CDN	Allowed	232.10 KB	17
23	HTTP.Video	Blocked	217.07 KB	40
24	HTTP.Audio	Allowed	190.44 KB	2
25	YouTube.Channel.Access	Allowed	177.84 KB	1
26	Teredo	Allowed	131.68 KB	8
27	Skype	Blocked	128.81 KB	120
28	Silverlight	Allowed	126.54 KB	4
29	LinkedIn	Allowed	119.02 KB	5
30	Google.Search	Allowed	114.20 KB	16
31	HTTP.Video	Allowed	112.55 KB	1
32	SSL.TLSv1.0	Allowed	98.23 KB	44
33	OCSP	Allowed	79.13 KB	25
34	Disqus	Allowed	66.75 KB	4
35	FTP	Blocked	57.30 KB	180

Gerado relatório específico para Filtro Web (URL):



Alguns resultados extraídos do relatório de recurso de Web:

Web Activity

Top 20 Most Active Users

#	User (or IP)	Requests
1	joaldir	1,594
2	10.69.70.65	478
3	10.69.70.222	169

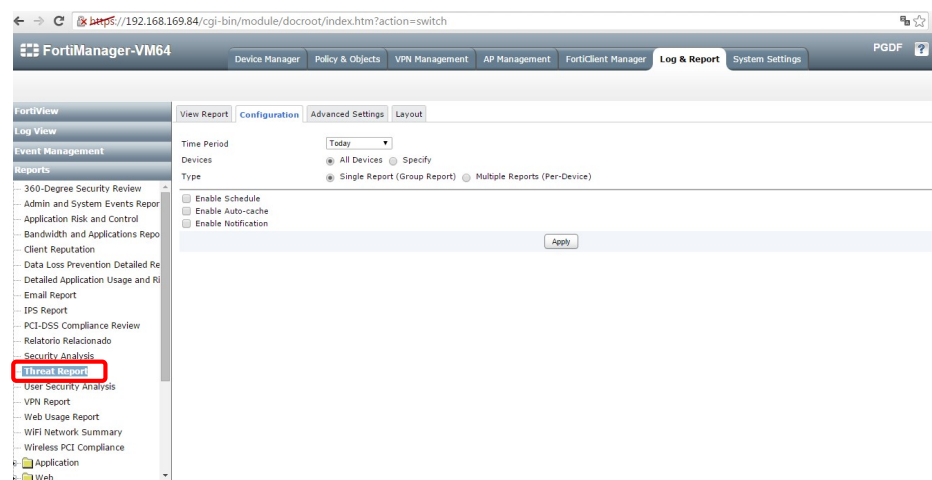
Top 20 Most Visited Categories

#	Category	Requests
1	Search Engines and Portals	653
2	Information Technology	439
3	Advertising	356
4	Content Servers	300
5	Business	139
6	Web-based Email	111
7	Streaming Media and Download	57
8	File Sharing and Storage	57
9	Finance and Banking	41
10	Meaningless Content	33
11	Peer-to-peer File Sharing	19
12	Social Networking	12
13	Proxy Avoidance	11
14	Domain Parking	8
15	Malicious Websites	3
16	Medicine	1
17	Real Estate	1

Top 50 Most Visited Sites

#	Website	Category	Requests
1	www.google.com	Business, Search Engines and Portals	139
2	beacon.rubiconproject.com	Information Technology	117
3	mail.google.com	Web-based Email	108
4	download.cdn.mozilla.net	Information Technology	97
5	www.google.com.br	Proxy Avoidance, Search Engines and Portals	83
6	hp.imguol.com.br	Content Servers	70
7	safebrowsing-cache.google.com	Search Engines and Portals	60
8	i.ytimg.com	Content Servers	57
9	cf.dropboxstatic.com	File Sharing and Storage	57
10	pagead2.googleadsyndication.com	Advertising	51
11	imguol.com	Content Servers	51
12	2.client-channel.google.com	Search Engines and Portals	41
13	unb.com	Finance and Banking	41
14	tpc.googleadsyndication.com	Search Engines and Portals	39
15	ssl.gstatic.com	Information Technology	37
16	tr2.terra.com	Search Engines and Portals	37
17	googleads.g.doubleclick.net	Advertising	37
18	rtax.criteo.com	Business	36
19	p.mtch.com	Advertising	36
20	bn.imguol.com	Information Technology	35
21	www.terraempresas.com.br	Business	33
22	cm.g.doubleclick.net	Advertising	30
23	apis.google.com	Search Engines and Portals	30
24	safebrowsing.clients.google.com	Search Engines and Portals	27
25	s.ytimg.com	Content Servers	26
26	accounts.google.com	Search Engines and Portals	26
27	www.youtube.com	Streaming Media and Download	24
28	cdn.btmmedianetwork.com	Advertising	24
29	userdup.com	Meaningless Content	19
30	skltn.mpmotion.com	Advertising	18
31	accounts.youtube.com	Streaming Media and Download	16
32	0.client-channel.google.com	Search Engines and Portals	16
33	pixel.wpstatz.com	Content Servers	15
34	b.sccrcaidresearch.com	Advertising	14
35	pixel.rubiconproject.com	Advertising	14
36	1.client-channel.google.com	Search Engines and Portals	14
37	csi.gstatic.com	Content Servers	13
38	fonts.gstatic.com	Information Technology	13

Gerado relatório específico para detalhado de ameaça:



The screenshot shows the FortiManager-VM64 web interface. The top navigation bar includes tabs for Device Manager, Policy & Objects, VPN Management, AP Management, FortiClient Manager, Log & Report, and System Settings. The 'Log & Report' tab is active. On the left, the 'Reports' sidebar lists various reports, with 'Threat Report' highlighted under the 'Security Analysis' section. The main content area shows the 'Threat Report' configuration page with options for 'Time Period' (Today), 'Devices' (All Devices, Specify), and 'Type' (Single Report (Group Report), Multiple Reports (Per-Device)). There are checkboxes for 'Enable Schedule', 'Enable Auto-cache', and 'Enable Notification', and an 'Apply' button.

Alguns resultados extraídos do relatório de ameaça:

Malware Detected

#	Malware Name	Malware Type	Counts
1	MSOffice/CVE_2013_3906.B/exploit	Virus	60
2	MSWord/CVE20103333.A/exploit	Virus	40
3	PDF/Shellcode.NT/exploit	Virus	40
4	HTML/CVE_2011_2000.A/exploit	Virus	40
5	PDF/CVE_2010_2883.A/exploit	Virus	40
6	PDF/CVE_2011_2462.A/exploit	Virus	39
7	SWF/Font/exploit.CVE20121535	Virus	30
8	virus_test	Virus	3
9	Riskware/UltraReach	Spyware	1

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 97/126

Intrusions

Intrusions Detected

#	Attack Name	Severity	CVE-ID	Counts
1	MS Word Linked Objects Memory Corruption	Critical	CVE-2010-1903	80
2	MS Publisher Pubconv.dll Pointer Overflow Memory Corruption	Critical	CVE-2011-1508	40
3	MS Visio Invalid Tag Handling Remote Code Execution	Critical	CVE-2009-0096	40
4	MS Windows MPEG4 Codec ASF Parsing Code Execution	Critical	CVE-2010-0818	40
5	Adobe Reader Font Parsing Integer Overflow	Critical	CVE-2010-2862	40
6	MS Office VBA Module Stream Use After Free Memory Corruption	Critical		40
7	MS Excel Record Parsing Memory Corruption	Critical	CVE-2010-3331	40
8	Oracle Outside CDR File Parser Integer Overflow	Critical	CVE-2011-3541	40
9	Apple QuickTime JPEG2000 COD Length Integer Underflow	Critical	CVE-2011-3250	32
10	Sophos AV RAR VMSF RGB Filter Parsing Remote Code Execution	Critical		30

Intrusion Victims

#	Attack Victim	Counts
1	172.26.10.14	370
2	172.25.10.13	39
3	172.25.10.43	39
4	172.25.10.137	39
5	172.25.10.115	39
6	172.25.10.139	39
7	172.25.10.76	39
8	172.25.10.196	39
9	172.25.10.17	39
10	172.25.10.138	39

Intrusion Sources

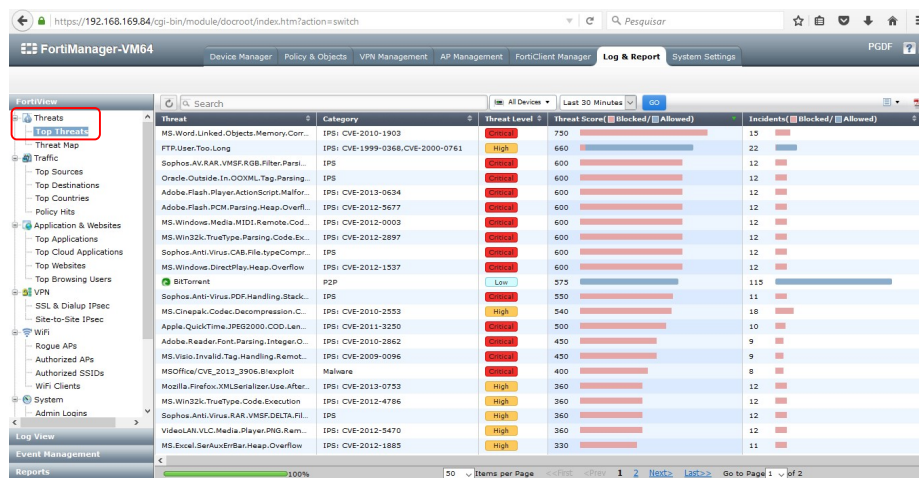
#	Attack Source	Counts
1	172.26.10.14	1,384
2	172.25.10.115	12
3	172.25.10.195	12
4	172.25.10.194	12
5	172.25.10.77	12
6	172.25.10.175	12
7	172.25.10.95	12
8	172.25.10.196	12
9	172.25.10.114	12
10	172.25.10.91	12

Comentário

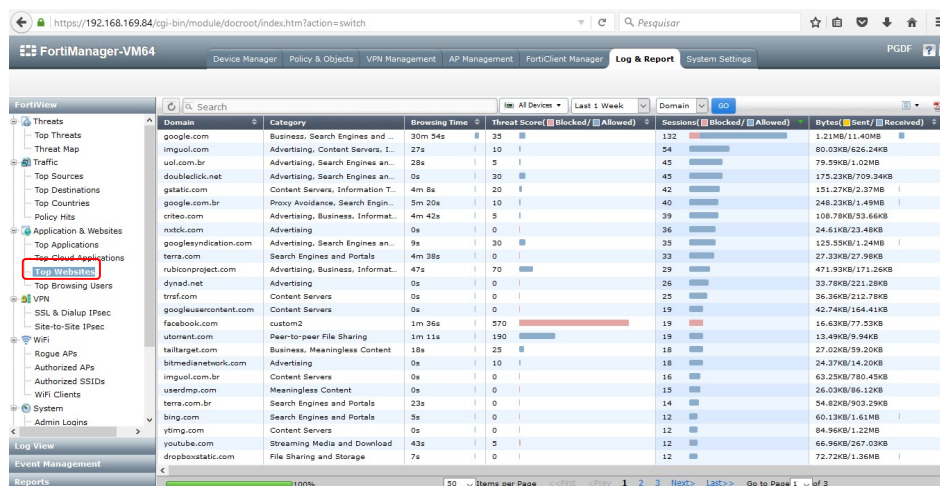
Assinatura do Cliente

Assinatura NCT

Item de Teste - 1.6.12.9	Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus e anti-spware) e URLs que passaram pela solução;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Acessar a aba do Fortiview referente a dados de segurança, a qual ira apresentar todos estes componentes solicitados.
Procedimento do Teste	Executar teste de filtros e drill-down dos dados listados sumarizados .
Evidências	



Sumário de ameaças



Sumário web

Comentário

Assinatura
do Cliente

Assinatura NCT

Item de Teste -
1.6.12.10

Deve possuir mecanismo "drill-down" para navegação nos relatórios em tempo real;

Objetivo do
Teste

Demonstrar funcionalidade conforme solicitado

Configuração do
Teste

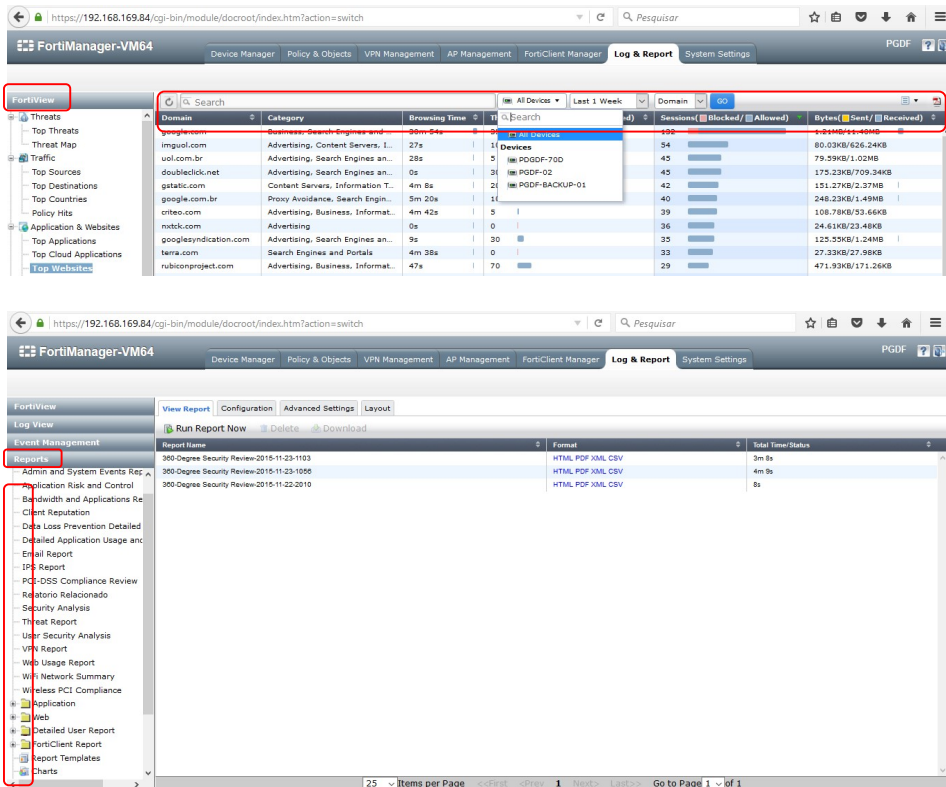
A partir aba Fortiview e Log&Report em qualquer uma dos módulos de sumarização clicar com o botão direito para executar um drill-down, para várias instancias de analise, ou expandir os reports para acesso as informações.

Procedimento
do Teste

Executar uma demonstração de drill-down conforme solicitado

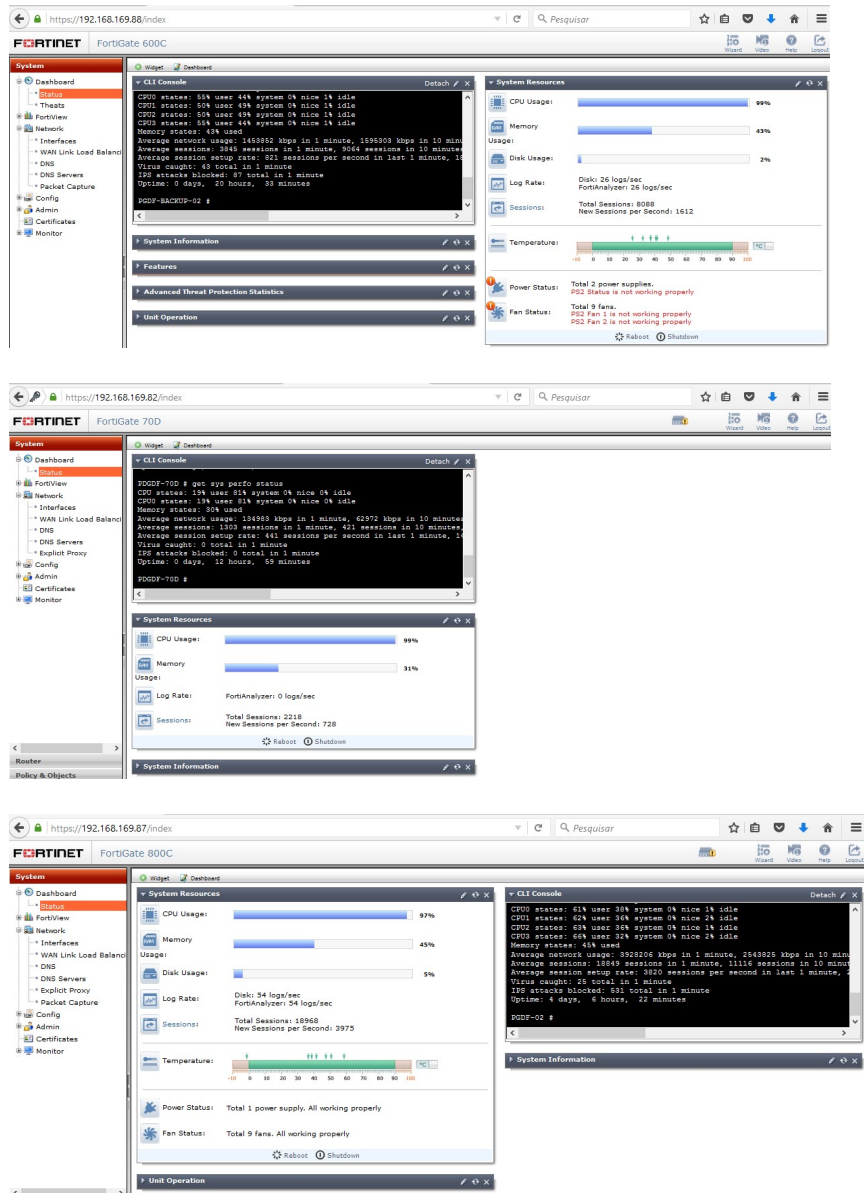
Evidências

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 99/126

	
Comentário	
Assinatura do Cliente	Assinatura NCT

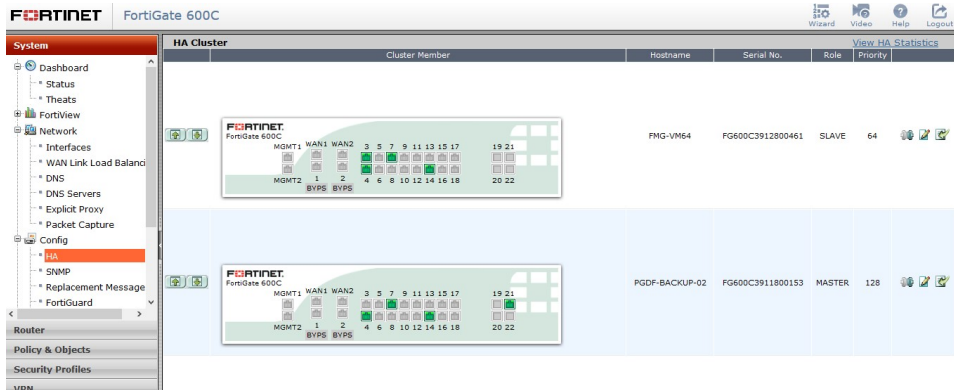
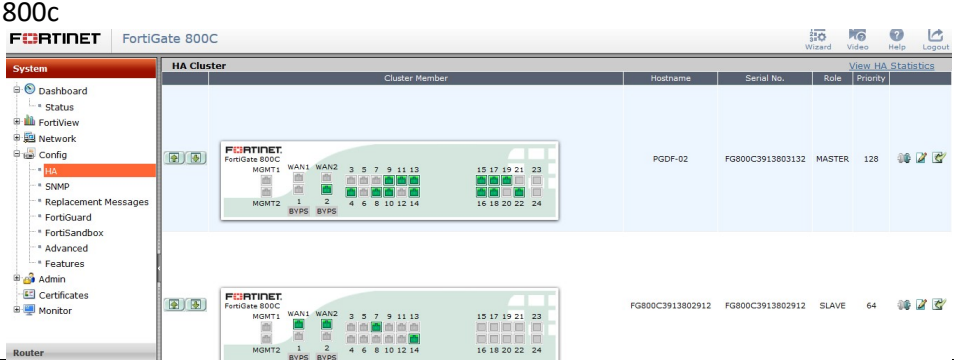
Item de Teste - 1.6.12.13	Deverá ser possível acessar a gerencia para visualizar ou aplicar configurações durante os momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiverem com taxas maiores que 99% de utilização;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Executar o teste conforme o solicitado
Procedimento do Teste	Durante todos os testes de performance dos equipamentos FGT 70D, FGT 600C e FGT 800C o processamento chegou aos níveis solicitados. Foi demonstrado a todos os presentes que todos os equipamentos continuavam operacionais aceitando alterações nos mesmos.
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 100/126

		Comentário	
Assinatura do Cliente		Assinatura NCT	

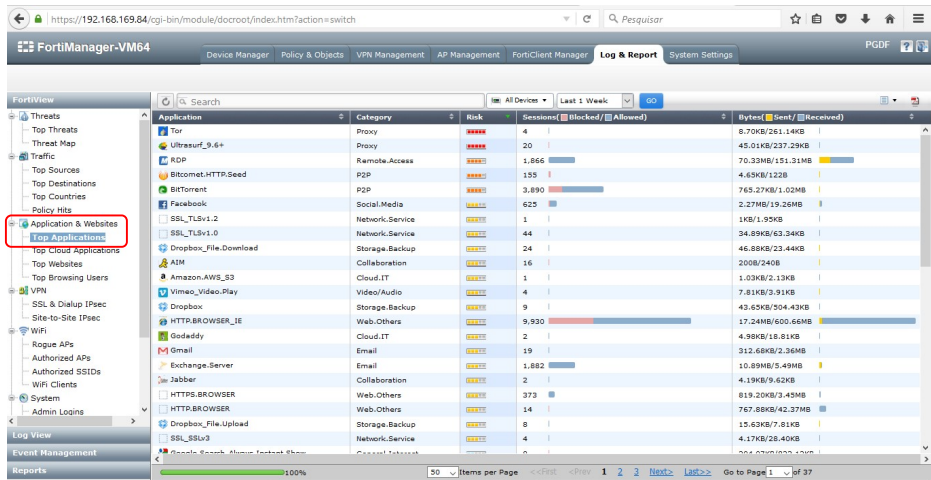
Item de Teste - 1.6.12.15.1	Situação do dispositivo e do cluster;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Equipamentos em HA
Procedimento do Teste	Demonstrar o status dos equipamentos na tela de monitor HA em ambos os cluster 600c e 800c

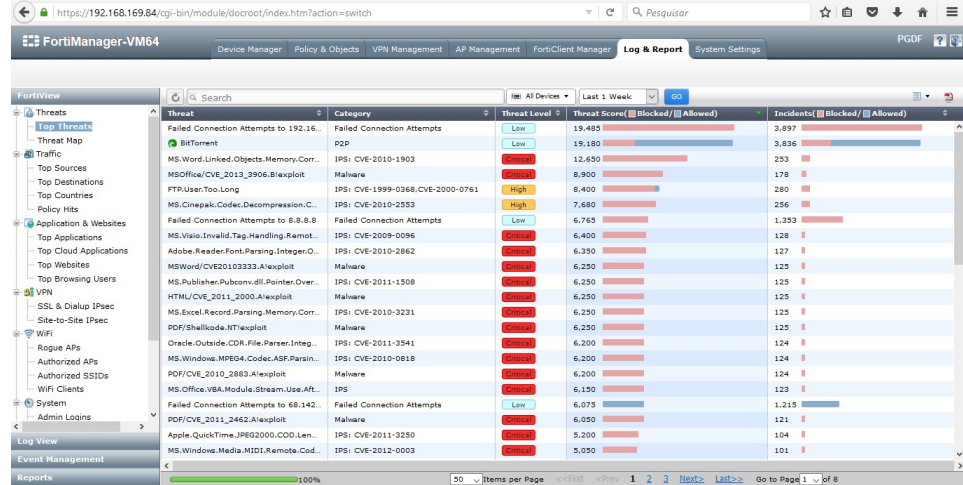
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 101/126

Evidências	600C 		
	800c 		
Comentário			
Assinatura do Cliente	Assinatura NCT		

Item de Teste - 1.6.12.15.2	Principais aplicações;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Na aba de FortiView abrir a tela de "application"
Procedimento do Teste	Mostrar a tela do FortiView
Evidências	

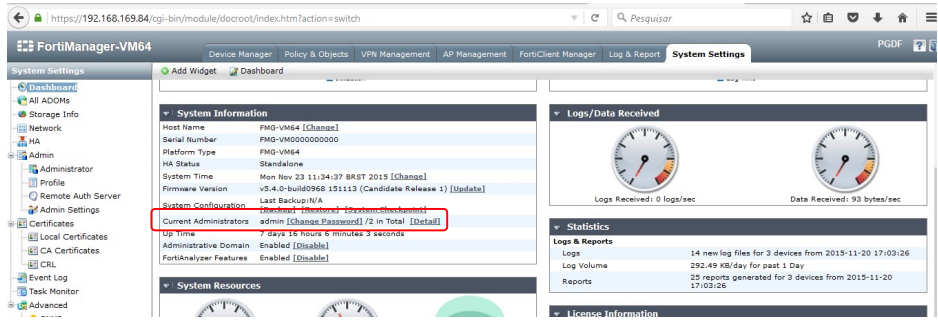
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 102/126

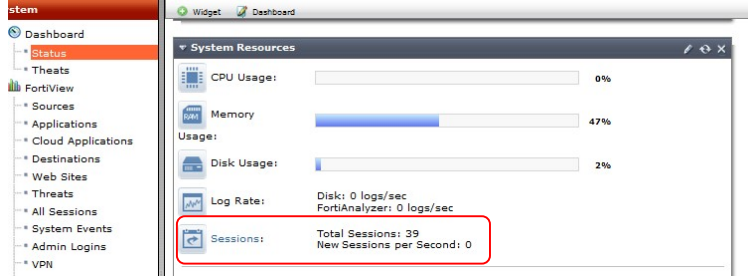
		Comentário	
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.12.15.3	Principais aplicações por risco;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Verificar no FortiView "Top Threats"		
Procedimento do Teste	Demonstrar o FortiView		
Evidências			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste -	Administradores autenticados na gerência da plataforma de segurança;
------------------------	--

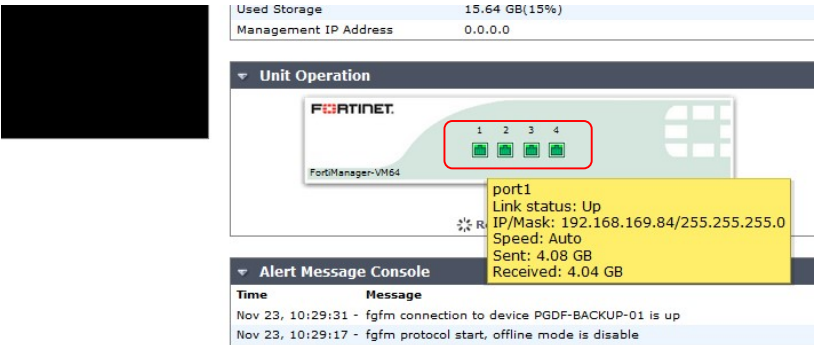
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 103/126

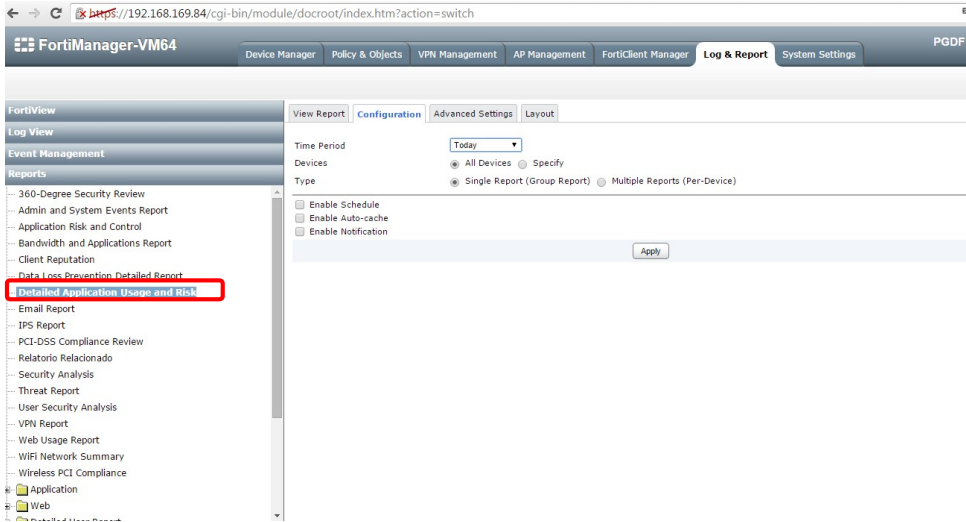
1.6.12.15.4	
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	No dashboard no widget "system information" há uma referência chamada "Current Administrator" que mostra quantos administradores logados.
Procedimento do Teste	Mostrar os administradores locais cadastrados
Evidências	
Comentário	
Assinatura do Cliente	Assinatura NCT

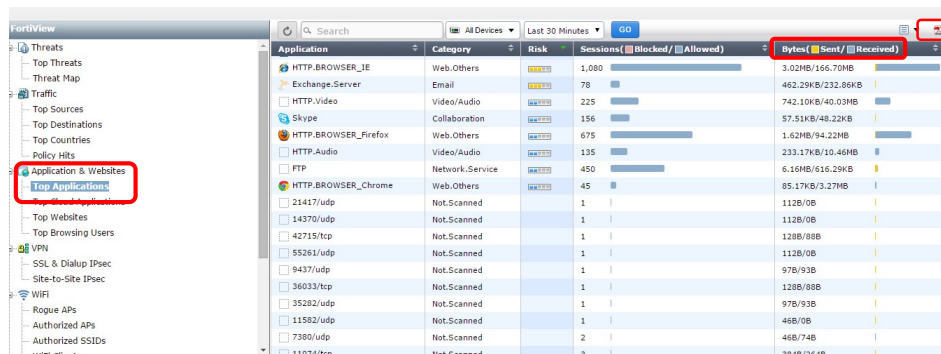
Item de Teste - 1.6.12.15.5	Número de sessões simultâneas;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	No dashboard no widget "system resource"
Procedimento do Teste	Mostrar o painel de system resource mostrar as informações conforme solicitado
Evidências	
Comentário	
Assinatura do Cliente	Assinatura NCT

Item de Teste - 1.6.12.15.6	Status das interfaces;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	No dashboard no widget "operation unit"
Procedimento do Teste	Mostra o status de todas as interfaces na imagem do próprio equipamento
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 104/126

			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.12.16.1	Resumo gráfico de aplicações utilizadas;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurado no modulo de "report" o relatório correspondente "application"
Procedimento do Teste	Gerado o relatório de uso de aplicações
Evidências	Executado a criação do relatório de uso de aplicação:  Resultado desse relatório correspondente ao uso de aplicação por consumo de banda:



Resultado do relatório extraído do FortiView:

Top Application				
Application	Category	Risk	Sessions (Blocked/Allowed)	Bytes (Sent/Received)
BitTorrent	P2P	High	78	21.18KB/22.17KB
RDP	Remote.Access	High	78	2.94MB/6.32MB
HTTP.BROWSER_IE	Web.Others	Low	1,080	3.02MB/166.70MB
Exchange.Server	Email	Low	78	462.29KB/232.86KB
HTTP.Video	Video/Audio	Low	225	742.10KB/40.03MB
Skype	Collaboration	Low	156	57.51KB/48.22KB
HTTP.BROWSER_Firefox	Web.Others	Low	675	1.62MB/94.22MB
HTTP.Audio	Video/Audio	Low	135	233.17KB/10.46MB
FTP	Network.Service	Low	450	6.16MB/616.29KB
HTTP.BROWSER_Chrome	Web.Others	Low	45	85.17KB/3.27MB
21417/udp	Not.Scanned	Low	1	112B/0B
14370/udp	Not.Scanned	Low	1	112B/0B
42715/tcp	Not.Scanned	Low	1	128B/88B
55261/udp	Not.Scanned	Low	1	112B/0B
9437/udp	Not.Scanned	Low	1	97B/93B
36033/tcp	Not.Scanned	Low	1	128B/88B
35282/udp	Not.Scanned	Low	1	97B/93B
11582/udp	Not.Scanned	Low	1	46B/0B
7380/udp	Not.Scanned	Low	2	46B/74B
11074/tcp	Not.Scanned	Low	3	384B/264B
9958/tcp	Not.Scanned	Low	1	128B/88B
32709/udp	Not.Scanned	Low	1	112B/0B
36513/tcp	Not.Scanned	Low	5	240B/200B
14359/udp	Not.Scanned	Low	1	112B/0B
31201/udp	Not.Scanned	Low	1	112B/0B
14736/tcp	Not.Scanned	Low	1	128B/88B
53571/tcp	Not.Scanned	Low	1	128B/88B

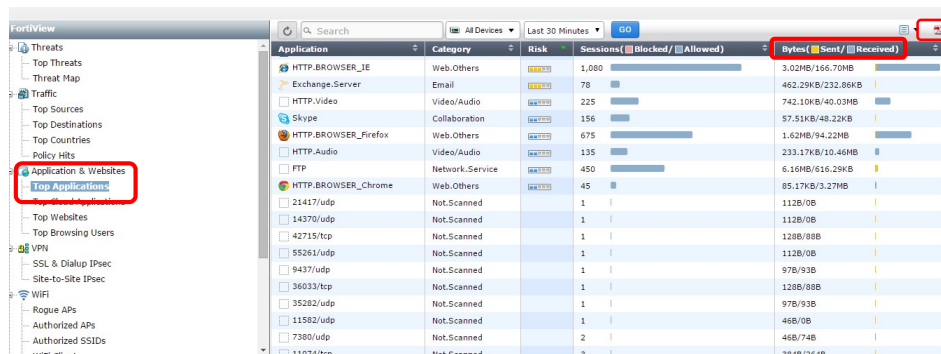
Evidências

Comentário

Assinatura
do Cliente

Assinatura NCT

Item de Teste - 1.6.12.16.3	Principais aplicações por taxa de transferência de bytes;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar no modulo de "report" o relatório correspondente conforme solicitado neste item
Procedimento do Teste	Gerar o relatório de utilização de aplicação por consumo de banda de saída e entrada:



Application	Category	Risk	Sessions (Blocked/Allowed)	Bytes (Sent/Received)
HTTP.BROWSER_IE	Web.Others	Low	1,080	3.02MB/166.70MB
Exchange.Server	Email	Low	78	462.29KB/232.86KB
HTTP.Video	Video/Audio	Low	225	742.10KB/40.03MB
Skype	Collaboration	Low	156	57.51KB/48.22KB
HTTP.BROWSER_Firefox	Web.Others	Low	675	1.62MB/94.22MB
HTTP.Audio	Video/Audio	Low	135	233.17KB/10.46MB
FTP	Network.Service	Low	450	6.16MB/616.29KB
HTTP.BROWSER_Chrome	Web.Others	Low	45	85.17KB/3.27MB
21417/udp	Not.Scanned	Low	1	112B/0B
14370/udp	Not.Scanned	Low	1	112B/0B
42715/tcp	Not.Scanned	Low	1	128B/88B
55261/udp	Not.Scanned	Low	1	112B/0B
9437/udp	Not.Scanned	Low	1	97B/93B
36033/tcp	Not.Scanned	Low	1	128B/88B
35282/udp	Not.Scanned	Low	1	97B/93B
11582/udp	Not.Scanned	Low	1	46B/0B
7380/udp	Not.Scanned	Low	2	46B/74B
11074/tcp	Not.Scanned	Low	3	384B/264B

Resultado do relatório extraído do FortiView:

Top Application

Application	Category	Risk	Sessions (Blocked/Allowed)	Bytes (Sent/Received)
BitTorrent	P2P	High	78	21.18KB/22.17KB
RDP	Remote.Access	High	78	2.94MB/6.32MB
HTTP.BROWSER_IE	Web.Others	Low	1,080	3.02MB/166.70MB
Exchange.Server	Email	Low	78	462.29KB/232.86KB
HTTP.Video	Video/Audio	Low	225	742.10KB/40.03MB
Skype	Collaboration	Low	156	57.51KB/48.22KB
HTTP.BROWSER_Firefox	Web.Others	Low	675	1.62MB/94.22MB
HTTP.Audio	Video/Audio	Low	135	233.17KB/10.46MB
FTP	Network.Service	Low	450	6.16MB/616.29KB
HTTP.BROWSER_Chrome	Web.Others	Low	45	85.17KB/3.27MB
21417/udp	Not.Scanned	Low	1	112B/0B
14370/udp	Not.Scanned	Low	1	112B/0B
42715/tcp	Not.Scanned	Low	1	128B/88B
55261/udp	Not.Scanned	Low	1	112B/0B
9437/udp	Not.Scanned	Low	1	97B/93B
36033/tcp	Not.Scanned	Low	1	128B/88B
35282/udp	Not.Scanned	Low	1	97B/93B
11582/udp	Not.Scanned	Low	1	46B/0B
7380/udp	Not.Scanned	Low	2	46B/74B
11074/tcp	Not.Scanned	Low	3	384B/264B
9958/tcp	Not.Scanned	Low	1	128B/88B
32709/udp	Not.Scanned	Low	1	112B/0B
36513/tcp	Not.Scanned	Low	5	240B/200B
14359/udp	Not.Scanned	Low	1	112B/0B
31201/udp	Not.Scanned	Low	1	112B/0B
14736/tcp	Not.Scanned	Low	1	128B/88B
53571/tcp	Not.Scanned	Low	1	128B/88B

Evidências

Comentário

Assinatura
do Cliente

Assinatura NCT

Item de Teste -
1.6.12.16.4

Principais hosts por número de ameaças identificadas;

Objetivo do Teste

Demonstrar funcionalidade conforme solicitado

Configuração do
Teste

Configurar no modulo de "report" o relatório correspondente conforme solicitado neste item

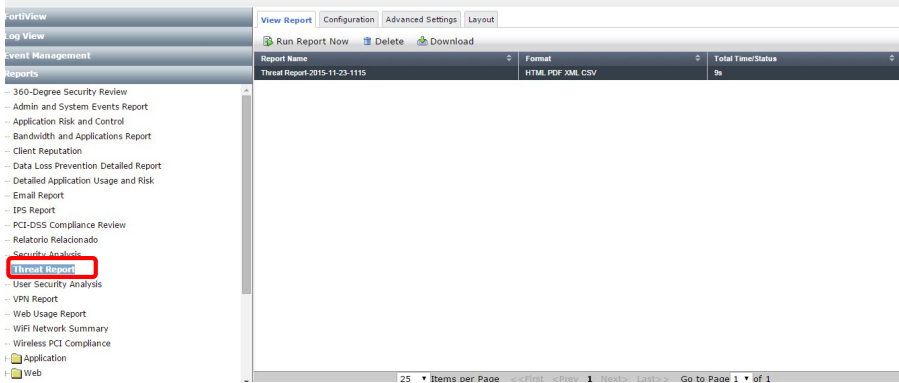
Procedimento do
Teste

Gerar o relatório ameaças

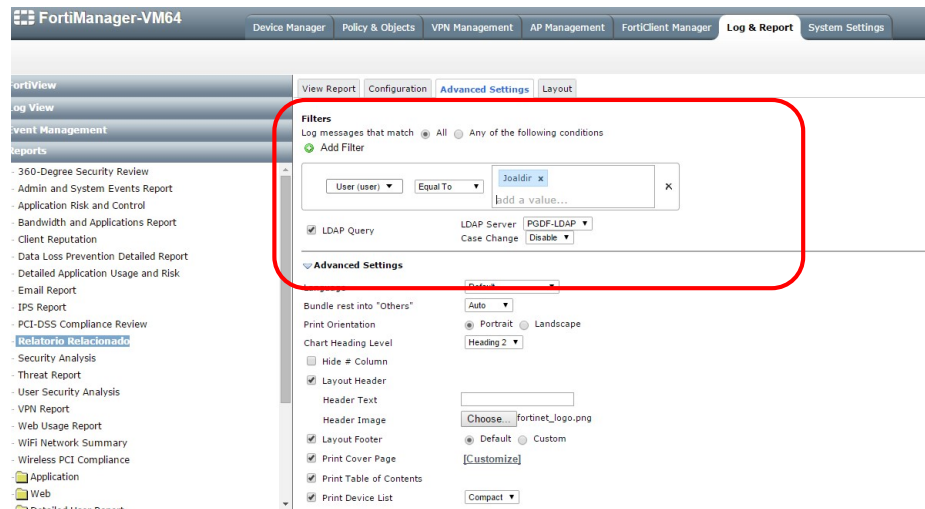
Evidências

Executado relatório de ameaças:

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 108/126

																																																																																															
Resultado extraído do relatório: Malware Victims <table border="1"> <thead> <tr> <th>#</th> <th>Victim Name (or IP)</th> <th>Counts</th> </tr> </thead> <tbody> <tr><td>1</td><td>172.25.10.13</td><td>8</td></tr> <tr><td>2</td><td>172.25.10.115</td><td>8</td></tr> <tr><td>3</td><td>172.25.10.195</td><td>8</td></tr> <tr><td>4</td><td>172.25.10.194</td><td>8</td></tr> <tr><td>5</td><td>172.25.10.77</td><td>8</td></tr> <tr><td>6</td><td>172.25.10.95</td><td>8</td></tr> <tr><td>7</td><td>172.25.10.175</td><td>8</td></tr> <tr><td>8</td><td>172.25.10.196</td><td>8</td></tr> <tr><td>9</td><td>172.25.10.114</td><td>8</td></tr> <tr><td>10</td><td>172.25.10.93</td><td>8</td></tr> <tr><td>11</td><td>172.25.10.74</td><td>8</td></tr> <tr><td>12</td><td>172.25.10.91</td><td>8</td></tr> <tr><td>13</td><td>172.25.10.44</td><td>8</td></tr> <tr><td>14</td><td>172.25.10.139</td><td>8</td></tr> <tr><td>15</td><td>172.25.10.217</td><td>8</td></tr> <tr><td>16</td><td>172.25.10.15</td><td>8</td></tr> <tr><td>17</td><td>172.25.10.42</td><td>8</td></tr> <tr><td>18</td><td>172.25.10.73</td><td>8</td></tr> <tr><td>19</td><td>172.25.10.137</td><td>8</td></tr> <tr><td>20</td><td>172.25.10.17</td><td>8</td></tr> <tr><td>21</td><td>172.25.10.45</td><td>8</td></tr> <tr><td>22</td><td>172.25.10.116</td><td>8</td></tr> <tr><td>23</td><td>172.25.10.11</td><td>8</td></tr> <tr><td>24</td><td>172.25.10.173</td><td>8</td></tr> <tr><td>25</td><td>172.25.10.76</td><td>8</td></tr> <tr><td>26</td><td>172.25.10.43</td><td>8</td></tr> <tr><td>27</td><td>172.25.10.138</td><td>8</td></tr> <tr><td>28</td><td>172.25.10.220</td><td>8</td></tr> <tr><td>29</td><td>172.25.10.219</td><td>8</td></tr> <tr><td>30</td><td>172.25.10.171</td><td>8</td></tr> </tbody> </table>			#	Victim Name (or IP)	Counts	1	172.25.10.13	8	2	172.25.10.115	8	3	172.25.10.195	8	4	172.25.10.194	8	5	172.25.10.77	8	6	172.25.10.95	8	7	172.25.10.175	8	8	172.25.10.196	8	9	172.25.10.114	8	10	172.25.10.93	8	11	172.25.10.74	8	12	172.25.10.91	8	13	172.25.10.44	8	14	172.25.10.139	8	15	172.25.10.217	8	16	172.25.10.15	8	17	172.25.10.42	8	18	172.25.10.73	8	19	172.25.10.137	8	20	172.25.10.17	8	21	172.25.10.45	8	22	172.25.10.116	8	23	172.25.10.11	8	24	172.25.10.173	8	25	172.25.10.76	8	26	172.25.10.43	8	27	172.25.10.138	8	28	172.25.10.220	8	29	172.25.10.219	8	30	172.25.10.171	8
#	Victim Name (or IP)	Counts																																																																																													
1	172.25.10.13	8																																																																																													
2	172.25.10.115	8																																																																																													
3	172.25.10.195	8																																																																																													
4	172.25.10.194	8																																																																																													
5	172.25.10.77	8																																																																																													
6	172.25.10.95	8																																																																																													
7	172.25.10.175	8																																																																																													
8	172.25.10.196	8																																																																																													
9	172.25.10.114	8																																																																																													
10	172.25.10.93	8																																																																																													
11	172.25.10.74	8																																																																																													
12	172.25.10.91	8																																																																																													
13	172.25.10.44	8																																																																																													
14	172.25.10.139	8																																																																																													
15	172.25.10.217	8																																																																																													
16	172.25.10.15	8																																																																																													
17	172.25.10.42	8																																																																																													
18	172.25.10.73	8																																																																																													
19	172.25.10.137	8																																																																																													
20	172.25.10.17	8																																																																																													
21	172.25.10.45	8																																																																																													
22	172.25.10.116	8																																																																																													
23	172.25.10.11	8																																																																																													
24	172.25.10.173	8																																																																																													
25	172.25.10.76	8																																																																																													
26	172.25.10.43	8																																																																																													
27	172.25.10.138	8																																																																																													
28	172.25.10.220	8																																																																																													
29	172.25.10.219	8																																																																																													
30	172.25.10.171	8																																																																																													
Comentário																																																																																															
Assinatura do Cliente		Assinatura NCT																																																																																													

Item de Teste - 1.6.12.16.5	Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL e tempo de utilização e ameaças (IPS, antivírus e anti-spware) vinculadas a este tráfego
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar no modulo de "report" o relatório correspondente conforme solicitado neste item
Procedimento do Teste	Gerar o relatório
Evidências	Executado a geração do relatório especificando o usuário específico autenticado pelo equipamento usando credenciais do AD fazendo uma consulta via LDAP:



Relatório feito filtrando o usuário Joaldir, que é um usuário autenticado pelo AD:

#	Victim Name (or IP)	Counts
41	User	3
42	joaldir	1

Web Activity

Top 20 Most Active Users

#	User (or IP)	Requests
1	joaldir	1,594

Web Browsing

Top 10 Online Users

#	User (or IP)	Browsing Time(hh:mm:ss)
1	joaldir	00:56:42

Report Filters(Logic: All)

#	Filter name	Value
1	User	include (joaldir)

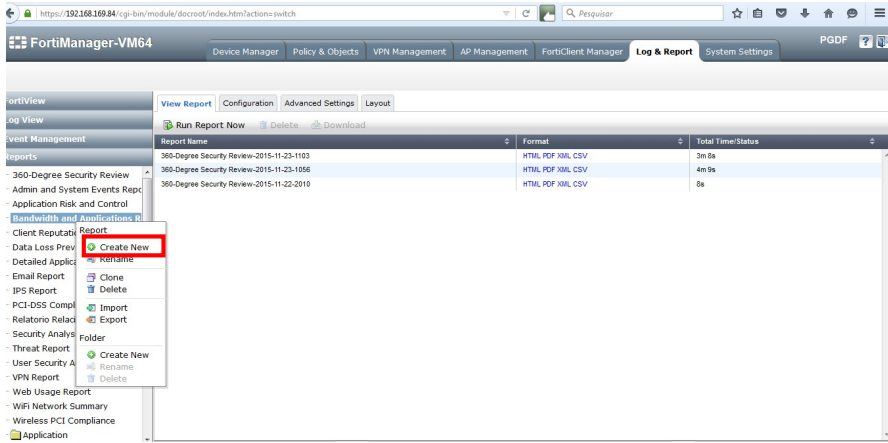
#	Website	Category	Bandwidth
1	download.cdn.mozilla.net	Information Technology	17.67 MB
2	mail.google.com	Web-based Email	2.59 MB
3	cf.dropboxstatic.com	File Sharing and Storage	1.43 MB
4	ssl.gstatic.com	Information Technology	1.15 MB
5	www.google.com.br	Search Engines and Portals	882.76 KB
6	lp.ingul.com.br	Content Servers	843.70 KB
7	www.uol.com.br	Search Engines and Portals	792.93 KB
8	tpc.googleusercontent.com	Search Engines and Portals	713.45 KB
9	hangouts.google.com	Search Engines and Portals	688.48 KB
10	apis.google.com	Search Engines and Portals	575.07 KB
11	www.terra.com.br	Search Engines and Portals	526.95 KB
12	securepubads.g.doubleclick.net	Advertising	524.02 KB
13	bn.ingul.com	Information Technology	443.09 KB
14	safebrowsing-cache.google.com	Search Engines and Portals	395.66 KB
15	accounts.google.com	Search Engines and Portals	376.95 KB
16	pagead2.googleusercontent.com	Advertising	344.87 KB
17	plus.google.com	Social Networking	334.79 KB
18	www.gstatic.com	Information Technology	327.22 KB
19	beacon.rubiconproject.com	Information Technology	320.42 KB
20	fonts.gstatic.com	Information Technology	240.97 KB
21	ingul.com	Content Servers	228.20 KB
22	www.google.com	Search Engines and Portals	189.45 KB
23	rtax.criteo.com	Business	141.83 KB
24	akhtml.msnmotion.com	Advertising	129.16 KB
25	www.google.com	Business	125.73 KB
26	stc.uol.com	Search Engines and Portals	98.18 KB
27	s.dynad.net	Advertising	95.34 KB
28	0.client-chomel.google.com	Search Engines and Portals	94.17 KB

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 110/126

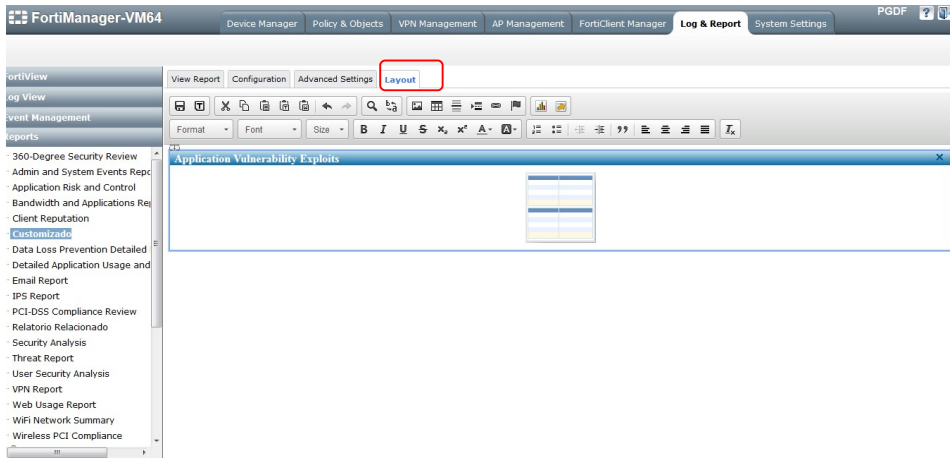
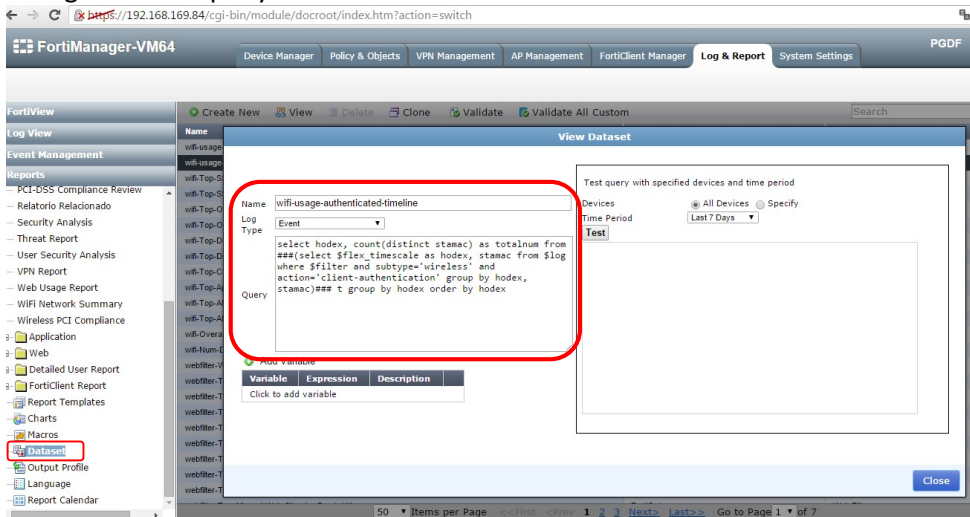
#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	2	HTTP.BROWSER_Firefox	Web.Client	Browser-Based	1	9.89 MB	404
2	3	HTTPS.BROWSER	Web.Client	Network-Protocol	1	263.60 KB	59
3	2	Google.Search_Safe.Off	General.Interest	Browser-Based	1	255.87 KB	2
4	3	Dropbox	Storage.Backup	Browser-Based	1	214.03 KB	3
5	3	HTTP.BROWSER_JE	Web.Client	Browser-Based	1	179.72 KB	79
6	5	Ultrasturf_9.6+	Proxy	Client-Server	1	158.04 KB	13
7	4	BitTorrent	P2P	Peer-to-Peer	2	133.71 KB	539
8	2	Skype	Collaboration	Peer-to-Peer	2	110.02 KB	113
9	2	Google.Search	General.Interest	Browser-Based	1	76.35 KB	8
10	3	Facebook	Social.Media	Browser-Based	1	58.87 KB	34
11	2	Silverlight	Network.Service	Browser-Based	1	25.87 KB	1
12	2	Google.Accounts	General.Interest	Browser-Based	1	22.44 KB	6
13	2	Google.Search_Always.Instant.Show	General.Interest	Browser-Based	1	12.86 KB	1
14	2	Teredo	Network.Service	Network-Protocol	1	11.01 KB	1
15	2	OCSP	Network.Service	Network-Protocol	1	8.18 KB	3
16	3	Amazon.AWS_S3	Cloud.IT	Browser-Based	1	3.16 KB	1
17	2	YouTube_Video.Embedded	Video.Audio	Browser-Based	1	3.10 KB	1
18	2	Twitter	Social.Media	Browser-Based	1	2.94 KB	21
19	4	Bitcomet.HTTP.Seed	P2P	Peer-to-Peer	1	176 B	8

Comentário

Assinatura do Cliente		Assinatura NCT	
------------------------------	--	-----------------------	--

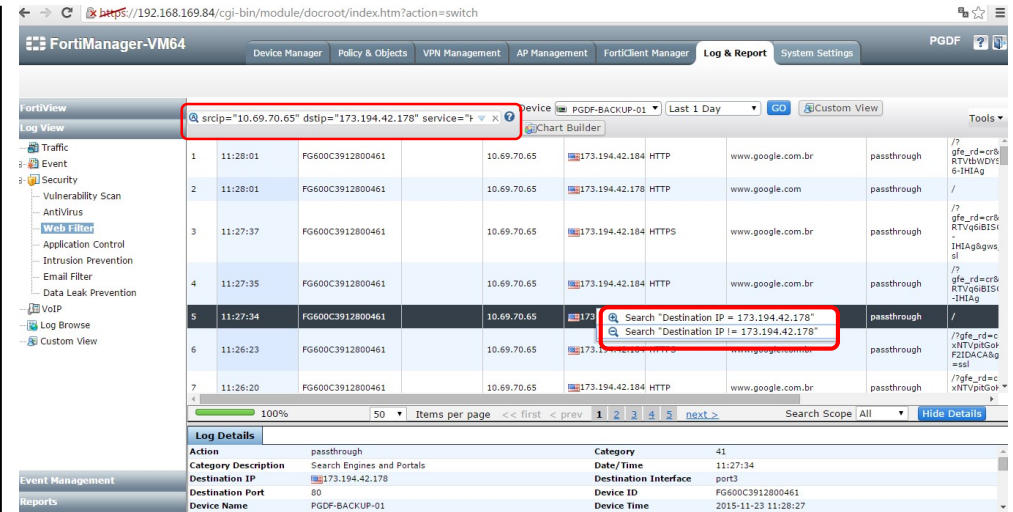
Item de Teste - 1.6.12.16.6	Deve permitir a criação de relatórios personalizados;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar no modulo de "report" um relatório com os charts e datasets customizados.
Procedimento do Teste	Gerar o relatório personalizado
Evidências	Criar um novo relatório:  Editando um novo layout:

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 111/126

		
Configurar uma query SQL customizada : 		
Comentário		
Assinatura do Cliente	Assinatura NCT	

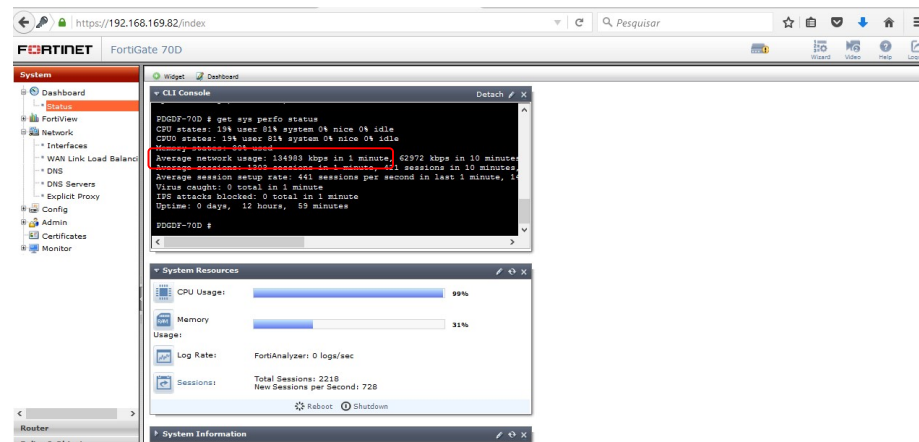
Item de Teste - 1.6.12.17	Em cada critério de pesquisa do log, deve ser possível incluir múltiplas entradas (por exemplo, 10 redes e IPs distintos, serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurado o pesquisa de log por variados origens , destinos e serviços como conforme solicitado
Procedimento do Teste	Gerado o filtro no log de Webfilter " srcip="10.69.70.65" dstip="173.194.42.178" service="HTTP" service="HTTPS" dstip="173.194.42.178" dstip="173.194.42.184" dstip="173.194.42.184"

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 112/126

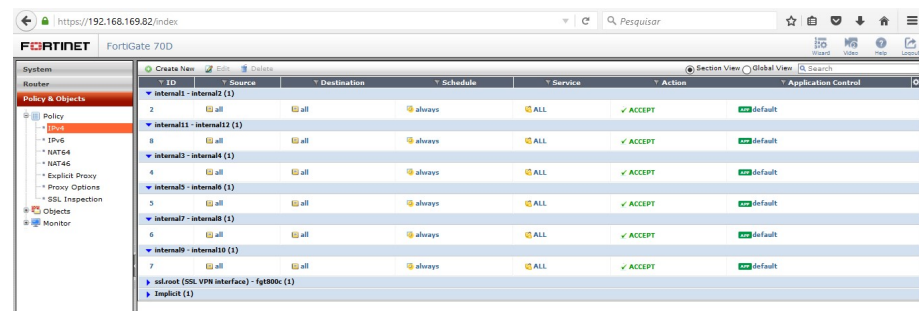
		
Evidências		
Comentário		
Assinatura do Cliente	Assinatura NCT	

CARACTERÍSTICAS ESPECÍFICAS PARA OS 2 (DOIS) EQUIPAMENTOS STANDALONE QUE CONECTARÃO OS ESCRITÓRIOS REMOTOS:

Item de Teste - 1.7.1.1	Throughput mínimo de 100 Mbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Foi configurado sensor de APP control as configurações de base e assinaturas default: -Sensor de APP control habilitado com todas as categorias de aplicações disponíveis no dia do teste. O sensor foi habilitado em todas as regras onde o tráfego foi gerado. O spirent foi configurado com os parâmetros de tráfego já descritos nesse caderno de testes.
Procedimento do Teste	O tráfego é gerado a partir de Spirent, pode ser observado que os números solicitados neste edital foram alcançados no equipamento FGT 70D
Evidências	

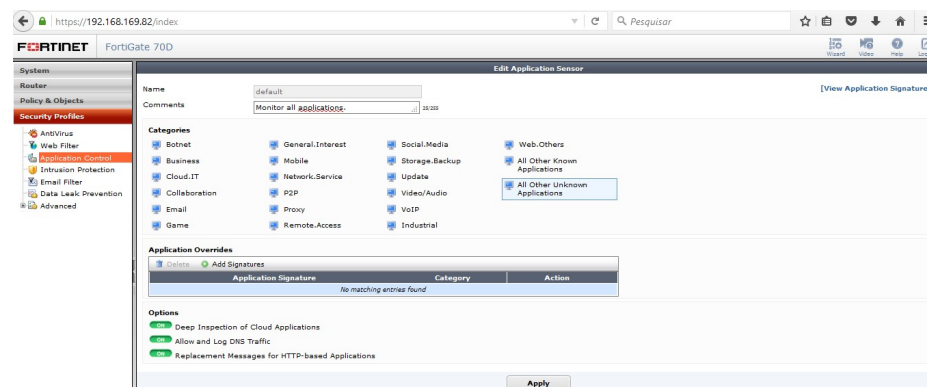


Equipamento alcançando throughput solicitado.



ID	Source	Destination	Schedule	Service	Action	Application Control
1	all	all	always	ALL	ACCEPT	default
2	all	all	always	ALL	ACCEPT	default
3	all	all	always	ALL	ACCEPT	default
4	all	all	always	ALL	ACCEPT	default
5	all	all	always	ALL	ACCEPT	default
6	all	all	always	ALL	ACCEPT	default
7	all	all	always	ALL	ACCEPT	default
8	all	all	always	ALL	ACCEPT	default

Regra de firewall

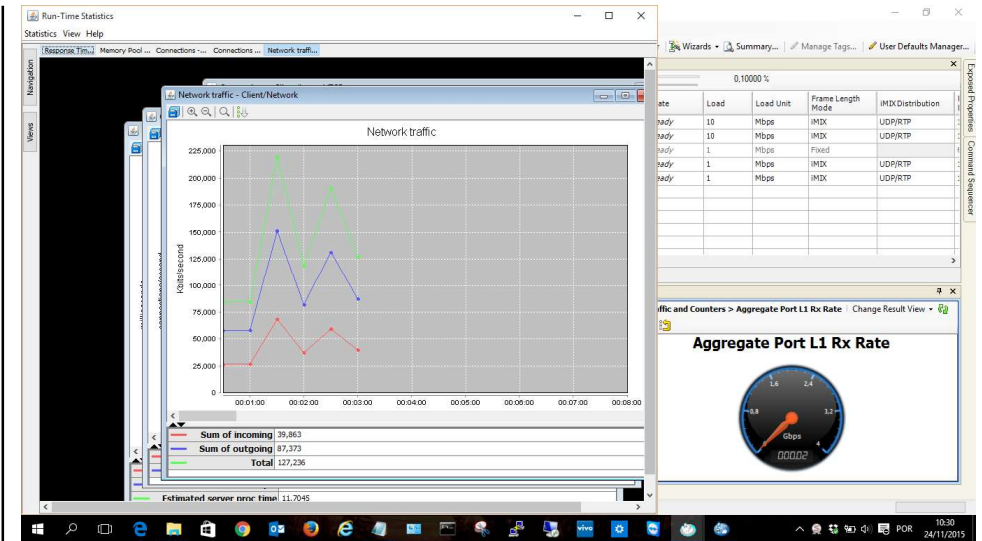


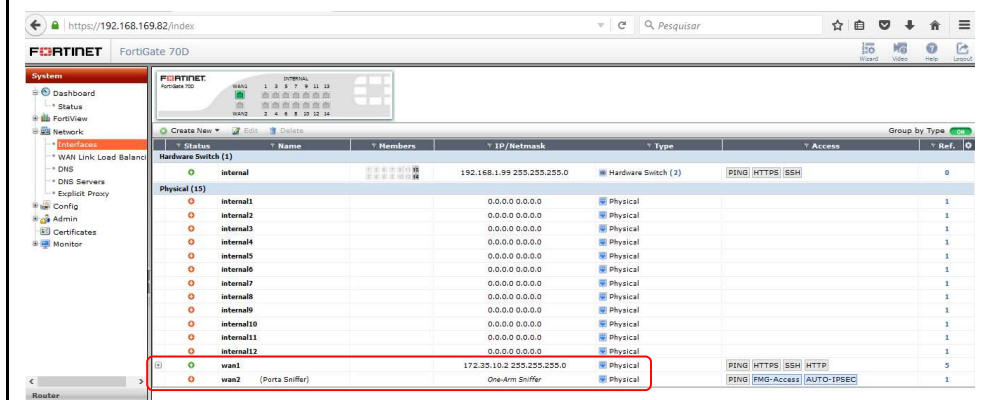
The screenshot shows the 'Edit Application Sensor' configuration page. The 'Name' field is set to 'default' and the 'Comments' field is set to 'Monitor all applications:'. The 'Categories' section is expanded, showing a list of application categories with checkboxes for selection. The 'Application Overrides' section is empty, and the 'Options' section is also empty.

Sensor de APPControl configurado

- Spirent

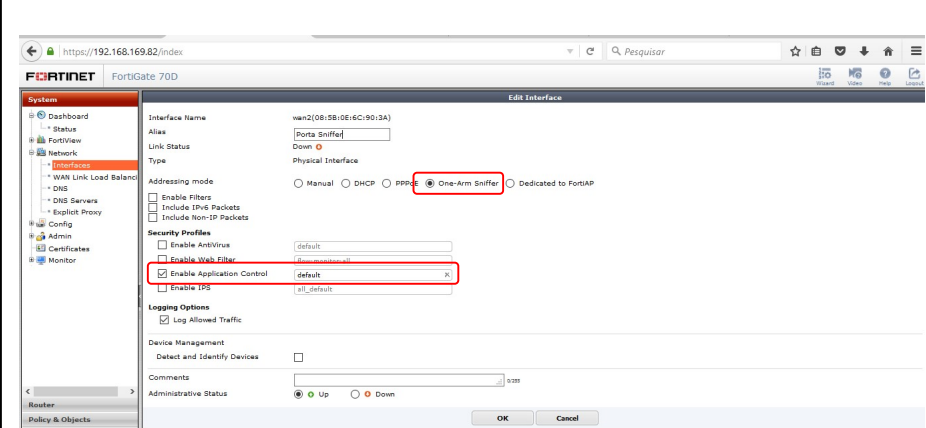
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 114/126

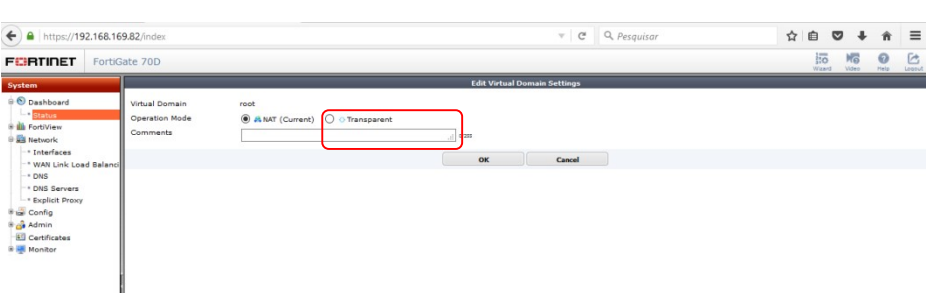
		
Comentário	Todas as configurações tanto do FGT 70D como do Spirent foram apresentadas/explicadas a todos os presentes na sala de homologação. Maiores detalhes sobre o relatório de tráfego gerado pelo spirent, podem ser encontrados no CD anexo a este caderno.	
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.7.2.17	Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer(monitoramento e análise do tráfego), camada 2 (L2) e camada 3 (L3);
Objetivo do Teste	Demonstrar funcionalidade de modo sniffer, L2 e L3
Configuração do Teste	Demonstrar modo one-arm-sniffer, transparent e router
Procedimento do Teste	System -> network -> interfaces / Status -> operation mode
Evidências	

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 115/126

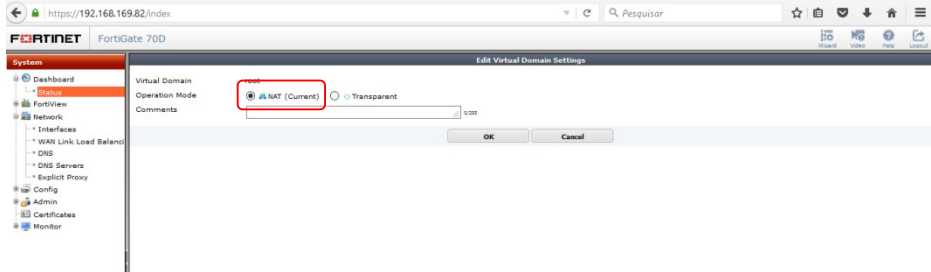
Comentário	
Assinatura do Cliente	Assinatura NCT

Item de Teste - 1.7.2.18	Modo sniffer, para inspeção via porta espelhada;	
Objetivo do Teste	Demonstrar funcionalidade de modo sniffer	
Configuração do Teste	Demonstrar modo one-arm-sniffer	
Procedimento do Teste	System -> network -> interfaces	
Evidências		
Comentário		
Assinatura do Cliente	Assinatura NCT	

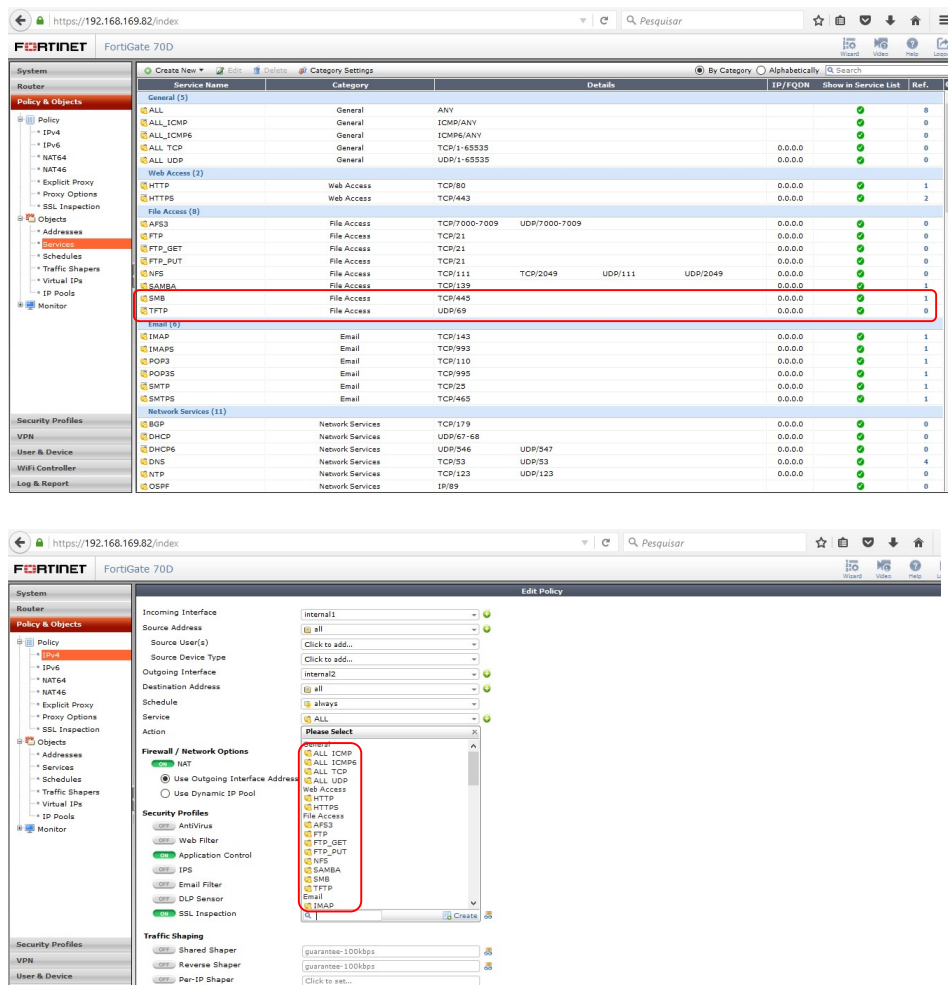
Item de Teste - 1.7.2.19	Modo L2, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;	
Objetivo do Teste	Demonstrar funcionalidade de L2 do equipamento	
Configuração do Teste	Demonstrar modo transparent	
Procedimento do Teste	Status -> operation mode	
Evidências		
Comentário		

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 116/126

Assinatura do Cliente		Assinatura NCT	
--------------------------	--	----------------	--

Item de Teste - 1.7.2.20	Modo L3, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação, operando como default gateway das redes protegidas;		
Objetivo do Teste	Demonstrar funcionalidade de L3 do equipamento		
Configuração do Teste	Demonstrar modo router		
Procedimento do Teste	Status -> operation mode		
Evidências			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.7.3.1	Controles de políticas por porta e protocolo;		
Objetivo do Teste	Demonstrar possibilidade de administração de portas e protocolos		
Configuração do Teste	Demonstrar formas de administração do firewall		
Procedimento do Teste	Firewall objects, address, service, policy		
Evidências			



FortiGate 70D - Policy & Objects

Service Name	Category	Details	IP/FQDN	Show in Service List	Ref.
General (5)					
ALL	General	ANY		0	8
ALL_ICMP	General	ICMP/ANY		0	0
ALL_ICMP6	General	ICMP6/ANY		0	0
ALL_TCP	General	TCP/1-65535	0.0.0.0	0	0
ALL_UDP	General	UDP/1-65535	0.0.0.0	0	0
Web Access (2)					
HTTP	Web Access	TCP/80	0.0.0.0	0	1
HTTPS	Web Access	TCP/443	0.0.0.0	0	2
File Access (8)					
AFS3	File Access	TCP/7000-7009	UDR/7000-7009	0.0.0.0	0
FTP	File Access	TCP/21		0.0.0.0	0
FTP_GET	File Access	TCP/21		0.0.0.0	0
FTP_PUT	File Access	TCP/21		0.0.0.0	0
NFS	File Access	TCP/111	TCP/2049	UDR/111	UDR/2049
SMB	File Access	TCP/139		0.0.0.0	1
SMB	File Access	TCP/445		0.0.0.0	1
TFTP	File Access	UDP/69		0.0.0.0	0
IMAP (8)					
IMAP	Email	TCP/143		0.0.0.0	1
IMAPS	Email	TCP/993		0.0.0.0	1
POP3	Email	TCP/110		0.0.0.0	1
POP3S	Email	TCP/995		0.0.0.0	1
SMTP	Email	TCP/25		0.0.0.0	1
SMTPS	Email	TCP/465		0.0.0.0	1
Network Services (11)					
BGP	Network Services	TCP/179		0.0.0.0	0
DHCP	Network Services	UDP/67-68		0.0.0.0	0
DHCP6	Network Services	UDP/546	UDR/547		0
DNS	Network Services	TCP/53	UDR/53		4
NTP	Network Services	TCP/123	UDR/123		0
OSPF	Network Services	IP/89		0.0.0.0	0

Edit Policy

Incoming Interface: internal1
Source Address: all
Source User(s): Click to add...
Source Device Type: Click to add...
Outgoing Interface: internal2
Destination Address: all
Schedule: always
Service: ALL
Action: Please Select

Firewall / Network Options

- ☒ Use Outgoing Interface Address
- ☐ Use Dynamic IP Pool

Security Profiles

- ☒ Antivirus
- ☒ Web Filter
- ☒ Application Control
- ☒ IPS
- ☒ Email Filter
- ☒ DLP Sensor
- ☒ SSL Inspection

Traffic Shaping

- ☐ Shared Shaper: guarantee-100Mbps
- ☐ Reverse Shaper: guarantee-100Mbps
- ☐ Per-IP Shaper: Click to set...

Comentário

Assinatura
do Cliente

Assinatura NCT

Item de Teste -
1.7.3.2

Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

Objetivo do
Teste

Demonstrar controle de aplicação

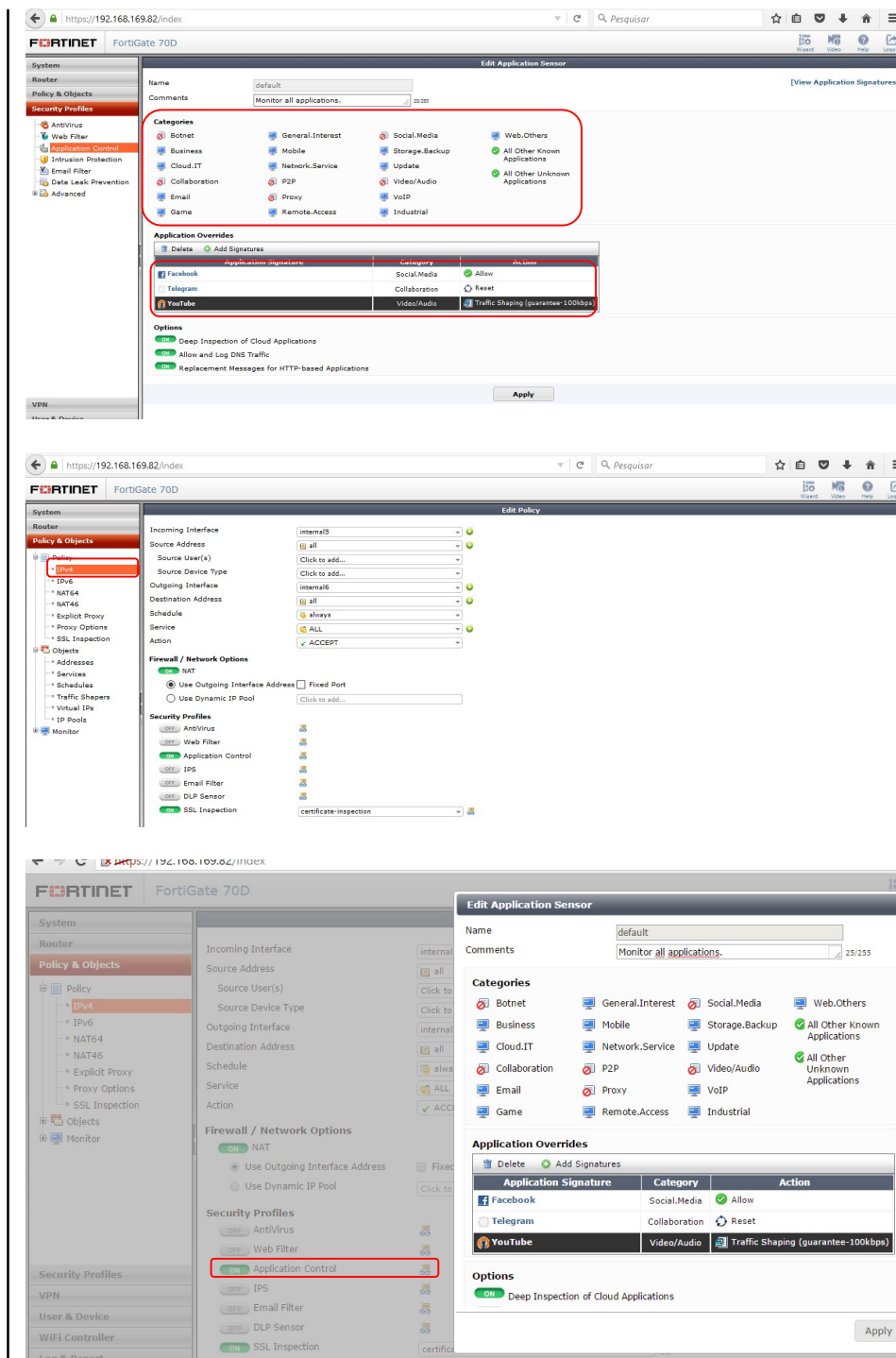
Configuração
do Teste

Demonstrar application control

Procedimento
do Teste

Security profiles -> application control

Evidências



The screenshots illustrate the configuration of application control on a FortiGate 70D. The first image shows the 'Edit Application Sensor' page where various application categories are listed. The second image shows the 'Edit Policy' page where the sensor is applied to a specific policy. The third image shows the 'Edit Application Sensor' page again, focusing on the 'Application Overrides' table which allows for specific actions (Allow, Reset, Traffic Shaping) for certain applications like Facebook, Telegram, and YouTube.

Comentário

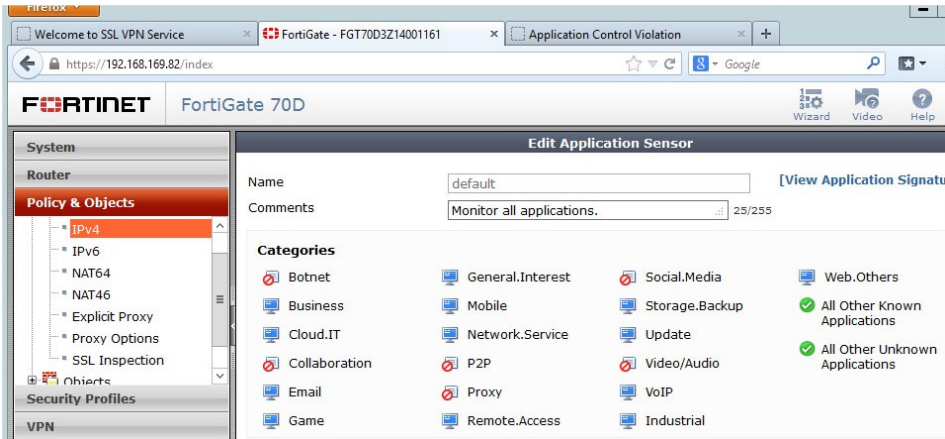
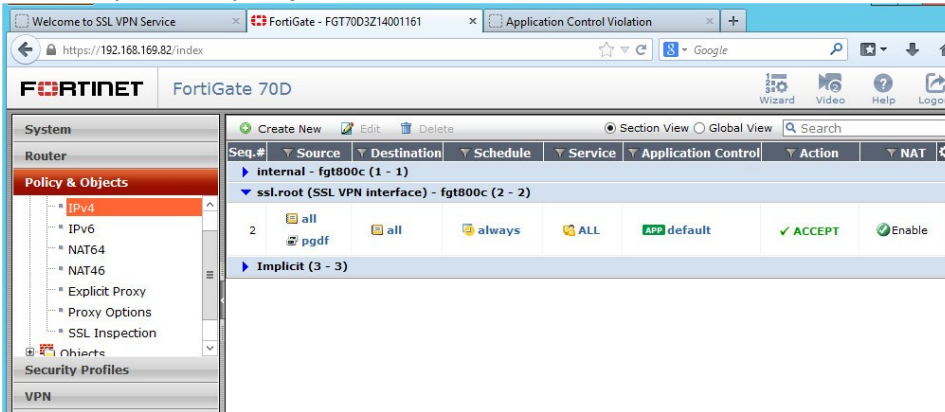
Assinatura
do Cliente

Assinatura NCT

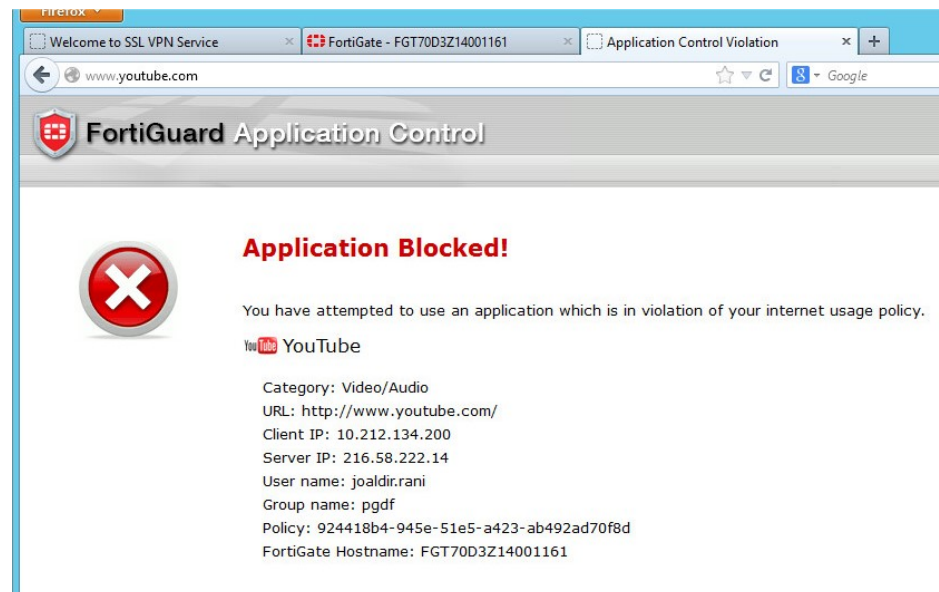
Item de Teste -
1.7.4.1.1.

Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

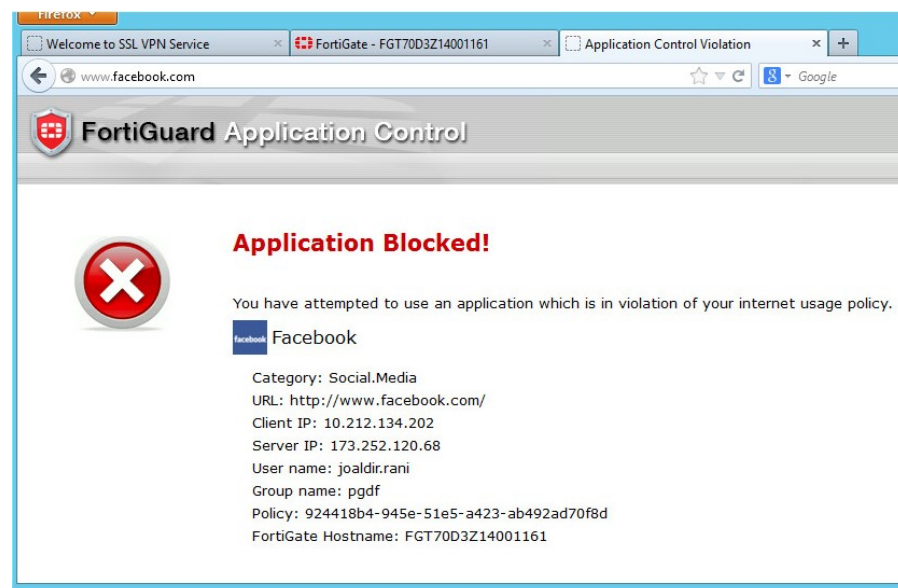
	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 119/126

Objetivo do Teste	Demonstrar controle de aplicação
Configuração do Teste	Configurado perfil de filtro de aplicação com bloqueios. Configurado regra de firewall permitindo todos serviços e com o perfil de filtro de aplicação.
Procedimento do Teste	Tentou acesso ao youtube, e recebeu o aviso de aplicação bloqueada. Tentou acesso ao facebook, e recebeu o aviso de aplicação bloqueada.
Evidências	 Perfil bloqueando aplicações como video/audio  Regra de firewall permitindo todos os serviços, o bloqueio somente é feito por aplicação.

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 120/126



Tela demonstra o bloqueio pela aplicação e não pela web.



Comentário		
Assinatura do Cliente	Assinatura NCT	

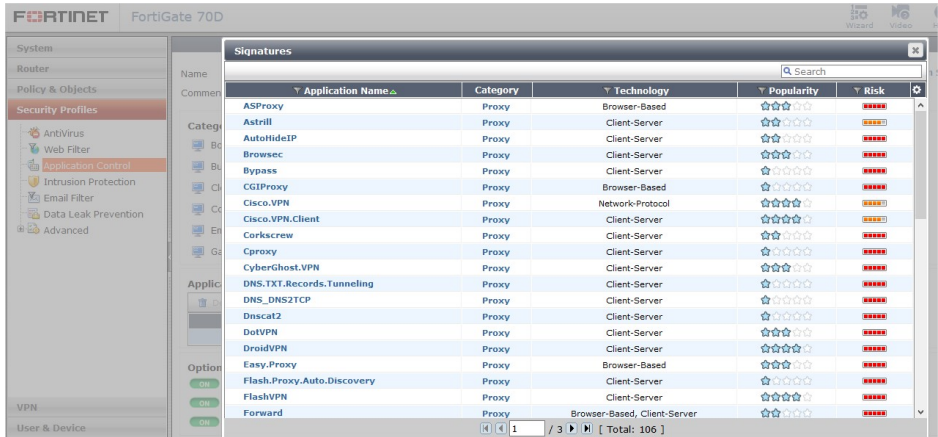
Item de Teste - 1.7.4.1.4	Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 389;
Objetivo do Teste	Demonstrar controle de aplicação

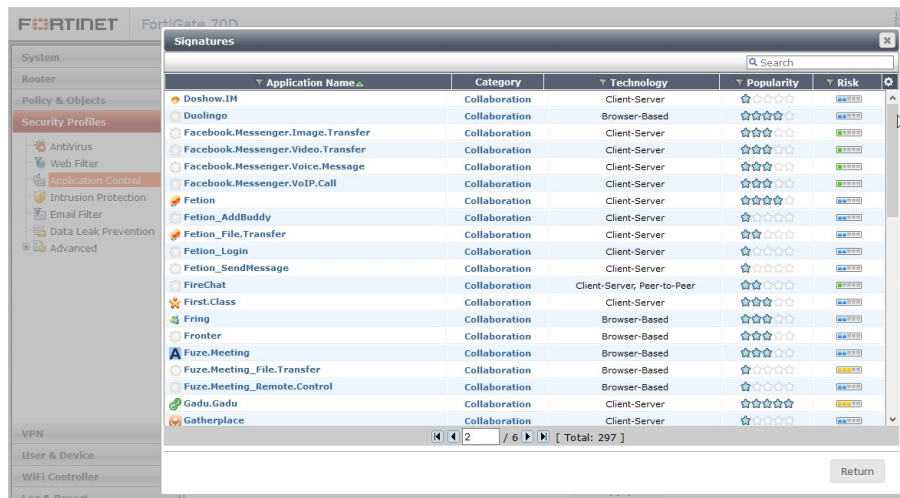
	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 121/126

Configuração do Teste	Configurado o perfil de controle de aplicação default. Configurado uma regra de firewall com o perfil de controle de aplicação default.																																																																																																																																																																																																						
Procedimento do Teste	De um cliente remote desktop tentou conexão 192.168.169.182:80 para a aplicação passar pela porta 80. De um cliente ssh(putty) colocou o ip 192.168.169.182:3389 para passar a aplicação na porta do remote desktop.																																																																																																																																																																																																						
Evidências	System Router Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller Log & Report Endpoint HA WiFi Security Log Antivirus Web Filter Application Control Intrusion Protection Anomaly Data Leak Prevention Log Config Monitor Application Name: rdp Add Filter <table><thead><tr><th>#</th><th>@</th><th>Date/Time</th><th>Source</th><th>Destination</th><th>Application Name</th><th>Action</th><th>Application User</th></tr></thead><tbody><tr><td>1</td><td></td><td>17:22:13</td><td>joaldir (10.69.70.65)</td><td>192.168.169.182</td><td>M RDP</td><td>pass</td><td></td></tr><tr><td>2</td><td></td><td>17:22:10</td><td>joaldir (10.69.70.65)</td><td>192.168.169.182</td><td>M RDP</td><td>pass</td><td></td></tr><tr><td>3</td><td></td><td>17:19:01</td><td>joaldir (10.69.70.65)</td><td>178.33.250.62</td><td>M RDP</td><td>pass</td><td></td></tr></tbody></table> 1 [Total: 9] <table><thead><tr><th>#</th><th>1</th><th>Action</th><th>pass</th></tr></thead><tbody><tr><td>Application Category</td><td>Remote.Access</td><td>Application Control List</td><td>default</td></tr><tr><td>Application ID</td><td>15511</td><td>Application Name</td><td>M RDP</td></tr><tr><td>Application Risk</td><td>*****</td><td>Date/Time</td><td>17:22:13</td></tr><tr><td>Destination</td><td>192.168.169.182</td><td>Destination Interface</td><td>port3</td></tr><tr><td>Destination Port</td><td>80</td><td>Event Type</td><td>app-ctrl-all</td></tr><tr><td>Group</td><td>joaldir</td><td>Level</td><td>*****</td></tr><tr><td>Log ID</td><td>28704</td><td>Message</td><td>Remote.Access: RDP,</td></tr><tr><td>Protocol</td><td>tcp</td><td>Protocol Number</td><td>6</td></tr><tr><td>Sequence Number</td><td>2171027</td><td>Service</td><td>HTTP</td></tr><tr><td>Source</td><td>joaldir (10.69.70.65)</td><td>Source Interface</td><td>port7</td></tr><tr><td>Source Port</td><td>1105</td><td>Sub Type</td><td>app-ctrl</td></tr></tbody></table> Detecção do Remote Desktop na porta 80 System Router Policy & Objects Security Profiles VPN User & Device WiFi & Switch Controller Log & Report Endpoint HA WiFi Security Log Antivirus Web Filter Application Control Intrusion Protection Anomaly Data Leak Prevention Log Config Monitor Add Filter Log location: Disk <table><thead><tr><th>#</th><th>@</th><th>Date/Time</th><th>Source</th><th>Destination</th><th>Application Name</th><th>Action</th><th>Application User</th><th>Application Details</th></tr></thead><tbody><tr><td>1</td><td></td><td>17:28:57</td><td>joaldir (10.69.70.65)</td><td>192.168.169.182</td><td>SSH</td><td>pass</td><td></td><td></td></tr><tr><td>2</td><td></td><td>17:27:01</td><td>joaldir (10.69.70.65)</td><td>46.43.34.31</td><td>HTTP.BROWSER_Firefox</td><td>pass</td><td></td><td>Firefox</td></tr><tr><td>3</td><td></td><td>17:26:43</td><td>joaldir (10.69.70.65)</td><td>212.13.197.229</td><td>HTTP.BROWSER_Firefox</td><td>pass</td><td></td><td>Firefox</td></tr><tr><td>4</td><td></td><td>17:26:43</td><td>joaldir (10.69.70.65)</td><td>212.13.197.229</td><td>HTTP.BROWSER_Firefox</td><td>pass</td><td></td><td>Firefox</td></tr><tr><td>5</td><td></td><td>17:26:35</td><td>joaldir (10.69.70.65)</td><td>212.13.197.229</td><td>HTTP.BROWSER_Firefox</td><td>pass</td><td></td><td>Firefox</td></tr></tbody></table> 1 / 2547 [Total: 127307] <table><thead><tr><th>#</th><th>1</th><th>Action</th><th>pass</th></tr></thead><tbody><tr><td>Application Category</td><td>Network.Service</td><td>Application Control List</td><td>default</td></tr><tr><td>Application ID</td><td>16060</td><td>Application Name</td><td>SSH</td></tr><tr><td>Application Risk</td><td>*****</td><td>Date/Time</td><td>17:28:57</td></tr><tr><td>Destination</td><td>192.168.169.182</td><td>Destination Interface</td><td>port3</td></tr><tr><td>Destination Port</td><td>3389</td><td>Event Type</td><td>app-ctrl-all</td></tr><tr><td>Group</td><td>joaldir</td><td>Level</td><td>*****</td></tr><tr><td>Log ID</td><td>28704</td><td>Message</td><td>Network.Service: SSH,</td></tr><tr><td>Protocol</td><td>tcp</td><td>Protocol Number</td><td>6</td></tr><tr><td>Sequence Number</td><td>2172019</td><td>Service</td><td>RDP</td></tr></tbody></table> Detecção de SSH sobre a porta 3389. FortiGate 70D Create New Edit Delete Section View Global View Search Wizard Video Help Logout System Router Policy & Objects Policy IPv4 IPv6 NAT64 NAT46 Explicit Proxy Proxy Options SSL Inspection internal - fgt800c (1 - 1) ssl.root (SSL VPN interface) - fgt800c (2 - 2) Implicit (3 - 3) <table><thead><tr><th>Seq.#</th><th>Source</th><th>Destination</th><th>Schedule</th><th>Service</th><th>Action</th><th>NAT</th><th>AV</th><th>Web Filter</th><th>Application Control</th><th>IPS</th></tr></thead><tbody><tr><td>2</td><td>all</td><td>all</td><td>always</td><td>ALL</td><td>ACCEPT</td><td>Enable</td><td>default</td><td>default</td><td>default</td><td>default</td></tr></tbody></table> Regra de firewall			#	@	Date/Time	Source	Destination	Application Name	Action	Application User	1		17:22:13	joaldir (10.69.70.65)	192.168.169.182	M RDP	pass		2		17:22:10	joaldir (10.69.70.65)	192.168.169.182	M RDP	pass		3		17:19:01	joaldir (10.69.70.65)	178.33.250.62	M RDP	pass		#	1	Action	pass	Application Category	Remote.Access	Application Control List	default	Application ID	15511	Application Name	M RDP	Application Risk	*****	Date/Time	17:22:13	Destination	192.168.169.182	Destination Interface	port3	Destination Port	80	Event Type	app-ctrl-all	Group	joaldir	Level	*****	Log ID	28704	Message	Remote.Access: RDP,	Protocol	tcp	Protocol Number	6	Sequence Number	2171027	Service	HTTP	Source	joaldir (10.69.70.65)	Source Interface	port7	Source Port	1105	Sub Type	app-ctrl	#	@	Date/Time	Source	Destination	Application Name	Action	Application User	Application Details	1		17:28:57	joaldir (10.69.70.65)	192.168.169.182	SSH	pass			2		17:27:01	joaldir (10.69.70.65)	46.43.34.31	HTTP.BROWSER_Firefox	pass		Firefox	3		17:26:43	joaldir (10.69.70.65)	212.13.197.229	HTTP.BROWSER_Firefox	pass		Firefox	4		17:26:43	joaldir (10.69.70.65)	212.13.197.229	HTTP.BROWSER_Firefox	pass		Firefox	5		17:26:35	joaldir (10.69.70.65)	212.13.197.229	HTTP.BROWSER_Firefox	pass		Firefox	#	1	Action	pass	Application Category	Network.Service	Application Control List	default	Application ID	16060	Application Name	SSH	Application Risk	*****	Date/Time	17:28:57	Destination	192.168.169.182	Destination Interface	port3	Destination Port	3389	Event Type	app-ctrl-all	Group	joaldir	Level	*****	Log ID	28704	Message	Network.Service: SSH,	Protocol	tcp	Protocol Number	6	Sequence Number	2172019	Service	RDP	Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	IPS	2	all	all	always	ALL	ACCEPT	Enable	default	default	default	default
#	@	Date/Time	Source	Destination	Application Name	Action	Application User																																																																																																																																																																																																
1		17:22:13	joaldir (10.69.70.65)	192.168.169.182	M RDP	pass																																																																																																																																																																																																	
2		17:22:10	joaldir (10.69.70.65)	192.168.169.182	M RDP	pass																																																																																																																																																																																																	
3		17:19:01	joaldir (10.69.70.65)	178.33.250.62	M RDP	pass																																																																																																																																																																																																	
#	1	Action	pass																																																																																																																																																																																																				
Application Category	Remote.Access	Application Control List	default																																																																																																																																																																																																				
Application ID	15511	Application Name	M RDP																																																																																																																																																																																																				
Application Risk	*****	Date/Time	17:22:13																																																																																																																																																																																																				
Destination	192.168.169.182	Destination Interface	port3																																																																																																																																																																																																				
Destination Port	80	Event Type	app-ctrl-all																																																																																																																																																																																																				
Group	joaldir	Level	*****																																																																																																																																																																																																				
Log ID	28704	Message	Remote.Access: RDP,																																																																																																																																																																																																				
Protocol	tcp	Protocol Number	6																																																																																																																																																																																																				
Sequence Number	2171027	Service	HTTP																																																																																																																																																																																																				
Source	joaldir (10.69.70.65)	Source Interface	port7																																																																																																																																																																																																				
Source Port	1105	Sub Type	app-ctrl																																																																																																																																																																																																				
#	@	Date/Time	Source	Destination	Application Name	Action	Application User	Application Details																																																																																																																																																																																															
1		17:28:57	joaldir (10.69.70.65)	192.168.169.182	SSH	pass																																																																																																																																																																																																	
2		17:27:01	joaldir (10.69.70.65)	46.43.34.31	HTTP.BROWSER_Firefox	pass		Firefox																																																																																																																																																																																															
3		17:26:43	joaldir (10.69.70.65)	212.13.197.229	HTTP.BROWSER_Firefox	pass		Firefox																																																																																																																																																																																															
4		17:26:43	joaldir (10.69.70.65)	212.13.197.229	HTTP.BROWSER_Firefox	pass		Firefox																																																																																																																																																																																															
5		17:26:35	joaldir (10.69.70.65)	212.13.197.229	HTTP.BROWSER_Firefox	pass		Firefox																																																																																																																																																																																															
#	1	Action	pass																																																																																																																																																																																																				
Application Category	Network.Service	Application Control List	default																																																																																																																																																																																																				
Application ID	16060	Application Name	SSH																																																																																																																																																																																																				
Application Risk	*****	Date/Time	17:28:57																																																																																																																																																																																																				
Destination	192.168.169.182	Destination Interface	port3																																																																																																																																																																																																				
Destination Port	3389	Event Type	app-ctrl-all																																																																																																																																																																																																				
Group	joaldir	Level	*****																																																																																																																																																																																																				
Log ID	28704	Message	Network.Service: SSH,																																																																																																																																																																																																				
Protocol	tcp	Protocol Number	6																																																																																																																																																																																																				
Sequence Number	2172019	Service	RDP																																																																																																																																																																																																				
Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	IPS																																																																																																																																																																																													
2	all	all	always	ALL	ACCEPT	Enable	default	default	default	default																																																																																																																																																																																													
Comentário																																																																																																																																																																																																							
Assinatura do Cliente	Assinatura NCT																																																																																																																																																																																																						

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 122/126

Item de Teste - 1.7.4.1.5	Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado;
Objetivo do Teste	Demonstrar uso de análise comportamental no equipamento
Configuração do Teste	Demonstrar regra de ips
Procedimento do Teste	Este item é comprovado com a documentação técnica enviada e apresentada no dia das demonstrações
Evidências	
Comentário	
Assinatura do Cliente	Assinatura NCT

Item de Teste - 1.7.4.1.19	Deve possibilitar a diferenciação de aplicações proxies (ghostsurf, freegate, dentre outros), Instant Messaging (AIM, Gtalk, Facebook Chat, dentre outros), peer-to-peer (Bittorrent, emule, neonet, dentre outros) permitindo um controle granular na configuração de políticas;
Objetivo do Teste	Demonstrar controle de aplicação
Configuração do Teste	Configurado o perfil de aplicação default para bloquear P2P, Collaboration(Instant Messenger), Proxy. Demonstrado o application overrides para a granularidade de opções. Configurado uma regra de firewall utilizando o perfil de aplicação.
Procedimento do Teste	O cliente windows xp tentou acesso ao facebook chat, utorrent e ultrasurf para certificar do bloqueio dos acessos.
Evidências	Lista de Aplicações  Proxies



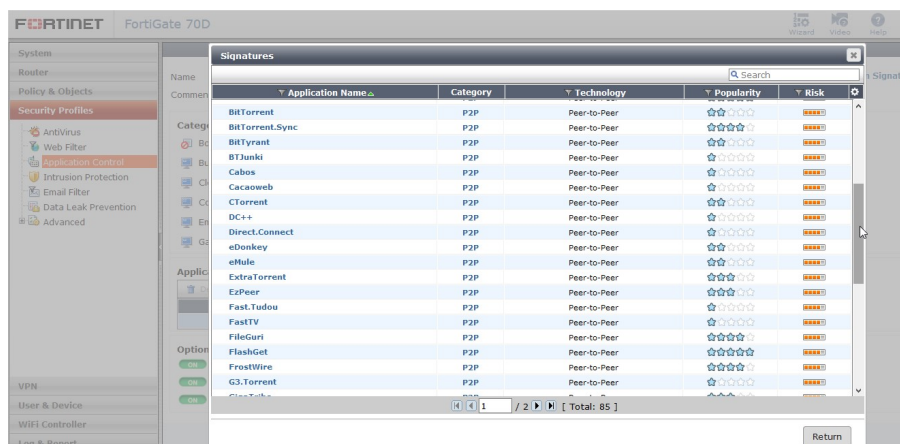
FortiGate 70D

Signatures

Application Name	Category	Technology	Popularity	Risk
Doshow.IM	Collaboration	Client-Server	☆☆☆☆☆	Low
Duolingo	Collaboration	Browser-Based	☆☆☆☆☆	Low
Facebook.Messenger.Image.Transfer	Collaboration	Client-Server	☆☆☆☆☆	Low
Facebook.Messenger.Video.Transfer	Collaboration	Client-Server	☆☆☆☆☆	Low
Facebook.Messenger.Voice.Message	Collaboration	Client-Server	☆☆☆☆☆	Low
Facebook.Messenger.VoIP.Call	Collaboration	Client-Server	☆☆☆☆☆	Low
Fetion	Collaboration	Client-Server	☆☆☆☆☆	Low
Fetion_AddBuddy	Collaboration	Client-Server	☆☆☆☆☆	Low
Fetion_File.Transfer	Collaboration	Client-Server	☆☆☆☆☆	Low
Fetion_Login	Collaboration	Client-Server	☆☆☆☆☆	Low
Fetion_SendMessage	Collaboration	Client-Server	☆☆☆☆☆	Low
FireChat	Collaboration	Client-Server, Peer-to-Peer	☆☆☆☆☆	Low
First.Class	Collaboration	Client-Server	☆☆☆☆☆	Low
Fring	Collaboration	Browser-Based	☆☆☆☆☆	Low
Frontier	Collaboration	Browser-Based	☆☆☆☆☆	Low
Fuze.Meeting	Collaboration	Browser-Based	☆☆☆☆☆	Low
Fuze.Meeting_File.Transfer	Collaboration	Browser-Based	☆☆☆☆☆	Low
Fuze.Meeting_Remote.Control	Collaboration	Browser-Based	☆☆☆☆☆	Low
Gadu.Gadu	Collaboration	Client-Server	☆☆☆☆☆	Low
Gatherplace	Collaboration	Client-Server	☆☆☆☆☆	Low

2 / 6 [Total: 297]

Collaboration (Instant Messenger)



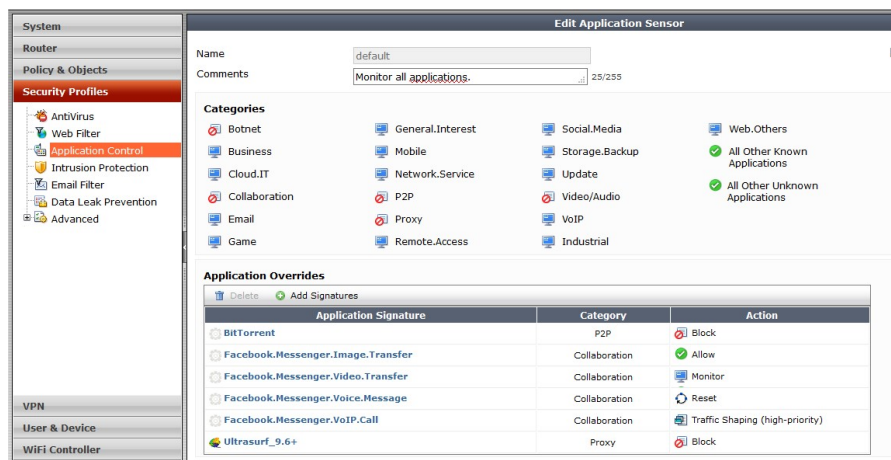
FortiGate 70D

Signatures

Application Name	Category	Technology	Popularity	Risk
BitTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	High
BitTorrent.Sync	P2P	Peer-to-Peer	☆☆☆☆☆	High
BitTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	High
BTJunkie	P2P	Peer-to-Peer	☆☆☆☆☆	High
Cabos	P2P	Peer-to-Peer	☆☆☆☆☆	High
CacaoWeb	P2P	Peer-to-Peer	☆☆☆☆☆	High
CTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	High
DC++	P2P	Peer-to-Peer	☆☆☆☆☆	High
Direct.Connect	P2P	Peer-to-Peer	☆☆☆☆☆	High
eDonkey	P2P	Peer-to-Peer	☆☆☆☆☆	High
eMule	P2P	Peer-to-Peer	☆☆☆☆☆	High
ExtrTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	High
EzPeer	P2P	Peer-to-Peer	☆☆☆☆☆	High
Fast.Tudou	P2P	Peer-to-Peer	☆☆☆☆☆	High
FastTV	P2P	Peer-to-Peer	☆☆☆☆☆	High
FileGuri	P2P	Peer-to-Peer	☆☆☆☆☆	High
FlashGet	P2P	Peer-to-Peer	☆☆☆☆☆	High
FrostWire	P2P	Peer-to-Peer	☆☆☆☆☆	High
G3.Torrent	P2P	Peer-to-Peer	☆☆☆☆☆	High

1 / 2 [Total: 85]

Pee-to-Peer



FortiGate 70D

Edit Application Sensor

Name: default

Comments: Monitor all applications. 25/255

Categories:

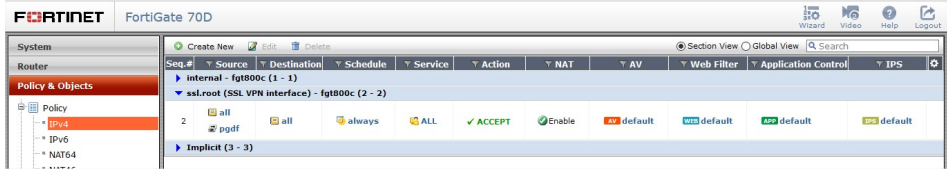
- Botnet
- Business
- Cloud.IT
- Collaboration
- Email
- Game
- General.Interest
- Mobile
- Network.Service
- P2P
- Proxy
- Remote.Access
- Social.Media
- Storage.Backup
- Update
- Video/Audio
- VoIP
- Industrial
- Web.Others
- All Other Known Applications
- All Other Unknown Applications

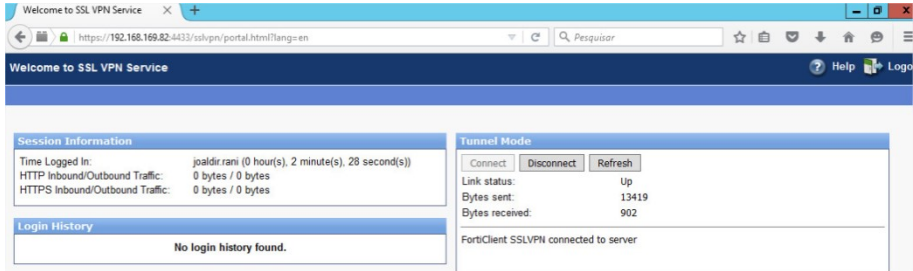
Application Overrides

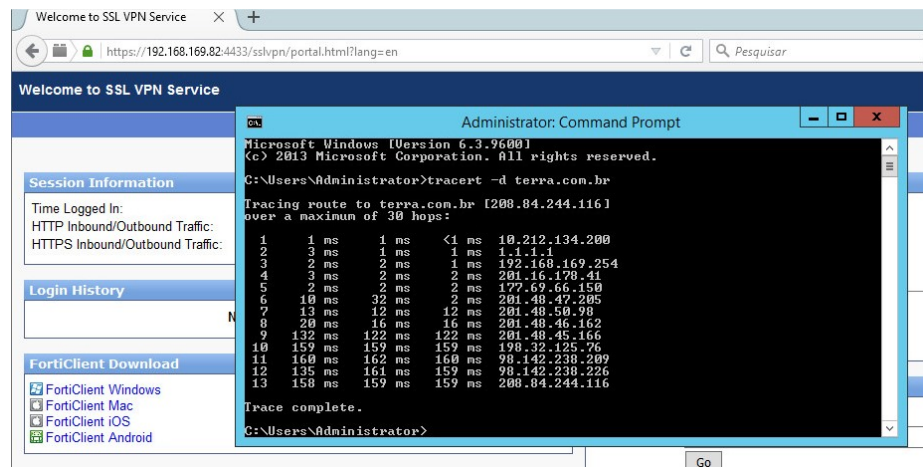
Application Signature	Category	Action
BitTorrent	P2P	Block
Facebook.Messenger.Image.Transfer	Collaboration	Allow
Facebook.Messenger.Video.Transfer	Collaboration	Monitor
Facebook.Messenger.Voice.Message	Collaboration	Reset
Facebook.Messenger.VoIP.Call	Collaboration	Traffic Shaping (high-priority)
Ultrastuff_9.6+	Proxy	Block

Perfil de controle de aplicação

	PREGÃO ELETRÔNICO Nº 04/2015	Revisão: 03
	CADERNO DE TESTES TÉCNICO	Página: 124/126

		
Comentário		
Assinatura do Cliente	Assinatura NCT	

Item de Teste - 1.7.5.6.6	Dever permitir criar políticas de controle de aplicações, IPS, antivírus, anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
Objetivo do Teste	Demonstrar regras de segurança
Configuração do Teste	Configurado um perfil de controle de aplicação, filtro de conteúdo, antivírus (função de spware incorporada) e sensor de IPS. Criado uma regra com todos os perfis e sensores.
Procedimento do Teste	Demonstrado o tunel em funcionamento com o usuário joaldir.rani que recebeu o ip 10.212.134.200. Demonstrado a ferramenta tracert para certificar que o trafego passa pelo túnel. Tentativa de acesso a um pagina e recebido pagina de bloqueio. Demonstrado as demais funcionalidades como bloqueio de aplicação, bloqueio de ataque, bloqueio de arquivos infectados, bloqueio de URL.
Evidências	 Tunel conectado



Administrator: Command Prompt

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

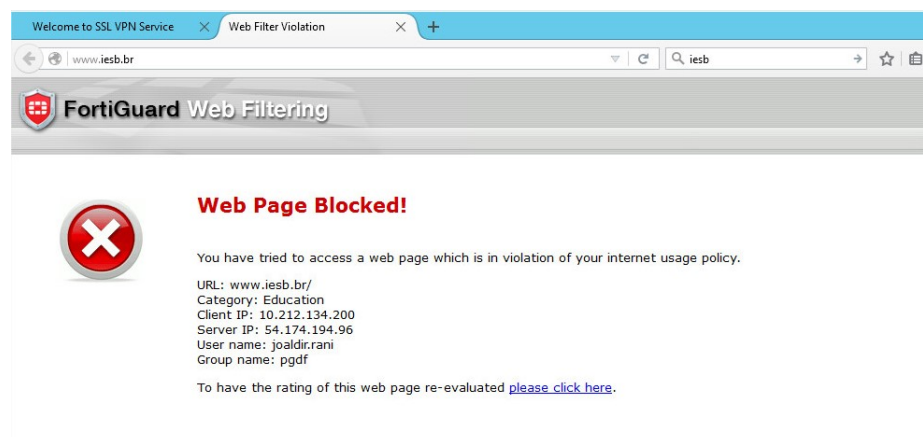
C:\Users\Administrator>tracert -d terra.com.br

Tracing route to terra.com.br [208.84.244.116]
over a maximum of 30 hops:
 0  0 ms  0 ms  0 ms  10.212.134.200
 1  1 ms  1 ms  1 ms  1.1.1.1
 2  3 ms  2 ms  1 ms  192.168.169.254
 3  2 ms  2 ms  2 ms  201.16.178.41
 4  3 ms  2 ms  2 ms  177.69.66.150
 5  2 ms  2 ms  2 ms  201.48.47.205
 6  10 ms  32 ms  2 ms  201.48.50.98
 7  13 ms  12 ms  12 ms  201.48.46.162
 8  20 ms  16 ms  16 ms  201.48.45.166
 9  132 ms  122 ms  122 ms  190.32.125.76
10  159 ms  159 ms  159 ms  98.142.238.209
11  160 ms  162 ms  160 ms  98.142.238.226
12  135 ms  161 ms  159 ms  208.84.244.116
13  158 ms  159 ms  159 ms  208.84.244.116

Trace complete.

C:\Users\Administrator>
```

Tracert



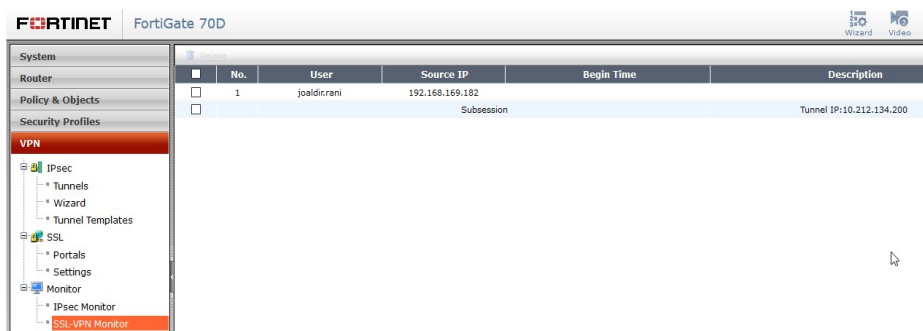
Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: www.iesb.br/
Category: Education
Client IP: 10.212.134.200
Server IP: 54.174.194.96
User name: joaldir.rani
Group name: pgdf

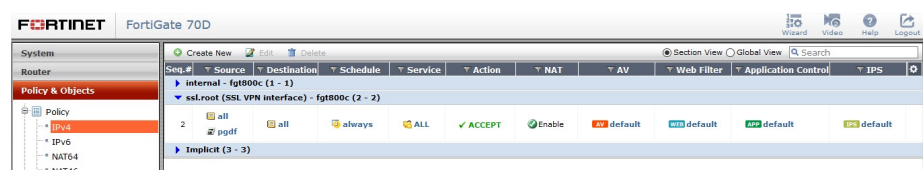
To have the rating of this web page re-evaluated [please click here](#).

Pagina de bloqueio



No.	User	Source IP	Begin Time	Description
1	joaldir.rani	192.168.169.182		
		Subsession		Tunnel IP: 10.212.134.200

Informações do tunel



Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	IPS
1	all	all	always	ALL	ACCEPT	Enable	default	default	default	default
2	pgdf	all	always	ALL	ACCEPT	Enable	default	default	default	default

Regra com os perfis de controle de aplicação, filtro de conteúdo, antivírus (função de spware incorporada) e sensor de IPS.

	PREGÃO ELETRÔNICO Nº 04/2015		Revisão: 03
	CADERNO DE TESTES TÉCNICO		Página: 126/126

Comentário			
Assinatura do Cliente		Assinatura NCT	